**CENTOS-RHEL COOKBOOK**

**YİĞİT AYDOĞ**

(general security hardening checklists)

[**https://highon.coffee/blog/security-harden-centos-7/**](https://highon.coffee/blog/security-harden-centos-7/)

**USE CentosCD as repo mount**

mount -o ro /dev/cdrom /mnt

vi /etc/yum.repos.d/test.repo

[test]

name=Software Repo

baseurl=file:///mnt

enabled=1

gpgcheck=1

gpgkey=file:///mnt/RPM-GPG-KEY-CentOS-7

vi /etc/fstab

/dev/cdrom /mnt iso9660 ro,users,auto 0 0

umount /dev/sr0

**OFFLINE REPOSITORY (servers without internet)**

**(alternative1:as file system)**

mkdir /rpms

mount -o ro /dev/cdrom /mnt

cp -Rv \* /rpms/

umount /dev/sr0

vi /etc/yum.repos.d/test.repo

[test]

name=Software Repo

baseurl=file:///rpms

enabled=1

gpgcheck=1

gpgkey=file:///rpms/RPM-GPG-KEY-CentOS-7

yum install --disablerepo=\* --enablerepo=test packagename

**(alternative1:as web server)**

yum install httpd

mkdir -p /var/www/html/centos

vi /etc/fstab

/dev/cdrom /var/www/html/centos iso9660 ro,users,auto 0 0

vi /etc/yum.repos.d/test.repo

[test]

name=Software Repo

baseurl=http://IP/centos/

enabled=1

gpgcheck=0

systemctl start httpd

**(base packages)**

yum install wget ksh rpcbind traceroute perl openssl-devel gzip unzip ghostscript bzip2 gedit xterm unzip vim gnuplot lsof lvm2 tree gnome-system-log nmap yum-plugin-downloadonly at ntp ntpdate rsync grsync audit audit-libs yum-utils nfs-utils xdpyinfo xorg-x11-apps xorg-x11-xauth xorg-x11-fonts-\* xorg-x11-font-utils xorg-x11-fonts-Type1 finger system-config-keyboard system-config-language firewall-config curl gedit rsync gawk cups sysstat htop gnome-system-monitor NetworkManager net-tools glogg bind-utils bash-completion tcpdump -y

**(epel release)**

wget https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm

rpm -ivh epel-release-latest-7.noarch.rpm

**(remi repo)**

wget http://rpms.famillecollet.com/enterprise/remi-release-7.rpm

rpm -Uvh remi-release-7.rpm

**JAVAJDK**

yum install java-1.8.0-openjdk

yum install java-1.8.0-openjdk-devel

**(pdf reader)**

yum install epel-release -y

rpm -ivh nux-dextop-release-0-5.el7.nux.noarch.rpm

yum localinstall AdbeRdr9.5.5-1\_i486linux\_enu.rpm

acroread

**(bash autocomplete)**

yum install bash-completion bash-completion-extras

Standard Data Structure

/boot>bootloader

/lib > linked library files

/bin >system binaries

/dev> list of devices

/etc >configuration file

/home> userfiles

/lib> system libraries

/root> root user file directory

/sbin> essential sys binaries

/temp > temp storage

/var > temporal files

/media>removable storage

/mnt > temporary file system

/usr/bin >

**(python)**

yum install gcc openssl-devel bzip2-devel libffi-devel -y

wget https://www.python.org/ftp/python/3.8.2/Python-3.8.2.tgz

tar xzf Python-3.8.2.tgz

cd Python-3.8.2

./configure --enable-optimizations

make altinstall

yum install python-devel

yum install python-pip

pip install --upgrade pip

python3.8 -V

python script.py

#! /usr/local/bin/python3.8

**Calling python script from bash**

/usr/local/bin/python3.8 /root/testing.py

tty> echoes the name (filename) of the current user's terminal

lsof -u “username” (open files by user)

