Commands and concepts

Basis IT Platformen
Blok 1 | Semester 1Verdieping
Software

Mayar Alakkad
HBO-ICT Cyber Security & Cloud
1852382
TICT-CSC-DU1B
2023 – 2024
V0.5

Inhoudsopgave

Inleiding .... **Error! Bookmark not defined.**
Versiebeheer 12

Week 1

Week 2

Windows

Linux

2.5.1.3

Map back-up, error logs loggen in backuperror

```
cp /etc/sysconfig sysconfbackup 2> backuperror.log
```

Map back-up, output loggen in back.lst

```
sudo cp -r -v /etc/sysconfig sysconfbackup > backup.lst
```

2.5.1.4

```
ls /usr/share/doc | grep linux
```

2.5.1.6

```
ps -e | grep gnome-session*
```

2.5.2

a:

```
sudo nano /root/.bashrc
echo "Welkom superman!"
```

b:

c:

```
sudo nano /etc/environment
pwsh=/opt/microsoft/powershell/7
```

d:

```
touch /etc/skel/todo.txt
```

Week 3

Windows

This command is used to sync the domain controllers with the main DC.

```
Repadmin /syncall
```

This command is used to disable ipv6 on an interface

```
Disable-NetAdapterBinding -Name “interface name” -componentID ms_tcpip6
```

This command is used to import users in active directory (-k makes sure that the import process doesn’t stop when a error occurs)

```
Csvde -i -k -v -f “filename”
Ldifde -I -k -v -f “filename”
```

Import users from CSV using powershell

Note: you have to make sure that the tool rsat-adds has been installed using the command Install-WindowsFeature rsat-adds

```
Import-Csv "C:\Users\Administrator\Desktop\BIPL_Users\BIPL_Users\patienten5.csv"| New-ADUser
```

To lookup for users that didn’t change their password in x amount of days

```
Dsquery user -stalepwd days
```

To lookup for users that hasn’t been active for x amount of days

```
Dsquery user -inactive days
```

To lookup for users that are disabled in AD

```
Dsquery user -disabled
```

Note: this command shows only 100 records, if you prefer to show all the matching users, use the parameter “–limit 0”

To move matching record to a file use the command > “*filename*” to the end of the command

To lookup for disabled users in specific OU and enable them and give the users temporary password

```
dsquery user OU=the-OU,DC=your-domain,DC=local -disabled -limit 0 | dsmod user -pwd Pa$$w0rd -disabled no
```

Linux

To create a new group in linux use the command

Groupadd

To delete a user completely

sudo userdel -r

to change the policy for user password expiration

chage -m 1 -M 40 -I 1 -W 7 *username*

Week 4

Windows

This command grants access to a new group to a share with the specified premissions

Grant-SmbShareAccess -Name "Shared folder" -AccountName "*Account Name*" -AccessRight Full -Force

This command revokes access to a share

Revoke-SmbShareAccess -Name “*Share*” -AccountName “*account*”

This command creates a folder

New-Item -Path ‘*Path’* -ItemType Directory

This command creates a SMB share with the share permissions to specified groups or accounts

New-SmbShare -Name “*foldername*” -Path “*path to folder*” [-FullAccess, -NoAccess, -ReadAccess] “*Groups/Accounts*”

Linux

To change the owner user/group of a folder/file use the command

Sudo chown *user*:*group* “*path to folder/file*”

Chmod numbering

1 = execute | 2 = Write | Read = 4

This command enables group inheritance from the parent directory (if the group owner of the parent folder is *example* then the group owner of the childitem becomes *example*)

sudo chmod g+s

To search from root folder “/” to file named passwd use the following command

sudo find / -name passwd

to search in the whole filesystem to files with the SID bit enabled as root

sudo find / -user root -perm -4000

these are examples of disk management programs

cfdisk, fdisk, parted, blkid, lsblk

This command is used to show the partitions and the used space/available space in a partition

