



**HBO-ICT: TICT-CV1BIPL-23**

**Basis**

**ICT-Platformen**

**Werkboek**

Versie 1.4.1 (voltijd)





[ Deze pagina is bewust leeg gelaten ]



# Inhoudsopgave

Toelatingseis Toets 2 .....	6
1 “Beter Medisch Centrum” (BMC) .....	7
2 Starten met Operating Systems .....	9
2.1 Voorbereiding .....	9
2.1.1 Introductie .....	9
2.1.2 Hardware .....	9
2.1.3 Software.....	9
2.1.4 Virtual Machines.....	10
2.1.5 IP-schema.....	11
2.1.6 Commandolijst.....	12
2.1.7 Voorbereiden op de theorie .....	12
2.2 Week 1, College 1: Windows Domain .....	13
2.2.1 Opdracht: 1 <sup>e</sup> Active Directory (AD) domain controller promoveren.....	14
2.2.2 Optioneel: 2 <sup>e</sup> (peer) domain controller (GUI) .....	16
2.2.3 Opdracht: Sub domein.....	16
2.2.4 Opdracht: client aan het domein toevoegen.....	17
2.2.5 Opdracht: Beheertools op client installeren.....	17
2.2.6 Opdracht: Organizational Units .....	17
2.2.7 Optioneel: 2 <sup>e</sup> peer domain controller verwijderen .....	18
2.2.8 Optioneel: Linux aan Active Directory (nadat Rocky Linux is geïnstalleerd!) .....	18
2.2.9 Vragen Active Directory .....	19
2.3 Week 1, College 2: Linux Installatie en Package Management.....	19
2.3.1 Inleiding .....	20
2.3.2 Opdracht: download de Rocky Linux 8 ISO .....	20
2.3.3 Opdracht: Maak de virtual machine aan .....	20
2.3.4 Opdracht: Handmatige installatie van Rocky Linux volgens profiel "Server with GUI" .....	21
2.3.5 Opdracht: Linux package management .....	23
2.3.6 Opdracht: Geautomatiseerde systeeminstallatie.....	27
2.3.7 Vragen Linux Installatie en Package Management.....	28
2.4 Week 2, College 1: Windows Core .....	28
2.4.1 Opdracht: Installatie van Windows Core .....	29
2.4.2 Opdracht: Basisconfiguratie met sconfig.....	29
2.4.3 Opdracht: Windows server Core Domain controller .....	30
2.4.4 Vragen Windows Core .....	30
2.5 Week 2, College 2: De Linux Shell .....	31



2.5.1	Opdracht 1: Kennismaking met de shell.....	32
2.5.2	Opdracht 2: scripting .....	35
2.5.3	Vragen Linux Shell.....	35
2.6	Week 3, College 1: Windows Gebruikers en Groepen.....	36
2.6.1	Opdracht: User Management met de GUI: ADAC.....	38
2.6.2	Opdracht: User Management met de GUI: ADUC .....	38
2.6.3	Opdracht: Command line tools Gebruikers importeren.....	38
2.6.4	Optioneel: Zelf importbestanden maken .....	39
2.6.5	Opdracht: Gebruikers importeren met powershell.....	39
2.6.6	Opdracht: Dsadd.....	40
2.6.7	Opdracht: Dsquery.....	40
2.6.8	Opdracht: Dsmod en Dsquery .....	40
2.6.9	Opdracht: Dsmove .....	41
2.6.10	Opdracht: Organizational Units .....	41
2.6.11	Opdracht: Homefolders .....	42
2.6.12	Opdracht: Profielen .....	42
2.6.13	Opdracht: Delegation of Control .....	42
2.6.14	Vragen Windows Gebruikers en Groepen .....	42
2.7	Week 3, College 2: Linux Gebruikers en Groepen .....	43
2.7.1	Opdracht: Gebruikers aanmaken.....	44
2.7.2	Opdracht: sudo .....	45
2.7.3	Vragen Linux Gebruikers en Groepen.....	45
2.8	Week 4, College 1: Windows bestandssystemen .....	46
2.8.1	Opdracht: voorbereiden van de basisomgeving.....	47
2.8.2	Opdracht: Aanmaken mappenstructuur en bijbehorende shares.....	47
2.8.3	Opdracht: Toevoegen van shares met verschillende rechten .....	48
2.8.4	Opdracht: Een share maken op een Core systeem.....	48
2.8.5	Opdracht: Toevoegen van beperkte rechten.....	49
2.8.6	Vragen Windows bestandssystemen.....	49
2.9	Week 4, College 2: Linux bestandssystemen.....	49
2.9.1	Opdracht: bestandsrechten .....	50
2.9.2	Opdracht: Harde schijf toevoegen (storage hardware toevoegen).....	52
2.9.3	Opdracht: Filesystems maken.....	52
2.9.4	Opdracht: Logical Volume Manager (LVM) Volumes aanmaken en in gebruik nemen.....	53
2.9.5	Opdracht: bestandspermissies en symbolic links .....	53
2.9.6	Vragen Linux bestandssystemen .....	54
2.10	Week 5, College 1: Core Network Services: DHCP/DNS.....	55



2.10.1	Opdracht: Inrichten van de basisomgeving .....	56
2.10.2	Opdracht: Linux DHCP Server .....	57
2.10.3	Opdracht: Windows DHCP Server.....	57
2.10.4	Opdracht: Windows DNS Server .....	58
2.10.5	Opdracht: Linux DNS Server.....	58
2.10.6	Vragen DHCP en DNS.....	61
2.11	Week 5, College 2: Application Services: HTTP/SMB.....	61
2.11.1	Opdracht: Installatie van een Linux webserver .....	62
2.11.2	Opdracht: Installeer Internet Information Server (IIS) onder Windows.....	63
2.11.3	Opdracht: Maak een Windows Shared Folder.....	64
2.11.4	Opdracht: Maak een Linux SMB share.....	65
2.11.5	Vragen SMB en Webserver.....	66
2.12	Week 6, College 1: Windows Group Policies .....	66
2.12.1	Opdracht: Aanmaken van verschillende group policies .....	67
2.12.2	Opdracht: Linken GPO aan de juiste OU.....	68
2.12.3	Opdracht: Hiërarchie en enforcement. ....	69
2.12.4	Opdracht: Controleer de juiste werking. ....	69
2.12.5	Opdracht: Backup/Restore .....	69
2.12.6	Opdracht: Folder Redirection .....	70
2.12.7	Opdracht: Administrative Templates.....	70
2.12.8	Opdracht: Deploy Software .....	71
2.12.9	Opdracht: Central Store.....	71
2.12.10	Opdracht: Preferences.....	71
2.12.11	Vragen Group Policies.....	71



# Inleiding

Besturingssystemen leer je pas echt goed kennen door ermee te werken op basis van “echte” praktijksituaties. Dat is precies wat we gaan doen deze cursus en dit werkboek helpt je erbij. Je vindt in dit document alle opdrachten die horen bij deze cursus. Elke les heeft ongeveer dezelfde opbouw:

- **Vorbereiding:** De docent gaat er vanuit dat je deze opdrachten hebt gedaan voordat je naar school gaat om het college bij te wonen.
- **Werkcollege 1:** Deze opdrachten mag je alvast thuis maken, maar dat hoeft niet: Je maakt deze opdrachten tijdens het college om de lesstof die de docent dan uitlegt gelijk te oefenen tijdens de les. Het is te veel werk om af te krijgen tijdens de les, dus thuis afmaken.
- **Werkcollege 2:** Zie “College 1”.
- **x.y.z. Opdracht:** Door het maken van de opdracht verwerk je de lesstof van die week, ga je steeds beter programmeren en zorg je ervoor dat je niet zo snel vergeet wat je hebt geleerd. Elke opdracht is genummerd.
- **x.y.z. Extra uitdagende Opdracht:** Deze opdrachten zijn bedoeld voor studenten die al veel kennis hebben van Windows en Linux, of voor studenten die een hoge score op de formatieve toetsen hebben gehaald.

Het is de bedoeling dat je de opdracht 2.1 die staat bij **Week 1** uitvoert **voordat** je op school komt om de lessen te volgen. Dit is dus de voorbereiding van deze cursus.

We gaan er vanuit dat je gebruik kunt maken van een eigen laptop. In beperkte mate kan je ook gebruik maken van de computers op school.

Heel zelden komt een student in aanmerking voor vrijstelling voor deze cursus. De informatie hierover vind je in een bijlage bij dit document.

## Toelatingseis Toets 2

Bij elke week van deze cursus hoort een opdracht (deze vind je terug op de *start/modules* pagina van Canvas, onderaan elke week met de naam "Practicum week 1" t/m "Practicum week 6". Je kunt ook rechtstreeks naar de *opdrachten* pagina navigeren). Verdeeld over deze 6 opdrachten moeten in totaal 12 screenshots worden ingeleverd.

Omdat de organisatie van de praktijktoets nogal arbeidsintensief is en deelname alleen zin heeft als je goed voorbereid bent, stellen we voor deelname aan de praktijktoets een toelatingseis:

- van de hierboven genoemde screenshots moeten er in ieder geval 9 door ons positief zijn beoordeeld (aan elk screenshot is in Canvas een punt verbonden, heb je meer dan 9 punten behaald dan mag je deelnemen aan de praktijktoets).

Deze eis geldt niet voor studenten die de cursus al in een eerder jaar gevolgd hebben, al is het ook voor hen zeer raadzaam om de opdrachten te maken (we zullen ook door hen ingezonden screenshots natuurlijk bekijken; als je beter presteert met een stok achter de deur, dan mag je met je eigen docent afspreken dat de norm ook voor jou geldt ondanks dat je in een eerder jaar aan de cursus begonnen bent).

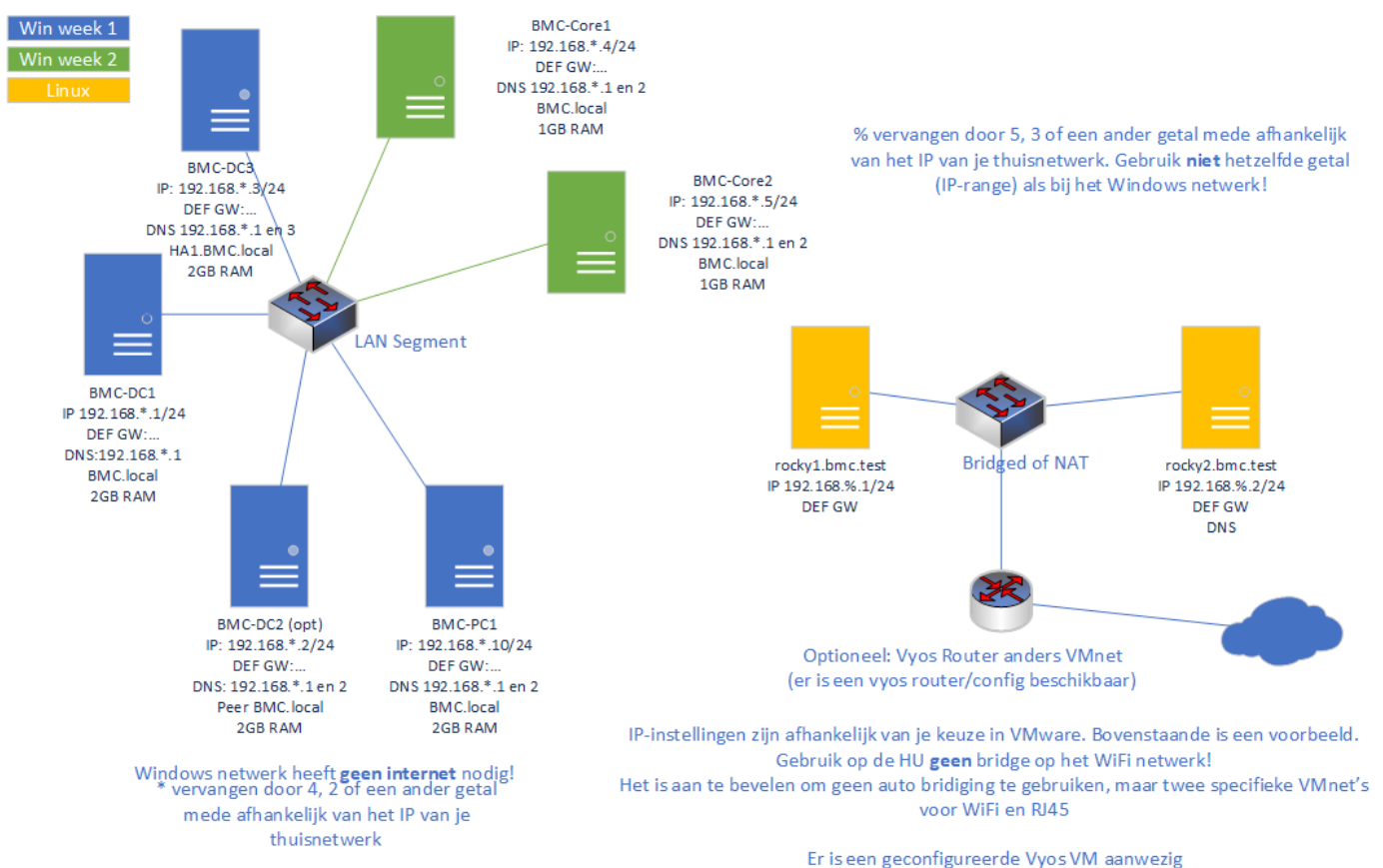
Voor deelname aan de herkansing van de praktijktoets in periode D geldt voor alle studenten de volgende eis:

- of je hebt eerder mogen deelnemen aan de praktijktoets
- of je hebt meer dan 9 punten behaald op een alternatieve verzameling van 12 screenshots die na de praktijktoets in periode C via een afzonderlijke opdracht gepubliceerd wordt.



# 1 “Beter Medisch Centrum” (BMC)

Bij het ontwerpen van deze cursus is gekeken naar de handelingen die een systeembeheerder zal moeten uitvoeren om een serveromgeving in te richten. Daarbij wordt ervan uitgegaan dat kennis en vaardigheden nog beperkt zijn. In de weekopdrachten (leertaak) zal daarom veelvuldig gebruik worden gemaakt van ondersteunende informatie om het leren zo optimaal mogelijk te laten verlopen. Samen met de *just-in-time* informatie moet het de student hulp bieden bij het uitvoeren van de verschillende taken. Bij de ondersteunende en de *just-in-time* informatie moet worden gedacht aan verwijzingen naar het boek, video's, specifieke student gerichte feedback van de docent maar ook aan de uitleg tijdens de hoor- en werkcolleges. Om ook de studenten met een MBO ICT achtergrond uitdaging te bieden zijn een aantal uitdagende, optionele, opdrachten gedefinieerd (die natuurlijk desgewenst door elke student mogen worden uitgevoerd).



FIGUUR 1 NETWERKTEKENING

Aan de basis van de cursus staat de inrichting van een netwerk voor een gezondheidscentrum in een nieuwbouwwijk. In de cursus “Netwerken” wordt gewerkt aan de infrastructuur die nodig is om de gebruikers, zoals huis- en tandartsen, met de servers te laten communiceren. In deze cursus (Basis ICT-Platformen) is er aandacht voor het inrichten van verschillende servers die nodig zijn om de verschillende medische diensten in het gezondheidscentrum goed te laten verlopen. Om een compleet beeld te geven: het gezondheidscentrum biedt onderdak aan drie huisartsen, twee tandartsen, een verloskundige praktijk, een fysiotherapeut en een apotheek. Om het netwerk in te richten en te onderhouden zijn er twee netwerk-/ systeembeheerders aangenomen.

De onderwerpen die in deze cursus aan bod gaan komen hebben een standaard thema gekregen.



De onderwerpen staan in Tabel 1. De tabel is hieronder weergegeven.

TABEL 1 WEEKOVERZICHT

	ALGEMEEN / Thema	WINDOWS	LINUX
Week 1	Start (Installation & Basic network)	Active Directory	installatie/package management
Week 2	Command line	core	shell
Week 3	User management	users / groups	
Week 4	Opslag	NTFS	filesystems
Week 5	Services	DHCP/DNS/HTTP/SMB	
Week 6	Overig	policies	n.v.t.





# 2 Starten met Operating Systems

## 2.1 Voorbereiding

### 2.1.1 Introductie

Bij de labs maken we gebruik van Rocky Linux 8 (een gratis alternatief dat vergaand compatibel is met Red Hat Enterprise Linux 8 maar zonder dat een abonnement onderhouden hoeft te worden), Windows Server (2016 of 2019), Windows 10 en software voor virtualisatie. We gaan er vanuit dat je deze omgeving hebt ingericht als je de eerste les krijgt.

Hieronder staat hoe je de benodigde voorbereidingen kunt treffen.

Hoewel er verschillende mogelijkheden zijn geven wij de voorkeur aan de onderstaande configuratie:

**Je eigen laptop met 16 GB of meer geheugen, een interne (HDD of) SSD in combinatie met een externe USB 3.0 (HDD of) SSD (totaal 200 GB vrije ruimte) en “VMware Workstation Pro” 16 of 17 voor Windows heeft de voorkeur!**

Bij sommige opdrachten zullen de stappen die je moet volgen om het doel te bereiken vrij nauwkeurig zijn uitgewerkt en leer je vooral de handelingen uit te voeren, om andere opdrachten tot een goed einde te brengen zal je meer zelf uit moeten zoeken. Ook voor dit laatste is bewust gekozen, aangezien dit een vaardigheid die in het werkveld van een CSC-er wordt verwacht en daarnaast in het algemeen een onderzoekende houding verwacht wordt van iemand die op HBO-niveau functioneert

Heb je nog vragen? Stel ze gerust aan je docent.

### 2.1.2 Hardware

De opdrachten worden door de meeste studenten gemaakt op een laptop. Het is in beperkte mate mogelijk om hardware van school te gebruiken, maar dat heeft als nadeel dat we niet kunnen garanderen dat er een computer beschikbaar is op het moment dat je les hebt. Bovendien zal je door de beperkte lengte van de lessen de weekopdrachten meestal niet afkrijgen tijdens de les. Met je laptop kan je thuis verder werken en hoef je niet opnieuw te beginnen. Aan de laptop zijn wel een aantal specifieke eisen verbonden (die je eerder al kon terugvinden in de studiegids):

- Voldoende geheugen: minimaal 16 GB RAM (zie studiegids), dus ook een x64 besturingssysteem. In de praktijk is nog meer geheugen mooi meegenomen (hoe meer geheugen, hoe meer VM's je naast elkaar kunt draaien);
- CPU (x64) en BIOS moeten Intel VT-x of AMD-V ondersteunen. Een mid-range CPU is voor de rekenkracht voldoende;
- Harde schijf met voldoende snelheid en omvang. Een extra interne of externe SSD met een USB3/(E)SATA/M2 aansluiting heeft prestatievoordelen. Je kan in dat geval de virtuele machines (VM's) over de verschillende schijven verdelen.

De keuze van een goede laptop (merk en type) zal de HU niet voorschrijven. Dit is sterk afhankelijk van persoonlijke voorkeur, de markt en natuurlijk van je eigen budget.

### 2.1.3 Software

Op je laptop bouwen we een klein netwerkje bestaande uit verschillende systemen. Dat kan doordat we gebruik maken van virtualisatie software. Als je deze software hebt geïnstalleerd dan kan je daarna verschillende besturingssystemen (VM's) tegelijkertijd gebruiken op je laptop.



We adviseren je gebruik te maken van de meest recente versie van VMware Workstation Pro. Deze virtualisatie software heeft een aantal voordelen:

- Eenvoudig in gebruik en bij de configuratie,
- Ook de computers in het lab zijn voorzien van VMware Workstation,
- Licenties gratis verkrijgbaar via school (via website [VMware IT Academy](https://www.vmware.com/academy)),

Het staat je overigens vrij om gebruik te maken van andere virtualisatiesoftware zoals Hyper-V, XEN, ESXi, Parallels, KVM of VirtualBox. De docenten zullen je dan niet altijd kunnen ondersteunen in geval van problemen.

## 2.14 Virtual Machines

### Windows Client en Server | Linux

De virtuele omgeving is vrij uitgebreid. Voor het maken van alle opdrachten heb je de volgende virtuele machines (minimaal) nodig:

- 3 à 4 x Windows Server 2016 of 2019 GUI servers,
- 2 x Windows Server 2016 of 2019 Core servers,
- 2 à 3 x Windows 10 client (geen Windows 11!),
- 2 à 3 x Rocky Linux 8 systemen; deze zullen tijdens de eerste weekopdracht geïnstalleerd worden dus klaarzetten van de 'kale' VM's is nu genoeg (1536 MB geheugen, 20 GB disk\*).

Niet alle systemen hoeven tegelijkertijd gebruikt te worden. Je bent zelf verantwoordelijk voor het creëren van de juiste omgeving, maar we helpen je wel een beetje op weg!

#### **Optie 1: Alles zelf installeren (voorwaarde: je hebt een paar honderd GB vrije ruimte op je harddisk).**

*Dit is een makkelijke oplossing waar je veel van leert omdat je alles zelf doet, maar kost je veel schijfruimte en veel tijd om in te richten.*

*Windows software downloaden:*

Ga naar de Azure for Students website (<https://aka.ms/startEDU>). De toegang tot deze site is gekoppeld aan je HU account.

Download daar:

1. Windows Server 2016 Datacenter, 64-bit (English)  
*of*  
Windows Server 2019 Datacenter (updated Sept 2019), 64-bit (English)
2. Windows 10 Education, Version 21H1 – DVD, 64-bit (English)  
*of*  
Windows 10 Education N, Version 21H1 – DVD, 64-bit (English)

*Installatie:*

We installeren alle systemen in de originele taal, het Engels. Installatie in het Nederlands leidt alleen maar tot verwarring doordat de vertalingen niet altijd even voor de hand liggend zijn; het is in het werkveld daarom goed gebruik om bij het Engels te blijven.

- Installeer 2 verschillende Windows Server Core (dat is de default) systemen, hiervoor gebruik je image 1 hierboven en selecteert de optie “Windows Server 2016/2019 Datacenter”.

---

\* Zie <https://access.redhat.com/articles/rhel-limits>



- Installeer daarna 3 of 4 Windows Server GUI (dus met een grafische interface) systemen, hiervoor gebruik je image 1 hierboven en selecteert de optie “Windows Server 2016/2019 Datacenter (Desktop Experience)”.
- Installeer daarna 2 of 3 Windows 10 Client systemen, hiervoor gebruik je image 2 hierboven.

### Optie 2: Zelf installeren gebruik makend van “Linked Clones”.

*Dit is iets lastiger, gaat uiteindelijk wat sneller dan de vorige optie en kost minder schijfruimte. We gebruiken hier [Linked Clones](#). Hierbij zijn de VM's opgebouwd als Parent/Child disks.*

Het besturingssysteem wordt hierbij eenmaal geïnstalleerd (Parent; zie de vorige optie) en vervolgens worden er een aantal nieuwe virtuele machines aangemaakt op basis van de parent. Dit zijn de childs. Deze child-machine schrijven alleen de wijzigingen ten op zichte van de parent op de “eigen harde schijf”. Een belangrijk voordeel is dat de totale omvang van alle schijven minder wordt. Nadeel is dat de prestaties iets verminderen. Door de parent en child-machine over verschillende (interne en/of externe) schijven te verdelen kunnen de beperkingen in de prestaties worden verminderd.

*Windows software downloaden:*

Zie de vorige optie.

*Installatie:*

1. Installeer eerst één Windows Core Server, één Windows Server GUI, één Windows Client systeem zoals beschreven bij de vorige optie.
2. Zorg op alle systemen voor de juiste datum/tijd.
3. Zet op alle Windows systemen Windows update “uit” (dat doe je natuurlijk alleen in een testomgeving).
4. Start daarna (in je VM's, niet op je laptop zelf!) C:\windows\system32\sysprep\sysprep.exe. Kies voor “OOBE” en zet een vinkje bij “Generalize” en kies “Shutdown”. Klik dan op OK en wacht tot je systeem “down” gaat.

*Als je geen sysprep gebruikt zal dat leiden tot hele “vreemde” situaties bij het uitvoeren van de opdrachten.*

5. Je base disk is nu klaar. Deze kan je gebruiken om op basis daarvan zelf nieuwe virtuele machines (clones) aan te maken.

Zie hiervoor tutorials op Internet of bekijk een filmpje zoals: <https://www.youtube.com/watch?v=x-OdUN9N7H8> (de video gaat uit van oudere software versies, maar de procedure is nog steeds hetzelfde).

Op deze manier maak je een kopie van je systeem en daarmee extra Windows systemen.

*De base-systemen moet je **nooit** meer starten!*

## 2.1.5 IP-schema

Je mag in het netwerk zelf een IP-range kiezen. Het advies is om de 192.168.4.0/24 range te gebruiken, waarbij je de lage nummers voor de verschillende servers gebruikt en de hoge nummers voor de clients. Noteer in het onderstaande schema de instellingen die je gaat gebruiken. Het kan handig zijn om het Excel bestand “IP-schema.xlsx” dat op Canvas staat te gebruiken, dan kun je het snel bekijken terwijl je met de opdrachten bezig bent.

Servernaam	IP adres	Subnet masker	DNS server	Default gateway
BMC-DC1	10.10.10.1	255.255.255.0	1.1.1.1	10.10.10.0
BMC-DC2				




## 2.16 Commandolijst

Gebruik de onderstaande lijst om commandline tools onder Windows en Linux op te schrijven zodat je ze makkelijk terug kan vinden!

Commando	Optionele opties / syntax	Voorbeeld	Wat doet het

## 2.17 Voorbereiden op de theorie

Bij deze cursus worden twee boeken gebruikt als verplichte literatuur:

Titel	Auteur(s)	ISBN
Unix And Linux System Administration Handbook, 5th Edition	Evi Nemeth, Garth Snyder, Trent R. Hein, Ben Whaley, Dan Mackin et al	978-0-13-427755-4
Windows Server 2016 Unleashed	Rand Morimoto, Jeffrey Shapiro, Guy Yardeni, Omar Droubi, Michael Noel	978-0-13-458375-4



In *Windows Server 2016 Unleashed* worden regelmatig screenshots gebruikt om te laten zien hoe iets moet worden uitgevoerd, *UNIX and Linux System Administration Handbook, 5th Edition* is meer op de command line gericht (de boeken passen in dat opzicht goed bij de respectievelijke besturingssystemen waar zij zich op richten).

Lees ter voorbereiding de volgende paragraaf van *UNIX and Linux System Administration Handbook, 5th Edition* om de verschillende command line voorbeelden beter te kunnen begrijpen: *1.5 Notation and typographical conventions* (blz. 12/13).

## 2.2 Week 1, College 1: Windows Domain

### Inleiding

In dit deel van het college ga je de centrale server(s) inrichten waarin alle gebruikersaccounts worden opgeslagen (zie netwerktekening Figuur 1). Zo'n server wordt een *domain controller (DC)* genoemd. Zoals in het college, het boek en de onderstaande video's is, of wordt, besproken kun je met de DC veel meer dan alleen maar de gebruikers opslaan. In latere colleges ga je een groot deel van de mogelijkheden ook bekijken.

Om te beginnen ga je in deze opdracht een *domain-tree* opzetten. Deze *domain-tree* bestaat uit een: *domain controller*, een *peer domain controller* en een subdomein. In de gecreëerde omgeving ga je daarna een client computer toevoegen, een OU aanmaken en beheertools installeren. Een optionele opdracht moet het mogelijk maken om Linux systemen op te nemen in het domein. Deze opdracht in z'n geheel zal de basis vormen voor de andere colleges.

### Theorie:

#### Verplicht:

- Slides,
- Dit werkboek met vragen en antwoorden (zie afzonderlijk document "Antwoorden\_BIPL\_Werkboek\_v1.4.0vt"!)
- Boek: "Windows Server 2016 Unleashed":
  - Hoofdstuk 1, *Windows Server 2016 Technology Primer*:
    - *Versions of Windows Server 2016 tot Improvements for Continuous Availability* (blz. 18 t/m 22)
  - Hoofdstuk 4, *Active Directory Domain Services Primer*:
    - begin tot *Outlining AD DS Components* (blz. 125 t/m 131);
    - *Defining Organizational Units tot Understanding AD DS replication* (blz. 137 t/m 141)
  - Hoofdstuk 31, *Optimizing Windows Server 2016 for Branch Office Communications*
    - *Understanding RODC tot Using Bitlocker* (blz. 1186 t/m 1202)

Het werken met PowerShell is een optionele opdracht voor studenten die de uitdaging zoeken.

#### Optioneel:

Documentatie: "Integrating RHEL systems directly with Windows Active Directory", Chapter 1.  
"Connecting RHEL systems directly to AD using SSSD" ([link naar webpagina](#))

### Video's:

Uitleg Active Directory:

1: <https://www.youtube.com/watch?v=OTpbQkW3kj4&list=PLBBA04BF566F0E0D6>

2: <https://www.youtube.com/watch?v=hoodfyq30NA&list=PLBBA04BF566F0E0D6&index=3>



3: <https://www.youtube.com/watch?v=Whh3kPS0FdA&list=PLBBA04BF566F0E0D6&index=4>

Installeren & promoveren van Active Directory:

4: <https://www.youtube.com/watch?v=9KNfPfwv4oA&list=PLBBA04BF566F0E0D6&index=6> (video is gebaseerd op server 2008, de verschillen met 2016 zijn beperkt)

## 2.2.1 Opdracht: 1<sup>e</sup> Active Directory (AD) domain controller promoveren

- Geef de Windows server een logische, herkenbare naam (vb: BMC-DC1) en configureer of controleer de IP-instellingen (de server heeft een vast IP adres nodig (geen DHCP adres), bijvoorbeeld: **192.168.2.1**).
- Installeer *Active Directory Domain Services (ADDS)* en promoveer de server tot *Domain Controller*.
  - De domeinnaam die je hiervoor gebruiken moet is **BMC.local**

Als je niet precies weet hoe je dit doen moet, bekijk dan de instructies in de volgende deelparagraaf en/of de video <https://www.youtube.com/watch?v=9KNfPfwv4oA&list=PLBBA04BF566F0E0D6&index=6>.

