

Uitwerkingen vragen BIPL werkboek

Deze uitwerkingen corresponderen met BIPL werkboek versie 1.4.0 (dual).

2.2 Week 1, College 1: Windows Domain

1. Wat is active directory (AD)?

AD is een centrale database waarin o.a. gebruikers en computers centraal kunnen worden beheerd

2. Welke handelingen moet je in Server 2016 uitvoeren om een AD te installeren en te configureren?

De server moet een IP-adres hebben voordat de Active directory Domain services kan worden geïnstalleerd. Voordat je de server kunt promoveren tot DC moet de server een logische herkenbare naam hebben. Voor of tijdens de installatie/ het promoveren moet een DNS-server of DNS-server rol zijn geïnstalleerd en geconfigureerd.

3. Op welk punt verschilt een workgroup van een domein?

Een werkgroep heeft geen centrale, managementserver zoals een domein een DC heeft. Er is geen hiërarchische rolverdeling. Alle systemen in een werkgroep hebben dezelfde mogelijkheden en/of beperkingen. Als je een gebruikerswachtwoord op 1 van de pc's wijzigt, dan wordt dat niet op andere pc's in een werkgroep aangepast.

4. Wat is het verschil tussen AD en Active Directory Domain Services (ADDS)?

AD staat voor Active Directory, dit is de feitelijke LDAP-database. ADDS is de LDAP-database service inclusief een aantal tools.

5. Wat is de functie van een Site?

Een site kan een representatie zijn van de fysieke structuur (topologie) van het netwerk. De definitie is: een collectie van 'well-connected' subnets. Hierin herken je IP-subnets. Systemen in het zelfde subnet zullen anders reageren (bijvoorbeeld het aanmelden en repliceren) dan systemen in twee verschillende subnetten.

6. Wat is replication?

Replicatie in de context van een domein heeft te maken met het repliceren van AD-objecten (gebruikers, wachtwoorden, printers, etc.) tussen meerdere DC's. Binnen en tussen sites varieert de replicatie-interval tussen 15 seconden en circa 180 minuten. AD replicateert (op een spanning-tree achtige manier) de gegevens via een het 'snelste pad'. Elke DC gebruikt een algoritme om het snelste pad te selecteren.

7. 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?

Alles wat in AD wordt opgeslagen (gebruiker, printer, groep) is een object. Elk object heeft een aantal kenmerken (attributes) zoals voornaam, wachtwoord en achternaam. Het schema 'beschrijft' de verschillende klassen aan objecten die kunnen worden opgeslagen in AD. De structuur van de database wordt bepaald door het schema. Objecten inclusief de kenmerken worden opgeslagen in de database.

8. Wat is de functie van een Organizational Unit?

Een OU is een 'map' waarin je objecten kunt plaatsen zodat het overzichtelijker wordt. OU's kun je gebruiken voor *delegation of control* (het overdragen van beheer mogelijkheden) en om Group Policy Objects (GPOs) aan te linken.

9. Wat is het verschil tussen een (domain) forest en een tree?

Een forest is een 'single instance' van AD. Het forest kan uit 1 of meerdere domeinen bestaan. Een forest is een 'security boundry' voor gebruikers, groepen, objecten en computers.

Een (domein)tree heeft een hoofddomein (contiguous namespace) en een gezamenlijk schema (bijvoorbeeld `bmc.local`). Elke 'boom' kan meerdere takken (subdomeinen) hebben, elke tak heeft een eigen subdomein welke is afgeleid van het hoofddomein. Bijvoorbeeld `HA1.bmc.local` en `TA2.bmc.local`. De verschillende subdomeinen hebben een transitieve *trust* relatie met elkaar.

10. Wat is de functie van een Global Catalog server?

Een GC heeft een samenvatting van alle objecten in een domein en heeft beperkte informatie van objecten in een forest. Het doel van de GC is het verhogen van de prestaties.

11. Wat is de functie van disaster recovery?

Met *disaster recovery* kun je gegevens uit AD terug proberen te krijgen.

12. Welke rol (service) moet er voor of tijdens het installeren van ADDS extra worden geïnstalleerd?

Deze rol wordt tijdens het promoveren van de server geconfigureerd als het op dezelfde server geïnstalleerd is: DNS

13. 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?

NTFS is noodzakelijk, ReFS kan niet worden gebruikt

14. Welke relatie is er tussen AD en DNS?

Zonder DNS geen mogelijkheid om met AD te communiceren. Naast A en PTR-records wordt er gebruik gemaakt van SRV-records om service te koppelen.

15. Wat is een Domain Functional Level (DFL) en welke DFLs zijn er?

DFL bepaalt de maximale functionaliteiten in een domein. DFL wordt bepaald door het 'oudste' OS in het netwerk. De DFL's die beschikbaar zijn: Windows Server 2008, 2008R2, 2012, 2012R2 en 2016. Een 2016 server moet minimaal een 2008 domein hebben om te kunnen toevoegen. Windows 2016 in combinatie met DFL 2000 of 2003 lukt niet.

16. Heeft een DFL invloed op een member server en/of een client?

Nee, alleen op de DC('s).

17. Wat wordt er verstaan onder een Forest Functional Level (FFL)?

FFL bepaalt de mogelijkheden van het forest. Je kunt het FFL niet hoger krijgen dan het laagste DFL.

18. Wat is sysvol?

Sysvol is een gedeelde folder voor het delen van informatie als, scripts, gpo's en eventuele andere informatie. AD en sysvol moeten beide op een NTFS-drive staan.

19. Wat is het DSRM?

DSRM staat voor Directory Services Restore Mode Password. In deze mode kan AD worden beheerd en/of worden teruggezet.

20. Welk protocol wordt door AD gebruikt om objecten op te slaan?

LDAP

2.3 Week 1, College 2: 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

Een aantal bekende voorbeelden waar de genoemde vijf waarschijnlijk tussen zullen zitten:

- Red Hat Enterprise Linux (RHEL): Red Hat-familie
- Fedora: Red Hat-familie
- CentOS: Red Hat-familie
- Oracle Linux: Red Hat-familie
- Debian: Debian-familie
- Ubuntu: Debian-familie
- Linux Mint: Debian familie
- Elementary OS: Debian-familie
- SUSE Linux Enterprise: SUSE-familie

- OpenSUSE: SUSE-familie
 - Slackware: geen van de drie families
 - Gentoo: geen van de drie families
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?**
Red Hat- en SUSE- families gebruiken het RPM formaat voor hun softwarepakketten, de Debian-familie gebruikt hiervoor het DEB formaat
3. **Waarin verschillen *enterprise* (zakelijk gerichte) distributies van overige distributies?**

Enterprise	Overig
Nadruk op stabiliteit en duurzaamheid	Nadruk op nieuwe functionaliteit en flexibiliteit
Supportcontract mogelijk	Enkel <i>community</i> support

4. **Welke services hebben we in het netwerk nodig als we willen installeren zonder gebruik te maken van een boot CD (image)?**
DHCP en TFTP (indien mogelijk gecombineerd in PXE)
5. **Wat zijn de voordelen van installaties met behulp van een geautomatiseerde *installer* (bijvoorbeeld Kickstart) ten opzichte van handmatige installaties?**
Installaties vereisen minder tijd van de beheerder, zijn reproduceerbaar en de installatieprofielen kunnen centraal beheerd worden.
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)?**
- Een installatie van een pakket is een enkele operatie die in zijn geheel kan worden teruggedraaid
 - De afhankelijkheden van een pakket zijn binnen het pakket vastgelegd, hiervoor hoeft dus geen externe bron geraadpleegd te worden
 - Een package bestand kan ook scripts bevatten die voorbereidingen aan het begin en/of *finetuning* ter afronding van de installatie kunnen verrichten
7. **Waarom bestaan er *high-level package management tools* als APT, YUM en ZYpp?**
- Om het vinden en downloaden van softwarepakketten te vergemakkelijken
 - Om het updaten of upgraden van systemen te automatiseren
 - Om het beheer van afhankelijkheden tussen softwarepakketten te faciliteren
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, pakket Y automatisch ook geïnstalleerd wordt (inclusief eventuele verdere *dependencies* die pakket Y zelf heeft)**
9. **Wat wordt in de context van Linux *package management* bedoeld met de term *repository*?**
Een centrale opslag (meestal in de vorm van een website) van softwarepakketten van waaruit *high-level package management tools* de benodigde bestanden kunnen downloaden ter installatie
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*”?**
- het eerste commando updatet of installeert een pakket dat reeds is gedownload op het systeem waar het geïnstalleerd wordt, het tweede commando haalt het pakket op uit een *repository*
 - het tweede commando updatet of installeert ook eventuele *dependencies*, het eerste doet dat niet; als er *dependencies* niet in de juiste versie op het systeem aanwezig zijn zal het eerste commando falen met de foutmelding “*error: Failed dependencies*” terwijl het tweede aanbiedt deze ook te downloaden en updaten danwel installeren
11. **Welke vijf beheerderstaken worden in de lesstof (hoofdstuk 6) genoemd als het gaat om software?**
- Automatiseren van bulkinstallaties;
 - Onderhouden OS-configuraties in een lokale omgeving;
 - Het up-to-date houden van systemen en applicaties;
 - Het bijhouden van softwarelicenties