df -h

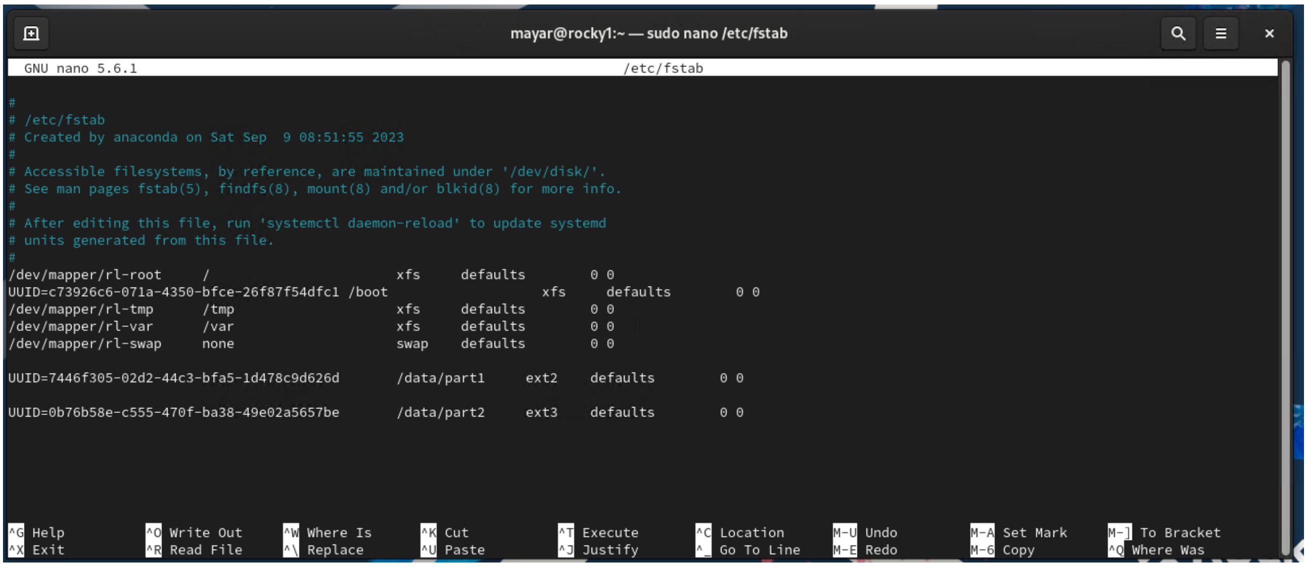
this command check the filesystem

fsck.[*ext2, ext3, ext4*]

Note: to mount disk to a default mountpoint you have to edit the file /etc/fstab file with the UUID

To find the UUID of a disk, use the command

blkid



```
mayar@rocky1:~ — sudo nano /etc/fstab

  GNU nano 5.6.1                                              /etc/fstab

#
# /etc/fstab
# Created by anaconda on Sat Sep  9 08:51:55 2023
#
# Accessible filesystems, by reference, are maintained under '/dev/disk/'.
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info.
#
# After editing this file, run 'systemctl daemon-reload' to update systemd
# units generated from this file.
#
/dev/mapper/rl-root     /                       xfs     defaults        0 0
UUID=c73926c6-071a-4350-bfce-26f87f54dfc1 /boot                   xfs     defaults        0 0
/dev/mapper/rl-tmp      /tmp                    xfs     defaults        0 0
/dev/mapper/rl-var      /var                    xfs     defaults        0 0
/dev/mapper/rl-swap     none                    swap    defaults        0 0

UUID=7446f305-02d2-44c3-bfa5-1d478c9d626d       /data/part1     ext2    defaults        0 0

UUID=0b76b58e-c555-470f-ba38-49e02a5657be       /data/part2     ext3    defaults        0 0



^G Help         ^O Write Out    ^W Where Is     ^K Cut          ^T Execute      ^C Location     M-U Undo        M-A Set Mark    M-] To Bracket
^X Exit         ^R Read File    ^\ Replace      ^U Paste        ^J Justify      ^_ Go To Line   M-E Redo        M-6 Copy        ^Q Where Was
```

To initialize a partition to be an LVM physical volume

Pvcreate */dev/your-disk*

Note: the disk will be in this case formatted

Add a LVM to a VG (volume group

Vgcreate *VG-Name /dev/your-disk*

To display the volume groups:

Vgdisplay

To create a Logical volume from a volume group

lvcreate -L 1GB -n *logical-volume-name volume-group-name*

to create a symbolic link

Ln -s *source-file symbolic-name*

Note: the symbolic name creates a (file?) in the path where the command has been entered

Week 5

Windows Server

Note: when using server manager, you manage the servers as the logged in user in Windows on the client or on the server itself

Note: Don't!!!!! ever add a new network card to a domain controller and turn it off without configure it to function in AD!!! This will fuck your whole AD. If you do that, you'll get the error that you cannot authenticate with the AD Domain Admin account (user name or password incorrect error). The solution is to disable the interface and restart the Domain controller

Linux

To release and renew DHCP configuration

```
Sudo dhclient -r #this command is used to release
Sudo dhclient #this command is used to renew
```

To watch logs in real time use the command

```
Watch tail -n 25 /var/log/messages
```

To change the ip address of an interface, use the ifconfig command

```
Ifconfig interface-name IP-address netmask subnet-mask
```

The path to the DHCP leases in Linux DHCP server

```
/var/lib/dhcpd/dhcpd.leases
```

To deactivate interface and reactivate it (apply changes in IP configuration) in Rocky Linux

```
Nmcli con down interface && nmcli con up interface
```

Nslookup in Linux, after the @ is specifying the DNS server

```
dig +noall +answer rocky1.bmc.test @192.168.20.1
```

Location of the files needed to configure DNS server on Linux

```
/etc/named.conf
/var/named/named.empty
```

Saves the running configuration of the firewall to the startup configuration of the firewall rules

```
sudo firewall-cmd --runtime-to-permanent
```

Week 6

Windows

To backup all GPOs

Backup-GPO -Domain *your-domain* -Path *path* -All

Versiebeheer

Auteur	**Datum**	**Wijziging**	**Versie**
Mayar Alakkad	23-09-2023	Week 3 uitgevoerd en verwerkt in documentatie	V0.1
Mayar Alakkad	24-09-2023	Week 4 uitgewerkt en verwerkt in documentatie	V0.2
Mayar Alakkad	29-09-2023	Week 5 gestart | Windows	V0.3