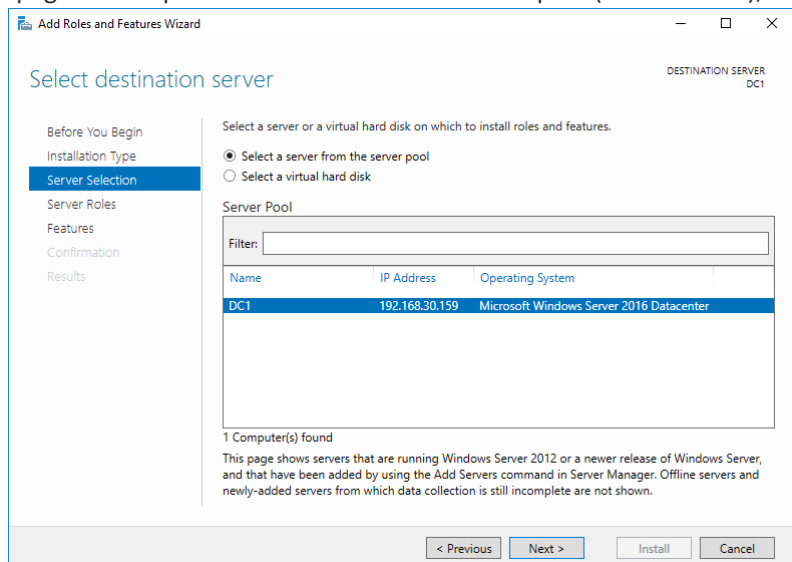
Nadat de *domain controller* gepromoveerd is, bekijk je de tool *Active Directory Users and Computers (ADUC)* en de *DNS Manager* om te oriënteren op de wijzigingen die door het promoveren zijn gemaakt. In latere opdrachten ga je met beide tools werken.

### 2.2.1.1 Instructies voor het promoveren van een AD domain controller

We gebruiken in dit voorbeeld de “Active Directory Domain Services Configuration Wizard”. Om deze beschikbaar te maken, moeten eerst de Active Directory componenten van Windows Server geïnstalleerd worden met behulp van de “Add Roles and Features Wizard”.

Voer daarvoor de volgende stappen uit (sluit elke stap af door op “Next >” te klikken):

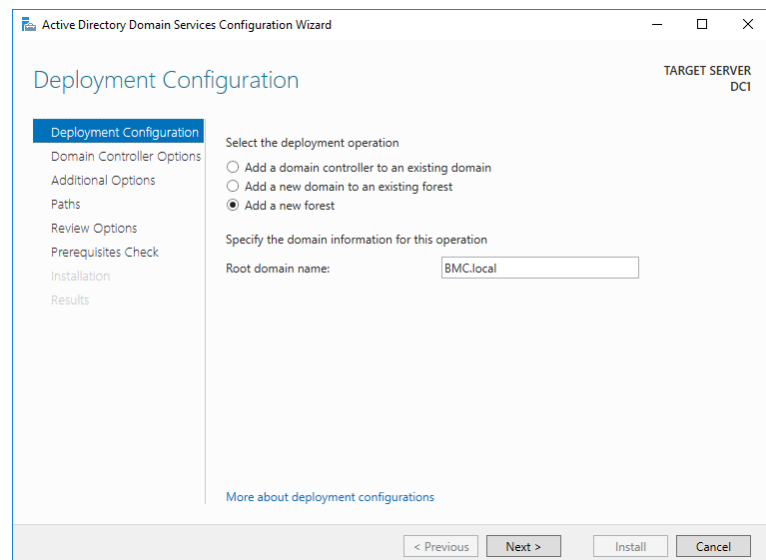
- Start, als dit niet al gebeurd is, “Server Manager”;
- Kies in Server Manager de optie Manage → Add Roles and Features;
- Lees de informatie op de “Before You Begin” pagina;
- Selecteer op de “Installation Type” pagina de optie “Role-based or feature-based installation”;
- Selecteer op de “Server Selection” pagina de te promoveren server uit de server pool (zie illustratie);



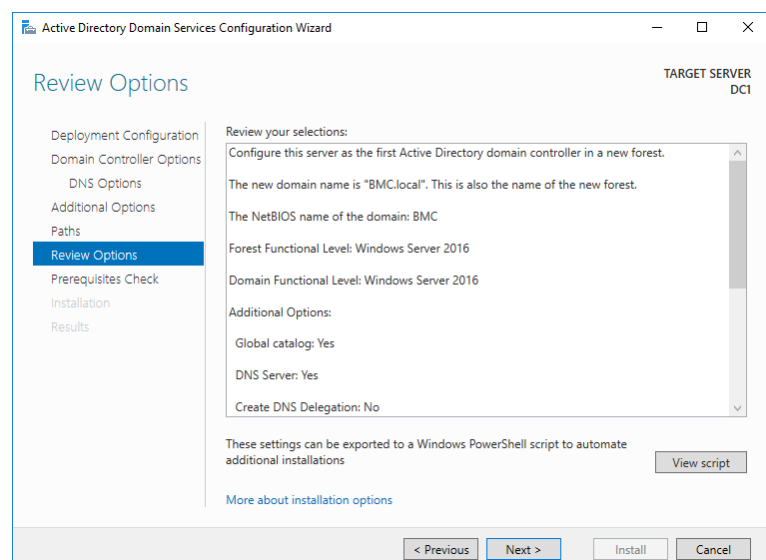
- Selecteer op de “Server Roles” pagina de “Active Directory Domain Services” rol en accepteer de aanbevolen bijbehorende features, waaronder Remote Server Administration Tools;
- Op de “Features” pagina hoeft je niets te veranderen;
- Kijk op de “Confirmation” pagina je keuzes nog een keer goed na voordat je deze bevestigt, als je dat handig vindt kun je hier de optie “Restart the destination server automatically if required” selecteren. Maar je kunt er ook voor kiezen dit handmatig te doen indien nodig;



- Na installatie van de rollen en features (en eventuele herstart) toont Server Manager een geel icoon met een uitroepteken. Klik hierop en volg de “Promote this server to a domain controller” link. De “Active Directory Domain Services Configuration Wizard” wordt gestart;
- Selecteer op de “Deployment Configuration” pagina de optie “Add a new forest” en vul de naam van het nieuwe domein in (BMC.local; zie illustratie);



- Op de “Domain Controller Options” pagina laat je het “domain functional level” op de default staan. Let erop dat de “Domain Name System (DNS) Server” optie geselecteerd moet zijn. De “Global Catalog (GC)” optie is automatisch geselecteerd (en kan doordat dit de eerste domain controller in het domein is niet gedeselecteerd worden).  
Voer twee keer hetzelfde wachtwoord in voor de Directory Services Restore Mode (DSRM). Dit wachtwoord zal je zelden of niet nodig hebben, maar zorg ervoor dat je het wachtwoord kunt herinneren of ergens vastlegt zodat je het beschikbaar hebt indien nodig;
- Active Directory gaat op zoek naar een DNS server voor het opgegeven domein (bij het AD domein hoort een DNS domein met dezelfde naam). Aangezien we geen DNS server voor dit domein hebben opgezet leidt dit tot een waarschuwing. Deze waarschuwing is geen reden tot zorg;
- De NetBIOS naam hoeft je niet te veranderen;
- Op de pagina “Paths” hoeft je de paden voor database, logfile en ‘sysvol’ niet te veranderen;
- Kijk op de “Review Options” pagina je keuzes nog een keer goed na voordat je deze bevestigt (zie illustratie);







- Op de “Prerequisites Check” pagina zullen twee waarschuwingen getoond worden, maar desondanks zal bovenaan de pagina een groen vinkje getoond dat aangeeft dat aan alle vereisten voldaan is. Voer de veranderingen door door op de “Install” knop te drukken;
- Wacht tot de veranderingen zijn doorgevoerd en de server automatisch opnieuw opgestart. Nadat je opnieuw bent ingelogd (met hetzelfde Administrator account dat eerst voor alleen de server gold; dit is overgenomen als het Domain Administrator account) en je kunt in Server Manager zien dat je nu over een domain controller beschikt.

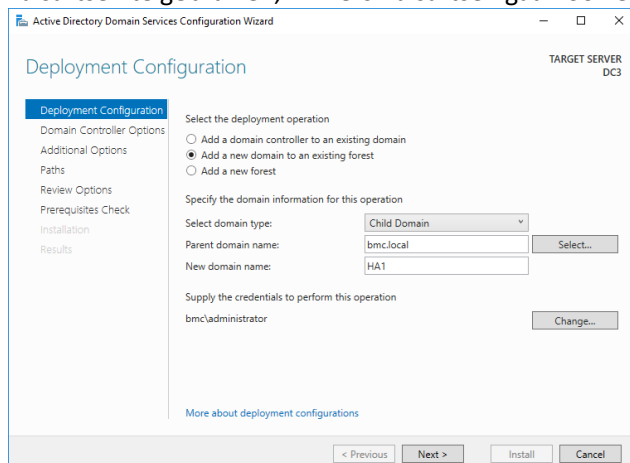
## 2.2.2 Optioneel: 2<sup>e</sup> (peer) domain controller (GUI)

Het gevaar bestaat dat gebruikers door een storing niet meer kunnen inloggen op het domein en dus ook niet meer hun werk kunnen uitvoeren. In het geval dat de huisarts daarom niet kan zien welke medicijnen een patiënt gebruikt of waar hij/ zij allergisch voor is, kan dat voor serieuze problemen zorgen. Om dit te voorkomen kun je een zogenaamde peer domain controller promoveren. Dit is een tweede server die in hetzelfde domein (lees: BMC.local) wordt geplaatst en die voor het overgrote deel dezelfde instellingen krijgt als de eerste domein controller. Deze opdracht is optioneel omdat niet elke student over een laptop beschikt die alle/ veel virtuele machines tegelijk kan draaien. Het is wel een leerzame, nuttige opdracht om uit te voeren, vooral ook in combinatie met opdracht 2.2.7 waarbij de 2<sup>e</sup> DC weer wordt verwijderd. Het verwijderen van een DC vereist een aantal specifieke handeling die volgens een specifieke procedure moeten worden uitgevoerd om problemen met de andere domein controllers te voorkomen. Als je deze opdracht nu niet hier kunt uitvoeren, dan doe je dat in week twee met een Windows 2016 Core machine.

- Geef de tweede Windows server een logische, herkenbare naam (vb: BMC-DC2) en geef de machine de IP-instellingen (192.168.x.2/24). Als DNS-server moet je het IP-adres van de eerste DC opgeven. Denk aan het bijwerken van het IP-schema. Zie hiervoor paragraaf 2.1.5.
- Installeer ook nu weer *Active Directory Domain Services (ADDS)* en promoveer de server tot *Domain Controller* in het domein: BMC.local. Let erop dat je hiervoor credentials binnen het domein gebruikt (bijvoorbeeld BMC\Administrator). De standaardinstellingen kun je accepteren.
- Test de werking van het domein door een testgebruiker (vb: test1) aan te maken op de eerste DC en te kijken of deze gebruiker naar de tweede DC wordt gerepliceerd. Het aanmaken van een gebruiker kan op verschillende manieren, gebruik hiervoor nu ADUC.

## 2.2.3 Opdracht: Sub domein

Omdat het niet wenselijk is dat alle huisartsen in elkaars patiëntenbestand kunnen kijken en om het domein beheersbaar te houden als het aantal patiënten en gebruikers groeit, is er besloten om voor de huis- en tandartsen een eigen ‘subdomein’ te creëren. Na overleg is er besloten om niet de voor- of achternaam van de huisartsen te gebruiken, immers huisartsen gaan ook eens met pensioen of verhuizen. In plaats daarvan werk je



met het subdomein HA (afkorting van HuisArts) en TA (TandArts). Dus voor huisarts1 maak je een nieuwe subdomein aan met de naam HA1.BMC.local en voor de tweede tandartspraktijk kun je het subdomein TA2.BMC.local maken. Het nut, het proces en de mogelijkheden van een subdomein worden pas verderop in het hoofdstuk besproken. Deze stof wordt in een latere cursus behandeld en is dus geen onderdeel voor het theorie tentamen, maar omdat de handelingen niet ingewikkeld zijn, kan het wel een onderdeel van het practicum tentamen zijn. In Figuur 2 hiernaast kun je zien welke optie(s) je tijdens het

FIGUUR 2 AD DEPLOYMENT VAN SUBDOMEIN





promoveren moet instellen om een subdomein te creëren. De rest van het proces wordt door de wizard in goede banen geleid.

- Geef de derde (of de tweede als je opdracht 2.2.2 niet hebt gedaan!) server een logische, herkenbare naam (vb: BMC-DC3) en geef de machine de IP-instellingen. Denk aan het bijwerken van het IP-schema (2.1.5)
- Installeer ook nu weer *Active Directory Domain Services (ADDS)* en promoveer de server tot *Domain Controller* in het domein: HA1.BMC.local of TA1.BMC.local. Het is voor de opdracht niet noodzakelijk om beide te doen. Eén subdomein is voldoende. De standaard, voorgestelde instellingen zijn goed.
- Mocht het promoveren niet lukken, denk dan o.a. aan het virtuele netwerk. Kan de server de eerste DC pingen? Heb je de goede IP-instellingen ingevoerd?
- Als je ADUC bekijkt, dan zal je zien dat de aangemaakte test-gebruiker in dit domein niet voorkomt.

## 2.2.4 Opdracht: client aan het domein toevoegen

Om de verschillende werknemers toegang te geven tot het netwerk, hardware als bijvoorbeeld printers en applicaties, moet er client-computers aan het netwerk worden toegevoegd. Na overleg is er besloten om bij voorkeur te werken met clients met een Windows client besturingssysteem. Gebruik daarvoor de *education* versie van Windows 10. Optioneel kan er met Linux of andere besturingssystemen worden gewerkt, maar dat is een optionele opdracht. Zie paragraaf 2.2.8 voor deze optionele opdracht.

- Voeg de Windows machine(s) toe aan het domein. Denk aan het wijzigen van de naam en de IP-instellingen!  
Als het toevoegen gelukt is, kun je de computer(s) terugvinden in ADUC in de 'map' Computers.

Optionele uitleg is te vinden in de video "BIPL\_windows\_week1\_server2016.mp4" (zie Canvas).

## 2.2.5 Opdracht: Beheertools op client installeren

Servers worden vanwege de veiligheid, maar ook voor bijvoorbeeld de koeling, in een afgesloten serverruimte geplaatst. Het beheer van de servers wordt meestal gedaan vanaf een computer en laptop welke lid is van het domein. Om het beheer mogelijk te maken is het noodzakelijk om de beheertools op een cliëntsysteem te installeren. De voorkeur gaat uit naar een combinatie van de Server Manager, RSAT en RDP. Optioneel kun je ADAC gebruiken. Om de tools in het domein te gebruiken, moet je wel inloggen op het domein. Omdat er nog geen andere gebruikers zijn aangemaakt doe je dat met het account van de administrator(@bmc.local)

- Installeer en configureer de managementtools Server Manager RSAT & RDP.  
Windows 10 RSAT Tools zijn op niet al te oude Windows 10 installaties standaard beschikbaar.
- Activeer de RSAT Tools door *Settings* onderdeel *Apps & Features* te openen, daar op "Optional features" te klikken, "Add a feature" te klikken en RSAT in de zoekregel te typen, waarna je diverse RSAT tools te zien krijgt die je kunt selecteren. Kies daarbij minimaal voor *RSAT: Active Directory Domain Services and Lightweight Directory Services Tools*, *RSAT: DHCP Server Tools*, *RSAT: DNS Server Tools*, *RSAT: Group Policy Management Tools* en *RSAT: Server Manager* want die komen in deze cursus allemaal goed van pas.
- In de server Manager kun je bij *All Servers* met *Add Servers* de verschillende servers van het domein toevoegen. Controleer of je de verschillende tools (ADUC en bijvoorbeeld DNS) ook daadwerkelijk kunt gebruiken. Door de *Performance counters* per server te starten, krijg je meer informatie te zien. Voor het subdomein is het remote beheer niet noodzakelijk!

## 2.2.6 Opdracht: Organizational Units

In een domein kunnen duizenden objecten worden aangemaakt, verschillende gebruikers, computers en bijvoorbeeld printers. Om enig overzicht aan te brengen in alle objecten, heb je in een domein de mogelijkheid om zogenaamde *Organizational Units (OU)* aan te maken.



- In dit deel van de opdracht maak je direct onder BMC.local de onderstaande OU's aan, doe dit vanaf de Windows client:
  - Fysiotherapie;
  - Huisartsen;
  - Tandartsen;
  - Verloskundigen;
  - Patiënten;
  - Gasten;
  - Beheerders.

Als je niet weet hoe je de OU's moet aanmaken, dan wordt dat uitgelegd in onderstaande instructies.

### **2.2.6.1 Instructies aanmaken Organizational Unit (OU)**

- Start Active Directory Administrative Center (ADAC) vanuit Server Manager of door windows+R in te drukken, dsac.exe te typen en OK te klikken.
- Klik met de rechter muisknop op het domein, kies in het menu New → Organizational Unit
- Vul in het window "Create Organizational Unit:" de naam van de nieuwe OU in, controleer dat het checkboxje "Protect from accidental deletion" geselecteerd is, en druk op OK.
- Om een OU binnen een andere OU te maken is het ook mogelijk om in ADAC in plaats van op het domein op de bestaande OU met de rechter muisknop te klikken en vervolgens dezelfde stappen te volgen.

### **2.2.7 Optioneel: 2<sup>e</sup> peer domain controller verwijderen**

*Deze optionele opdracht is alleen van toepassing als je de optionele opdracht in paragraaf 2.2.2 hebt uitgevoerd.*

Als je computer weinig resources heeft, dan kun je ervoor kiezen om de in paragraaf 2.2.2 gebouwde peer domain controller nu verwijderen.

**Let op:** verwijder niet het subdomein!

Hoe je de DC moet verwijderen doen wordt uitgelegd op <https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/deploy/demoting-domain-controllers-and-domains--level-200->. Volg deze procedure nauwkeurig!

- Verwijder de tweede domeincontroller.

### **2.2.8 Optioneel: Linux aan Active Directory (nadat Rocky Linux is geïnstalleerd!)**

In deze optionele opdracht kun je één of meerdere Linux clients aan het domein koppelen nadat je eerst de Linux installatie(s) in paragraaf 2.3 hebt afgerond. De benodigde informatie hiervoor vind je in "[Integrating RHEL systems directly with Windows Active Directory](#)", Chapter 1. "[Connecting RHEL systems directly to AD using SSSD](#)". Lees van dit document hoofdstuk 1 tot en met paragraaf 1.3 door en volg daarna van paragraaf 1.4 de instructies tot aan 1.4.1 (de diverse opties hebben we niet nodig om een werkende integratie te realiseren).

Let bij het uitvoeren op het volgende:

1. de Rocky VM zal onderdeel moeten uitmaken van hetzelfde netwerk als de domain controller
2. de Rocky VM moet de domain controller als primaire DNS server gebruiken (want: zonder DNS geen AD!)

Zorg dat je alle benodigde extra software op de VM hebt geïnstalleerd alvorens je de netwerkconfiguratie in VMware aanpast, anders wordt de installatie van deze packages veel meer werk (hoewel je er bijvoorbeeld de DVD ISO voor zou kunnen mounten komt dit niet in de buurt van het gemak dat de *package manager* biedt bij een beschikbare Internetverbinding).



## 2.2.9 Vragen Active Directory

Als je de opdrachten hebt doorgenomen, de voorgeschreven delen van hoofdstuk 4 van *Windows 2016 Unleashed* hebt gelezen en de colleges hebt bijgewoond, dan moet het niet lastig zijn om de onderstaande vragen te beantwoorden.

3. Wat is active directory (AD)?
4. Welke handelingen moet je in Server 2016 uitvoeren om een AD te installeren en te configureren?
5. Op welk punt verschilt een workgroup van een domein?
6. Wat is het verschil tussen AD en Active Directory Domain Services (ADDS)?
7. Wat is de functie van een Site?
8. Wat is *replication*?
9. In AD heb je te maken met Objects en een schema. Wat zijn de kenmerken van beide en welke relatie hebben ze met de database?
10. Wat is de functie van een Organizational Unit?
11. Wat is het verschil tussen een (domain) forest en een tree?
12. Wat is de functie van een Global Catalog server?
13. Wat is de functie van disaster recovery?
14. Welke rol (service) moet er voor of tijdens het installeren van ADDS extra worden geïnstalleerd? Deze rol wordt tijdens het promoveren dan de server geconfigureerd als het op dezelfde server geïnstalleerd is.
15. Welk bestandssysteem moet op de harde schijf zijn toegepast om een server te kunnen promoveren tot DC? Kun je hiervoor ook het nieuwe bestandssysteem Resilient File System (ReFS) gebruiken?
16. Welke relatie is er tussen AD en DNS?
17. Wat is een *Domain Functional Level (DFL)* en welke DFLs zijn er?
18. Heeft een DFL invloed op een *member* server en/of een client?
19. Wat wordt er verstaan onder een *Forest Functional Level*?
20. Wat is *sysvol*?
21. Wat is het DSRM?
22. Welk protocol wordt door AD gebruikt om objecten op te slaan?

## 2.3 Week 1, College 2: Linux Installatie en Package Management

### Inleiding

Binnen Beter Medisch Centrum worden naast Windows servers ook een aantal servers met Linux ingezet. Omdat niet iedereen al eerder een Linux systeem heeft geïnstalleerd of daarop software heeft geïnstalleerd of juist verwijderd, zal je daar in de komende opdrachten bij begeleid worden.

Omdat Red Hat Enterprise Linux (RHEL) in productie-omgevingen veel gebruikt worden, en voor deze distributies de meeste software beschikbaar is die BMC nodig denkt te kunnen hebben, wordt voor het met RHEL compatibele Rocky Linux gekozen, en wel Rocky Linux versie 8.

### Theorie

#### Verplicht:

- Slides,
- Dit werkboek met vragen en antwoorden (zie afzonderlijk document “Antwoorden\_BIPL\_Werkboek\_v1.4.1vt”!)
- Boek: “Unix and Linux System Administration Handbook, 5th Edition”:
  - Chapter 1 – *Where to start*
    - 1.3 *Linux distributions*: blz. 8 t/m 11 (tot: *Example UNIX distribution*)
  - Chapter 6 - *Software Installation and Management*
    - Inleiding: blz. 153



- 6.1 *Operating system installation*: blz. 154 t/m 159 (tot: *Automating installation for Debian and Ubuntu*)
- 6.2 *Managing packages*: blz. 162 t/m 164
- 6.3 *Linux package management systems*: blz. 164 t/m 165
- 6.4 *High-level Linux package management systems*: blz. 166 t/m 169 (tot: *RHN: the Red Hat Network*), blz. 174.

Optioneel:

- Documentatie: “Red Hat Enterprise Linux 8 Documentation” ([online](#))

#### Video's

- Optioneel: “RHEL 8 handmatige installatie.mp4” (zie Canvas)

### 2.3.1 Inleiding

Onbekend maakt onbemind, maar hoewel Linux de reputatie heeft moeilijk te installeren te zijn, hebben moderne *installers* een en ander vrij makkelijk gemaakt. De Red Hat Enterprise Linux 8 *installer* (genaamd Anaconda) is er hier één van.

### 2.3.2 Opdracht: download de Rocky Linux 8 ISO

Hoewel we de meeste software tijdens de installatie *live* via Internet zullen binnenhalen, zal net als bij elke installatie vanaf een bestaand medium geboot moeten worden. Omdat dit onder VMware nog het makkelijkst is vanaf een virtuele DVD-ROM zullen we nu een ISO image downloaden met daarop het Rocky Linux 8 installatieprogramma.

Deze vind je op <https://rockylinux.org/> de “Download” knop te klikken.

Download daar de meest recente Rocky 8 DVD ISO<sup>†</sup> voor de x86\_64 architectuur.

### 2.3.3 Opdracht: Maak de virtual machine aan

De systeemeisen van Rocky Linux 8 zijn naar hedendaagse begrippen niet heel hoog.

Maak een VM aan (kies voor de optie om het operating systeem later te installeren). Het meest leerzaam is het om te kiezen voor een “Custom” configuratie. Zie hieronder welke instellingen je dan het best kunt selecteren.

**Koppel op dit moment nog geen ISO image!** Kies onder “Install from:” voor “I will install the operating system later”, **niet** voor “Installer disc image file (iso)”. Als je direct een ISO koppelt, dan wordt *Easy Install* gestart die veel keuzes uit handen neemt, daardoor kun je ook niet de keuzes maken die het beste bij deze cursus passen. Daarnaast mis je een groot deel van het door ons beoogde leereffect bij de handmatige installatie en werkt dit niet samen met de automatische installatie in paragraaf 2.3.6.

Gebruik verder de volgende instellingen:

- Guest operating system: Linux, version: Red Hat Enterprise Linux 8 64-bit

Gebruik als je hebt gekozen voor een “Custom” configuratie de volgende extra instellingen:

- Processor configuration: 1 processor, 1 core per processor
- Memory: 1536 MB<sup>‡</sup>
- Network type: NAT
- I/O controller: LSI Logic

---

<sup>†</sup> Voor de eerste installatie werkt de *Boot* of *Minimal* ISO ook wel, maar voor de tweede installatie (paragraaf 2.3.6.2) niet.

<sup>‡</sup> Conform <https://access.redhat.com/articles/rhel-limits>



- Disk type: NVMe
- Disk: Create a new virtual disk
- Disk capacity: 20.0 GB (aanbevolen: split into multiple files)

Desgewenst kun je ervoor kiezen om de virtuele printer en sound card hardware niet aan te laten maken (onder “Customize Hardware...”), want die gaan we niet gebruiken. Indien je virtualisatie host het toelaat zou je er ook voor kunnen kiezen meer CPU’s, RAM en/of disk toe te wijzen, maar gegeven waarden zijn voldoende.

### 2.3.4 Opdracht: Handmatige installatie van Rocky Linux volgens profiel “Server with GUI”

Installatie van Rocky Linux verloopt in een drietal stappen die hieronder verder worden uitgewerkt:

1. Opstarten van de installatie door de ISO te booten
2. Configuratie van het te installeren systeem
3. Installatie van de software op de harddisk van het nieuwe systeem

Dit duurt ongeveer een half uur bij gebruik van een voldoende snelle harddisk of SSD, een groot deel van deze tijd hoeft je er niet actief mee bezig te zijn.

Als je ergens niet direct uitkomt, kun je even kijken in de aangeleverde video waarin versneld de installatie van een VM met profiel “Server with GUI” onder RHEL 8 wordt getoond (de verschillen met Rocky 8 zijn minimaal).

#### 2.3.4.1 Opstarten

Verbind het in §2.3.2 gedownloade image met de CD/DVD drive van de nieuw aangemaakte VM en start de VM. Als je even wacht, dan start de installatie automatisch op.

*TIP:* als je op wilt schieten kun je met behulp van de cursortoetsen en de Enter toets de menu-optie “Install Rocky Linux 8.x” kiezen..

#### 2.3.4.2 Configuratie van het te installeren systeem

De eerste configuratiestap is keuze van taal en toetsenbord. We installeren alle systemen in de originele taal, het Engels. Installatie in het Nederlands leidt alleen maar tot verwarring doordat de vertalingen niet altijd even voor de hand liggend zijn; het is in het werkveld daarom goed gebruik om bij het Engels te blijven.

Accepteer dus de standaard instellingen *English/English (United States)* en ga verder door op “Continue” te klikken.

Vervolgens kom je op een scherm waarop verschillende categorieën van instellingen staan weergegeven. Deze lopen we een voor een af:

1. Stel de netwerkkaart in, via “Network & Host Name” iets onder het midden in de rechter kolom. Omdat we gebruik maken van DHCP is het voldoende om links onderin de hostname op te geven (*rocky1.bmc.test*) en vervolgens de switch rechts bovenin te activeren van “OFF” naar “ON”. Verlaat deze pagina door linksboven op “DONE” te klikken (dit geldt ook voor alle volgende pagina’s);
2. Vervolgens stellen we de juiste tijdzone in onder “Time & Date” onderaan de linker kolom. Omdat we een werkend netwerk hebben heeft de *installer* zelf al ingesteld dat we de exacte tijd van Internet binnenhalen, we hoeven alleen nog even dicht in de buurt van Nederland te klikken om tijdzone “Europe/Amsterdam” in te stellen. Verlaat de pagina;
3. Nu kun je verder gaan met de diskinstellingen, “Installation Destination”, rechts bovenin. De juiste (want enige) disk is al geselecteerd, evenals “Storage Configuration” → “Automatic”. De automatische partitionering is echter meer geschikt voor workstations dan voor servers, kies daarom (en omdat je nu de rol van system engineer vervult in plaats die van eindgebruiker) voor “Storage Configuration” → “Custom”. Verlaat de pagina.  
Nu toont de *installer* de partitioneringspagina. Laat door op “Click here to create them automatically.” alvast de basis-partities voorbereiden (lekker makkelijk). De installer maakt hiervoor LVM volumes aan en dat is precies wat we willen, dus daar hoeft je niets aan te doen. Als bestandssysteem (hier gaan we in week 4 nader op in) wordt *by default* XFS gebruikt, voor algemene doeleinden is dit prima (daarom is het ook de default).



Het eerste wat we nu doen is de root partitie (/) verkleinen om ruimte te maken voor eigen partities. Selecteer de root partitie en vul “8 GiB” in. Bevestig de aanpassing door op een van de andere partities te klikken (dit is een beetje vreemd, helemaal omdat de geklikte partitie nog niet geselecteerd wordt, maar zo werkt de installer nu eenmaal), voor / wordt nu ook links in het beeld een grootte van 8 GiB aangegeven.