- v. Het beheren van *add-on* softwarepakketten
12. **Benoem de stappen die noodzakelijk zijn bij installeren van Linux.**
- Booten van dvd/USB;
 - Beantwoorden van een aantal basisvragen;
 - Configureren de harde schijf en partities
 - Het aangeven van welke software moet worden geïnstalleerd.
13. **Wat is PXE?**
- De Preboot eXecution Environment (PXE). Dit is een standaard van Intel waarmee de computer vanaf de netwerkkaart kan starten. Met PXE is geen specifieke driver verplicht. In het proces wordt er een DHCP Discover gestuurd en omdat de PXE flag aan staat worden ook de PXE opties (BootServer en bootfile) meegegeven. Het bootbestand wordt van de TFTP-server afgehaald en gestart.
14. **Waar staat de afkorting YUM voor?**
- Yellowdog Updater, Modified
15. **Wat is de functie van een een `ks.cfg` bestand?**
- Een `ks.cfg` bestand kan helpen bij het installeren en configureren van een Red Hat gerelateerd Linux OS.
16. **In welke sectie van het `ks.cfg` bestand wordt aangegeven welke pakketten er geïnstalleerd moeten worden.**
- In de sectie `%packages`
17. **Wat is het verschil tussen `rpm` en `dpkg`?**
- De verschillen tussen beide zijn niet zo groot. Het belangrijkste van beide extensie is dat je `rpm`'s oorspronkelijk en hoofdzakelijk zal tegenkomen bij Red Hat (en afgeleiden daarvan) en dat bestanden met `dpkg` als extensie oorspronkelijk van Debian afkomstig zijn.
18. **Wat zijn de drie doelen van het gebruik van metapackage management systems als APT, YUM en Red Hat Network?**
- het simplificeren van de taak om pakketten te lokaliseren en te downloaden;
 - het automatiseren van het proces van updaten en/of upgraden;
 - het faciliteren van afhankelijkheden binnen de software
19. **Met welk commando en syntax kun je een Linux systeem up-to-date houden?**
- Op distributies uit de Red Hat familie met `sudo yum upgrade`, op distributies uit de Debian familie met `sudo apt-get upgrade` (en/of `update`).
20. **Welke optie kun je gebruiken om bij `apt-get upgrade` direct de software te installeren?**
- De optie `-yes`

2.4 Week 2, College 1: Windows Core

1. Wat zijn de voordelen van de Core Editie?

Installation Requirements for Windows Server 2012



Wat is Server Core?

Server Core is een "minimale" installatie optie van Windows Server 2008 of later

Server Core heeft de volgende voordelen:

- Reduces software maintenance
- Reduces attack surface
- Reduces the require disk space and the number of restarts

Component	Requirements
Processor	<ul style="list-style-type: none"> Minimum 1.4 GHz 64-bit processor
Memory	<ul style="list-style-type: none"> Minimum 512 MB RAM (Core) Maximum Depends, 4TB for standard or datacenter editions. 32 GB for foundation, 64 GB for essentials.
Available Disk Space	<ul style="list-style-type: none"> Minimum 32 GB
Optical Drive	<ul style="list-style-type: none"> DVD-ROM
Display and Peripherals	<ul style="list-style-type: none"> Super VGA (800 x 600) or higher-resolution monitor Keyboard Microsoft mouse or compatible pointing device

2. Wat zijn de nadelen van de Core Editie

Geen GUI (hoewel sommige dit misschien ook wel als voordeel zien). Niet alle roles en services kunnen worden gebruikt.

3. Welke Server Roles kunnen op de Core editie worden geïnstalleerd?

The Server Core installation option includes the following server roles.

- Active Directory Certificate Services
- Active Directory Domain Services
- Active Directory Federation Services
- Active Directory Lightweight Directory Services
- Active Directory Rights Management Services
- Device Health Attestation
- DHCP Server
- DNS Server
- File and Storage Services
- Host Guardian Service
- Hyper-V
- Print and Document Services
- Remote Access
- Remote Desktop Services
- Volume Activation Services
- Web Server IIS
- Windows Server Essentials Experience
- Windows Server Update Services

4. Kan een Core machine een Read Only Domain Controller(RODC) role krijgen?

Ja

5. Met behulp van welk script kun je een Windows Core machine activeren?

start /w slmgr.vbs -ato

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?

netsh.exe is een hulpprogramma dat beheerders kunnen gebruiken voor het configureren en controleren van Windows-computers vanaf een opdrachtprompt.

7. Wat is de netsh syntax om de IP-instellingen op te vragen?

Voor IPv4: netsh interface ipv4 show ipaddress

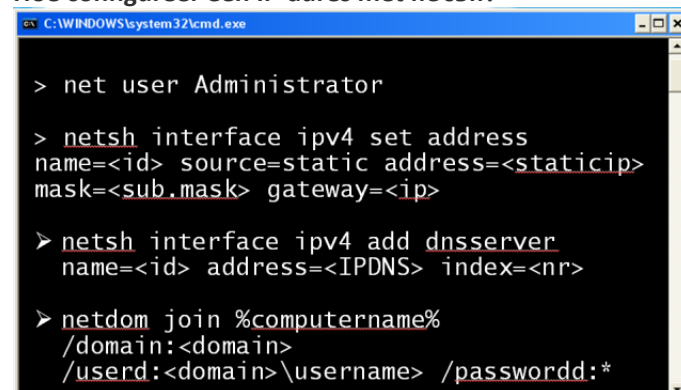
Voor IPv6: netsh interface ipv6 show address

Hiermee wordt informatie weergegeven voor een bepaald IP-adres. Bij gebruik van show ipaddress zonder parameters wordt de informatie voor alle IP-adressen op alle interfaces eenmaal weergegeven

Syntaxis

show ipaddress [[index=]IP-adres] [[rr=]Vernieuwingsfrequentie]

8. Hoe configureer een IP-adres met netsh?



```
C:\WINDOWS\system32\cmd.exe

> net user Administrator

> netsh interface ipv4 set address
name=<id> source=static address=<staticip>
mask=<sub.mask> gateway=<ip>

> netsh interface ipv4 add dnsserver
name=<id> address=<IPDNS> index=<nr>

> netdom join %computername%
/domain:<domain>
/user:<domain>\username /passwordd:*
```

9. Bij het opgeven van een DNS-server via netsh kom je optie index tegen. Wat is hiervan de functie?

[index=]DNS-index

De positie van de toegevoegde DNS-server in de list met DNS-servers voor de interface. Hoe lager het nummer bij de parameter DNS-index, hoe hoger de voorkeur. Als er geen index is opgegeven, wordt de server toegevoegd met het laagste voorkeursniveau.

10. Welk commando kun je gebruiken om een core machine te herstarten?

shutdown -r -t 0 (of met PowerShell: Restart-Computer)

11. Wat is de syntax voor het aanmelden van de core machine bij het domein?

Zie vraag 8 (of met PowerShell: Add-Computer)

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?

Het controleren van de activatie EN een nieuwe evaluatie periode verkrijgen.

SLMgr Usage

Syntax

```
s1mgr.vbs [MachineName [User Password]] [<Option>]
    * MachineName: Name of remote machine (default is local machine)
    * User: Account with required privilege on remote machine
    * Password: password for the previous account
```

Global Options

```
-ipk <product key>
    Install product key (replaces existing key)
-upk
    Uninstall product key
-ato
    Activate Windows
-dli [Activation ID | All]
    Display license information (default: current license)
-dlv [Activation ID | All]
    Display detailed license information (default: current license)
-xpr
    Expiration date for current license state
```

Advanced Options

```
-cpky
    Clear product key from the registry (prevents disclosure attacks)
-ilc <License file>
    Install license
-reatm
    Reset the licensing status of the machine
-atp <Confirmation ID>
    Activate product with user-provided Confirmation ID
```

KMS Options

```
-skms <KMS activation server name>
    Set KMS server name

-skms <KMS activation server port number>
    Set KMS server port number
-skms <KMS activation server name:port number>
    Set KMS server name and port number in single command
-ckms
    Clear KMS server name and port number to default
```

13. Wat is de functie van sconfig.cmd?

Server Configuration tool (sconfig.cmd) is er voor het configureren en managen van verschillende veel voorkomende aspecten binnen de Server Core installatie.

14. In welke directory staat de tool (sysprep) om de Security ID's (SID) te vernieuwen?

sysprep.exe bevindt zich in C:\Windows\System32\sysprep

Vink generalize aan. Bij de volgende sysprep boot zal deze opnieuw de SID's genereren.

15. Welke opties heeft sysprep?

```
sysprep.exe [/oobe|/audit] [/generalize] [/reboot|/shutdown|/quit] [/quiet]
[/unattend:answerfile]
```

16. Wat is de functie van de tool mountvol?

Creëert, verwijdert, of laat een lijst zien van volume Mount point(s). Mountvol is een manier om volumes te linken zonder drive letter.

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?

Het getal is een GUID (*Globally Unique Identifier*). Dit is een uniek nummer welke gebruikt wordt om ervoor te zorgen dat bepaalde componenten, applicaties, files, database entry's en/of gebruikers herkent kunnen worden.

18. Wat doet de parameter /d bij mountvol?

Verwijder het volume Mount point van een specifieke folder.

19. Wat is het PowerShell commando waarmee je de AD-Domain-Services kunt installeren op de Core server?

```
Install-WindowsFeature AD-Domain-Services -IncludeManagementTools
```

2.5 Week 2, College 2: De Linux Shell

1. Op welke manier verschillen de commando's

```
ls -l /etc
```

en

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

met elkaar?

Het eerste commando laat de output van ls (een directory listing) op *standard output* zien, het tweede commando schrijft diezelfde directory listing naar het bestand /tmp/lijstje.