console settings: /etc/systemd/logind.conf

vi /etc/shells : known shells in Linux System

vi /etc/init.d : startup scripts

ldd cmd > shows library dependency of a command

#!/bin/bash

chmod +x : make script executable for all user

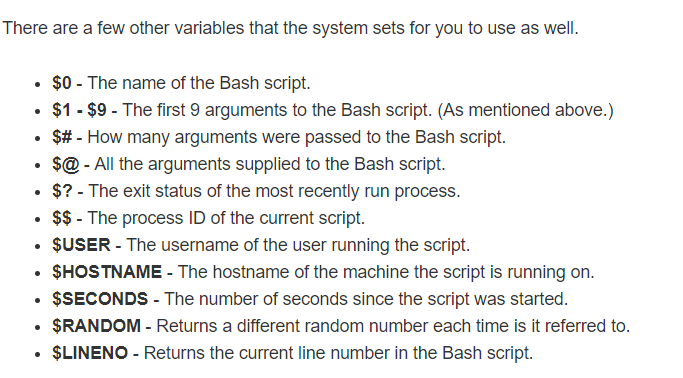
chmod +x scriptname then ./scriptname

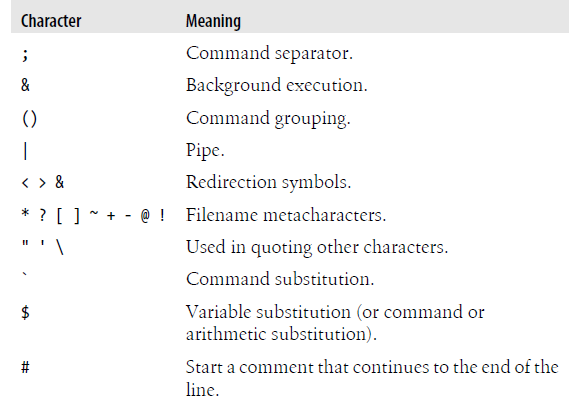
bash scriptname (running script without chmod executable)

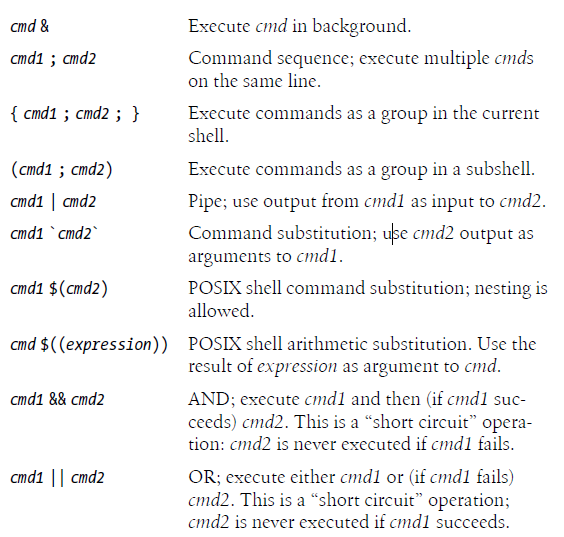
Checking global variables

printenv

Special variables in script







(date; who; pwd) > logfile

Fri Aug 17 11:21:19 +03 2018

root :0 2018-07-31 11:10 (:0)

root pts/0 2018-08-17 10:43 (:0)

/root

cat logfile | grep word || echo "word not found"

logfile içinde istenilen kelimeyi bulamazsa not found verir

Redirection



Finding execute commands

History

fc –l -5 displays last executed 5 cmd

fc -l 50 display cmds after 50th cmd in history

history -c : clears history

echo $HISTSIZE > historysize value

Bash file testing

file="logfile"

if [ -x $file ]; then

echo "Executable"

else

echo "NotExecutable"

fi

Quoting



e.x

[root@localhost ~]# echo $'web: www.linuxconfig.org\temail: web\x40linuxconfigorg'

web: www.linuxconfig.org email: web@linuxconfigorg

Getting user input

read myvar

echo $myvar

[root@localhost ~]# read -p 'Username: ' uservar

Username:

**Empty File Content by Redirecting to Null**

>filename

Silent install and installation check example

yum install -y mysql &>/dev/null

if [ $? == 0 ]; then

echo "mysql is installed"

else

echo "mysql is not installed"

fi

FIND

find “directory”

-name “.\*” (find hidden files)

–iname “filename” (case insensitive find)

–type f/d (file or directory)

–size +100k

-size +100k -200k

–cmin -60(changed in last 60min)

-amin -60 (accessed in last 60min)

-mtime +10 (modified in last 10days)

-user (find according to owner)

-group (find according to group owner)

-perm 777 (find according to permission code)

-empty (find empty files)

Find <location> <options> -exec command

(example)

find / -type f -perm 777 -exec rm -i {} +;

SORT

sort -r (reverse)

sort -n (sort numeric)

sort -k “column number” (sort column)

sort -u (removes duplicate ones)