Vervolgens maken we de volgende twee nieuwe partities aan (met behulp van de + knop; **let op:** in het voorbeeld in de video worden andere groottes gebruikt, hou je aan deze waarden):

- a. /var van 3 GiB (voor variabele, veranderlijke bestanden zoals systeem logs en gedownload updates)
  - b. /tmp van 1 GiB (voor tijdelijke bestanden van zowel systeem als gebruikers)
- /boot moet een fysieke partitie zijn (zoals de naam zegt wordt daarvan geboot) en is met 1024 MiB groot genoeg, een *swap size* van 2 GiB is ook prima voor deze VM. Laat deze twee ongemoeid, verlaat de pagina en accepteer de veranderingen;
4. *Installation Source* (middenin) geeft nu als het goed is “Local media” aan, dit laten we ongewijzigd;
  5. Nu moet nog geselecteerd worden welke software op het nieuwe systeem geïnstalleerd moet worden: “Software selection” rechts middenin.  
Hier selecteer je “Server with GUI” voor een op het verlenen van diensten gericht systeem waarop je desondanks niet alleen via de command line maar ook met een grafische interface kunt werken (waarschijnlijk is deze al geselecteerd). Verlaat de pagina;
  6. De *installer* controleert nu of de gekozen installatiebron de gevraagde installatie daadwerkelijk kan leveren, na enige tijd moet dit resulteren in een scherm met alleen een waarschuwings-driehoekje bij “Root Password”;
  7. De laatste stap voor de installatie kan beginnen (de knop “Begin Installation” rechts onderin is nog niet beschikbaar) is het instellen van het root (het Linux beheeraccount) wachtwoord. Klik hiervoor linksonder op “Root Password” en voer twee keer hetzelfde wachtwoord in. Dit mag een eigen wachtwoord zijn of hetzelfde wachtwoord als voor de Windows VM’s gebruikt wordt, zolang je zelf maar kunt onthouden wat het is. Verlaat de pagina.
  8. Hoewel het nu mogelijk is de installatie te starten, is het een beter idee om eerst een gebruiker te maken waarmee je standaard in zult loggen. Klik hiervoor op “User creation” helemaal linksonderin (misschien moet je even naar beneden scrollen om dit te zien). Vul de gevraagde gegevens in, selecteer “Make this user administrator” en “Require a password to use this account”, geef twee keer hetzelfde wachtwoord in en verlaat de pagina.
  9. Klik nu op de blauw geworden knop “Begin Installation” en wacht af tot de installatie is afgerond (je kan ondertussen wat anders gaan doen, het duurt wel even en als je het einde mist dan is er weinig aan de hand).

**Indien de installatie niet goed verloopt:** onder specifieke omstandigheden kan het gebeuren dat de installatie vastloopt. De kans is dan groot dat er iets misgaat in de communicatie met de installatiebron op Internet. Download in dat geval het grotere “DVD ISO” image, verwijder de VM en maak hem opnieuw aan. Download in dat geval alsnog het grotere “DVD ISO” image, verwijder de VM en maak hem opnieuw aan. Voer verder bovenstaande stappen hetzelfde uit.

Aan het einde van de installatieprocedure verschijnt rechts onderin een “Reboot” knop, waarmee je ervoor kunt zorgen dat je nieuwe Linux VM wordt opgestart.

Meestal moet nu de Red Hat licentie geaccepteerd worden, dit zogenaamde *firstboot* proces wijst zichzelf.

Log in op de desktop met het account dat je tijdens de installatie hebt aangemaakt (**niet** het root account). Als dit de eerste keer is, dan moet je door een paar vragen heen, dit wijst zichzelf (locatie service kun je uit laten). De “Getting Started” van GNOME kun je doornemen als je wilt, maar je kunt hem ook wegklikken met het kruisje rechtsboven.





## 2.3.5 Opdracht: Linux package management

Package management in Linux is in theorie zowel mogelijk via de GUI als via de command line, maar de met Rocky 8 standaard meegeleverde GUI faciliteiten hiervoor zijn zo beperkt dat we daar onze tijd in deze cursus niet aan verspillen.

In tegenstelling tot de beperkte package management mogelijkheden via de GUI, zijn de Linux package management tools via de CLI zeer krachtig.

De standaard command line tool voor package management onder Rocky is DNF (voorheen YUM; als je YUM in het verleden al gebruikt hebt dan zul je merken dat DNF een *compatibility mode* aanbiedt).

Om te beginnen moet je hiervoor een command line ter beschikking hebben. Hiervoor heb je drie keuzes:

1. Een command line binnen de grafische omgeving. Open hiervoor de applicatie Terminal (klik hiervoor op “Activities” linksboven in het scherm)
2. Een *text-mode* console. Typ hiervoor Ctrl+Alt+F3, Ctrl-Alt-F4, Ctrl-Alt-F5 of Ctrl-Alt-F6 en log in (bij het intypen van je wachtwoord zie je niets, maar wat je typt wordt wel verwerkt)
3. Gebruik van een SSH client op je Windows laptop, bijvoorbeeld [PuTTY](#). Om de SSH client te kunnen gebruiken moet je wel even achterhalen wat het IP adres van je Linux VM is door rechtsboven op het netwerkoontje te drukken en vervolgens Wired Connected → Wired Settings te kiezen, waarna je de daadwerkelijke instellingen kunt zien door het tandwielte onder “Wired” te klikken.

Nu je de beschikking hebt over een command line, kunnen we een paar package management taken uitvoeren met behulp van DNF.

### 2.3.5.1 Updaten van software via de CLI

Op alle platformen is het belangrijk om de meest recente versie van alle software te draaien, omdat daar fouten (bugs) en beveiligingslekken in zijn opgelost die in oudere versies aan het licht zijn gekomen.

Ondanks het gebruik van een zo recent mogelijk DVD image voor de installatie is van niet alle software de meest recente versie geïnstalleerd. Daarom kan de nieuw geïnstalleerde VM gebruikt worden om ervaring op te doen met het uitvoeren van updates onder Linux.

Onder Windows wordt dit verzorgd door Windows Update, onder Linux doen we dit handmatig met behulp van DNF. Hoewel we het vaak hebben over ‘updates’ spreekt DNF van ‘upgrades’ (dit is meer in overeenstemming met Debian APT dan dat YUM dat was).

We gebruiken om de updates te installeren het commando:

```
sudo dnf upgrade
```

(Het eigenlijke commando komt na “sudo”, “sudo” zorgt ervoor dat het commando met root rechten wordt uitgevoerd, te vergelijken met runas onder Windows; in week 3 kom je meer te weten over deze tool).

Na authenticatie met je **eigen** gebruikerswachtwoord (dus in dit geval van user, niet van root) gaat DNF voor je aan het werk om uit te zoeken wat er precies moet gebeuren. Hij rapporteert hierover in je terminal window.

Vervolgens moet je controleren en bevestigen dat wat DNF voorstelt (een lijst van pakketten die geïnstalleerd en geüpgrade moeten worden) overeenkomt met wat je in gedachten had.

Dat ziet er ongeveer uit als volgt:

```
[marco@rocky1 ~]$ sudo dnf upgrade

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

#1) Respect the privacy of others.
#2) Think before you type.
#3) With great power comes great responsibility.
```



```
[sudo] password for marco:
Rocky Linux 8 - AppStream                2.8 MB/s | 11 MB    00:03
Rocky Linux 8 - BaseOS                  2.6 MB/s | 6.0 MB   00:02
Rocky Linux 8 - Extras                   30 kB/s | 14 kB    00:00
Dependencies resolved.
=====
Package                                Arch    Version                                Repo      Size
=====
Installing:
kernel                                x86_64  4.18.0-477.21.1.el8_8                baseos    9.4 M
Upgrading:
ModemManager                         x86_64  1.20.2-1.el8                        baseos    1.2 M
ModemManager-glib                    x86_64  1.20.2-1.el8                        baseos    337 k
NetworkManager                       x86_64  1:1.40.16-4.el8_8                  baseos    2.3 M
NetworkManager-adsl                  x86_64  1:1.40.16-4.el8_8                  baseos    154 k
NetworkManager-bluetooth              x86_64  1:1.40.16-4.el8_8                  baseos    179 k
NetworkManager-config-server          noarch  1:1.40.16-4.el8_8                  baseos    141 k
NetworkManager-libnm                  x86_64  1:1.40.16-4.el8_8                  baseos    1.9 M
NetworkManager-team                   x86_64  1:1.40.16-4.el8_8                  baseos    158 k
NetworkManager-tui                    x86_64  1:1.40.16-4.el8_8                  baseos    353 k
NetworkManager-wifi                   x86_64  1:1.40.16-4.el8_8                  baseos    200 k
NetworkManager-wwan                   x86_64  1:1.40.16-4.el8_8                  baseos    185 k
adcli                                 x86_64  0.9.2-1.el8                         baseos    132 k
alsa-lib                              x86_64  1.2.8-2.el8                         appstream 495 k
alsa-sof-firmware                     noarch  2.2.4-2.el8                         baseos    885 k
: hier is een stuk van de output weggelaten aangezien deze nogal lang is
xorg-x11-server-Xwayland              x86_64  21.1.3-10.el8                       appstream 965 k
xorg-x11-server-common                 x86_64  1.20.11-15.el8                      appstream 43 k
yum                                    noarch  4.7.0-16.el8_8                      baseos    207 k
zlib                                    x86_64  1.2.11-21.el8_7                     baseos    102 k
Installing dependencies:
grub2-tools-efi                       x86_64  1:2.02-148.el8_8.1.rocky.0.3        baseos    478 k
kernel-core                           x86_64  4.18.0-477.21.1.el8_8                baseos    42 M
kernel-modules                         x86_64  4.18.0-477.21.1.el8_8                baseos    34 M
libwpe                                x86_64  1.10.0-4.el8                         appstream 25 k
wpebackend-fdo                         x86_64  1.10.0-3.el8                         appstream 43 k
Installing weak dependencies:
libvirt-client                         x86_64  8.0.0-19.2.module+el8.8.0+1321+70d049b2
                                         appstream 418 k
python3-magic                          noarch  5.33-24.el8                          baseos    45 k

Transaction Summary
=====
Install      8 Packages
Upgrade    443 Packages

Total download size: 897 M
Is this ok [y/N]:
```

Waarschijnlijk heb je op dit moment nog niet een heel duidelijk beeld van wat er zou moeten gebeuren dus vertrouw deze keer maar op DNF; bevestig met 'y' en Enter).

```
Is this ok [y/N]: y
Downloading Packages:
(1/451): libwpe-1.10.0-4.el8.x86_64.rpm    188 kB/s | 25 kB    00:00   A
(2/451): wpebackend-fdo-1.10.0-3.el8.x86_64.rpm 325 kB/s | 43 kB    00:00
(3/451): libvirt-client-8.0.0-19.2.module+el8.8 2.4 MB/s | 418 kB    00:00
(4/451): grub2-tools-efi-2.02-148.el8_8.1.rocky 2.3 MB/s | 478 kB    00:00
(5/451): kernel-4.18.0-477.21.1.el8_8.x86_64.rp 2.2 MB/s | 9.4 MB    00:04
(6/451): python3-magic-5.33-24.el8.noarch.rpm  459 kB/s | 45 kB    00:00
(7/451): alsa-lib-1.2.8-2.el8.x86_64.rpm      1.2 MB/s | 495 kB    00:00
(8/451): alsa-ucm-1.2.8-2.el8.noarch.rpm      1.0 MB/s | 118 kB    00:00
(9/451): alsa-utils-1.2.8-1.el8.x86_64.rpm    2.7 MB/s | 1.1 MB    00:00
(10/451): anaconda-core-33.16.8.9-1.el8_8.rocky 3.2 MB/s | 2.5 MB    00:00
: hier is een stuk van de output weggelaten aangezien deze nogal lang is
(448/451): xfsprogs-5.0.0-11.el8_8.x86_64.rpm 2.8 MB/s | 1.1 MB    00:00
(449/451): yum-4.7.0-16.el8_8.noarch.rpm      2.4 MB/s | 207 kB    00:00
(450/451): zlib-1.2.11-21.el8_7.x86_64.rpm   1.6 MB/s | 102 kB    00:00
(451/451): linux-firmware-20230404-114.git2e92a 5.3 MB/s | 264 MB    00:49
-----
Total                                5.2 MB/s | 897 MB    00:50
```





```
Rocky Linux 8 - AppStream 1.6 MB/s | 313 MB 00:00
Importing GPG key 0x6D745A60:
  Userid      : "Release Engineering <infrastructure@rockylinux.org>"
  Fingerprint: 7051 C470 A929 F454 CEBE 37B7 15AF 5DAC 6D74 5A60
  From        : /etc/pki/rpm-gpg/RPM-GPG-KEY-rockyofficial
Is this ok [y/N]:
```

Vermoedelijk weet je ook hier niet zo goed wat te antwoorden, maar aangezien we vanaf een ISO installeren kan er weinig onbetrouwbaars gebeurd zijn; bevestig opnieuw met 'y' en Enter).

```
Is this ok [y/N]: y
Key imported successfully
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Running scriptlet: kmod-kvdo-6.2.8.7-88.el8.x86_64 1/1
  Preparing : 1/1
  Running scriptlet: libgcc-8.5.0-18.el8.x86_64 1/1
  Upgrading : libgcc-8.5.0-18.el8.x86_64 1/894
  Running scriptlet: libgcc-8.5.0-18.el8.x86_64 1/894
  Upgrading : grub2-common-1:2.02-148.el8_8.1.rocky.0.3.noarch 2/894
  :: hier is een stuk van de output weggelaten aangezien deze nogal lang is
  Upgrading : systemd-239-74.el8_8.3.x86_64 187/894
  Running scriptlet: systemd-239-74.el8_8.3.x86_64 187/894
  Upgrading : dbus-1:1.12.8-24.el8_8.1.x86_64 188/894
  Verifying : libvirt-client-8.0.0-19.2.module+el8.8.0+1321+70 1/894
  Verifying : libwpe-1.10.0-4.el8.x86_64 2/894
  Verifying : wpebackend-fdo-1.10.0-3.el8.x86_64 3/894
  Verifying : grub2-tools-efi-1:2.02-148.el8_8.1.rocky.0.3.x86_64 4/894
  :: hier is een stuk van de output weggelaten aangezien deze nogal lang is
  Verifying : yum-4.7.0-11.el8.noarch 892/894
  Verifying : zlib-1.2.11-21.el8_7.x86_64 893/894
  Verifying : zlib-1.2.11-20.el8.x86_64 894/894

Upgraded:
  ModemManager-1.20.2-1.el8.x86_64
  ModemManager-glib-1.20.2-1.el8.x86_64
  NetworkManager-1:1.40.16-4.el8_8.x86_64
  :: hier is een stuk van de output weggelaten aangezien deze nogal lang is
  yum-4.7.0-16.el8_8.noarch
  zlib-1.2.11-21.el8_7.x86_64

Installed:
  grub2-tools-efi-1:2.02-148.el8_8.1.rocky.0.3.x86_64
  kernel-core-4.18.0-477.21.1.el8_8.x86_64
  kernel-modules-4.18.0-477.21.1.el8_8.x86_64
  libwpe-1.10.0-4.el8.x86_64
  wpebackend-fdo-1.10.0-3.el8.x86_64
  libvirt-client-8.0.0-19.2.module+el8.8.0+1321+70d049b2.x86_64
  python3-magic-5.33-24.el8.noarch

Complete!
[marco@rocky1 ~]$
```

Als je nu nog een keer een upgrade uitvoert, dan is er ook niets meer te doen: het systeem is up-to-date:

```
[user@rocky1 ~]$ sudo dnf upgrade
[sudo] password for user:
Last metadata expiration check: 0:07:51 ago on Mon 11 Sep 2023 10:48:12 AM CEST.
Dependencies resolved.
Nothing to do.
Complete!
[user@rocky1 ~]$
```



### 2.3.5.2 De-installatie van onnodige packages via de CLI

Ondanks de keuze van het profiel "Server with GUI" heeft de *installer* een aantal softwarepakketten geïnstalleerd die niet server-waardig zijn (zoals WiFi firmware, niet veel servers zullen een wireless interface hebben). Deze gaan we nu van het systeem verwijderen.

Eerst verwijderen we het pakket *cheese* (een utility om via een webcam beelden mee op te nemen, een vreemd programma voor op een server). Geef hiertoe het commando

```
sudo dnf remove cheese
```

Als het even geleden is dat je de updates hebt geïnstalleerd, dan laat *sudo* je misschien opnieuw je wachtwoord invoeren.

Vervolgens moet je controleren en bevestigen dat wat DNF voorstelt (het verwijderen van *sox* en nog 4 pakketten die ervan afhankelijk zijn) overeenkomt met wat je in gedachten had (bevestig met 'y' en Enter).

Het handigste van de command line tool is dat meerdere packages in een keer kunnen worden opgegeven, met gebruik van *wildcards* (bijvoorbeeld \* om willekeurige tekst te *matchen*).

Verwijder in een of meer DNF sessies de packages:

- *cups* (print faciliteiten)
- *iwl\*-firmware* (firmwares voor WiFi chipsets; gebruik de wildcard om er 16 tegelijk te doen)
- *lohit-\*-fonts* (fonts voor een aantal niet-westerse lettertypen die we niet nodig hebben)
- *NetworkManager-adsl* (ondersteuning voor ADSL)

Dit kan indien je daarvoor kiest allemaal met behulp van een enkel "dnf remove" commando (wederom voorafgegaan door "sudo").

### 2.3.5.3 Installatie van nieuwe software op het systeem via CLI

We zullen de DNF tool nu gebruiken om het tekst-mailprogramma *mutt* aan het systeem toe te voegen.

Geef hiertoe het commando

```
sudo dnf install mutt
```

en bevestig de vragen die gesteld worden.

Doe hetzelfde voor de grafische versie van Wireshark, *wireshark*. Valt je op dat deze meer (maar niet enorm veel) *dependencies* heeft?

### 2.3.5.4 Installatie van nieuwe software in groepsverband

Met DNF is het ook mogelijk om samenhangende groepen van packages tegelijk te installeren.

Een overzicht van de belangrijkste groepen kun je bekijken met behulp van het commando

```
sudo dnf group list
```

Een overzicht van alle groepen waarvan de naam begint met "Network" en hun inhoud kun je bekijken met behulp van het commando

```
sudo dnf group info Network\*
```

In dat laatste overzicht komt ook de groep "*Networking Tools*" voor, waarvan bij de initiële installatie niet alle 'default' (=standaard) packages geïnstalleerd zijn. Die hebben we wel niet heel hard nodig, maar het is een voorbeeld dat niet al te veel ruimte en tijd kost.

De gehele groep kan geïnstalleerd worden met het commando:

```
sudo dnf group install "Networking Tools"
```



## 2.3.6 Opdracht: Geautomatiseerde systeeminstallatie

Wanneer meerdere systemen geïnstalleerd moeten worden, is de handmatige installatie die jullie hiervoor hebben uitgevoerd nogal omslachtig. Daarom hebben veel UNIX en Linux varianten een oplossing voor geautomatiseerde installaties, voor Rocky/Red Hat/CentOS/Fedora is dit Kickstart.

Bij elke installatie wordt in de home directory van het root account een voorbeeld Kickstart configuratie achtergelaten onder de naam `anaconda-ks.cfg`. Deze kun je bekijken door op de command line het volgende commando te geven:

```
sudo cat /root/anaconda-ks.cfg
```

Hoewel dit een goed uitgangspunt is voor geautomatiseerde installaties, is het bestand helaas nog niet perfect, zodat Kickstart tegen wat problemen zal aanlopen als de configuratie niet op enkele punten wordt aangepast. Daarom hebben we op OneDrive een werkend exemplaar neergezet dat je kunt gebruiken via verkorte link: <https://edu.nl/vhv44>. Hierin zijn de volgende aanpassingen gemaakt:

- De *hostname* is aangepast naar `rocky2` en de LVM *volume group* heeft een hierop aangepaste naam gekregen
- Het root password is ingesteld als `Pa$$w0rd`
- Een gebruikersaccount `user` wordt aangemaakt met password `Pa$$w0rd`
- De in paragraaf 2.3.5.1 verwijderde software wordt om te beginnen al niet geïnstalleerd
- In plaats van de grafische wordt de *text-mode* installatie gebruikt
- `Clearpart` wordt geïnstrueerd om de disk te overschrijven, dit is voor automatische installaties veel praktischer dan wanneer er nog bevestiging moet worden gevraagd

Het eenmalig aanpassen van een Kickstart bestand voorkomt zoals je ziet veel handmatig werk achteraf. Dit is een van de grote krachten van geautomatiseerde installaties.

### 2.3.6.1 Maak de virtual machine aan

Gebruik hiervoor dezelfde instellingen als voor de eerste server, beschreven in paragraaf 2.3.3.

### 2.3.6.2 Installeer met behulp van kickstart

**Let op:** maak de VM dit keer aan met 'custom' instellingen en zet het geheugen op minstens 3072 MB<sup>§</sup>, anders gaat er waarschijnlijk iets mis met Kickstart; als je wilt kun je later een lagere hoeveelheid geheugen instellen.

Nadat je de VM hebt aangemaakt, zorg je ervoor dat weer vanaf virtuele CD-ROM/DVD geboot wordt; het inrichten van een network boot environment voert op dit moment van het curriculum te ver.

Onderbreek de boot loader tijdens het menu met de Tab toets en voeg de volgende tekst toe aan de GRUB command line die getoond wordt: " `inst.ks=https://edu.nl/vhv44"` (let op de spatie aan het begin).

Bevestig deze aangepaste command line met Enter en bewonder hoe moeiteloos de *text-mode* installatie verloopt als alles al goed is ingesteld. Op deze manier kunnen talloze systemen met relatief weinig inspanning naar eigen inzicht geïnstalleerd worden.

### 2.3.6.3 Reboot en neem het systeem in gebruik

Aan het einde van de installatie wordt gevraagd om de Enter toets te drukken om het systeem te rebooten waarna het opstart met de nieuwe Linux installatie.

<sup>§</sup> Conform <https://access.redhat.com/articles/rhel-limits>



Het systeem wordt nu opgestart voor normaal gebruik, de installatie is afgerond.

Optioneel kun je één of beide Rocky systemen aan het Windows domein toevoegen. Zie hiervoor opdracht 2.2.8.

### 2.3.7 Vragen Linux Installatie en Package Management

1. Noem een vijftal Linux distributies en geef aan of deze in de Red Hat-, Debian- of SUSE-familie thuishoren of van geen van deze drie afgeleid zijn
2. Wat is het meest in het oog springende verschil tussen de distributies in de Red Hat- en SUSE-families enerzijds en in de Debian-familie anderzijds?
3. Waarin verschillen *enterprise* (zakelijk gerichte) distributies van overige distributies?
4. Welke services hebben we in het netwerk nodig als we willen installeren zonder gebruik te maken van een boot CD (image)?
5. Wat zijn de voordelen van installaties met behulp van een geautomatiseerde *installer* (bijvoorbeeld Kickstart) ten opzichte van handmatige installaties?
6. Wat zijn de voordelen van package bestanden (bijvoorbeeld `.rpm` of `.deb`) ten opzichte van eenvoudige archieven (bijvoorbeeld `.tar.gz` zoals in hele vroege Linux distributies gebruikt werden)?
7. Waarom bestaan er *high-level* package management tools als APT, YUM en ZYpp?
8. Maak de volgende zin af: Als softwarepakket *X* afhankelijk is (ofwel: een *dependency* heeft) van softwarepakket *Y*, dan zorgt een *high-level* package management tool ervoor dat wanneer pakket *X* geïnstalleerd wordt, ...
9. Wat wordt in de context van Linux *package management* bedoeld met de term *repository*?
10. Wat zijn de belangrijkste verschillen tussen het commando “`sudo rpm -U openssl-1.0.1e-51.el7_2.2.x86_64.rpm`” en het commando “`sudo yum update openssl`”?
11. Welke vier beheerderstaken worden in de lesstof (hoofdstuk 6) genoemd als het gaat om software?
12. Benoem de stappen die noodzakelijk zijn bij installeren van Linux.
13. Wat is PXE?
14. Waar staat de afkorting YUM voor?
15. Wat is de functie van een `ks.cfg` bestand?
16. In welke sectie van het `ks.cfg` bestand wordt aangegeven welke pakketten er geïnstalleerd moeten worden?
17. Wat is het verschil tussen `rpm` en `dpkg`?
18. Wat zijn de drie doelen van het gebruik van metapackage management systems als APT, YUM en Red Hat Network?
19. Met welk commando en syntax kun je een Linux systeem up-to-date houden?
20. Welke optie kun je gebruiken om bij `apt-get upgrade` direct de software te installeren?

## 2.4 Week 2, College 1: Windows Core

### Inleiding

De introductie van Microsoft Windows Server Core bij de release van Windows Server 2012 is globaal gezien één van de meest in het oog springende veranderingen in het Microsoft Server programma. Immers, het besturingssysteem heeft de naam “Windows”, maar laat zich beheren vanaf de console (ondertussen is Microsoft nog een stap verder gegaan met de introductie van [Windows Server Nano](#))!

Wat is Windows Server 2016 Core? Kort gezegd, een besturingssysteem zonder een volledige grafische omgeving. De GUI is in ieder geval zeer beperkt! De voordelen en mogelijkheden ga je in deze opdracht gaan bestuderen.

Beter Medisch Centrum wil graag van deze functionaliteit gebruik maken, om dat een server zonder grafische omgeving minder resources nodig heeft en minder storingsgevoelig is.



De omgeving waarin je deze opdrachten gaat uitvoeren kan dezelfde virtuele omgeving zijn die je eerder hebt gebruikt. Je hebt hiervoor minimaal nodig:

- Een Windows Server 2016/2019 DC in het domein `bmc.local`. (vorige opdracht!)
- Twee 2016/2019 Core machines
- Een cliënt binnen het domein. Bij voorkeur Windows 10 uit 2020 of later in verband met de installatie van RSAT en latere opdrachten. Geef de cliënt een statisch IP-adres! De DHCP-server komt later.

#### Theorie:

##### Verplicht:

- Slides,
- Dit werkboek met vragen en antwoorden (zie afzonderlijk document "Antwoorden\_BIPL\_Werkboek\_v1.4.1vt"!)
- Boek: "Windows Server 2016 Unleashed":
  - Hoofdstuk 3, *Installing Windows Server 2016 and Server Core*:
    - volledig (blz. 89 t/m 124)

##### Optioneel:

- Introductie Windows Server Core met links naar meer informatie: <https://docs.microsoft.com/en-us/windows-server/administration/server-core/what-is-server-core>
- Installeren in Core mode: <https://www.dtonias.com/install-windows-server-2016-core/>

##### Video's

- Server Core installatie, configuratie en management: <https://www.youtube.com/watch?v=EWqiEA3OU-c>
- Optioneel: "BIPL\_windows\_week2\_core2016.mp4" (zie Canvas)

## 2.4.1 Opdracht: Installatie van Windows Core

Installeer een Windows Core server zoals beschreven in de genoemde theorie en/of video's.

## 2.4.2 Opdracht: Basisconfiguratie met sconfig

Nadat je de Core-machine geïnstalleerd en gestart hebt, ga je de onderstaande handelingen uitvoeren.

- 1) Geef de eerste Core Server een IP-adres in de range van het netwerk.  
Je kunt hierbij gebruikmaken van van het netsh commando of van sconfig. Extra informatie over netsh vind je in de eerder genoemde documentatie "Server Core installation ..." en hier: [http://technet.microsoft.com/en-us/library/cc785383\(Ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc785383(Ws.10).aspx). Extra informatie over sconfig vind je hier: <http://technet.microsoft.com/en-us/library/jj647766.aspx>. Voor het configureren van Server core 2016 kun je ook dit doornemen: <http://technet.microsoft.com/en-us/library/jj592692.aspx> (o.a. firewall, IP).
- 2) Denk ook aan het toekennen van een IP-adres voor de DNS-server in het domein.
- 3) Wijzig de computernaam naar bijvoorbeeld 2016-core1. Hiervoor heb je verschillende opties waaronder:
  - Gebruikmaken van PowerShell. In de command prompt kun je naar PowerShell switchen door powershell in te typen. Vervolgens:
    - `rename-computer <computernaam>;`
    - Herstarten gaat met `restart-computer`.
  - Gebruik maken van sconfig. Start dit door het commando sconfig te geven en kies voor optie 2. Herstart de computer wanneer dit voorgesteld wordt.
- 4) Als je een 2016 server met powershell op afstand beheert moet *remoting* enabled zijn: `Enable-PSRemoting`.
- 5) Maak de 2016-core1 machine na een herstart lid van het domein `bmc.local`. De server wordt dus een *member server* ([http://technet.microsoft.com/en-us/library/cc737599\(Ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc737599(Ws.10).aspx)).



- 6) De Core machine kan van een willekeurige andere computer in het domein worden beheerd met behulp van de Server Manager of een MMC en de juiste *snap-ins*. Zorg dat remote beheer mogelijk is. Configureer vanaf de command line de firewall zodat remote beheer via RDP mogelijk is. Log in op de Core machine (let op dat je bij het opstarten niet automatisch wordt ingelogd in het domein. Je moet in het zwarte scherm na de reboot klikken op Esc en dan kiezen voor Other user. Het menu wat je dan krijgt moet je even invullen. Het wijst zich vanzelf. Let wel op dat het invoeren van Administrator er zeer waarschijnlijk toe zal leiden dat het de local admin is. Geef @bmc.local mee, de domeinnaam wordt dat weer aangepast). Gebruik vervolgens sconfig om het remote beheer mogelijk te maken. Voor informatie over het beheer van een Server Core machine kun je hier vinden: <http://technet.microsoft.com/en-us/library/jj574205.aspx>. (Gaat over versies 2012 en 2012R2 maar klopt nog steeds en geeft meer informatie dan het vergelijkbare artikel met betrekking tot versies 2016 en later). De firewall op de Core machine mag eventueel in deze fase ook volledig worden uitgezet om grafisch vanaf een andere machine de firewall te configureren.
- 7) Controleer of je vanaf de DC met behulp van een *snap-in* in een MMC computer management op de Core server kunt starten. Mogelijk kun je *local users*, *event viewer* en *performance* ook starten en bekijken. *Disk management*, *device manager* en de firewall kunnen doorinstellingen in de firewall en services op dit moment nog niet worden gestart!