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
```

Slechts indien het bestand /etc/shadow bestaat en leesbaar is, wordt de tekst "Ingelogd als root of je shadow password file staat te open" getoond.

3. Wat is het verschil tussen SIGINT en SIGTERM enerzijds en SIGKILL anderzijds?

SIGINT en SIGTERM worden afgehandeld door het programma waarvoor het signaal bedoeld is, SIGKILL wordt door de kernel afgehandeld. Daardoor heeft bij gebruik van SIGKILL het programma niet de kans zijn afsluitroutine uit te voeren.

4. Leg uit wat er "nice" is aan een programma waarvan met het nice commando de prioriteit is verlaagd

Het programma is vriendelijker, dus "nicer", voor andere programma's doordat het verlagen van de prioriteit ervoor zorgt dat het minder CPU resources verbruikt die daardoor voor andere programma's met een hogere prioriteit beschikbaar zijn.

5. Wat is het doel van het werken met scripts?

Scripts standaardiseren en automatiseren de werking en uitvoering van administratieve taken om op die manier extra tijd vrij te maken om andere taken te kunnen uitvoeren

6. Noem drie Linux Shell-versies.

Drie uit het volgende rijtje: Bash, Bourne shell (sh), Korn Shell (ksh), C Shell (csh), Z Shell (zsh), tcsh

7. Welke programmeertalen worden in het boek genoemd om te gebruiken als het gaat om complexere scripts (meer dan 100 regels)?

Perl en Python

8. Wat zijn de nadelen van de bij vraag 7 genoemde talen?

Het nadeel van deze talen is dat het lastiger is om een 'werkomgeving' op te zetten omdat er mogelijk meerdere *libraries* nodig zijn met *compiled components*.

9. Welke toetscombinaties kun je in een tekst-editor als Emacs gebruiken om naar het begin of eind van een tekstregel te springen?

Uit de paragraaf "Command editing" op blz. 109 van het boek:

- control-e naar het einde van de regel
- control-a naar het einde van de regel

- control-p stapsgewijs terug door de eerdere commando's
 - control-r incrementeel zoeken door de eerdere commando's
- 10. Processen onder Linux hebben drie communicatiekanalen. Welke drie zijn dat?**
standaard input (STDIN), Standaard output (STDOUT) en standaard error (STDERR).
- 11. Geef een korte beschrijving van STDIN, STDOUT en STDERR.**
STDIN 'leest' van het toetsenbord en STDOUT en STDERR schrijven de output naar het beeldscherm. STDOUT is in principe voor 'gewone' output, STDERR voor (fout)meldingen.
- 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?**
- < lezen van bestand
 - > stdout naar bestand schrijven
 - >> stdout aan bestaand bestand toevoegen
 - 2> stdout naar bestand schrijven
 - >& stdout en stderr naar bestand schrijven
 - | stdout doorsturen naar stdin van ander commando
- 13. Welk commando kun je gebruiken om in bijvoorbeeld /var/messages te zoeken naar specifieke foutmeldingen?**
grep of de zoekfunctie van more of less (/) of een tekst editor.
- 14. Op welke manier worden in de shell variabele gedefinieerd en aangeroepen?**
Variabelen worden bij het 'toekennen' niet met een speciaal teken gedefinieerd. Bij het aanroepen wordt het dollarteken (\$) aangeroepen
- 15. In de Shell zijn variabelen niet hoofdletter gevoelig? (Eens/oneens)**
Oneens, variabelen zijn wel hoofdletter gevoelig.
- 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?**
wc voor het tellen van woorden (staat ook voor *word count*)
grep voor het printen van regels die met een patroon overeenkomen
- 17. Hoe kun je aan een script aflezen dat het om een Bash-script gaat?**
#!/bin/bash
- 18. Welk commando heb je nodig om de permissies van een bestand (lees: een script) aan te passen zodat deze kan worden uitgevoerd?**
chmod (bijvoorbeeld "chmod +x" om het voor iedereen uitvoerbaar te maken, al moet een script ook leesbaar zijn voor degene die het wil uitvoeren)
- 19. Wat is kenmerkend voor variabelen in Bash?**
Alle variabelen zijn strings. Er is geen verschil tussen het getal 1 en een tekstuele 1.
- 20. Welke richtlijnen voor scripts worden in het boek genoemd?**
Zie blz. 187/188:
- bij niet gebruikelijke argumenten moet het script stoppen en een bericht weergeven. Het toevoegen van --help is aanbevolen;
 - controleer goed dat het script doet wat het moet doen voor elke input, denk aan de gevolgen van rm -rf met de verkeerde argumenten;
 - geef een goede exit code op: 0 voor succes, elk ander getal bij een fout;
 - gebruik 'goede' namen voor variabelen, scripts en routines;
 - zorg dat de variabele naam verwijst naar de waarde/inhoud van de variabele maar hou het kort;
 - ontwikkel een *style guide* zodat collega's het kunnen begrijpen;
 - start elk script met een regel commentaar welke duidelijk maakt wat het script doet, inclusief je naam, datum en eventueel de tools en libraries of modules die noodzakelijk zijn;
 - geef logische uitleg per 'regel', block of functie;
 - starten van een script als root is 'geen' probleem, maar wees voorzichtig met het gebruik van setuid;
 - gebruik bij Bash de optie -x voor printen van commando's en de optie -n om de syntax te controleren zonder dat de regels daadwerkelijk worden uitgevoerd.

21. Welke componenten behoren bij een (Linux/ Unix) proces?

Een proces bevat een *address space* en een set *data structures* naar de kernel toe. De geheugenruimte wordt voor het proces gereserveerd. Het bevat de code, proces variables, de stack, extra info en de libraries welke door het proces worden uitgevoerd. Linux en Unix hebben geen directe koppeling tussen het virtuele geheugen en het fysieke of swap geheugen.

22. Wat is een Proces ID (PID)?

Elk process krijgt een uniek nummer, dit is het PID. Met deze waarde is te bepalen om welk proces het gaat en welke systeembronnen daaraan toegekend (mogen) worden. Commando's en system calls vragen vaak om de PID van het proces. De PID-waardes worden vaak in volgorde uitgegeven.

23. Welke twee gebruikers en groeps ID's zijn er in Linux?

UID en EUID (User ID en Effective User ID); GID en EGID (Group ID en Effective GID)

24. Op welke manier bepaalt de kernel hoeveel CPU-tijd een proces bijvoorbeeld krijgt?

De kernel gebruikt een dynamisch algoritme om de prioriteit te bepalen op basis van gebruikte tijd en de tijd die het proces heeft moeten wachten.

25. Hoe wordt de administratieve waarde genoemd die mede kan bepalen hoeveel CPU-tijd een proces krijgt?

Nice-value of niceness.

26. Wat is de functie van init binnen Linux?

Init is verantwoordelijk voor uitvoeren van de system startup scripts. Alle processen anders dan die door de kernel worden gecreëerd 'stammen af' van init. Init speelt een belangrijke rol in proces-management.

27. Wat zijn onder Linux belangrijke signalen?

Zie tabel 4.1 in *UNIX and Linux System Administration Handbook, 5th Edition*:

# ^b	Name	Description	Default	Can catch?	Can block?	Dump core?
1	HUP	Hangup	Terminate	Yes	Yes	No
2	INT	Interrupt	Terminate	Yes	Yes	No
3	QUIT	Quit	Terminate	Yes	Yes	Yes
9	KILL	Kill	Terminate	No	No	No
10	BUS	Bus error	Terminate	Yes	Yes	Yes
11	SEGV	Segmentation fault	Terminate	Yes	Yes	Yes
15	TERM	Software termination	Terminate	Yes	Yes	No
17	STOP	Stop	Stop	No	No	No
18	TSTP	Keyboard stop	Stop	Yes	Yes	No
19	CONT	Continue after stop	Ignore	Yes	No	No
28	WINCH	Window changed	Ignore	Yes	Yes	No
30	USR1	User-defined #1	Terminate	Yes	Yes	No
31	USR2	User-defined #2	Terminate	Yes	Yes	No

a. A list of signal names and numbers is also available from the **bash** built-in command **kill -l**.

b. May vary on some systems. See `/usr/include/signal.h` or **man signal** for more information.

28. Welke twee signalen kunnen niet worden geblokkeerd of worden gestopt?