### 2.4.3 Opdracht: Windows server Core Domain controller

Het configureren van een Core machine kan dus met sconfig, netsh of PowerShell gebeuren.

In dit deel van de opdracht ga je een tweede Core machine configureren en daarbij mag je gebruikmaken van bovenstaande tools op de Core machine zelf of de ServerManager (remote) op een GUI machine.

De volgende opdrachten ga je uitvoeren op de tweede Core-server:

1. De tweede Core machine ga je promoveren tot Domain Controller. Dit kan bijvoorbeeld met PowerShell op de lokale computer of met de Server Manager vanaf een andere computer. Voordat je dit gaat doen moet je ook hier weer:
  - De server een naam geven: Servernaam: 2016-core2
  - IP-instellingen configureren: een IP-adres in de range van de DC
  - Zorg ervoor dat remote beheer mogelijk is, dat kan met behulp van sconfig
2. Installeer vervolgens de DNS-server rol om de tweede Core server te kunnen gebruiken als secundaire DNS-server in het domein.
3. Installeer Active Directory Domain Services en promoveer de server tot (peer) DC in het bestaande domein bmc.local.
4. Maak op de cliënt een MMC met daarin de snap-in Active Directory Users & Computers (ADUC). Voeg via de Core machine een nieuwe OU en gebruiker toe. Controleer of deze op DC1 te zien zijn. De replicatie van de objecten kan de nodige tijd in beslag nemen.
5. Controleer bij de DNS-server of er voor de Core machine ook een NS-record is aangemaakt. Ook hiervoor moet je rekening houden met replicatie tijd. Maak een (fictief) CNAME of A-record aan. Controleer de replicatie.

### 2.4.4 Vragen Windows Core

1. Wat zijn de voordelen van de Core Editie?
2. Wat zijn de nadelen van de Core Editie?
3. Welke Server Roles kunnen op de Core editie worden geïnstalleerd?
4. Kan een Core machine een Read Only Domain Controller (RODC) *role* krijgen?
5. Met behulp van welk script kun je een Windows Core machine activeren?
6. Configuratie van o.a. de netwerkinstellingen en de firewall gebeurt onder de Core editie vanaf de command-line of PowerShell met het programma netsh. Wat is de functie van netsh? Bij de specifieke opdrachten over de basisconfiguratie vind je een link naar informatie over netsh.
7. Wat is de netsh syntax om de IP-instellingen op te vragen?
8. Hoe configureer een IP-adres met netsh?
9. Bij het opgeven van een DNS-server via netsh kom je optie index tegen. Wat is hiervan de functie?



10. Welk commando kun je gebruiken om een core machine te herstarten?
11. Wat is de syntax voor het aanmelden van de core machine bij het domein?
12. Microsoft levert in de Core editie een aantal VBS scripts mee, wat is de functie van het script `s1mgr.vbs` en welke parameters kun je hier aan meegeven?
13. Wat is de functie van `sconfig.cmd`?
14. In welke directory staat de tool (`sysprep`) om de Security ID's (SID) te vernieuwen?
15. Welke opties heeft `sysprep`?
16. Wat is de functie van de tool `mountvol`? <http://technet.microsoft.com/en-us/library/cc976820.aspx>
17. De command line tool `mountvol` geeft bij het uitvoeren ervan een lijst met alle volumes weer. Hierbij wordt tevens een getal weergegeven wat is dit voor een getal en wat is hiervan de functie?
18. Wat doet de parameter `/d` bij `mountvol`?
19. Wat is het PowerShell commando waarmee je de AD-Domain-Services kunt installeren op de Core server?

## 2.5 Week 2, College 2: De Linux Shell

### Inleiding

Vorige week heb je voor een deel van de Linux *package management* opdracht al een paar taken uitgevoerd via de command line. In de UNIX en Linux wereld staat de command line interpreter bekend als de *shell*.

Dit is voor beheerders de meest krachtige omgeving binnen Linux, die ook de gelegenheid biedt taken te automatiseren door commando's op te slaan in zogenaamde *shell scripts*. Daarnaast zijn een aantal configuraties alleen te maken via configuratiebestanden.

Beter Medisch Centrum verwacht daarom dat je voor het beheeren van de Linux systemen goed uit de voeten kunt met de Linux shell, en niet afhankelijk bent van grafische hulpmiddelen, al helemaal om dat met het oog op de prestaties en de veiligheid de productieservers zo kaal mogelijk uitgerust zullen worden, dus liefst zonder GUI.

### Theorie

#### Verplicht:

- Slides,
- Dit werkboek met vragen en antwoorden (zie afzonderlijk document "Antwoorden\_BIPL\_Werkboek\_v1.4.1vt"!)
- Boek: "Unix and Linux System Administration Handbook, 5<sup>th</sup> Edition":
  - Chapter 7 – *Scripting and the Shell*
    - Inleiding (blz. 182)
    - 7.1 *Scripting philosophy*: blz. 183 t/m 188
    - 7.2 *Shell basics*: blz. 189 t/m 198
    - 7.3 *sh scripting*: blz. 198 t/m 209
    - 7.4 *Regular expressions*: blz. 209 t/m 215 (tot: 7.5 Python programming)
  - Chapter 4 – *Process Control*
    - Alles behalve 4.9 *Periodic processes*: blz. 90 t/m 109
    - FreeBSD onderdelen niet verplicht voor tentamen
- Learning the Shell: [http://linuxcommand.org/lc3\\_learning\\_the\\_shell.php](http://linuxcommand.org/lc3_learning_the_shell.php), alle 10 hoofdstukken.

#### Optioneel:

##### Video's

- [https://www.youtube.com/watch?v=3BZzFRPYU\\_I](https://www.youtube.com/watch?v=3BZzFRPYU_I)
- <https://www.youtube.com/watch?v=ZAnI2DB4D08>





## 2.5.1 Opdracht 1: Kennismaking met de shell

### 2.5.1.1 Help!

Start een command line sessie. Hiervoor heb je weer dezelfde opties als in paragraaf 2.3.5 (blz. 23).

Gelukkig hoef je niet alle commando's en hun opties uit je hoofd te kennen om met de shell te kunnen werken. Wanneer je even niet weet hoe iets werkt, dan zijn er verschillende opties waarmee we nu zullen oefenen. Probeer altijd te onthouden dat je op deze hulpmiddelen kan terugvallen wanneer je met de command line interface bezig bent.

#### Het --help argument dat door de meeste programma's ondersteund wordt

Het programma "cat" kan gebruikt worden om tekst naar het scherm te sturen, bijvoorbeeld:

```
[user@rocky1 ~]$ cat /etc/hosts
127.0.0.1    localhost localhost.localdomain localhost4 localhost4.localdomain4
::1         localhost localhost.localdomain localhost6 localhost6.localdomain6
[user@rocky1 ~]$
```

Geef het commando "cat --help" en je krijgt de volgende output te zien:

```
Usage: cat [OPTION]... [FILE]...
Concatenate FILE(s) to standard output.

With no FILE, or when FILE is -, read standard input.

  -A, --show-all           equivalent to -vET
  -b, --number-nonblank    number nonempty output lines, overrides -n
  -e                       equivalent to -vE
  -E, --show-ends          display $ at end of each line
  -n, --number             number all output lines
  -s, --squeeze-blank      suppress repeated empty output lines
  -t                       equivalent to -vT
  -T, --show-tabs          display TAB characters as ^I
  -u                       (ignored)
  -v, --show-nonprinting   use ^ and M- notation, except for LFD and TAB
      --help              display this help and exit
      --version            output version information and exit

Examples:
  cat f - g  Output f's contents, then standard input, then g's contents.
  cat       Copy standard input to standard output.

GNU coreutils online help: <https://www.gnu.org/software/coreutils/>
Full documentation at: https://www.gnu.org/software/coreutils/cat
or available locally via: info '(coreutils) cat invocation'
```

Kijk naar de output van "cat --help", bepaal welke optie er voor zorgt dat elke regel genummerd wordt en toon /etc/hosts op jouw Linux VM met regelnummers.

#### De handleiding voor een commando

Het commando "clear" maakt het terminal window leeg en heeft een redelijk overzichtelijke manpage (de gangbare term voor een handleiding, kort voor "manual page"). Vraag deze op met het commando "man clear". De pagina wordt geopend in een zogenoemde *pager*, die voorkomt dat de output het scherm afscrollt. Indien nodig kun je verder lezen door spatie of de f-toets (van forward) te drukken of teruggaan door de b-toets (van backward) te drukken. Na het lezen verlaat je de pagina weer door op de q-toets (van quit) te drukken. De output ziet eruit als volgt:





```
clear(1)                                General Commands Manual                                clear(1)

NAME
    clear - clear the terminal screen

SYNOPSIS
    clear [-Ttype] [-V] [-x]

DESCRIPTION
    clear clears your screen if this is possible, including its scrollback
    buffer (if the extended "E3" capability is defined).  clear looks in
    the environment for the terminal type given by the environment variable
    TERM, and then in the terminfo database to determine how to clear the
    screen.

    clear writes to the standard output.  You can redirect the standard
    output to a file (which prevents clear from actually clearing the
    screen), and later cat the file to the screen, clearing it at that
    point.

OPTIONS
    -T type
        indicates the type of terminal.  Normally this option is unneces-
Manual page clear(1) line 1 (press h for help or q to quit)
```

De manpage is opgedeeld in een aantal standaardhoofdstukken, waaronder enkele die in vrijwel elke manpage voorkomen:

- "SYNOPSIS" met daarin de naam van het commando en vaak ook een korte omschrijving
- "DESCRIPTION" met daarin een uitgebreide omschrijving, inclusief een lijst met beschrijvingen van de eventuele opties die gegeven kunnen worden
- "SEE ALSO" (tweede pagina) met daar verwijzingen naar manpages die een relatie hebben met de manpage die bekeken wordt

Een uitgebreider commando is "ls" voor het tonen van directory-inhoud.

- Bekijk bijvoorbeeld eens de inhoud van de directory /etc/sysconfig.
- Bekijk de manpage voor "ls" en zoek naar de optie die de sorteervolgorde omdraait. Gebruik deze optie om de inhoud van de directory /etc/sysconfig in omgekeerde volgorde weer te geven. Is de volgorde precies omgedraaid?

### Een commando zoeken op trefwoord

Dit vergt een kleine voorbereiding voor een zojuist geïnstalleerd systeem: dagelijks wordt de database met daarin de index van alle manpages aangemaakt of ververst, maar de kans is zeer klein dat dat al is gebeurd wanneer je aan deze opdracht begint.

- Voer daarom het volgende commando uit: "sudo mandb". Vervolgens is het mogelijk te zoeken op basis van een trefwoord in de omschrijving van manpages.
- Zoek met behulp van het commando "man -k logged" naar het commando dat laat zien wie er zijn ingelogd (de omschrijving die "man -k" teruggeeft en waarin we nu geïnteresseerd zijn is "show who is logged on". Open vervolgens de manpage voor het commando met deze omschrijving.
- Met behulp van welke optie kan getoond worden wanneer het systeem voor het laatst geboot is? Probeer het commando met deze optie uit.

### 2.5.1.2 Omgevingsvariabelen

Binnen de *shell* heb je de beschikking over een groot aantal omgevingsvariabelen (ofwel *environment variables*). Enkele daarvan zullen we in deze opdracht bekijken.



Start een command line sessie. Hiervoor heb je weer dezelfde opties als in paragraaf 2.3.5 (blz. 23).  
Nu kunnen we een paar handige omgevingsvariabelen bekijken:

- Bekijk via de omgevingsvariabele \$USER met welk account je ingelogd bent
- Bekijk via de omgevingsvariabele \$HOSTNAME wat de naam van de VM is
- Kijk ook in welke directory je nu staat, als het goed is kan je via een omgevingsvariabele hetzelfde pad achterhalen als met het commando pwd.

### 2.5.13 Werken met directories

Onder Windows en in andere GUI's ben je gewend dat je "mapjes" van de ene naar de andere plek kunt slepen of knippen en plakken. Op de command line zit dat natuurlijk iets anders in elkaar, terwijl het wel belangrijk is om directories te kunnen kopiëren, verplaatsen of hernoemen.

Kopieer de directory /etc/sysconfig naar een directory in je home directory genaamd sysconfbackup. Zorg dat eventuele fouten die daarbij optreden gelogd worden in je home directory in het bestand backuperror.log. Welk commando met welke opties heb je hiervoor gebruikt en wat is de inhoud van het bestand backuperror.log?

Geef een verklaring voor de foutmeldingen die je ziet in het bestand backuperror.log. Hernoem de zojuist gemaakte directory sysconfbackup naar sysconfbackup.oud. Welk commando gebruik je hiervoor?

Kopieer opnieuw de directory /etc/sysconfig naar een directory in je home directory genaamd sysconfbackup. Ditmaal willen we echter een lijst hebben van alle bestanden die wel goed gekopieerd zijn. Normaal gesproken laat het commando cp niets zien als het goed gaat. Zoek dus eerst uit (via bijv. man) hoe je ervoor kunt zorgen dat cp dit wel laat zien.

Zorg er dan ook voor dat de lijst met gekopieerde bestanden vastgelegd wordt in een bestand in je home directory genaamd backup.1st. Welk commando met welke opties heb je hiervoor gebruikt?

Geef een verklaring waarom er geen foutmeldingen te zien zijn in het bestand backup.1st, terwijl die wel op je scherm verschenen.

Verwijder beide backup-directories volledig. Welk commando met welke opties heb je hiervoor gebruikt?

### 2.5.14 Zoeken naar tekst in bestanden

Een van de meest voorkomende acties die je in de shell zult uitvoeren in het kader van beheerswerkzaamheden is het zoeken naar tekst: specifieke termen in logfiles of instellingen in configuratiebestanden waarvan je wel de waarde maar niet de locatie kent bijvoorbeeld.

- Zoek in het bestand /var/log/messages naar het woord "started". Welk commando heb je hiervoor gebruikt en hoe zag de output eruit? (Tips: denk aan man -k <zoekterm>, hulp via de manpage, het gebruik van sudo en de hoofdletter gevoeligheid van Linux!)
- Zoek onder de directory /usr/share/doc naar alle bestanden waar in de bestandsnaam het woord "linux" voorkomt (tip: hoofdletters zijn belangrijk!). Welk commando heb je hiervoor gebruikt en hoe zag de output eruit?
- Ga na hoeveel bestanden er bestaan onder /usr/share/doc waar in de bestandsnaam het woord "README" voorkomt (tip: kijk hiervoor eens naar het commando wc, en de opties van dat commando). Welk commando heb je hiervoor gebruikt en hoe zag de output eruit?



### 2.5.15 Procesbeheer

Processen zijn prima vanaf de command line te beheren, Linux biedt daarvoor alle benodigde hulpmiddelen. Laat een lijst zien met alle processen die er op het systeem draaien.

- Welk commando met welke opties gebruik je hiervoor (tip: kijk naar de output van “man -k “current process””)?
- Kijk nu ook eens “realtime” naar welke processen er op dit moment draaien. Welk proces maakt op dit moment het meest gebruik van de CPU (tip: top)?

#### **SLA NU AL HET WERK WAT JE IN DE VM NOG OPEN HEBT STAAN OP!**

- Zoek het proces met de naam gnome-session-binary. Welk commando gebruik je hiervoor? En wat is het PID van dat proces?
- Voer het volgende commando uit: kill <PID van gnome-session-binary>  
Wat gebeurt er?

### 2.5.2 Opdracht 2: scripting

*Shell scripting* is de term voor het automatiseren van taken door shell commando's samen te voegen in een tekstbestand zodat deze voortaan met alleen een aanroep van dat bestand, het *shell script*, kan worden uitgevoerd.

Een goed voorbeeld is de scripting die automatisch wordt uitgevoerd wanneer de BASH shell wordt gestart en die al standaard op het systeem aanwezig is. Dit is daarom goede scripting om wat mee te experimenteren.

Pas de BASH opstart-scripts zo aan, dat **alleen voor de gebruiker root**:

- a. bij een inlog-shell op het scherm “Welkom, super(wo)man!” verschijnt,
- b. bij alle (dus ook niet-inlog-) shells de inhoud van het bestand /etc/redhat-release weergegeven wordt.

Zorg ervoor dat:

- c. /opt/microsoft/powershell/7 **voor alle gebruikers** voorkomt in hun PATH environment variabele.  
Uitleg: stel er zijn (technische) gebruikers die verschillende versies van PowerShell onder Linux willen gebruiken en je wilt dat het commando pwsh standaard de versie in /opt/microsoft/powershell/7 start (mocht je het daadwerkelijk willen testen, instructies voor de installatie van PowerShell 7 onder RHEL/CentOS/Rocky 8 vind je [hier](#)).
- d. voor gewone gebruikers (dus **niet** voor de root-gebruiker) bij het opstarten van alle shells (dus ook niet-inlog-)shells getest wordt of het bestand “todo.txt” bestaat in diens home-directory:
  - i. als dit bestand bestaat, zorg er dan voor dat de inhoud daarvan wordt weergegeven,
  - ii. als het niet bestaat, geef dan de melding “Je hebt nog geen todo.txt! Maak deze z.s.m. aan.” weer.

### 2.5.3 Vragen Linux Shell

1. Op welke manier verschillen de commando's

```
ls -l /etc
```

en

```
ls -l /etc > /tmp/lijstje
```

met elkaar?

2. Wat doet de onderstaande regel shell scripting?

```
if [ -r /etc/shadow ] ; then echo "Ingelogd als root of je shadow password file staat te open"; fi
```



3. Wat is het verschil tussen SIGINT en SIGTERM enerzijds en SIGKILL anderzijds?
4. Leg uit wat er “nice” is aan een programma waarvan met het nice commando de prioriteit is verlaagd
5. Wat is het doel van het werken met scripts?
6. Noem drie Linux Shell-versies.
7. Welke programmeertalen worden in het boek genoemd om te gebruiken als het gaat om complexere scripts (meer dan 100 regels)?
8. Wat zijn de nadelen van de bij vraag 7 genoemde talen?
9. Welke toetscombinaties kun je in een tekst-editor als Emacs gebruiken om naar het begin of eind van een tekstregel te springen?
10. Processen onder Linux hebben drie communicatiekanalen. Welke drie zijn dat?
11. Geef een korte beschrijving van STDIN, STDOUT en STDERR. Welke symbolen kunnen in een pipeline worden gebruikt om commando aan elkaar te koppelen of om bijvoorbeeld de output weg te schrijven in een tekstfile?
12. Welke symbolen kunnen in een pipeline worden gebruikt om commando aan elkaar te koppelen of om bijvoorbeeld de output weg te schrijven in een tekstfile?
13. Welk commando kun je gebruiken om in bijvoorbeeld /var/messages te zoeken naar specifieke foutmeldingen?
14. Op welke manier worden in de shell variabele gedefinieerd en aangeroepen?
15. In de Shell zijn variabelen niet hoofdletter gevoelig? (Eens/oneens)
16. Welk commando kan in een Shell worden gebruikt om woorden en zinnen te tellen en welk commando gebruik je om een specifiek patroon in directory of een bestand weer te geven?
17. Hoe kun je aan een script aflezen dat het om een Bash-script gaat?
18. Welk commando heb je nodig om de permissies van een bestand (lees: een script) aan te passen zodat deze kan worden uitgevoerd?
19. Wat is kenmerkend voor variabelen in Bash?
20. Welke richtlijnen voor scripts worden in het boek genoemd?
21. Welke componenten behoren bij een (Linux/ Unix) proces?
22. Wat is een Proces ID (PID)?
23. Welke twee gebruikers en groeps ID's zijn er in Linux?
24. Op welke manier bepaalt de kernel hoeveel CPU-tijd een proces bijvoorbeeld krijgt?
25. Hoe wordt de administratieve waarde genoemd die mede kan bepalen hoeveel CPU-tijd een proces krijgt?
26. Wat is de functie van init binnen Linux?
27. Wat zijn onder Linux belangrijke signalen?
28. Welke twee signalen kunnen niet worden geblokkeerd of worden gestopt?
29. Welke command/syntax moet je gebruiken om een proces, zoals dat van de Apache Webserver, te stoppen?
30. Welke vier process states kent Linux?
31. Kan een administrator (root) wanneer een proces met een STOP of een TSTP signaal gestopt is, het proces administratief weer starten (Ja, dat kan / Nee, dat kan niet)
32. Een hoge nice waarde betekent dat de kernel het proces een hoge prioriteit toekent. (Juist/ Onjuist)
33. Welk commando kun je gebruiken om te zien welke processen op een systeem draaien?
34. Met welk commando kun je informatie krijgen over de processen die het meeste systeembronnen vragen.? (De informatie moet ook circa elke 10 seconden worden ververs!)
35. Uit welke directory halen de tools ps en top hun informatie?
36. Welk commando kun je gebruiken om te achterhalen wat een proces doet?

## 2.6 Week 3, College 1: Windows Gebruikers en Groepen

### Inleiding

Geen school zonder studenten, geen bedrijf zonder medewerkers, geen domein zonder gebruikers. Studenten, medewerkers en gebruikers hebben allemaal met elkaar gemeen dat ze in een Windows domeinomgeving een gebruikersaccount moeten krijgen.



De accounts moeten worden aangemaakt en ze moeten tevens worden onderhouden. Hiervoor heeft Microsoft o.a. de onderstaande tools ontwikkeld:

- Active Directory Users and Computers (ADUC), Active Directory Administrative Center (ADAC), PowerShell, DSadd, csvde, Ldifde enz.
- Dsmode, Dsquery en Dsmove zijn command line tools voor het aanpassen van gebruikers. Ook Batch files en scripts kun je gebruiken om een groot aantal gebruikers tegelijk in Active Directory aan te maken.

Naast het aanmaken van de gebruikers ga je kijken naar het aanmaken van o.a. profielen, homefolders en het aanpassen van gebruikers specifieke eigenschappen en *Organizational Units (OU's)*. OUs zijn container objecten binnen het domein. OU's kunnen onder andere worden gebruikt om gebruikers overzichtelijk te rangschikken, Group Policies aan te linken en om het beheer over te dragen. De opdracht moet de verschillende technieken belichten en de voor- en nadelen van de tools en de OU's bekijken.

Voor het uitvoeren van de opdracht heb je een domeinomgeving nodig. Je kunt verder werken met de bestaande omgeving. Om te voorkomen dat je bij een foutje opnieuw moet beginnen, is het verstandig om te werken met snapshots. Vraag eventueel aan de docenten wat dit is en hoe je dat doet. Om deze opdracht te kunnen uitvoeren heb je minimaal de volgende machines nodig. De omgeving moet minimaal bestaan uit een DC in het bmc.local domein en een cliënt. Bij voorkeur een 2016 machine en als cliënt Windows 10. Je kunt gebruik maken van de omgeving uit de Windows 2016 Core opdracht.

#### Theorie Verplicht:

- Slides,
- Dit werkboek met vragen en antwoorden (zie afzonderlijk document "Antwoorden\_BIPL\_Werkboek\_v1.4.1vt"!)
- Boek: "Windows Server 2016 Unleashed":
  - Hoofdstuk 6, *Designing Organizational Unit and Group Structure*:
    - volledig (blz. 185 t/m 206)
  - Hoofdstuk 17, *Windows Server 2016 Administration*:
    - *Windows Server 2016 Active Directory Groups tot Managing Users with Local Security and Group Policies* (blz. 574 t/m 579)

#### Optioneel:

- Informatie over csvde:
  - [http://technet.microsoft.com/en-us/library/cc732101\(Ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc732101(Ws.10).aspx)
- Informatie over Ldifde:
  - <http://support.microsoft.com/kb/237677>
  - [http://technet.microsoft.com/en-us/library/cc731033\(Ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc731033(Ws.10).aspx)
- Informatie over dsadd: [http://technet.microsoft.com/en-us/library/cc731279\(Ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc731279(Ws.10).aspx)
- Informatie over dsquery: [http://technet.microsoft.com/en-us/library/cc725702\(Ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc725702(Ws.10).aspx)
- Informatie over dsmode: [http://technet.microsoft.com/en-us/library/cc732954\(Ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc732954(Ws.10).aspx)
- Opzetten roaming profiles: <https://docs.microsoft.com/en-us/windows-server/storage/folder-redirection/deploy-roaming-user-profiles>

#### Video's

- 1) ADUC: <https://www.youtube.com/watch?v=LPdcoEDasu4>
- 2) Dsadd: <https://www.youtube.com/watch?v=HUNllp4aWHs>
- 3) Dsquery: <https://www.youtube.com/watch?v=wyFLGExR5i4>
- 4) CSVDE: <https://www.youtube.com/watch?v=iUAqz7FbqSs>



### 2.6.1 Opdracht: User Management met de GUI: ADAC

**Let op: Je moet voor deze opdracht de OU's uit opdracht 2.2.6 minimaal hebben aangemaakt. Mocht je dat (nog) niet hebben gedaan, doe dit dan eerst. Denk er verder aan dat tijdens het importeren van de gebruikers er mogelijk nog ontbrekende OU's zijn!**

Om toegang tot het netwerk te krijgen moet een gebruiker beschikken over een gebruikersaccount. In eerste opzicht lijkt deze te bestaan uit één naam en een wachtwoord. In de rest van de weekopdracht zal je zien dat een gebruikersaccount uit veel meer bestaat, maar nu eerst maar eens de gebruiker aanmaken met Active Directory Administrative Center (ADAC).

- Maak met ADAC de onderstaande gebruiker aan. Plaats deze in de OU Medewerkers. Als de OU nog niet bestaat, maak deze dan nu aan! Bij de User logon naam kiezen we de volledige voor- en achternaam gescheiden door een punt.
  - Pieter Florisse met het wachtwoord Pa\$\$w0rd
- Let op de "Windows PowerShell History" onderaan het scherm. Mogelijk moet je de Powershell History eerst zichtbaar te maken door rechts onderin op het knopje met het dakje (^) te klikken. Je ziet daar welke acties je hebt uitgevoerd via de GUI en je kan deze eventueel kopiëren, aanpassen en uitvoeren via de command line/ PowerShell.

### 2.6.2 Opdracht: User Management met de GUI: ADUC

In de inleiding zijn een aantal tools aangegeven die kunnen worden gebruikt voor het aanmaken van gebruikers. Eén daarvan is de grafische tool/ snap-in Active Directory Users and Computers (ADUC).

- 1) Maak met Active Directory Users and Computers de onderstaande gebruiker aan. Plaats deze in de OU Medewerkers. Bij de User logon naam kiezen we de volledige voor- en achternaam gescheiden door een punt.
  - Jacob van Obdam met het wachtwoord Pa\$\$w0rd. De default instellingen voor het wachtwoord zijn voor nu voldoende.
- 2) Maak de onderstaande template user aan en pas de instellingen aan. Maak ook deze weer in de OU medewerkers.
  - \_templateuser1 met het wachtwoord Pa\$\$w0rd. (Uit praktische overwegingen vinkje bij *user must change password at next logon* weghalen. Uit veiligheidsoverwegingen in een bedrijfsomgeving niet aan te raden)
  - General: Telephone number 035-432567, Description: Medewerker
  - Address: Nijenoord 1, Utrecht, Utrecht 3552 AS Netherlands
  - Account: logon Hours van 7.00 tot 19.00 van Maandag t/m Zaterdag
  - Telephones: home 1111, mobile 2222
  - Organization: Job title: Medewerker, Department Systeembeheer
  - Member of: Server Operators
- 3) Maak de onderstaande gebruikers aan door van \_templateuser1 een kopie te maken:
  - Cornelis de Oude
  - Abraham van den Hulst
- 4) Wat wordt er van de templategebruiker overgenomen?
- 5) Uit veiligheidsoverweging is het verstandig om een template user uit te schakelen (disable user) als deze niet wordt gebruikt. Zorg ervoor dat de template user niet zomaar gebruikt kan worden.
- 6) Hoe herken je in ADUC dat de gebruiker op *disabled* staat?

### 2.6.3 Opdracht: Command line tools Gebruikers importeren

Het aanmaken van gebruikers via ADAC en ADUC is vrij eenvoudig en vlot te doen, totdat je honderden gebruikers moet gaan aanmaken. Command-line tools en scripts (waarin commandline tools worden gebruikt!) zijn dan vaak handiger. Deze tools ga je in de volgende opdrachten gebruiken. We beginnen met CSVDE en LDIFDE. De genoemde bestanden vind je overigens op Canvas (*BIPL\_Users.zip*). Let op dat als je de optionele





opdrachten niet zelf uit gaat voeren, dat je mogelijk wel de extra gebruikers, groepen en/of OU's zal moeten toevoegen. Hiervoor is op Canvas een extra zip-bestand (*BIPL\_Optioneel\_Users.zip*) beschikbaar. Schrijf ook de Windows commando's weer op!

#### CSVDE en LDIFDE:

- 1) Importeer de gebruikers uit het bestand *patienten1.csv* met *csvde*.
  - Welke syntax heb je hiervoor gebruikt? (Schrijf dit op, het kan voor het practicumtentamen van belang zijn!)
  - Zie je de geïmporteerde gebruikers direct in ADUC verschijnen?
- 2) Importeer de gebruikers uit het bestand *patienten2.csv*. Het is handig om de optie *-k* te gebruiken bij het importeren. Hierin is door een beheerder per ongeluk een fout gemaakt. Bekijk het bestand (kan ook met Wordpad) en corrigeer de twee fouten.
  - Welke syntax kun je gebruiken om tijdens het importeren de fout te laten weergeven?
  - Welke parameter kun je gebruiken om fouten of mededelingen, ten aanzien van een al bestaand object, tijdens het importeren over te slaan?
- 3) Importeer het bestand *patienten3.ldf* met *ldifde*.
  - Welke parameters heb je hiervoor gebruikt?

Met de bovenstaande documenten heb je gebruikers geïmporteerd. Als je de *csv* en *ldf*-bestanden bekijkt, dan bevatten ze een beperkte hoeveelheid informatie over de gebruikers. Dan kan ook anders.

- 4) Bekijk de eerste regel van het bestand *patienten4.csv*.

- Wat valt je hierbij op?

Als je zelf extra opties zou willen toevoegen aan het *csv*-bestand, dan kun je de LDAP attributes vinden via de volgende URL's (scroll naar properties!):

[http://msdn.microsoft.com/en-us/library/aa746340\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/aa746340(VS.85).aspx) of

[http://www.computerperformance.co.uk/Logon/LDAP\\_attributes\\_active\\_directory.htm](http://www.computerperformance.co.uk/Logon/LDAP_attributes_active_directory.htm)

- Importeer het bestand *patienten4.csv* en controleer of (één) van de gebruikers ook daadwerkelijk de opgegeven LDAP-attributes heeft mee gekregen.

## 2.6.4 Optioneel: Zelf importbestanden maken

In de zip-bestand *BIPL\_optioneel\_Users.zip* zit een Excel template (*Template voor omzetten naar AD.xlsx*) waarmee je een *csv*-bestand kunt maken om eenvoudig gebruikers te kunnen importeren. Hiervoor kopieer je alle gebruikersnamen naar het tabblad "namen". Vervolgens ga je op het tabblad "domeingegevens" de domeininstellingen opgeven. Als je de domeingegevens hebt opgegeven, dan kom je op het tabblad de gegevens tegen die van belang zijn voor het importeren met *csvde*. Als je deze gegevens kopieert en het vervolgens opslaat als *csv(ms-dos)* dan kun je het naderhand met *csvde* importeren. In hetzelfde zip-bestand bevindt zich *patienten\_VB.csv* met daarin een aantal optionele gebruikers die je eventueel aan het template kunt toevoegen.

## 2.6.5 Opdracht: Gebruikers importeren met powershell

De hierboven genoemde methodes met *csvde* en *ldifde* bestaan al vrij lang. User management met behulp van PowerShell is een nieuwere en krachtige methode. PowerShell zal in een latere cursus uitgebreidere worden behandeld, nu gebruiken we PowerShell om wederom een *csv*-file te importeren. Bekijk optioneel de PowerPointpresentatie voor de syntax die nodig is. Probeer met behulp van de PowerShell cmdlet *import-csv* samen met de cmdlet *New-ADUser* de testgebruikers zoals aangegeven inde file *patienten5.csv* aan te maken.

- 1) Maar maak hiervoor eerst een OU "test" aan.
- 2) Importeer met PowerShell het bestand *patienten5.csv*.
  - Welke syntax heb je hiervoor gebruikt?
  - Toont PowerShell informatie dat de handeling geslaagd is?
  - Zijn de gebruikers toegevoegd?



### 2.6.6 Opdracht: Dsadd

De tools Dsadd, dsmove, dsmod en dsquery kunnen ook gebruikt worden om gebruikers, al dan niet in een batch file, aan het domein toe te voegen. Ook hier vind je weer veel overeenkomsten in de syntax. Veel van de attributes kun je ook hiermee toevoegen of wijzigen. Met dsquery kun je tevens zoekacties uitvoeren. Het antwoord op de zoekactie kun je vervolgens weer aan bijvoorbeeld dsmod geven die wijzigingen kan doorvoeren. Laten we beginnen met dsadd. Het bestand medewerkers6.txt geeft een voorbeeld voor het toevoegen van een gebruiker met dsadd.

- 1) Bekijk de structuur van de syntax die door dsadd wordt gebruikt. Welk verschil is er met de eerdere documenten?
- 2) Voer de gebruikers uit medewerkers6.txt in. Knippen en plakken is hierbij een mogelijkheid. Hernemen van het bestand medewerkers6.txt naar medewerkers6.bat en deze uitvoeren geeft hetzelfde resultaat.

### 2.6.7 Opdracht: Dsquery

Dsquery is een command line tool die gebruikt kan worden om zoekacties uit te voeren. In een organisatie kan het vanuit veiligheidsoverwegingen handig zijn om te weten of er bijvoorbeeld accounts zijn die een aantal weken niet gebruikt zijn of dat er gebruikers zijn die de laatste 10 dagen hun wachtwoord niet hebben aangepast.

- 1) Ga na welke accounts al twee weken niet gebruikt zijn. (dsquery /? en/of dsquery user /? Geeft uitleg!). Het kan zijn dat dat je niets ziet. Gebruik dan de waarde 0 achter -inactive.
  - o Welke syntax heb je hiervoor gebruikt? (Schrijf de syntax weer op, dat kan handig zijn!)
- 2) Ga na welke gebruikers de laatste 10 dagen hun wachtwoord niet hebben aangepast
  - o Welke syntax heb je hiervoor gebruikt?

### 2.6.8 Opdracht: Dsmod en Dsquery

Dsmod is de command line tool die gebruikt kan worden om bestaande gebruikersaccounts aan te passen. Het bestand medewerkers7.txt bevat een voorbeeld van de mogelijkheden.

- 1) Bekijk de inhoud van het bestand medewerkers7.txt. Wat valt daarbij op?
- 2) Voer het commando van medewerkers7.txt of medewerkers7.bat uit en controleer of de werkingen juist is doorgevoerd.

Zoals eerder aangegeven is het mogelijk om de output van een command line tool door te sturen naar een andere command line tool. In het bestand medewerkers8.txt of medewerkers8.bat zie je hiervan een voorbeeld. Door met dsquery AD te doorzoeken, bijvoorbeeld op basis van een description, kun je de resultaten van deze zoekactie doorgeven aan bijvoorbeeld dsmod.

In het voorbeeld krijgen de medewerkers extra informatie in de vorm van bijvoorbeeld een titel, een ander telefoonnummer of een webpagina. In het voorbeeld (medewerkers8.txt) geven wij de patiënten een medisch vertrouwenspersoon. Deze manier van het overdragen van de output van het eerste commando/tool als input voor het tweede commando/tool wordt ook vaak gebruikt bij PowerShell. Bij PowerShell heet dat een pipeline.

- 3) Voer medewerkers8.txt/ bestand medewerkers8.bat uit en controleer de werking.

Het gebruik van dsquery en dsmove heb je nu een aantal keer bekeken, maar mogelijk is de 'kracht' van de beide tools nog niet helemaal duidelijk. Anders gezegd het meeste wat wij hiervoor hebben gedaan zou je ook kunnen doen via ADUC en ADAC. Nu nog wat voorbeelden wat je met dsquery kunt doen, wat in ADUC en ADAC veel lastiger zal gaan en/of zeer arbeidsintensief zal zijn..

- 4) Controleer met dsquery welke accounts uitgeschakeld (disabled) zijn. Welke syntax heb je hiervoor gebruikt?
- 5) Als je een overzicht gekregen hebt van de accounts die op dit moment op disabled staan dan is dat beperkt tot 100 accounts, maar misschien zijn er wel meer accounts. Hoe krijg je dsquery zover dat je alle accounts te zien krijgt die op disabled staan? Welke syntax heb je gebruikt? Je kunt het antwoord vinden met dsquery user /?





- 6) Wat doet de optie `> disabled.txt` achter je `dsquery`?
- 7) Nu je de accounts gevonden hebt die nog op disabled staan, ga je ze niet een voor een maar met meerdere tegelijk activeren en een wachtwoord geven. Geef de gevonden gebruikersaccounts die zijn uitgeschakeld een tijdelijk wachtwoord (`Pa$$w0rd`) en enable de accounts. De zoekactie moet plaatsvinden in de OU Patiënten omdat je er anders voor zorgt dat de accounts Guest, krbtgt en \_templateuser1 ook worden geactiveerd. De optie `-c` kan bij problemen oplossing bieden omdat mogelijk al een aantal gebruikersaccount geactiveerd zijn. Dsmod zal hierover vallen en een errorcode geven! Hulp om deze taak uit te voeren kun je in de helpfunctie van de twee tools vinden (`dsquery user /?` En `dsmod user /?`).
- 8) Controleer welke gebruikersaccounts nog zijn uitgeschakeld.

## 2.6.9 Opdracht: Dsmove

Dsmove is de command line tool die je kunt gebruiken om bijvoorbeeld gebruikers te verplaatsen naar een andere OU. Omdat de verschillende OU's nog niet zijn aangemaakt, zullen we dsmove pas later gaan gebruiken.

## 2.6.10 Opdracht: Organizational Units

Organizational Units(OU) hebben hun intrede gemaakt in Windows 2000. Een OU heeft met name in complexe domeinen met veel objecten als gebruikers en computer een aantal belangrijke taken. OU's kunnen ook weer worden aangemaakt met Active Directory Users and Computers of dsadd. In weekopdracht 1 zijn een aantal OU's aangemaakt.

- 1) Onder de OU "Huisartsen" en de OU "Tandartsen" maak je met behulp van ADUC, ADAC, met ds..... of met PowerShell de onderstaande OU's aan.
  - HA1;
  - HA2;
  - TA1;
  - TA2.
- 2) Maak vanaf de command line in de onderstaande OU's de kalenderjaren 2020, 2021 en 2022 aan. Gebruik hiervoor het PowerShell cmdlet `New-ADOrganizationalUnit`. Geef daarbij tevens een passende beschrijving op.
  - Fysiotherapie;
  - Verloskundigen;

Welke syntax heb je hiervoor gebruikt?

Alle patiënten zijn nu nog ongeordend in de OU patiënten en de aangemaakte OU's zijn nog niet echt nuttig. De patiënten moeten keurig worden verplaatst naar de juiste OU. Vanuit ADUC kun je dit doen door ze te sorteren of door een filter te maken. Wij kiezen er in deze situatie voor om dit uit te voeren met een combinatie van `dsquery` en `dsmove`. Omdat een directe koppeling van beide tools op problemen stuit mag je gebruik maken van het script `dsquerydsmove.bat`.

- 3) Bestuderen van het script leert dat de output van `dsquery` op basis van de description wordt weggeschreven in een tekstbestand. Het tekstbestand wordt vervolgens als basis gebruikt om een nieuwe batch file te maken met `dsmove`. De nieuw gemaakte batch file met de bijvoorbeeld de naam `HA1.bat` moet in deze situatie handmatig worden uitgevoerd.
- 4) Voer het script `dsquerydsmove.bat` uit. Doe dit, zelfs als je bent ingelogd als Administrator, met behulp van `runas:runas /user:administrator dsquerydsmove.bat`. Het uitvoeren van het script kan je het beste doen vanaf je bureaublad omdat het script een nieuw script aanmaakt wat ook weer moet worden uitgevoerd.
- 5) Pas het bovenstaande script op vijf of zes plaatsen aan zodat alle gebruikers, dus ook de medewerkers die in de OU staan, op basis van hun description in de juiste OU worden geplaatst. Welke syntax heb je hiervoor gebruikt?
- 6) De medewerkers met de description verpleegkunde mogen in de OU voor de verloskundige worden geplaatst. Dat kan met het script, maar je kunt in een grafische tool de overgebleven gebruikers ook allemaal selecteren en via het menu onder de rechtermuisknop voor "move" kiezen.



### 2.6.11 Opdracht: Homefolders

In een groot netwerk wordt er vaak gebruik gemaakt van een centrale fileserver. Hierop kunnen de gebruikers hun documenten opslaan. Dit maakt het maken van een backup makkelijker.

In deze opdracht ga je de homefolder en de profielen op de domain controller opslaan. Hiervoor moeten de onderstaande drie shares worden aangemaakt. Shares worden in een latere week besproken en toegelicht.

Maak ze nu 'gewoon' aan zoals hieronder aangegeven. Weet je niet hoe? Vraag het je docent.

- 1) Maak de onderstaande mappen aan op een van de DC's en geef de groep "Authenticated users" *Full control* over alle drie de shares (doe dit door in de 'properties' van elk van de mappen onder het tab 'Sharing' de knop 'Advanced Sharing ...' te klikken).
  - Homefolders
  - Mandatory
  - Roaming

De verwijzingen maken naar de homefolders en de profielen zou je kunnen doen met dsmod, maar in dit geval kiezen we ervoor om dit voor elkaar te krijgen met ADUC.

- 2) Geef alle medewerkers een Homefolder. Selecteer hiervoor alle gebruikers en verwijs alle homefolders naar de share Homefolders op de DC.
  - Welke variabele kun je gebruiken om alle gebruikers een eigen share te geven?
  - Controleer of de mappen zijn aangemaakt!

### 2.6.12 Opdracht: Profielen

Een profiel bevat alle gezamenlijke en individuele instellingen van een gebruiker. Op een Windows systeem kun je weer een aantal verschillende profielen tegenkomen.

- 1) Geef de medewerkers een *roaming* profiel (**LET OP:** doe dit in een andere gedeelde map dan de homefolders van de vorige opdracht!).
  - Geef aan hoe je dit hebt gedaan.
  - Controleer of de profielmap wordt aangemaakt als je met een van de gebruikersaccounts in- en uitlogt op het domein.
- 2) Kun je als beheerder/administrator standaard in de profielmap van de gebruiker kijken?

### 2.6.13 Opdracht: Delegation of Control

Met *delegation of control* kun je het beheer van een OU overdragen aan bijvoorbeeld een teammanager of een mentor. Delegation of control ga je nu uitvoeren op de onderstaande OU's.

- 1) Draag de onderstaande beheertaken over aan de onderstaande aanspreekpunten/receptionisten van de patiënten.
  - Bloys van Treslong: HA1
  - Jan van Galen: HA2
  - Gerard Callenberg: TA1
  - Juliana Stolberg: TA2
- 2) Gebruik hiervoor ADUC.
  - Wijzigen van wachtwoorden
  - Maken en aanpassen van gebruikers
  - Lezen van gebruikersinformatie

### 2.6.14 Vragen Windows Gebruikers en Groepen

1. Microsoft Windows kent drie verschillende soorten gebruikersaccounts, Welke drie zijn dat?
2. Om toegang te krijgen tot een domein en om binnen het domein taken te kunnen uitvoeren wordt er gesproken over *authentication* en *authorization*. Wat is het verschil tussen beide?
3. Een gebruikersaccount in een Windows domeinomgeving kent meerdere namen. Beschrijf de kenmerken/ verschillen tussen de onderstaande namen:
  - Display name



- Logon name
  - User Principle Name (UPN)
  - Pre-Windows logon name
4. Gebruikersaccounts worden binnen een Windows domein opgeslagen in Active Directory. Hierdoor krijgt een gebruikersaccount nog een aantal namen, te weten een User Principal Name (UPN), een Distinguished Name (DN) en een Relative Distinguished Name (RDN).
    - Wat is een UPN? Geef een voorbeeld.
    - Wat is het verschil tussen een DN en een RDN?
  5. In welke situatie kom je een UPN en een DN tegen?
  6. Ondanks al deze verschillende namen maakt Windows Server 2016 geen gebruik van deze namen om een gebruiker permissies of rechten te geven. Hiervoor wordt gebruik gemaakt van een SID. Wat is een SID en uit welke twee delen zijn ze opgebouwd?
  7. Welke aanpassingen kun je via ADUC bij het aanmaken van het account nog meer maken?
  8. Wat als je voor een grote groep gebruikers veel meer gegevens dan alleen een naam en een wachtwoord wilt invullen en je wilt dat toch via Active Directory Users and Computers doen? Dan biedt een zogenaamde *template user* mogelijk een oplossing. Wat is een template user?
  9. Welke gegevens van een template user worden gekopieerd en welke niet?
  10. Wat is een DN?
  11. Wat is een CN?
  12. Wat is een DC?
  13. Wat is een sAMAccountName?
  14. Wat is csvde?
  15. Welke syntax is er minimaal nodig om een CSV-file te importeren?
  16. Kan je met dsadd ook het tabblad Address volledig invullen?
  17. Kan je dit (vraag 16) met een andere command line tool wel voor elkaar krijgen?
  18. Welke syntax moet je bij dsquery gebruiken om te achterhalen welke gebruikers een HA2 description hebben?
  19. Bij het uitvoeren van “Dsquery user” worden niet alle gebruikers weergegeven. Er is een limiet van 100. Welke parameter moet je gebruiken om alle gebruikers te kunnen zien?
  20. Van hoeveel gebruikers in het domein begint hun voornaam met een C?
  21. Met welke syntax kun je zien welke gebruikersaccounts uitgeschakeld zijn?
  22. Wat is een OU?
  23. Welke functies heeft een OU?
  24. Wat is een *nested OU*?
  25. Kan een OU in het domein bmc.local gebruikers bevatten vanuit het domein HA1.bmc.local?
  26. Welke OU's zijn op een nieuw gepromoveerde domain controller standaard aanwezig?
  27. Welke share en security settings zijn er automatisch gemaakt op de nieuwe shares?
  28. Wat is een UNC?
  29. Welke drie profielen kun je op een Windows systeem tegenkomen?
  30. Wat is het verschil tussen deze drie profielen?

## 2.7 Week 3, College 2: Linux Gebruikers en Groepen

### Inleiding

Natuurlijk is het ook onder Linux belangrijk om te weten hoe je gebruikers en groepen moet beheren. Daar gaan we in onderstaande opdrachten mee aan de slag.

### Theorie

#### Verplicht:

- Slides,
- Dit werkboek met vragen en antwoorden (zie afzonderlijk document “Antwoorden\_BIPL\_Werkboek\_v1.4.1vt”!)
- Boek: “Unix and Linux System Administration Handbook, 5<sup>th</sup> Edition”:



- Chapter 3 – *Access Control and Rootly Powers*:
  - Volledig: blz. 65 t/m 89
- Chapter 8 – *User Management*
  - Begin t/m 8.9 *User login lockout*: blz. 243 t/m 266
  - FreeBSD onderdelen niet verplicht voor tentamen
- Chapter 27 – *Security*
  - Begin t/m 27.4 *Passwords and user accounts*: blz. 981 t/m 996

## 2.7.1 Opdracht: Gebruikers aanmaken

Bij de Windows opdracht heb je op verschillende manieren gebruikers toegevoegd aan AD. In deze Linux opdracht ga je lokale gebruikers en groepen aanmaken. Hieronder staan twee tabellen met gebruikers en groepen waar je in deze gehele opdracht mee gaat werken. Als naar bepaalde users verwezen wordt, is het dus de bedoeling dat je ze hier opzoekt. We beginnen met het aanmaken van de groepen!

TABEL 2 GEBRUIKERS LINUX

Voornaam	Achternaam	Usernaam
Marion	Aster	master
Leo	Oser	loser
Antoinette	Verage	average
Gideon-Eibert	Woon	gewoon
Arno	Part	apart
Harry	Acker	hacker

TABEL 3 GROEPEN LINUX

Groepsnaam	Leden
sales	average
	gewoon
to1-project	apart
	average
to2-project	apart
	gewoon

- 1) Maak de bovenstaande groepen (Tabel 3) aan. Stel geen wachtwoord in op de groepen.
  - Welke commando's heb je hiervoor gebruikt?  
**Let op:** `man -k group` kan je op weg helpen om te achterhalen welk commando je moet gebruiken.  
Noteer de commando's die je gebruikt!
- 2) Maak bovenstaande gebruikers (Tabel 2) aan.
  - Het wachtwoord voor de gebruikers mag je zelf verzinnen.
  - Zorg ervoor dat elke gebruiker een eigen home-directory krijgt onder `/home` en dat daar de standaard-instellingen (uit `/etc/skel`) in geplaatst worden.
  - Elke user moet als primary group users ingesteld hebben, en ze moeten lid zijn van de andere (additionele) groepen zoals in bovenstaande tabellen is aangegeven.

Welke commando's heb je hiervoor gebruikt?

**Let op:** op veel Linux systemen zijn er meerdere commando's/tools om gebruikers aan te maken, `useradd` en `adduser` zijn daarvan voorbeelden! `adduser` is op Rocky 8 een verwijzing naar `useradd`, dus daar heb je weinig keuze.

- 3) Nu de gebruikers zijn aangemaakt:
  - In welke bestanden kun je deze instellingen nu terugvinden?
  - Bekijk de inhoud van deze bestanden.

De naam van het bestand met daarin de aangemaakte groepen zou 'eenvoudig' te bedenken zijn als je weet dat veel configuratie bestanden die niet veelvuldig worden gewijzigd in `/etc` staan.

Als je `ls -l` in deze directory gebruikt, dan zijn (standaard) de niet gekleurde teksten de configuratie bestanden. De blauw teksten verwijzen naar een directory. Voor de aangemaakte gebruikers is het configuratiebestand minder logisch, tenzij je bedenkt dat elke gebruiker een wachtwoord nodig heeft.

- Zoek het bestand met deze verwijzing en open het bestand met bijvoorbeeld `cat`.
- Kun je nu inloggen met deze users?
- Zo nee, wat moet je nog doen om dat wel mogelijk te maken?



Je hoeft niet de grafische omgeving te verlaten om dit te testen. Je kunt ook een terminal openen en het commando `su <naam>` uitvoeren (`su` staat voor *substitute user*).

Als je de opmerking 'authentication failure' krijgt, dan is het zeer waarschijnlijk dat je nog een wachtwoord moet toekennen aan de gebruiker. Dit kun je o.a. doen met `passwd`.

Denk weer aan de helpfunctie als je er niet uitkomt! Het wachtwoord van de gebruiker wordt opgeslagen in `/etc/shadow`. Uit veiligheidsoverwegingen zijn de wachtwoorden hier versleuteld opgeslagen.

- 4) Zorg ervoor dat de gebruiker `master`:
- o iedere 40 dagen een nieuw wachtwoord moet instellen,
  - o dat zij daarvoor 7 dagen van tevoren wordt gewaarschuwd en
  - o dat er minimaal 1 dag tussen wachtwoordwijzigingen moet zitten.

Met `man -k expiry` kun je achterhalen welk commando je hiervoor zou kunnen gebruiken.

- o Laat zien hoe je de instellingen kunt aanpassen,
  - o laat de regels in de bestanden zien waar je die instellingen kunt terugvinden (denk aan de vraag over het wachtwoord van de gebruiker! Bij de gebruiker moet je iets tegen komen als `:1:40:7:::`) en/of
  - o hoe je de instellingen per user kunt opvragen (tip: argument `"-l"` (kleine letter L)).
- 5) Zorg er nu voor dat "Harry Acker" niet meer kan inloggen, maar dat zijn account wel blijft bestaan (we noemen dit het *locken* van een account). Laat zien hoe je dit doet. Kijk eens in de manpage van `usermod` om te achterhalen hoe je dit moet doen. Wat geeft `less /etc/shadow` (we gebruiken hier `less`, maar je kunt ook `more`, `cat`, `grep` of iets anders gebruiken!) aan bij het account van Harry? Vergelijk het met een ander account!
- 6) Probeer of je nog met Harry kunt inloggen. Welke melding wordt er gegeven?
- 7) Verwijder tenslotte het gebruikersaccount van "Leo Oser", inclusief zijn `homedirectory` en alles wat daarin staat. Laat zien hoe je dit doet. Het commando om een gebruiker aan te maken is `useradd` (of `adduser`), wat zal het commando zijn om een gebruiker te verwijderen?
- Wordt er (zoals bij Windows) nog gevraagd of je het zeker weet?
- 8) Controleer of de gebruiker en zijn `homedirectory` ook daadwerkelijk zijn verdwenen.

## 2.7.2 Opdracht: sudo

- 1) Pas de configuratie van `sudo` aan, zodat de gebruiker `master` via `sudo` commando's als `root` mag uitvoeren. Er zijn meerder mogelijkheden om dit voor elkaar te krijgen. De eerste mogelijkheid maakt de gebruiker lid van de 'sudo' groep (In Rocky Linux heet deze groep `"wheel"`, de reden daarvoor is een beetje [vreemd verhaal](#)); dit is wat de installatiesoftware doet als je de optie "Make this user administrator" kiest bij het aanmaken van een gebruikersaccount) de tweede mogelijkheid is om `visudo` te gebruiken, waarmee configuratiebestand `/etc/sudoers` kan worden aangepast.
- o Welke aanpassingen heb je gemaakt?
  - o Denk er weer aan om het commando aan je commandolijstje (§2.1.6) toe te voegen!
- 2) Test de configuratie door
- o eerst zonder `sudo` te proberen een bestand aan te maken in `/root` (bijvoorbeeld doormiddel van `"cp -v /etc/hosts /root/"`)
  - o en vervolgens met gebruik van `sudo` (voer hetzelfde commando uit met `"sudo"` ervoor).

Wat is het verschil?

## 2.7.3 Vragen Linux Gebruikers en Groepen

1. Wat is de betekenis van het user id (UID)?
2. Wat is de betekenis van het group id (GID)?



3. Als twee loginnamen met eigen passwords zijn gekoppeld aan hetzelfde user id, bieden zij dan toegang tot hetzelfde account?
4. Wat is de functie van de shadow password file?
5. Kunnen gebruikers aangemaakt worden zonder gebruik van useradd of adduser tool?
6. Welke vier algemene regels zijn er opgesteld rondom de traditionele manier van Access Control onder Linux?
7. Mag een 'gewone' gebruiker onder Linux de systeemtijd en de datum aanpassen?
8. Met welke tool kun je vanaf de commandline opvragen wie de eigenaar is van een specifiek bestand?
9. Welke *identities* kan een proces hebben?
10. Welk UID heeft het root account?
11. Wat zijn voorbeelden van moderne access control methodes onder Linux?
12. Waaraan moet een rootwachtwoord voldoen?
13. Met welk commando kun je, bijvoorbeeld in een shell, van gebruiker wisselen?
14. Een gebruiker die gebruik mag maken van het sudo commando moet lid zijn van welke groep?
15. Hoeveel UID mogelijkheden zijn er?
16. Met welke tools kun je gebruikers aanmaken, wijzigen of verwijderen?
17. Welke modernere vormen van gebruiker beheer doen de laatste jaren hun intrede in de Linux wereld?
18. Een gebruikersnaam onder Linux moet op twee punten uniek zijn. Welke twee zijn dat?
19. Welke drie encryptiemethodes worden veelvuldig op Linux Systemen gebruikt als het gaat om het versleutelen van de wachtwoorden in /etc/passwd?
20. Wat is een belangrijk nadeel van een MD5 hash?
21. Welk GID heeft de groep van root?
22. Wat is de functie van een GECOS field?
23. Welke gebruiker(s) mag de bestanden /etc/shadow en/of /etc/security standaard lezen?
24. In welk bestand kun je zien van welke groepen een gebruiker lid is?
25. Wat zijn de standaard startup files onder Linux?
26. Wat is LDAP?
27. Met welke tool kun je onder Linux de maximale tijd instellen voordat een gebruiker zijn wachtwoord moet aanpassen?

## 2.8 Week 4, College 1: Windows bestandssystemen

### Inleiding

Beter Medisch Centrum (BMC) heeft behoefte aan centrale opslag van gegevens.

Daarom zal een server worden ingericht als file server. Omdat de meeste clients Windows-gebaseerd zijn en het makkelijker en veiliger is om vanaf een Linux client met Windows shares te werken dan andersom, is ervoor gekozen de file server in te richten op basis van Windows.

Om alle opdrachten te kunnen uitvoeren heb je de volgende VM's nodig (je mag de bestaande hergebruiken of een nieuwe omgeving creëren):

- Een Windows 2016 Server als DC (dc1.bmc.local)
- Een Windows 10 Client (client1)
- Optioneel: een Rocky Linux 8 systeem (rocky1)

De domein controller wordt voor deze opdracht tevens ingezet als fileserver, wat in een productie-omgeving niet direct is aan te raden.

Met de komst van het bestandssysteem NTFS in het besturingssysteem NT werden de mogelijkheden om bestanden en folders op verschillende niveaus te beveiligen veel groter. Zeker in vergelijking met de mogelijkheden die er eind vorige eeuw waren onder client versies Windows 95 en 98. Af en toe worden er aanpassingen gemaakt in het NTFS bestandssysteem. In Windows Server 2016 heb je te maken met versie 3.1 (te controleren met het commando "`fsutil fsinfo ntfsinfo c:`"). Op een lokaal systeem en binnen een netwerk moet je specifieke bestanden beveiligen. De mogelijkheden die je hierbij kan tegenkomen zijn:

- Share-rechten





- NTFS-rechten
- Versleuteling van bestanden met bijvoorbeeld BitLocker

Binnen deze cursus kijken we alleen naar de eerste twee.

#### Theorie *Verplicht:*

Slides,

- Dit werkboek met vragen en antwoorden (zie afzonderlijk document “Antwoorden\_BIPL\_Werkboek\_v1.4.1vt”!)
- Boek: “Windows Server 2016 Unleashed”:
  - Hoofdstuk 27, *File System Management*:
    - begin tot *File Server Resource Manager* (blz. 1023 t/m 1032)
  - Hoofdstuk 30, *Recovering from a Disaster*:
    - *Recovering from a Server of System Failure* tot *Managing and Accessing Windows Server Backup Media* (blz. 1166 t/m 1173)

#### *Optioneel:*

- NTFS permissies (1a): <http://technet.microsoft.com/en-us/magazine/2005.11.howitworksntfs.aspx>
- NTFS permissies (1b): <http://technet.microsoft.com/en-us/magazine/2006.01.howitworksntfs.aspx>
- NTFS permissies (2): <http://www.windowsecurity.com/articles/Understanding-Windows-NTFS-Permissions.html>
- Security Descriptors en ACL's: [http://technet.microsoft.com/en-us/library/cc783702\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc783702(WS.10).aspx)
- Security Identifiers: [http://technet.microsoft.com/en-us/library/cc778824\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc778824(WS.10).aspx)

#### Video's

- NTFS/ ReFS <https://www.youtube.com/watch?v=TLKZEU1DZ9c>
- Advanced NTFS permissions <https://www.youtube.com/watch?v=H2I3Ar0ZraU>

### 2.8.1 Opdracht: voorbereiden van de basisomgeving

- 1) Importeer, indien je ervoor hebt gekozen om een nieuwe omgeving voor deze opdracht op te zetten, de gebruikers en maak de OU's en groepen aan met behulp van de bestanden uit de *resource* directory van de les over gebruikers:
  - setup\_usersenou.bat
  - patienten1.csv
  - patienten4.csv

Als je de reeds bestaande omgeving hergebruikt, dan kun je deze stap overslaan.