STOP en KILL

29. Welke command/syntax moet je gebruiken om een proces, zoals dat van de Apache Webserver, te stoppen?

`sudo killall httpd`

30. Welke vier process states kent Linux?

In *UNIX and Linux System Administration Handbook, 4th Edition* werd dit compact samengevat in tabel 5.2:

Table 5.2 Process states

State	Meaning
Runnable	The process can be executed.
Sleeping	The process is waiting for some resource.
Zombie	The process is trying to die.
Stopped	The process is suspended (not allowed to execute).

31. Kan een administrator (de root) een proces dat met een STOP of een TSTP gestopt is, het proces administratief weer starten (Ja, dat kan / Nee, dat kan niet)

Nee dat kan in principe niet, zeker niet met behoud van o.a. PID.

32. Een hoge *nice* waarde betekent dat de kernel het proces een hoge prioriteit toekent. (Juist/ Onjuist)

Nee, dat is onjuist. Een hoge *nice* waarde betekent dat het proces een lage prioriteit krijgt (erg aardig (=nice) is tegenover andere processen).

33. Welk commando kun je gebruiken om te zien welke processen op een systeem draaien?

ps (vb: ps -ef of ps aux)

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!)
top

35. Uit welke directory halen de toosl ps en top hun informatie?

/proc

36. Welk commando kun je gebruiken om te achterhalen wat een proces doet?

strace

2.6 Week 3, College 1: Windows Gebruikers en Groepen

1. Microsoft Windows kent drie verschillende soorten gebruikersaccounts, Welke drie zijn dat?

Tools for Configuring User Accounts

Local and Domain accounts each have their own tools for creating and managing properties:

Account	Tools
Local computer account	Control Panel\User Accounts\User Accounts
Domain account	<ul style="list-style-type: none"> Windows Server GUI tool: Active Directory Users and Computers, ADAC Command-line utilities: dsadd, Windows Powershell™, CSVDE, LDIFDE

en Builtin accounts

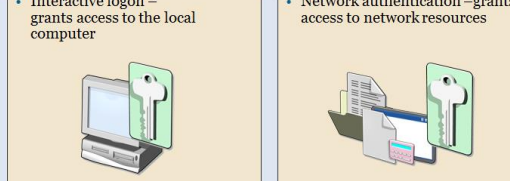
2. Om toegang te krijgen tot een domein en om binnen het domein taken te kunnen uitvoeren wordt er gesproken over *authentication* en *authorization*. Wat is het verschil tussen beide?

What is Authentication?

Authentication is the process of verifying a user's identity on a network

Authentication includes two components:

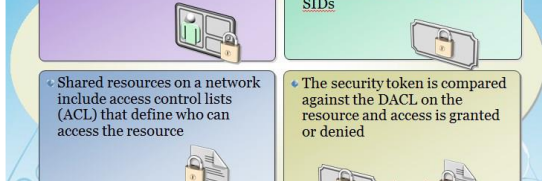
- Interactive logon – grants access to the local computer
- Network authentication – grants access to network resources



What is Authorization?

Authorization is a process of verifying that an authenticated user has permission to perform an action

- Security principals are issued security identifiers (SIDs) when the account is created
- User accounts are issued security tokens during authentication that include the user's SID and all related group SIDs
- Shared resources on a network include access control lists (ACL) that define who can access the resource
- The security token is compared against the DACL on the resource and access is granted or denied



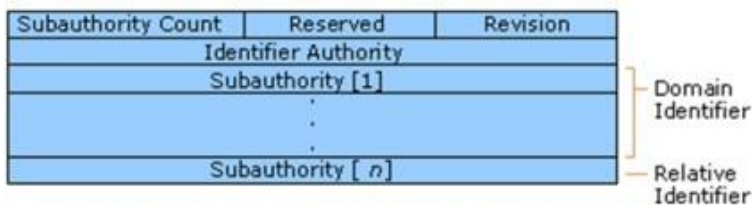
3. Een gebruikersaccount in een Windows domeinomgeving kent meerdere namen. Beschrijf de kenmerken / verschillen tussen de onderstaande namen:

Naming options for domain user accounts:

Object Names	Example	Uniqueness requirement
User logon name	Gregory	Must be unique within domain
User logon name (pre-Microsoft® Windows® 2000)	Woodgrove\Gregory	Must be unique within domain
User principal name (UPN)	Gregory@WoodgroveBank.com	Must be unique within forest
LDAP distinguished name	CN=Gregory,OU=IT,DC=WoodgroveBank,DC=com	Will be globally unique, combining RDN, container name, and domain names
Relative distinguished name (RDN)	CN=Gregory	Must be unique in OU

- 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.
Een naam in de vorm van een e-mail adres, bv jan.jansen@hu.nl
 - Wat is het verschil tussen een DN en een RDN?
Een distinguished name is een unieke string die de intentificatie van een entry in de active directory representeert. Een RDN is een onderdeel van een DN. Bijvoorbeeld "CN=anna"
- In welke situatie kom je een UPN en een DN tegen?
In een netwerk omgeving met Microsoft server omgeving met de rol AD DS / DNS onder andere bij het gebruik van dsadd, dsmod, csvde....
- 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?

SID Structure



The individual values of a SID are described in the table below.

S-R-X-Y1-Y2-Yn-1-Yn

S-1-5-32-544

Component	Definition
S	Indicates that the string is a SID
R	Revision level
X	Identifier authority value
Y	A series of <u>subauthority</u> values, where <i>n</i> is the number of values

This SID has four components:

- A revision level (1)
- An identifier authority value (5, NT Authority)
- A domain identifier (32, Builtin)
- A relative identifier (544, Administrators)

- Welke aanpassingen kun je via ADUC bij het aanmaken van het account nog meer maken?
ADUC staat voor de snap-in Active Directory Users and Computers. Hiermee kunnen alle gebruikers worden aangepast.

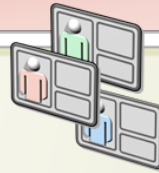
8. Wat als je voor een grote groep gebruikers veel meer gegevens dan alleen een naam en een wachtwoord wilt invullen en je wilt dat toch via Active Directory Users and Computers doen? Dan biedt een zogenaamde *template user* mogelijk een oplossing. Wat is een template user?

A user account template is an account with common properties already configured

User accounts templates take advantage of similarity between user accounts

To use user templates:

- Create several typical users reflecting various groups within your organization
- Copy the user account most like the new account you want to create
- Modify the attributes: names, e-mail address, logon name, etc.



9. Welke gegevens van een template user worden gekopieerd en welke niet?
Niet gebruikersspecifiek gegevens worden gekopieerd, gebruikersspecifieke gegevens niet.
10. Wat is een DN?
Distinguished Name
11. Wat is een CN?
Common Name
12. Wat is een DC?
Domain Component
13. Wat is een sAMAccountName?
Oudere NT 4.0 login naam, deze moet uniek zijn in het domein.
Voorbeeld: als de CN Guy Thomas is kan de sAMAccountName guyt zijn.
14. Wat is csvde?

Csvde is a command-line tool that is built into Server 200x

- Imports and exports data from Active Directory Domain Services using files that store data in the comma-separated value (CSV) format
- Csvde command must be run from an elevated command prompt
- Csvde -i -v -k -F users.csv
- Cannot import user passwords (encrypted channel)
- No editing or deleting existing objects

15. Welke syntax is er minimaal nodig om een CSV file te importeren?
csvde -i -f
-i: import, -v: verbose, -F: file, -k: show but skip errors
16. Kan je met dsadd ook het tabblad Address volledig invullen?
Nee.
17. Kan je dit (vraag 16) met een andere command line tool wel voor elkaar krijgen?
Ja, met PowerShell
18. Welke syntax moet je bij dsquery gebruiken om te achterhalen welke gebruikers een BHI2 description hebben?
dsquery user -desc BHI2

Finds users in the directory who match the search criteria that you specify

-name <Name>	Searches for users whose name attributes match <Name>. For example, "john", "smith", or "j*th".
-desc <Description>	Searches for users whose description attributes match <Description>. For example, "john", "smith", or "j*th".
-upn <UPN>	Searches for users whose UPN attribute matches <UPN>.
-samid <SAMName>	Searches for users whose SAM account name matches <SAMName>.
-inactive	Searches for users who have been inactive (stale) for at least the number of weeks that you specify.