### 2.8.2 Opdracht: Aanmaken mappenstructuur en bijbehorende shares

Voor het configureren van de share- en NTFS-rechten kun je gebruik maken van de Explorer maar ook van de Server Manager die verschijnt na het installeren van “File and Storage Services” onder Server 2016.

Op de file-server, dit mag voor deze opdracht ook gewoon de DC zijn, moet een mappenstructuur komen zodat de behandelaars daar hun patiëntgegevens kunnen opslaan. Behandelaars mogen alleen maar lezen en schrijven in de mappen van hun eigen praktijk, niet in de map van een andere praktijk. Bijvoorbeeld: alle tandartsen mogen alleen lezen en schrijven in de share van de tandartsen en mogen niets in de share van de huisartsen.

- 1) Schrijf hiervoor (bovenstaande casus) een plan en voer dit uit. Je mag gebruik maken van share rechten, NTFS rechten en groepen. Gebruik hiervoor het AGDLP-principe. Dit betekent ook dat je nieuwe Domain Local groepen moet aanmaken en deze de juiste rechten moet toekennen.



### 2.8.3 Opdracht: Toevoegen van shares met verschillende rechten

Wanneer de huisartsen een apotheekrecept uitschrijven, dan moet de apotheek dit natuurlijk ook kunnen lezen om het juiste recept aan de patiënt mee te kunnen geven.

- 1) Maak voor de apothekers een nieuwe OU aan. Zet daarin een gebruiker (de apotheker) en een groep
- 2) Maak vervolgens een share genaamd “recepten” waarin de huisartsen volledige rechten hebben, maar de apothekers slechts leesrechten. Alle anderen hebben helemaal geen toegang.

Daarnaast zal een huisarts af en toe een verwijzing schrijven voor fysiotherapie, die door een fysiotherapeut gelezen moet kunnen worden om de juiste zorg aan te kunnen bieden.

- 3) Maak voor de fysiotherapeuten een nieuwe OU aan. Zet daarin een of meer gebruikers (de fysiotherapeut(en)) en een groep
- 4) Maak daarom ook een share genaamd “fysio\_verwijzingen” waarin de huisartsen volledige rechten hebben, maar de fysiotherapeuten slechts leesrechten. Ook hier mogen de anderen helemaal geen toegang toe hebben.

### 2.8.4 Opdracht: Een share maken op een Core systeem

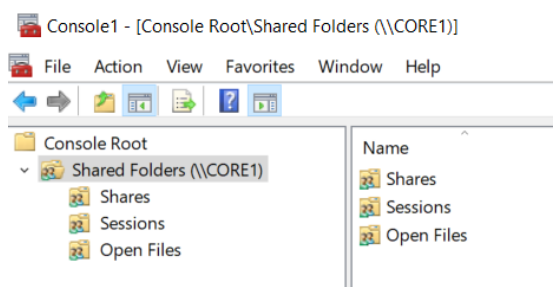
Karel Doorman wil graag een share hebben op een van de Core machines. Op de grafische machine is het aanmaken van de share relatief eenvoudig, maar hoe doe je dat op de Core machine?

Er zijn meerdere mogelijkheden. Zo kun je het vanaf de commandline doen met de tool net of je kunt PowerShell gebruiken. Grafisch moet het vanaf een ander systeem ook kunnen. Ook hier zijn dan weer verschillende mogelijkheden. Je mag zelf bepalen welke methode je kiest. Om de opdracht niet te lang te laten worden geven wij één voorbeeld van een methode die niet per se de beste, snelste of veiligste is. Heb je zelf een andere methode, dan mag je die, ook op het tentamen, gewoon gebruiken.

Een van de mogelijkheden is:

- 1) Op de DC of een andere grafische: Turn on network discovery and file sharing op de grafische machine. Kies dan in de explorer het icon Network. Er zal dan worden gevraagd of je filesharing wilt aanzetten. Zodra je dat hebt aangezet, moet je een pictogram tegenkomen van de DC. Als je daarop klikt, dan moet je alle share op die machine kunnen zien. Dat zijn de zelf aangemaakte shares en de shares netlogon en sysvol. Deze twee shares zullen worden besproken bij GPO's in week 6.
- 2) Op de core moet je file and printer sharing ook aanzetten. Dit kan o.a. met:  
netsh advfirewall firewall set rule group="File and Printer Sharing" new enable=Yes  
Als je naar de grafische machine teruggaat, dan moet je na een tijdje ook de core machine tegenkomen. Als je niet wilt wachten, dan kun in de adresbalk ook \\core1 of \\<het IP-adres> opgeven. Zeer waarschijnlijk is er op die machine geen share te zien, tenzij het om een Core Domain Controller gaat.
- 3) Op de Core machine kun je, zoals je ook bij Linux gaat doen, vanaf de commandline een directory aanmaken. Dit kan met bijvoorbeeld: mkdir Doorman. Je kunt het ook doen met PowerShell. Er is voor nu echter een eenvoudigere methode, die je bij voorkeur ook gaat gebruiken.

Op de grafische machine open je met Windowstoets + R de Windows prompt. Daarin type je **mmc**. MMC staat voor Microsoft Management Console. In de geopende mmc ga je via File, Add/remove



Snap-in een tool toevoegen. De tool/snap-in die je gaat toevoegen heet **Shared Folders**. Je kiest dan **niet** de local computer, maar je selecteert “Another Computer” en kiest daar dan de core machine. Je krijgt dan het onderstaande scherm te zien. Al je vervolgens Shares aanklikt, dan kun je via de rechtermuisknop een new share toevoegen. Dit gaat via een wizard. Als een directory niet bestaat, dan kan deze worden aangemaakt. Ook de permissies





kun je mbv de wizard instellen. Als je teruggaat naar de Windows Explorer en je ververs het scherm van de Core1 machine, dan zou je de shares terug moeten kunnen vinden. Je kunt vervolgens o.a. de security settings van de share wijzigen en bekijken. Let op dat deze methode standaard alleen de share permissies instelt en niet de NTFS permissies. In de Windows Explorer kun je niet, zomaar, een share aanmaken. Je zult daar meer voor moeten doen. Voor nu gaat dat echter te ver. Het is verstandig om de mmc te bewaren. Dit kan via file en save. Op de Core machine kun je vanaf de commandline met o.a. net share alle shares opvragen.

Als je op de Windows Server de Firewall compleet wilt uitzetten, dan kan dat in PowerShell via:  
`Set-NetFirewallProfile -Profile Domain,Public,Private -Enabled false`

Vanwege de veiligheid niet verstandig, maar voor het beheer in deze oefenomgeving is het mogelijk wel handiger.

## 2.8.5 Opdracht: Toevoegen van beperkte rechten

Karel Doorman wil graag dat zijn share alleen toegankelijk is voor hem en voor Piet Hein. Hij vraagt aan Piet of hij dat kan organiseren.

- 1) Wat moet Piet hiervoor doen? Voer dat ook uit!

## 2.8.6 Vragen Windows bestandssystemen

1. Welke standaard permissies kunnen er op een bestand worden ingesteld?
2. Op welk punt verschillen de permissies op een folder met die van een bestand?
3. Welk verschil is er tussen standaard en geavanceerde permissies?
4. Uit welke geavanceerde permissies is de standaard permissie "read" opgebouwd?
5. Op welke twee manieren kan een bestand of een folder te maken krijgen met permissies?
6. Op welke manier kan je het erven (inheritance) worden tegengegaan?
7. Wat heeft in het geval van een conflict voorrang. Een implicit deny of een explicit allow?
8. Als de share permissie op een map "read" is, maar de gebruiker heeft "Full Control" op de bestanden in de map. Wat mag de gebruiker dan wel en/of niet met de bestanden doen?
9. Wat is een DACL?
10. Wat wordt er verstaan onder een Access Control Entry?
11. Wat is een SID?
12. Wordt er bij het weergeven van de effectieve permissie rekening gehouden met de share permissies?
13. Wat is de functie van een UNC?
14. Uit welke delen is een Access token van een gebruiker opgemaakt?
15. Wat is een SACL?
16. Uit welke onderdelen is een SID opgebouwd?
17. Welk nieuw filesysteem is met de komst van Windows Server 2012 toegevoegd?
18. Wat is een beperking van dit nieuwe filesysteem?

## 2.9 Week 4, College 2: Linux bestandssystemen

### Inleiding

Vorige week heb je voor een deel van de Linux *package management* opdracht al een paar taken uitgevoerd via de command line. In de UNIX en Linux wereld staat de command line interpreter bekend als de *shell*.

Dit is voor beheerders de meest krachtige omgeving binnen Linux, die ook de gelegenheid biedt taken te automatiseren door commando's op te slaan in zogenaamde *shell scripts*. Daarnaast zijn een aantal configuraties alleen te maken via configuratiebestanden.

Beter Medisch Centrum verwacht daarom dat je voor het beheren van de Linux systemen goed uit de voeten kunt met de Linux shell, en niet afhankelijk bent van grafische hulpmiddelen, al helemaal om dat met het oog



op de prestaties en de veiligheid de productieservers zo kaal mogelijk uitgerust zullen worden, dus liefst zonder GUI.

## Theorie

### Verplicht:

- Slides,
- Dit werkboek met vragen en antwoorden (zie afzonderlijk document "Antwoorden\_BIPL\_Werkboek\_v1.4.1vt"!)
- Boek: "Unix and Linux System Administration Handbook, 5<sup>th</sup> Edition":
  - Chapter 5 – *The Filesystem*:
    - Volledig, behalve *NFSv4 ACLs*: blz. 120 t/m 147
    - FreeBSD onderdelen niet verplicht voor tentamen
  - Chapter 20 – *Storage*
    - Begin t/m 20.2 *Storage hardware*: blz. 717 t/m 730
    - 20.4 *Attachment and low-level management of drives* t/m 20.7 *Logical Volume Management*: blz. 733 t/m 753
    - 20.9 *Filesystems* t/m 20.11 *Next-generation filesystems: ZFS and Btrfs*: blz. 762 t/m 773
    - FreeBSD onderdelen niet verplicht voor tentamen

### Video's

- Structuur: <https://www.youtube.com/watch?v=vSMriAHpzQM>
- LVM: <https://www.youtube.com/watch?v=BysRGDggtwY>
- Symbolic links [https://www.youtube.com/watch?v=l\\_1Q3DG3uoE](https://www.youtube.com/watch?v=l_1Q3DG3uoE)
- Managing the linux filesystem <https://www.youtube.com/watch?v=8AzZwKk9zUw>

## 2.9.1 Opdracht: bestandsrechten

In deze opdracht ga je een omgeving voor de gebruikers in de opdracht van vorige week inrichten waarin zij hun bestanden veilig kunnen opslaan. Daarnaast zorg je ervoor dat kwaadwillende gebruikers niet meer kunnen inloggen.

- 1) Maak de volgende directories aan en zorg er daarbij voor dat de owner en groep volgens onderstaande Tabel 4 zijn ingesteld (laat zien hoe je dit doet)! Neem de commando's die je nodig hebt weer op in je lijstje!

TABEL 4 DIRECTORIES

Directory	Owner (user)	Group
/data	root	root
/data/algemeen	root	users
/data/sales	root	sales
/data/to1-project	root	to1-project
/data/to2-project	root	to2-project

- 2) Nu de directories zijn aangemaakt, ga je net als onder Windows de rechten (officieel zijn dit onder Windows geen rechten, maar permissies!) aanpassen. Je hebt daar de commando's `chown` en `chmod` zeer waarschijnlijk voor nodig. Kijk in de manpage (of de presentatie) na hoe je beide commando's moet gebruiken. Stel de rechten op de `sales`, `to1-project` en `to2-project` subdirectories van `/data` (dus `/data` zelf en `/data/algemeen` niet) in zoals weergegeven in Tabel 5:

TABEL 5 DIRECTORYRECHTEN

Directory	owner (user)	group	others
/data	alle rechten	read + execute	read + execute
/data/algemeen	alle rechten	read + execute	read + execute



/data/sales	alle rechten	alle rechten	geen rechten
/data/to1-project	alle rechten	alle rechten	geen rechten
/data/to2-project	alle rechten	alle rechten	geen rechten

Laat zien hoe je dit doet.

- 3) Hoe (met welk commando) kun je laten zien dat de directories daadwerkelijk zijn aangemaakt en welke rechten erop zijn ingesteld?
- 4) Log in als “gewoon” (kan in een shell, opnieuw inloggen is niet per se noodzakelijk! VB: su gewoon) en maak de volgende bestanden aan (zet ook wat tekst in de bestanden):
  - a. /data/sales/klantgegevens.txt
  - b. /data/to2-project/deadlines.txt

Mocht het aanmaken van de bovenstaande bestanden niet lukken, kijk dan nog eens goed naar de rechten die je hebt ingesteld en naar de groeplidmaatschap van de gebruiker(s). Mocht je de gebruiker niet van de juiste groep(en) lid hebben gemaakt, dan kan usermod je daarbij helpen. Voor het aanmaken van de bestanden kun je een commandline-editor gebruiken als nano of vi, maar er zijn meerdere mogelijkheden.

- 5) Log nu in als de gebruiker “apart” en probeer de inhoud van het bestand “klantgegevens.txt” weer te geven met bijvoorbeeld cat of nano. Lukt dit? (Gebruik **geen** sudo!) Laat de rechten op het bestand en de directory zien; welke verklaring heb je hiervoor?
- 6) **Bonus-opdracht (niet verplicht):** in deelopdracht 2) heb je de “groeps-directories” beveiligd, zodat niet iedereen er zomaar in kan lezen en/of schrijven. Kun je er ook voor zorgen dat de juiste groep aan elk nieuw bestand in de directory verbonden wordt? TIP: chmod en set group ID

Hieronder staan 2 tabellen met gebruikers en groepen waar je in deze opdracht mee gaat werken. Deze zijn in vorige weekopdracht al aangemaakt en staan hier nogmaals zodat je niet terug hoeft te bladeren. Als naar bepaalde users verwezen wordt, is het dus de bedoeling dat je ze hier opzoekt.

TABEL 6 HERHALING GEBRUIKERS EN GROEPEN

Voornaam	Achternaam	Usernaam
Marion	Aster	master
Leo	Oser	loser
Antoinette	Verage	average
Gideon-Eibert	Woon	gewoon
Arno	Part	apart
Harry	Acker	hacker

Groepsnaam	Leden
sales	average gewoon
to1-project	apart average
to2-project	apart gewoon

- 7) Maak bovenstaande gebruikers en groepen aan als je dat nog niet eerder hebt gedaan. Na het practicum van vorige week weet je hoe dat moet. Zorg dat de gebruikers lid zijn van de groepen zoals weergegeven.

TABEL 7 NIEUWE DIRECTORYSTRUCTUUR

Owner	Group	Rechten	Directory
root	root	drwxr-xr-x	/gegevens
root	to1-project	drwxrwx---	/gegevens/to1
root	to2-project	drwxrwx---	/gegevens/to2
root	users	drwxrwxrwx	/gegevens/tmp

- 8) Maak de bovenstaande directorystructuur aan (dit verloopt grotendeels hetzelfde als in deelopdrachten 1) t/m 2), op die manier kun je een beetje handigheid ontwikkelen in deze handelingen).



- 9) Normaal gesproken krijgen nieuw aangemaakt bestanden de *primary group* van de gebruiker die ze aanmaakt. Zorg er nu echter bij de directory `/gegevens/to1` en `/gegevens/to2` voor, dat nieuwe bestanden niet de *primary group* van de gebruiker krijgen, maar van de *group* van deze directories (dus resp. `to1-project` en `to2-project`). Laat zien hoe je dat doet, en dat het werkt.
- 10) Zorg er nu ook voor, dat bestanden in de `/gegevens/tmp` directory alleen verwijderd of hernoemd kunnen worden door de eigenaar (user) van dat bestand. De leesrechten voor de groep *users* en alle anderen moeten wel blijven! Laat zien hoe je dat doet en dat het werkt.
- 11) Maak een kopie van `/usr/bin/tail` naar `/tmp` en zet op de nieuwe kopie van het commando eigenaar *root* (met `chown`) en het SUID-bit (dit kan met `chmod`, kijk in de manpage bij de *description*!). Bekijk vervolgens de permissies op `/etc/shadow`.  
Log in als de gebruiker gewoon en probeer eerst met `/usr/bin/tail` het laatste deel van de inhoud van `/etc/shadow` te bekijken en daarna met `/tmp/tail`. Hoe verklaar je het verschil?  
Verwijder `/tmp/tail` zodat er geen misbruik van gemaakt kan worden.
- 12) Zoek nu binnen heel het bestandssysteem naar alle bestanden met als owner (user) *root* en waarbij het SUID-bit gezet is (tip: `find` kan je daarbij helpen!) Laat zien hoe je dat doet.

## 2.9.2 Opdracht: Harde schijf toevoegen (storage hardware toevoegen)

Na het toevoegen van directories en het aanpassen van de rechten, ga je nu een extra (virtuele) harde schijf toevoegen die we in de volgende opdracht gaan gebruiken om een bestandssysteem op aan te maken. Daarna ga je op de overige ruimte werken met een Logical Volume Manager!

- 1) Maak vanuit de shell een overzicht van alle harde schijven en partities op je systeem. Welk(e) commando('s) (tip: `fdisk`, `fdisk`, `parted`, `blkid`, `lsblk` (geeft een 'mooi' overzicht, ....(er zijn er vast nog meer)) met welke opties heb je hiervoor gebruikt en wat zijn de resultaten?
- 2) Voeg een harde schijf toe aan je VM. (In VMware: VM → Settings... en dan Add... → Harddisk, in sommige gevallen moet je VM hiervoor uit staan) (optioneel: op welke manier kun je vanaf de commandline de machine uitzetten? ).  
**LET OP:** als je bestaande harddisk van type NVMe is (hoogstwaarschijnlijk wel na keuze voor Red Hat Enterprise Linux 8 profiel in VMware), maak je extra disk dan ook van type NVMe; als je kiest voor SCSI dan is de kans groot dat het systeem niet meer boot tot je de extra disk weer verwijderd hebt;
- 3) Kijk nu nogmaals welke harde schijven en partities in je VM aanwezig zijn. Welke commando's met welke opties heb je dit keer gebruikt en wat zijn de resultaten?
- 4) Maak vanuit de shell op de nieuwe harde schijf 2 *primary* partities van ieder 512MB aan (meer mag natuurlijk ook, als je je schijf groter hebt gemaakt). Doe dit op basis van een DOS/MBR partitietabel/*disklabel*. Interactief is `fdisk` vrij gebruiksvriendelijk, maar de andere bij nummer 1) genoemde comando's kun je hiervoor ook gebruiken.  
Welk commando heb je gekozen en hoe ben je toen verder gegaan?
- 5) Maak nu nog 2 *primary* partities aan van ieder 128MB en probeer daarna een derde aan te maken. Wat valt je op?  
Verwijder partitie 4 en maak in plaats daarvan een *extended* partitie aan ter grootte van de rest van de schijf. Maak nu nog 2 partities van 128MB aan. Schrijf tot slot de wijzigingen naar disk.
- 6) Bekijk nu nóg eens welke harde schijven en partities er op je systeem aanwezig zijn. Benoem voor elke partitie op de nieuwe schijf wat voor partitie het is.

## 2.9.3 Opdracht: Filesystems maken

- 1) Maak op de eerste partitie uit deelopdracht 2.9.2 een *ext2*-filesystem aan en op de tweede een *ext3*-filesystem. Welke commando's met welke opties heb je hiervoor gebruikt? (Denk aan: `man -k` en bijvoorbeeld het woord *filesystem*). Schrijf de commando's die je gebruikt weer op!



- 2) Wat is het verschil tussen die twee filesystems? En wat houdt dat verschil in?
- 3) Koppel de eerste partitie aan de directory `/data/part1` en de tweede aan directory `/data/part2` (vergeet niet ervoor te zorgen dat voorafgaand aan het koppelen de directories bestaan. TIP: gebruik bij de diverse commando's de optie `-v` (*verbose*) om meer feedback te krijgen wat er tengevolge van het uitvoeren van het commando op het systeem gebeurt).  
Welke commando's met welke opties heb je hiervoor gebruikt? Het koppelen van een disk, of partitie wordt *mounten* genoemd!
- 4) Test of het lukt om de directory `/etc` (of een deel daarvan!) naar beide partities te kopiëren. Voor het kopiëren van directories moet je mogelijk een extra optie meegeven!
- 5) Bekijk hoeveel ruimte op beide partities nu vrij en in gebruik is (gebruik bijvoorbeeld `df -h`). Zie het verschil tussen die twee? Dat is te verklaren door het verschil tussen `ext3` en `ext2` waar we naar vroegen bij vraag 2.
- 6) Controleer of de beide filesystems nog in orde zijn. Welk commando met welke opties heb je hiervoor gebruikt? (Tip: `man -k filesystem`). Mogelijk moet je eerst `umount` gebruiken om de partitie / het filesystem vrij te geven.
- 7) Zorg ervoor dat de partities automatisch aangekoppeld worden op de plaatsen zoals beschreven in punt 3) hierboven. Welke wijzigingen heb je gemaakt?
- 8) Test het door je systeem opnieuw op te starten en daarna te kijken of de filesystems inderdaad gekoppeld zijn.

## 2.9.4 Opdracht: Logical Volume Manager (LVM) Volumes aanmaken en in gebruik nemen

- 1) Unmount `/data/part1` (uit deelopdracht 2.9.3) en initialiseer de bijbehorende partitie als een LVM *physical volume*. Welke commando's met welke opties heb je hiervoor gebruikt? (Tip: `pvcreate`)
- 2) Maak een volume group genaamd `vg_data` die bestaat uit bovenstaand physical volume. Welk(e) commando('s) met welke opties heb je hiervoor gebruikt? (Tip: `vgcreate`)
- 3) Bekijk de eigenschappen (waaronder de grootte) van deze volume group. (Tip: `vgdisplay`)
- 4) Maak nu twee logical volumes aan in deze volume group: (Tip: `lvcreate`)
  - o Naam: `lv_webcontent`                      Size: 64 MB
  - o Naam: `lv_database`                        Size: 192 MB
- 5) Maak op beide volumes een XFS filesystem aan. Welk(e) commando('s) met welke opties heb je hiervoor gebruikt? (Tip: `mkfs.xfs`)
- 6) Zorg ervoor dat het filesystem in `lv_webcontent` bij het booten van je systeem automatisch gemount wordt in `/data/webcontent`, in plaats van de mount van `/data/part1` die je in deelopdracht 2.9.2 hebt aangemaakt, en het filesystem in `lv_database` in `/data/db`. Mount ze ook nu meteen. Welk(e) commando('s) met welke opties heb je hiervoor gebruikt?
- 7) Kopieer nu de inhoud (inclusief alle onderliggende subdirectories) van `/usr/share/man` en `/usr/share/vim` naar `/data/webcontent`, resp. `/data/db`.

## 2.9.5 Opdracht: bestandspermissies en symbolic links

- 1) Log in als de user `root` (of gebruik `sudo`) en maak het volgende bestand aan: `/data/topsecret.txt`.
- 2) Wat zijn de permissies van dit bestand? Wat betekent dat?
- 3) Zorg er nu voor dat niemand behalve `root` het bestand kan lezen, schrijven of uitvoeren. Welk(e) commando('s) met welke opties gebruik je hiervoor? Wat zijn de nieuwe permissies?
- 4) Test of dit werkt door als user (of een andere normale gebruiker) in te loggen en probeer het bestand te openen of te tonen. Laat zien dat je dit doet en wat het resultaat is.



- 5) Maak nu een symbolic link aan in de home-directory van root naar bovenstaand bestand, genaamd `secretpassage.txt`. (Tip: In) Welk(e) commando('s) met welke opties heb je hiervoor gebruikt?
- 6) Wijzig de inhoud van `secretpassage.txt`, zet er iets in als "Only for carrots.". Laat nu de inhoud van `/data/topsecret.txt` zien. Hoe verklaar je dit?

## 2.9.6 Vragen Linux bestandssystemen

1. Beschrijf wat *journaling* inhoudt binnen de context van bestandssystemen
2. Welk van de volgende bestandssystemen hebben *journaling* als faciliteit?
  - a. ext2
  - b. xfs
  - c. ext3
  - d. ext4
  - e. NTFS
  - f. FAT
3. Wat betekenen de klassieke rechten (u, g, o en r, w, x) onder UNIX/Linux?
4. Geef van de volgende paren symbolische en numerieke rechten aan of deze identiek zijn en wat de rechten betekenen (voor elk identiek paar natuurlijk maar een enkele betekenis, voor de niet-identieke de twee verschillende betekenissen).

Voorbeeld "rwxr-xr-x 751" is niet identiek, want rwxr-xr-x betekent "volledige rechten voor de eigenaar, lees- en uitvoerrechten voor de groep en alle anderen" terwijl de numerieke rechten 751 betekenen "volledige rechten voor de eigenaar, lees- en executierechten voor de groep, uitvoerrechten voor alle anderen".

De paren die jullie zelf moeten beschrijven:

a.	rwxrwxr-x	775
b.	rwxr-xr-x	755
c.	rw-r--r--	622
d.	rw-r-----	640
e.	rwxr-x--x	752
f.	rw-x--x---	710
5. Wanneer een *umask* actief is met waarde (0)022, welke rechten worden toegekend aan een nieuw aangemaakt bestand (bijvoorbeeld door deze met touch aan te maken)?
6. Waarvoor wordt een bestandssysteem gebruikt?
7. Wat is het hoofddoel van een bestandssysteem?
8. Uit welke vier componenten bestaat een bestandssysteem?
9. Wat is onder Linux het startpunt van het bestandssysteem (Bij Windows is het C:\)?
10. Wat is het verschil tussen een absoluut en een relatief pad?
11. Met welk commando kun je de huidige directory opvragen?
12. Welke beperkingen heeft een padnaam onder Linux?
13. Welk commando kun je gebruiken om een disk of een partitie te koppelen aan het OS?
14. In welk bestand worden de gekoppelde partities (mounted) opgeslagen?
15. Wat zijn de belangrijkste standaard directories onder linux?
16. De meeste bestandssystemen onder Linux kunnen werken met
17. Met welk commando kun je een hard link maken en verwijderen?
18. Wat is een symbolic link?
19. Linux kent vier file-type bits. Welke zijn dat?
20. Met welk commando kun je informatie opvragen over een bestand of een directory?
21. Wat is de functie van `chmod`?
22. Wat is de functie van `chown` en `chgrp`?
23. Wat is de functie van `umask`?
24. Hoeveel bitjes gebruikt Linux om een gebruikers en groepen permissies te verlenen (*permission bits*)?
25. Welk 'software' is nodig om data op een harde schijf te kunnen schrijven?
26. Met welk commando kun je zien welke disken en partities er op het systeem beschikbaar zijn?
27. Met welke commando's kun je een harde schijf indelen?





28. Geef een schematische weergave van hoe schijven, partities en bestandssystemen aan elkaar verbonden zijn.
29. In welke directory kom je de device file van een harde schijf tegen?
30. Wat is de functie van de *swap* partitie?
31. Welke twee typen partitie-tabellen kun je tegenkomen op een een harde schijf?
32. Noem een aantal voordelen van het gebruik van *logical volume management (LVM)*.
33. Wat is kenmerkend aan de commando's die bij LVM worden gebruikt?
34. Met welk commando kun je informatie over LVM opvragen?
35. Kun je een harde schijf na het partitioneren direct met bestanden beschrijven?
36. Wat zijn belangrijke kenmerken van een bestandssysteem?
37. Met welke tool kun je onder Linux controleren of het bestandssysteem problemen vertoont?
38. Beschrijf hoe je onder Linux een partitie een bestandssysteem geeft.

## 2.10 Week 5, College 1: Core Network Services: DHCP/DNS

### Inleiding

Het Beter Medisch Centrum (BMC) heeft een uitgebreid netwerk. Het is belangrijk dat IP-adressen automatisch uitgedeeld kunnen worden via DHCP en dat namenresolutie foutloos gaat door gebruik te maken van DNS.

Aan jou de taak om dit allemaal te realiseren! Beide onderwerpen voer je zowel onder Linux als onder Windows uit.

Om alle opdrachten te kunnen uitvoeren heb je de volgende VM's nodig (je mag de bestaande hergebruiken – het is dan aanbevolen vooraf een snapshot van elke VM te maken – of een nieuwe omgeving creëren):

- Een Windows 2016 Server DC (dc1.bmc.local)
- Een Windows 2016 Core Server (core1, onderdeel van het bmc.local domain)
- Een Windows 10 Client (client1)
- Een Rocky Linux 8 systeem (rocky1)

### Theorie:

#### Verplicht:

- Slides,
- Dit werkboek met vragen en antwoorden (zie afzonderlijk document “Antwoorden\_BIPL\_Werkboek\_v1.4.1vt”!)
- Boek: “Unix and Linux System Administration Handbook, 5th Edition”:
  - Chapter 13 – *TCP/IP Networking*:
    - 13.7 *DHCP: The Dynamic Host Configuration Protocol*: blz. 402 t/m 406
  - Chapter 16 – *DNS*:
    - Inleiding t/m *Running in a chrooted jail*: blz. 498 t/m 554
- Boek: “Windows Server 2016 Unleashed”:
  - Hoofdstuk 9 – *Domain Name System, WINS, and DNSSEC*:
    - Inleiding t/m *Managing DNS with PowerShell*: blz. 258 t/m 304
  - Hoofdstuk 10 – *DHCP, IPV6, IPAM*:
    - Inleiding t/m *DHCP Split-Scope Configuration Wizard*: blz. 321 t/m 347

#### Optioneel:

- <https://www.tecmint.com/install-bind-private-dns-server-on-rhel-8/>

#### Video's

- DHCP: <https://www.youtube.com/watch?v=leCH-bs38UM>
- DHCP Failover Windows 2016: <https://www.youtube.com/watch?v=6zjU6uQMY3o> (beschrijft Windows 2012 maar ook geldig voor Windows 2016)
- DNS: <https://www.youtube.com/watch?v=W07dxCREOTc>
- DNS Zones: <https://www.youtube.com/watch?v=WYCPTuGNj7U>





## 2.10.1 Opdracht: Inrichten van de basisomgeving

Voor het uitvoeren van de opdracht is belangrijk dat je je omgeving inricht zoals afgebeeld in Figuur 1 op bladzijde **Error! Bookmark not defined.**

Richt dit in op je VMware Workstation voordat je verder gaat met de volgende opdrachten. Je mag afwijken van het gekozen VMnet of IP-range als je snapt wat de consequenties zijn... zoals het gebruik van een Virtual Switch zoals we eerder hebben gebruikt.

**Let op:** voor het installeren van software onder Linux heb je zeer waarschijnlijk toegang tot het internet nodig. Je kunt besluiten om een tweede netwerkkaart aan de VM toe te voegen en deze uit te schakelen als de installatie gelukt is of door via een VyOS router te werken die met zijn WAN interface aan VMnet8 is gekoppeld. Het gevaar van meerdere DHCP-servers in een netwerk is dat de DHCP-server van VMware kan worden uitgeschakeld.

VMnet8 van het type NAT kan je gebruiken om je VM toegang te geven tot het Internet. Dat is bijvoorbeeld heel bruikbaar bij het Linux systeem bij het installeren van pakketten.

TABEL 8 IP-INSTELLINGEN

VM	NIC	Netwerk	IP adres	Geïnstalleerde services tijdens labs:
<b>BMC-DC1</b> (Win2016Srv)	ethernet0	LAN Segment "Windows" of VMnet2 Host-only	192.168.4.1/24	SMB Server IIS Management
<b>BMC-Core1</b> (Win2016Core)	ethernet0	LAN Segment "Windows" of VMnet2 Host-only	192.168.4.4/24	DHCP server x.y.2.0 HTTP + SMB server
<b>BMC-PC1</b> (Win10Client)	ethernet0	LAN Segment "Windows" of VMnet2 Host-only	DHCP	Voor tests van Windows gebaseerde services
	ethernet1	LAN Segment "Linux" of VMnet3 Host-only	DHCP	Voor tests van Linux gebaseerde services
<b>rocky1.bmc.test</b> (Rocky 8)	ethernet0	LAN Segment "Linux" of VMnet3 Host-only	192.168.5.1/24	DHCP server x.y.3.0 Apache   Squid   Samba
	ethernet1	VMnet8 NAT	DHCP	Optioneel, bij gebruik van VyOS niet nodig
<b>VyOS</b>	ethernet0	VMnet8 NAT	DHCP	Systeem is optioneel, indien niet gebruikt dan moet rocky1.bmc.test een ethernet1 aansluiting aan VMnet8 NAT hebben
	ethernet1	LAN Segment "Linux" of VMnet3 Host-only	192.168.5.254/24	

**Let op: BMC-PC1 wordt nu op beide interfaces een DHCP client, eerder had deze een vast adres**

Als je hebt gekozen voor VMnet2 en VMnet3 en niet voor LAN segmenten, controleer dan in VMware Workstation → Edit → Virtual Network Editor dat zowel VMnet 2 als ook VMnet 3 van het type "Host-only" is en dat er geen VMware DHCP-service actief is op beide subnetten. Gelukt? Je bent klaar voor de volgende opdracht.

Het is voor elke dienst die je vanaf een server wilt aanbieden van groot belang dat de server eerst een IP adres heeft dat voor andere systemen bereikbaar is. Zorg dus eerst dat je de server kunt pingen vanaf de beoogde client(s) voor je met de diensten aan de slag gaat!



## 2.10.2 Opdracht: Linux DHCP Server

We gaan allereerst een Linux DHCP-server configureren op het eerste Rocky 8 systeem. We gebruiken BMC-PC1 om te zien of dit is gelukt. Voor de Installatie van de DHCP Server kun je gebruik maken van de informatie op de slides, van hoofdstuk 14 van “Unix and Linux System Administration Handbook, 5th Edition” en/of de output van het commando: `less /usr/share/doc/dhcp*/dhcpd.conf.example`:

- 1) Installeer op “rocky1” DHCP met `sudo dnf install dhcp-server`.
- 2) Stel de configuratie van de DHCP-server in volgens deze specificaties (TIP: je kunt de `dhcpd.conf.example` file compleet kopiëren (en hernoemen naar `dhcpd.conf`) naar de `/etc/dhcp` directory of je kunt delen uit het voorbeeld bestand kopiëren en vervolgens aanpassen naar de onderstaande instellingen. Zelf typen is natuurlijk ook een optie, kijk dan naar het voorbeeld in de presentatie bij de eerste les van week 5! TIP 2: denk aan de manpage):
  - o Alle clients krijgen als *domain name* “bmc.test”.
  - o Alle clients krijgen als *name server* `rocky1.bmc.test` toegewezen.
  - o De *default lease time* is 600.
  - o De *max lease time* is 7200.
  - o Clients in het subnet `192.168.5.0/24` krijgen een IP-adres in de range `192.168.5.100-192.168.5.150`
  - o Clients in het subnet `192.168.5.0/24` krijgen als router “192.168.5.254”.
- 3) Start de DHCP-service op en zorg ervoor dat deze bij een reboot wordt gestart. (TIP: bekijk de manpage van `systemctl`). Met `systemctl status dhcpd` kun je opvragen of de service gestart is en of er eventuele fouten zijn. Let op de volgorde van beide tools.  
Mocht de service niet succesvol gestart worden, dan is het eerste om te controleren of je elke option-en range-regel in `/etc/dhcp/dhcpd.conf` wel hebt afgesloten met een puntkomma (;).
- 4) Zorg dat “IBM-PC1” via DHCP een adres krijgt toegewezen door deze aan te zetten of een nieuw adres op te vragen met cmd → `ipconfig /renew Ethernet1`.  
Controleer met cmd → `ipconfig` of dit is gelukt.
- 5) Kijk op de Linux DHCP-server in de DHCP *leases* database en ga na of je daar inderdaad ziet dat er een IP-adres is uitgedeeld. Via `man dhcpd` (bijna aan het eind!) kun je achterhalen in welk bestand de uitgegeven IP-adressen (de *leases*) staan.

## 2.10.3 Opdracht: Windows DHCP Server

De beheerders bij BMC willen niet afhankelijk zijn van een enkel platform. Daarom willen zo ook een MS Windows DHCP-server. Wij gaan daarom een Windows DHCP-server configureren op het Win2016Core systeem. We gebruiken de Win10Client in combinatie met een andere virtuele netwerkkaart om te zien of dit is gelukt.

Installatie van de DHCP Server:

- 1) Installeer DHCP op de eerste Core machine. Maak hierbij gebruik van de Server Manager op Win2016Srv of installeer dit met PowerShell vanaf de Core server zelf.
- 2) Vanaf DC1/PC1 moet je met behulp van een Microsoft Management Console (MMC; te starten als `mmc.exe`) de configuratie van de DHCP-server kunnen bekijken en aanpassen. Hiervoor moet aan een MMC de DHCP-server snap-in worden toegevoegd. Omdat op de grafische Windows server de DHCP-service niet is geïnstalleerd, moet je de feature *DHCP-server tools* eerst installeren. Met PowerShell is dat eenvoudig. De Windows feature heet “rsat-dhcp”. De client heeft met de installatie van RSAT al de mogelijkheid om direct de snap-in toe te voegen. Toch heeft beheer vanaf de server in dit geval de voorkeur omdat we de client gebruiken om werking van de DHCP te testen.
- 3) Configureer de DHCP-server. Geef in de scope naast een IP-range (`192.168.2.100-199/24`) ook een DNS-server (`192.168.2.2`). Geef daarbij tevens de domeinnaam “bmc.local” op. Voor het configureren



van een gateway, dns-server en een domeinnaam moet je gebruik maken van opties die gedefinieerd zijn in [RFC 2132](https://tools.ietf.org/html/rfc2132). De DNS server heeft de waarde 006 en met 015 kun je een domeinnaam definiëren. Zie ook [http://technet.microsoft.com/en-us/library/cc787375\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc787375(WS.10).aspx)

- 4) Activeer de scope.
- 5) Controleer op je client nu op iedere netwerkkaart een ip adres heeft gekregen en controleer met `ipconfig /all` of deze adressen afkomstig zijn van de juiste DHCP Servers (Linux en Windows). Let op dat het gelijktijdig in hetzelfde netwerk aan hebben staan van de Linux en Windows DHCP-server kan er voor zorgen dat de geautoriseerde Windows DHCP-server wordt uitgeschakeld. Het is 'lastig' om dit weer ongedaan te maken.
- 6) **Optioneel** voor Server 2016: Installeer ook de DHCP-service op een andere server en configureer "fail-over". Controleer of de cliënt ook een IP-adres krijgt als je de DHCP-service op een server uitzet.

## 2.10.4 Opdracht: Windows DNS Server

Het BMC beheert de DNS voor de eigen webserver. Als om 9:00 iedereen aanlogt kan het best druk worden. Daarom moet de load worden verdeeld over een drietal webserver. Dit kan vrij eenvoudig door middel van load balancing via Round Robin. Daar gaan we:

- 1) De interne website van BMC staat in het `bmc.local` domein onder de naam [home.bmc.local](http://home.bmc.local)
- 2) Configureer voor de webserver (www) het zogenaamde "round robin" via de DNS Manager. Round Robin zorgt ervoor dat je een enkele naam koppelt aan meerdere ip adressen. Dit zorgt op een eenvoudige manier voor load balancing. Om dit mogelijk te maken koppel je de hostnaam [home.bmc.local](http://home.bmc.local) via drie verschillende A-records aan de (fictieve) ip adressen 1.0.0.1, 1.0.0.2 en 1.0.0.3. Gebruik hiervoor de DNS Manager op je Domain Controller dc1 en voeg drie A-records toe aan de `bmc.local` zone.
- 3) Test vanaf client1 met "ping" of `www.bmc.local` steeds verwijst naar een ander ip-adres. Het pingen zelf lukt natuurlijk niet want de ip-adressen waar naar wordt verwezen zijn niet bereikbaar:
  - a. `ipconfig /flushdns`
  - b. `ping home.bmc.local` (naar welk IP-adres wordt verwezen?)
  - c. `ipconfig /flushdns`
  - d. `ping home.bmc.local` (naar welk IP-adres wordt verwezen?)
  - e. `ipconfig /flushdns`
  - f. `ping home.bmc.local` (naar welk IP-adres wordt verwezen?)

## 2.10.5 Opdracht: Linux DNS Server

Configureer op de Rocky Linux server een DNS Server. Gebruik hiervoor de onderstaande informatie en de informatie uit de presentaties, hoofdstuk 16 (paragraaf 16.8) van "Unix and Linux System Administration Handbook, 5th Edition" of tutorials zoals te vinden op het Internet zoals <https://www.tecmint.com/install-bind-private-dns-server-on-rhel-8/> (als je een andere tutorial wilt gebruiken, controleer dan wel of deze in grote lijnen overeenstemt met wat in de presentatie beschreven staat, want niet alles wat op Internet te vinden is klopt helemaal (en dat geldt niet alleen voor dit onderwerp!)).

- 1) Installeer op "rocky1" de DNS server en bijbehorende tooling: `sudo dnf install bind bind-utils`. (let op: de bind directory onder `/etc/` bestaat niet, kijk / zoek naar `named`)
- 2) Bereid de lokale BIND-configuratiefile (`named.conf`) voor: luisteren op de juiste poorten (behorend bij IP adressen 127.0.0.1 en 192.168.5.1) en naar juiste clients (localhost en 192.168.5.0/24). Maak daarnaast een definitie aan voor de (*forward*) zone "`bmc.test`" (bekijk documentatie, presentatie, boek, manpage of configfiles om te bepalen wat, waar en hoe je dat moet configureren).



- 3) Maak de zone-database aan met de bestandsnaam die je in je configuratie hebt opgenomen en stel de opties en het SOA-record als volgt in (je kunt beginnen met een lege configuratie-file, maar je kunt ook een bestaande zone-database zoals “/var/named/named.empty” kopiëren en in de kopie de aanpassingen maken):

Configuratie-item	Waarde	Toelichting
<b>Default time-to-live</b>	300	300 seconden (5 minuten). Erg kort, maar wijzigingen van bijv. IP-adressen zijn dan snel bekend op clients en caching DNS-servers. Niet aan te raden voor productie.
<b>Zone's master name server</b>	rocky1.bmc.test.	De master (en voor dit moment enige) nameserver van dit domein.
<b>Zone's responsible person</b>	hostmaster.bmc.test.	Mailbox van de verantwoordelijke beheerder; dit wordt geïnterpreteerd als hostmaster@bmc.test.
<b>Serienummer</b>	In het formaat: YYYMMDD## Bijv.: 2021100601 (1 <sup>e</sup> wijziging op 6-oct-2021)	Dit formaat is een “best practice”. Je kunt hieraan zien wanneer de laatste wijziging heeft plaatsgevonden en je voorkomt zoveel mogelijk dat je per ongeluk een lager serienummer ingeeft.
<b>Refresh</b>	3M	3 minuten. Omdat we de TTL zo laag hebben ingesteld, moeten we ervoor zorgen dat eventuele slave server ook zo snel mogelijk updates krijgen. Zo'n lage waarde is niet aan te raden voor productie!
<b>Retry</b>	1M	1 minuut. Slave servers proberen bij een mislukte update het elke minuut opnieuw. Nogmaals: zo'n lage waarde is niet aan te raden voor productie!
<b>Expire</b>	30D	30 dagen. Als een slave-server geen contact kan krijgen met de master, gaat deze nog 30 dagen door met het beantwoorden van queries.
<b>Minimum</b>	1M	60 seconden. Als een DNS-server een query niet kan beantwoorden (record bestaat niet), dan wordt dit 60 seconden gecachet. Daarna proberen clients opnieuw of de DNS-server inmiddels het antwoord toevallig wel weet. Zo'n lage waarde is niet aan te raden voor productie.

- 4) Neem een nameserver (NS) record voor deze zone op die wijst naar “rocky1.bmc.test.” (let op de punt aan het einde).
- 5) Neem een host (A) record op voor de host “rocky1” zelf, die wijst naar het IP-adres van “rocky1.bmc.test.”.
- Let op de syntax: <name> IN <type record> <IP>, bijvoorbeeld: test.bmc.test. IN A 1.1.1.1
- Let ook op de punt achter de *fully qualified* host-/domeinnaam! Let bij de Linux DNS-server sowieso goed op de plaatsing van punten, anders levert dat problemen op. Aan het eind van een *fully qualified* domeinnaam **moet** altijd een punt staan anders wordt deze geïnterpreteerd als een hostname waaraan de domeinnaam nog moet worden toegevoegd!
- 6) Neem host (A) records op voor al je systemen in dit netwerk behalve de client.



- 7) Waarom is het niet verstandig handmatig een host-record voor de client in te vullen? Hoe zou je op een goede manier toch naamresolutie voor “client1” mogelijk kunnen maken?
- 8) Is de zonefile leesbaar voor de named user? (Dit is belangrijk!). (Hoe kon je dat controleren? Kijk terug in de commando-lijstje!)
- 9) Controleer je complete BIND configuratie met `sudo -u named named-checkconf -z` (“sudo -u named” zorgt ervoor dat je het meteen ziet als de bestandsrechten niet goed staan, je ziet dan “not loaded” en “permission denied” errors). Als er alleen meldingen zijn met daarin “loaded serial”, dan wordt de syntax van zowel `/etc/named.conf` als van je zone bestanden als correct gezien en kan de service gestart worden. Staan er errors tussen (anders dan “not loaded” en “permission denied” errors), lees deze dan goed om erachter te komen wat er mis is (het getal achter de bestandsnaam is het regelnummer waar de fout zich (ongeveer) bevindt).
- 10) Voor het starten van de service kun je weer `systemctl` gebruiken. Let op dat `named-checkconf` alleen de syntax bekijkt, mocht de DNS server niet gestart kunnen worden dan wil het niet zeggen dat `named.conf` daar niet ‘schuldig’ aan kan zijn. Het is in onze situatie niet waarschijnlijk dat `named.conf` de oorzaak is, maar je weet het niet voor 100% zeker.  
`systemctl status named` geeft mogelijk behulpzame informatie!
- 11) Zet de lokale firewall open voor DNS verkeer (de functie en mogelijkheden van de firewall zullen in een andere cursus worden besproken, voor nu is het voldoende om te weten dat je de firewall moet vertellen dat DNS-verzoeken moet worden toegelaten en dat je dit doet door de onderstaande regel over te nemen!) met het commando:  
`sudo firewall-cmd --add-service=dns ; sudo firewall-cmd --runtime-to-permanent`
- 12) Reload of herstart de named daemon en test met het commando “dig” op je Linux systeem of je DNS-server antwoorden kan geven voor het domein “bmc.test”.  
Bijv.: “dig +noall +answer rocky1.bmc.test @127.0.0.1”. @127.0.0.1 betekent dat je gebruik wilt maken van de DNS-server op IP-adres 127.0.0.1 (localhost dus).
- 13) Doe daarna hetzelfde maar gebruik in plaats van 127.0.0.1 het externe IP-adres van de server (dus bijvoorbeeld “... @192.168.5.1”)
- 14) Zorg er voor dat de DNS-server automatisch start na een reboot. Dit doe je met behulp van het commando `sudo systemctl enable named`. (Overigens geldt dit ook voor de andere services zoals die van de DHCP-server!)
- 15) Stel je netwerk-configuratie op je Linux servers zo in, dat zij gebruik maken van de lokale DNS-service (controleer `/etc/resolv.conf` nadat je het netwerkinterface hebt gedeactiveerd en opnieuw geactiveerd).
- 16) Kan je vanaf je Windows client ook rocky1.bmc.test resollen (misschien moet je het netwerkinterface in het Windows netwerk even loskoppelen, dit gaat het makkelijkst via VMware)?

Nu *forward* DNS lookups correct werken is het tijd om ervoor te zorgen dat *reverse lookups* ook gaan werken, dus ook vertaling van IP adressen naar domeinnamen in plaats van alleen andersom.

- 1) maak een definitie aan voor de reverse zone die past bij netwerk 192.168.5.0/24: “5.168.192.in-addr.arpa” (bekijk documentatie, PPT, boek, manpage of configfiles om te bepalen wat, waar en hoe je dat moet configureren).
- 2) Maak de zone-database aan met de bestandsnaam die je in je configuratie hebt opgenomen en stel de opties en het SOA-record hetzelfde in als voor je *forward* zone (misschien is het het handigst om de *forward* zone te kopiëren en in de kopie de aanpassingen maken) en neem daarin tenminste twee *resource records* op: een NS record voor de zone en een PTR record voor je server. En liefst daarnaast PTR records voor alle systemen in je *forward* zone die een adres in 192.168.5.0/24 hebben.



- 3) Controleer opnieuw de configuratie met `sudo -u named named-checkconf -z` en breng indien nodig verbeteringen aan.
- 4) Herlaad de BIND configuratie (gebruik bijvoorbeeld `sudo systemctl reload named`) en controleer de status (met `systemctl status named`).
- 5) Kun je het IP adres van de server resolvable naar een *fully qualified domain name*? Ook vanaf je Windows client?

## 2.10.6 Vragen DHCP en DNS

1. Welke service geeft de mogelijkheid om computers een DNS en WINS-server mee te geven?
2. Welke vier stappen heeft het DHCP proces?
3. Wat is de voorloper van DHCP?
4. In welk directory kun je onder Linux (in veel gevallen) de DHCP configuratie bestanden vinden?
5. Welke service heb je nodig om DHCP-verzoeken door een router te krijgen?
6. Wat is DHCP failover?
7. Hoe worden de databases van een DNS-server genoemd?
8. Wat is een namespace als het gaat om een DNS-server?
9. In welk lokale bestand wordt bij Linux en Windows altijd eerst gekeken (eigenlijk wordt dit bestand in het cache geladen) voordat er een DNS-verzoek wordt verzonden?
10. Waarom wordt er gesteld dat DNS een hiërarchisch structuur heeft?
11. Hoe wordt het proces genoemd dat ervoor zorgt dat een DNS-server het antwoord op een vraag kan geven als de server het antwoord niet zelf weet?
12. Wat is Dynamic DNS?
13. Welke DNS-records kun je in een DNS-server tegenkomen met betrekking tot IPv4?
14. Wat is een Start of Authority record?
15. Met welke commando's kun je de werking van een DNS-server testen?
16. Op welk manier kun je DNS-verzoeken veiliger maken?
17. Wat is het verschil tussen een *master* en een *slave* (DNS) zone?
18. Welke configuratiefile wordt onder Linux gebruikt om de DNS-server te configureren?
19. Wat is een Authoritative nameserver?
20. Wat is de meest gebruikte Linux DNS-server?

## 2.11 Week 5, College 2: Application Services: HTTP/SMB

### Inleiding

Het Beter Medisch Centrum (BMC) heeft natuurlijk een website zodat patiënten van het ziekenhuis zich al voor de opname kunnen oriënteren en informatie kunnen krijgen over het ziekenhuis. Daarnaast is het belangrijk dat het personeel in het ziekenhuis informatie met elkaar kan delen. Denk bijvoorbeeld aan het delen van foto's of MRI-scans. Aan jou de taak om dit te realiseren! Om alle opdrachten te kunnen uitvoeren maak je gebruik van de omgeving uit de vorige les.

Om alle opdrachten te kunnen uitvoeren heb je de volgende VM's nodig (je mag de bestaande hergebruiken – het is dan aanbevolen vooraf een snapshot van elke VM te maken – of een nieuwe omgeving creëren):

- Een Windows 2016 Server DC (dc1.bmc.local)
- Een Windows 2016 Core Server (core1, onderdeel van het bmc.local domain)
- Een Windows 10 Client (client1)
- Een Rocky Linux 8 systeem (rocky1)

### Theorie:

#### Verplicht:

- Slides,





- Dit werkboek met vragen en antwoorden (zie afzonderlijk document “Antwoorden\_BIPL\_Werkboek\_v1.4.1vt”!)
- Boek: “Unix and Linux System Administration Handbook, 5th Edition”:
  - Chapter 19 – *Web Hosting*:
    - Inleiding t/m *Caches*: blz. 674 t/m 689
    - 19.4 *Apache httpd*: blz. 696 t/m 704
  - Chapter 22 – *SMB*:
    - Alles: blz. 819 t/m 829
- Boek: “Windows Server 2016 Unleashed”:
  - Hoofdstuk 11 – *Internet Information Services*
    - Inleiding t/m *Creating a Virtual Directory*: blz. 392 t/m 406
    - *Windows Server 2016 Security*: blz. 423

#### Optioneel:

- HTTP: [http://www.tutorialspoint.com/http/http\\_message\\_examples.htm](http://www.tutorialspoint.com/http/http_message_examples.htm)
- Apache op RHEL: [RHEL 8 – Deploying different types of servers – Chapter 1. Setting up the Apache HTTP web server](#) (t/m 1.4 “Setting up a single-instance Apache HTTP Server”)
- IIS: <http://www.iis.net/learn/install/installing-iis-85/installing-iis-85-on-windows-server-2012-r2> | <http://www.sherweb.com/blog/manage-and-install-iis8-on-windows-2012-server-core/> (beide nog gebaseerd op Windows Server 2012 (R2) en IIS 8(.5), maar zelfs Microsoft zelf vond de verschillen met IIS 10 niet groot genoeg om een nieuwe versie van hun installatiebeschrijving uit te brengen).
- Samba: [RHEL 8 – Deploying different types of servers – Chapter 3. Using Samba as a server](#) (t/m 3.3 “Setting up Samba as a standalone server”)

#### Video's

- 1) Apache: <https://www.youtube.com/watch?v=k2w-0GHclpl>

### 2.11.1 Opdracht: Installatie van een Linux webserver

- 1) Installeer op “rocky1” het httpd package (de Apache webserver). Bekijk hiervoor eventueel de presentatie voor deze les. Na de installatie moet je mogelijk de service nog *enablen* en starten en de firewall openzetten voor HTTP verkeer. Controleer dit met `sudo systemctl status httpd` resp. `sudo firewall-cmd --list-all`. Hoofdstuk 19 van het Linux boek geeft uitleg over de Webserver! Test op “client1” of de webserver werkt en DNS goed is geconfigureerd door naar de volgende URL's te gaan: <http://192.168.5.1> & <http://rocky1.bmc.test>
- 2) Dat stelde niet veel voor. Maar erg nuttig is het dan ook nog niet. Je gaat nu dan ook een website maken waar wat ‘nuttigers’ opstaat, namelijk een contact pagina voor [www.bmc.test](http://www.bmc.test). Maak daarvoor eerst de directory `/var/www/bmc.test` aan en maak daarin een `index.html` pagina aan. Zet er nuttige contactinformatie op zoals een adres en telefoonnummer.
- 3) Als je nu naar de inhoud van die directory kijkt, zie je dat root lees- en schrijfrechten heeft, en dat verder iedereen leesrechten heeft. Zorg er in ieder geval voor dat de apache user de files mag lezen, maar niet mag schrijven.  
Het is de bedoeling dat deze website benaderbaar is via een makkelijk te onthouden URL. De naam van de URL moet worden: <http://www.bmc.test>. Neem daarom nu eerst in je DNS-zone database een CNAME record (een soort “alias” voor een bestaande host) met de naam `www`, die verwijst naar `rocky1.bmc.test`.  
(Vergeet niet het serienummer bij te werken en de DNS-configuratie actief te maken via een reload.)



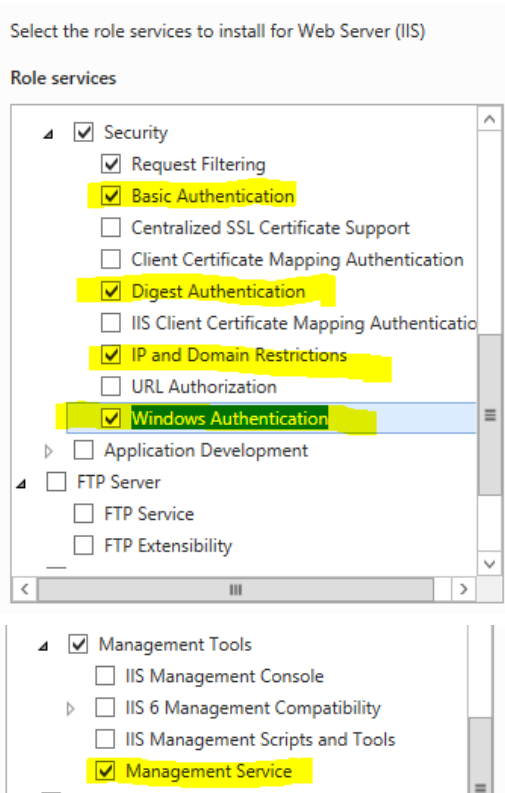


- 4) Test voor je verder gaat of het werkt door vanaf de client een nslookup te doen van “www.bmc.test”. Misschien moet je daarvoor op BMC-PC1 nog instellen dat deze zijn DNS informatie bij je Linux DNS server haalt.
- 5) In Rocky 8 worden “sites” (*virtual hosts* ofwel *vhosts*) aangemaakt onder `/etc/httpd/conf.d`. Het bestand dat daarvoor meestal wordt gebruikt is `vhost.conf` of een bestand per vhost met een bestandsnaam waaraan de vhost herkend kan worden, bijvoorbeeld `www.bmc.test.conf`. Deze zal je in de meeste gevallen zelf eerst moeten aanmaken. Zie voor de inhoud de slides bij deze les.  
Maak nu een nieuwe beschikbare site door in de juiste directory een configuratiefile aan te maken genaamd `www.bmc.test.conf`  
De site moet bereikbaar zijn via alle IP-adressen van “rocky1” (dit is de default instelling d.m.v. de *directive* `<VirtualHost *:80>`). Content voor deze site moet alleen gereserveerd worden als de client browser erheen gaat met de URL <http://www.bmc.test> of eventueel <http://bmc.test>. Gebruik hiervoor de *ServerName directive* (en eventueel het *ServerAlias directive*).  
Zorg er daarnaast voor dat de `DocumentRoot` wijst naar de directory waarin je het HTML-bestand met de contactinformatie geplaatst hebt.
- 6) Voordat je de configuratie door Apache laat inladen, is het verstandig te testen of je geen fouten hebt gemaakt (in het geval van een productie-server zou je mogelijk anders alle andere sites op de server uit de lucht kunnen halen). Gebruik hiervoor “`apachectl configtest`”.  
Als alles in orde is kun je de configuratie actief maken door `httpd` te (her)starten.
- 7) Test nu of je vanaf “rocky1” en “BMC-PC1” inderdaad je pagina te zien krijgt als je naar <http://www.bmc.test> gaat.

### 2.11.2 Opdracht: Installeer Internet Information Server (IIS) onder Windows

BMC maakt gebruik van zowel Linux als Windows. Daarom wil het bedrijf ook een Windows Webserver. Het is wel belangrijk dat de website goed is beveiligd! De informatie op deze webserver is voor intern gebruik.

- 1) Installeer IIS op de DC of als je uitdaging wilt op de Core (!) server. Dat gaat prima vanaf de Server Manager op de DC, aangenomen dat de Core server onderdeel is van het domein. Let erop dat je de extra beveiligingsopties en de “Management service” installeert.



Voor een veilige webserver...

Voor remote beheer...

Heb je problemen met het installeren van .NET Framework? Zorg ervoor dat de installatie ISO van Windows 2016 is “gemount” (geconnect)...