```

dsquery user -desc medewerker | dsmod user -title Docent -webpg www.school.
dsquery user -desc BHI2 | dsmod user -mgr "cn=Doorman Karel,OU=leerlingen,D
dsquery user -desc BHI3 | dsmod user -mgr "cn=Buren Anna,OU=leerlingen,DC=s

```

{-s <Server> -d <Domain>}	Connects a computer to a remote server or domain that you specify. By default, dsquery connects to the local domain.
-u <UserName>	Specifies the user name with which the user logs on to a remote server. By default, -u uses the format to specify a user name: <ul style="list-style-type: none"> user name (for example, Linda) domain/user name (for example, widgets\Linda) UPN (for example, Linda@widgets.contoso.com)
-p (<Password> *)	Specifies to use either a password or an asterisk (*) to log on to a remote server. If you type an asterisk, the password is not displayed.
-q	Suppresses all output to standard output (quiet mode).
-r	Specifies that the search use recursion or follow referrals. By default, the search does not follow referrals.
-gc	Specifies that the search use the Active Directory global catalog.

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?

-limit 0

20. Van hoeveel gebruikers in het domein begint hun voornaam met een C?

dsquery user -name C* (antwoord afhankelijk van gebruikers)

21. Met welke syntax kun je zien welke gebruikersaccounts uitgeschakeld zijn?

-disabled -limit 0

22. Wat is een OU?

An organizational unit (OU):

- Is a directory object within the domain
- Is the smallest scope or unit to which you can assign Group Policy settings or delegate administrative authority
- Can contain users, computers, groups, printers, and other OUs

OUs are used to:

- Delegate authority (create users, reset passwords)
- Create containers within the domain model to represent logical structures
- Create administrative boundaries within the domain
- Enforce Group Policy

23. Welke functies heeft een OU?

Zie vraag 22

24. Wat is een *nested OU*?

Dat is een OU binnen een OU

25. Kan een OU in het domein `bmc.local` gebruikers bevatten vanuit het domein `HA1.bmc.local`?

Dat ligt aan lidmaatschap van een (Universal) Group en of de trusts dienovereenkomstig ingesteld zijn

26. Welke OU's zijn op een nieuw gepromoveerde domain controller standaard aanwezig?

Alleen de OU Domain controllers, de andere zijn container objecten maar zijn geen OUs. OU is te herken aan een map met een tekening erop. Een niet OU heeft de tekening niet!

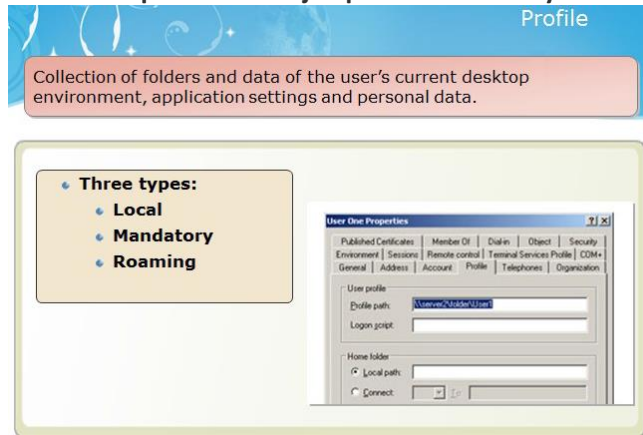
27. Welke share en security settings zijn er automatisch gemaakt op de nieuwe shares?

Share is standaard *read* voor *everyone*

28. Wat is een UNC?

Universal Naming Convention. `\\servernaam\share\share\...` . Benaderen share, maken van drive

29. Welke drie profielen kun je op een Windows systeem tegenkomen?



30. Wat is het verschil tussen deze drie profielen?

- *Local*: alleen lokaal aanwezig en bruikbaar
- *Mandatory*: Aanpassingen worden niet opgeslagen. Profiel is op meerdere computers te gebruiken
- *Roaming*: Aanpassingen worden opgeslagen. Profiel is op meerdere computers te gebruiken

2.7 Week 3, College 2: Linux Gebruikers en Groepen

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

Een uniek ID waarmee het systeem gebruikersaccounts identificeert. De loginnaam is er vooral voor het gemak van menselijke gebruikers

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

Een uniek ID waarmee het systeem gebruikersgroepen identificeert, vergelijkbaar met een UID voor groepen. De groepnaam is er vooral voor het gemak van menselijke gebruikers

3. Als twee loginnamen met eigen passwords zijn gekoppeld aan hetzelfde user id, bieden zij dan toegang tot hetzelfde account?

Ja, de *username* na inloggen is dan de username die voor dat user id het eerst voorkomt in de password file, ongeacht welke loginnaam is gebruikt

4. Wat is de functie van de *shadow password file*?

Opslag van password *hashes* in een bestand dat niet door normale gebruikers gelezen kan worden

5. Kunnen gebruikers aangemaakt worden zonder gebruik van *useradd* of *adduser* tool?

Ja, dit kan, het is alleen meer werk: *passwd*, *shadow* en *group* bestanden moeten handmatig worden aangepast en *homedirectory* en *mail* bestand moeten handmatig worden aangemaakt.

6. Welke vier algemene regels zijn er opgesteld rondom de traditionele manier van Access Control onder Linux?

- Objecten hebben eigenaars en de eigenaar heeft meer controle over dat object,
- je bent eigenaar van de objecten die je creëert,
- root kan eigenaar worden van elk object en
- root kan gevoelige administratieve functies uitvoeren.

7. Mag een 'gewone' gebruiker onder Linux de systeemtijd en de datum aanpassen?

Nee dat alleen worden gedaan door een gebruiker met root-rechten.

8. Met welke tool kun je vanaf de commandline opvragen wie de eigenaar is van een specifiek bestand?

`ls -l`.

9. Welke *identities* kan een proces hebben?

Real, *effective* en *saved*.

10. Welk UID heeft het root account?

De waarde 0.

11. Wat zijn voorbeelden van moderne access control methodes onder Linux?

- Role-Based Access Control (RBAC)
- SELinux (SE = Security Enhanced)

- c. POSIX
- d. PAM: Pluggable Authentication Modules
- e. Kerberos
- f. Access Control Lists (o.a. NFSv4)

12. Waaraan moet een rootwachtwoord voldoen?

Het wachtwoord van root moet complex en veilig zijn. De lengte (min 8 karakters) is daarbij vaak een belangrijke factor. Op systemen met een DES-password is meer dan 8 karakters niet zinvol omdat alleen de eerste 8 gebruikt worden. MD5 en SHA-512 encryptie voor wachtwoorden geeft een hogere mate van veiligheid, de wachtwoorden kunnen ook langer worden. Een wachtwoord bestaat uit een aantal letters, punctuations (leestekens) en cijfers.

13. Met welk commando kun je, bijvoorbeeld in een shell, van gebruiker wisselen?

su.

14. Een gebruiker die gebruik mag maken van het sudo commando moet lid zijn van welke groep?

De groep wheel.

15. Hoeveel UID mogelijkheden zijn er?

65536 (2^{16})

16. Met welke tools kun je gebruikers aanmaken, wijzigen of verwijderen?

useradd, userdel en usermod. Daarnaast is er newusers die meerdere gebruikers tegelijk kan aanmaken maar zijn beperkingen heeft.

17. Welke modernere vormen van gebruikerbeheer doen de laatste jaren hun intrede in de Linux wereld?

NIS en LDAP.

18. Een gebruikersnaam onder Linux moet op twee punten uniek zijn. Welke twee zijn dat?

Een username moet op twee punten uniek zijn: 1) username moet op elk systeem hetzelfde zijn 2) een specifieke naam moet altijd naar de zelfde gebruiker verwijzen.

19. Welke drie encryptiemethodes worden veelvuldig op Linux Systemen gebruikt als het gaat om het versleutelen van de wachtwoorden in /etc/passwd?

DES, MD5 (beide verouderd en niet meer veilig) en SHA-512 (tegenwoordig de default).

20. Wat is een belangrijk nadeel van een MD5 hash?

Uit de MD5 hashes kunnen 'eenvoudig' met een bruteforce-attack de wachtwoorden worden achterhaald.

21. Welk GID heeft de groep van root?

De waarde 0.

22. Wat is de functie van een GECOS field?

Wordt soms gebruikt om persoonlijke informatie van een gebruiker op te slaan.

23. Welke gebruiker(s) mag de bestanden /etc/shadow en/of /etc/security standaard lezen?

root, standaard als enige

24. In welk bestand kun je zien van welke groepen een gebruiker lid is?

/etc/group

25. Wat zijn de standaard startup files onder Linux?

Zie tabel 8.2 in *UNIX and Linux System Administration Handbook, 5th Edition*:

Target	Filename	Typical uses
<i>all shells</i>	.login_conf	Sets user-specific login defaults (FreeBSD)
sh	.profile	Sets search path, terminal type, and environment
bash^a	.bashrc	Sets the terminal type (if needed) Sets biff and mesg switches
	.bash_profile	Sets up environment variables Sets command aliases Sets the search path Sets the umask value to control permissions Sets CDPATH for filename searches Sets the PS1 (prompt) and HISTCONTROL variables
	.login	Read by "login" instances of csh
	.cshrc	Read by all instances of csh
vi/vim	.vimrc/.viminfo	Sets vi/vim editor options
emacs	.emacs	Sets emacs editor options and key bindings
git	.gitconfig	Sets user, editor, color, and alias options for Git
GNOME	.gconf	GNOME user configuration via gconf
	.gconfpath	Path for additional user configuration via gconf
KDE	.kde/	Directory of configuration files

a. **bash** also reads **.profile** or **/etc/profile** in emulation of **sh**. The **.bash_profile** file is read by login shells, and the **.bashrc** file is read by interactive, non-login shells.

26. Wat is LDAP?

LDAP biedt een hiërarchisch client-server model welke op meerder servers kan worden gebruikt. Belangrijkste voordeel is de centrale opslag van gebruikersgegevens. Microsofts AD gebruikt LDAP en Kerberos.

27. Met welke tool kun je onder Linux de maximale tijd instellen voordat een gebruiker zijn wachtwoord moet aanpassen?

chage.

2.8 Week 4, College 1: Windows bestandssystemen

1. Welke standaard permissies kunnen er op een bestand worden ingesteld?

- Samenvoeging detail permissies
- Full Control
- Modify
- Read & Execute
- Read
- Write
- List Folder Contents

2. Op welk punt verschillen de permissies op een folder met die van een bestand?

Zie vraag 1, de optie "List Folder Contents"

3. Welk verschil is er tussen standaard en geavanceerde permissies?

- Advanced
 - Detail permissies
- Standaard “Read”



Figure 2: Advanced permissions for an OU in Active Directory

List Folder/Read Data
Read Attributes
Read Extended Attributes
Read Permissions

Standaard permissies zijn opgebouwd uit advanced permissions, zie illustratie voor Read.

4. Uit welke geavanceerde permissies is de standaard permissie “read” opgebouwd?
Zie vraag 3
5. Op welke twee manieren kan een bestand of een folder te maken krijgen met permissies?

- Inherited
- Explicit
- Cumulatief
- Effective Permissions
- Share permissions
 - Default Read

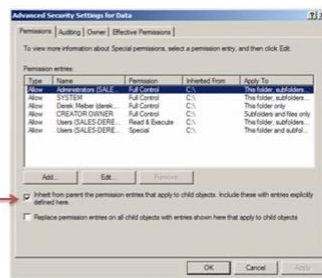


Figure 3: You can control inherited permissions on any folder or file

6. Op welke manier kan je het erven (inheritance) worden tegengegaan?
Zie rode pijl in illustratie bij antwoord op vraag 5
7. Wat heeft in het geval van een conflict voorrang. Een implicit deny of een explicit allow?
Kort door de bocht is dat een explicit allow, maar voor specifiek antwoord:

<http://technet.microsoft.com/en-us/magazine/2005.11.howitworksntfs.aspx>

- Allow
- Deny
- Deny heeft “default” voorrang op allow! (maar....)
 - Explicit deny
 - Explicit allow
 - Inherited deny
 - Inherited allow

DAACL	Permissions
Child Deny	N/A
Child Allow	N/A
Parent Deny	N/A
Parent Allow	Modify
Grandparent Deny	Write
Grandparent Allow	Read & Execute, List Folder Contents, Read

(How it works 1 / 2 best practice!!)

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?
Share permissie Read is de beperkende factor, dus alleen read.

9. Wat is een DACL?

NTFS uses Discretionary Access Control Lists (DACLs) to detail permissions to files and folders. A DACL is a list of zero or more access control entries (ACEs) which are ordered in a specific way. The example I've created includes a grandparent folder, a parent folder, and a child file. The DACL will start with the permissions for the child file. Any Deny permissions for the child will be listed first, followed by any Allow permissions for the child. Next, the DACL will show the entries for the parent folder, again with the Denies listed before the Allows

10. Wat wordt er verstaan onder een Access Control Entry?

Each permission that an object's owner grants to a particular user or group is stored as an access control entry (ACE) in a DACL that is part of the object's security descriptor. In the user interface, ACEs are displayed as Permission Entries.

11. Wat is een SID?

Security Identifiers (SID)

- 48 bit ID (281.474.976.710.656)
- Identificeert een object met uniek nummer
- Local Security Authority (LSA) genereert local SID
- SID moet in domein uniek zijn
- RID master deelt blokken SID's uit om deze uniek te houden

SID structure

SID Structure

Subauthority Count	Reserved	Revision
Identifier Authority		
Subauthority [1]		
.		
Subauthority (n)		

The individual values of a SID are described in the table below.

S-B-X-Y1-Y2-Yn-1-Yn

S-1-5-32-544

Component	Definition
S	Indicates that the string is a SID
R	Revision level
X	Identifier authority value
Y	A series of subauthority values, where n is the number of values

This SID has four components:

- A revision level (1)
- An identifier authority value (5, NT Authority)
- A domain identifier (32, Built-in)
- A relative identifier (544, Administrators)

SID Structure & GUID

The SID for Contoso\Domain Admins has:

- A revision level (1)
- An identifier authority (5, NT Authority)
- A domain identifier (21-1004336348-1177238915-682003330, Contoso)
- A relative identifier (512, Domain Admins)

- GUID = Global unique ID

- 128 bit

- Opgenomen in GC

- SIDHistory

- SID: S-1-5-11
Name: Authenticated Users
Description: A group that includes all users whose identities were authenticated when they logged on. Membership is controlled by the operating system.
- SID: S-1-5-12
Name: Restricted Code
Description: This SID is reserved for future use.
- SID: S-1-5-13
Name: Terminal Server Users
Description: A group that includes all users that have logged on to a Terminal Services server. Membership is controlled by the operating system.
- SID: S-1-5-14
Name: Remote Interactive Logon
Description: A group that includes all users who have logged on through a terminal services logon.

12. Wordt er bij het weergeven van de effectieve permissie rekening gehouden met de share permissies?

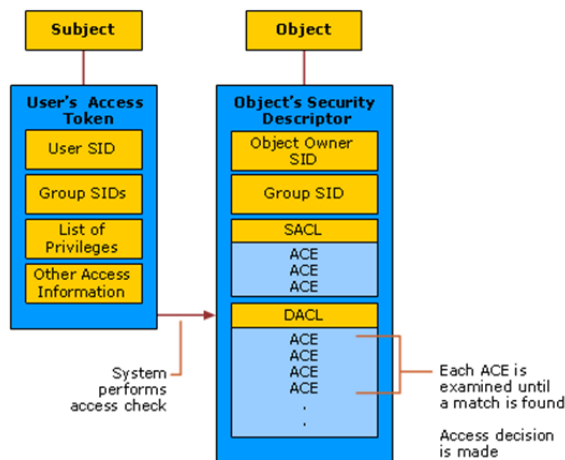
Bij het "berekenen" van de effectieve permissies wordt niet gekeken naar de share permissies.

13. Wat is de functie van een UNC?

Universal Naming Convention. \\servernaam\share\share\.... Benaderen share, maken van drive-mappings

14. Uit welke delen is een Access token van een gebruiker opemaakt?

ACL & ACE



15. Wat is een SACL?

The SACL on the object is still the ultimate authority in determining whether an access check must be audited or not. The SACL is the part of an object's security descriptor that specifies which operations are to be audited for a security principal.

The content of the SACL is controlled by security administrators for the local system. Security administrators are users who have been assigned the Manage Auditing and Security Log (SeSecurityPrivilege) privilege. By default, this privilege is assigned to the built-in Administrators group.

16. Uit welke onderdelen is een SID opgebouwd?

Zie het antwoord op vraag 11

17. Welk nieuw filesystem is met de komst van Windows Server 2012 toegevoegd?

ReFS

18. Wat is een beperking van dit nieuwe filesystem?

Je kan niet booten vanaf een ReFS volume.

2.9 Week 4, College 2: Linux bestandssystemen

1. Beschrijf wat *journaling* inhoudt binnen de context van bestandssystemen

Older filesystems in this category were subject to subtle corruption if power was interrupted in the middle of a write operation, because then disk blocks could contain inconsistent data structures. The `fsck` command was used at boot time to check filesystems for this kind of problem and to automatically patch the most common issues.

Modern filesystems include a feature called *journaling* that averts the possibility of this type of corruption. When a filesystem operation occurs, the required modifications are first written to the journal. Once the journal update is complete, a "commit record" is written to mark the end of the entry. Only then is the normal filesystem modified. If a crash occurs during the update, the filesystem can later replay the journal log to reconstruct a perfectly consistent filesystem.

Journaling reduces the time needed to perform filesystem consistency checks to approximately one second per filesystem. Barring some type of hardware failure, the state of a filesystem can almost instantly be assessed and restored.

[UNIX and Linux System Administration Handbook 5th Edition, §20.10]

2. Welk van de volgende bestandssystemen hebben *journaling* als faciliteit?

- ext2
- xfs
- ext3

- ext4
- NTFS
- ~~FAT~~

3. Wat betekenen de klassieke rechten (u, g, o en r, w, x) onder UNIX/Linux?

- u, g en o geven aan voor *wie* de rechten gelden:
 - u = **user**: de eigenaar van het bestand
 - g = **group**: de user group die aan het bestand is toegekend
 - o = **others**: alle gebruikers die niet de eigenaar zijn of tot de user group behoren
- r, w en x geven aan *welke* rechten:
 - r = **read** (only)
 - w = **write**
 - x = **execute** (voor directories houdt dit in dat in de directory afgedaald kan worden, ook als de directory niet leesbaar is)

4. Geef van de 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):

- **rw-rwxr-x 775**
identiek: read, write en execute voor zowel user als group, alleen read en execute voor alle anderen
- **rw-r-xr-x 755**
identiek: read, write en execute voor user, alleen read en execute voor group en alle anderen
- **rw-r--r-- 622**
niet identiek:
 - rw-r--r-- staat voor read en write voor user, read voor group en alle anderen (komt overeen met 644)
 - 622 staat voor read en write voor user, write voor group en alle anderen (komt overeen met rw--w--w-)
- **rw-r----- 640**
identiek: read en write voor user, read en execute voor group en alleen execute voor alle anderen
- **rw-r-x--x 752**
niet identiek:
 - rw-r-x--x staat voor read, write en execute voor user, read en execute voor group en alleen execute voor alle anderen (komt overeen met 751)
 - 752 staat voor read, write en execute voor user, read en execute voor group en alleen write voor alle anderen (komt overeen met rwxr-x-w-)
- **rw-x--x--- 710**
identiek: read, write en execute voor user, alleen execute voor group en geen rechten voor alle anderen

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)?

Het is een masker ten opzichte van standaard read en write rechten voor iedereen (execute rechten worden door de meeste programma's, waaronder touch, niet standaard aangevraagd voor een nieuw bestand), dus de resulterende rechten zijn het resultaat van een EXOR operatie tussen 666 (read en write voor iedereen) en het *umask*, in dit geval 022:

666 → 110110110

022 → 000010010

110100100 → 644 ofwel rw-r--r-- (betekenis: zie het antwoord op vraag 2)

6. Waarvoor wordt een bestandssysteem gebruikt?

Het bestandssysteem wordt gebruikt voor verschillende processen, kernel data, *interprocess*, communicatiekanalen en drivers zoals van bijvoorbeeld een geluidskaart.

7. Wat is het hoofddoel van een bestandssysteem?

Het hoofddoel van het bestandssysteem is het organiseren en reproduceren van data op de interne (of externe) disk of SSD (lees: storage). Een filesystem wordt niet alleen gebruikt om data op te slaan en op te halen, maar ook om bijvoorbeeld rechten of permissies in te stellen.

8. Uit welke vier componenten bestaat een bestandssysteem?

- een *namespace*: een naam voor de organisatie in de hiërarchie
- een API: *system calls* voor navigatie en manipulatie van objecten
- een beveiligingsmodel: voor het beveiligen, het onzichtbaar maken en delen van objecten
- een implementatie van software die het mogelijk maakt dat de hardware (de disk) wordt beschreven.

Sommige bestandssystemen zijn traditionele schijfimplementaties, terwijl andere (NFS en CIFS) worden afgehandeld door een driver, waarbij de informatie vaak op een andere computer of harde schijf zal worden opgeslagen. De scheidslijn van de architectuur is niet scherp getrokken en er zijn speciale toepassingen. Zo kan een *device file* bijvoorbeeld ook rechtstreeks communiceren met drivers in de kernel.

9. Wat is onder Linux het startpunt van het bestandssysteem (Bij Windows is het C:\)?

Onder Linux is het startpunt van het bestandssysteem altijd de root (/).

10. Wat is het verschil tussen een absoluut en een relatief pad?

Het absolute pad beschrijft het volledige pad van een bestand of directory. Hierbij is de root (/) het beginpunt. Een voorbeeld hiervan is: `/etc/dhcp/dhcpd.conf`. Het relatieve pad begint in tegenstelling tot het absolute pad in de huidige directory. Bijvoorbeeld: je zit in `/home/piet/` en geeft dan `cd Documents/belangrijke_data` op.

11. Met welk commando kun je de huidige directory opvragen?

`pwd`

12. Welke beperkingen heeft een padnaam onder Linux?