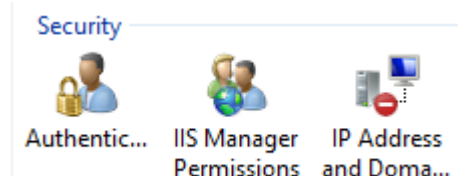
- 2) Is de installatie gelukt? Controleer het met: <http://dc1.bmc.local> of <http://core1.bmc.local/>
- 3) **Optioneel voor Core:** We moeten de core server op afstand beheren en daarom moet je op de core server remote management nog “aanzetten”:

```
Set-ItemProperty -Path HKLM:\SOFTWARE\Microsoft\WebManagement\Server -Name  
EnableRemoteManagement -Value 1
```

Gevolgd door een (her)start van de service: `Net Stop WMSVC → Net Start WMSVC`

- 4) Beveilig nu de “Default Web Site”. Eisen met betrekking tot de veiligheid die hieraan worden gesteld zijn:

- a. IP-restrictie (alleen benadering vanuit 192.168.2.0/24 netwerk, maar niet door 192.168.2.2). Default toegang is “deny”.
- b. De website mag alleen toegankelijk zijn via Basic Authenticatie. Zet ook een realm met de tekst “Basic authentication”.
- c. Disable nu de Basic Authenticatie, want deze is minder veilig (Waarom eigenlijk?). Enable nu de Windows Authentication. Benader de website vanaf een linux en vanaf een windows host. Zie je verschil? Hoe komt dit?
- d. Enable alle beschikbare Velden in de logging,



### 2.11.3 Opdracht: Maak een Windows Shared Folder

BMC wil haar patiëntgegevens kunnen opslaan. Onder Windows kan je dat doen via Shared Folders: We gaan Windows Shared Folder aanmaken op zowel een core server als ook via de GUI.

- 1) Maak de c:\data\share1 folder aan op je domein controller. Configureer de NTFS rechten als volgt:



- Users: Read & Execute
  - Administrators: Full Control
- 2) Deel de c:\data\share1 folder. De rechten voor het delen zijn "Read".
  - 3) Probeer nu als administrator vanaf de client de share te benaderen via een UNC-pad: <\\DC1\share1> .  
Mag je schrijven in de directory? Waarom (niet)?
  - 4) Maak nu de directory c:\data\share1 folder aan op je core server.
  - 5) Kopieer een logfile uit c:\inetpub\logs\logfiles\w3svc1 naar deze map.
  - 6) Deel deze directory en gebruik hiervoor de PowerShell cmdlet "new-smbshare" . Bekijk het resultaat met "get-smbshare". Welke mappen zijn allemaal gedeeld?

### 2.11.4 Opdracht: Maak een Linux SMB share

Ook onder Linux kan je mappen delen die je dan vervolgens vanaf Windows en Linux systemen kunt gebruiken. In deze opdracht ga je op "rocky1" Samba installeren en een directory delen zodat deze via het netwerk benaderbaar zijn. Je gaat ook zorgen dat die shares toegankelijk zijn op "BMC-PC1". Kijk voor tips naar de presentatie die hoort bij deze les.

- 1) Installeer het package samba met zijn *dependencies* op "rocky1". Zorg ervoor dat de service is gestart en ook na een reboot automatisch wordt gestart.
- 2) De samba configuratie staat in de file /etc/samba/smb.conf . Hernoem deze file naar /etc/samba/smb.conf~ (tilde aan het eind) en maak een nieuwe file met de onderstaande inhoud:

```
[global]
  workgroup = bmc
  server string = Samba Server %v
  netbios name = rocky1
  security = user
  map to guest = bad user
  dns proxy = no
#===== Share Definitions =====
[secure]
  path = /home/secure
  valid users = @smbgrp
  guest ok = no
  writable = yes
  browsable = yes
```

Zoals je ziet zijn een paar dingen benodigd om deze share daadwerkelijk in het leven te roepen:

- a. een gebruikersgroep smbgrp
- b. een directory /home/secure
- c. de gebruikers uit de groep "smbgrp" moeten recht hebben om te schrijven in /home/secure.

We moeten dus zorgen voor geldige gebruikers in die groep en rechten op de directory.

- 3) We maken eerst een Linux gebruiker aan:

```
sudo useradd hu                # een nieuwe user
sudo groupadd smbgrp           # een nieuwe groep
sudo usermod -a -G smbgrp hu   # we voegen de user hu toe aan de groep
sudo smbpasswd -a hu           # we geven de user een Samba password
```

- 4) Nu de rechten op de directory:

```
sudo mkdir /home/secure
sudo chown -R hu:smbgrp /home/secure/ # hu=owner, smbgrp=group
sudo chmod -R 0770 /home/secure/      # De owner+groep mag schrijven
```



```
sudo chcon -t samba_share_t /home/secure/ # ivm SELinux
```

- 5) Aanpassen van de Firewall:

```
sudo firewall-cmd --add-service=samba  
sudo firewall-cmd --runtime-to-permanent
```

- 6) Herstart de samba services:

```
systemctl restart smb  
systemctl restart nmb # (mag ook achter elkaar; dus: systemctl restart smb nmb)
```

- 7) Probeer nu de share vanaf BMC-PC1 te benaderen door er een nieuwe drive naar te mappen (in Windows Explorer met de rechtermuisknop op de eigen computer klikken en “Map network drive...” selecteren, voer als sharenaam “\\rocky1.bmc.test\\secure” in, deselecteer “Reconnect at sign-in” en selecteer “Connect using different credentials” voor je verder gaat, je mag dan de credentials van de hu user invoeren). Als dit niet lukt, probeer het dan eens vanaf een Windows client die niet lid is van een domein of vanaf een Linux systeem.

## 2.11.5 Vragen SMB en Webserver

1. Welke vijf basis services worden door SMB/CIFS geboden?
2. Samba onder Linux kan voor file sharing worden gebruikt, maar ook voor....
3. Op welk punt verschillen NFS en SMB van elkaar?
4. Wat is het configuratiebestand van SMB onder Linux?
5. Hoe wordt de mogelijkheid genoemd die het onder Windows mogelijk maakt om te bepalen wat de permissies een gebruiker krijgt als zowel NTFS- als sharepermissies zijn ingesteld?
6. Hoe kun je onder Windows een share *hidden* maken en hoe maken je bestanden onder Linux onzichtbaar voor ls?
7. Welke vijf basis componenten kom je tegen bij een URL-object?
8. Met welke commandline tools kun je een webserver testen en/of benaderen?
9. Hoe kun je op een webserver met een enkel IP-adres toch meerdere Websites hosten?
10. Op welke manier kun je HTTP-communicatie beveiligen?
11. Wat is de default poort waarop een webserver luistert?
12. Welke security role moet je toevoegen aan een Windows server om ervoor te zorgen dat alleen gebruikers met een AD-account de website kunnen benaderen?

## 2.12 Week 6, College 1: Windows Group Policies

### Inleiding

Het Beter Medisch Centrum (BMC) heeft dagelijks te maken met vertrouwelijke gegevens en een groot aantal servers en werkplekken die moeten worden beheerd. Dankzij group policies wordt de configuratie van deze Windows systemen veel eenvoudiger en betrouwbaarder en jou de taak om dit te realiseren!

Om alle opdrachten te kunnen uitvoeren heb je de volgende VM's nodig (je mag de bestaande hergebruiken of een nieuwe omgeving creëren):

- Een Domain Controller (Windows 2016) DC1 (voorkeursadres: 192.168.2.2/24)
- De domeinnaam is bmc.local
- Twee Windows Clients. De Windows clients client1 en client2 zijn onderdeel van het domein
  - Client1 (voorkeursadres: 192.168.2.100/24)
  - Client2 (voorkeursadres: 192.168.2.101/24)

### Theorie:

#### Verplicht:

- Slides,



- Dit werkboek met vragen en antwoorden (zie afzonderlijk document “Antwoorden\_BIPL\_Werkboek\_v1.4.1vt”!)
- Boek: “Windows Server 2016 Unleashed”:
  - Hoofdstuk 4 – *Active Directory Domain Services Primer*:
    - *Implementing Multiple Password Policies per Domain*: blz. 150 t/m 152
  - Hoofdstuk 17 – *Windows Server 2016 Administration*:
    - *Managing Users with Local Security and Group Policies*: blz. 580 t/m 587
  - Hoofdstuk 18 – *Windows Server 2016 Group Policies and Policy Management*:
    - Alles: blz. 595 t/m 649












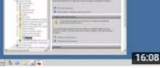
#### Optioneel:

Microsoft heeft een speciale website gemaakt over Group Policies met daarop verwijzingen naar video's step-by-step guides etc. <https://blogs.technet.microsoft.com/grouppolicy/>

#### Video's

Er zijn een aantal hele goede video's te bekijken gemaakt door ITFreeTraining:

<http://www.youtube.com/user/itfreetraining/search?query=gpo>

 <p><b>Group Policy Mechanics</b> Client driven</p>	<b>MCITP 70-640: Group Policy Introduction</b> door itfreetraining 3 jaar geleden • 44.019 weergaven This video provides an overview of Group Policy. Explaining the basic of how Group Policy works and what can be achieved using Group Policy. CC	 <p><b>MCITP 70-640: Group Policy Software Install Demonstration</b> door itfreetraining 2 jaar geleden • 34.817 weergaven This video looks at how to install, upgrade and remove software using Group Policy. The video also looks at how to set up a software share to store the install files and how software...</p>
 <p><b>MCITP 70-640: Configuring Group Policy</b> door itfreetraining 2 jaar geleden • 37.689 weergaven Group Policy has over 3000 settings. This video looks at how to perform the basic configuration of Group Policy and how to find a setting that you require. CC</p>	 <p><b>MCITP 70-640: Enforcing and Blocking Group Policy</b> door itfreetraining 2 jaar geleden • 21.761 weergaven This video will look at using the Group Policy options block and enforce. These options allow you to change the way Group Policy is processed in your domain; however this does make...</p>	
 <p><b>MCITP 70-640: Group Policy Starter GPOS</b> door itfreetraining 2 jaar geleden • 17.643 weergaven Starter GPOS provide a template like function for Group Policy. This video looks at how to use Starter GPOS and also how to copy GPOS in the same domain and to other domains. CC</p>	 <p><b>MCITP 70-640: Troubleshooting Group Policy</b> door itfreetraining 2 jaar geleden • 19.509 weergaven This video will look at how to troubleshoot which setting in Group Policy are applied by using the internal modeling tools and Resultant Set of Policy (RSOP). RSOP is the actual settings...</p>	
 <p><b>MCITP 70-640: Group Policy Filtering</b> door itfreetraining 2 jaar geleden • 24.048 weergaven There are a number of different options in Group Policy that allows you to target Group Policy to particular users and computers. This video looks at WMI filters and security that can be...</p>	 <p><b>MCITP 70-640: Group Policy Preferences</b> door itfreetraining 2 jaar geleden • 30.617 weergaven Group Policy Preferences is a technology that was added with Windows Server 2008 which greatly expands what can be achieved with Group Policy. Group Policy Preferences allows t...</p>	
 <p><b>MCITP 70-640: Group Policy Processing Order</b> door itfreetraining 2 jaar geleden • 24.664 weergaven In your domain you are more than likely going to have multiple Group Policies applied at different levels throughout your domain. This video looks at which order the Group Policies</p>	 <p><b>MCITP 70-640: Installing Group Policy Tools</b> door itfreetraining 2 jaar geleden • 26.801 weergaven This video looks at installing Remote Server Administration Tools in order to administer Group Policy from a Windows 7 Client. The video also looks at how to centralize the ADMX file....</p>	
 <p><b>MCITP 70-640: Group Policy Loopback Processing</b> door itfreetraining 2 jaar geleden • 35.209 weergaven Loopback processing allows the administrator to apply user Group Policy settings based on where the computer accounts are located rather than basing it on the user account. This is ...</p>	 <p><b>MCITP 70-640: AppLocker</b> door itfreetraining 2 jaar geleden • 23.175 weergaven AppLocker allows the administrator to control which applications are run on the computers in your domain. The rules AppLocker uses allow the scope of an application to be defined, like...</p>	

## 2.12.1 Opdracht: Aanmaken van verschillende group policies

We gaan vanuit de GPMC van de domeincontroller de onderstaande GPO's aanmaken. Geef ze ook deze namen:

- Baseline Security
- Kiosk Computer Security
- Restrict Control Panel:
- Restrict Desktop Display
- Restrict Run Command

Omdat er onder Windows server 2016 duizenden verschillende GPO settings zijn, geven we hieronder een duidelijke indicatie waar je de instelling moet kunnen vinden. Het pad naar de specifieke instellingen wordt echter niet volledig beschreven. Hierdoor zie je automatisch een groot deel van de beschikbare instellingen voorbij komen.

#### 1) Baseline Security policy



Deze policy moet ervoor zorgen dat de naam van de als laatst ingelogde gebruiker niet wordt weergegeven. De belangrijkste reden hiervoor is veiligheid. Een kwaadwillende hoeft dan “alleen” nog maar het wachtwoord te raden.

(Computer Configuration, Policies, Windows Settings, Security Settings, Local Policies, Security Options).



FIGUUR 3: BIJ DEZE COMPUTER IS DE BASELINE SECURITY POLICY NOG NIET VAN KRACHT.

2) *Kiosk Computer Security policy*

Bij de ingang van het BMC staan een aantal computers met toegang tot het netwerk en dan met name tot het internet. Om te voorkomen dat gasten, medewerkers of patiënten “vertrouwelijke” informatie kunnen achterlaten, moeten de systemen extra worden beveiligd.

Er wordt voor de optie user Group Policy loopback processing gekozen (mode “replace”). Bovendien mogen alle iconen op de desktop niet zichtbaar zijn. In deze policy wordt de computer en de user configuratie aangepast. (Computer Configuration, Policies, Administrative Templates, System, Group Policy. en User Configuration, Policies, Administrative Templates, Desktop.)

3) *Restrict Control Panel policy*

Het doel van deze policy is het ontnemen van de mogelijkheid om rechtstreeks toegang te krijgen tot de control panel en PC settings.

(User Configuration, Policies, Administrative Templates, Control Panel)

4) *Restrict Run Command policy*

Gebruikers mogen geen directe toegang krijgen tot de “run command” prompt om zo allerlei programma’s te kunnen starten. Het doel is niet om het starten van programma’s volledig tegen te gaan, maar meer om het ze moeilijker te maken.

(User Configuration, Policies, Administrative Templates, Start Menu and Taskbar)

## 2.12.2 Opdracht: Linken GPO aan de juiste OU

Om aan de eerder gestelde eisen te kunnen voldoen moeten de gemaakte policies nog wel aan de juiste OU(s) worden gelinked. Hieronder zie je welke GPO je waar moet linken om het gewenste resultaat te krijgen.

- 1) Maak eerst in je domein de volgende OU’s: gasten, medewerkers, kiosk-computers
- 2) Maak in de OU medewerkers de volgende child OU’s: artsen, verpleging, directie, admin
- 3) Maak de volgende medewerkers aan: Piet Hein, Kioskuser, Ad
- 4) De Kioskuser plaats je in de OU gasten, Piet Hein in de OU medewerkers en Ad in de OU admin. Zorg ervoor dat Ad lid is van dezelfde groepen als je domein-administrator.
- 5) Client1 is lid van “Computers” (dat is waarschijnlijk al zo) en Client2 voeg je toe aan de “kiosk-computers”.
- 6) De policy “Baseline security” moet aan het domein worden gelinked.
- 7) De policy “Restrict run command” aan de medewerkers en kiosk-computers.
- 8) De policy “Restrict Control Panel” linken aan de kiosk-computers.
- 9) De policy “Kiosk Computer Security” linken aan de kiosk-computers.





### 2.12.3 Opdracht: Hiërarchie en enforcement.

Als je op dit moment de gestelde eisen zou gaan controleren, merk je dat nog niet alle eisen worden afgedekt. Na het aanmaken en linken van de GPOs moeten er nog een aantal specifiek handelingen worden uitgevoerd. Van invloed op de werking van GPOs zijn o.a. de hiërarchische volgorde, overerving (inheritance) of juist het blokkeren daarvan en de verplichte doorvoering met behulp van een enforcement. Om aan alle eisen te voldoen maak je nog de volgende wijzigingen:

- 10) De Baseline security policy moet worden “enforced”. Omdat er in het gebruikers deel van de policy geen instellingen zijn gemaakt, moet het gebruikersdeel worden uitgeschakeld om zo performance winst te behalen bij het laden van de instellingen.
- 11) Om te voorkomen dat ook de beheerders met allerlei beperkingen te maken krijgen, moet het erven van de policies op de admin OU worden uitgeschakeld. Controleer voor en nadat je inheritance uitschakelt welke GPOs er aan de Admin OU zijn gelinked.
- 12) Met welke drie policies heeft de admin OU te maken voordat inheritance wordt geblokkeerd?
- 13) En met welke policy nadat inheritances is geblokkeerd? Waarom eigenlijk?

### 2.12.4 Opdracht: Controleer de juiste werking.

*Medewerkers PC: Client1*

- 1) Log in op Client1. Maak hierbij gebruik van een medewerkersaccount, bijvoorbeeld “piethein”.
- 2) Welke GPO’s zijn nu van toepassing voor de computer denk je?
- 3) Welke GPO’s zijn van toepassing voor de gebruiker? Controleer dit met gpresult /r
- 4) Controleer of het volgende mogelijk is:
  - Kan je als de desktop aanpassen?
  - Kan je het run commando gebruiken? (win-r toets)
  - Is de control panel direct toegankelijk?
- 5) Log nu in op Client1 met het admin account “ad”.
- 6) Welke GPO’s zijn van toepassing voor deze beheerder? Kan je het run commando gebruiken? Waarom?

*Kiosk PC: Client2*

Log in op één van de Kiosk-computers met de gebruiker “piethein” en controleer de werking van de GPOs. Hieronder worden een aantal punten genoemd die je zou moeten controleren. Indien de instellingen niet zijn zoals verwacht, dan kun je gebruik maken van gpresult en gpupdate. Let bovendien op de tijd synchronisatie tussen cliënt en server! Is de computer toegevoegd aan de OU kiosk-computers?

- 7) Staat er na het in- en uitloggen bij het inlogscherf een gebruikersnaam?
- 8) Controleer of het volgende mogelijk is:
  - Kan in het run commando worden gebruikt?
  - Kan je als de desktop aanpassen?
  - Is de control panel direct toegankelijk?
  - Is de laatst gebruikte username na het uitloggen?
- 9) Hoe kan je het verschil tussen piethein op client1 en piethein op client2 verklaren?
- 10) Controleer de werking tevens met het admin account “ad”.

### 2.12.5 Opdracht: Backup/Restore

BMC wil er nu voor zorgen dat alles wat er is gemaakt niet verloren kan gaan. Daarom moet er van de GPO’s een back-up worden gemaakt. Maak via de GPMC een back-up naar een willekeurige share op de lokale c-schijf. Powershell kan dit ook voor je uitvoeren.

- 1) Gebruik het commando “get-command -noun gpo” om te bepalen welke cmdlet je moet gebruiken voor de back-up van alle Group Policies.





- 2) Voer de cmdlet op zo'n manier uit dat van alle GPO's een backup wordt gemaakt en bekijk het resultaat.

Het is ook verstandig om meerdere personen de mogelijkheid te geven om een GPO te linken door middel van een delegation of control.

### 2.12.6 Opdracht: Folder Redirection

Het BMC wil ervoor zorgen dat er geen vertrouwelijke informatie op de clients achterblijft. Van deze informatie wordt namelijk geen back-up gemaakt en bovendien is deze informatie bij diefstal van de client niet meer vertrouwelijk. We kunnen dit mogelijk maken met "Folder Redirection".

- 1) Deel eerst de map c:\shares\medewerkers op de lokale schijf van de DC. Zorg er vervolgens voor dat de groep "Domain Users" de permissie full control krijgt. Alle andere groepen mogen worden verwijderd.
- 2) Maak nu een nieuwe GPO "Folder Redirection" ...  
(User configuration, Policies, Windows settings, folder redirection, Documents, properties)  
...en zorg ervoor dat de "Documents"-folder wordt geredirect. Kies hierbij voor de optie "Basic - Redirect everyone's folder to the same location". Maak daarbij de verwijzing naar de share maar doe dat wel volgens het UNC formaat (\\dc1\medewerkers). Link vervolgens de GPO aan de medewerker OU. Voor de uitvoering van een Folder redirection moet de gebruiker eerst uitloggen.
- 3) Controleer of de redirection werkt. Het controleren van de policy kan je doen op client1. Op de DC kijk je in de Medewerkers-share of daar de nieuwe folders voorkomen. Op de client kun je de eigenschappen van de documents map bekijken.

### 2.12.7 Opdracht: Administrative Templates

Een administratieve template bevat nieuwe of extra instellingen die je kunt gebruiken in een Group Policy. In de bestaande omgeving ga je gebruik maken van Administrative Templates om de gebruikers en computeromgeving te beheren. Naast de vele instellingen die standaard al beschreven kunnen worden is het dus mogelijk om nieuwe instellingen via een template in te lezen. Bij nieuw Service packs en/of updates zitten regelmatig ook nieuwe administrative templates. Microsoft levert een hele serie met andere extra templates. Wij zullen gaan kijken naar Office specifieke templates. In Windows 2008 en Vista is men overgegaan naar een Microsoft variant van xml. In plaats van één bestand is Microsoft tevens overgegaan naar twee bestanden. Een admx en een adml bestand. De administrative templates ga je combineren met de mogelijkheid om software te installeren via een GPO. Zoals wellicht bekend heeft Windows server 2016 duizenden verschillende policy settings. Gelukkig zijn zoekacties mogelijk, maar zijn beperkt tot de instellingen die vallen binnen de administratieve templates. Microsoft brengt voor Office altijd speciale templates uit. Zo ook voor Office 2016 en nieuwer: <https://www.microsoft.com/en-us/download/details.aspx?id=49030> | <http://www.ntweekly.com/?p=10088>

- 1) Installatie:
  - Haal de AdminTemplates file voor Office 2016 en nieuwer op en installeer deze op de DC1:
  - Maak de volgende twee onderstaande GPOs aan: Powerpoint 2016 en Word 2016
  - Kopieer nu alle ADMX bestanden en plak deze in de "C:\Windows\PolicyDefinitions\" map.
  - Kopieer ook de bijbehorende ADML bestanden en plak deze op de juiste plek.  
"C:\Windows\PolicyDefinitions\en-US" is wellicht voldoende?

Om de installatie van Word of Powerpoint te kunnen uitvoeren moet je over een \*.MSI file beschikken of een administratieve installatie uitvoeren. Het uitvoeren van een administratieve installatie van office neemt circa 15 minuten in beslag en draagt niet veel bij aan het begrip van een GPO. Je mag dit uitvoeren als je dat wilt, maar het is niet verplicht. Het maken van een .msi file van Powerpoint of Word is ook arbeidsintensief en valt dus ook buiten de scope van dit document.

- 2) Configuratie van Powerpoint 2016 (gebruik een filter om de user opties te vinden):
  - Default file location verwijzen naar een share op de DC
  - Autorecovery save frequency op 10 minuten
- 3) Configureer voor de GPO Word 2016:



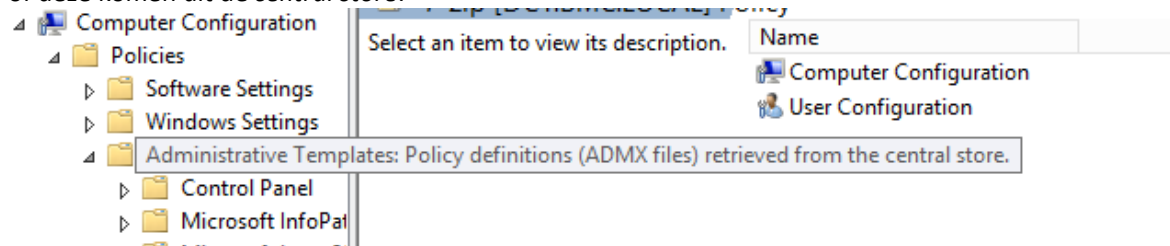
- Save AutoRecover info elke 5 minuten.
- 4) Link beide GPOs aan het domein.
- 5) Controleer de werking. Als je office niet volledig gaat installeren, kun je de met gpresult controleren of de GPO wordt doorgegeven.

## 2.12.8 Opdracht: Deploy Software

- 1) Maak een nieuwe GPO aan met de naam 7-Zip.
- 2) Zorg ervoor dat hiermee het compressie programma 7-Zip kan worden geïnstalleerd op iedere computer. Gebruik hiervoor de MSI van: <http://www.7-zip.org/download.html>
- 3) Assign 7z1900-x64.msi en controleer de werking van de policy. Om 7-Zip te kunnen installeren moet je wel een 64 bit besturingssysteem hebben geïnstalleerd.
- 4) Kijk hiervoor naar Computer Configuration → Policies → Software Settings → Software installation)
- 5) Link deze policy aan het domain en test met de user “Ad” op “client1” of 7-Zip goed wordt geïnstalleerd. Misschien is een reboot nodig...

## 2.12.9 Opdracht: Central Store.

- 1) Bij .admx bestanden kun je gebruik maken van een centrale opslagplaats die in de Microsoft documentatie “Central Store” wordt genoemd. Ook voor BMC is dit heel bruikbaar, want daardoor is op iedere DC een recente set van ADMX en ADML bestanden aanwezig.
- 2) Maak daarom op de DC een centrale opslag plaats voor ADMX en ADML files:  
\\<dc>\SYSVOL\<domain>\Policies\PolicyDefinitions\
- 3) Kopieer de admx en adml files naar deze *centrale store*.
- 4) Als je in de Group Policy Management Editor boven de administrative templates “hovert\*\*” kan je zien of deze komen uit de *central store*:



Staat hier “Administrative Templates: Policy definitions (ADMX files) retrieved from the local computer.” dan gebruik je niet daadwerkelijk een *central store*, dus controleer of je de vorige stap correct hebt uitgevoerd.

## 2.12.10 Opdracht: Preferences

- 1) Maak een GPO met daarin de onderstaande Preferences:
    - *Drive Maps*. Maak een file share op de DC en verwijst een drive mapping naar een share “data” op de domain controller dc1. De share mag pas toegewezen worden als de schijfruimte op de target computer minder dan 20GB bedraagt.
    - *Internet explorer*: homepage verwijzen naar <http://www.umcutrecht.nl/nl/>
    - *Local user*: zorg voor het aanmaken van een lokale gebruiker met de naam helpdesk. Het wachtwoord hoeft niet te worden aangepast.
- Link de policy aan de medewerkers-OU en test de werking.

## 2.12.11 Vragen Group Policies

1. Wat is een *group policy*?
2. Wat is een GPMC?

\*\* Uit Engels: ‘to hover’: hangen (boven), (blijven) zweven. Dus de muispointer er even boven stil houden



3. Op welke vier niveaus kun je een GPO linken?
4. Welke twee policies zijn standaard op een gepromoveerde domain controller aanwezig?
5. Aan welke gebruikers groep is de default domain policy gelinked?
6. Op welke twee categorieën kunnen settings binnen een GPO invloed hebben?
7. Op welke centrale locatie worden GPOs binnen een domein opgeslagen?
8. Wat is de functie van een GUID (unique ID) bij een GPO?
9. Welke GUID hoort bij welke policy in de share?
10. Wat is de functie van de waardes "User version" en "Computer version"? Onderzoek tevens de functie van (AD) en (sysvol).
11. Wat wordt er bedoeld met een *enforcement*?
12. Wat is het doel van het uitschakelen van de computer- of usersettings in een GPO?
13. Hoe kun je met gresult op de DC controleren welke settings gelden voor de gebruiker floris.devijfde?
14. Zoek uit in welke volgorde de GPOs worden uitgevoerd en welke setting wint in het geval van een conflict. Je kunt dit met een test GPO uitproberen!
15. Bekijk in de Default domain Policy het bestand GPT.ini. Welke informatie kun je hier vinden en wat is de functie van deze bestanden?
16. Hoe weten domain controllers of ze de juiste versie van een GPO hebben of dat ze om de nieuwe versie moeten vragen?
17. Met welk PowerShell cmdlet kan je een report maken in HTML-formaat?
18. Wat is het verschil tussen een GPO restore en een GPO Import.
19. Welke functionaliteiten biedt GPMA bovenop die van GPMC?
20. Welke AGPM roles zijn er?
21. Bekijk van de ADMX/ADMS bestandstypes een voorbeeld en geef aan wat de specifieke kenmerken zijn.
22. Op welke manier zijn corresponderende admx en het adml bestanden aan elkaar gelinked?
23. Bij administrative templates kun je de term *Tattooing* tegenkomen. Wat wordt hiermee bedoeld?
24. Softwareinstallatie met GPOs kan op twee manieren. De twee manieren zijn *Publish* en *Assign*. Wat zijn de verschillen?
25. Welke applicaties zijn geschikt om te installeren via een GPO.
26. Wat zijn de voordelen van het installeren van een applicatie in \*.msi vorm?
27. Wat is een *software Distribution Point*?
28. Wat zijn de voordelen van een centrale opslag?
29. Zoals je bij de introductie gezien hebt, bestaat een GPO uit een computerdeel en een userdeel. Wat is de volgorde waarin deze worden doorgevoerd? (Eerst het computerdeel of eerst het gebruikersdeel) Wat is hiervan de reden?
30. In welke situatie zou het handig kunnen zijn om de refresh interval te verhogen of te verlagen. Beschrijf dit ook voor de Random Offset time.
31. Omschrijf de functie van *Slow link detection* en *cached credentials*.
32. Wat is de (standaard) instelling voor *Processing Group Policy over Slow Links*?
33. Nu duidelijk is geworden wat er wordt bedoeld met *slow link detection*, is het handig om te weten hoe dit wordt getest. Alle Microsoft besturingssystemen van voor Vista en 2008 maakten gebruik van het ICMP protocol om een slow link te detecteren. Vista en Windows server 2008 maken gebruik van Network location Awareness (NLA). Wat is NLA?
34. Aan welke eisen moet een wachtwoord voldoen als de policy "password must meet complexity requirement" is geselecteerd?
35. Wat is de functie van *account Lockout threshold*.
36. Wat is *account lockout duration*.
37. Wat gebeurt er als de tijd tussen DC en client te veel uiteenloopt. Wat is de default instelling.
38. Waar staat EC voor in de starter GPOs?
39. Wat is het verschil tussen een *preference* en een GPO?



40. Wat wordt er bedoeld met *targeting* ?
41. Wat is de functie van de GPO Results Wizard?
42. Wat is de functie van GPO modeling?