Een beperking van een *pathname* is dat het (in principe) niet langer mag zijn dan 255 karakters. Voor de *path length* geldt een beperking van 4095 Bytes. Een *pathname* langer dan 255 karakters kan meestal wel worden bereikt via een *change directory* (`cd`) naar tussenliggende directory en daarna het relatieve pad te gebruiken. Namen van bestanden en directories mogen, naast de lengte, geen slash (/ = directory separator) of 'null' (terminate segmenst of tekst) bevatten. Een *space* (spatie) is toegestaan, maar bij bepaalde software kan dat tot problemen leiden. Om een spatie in de naam te kunnen gebruiken, moet je o.a. scripts erop voorbereiden. Dit kan o.a. door gebruik te maken van aanhalingstekens, bijvoorbeeld: `"Boekjaar 2017"`. Het gebruik van een backslash (\) kan (ook bij Windows) een spatie 'vervangen'.

13. Welk commando kun je gebruiken om een disk of een partitie te koppelen aan het OS?

`mount`, bijvoorbeeld: `sudo mount /dev/sdb2 /backup_data`.

14. In welk bestand worden de gekoppelde partities (mounted) opgeslagen?

`/etc/fstab`.

15. Wat zijn de belangrijk standaard directories onder linux?

Zie tabel 5.1 in *UNIX and Linux System Administration Handbook, 5th Edition*:

Pathname	OS*	Contents
/bin	All	Core operating system commands ^b
/boot	LS	Kernel and files needed to load the kernel
/dev	All	Device entries for disks, printers, pseudo-terminals, etc.
/etc	All	Critical startup and configuration files
/home	All	Default home directories for users
/kernel	S	Kernel components
/lib	All	Libraries, shared libraries, and parts of the C compiler
/media	LS	Mount points for filesystems on removable media
/mnt	LSA	Temporary mount points, mounts for removable media
/opt	All	Optional software packages (not consistently used)
/proc	LSA	Information about all running processes
/root	LS	Home directory of the superuser (often just /)
/sbin	All	Commands needed for minimal system operability ^c
/stand	H	Stand-alone utilities, disk formatters, diagnostics, etc.
/tmp	All	Temporary files that may disappear between reboots
/usr	All	Hierarchy of secondary files and commands
/usr/bin	All	Most commands and executable files
/usr/include	All	Header files for compiling C programs
/usr/lib	All	Libraries; also, support files for standard programs
/usr/lib64	L	64-bit libraries on 64-bit Linux distributions
/usr/local	All	Software you write or install; mirrors structure of /usr
/usr/sbin	All	Less essential commands for administration and repair
/usr/share	All	Items that might be common to multiple systems
/usr/share/man	All	On-line manual pages
/usr/src	LSA	Source code for nonlocal software (not widely used)
/usr/tmp	All	More temporary space (preserved between reboots)
/var	All	System-specific data and configuration files

16. De meeste bestandssystemen onder Linux kunnen werken met zeven file types. Welke zijn dat?

Zie tabel 5.1 in *UNIX and Linux System Administration Handbook, 5th Edition*:

- regular files,
- directories,
- character device files,
- block device files,
- local domain sockets,
- named pipes (FIFOs),
- symbolic links.

File type	Symbol	Created by	Removed by
Regular file	-	editors, cp , etc.	rm
Directory	d	mkdir	rmdir , rm -r
Character device file	c	mknod	rm
Block device file	b	mknod	rm
Local domain socket	s	socket(2)	rm
Named pipe	p	mknod	rm
Symbolic link	l	ln -s	rm

17. Met welk commando kun je een hard link maken en verwijderen?

Maken met **ln** en verwijderen met **rm**.

18. Wat is een symbolic link?

Symbolic (of soft) links: verwijzen naar een file aan de hand van diens naam. Als de kernel een symbolic link tegenkomt, dan wordt er verwezen naar het bestand via de pathname. Het is een referentie naar een ander bestand of directory. Hierbij kan zowel een absoluut als relatief path worden gebruikt. Het verschil tussen een hard link en een symbolic link is dat een hard link een directe referentie is en een symbolic link verwijst naar een naam.

19. Linux kent vier file-type bits. Welke zijn dat?

Dit zijn:

- de permission bits,
- de setuid bit,
- de setgid bit,
- de sticky bits.

20. Met welk commando kun je informatie opvragen over een bestand of een directory?

ls

21. Wat is de functie van chmod?

Met **chmod** kan de eigenaar of de superuser de permissies aanpassen.

22. Wat is de functie van chown en chgrp?

chown verandert de *ownership* van een file of een directory. Je kunt **chown** ook gebruiken voor een groep.

Het commando **chgrp** wijzigt het eigenaarschap voor een groep.

De syntax van **chown** is: **chown** <user>.<group> <file> of **chown** <user>:<group> <file>, van **chgrp**: **chgrp** <group> <file>

23. Wat is de functie van umask?

Met *umask* kun je default permissies instellen op bestanden (en directories) die worden aangemaakt. Elk proces heeft zijn eigen *umask attribute*.

24. Hoeveel bitjes gebruikt Linux om gebruikers en groepen permissies te verlenen (*permission bits*)?
negen bitjes, van 000 tot 777.

25. Welk 'software' is nodig om data op een harde schijf te kunnen schrijven?

De software bestaat uit: device drivers, partitioning conventions, RAID implementaties. Logical Volume Managers (LVM), systemen voor het virtualiseren van Disks over het netwerk in de feitelijke bestandssystemen.

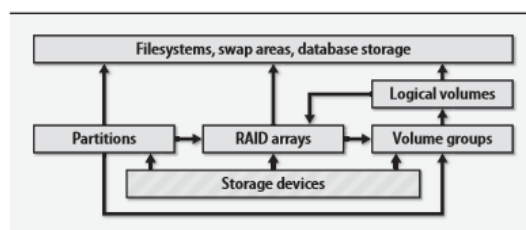
26. Met welk commando kun je zien welke disken en partities er op het systeem beschikbaar zijn?
`Fdisk -l`

27. Met welke commando's kun je een harde schijf indelen?

o.a. **fdisk**, **sfdisk**, **parted** of **gparted**

28. Geef een schematische weergave van hoe schijven, partities en bestandssystemen aan elkaar verbonden zijn.

Zie Exhibit A in *UNIX and Linux System Administration Handbook, 5th Edition*:



29. In welke directory kom je de device file van een harde schijf tegen?

`/dev`, bijvoorbeeld: `/dev/sda1`.

30. Wat is de functie van de *swap* partitie?

De *swap* partitie wordt gebruikt als virtueel geheugen.

31. Welke twee typen partitie-tabellen kun je tegenkomen op een harde schijf?

MBR en GPT (GUID).

32. Noem een aantal voordelen van het gebruik van *logical volume management (LVM)*.

- je kunt LVs over meerdere schijven verdelen,
- LVs kunnen groter en/of kleiner worden gemaakt (on the fly),
- Je kunt snapshots maken,
- je kunt *online* drives vervangen zonder dat services worden onderbroken,
- je kunt mirroring of striping(RAID) toevoegen. Striping zorgt o.a. voor een hogere bandbreedte en een lagere *latency*.

33. Wat is kenmerkend aan de commando's die bij LVM worden gebruikt?

De beginletters van LVM commando's geven aan wat de functie is.

- PV = physical volume,
- VG = volume group,
- LV = logical volume.

34. Met welk commando kun je informatie over LVM opvragen?

`lvdisplay`.

35. Kun je een harde schijf na het partitioneren direct met bestanden beschrijven?

Nee, nadat een harde schijf is opgedeeld in partities of logische volumes is het nog niet bruikbaar om informatie op te slaan. Er moet een bestandssysteem worden toegevoegd om de *raw disk blocks* toegankelijk te maken voor data. Linux ondersteunt veel verschillende soorten bestandssystemen. Voorbeelden zijn: ext2, ext3, NFS en FAT.

36. Wat zijn belangrijke kenmerken van een bestandssysteem?

Belangrijk voor bestandssystemen is dat ze:

- goed presteren,
- tolerant zijn voor crashes en verlies van spanning/stroom zonder dat het bestandssysteem daardoor corrupt raakt,
- ondersteuning bieden voor grote schijven.

Alle moderne bestandssystemen bieden in bijna elk geval deze mogelijkheden.

37. **Met welke tool kun je onder Linux controleren of het bestandssysteem problemen vertoont?**
fsck (filesystem check).
38. **Beschrijf hoe je onder Linux een partitie een bestandssysteem geeft.**
mkfs -t <fstype> [-o options] <rawdevice>, bijvoorbeeld mkfs -t ext4 /dev/sdb2

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

1. **Welke service geeft de mogelijkheid om computers een DNS en WINS-server mee te geven?**
DHCP.
2. **Welke vier stappen heeft het DHCP proces?**
Discover Offer Request Acknowledge (DORA).
3. **Wat is de voorloper van DHCP?**
BOOTP.
4. **In welk directory kun je onder Linux (in veel gevallen) de DHCP configuratie bestanden vinden?**
/etc/dhcp
5. **Welke service heb je nodig om DHCP-verzoeken door een router te krijgen?**
(DHCP) relay-agent.
6. **Wat is DHCP failover?**
Hiermee kun je DHCP-servers en scopes hoog beschikbaar maken.
7. **Hoe worden de databases van een DNS-server genoemd?**
Zones.
8. **Wat is een *namespace* als het gaat om een DNS-server?**
De naam van het domein (meestal zonder hostname).
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?**
hosts-file.
10. **Waarom wordt er gesteld dat DNS een hiërarchisch structuur heeft?**
De naam (FQDN) van een systeem wordt opgebouwd met meerdere namen of karakters die gescheiden worden door een punt (.). Per deel van de FQDN is een server specifiek verantwoordelijk voor de omzetting van dat deel dat tussen punten in staat.
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?**
Recursion.
12. **Wat is Dynamic DNS?**
Systemen krijgen hiermee de mogelijkheid om hun IP-adres, verkregen van een DHCP-server, zelf te registreren van een DNS-server.
13. **Welke DNS-records kun je in een DNS-server tegenkomen met betrekking tot IPv4?**
A, PTR, SRV, MX, CNAME.
14. **Wat is een Start of Authority record?**
Een SOA record bevat de gegevens (zoals timers) van een specifieke zone.
15. **Met welke commando's kun je de werking van een DNS-server testen?**
nslookup en dig.
16. **Op welk manier kun je DNS-verzoeken veiliger maken?**
Door DNSSEC te gebruiken.
17. **Wat is het verschil tussen een *master* en een *slave* (DNS) zone?**
In een master zone mag worden geschreven en er kan worden gelezen. Een slave zone is alleen maar leesbaar.
18. **Welke configuratiefile wordt onder Linux gebruikt om de DNS-server te configureren?**
/etc/named.conf.
19. **Wat is een *authoritative* nameserver?**
Een DNS-server die voor een domeinnaam verantwoordelijk is en/of het antwoord op een DNS-verzoek weet. Zegt niets over het feit of een server een master of een slave is.
20. **Wat is de meest gebruikte Linux DNS-server software?**

BIND (oorspronkelijk “Berkeley Internet Name Domain”).

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

1. **Welke vijf basis services worden door SMB/CIFS geboden?**
File sharing, Network printing, authentication & authorization, Name resolution and Service announcement.
2. **Samba onder Linux kan voor file sharing worden gebruikt, maar ook voor....**
Basis functionaliteiten voor AD-controller.
3. **Op welk punt verschillen NFS en SMB van elkaar?**
SMB heeft in tegenstelling tot NFS geen ondersteuning van de kernel nodig.
4. **Wat is het configuratiebestand van SMB onder Linux?**
smb.conf. Staat meestal in /etc(/samba).
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?**
Effective permissions.
6. **Hoe kun je onder Windows een share *hidden* maken en hoe maken je bestanden onder Linux onzichtbaar voor ls?**
Je moet dan een dollarteken \$ aan het eind van de naam plaatsen. Bij Linux zet je een . voor de naam van een bestand.
7. **Welke vijf basis componenten kom je tegen bij een URL-object?**
Protocol or application, Hostname, TCP/IP port, Directory, Filename (laatste drie zijn optioneel!)
8. **Met welke commandline tools kun je een webserver testen en/of benaderen?**
telnet (handmatig HTTP requests uitvoeren), wget, curl en PowerShell commandlet Invoke-WebRequest.
9. **Hoe kun je op een webserver met een enkel IP-adres toch meerdere Websites hosten?**
Werken met *virtual hosts* of met verschillende poorten, hostnamen of virtuele interfaces die je een apart IP-adres geeft.
10. **Op welke manier kun je HTTP-communicatie beveiligen?**
Versleuteling en authenticatie met behulp van SSL.
11. **Wat is de default poort waarop een webserver luistert?**
Poort 80
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?**
Windows authentication.

2.12 Week 6, College 1: Windows Group Policies

1. **Wat is een *group policy*?**
De manier om configuratie management in een windows omgeving te vereenvoudigen en te centraliseren.
2. **Wat is een GPMC?**
Group Policy Management Console voor het beheer van GPO's.
3. **Op welke vier niveaus kun je een GPO linken?**
Local, Site, Domain, OU
4. **Welke twee policies zijn standaard op een gepromoveerde domain controller aanwezig?**
Default Domain Controller policy / Default domain policy
5. **Aan welke gebruikers groep is de default domain policy gelinked?**
Aan alle gebruikers en groepen in het domein.
6. **Op welke twee categorieën kunnen settings binnen een GPO invloed hebben?**
Computer settings en user settings

7. **Op welke centrale locatie worden GPOs binnen een domein opgeslagen?**
\sysvol op de DC.
8. **Wat is de functie van een GUID (unique ID) bij een GPO?**
Een uniek referentie nummer zonder naam (naam onafhankelijk)
9. **Welke GUID hoort bij welke policy in de share?**
Afhankelijk van het domein.
10. **Wat is de functie van de waardes "User version" en "Computer version"? Onderzoek tevens de functie van (AD) en (sysvol).**
De user version en computer version slaan op de actuele versie van het gebruiker gebonden deel en het computer gebonden deel.
11. **Wat wordt er bedoeld met een *enforcement*?**
Een GPO net de "enforce"optie, krijgt voorrang bij onderliggende objecten en conflicten.
12. **Wat is het doel van het uitschakelen van de computer- of usersettings in een GPO?**
Minder data verkeer → Verhogen prestaties
13. **Hoe kun je met gpresult op de DC controleren welke settings gelden voor de gebruiker floris.devijfde?**
Door met admin rechten een cmd te openen en via Gpresult /user de actuele settings op te vragen. Afh van situatie kan / moet je ook de computer specificeren
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!**
Alle policies worden uitgevoerd (direct gekoppeld en via erven verkregen) en de meest beperkende versie wint. Local, site, domain, ou, ou(is ook de volgorde) In principe wint de laatst geschreven setting met uitzondering van o.a. een enforcement.
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?**
GPT.ini o.a versie nummer
16. **Hoe weten domain controllers of ze de juiste versie van een GPO hebben of dat ze om de nieuwe versie moeten vragen?**
Door de versie nummers te vergelijken van de versie op de DC en de lokale versie.
17. **Met welk PowerShell cmdlet kan je een report maken in HTML formaat?**
Get-GPOReport -Name TestGPO1 -ReportType HTML -Path
C:\GPOReports\GPOReport1.html
18. **Wat is het verschil tussen een GPO restore en een GPO Import.**
Restore is terugzetten vanuit een backup, bij import kunnen bepaalde instellingen worden geïmporteerd.
19. **Welke functionaliteiten biedt GPMA bovenop die van GPMC?**
Extra mogelijkheden met name op het gebied van beheer.
20. **Welke AGPM roles zijn er?**
Full Control – AGPM Admins Role
Approver Role
Reviewer Role
Editor Role
21. **Bekijk van de ADMX/ADMS bestandstypes een voorbeeld en geef aan wat de specifieke kenmerken zijn.**
ADMX bevat de instellingen en ADML de taalbestanden
22. **Op welke manier zijn corresponderende admx en het adml bestanden aan elkaar gelinked?**
Met GUID.

23. Bij administrative templates kun je de term *Tattooing* tegenkomen. Wat wordt hiermee bedoeld?

Registry policy is not the only area in Group Policy that is subject to tattooing. Basically any policy area that does not have an option to explicitly remove itself if the GPO falls out of scope of the computer or user will leave a trail behind. Some obvious ones that come to mind include registry, file system and restricted groups security policy. These policy areas aren't undone if the GPO no longer applies. In the case of registry and file system security, permissions are changed only when the GPO is applied, but since there is no easy "rollback" of file system or registry security, these permissions changes linger after the policy is removed. Similarly restricted groups policy may be removed but the users are not removed from the groups they've been added to. However, subsequent changes to group membership will not be restricted since the policy no longer applies.

Similarly, Software Installation and Folder Redirection policy can be tricky in terms of its tattooing effect. Both have options to "un-do" things that were done, like uninstalling software when the machine or user falls out of scope or redirecting My Documents back to the local user profile in the case of Folder Redirection policy. However, in both cases this mechanism has proven problematic for administrators and users alike. So, it's important to never un-do one of these kinds of policies lightly without a good plan in place for dealing with the fallout.

24. Software installatie met GPOs kan op twee manieren. De twee manieren zijn *Publish* en *Assign*. Wat zijn de verschillen?

Met Publish wordt de software gepubliceerd en kan een gebruiker zelf bepalen of het moet worden geïnstalleerd. Bij assign wordt het systeem geïnstalleerd en heeft de gebruiker daar geen invloed op.

25. Welke applicaties zijn geschikt om te installeren via een GPO.

*.MSI bestanden.

26. Wat zijn de voordelen van het installeren van een applicatie in *.msi vorm?

MSI bestanden zijn aan te passen om de installatie automatische / aangepast te laten verlopen.

27. Wat is een *software Distribution Point*?

A distribution point is a site system that stores packages for clients to install. Distribution points are required for software distribution and updates, as well as for using advertised task sequences to deploy operating system software

28. Wat zijn de voordelen van een centrale opslag?

Geen problemen met versie verschillen en updates.

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?

Het computerdeel wordt al uitgevoerd bij aanmelden op het netwerk. Het gebruikersdeel wordt uitgevoerd bij aanmelden. Reden hiervan is dat een client computer geen gebruiker aangemeld heeft staan.

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*.

Bij veel of weinig aanpassingen, of een bandbreedte probleem in het netwerk. De random offset heeft te maken met het verdeeld blijven van de aanvragen bij de DC (geen 300 aanvragen op hetzelfde moment als bijvoorbeeld na stroomuitval alle computers tegelijkertijd opstarten).

31. Omschrijf de functie van *Slow link detection* en *cached credentials*.

Slow link detection wordt gebruikt voor het bepalen van de ruimte die er nog in de verbinding zit. Als deze te beperkt is worden de lokaal opgeslagen policies gebruikt of een gebruik mag het systeem niet gebruiken.

32. Wat is de (standaard) instelling voor *Processing Group Policy over Slow Links*?

500kbps

- 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?**

Windows Vista® en Windows Server® 2008 ondersteunen Network Location Awareness, waardoor programma's die deze functie ondersteunen hun gedrag kunnen wijzigen op basis van de manier waarop de computer met het netwerk is verbonden. In het geval van Windows Firewall with Advanced Security kunt u regels maken die alleen van toepassing zijn als het profiel dat is gekoppeld aan een specifiek netwerklocatietype actief is op de computer. GPOs kunnen overweg met NLA.

- 34. Aan welke eisen moet een wachtwoord voldoen als de policy "password must meet complexity requirement" is geselecteerd?**

Complexity requirement bepaald uit hoeveel Letters (hoofd- en kleine), nummers, leestekens een wachtwoord moet bevatten.

- 35. Wat is de functie van *account Lockout threshold*.**

Het maximaal foutieve inlogpogingen voordat een account wordt gelocked.

- 36. Wat is *account lockout duration*.**

De lockout duration bepaald de periode voor de blokkering voor opnieuw aanmelden mogelijk is.

- 37. Wat gebeurt er als de tijd tussen DC en client te veel uiteenloopt. Wat is de default instelling.**

Er ontstaan problemen met versie vergelijkingen als deze gebaseerd zijn op een tijdstip, een systeem of gebruiker mag niet aanmelden

- 38. Waar staat EC voor in de starter GPOs?**

Enterprise client

- 39. Wat is het verschil tussen een *preference* en een GPO?**

Preference kan worden veranderd, applicaties hoeven niet policy aware te zijn, tattooing. Policies kan de user niet weigeren, hogere prioriteit, applicatie moeten policy aware zijn.

- 40. Wat wordt er bedoeld met *targeting* ?**

GPO's heel specifiek van toepassing laten zijn, bv afhankelijk van de hoeveelheid geheugen of het OS.

- 41. Wat is de functie van de GPO Results Wizard?**

Geeft de specifiek GPO instellingen van een gebruiker op een willekeurig of specifiek systeem weer.

- 42. Wat is de functie van GPO modeling?**

Een what-if scenario uitvoeren: "wat zou er gebeuren als we dit zouden configureren".