UNIQ (to find repeated lines) –one line data-

sort file| uniq -c (display how many times repeated)

uniq -u (show not repeated lines)

uniq -d (show repeated lines)

AWK

yum install gawk

awk '/optional\_pattern/ { action }' file

e.x

awk '/root/ { print }' /etc/passwd (search for word)

awk -F : '{ print $1 }' /etc/passwd (: as delimeter and take 1st column)

awk -F : '/bash/ { print $1,$3,$4 }' /etc/passwd (another example)

awk -F , '{ if ($1 ~ /ah\*/) print $3 }' test (condition in awk)

awk -F : '{print FNR, $1}' /etc/passwd (display row numbers)

1 root

2 bin

3 daemon

4 adm

5 lp

6 sync

SED

sed -n 1,3p /etc/passwd (take1,2,3rows)

sed 1,3d /etc/passwd (don’t take only 1,2,3rows)

sed Nd testfile.txt (delete nth line)

sed $d testfile.txt (delete last line)

sed '29-34!d' testfile.txt (delete between N ve M line)

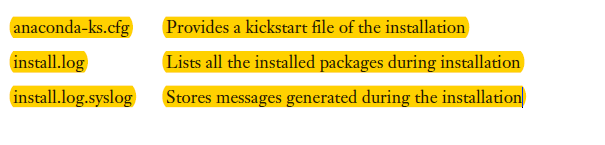
sed 's/danger/safe/g' testfile.txt (change danger word with safe)

sed ‘s/danger/safe/2’ testfile.txt (change 2nd danger word with safe)

sed '4 s/danger/safety/' testfile.txt (change danger word with safe for 4th line)

sed -e 's/#.\*//' testfile.txt (removes comment lines)

**İnstallation files**



not to see output of the command

command >/dev/null

testing command worked

echo $? Should be zero

running command2 if command1 is true

command1 >/dev/null && command2

running command2 if command1 is false

command1 >/dev/null || command2

**CLAMAV ANTIVIRUS**

yum install epel-release

yum install clamav-server clamav-data clamav-update clamav-filesystem clamav clamav-scanner-systemd clamav-devel clamav-lib clamav-server-systemd

sed -i -e "s/^Example/#Example/" /etc/clamd.d/scan.conf

vi /etc/clamd.d/scan.conf

#LocalSocket /var/run/clamd.scan/clamd.sock >> LocalSocket /var/run/clamd.scan/clamd.sock

sed -i -e "s/^Example/#Example/" /etc/freshclam.conf

freshclam (to update virus definition database)

systemctl start clamd@scan

systemctl enable clamd@scan

clamscan -ir /home (checks for infected files)

clamscan -rl /home/clamav.log (scan all system and log)

clamscan -r --remove /home (remove infected files)

**RUN AS ADMIN ON CENTOS=SUID**

Normal users who can execute the file gain privileges associated with the file

[root@test1 ~]# ls -la /usr/bin/passwd

-rwsr-xr-x. 1 root root 27832 Jun 10 2014 /usr/bin/passwd

Passwd komutu run as admin şeklinde standard kullanıcılar tarafından çalışırılabilir

**FİLE SİZE**

ls –lah

du –sh “foldername”

du –h “filename”

(create file with random size) fallocate -l 10G file

**CONFIGURATION FILES SYNTAX AND EXPLANATION**

find /usr/share/doc/ -iname \*.conf -type f -print

**FOLDER MODIFICATION DATE**

stat foldername

date -r foldername

**ALIAS**

(shows cmd switches)

alias rm='rm -i'

**FİLESYSTEM**

Naming convension

First letter: identifies drive type (s: sata, iscsi v: virtual kvm based disk)

Second letter: d for disk

Third letter: relative position of the disk (starting with a)

Volume management

Formats: Xfs ext4

df -h /root >> getting info about specific path

partitioning (maximum allowed is 16) sata,pata,iscsi drives

fdisk /dev/sdb

n (new partition)

p (primary partition)

1 (partition number)

First sector> default

Last sector> +5G

t> 83 (8e for LVM)

w

partprobe /dev/sdb

make sure kernel reads partition table to recognize disks and partitions : partprobe

fdisk -l : give information about disks (more detailed info)

mkfs.ext4 –L “labelname”/dev/sdb1

mkfs.xfs –L “labelname” /dev/sdb1

lsblk --output name,size,fstype,mountpoint

blkid >> partition label’lerini gösterir (UUID leri gösterir)

(MOUNT TEMPORARILY)

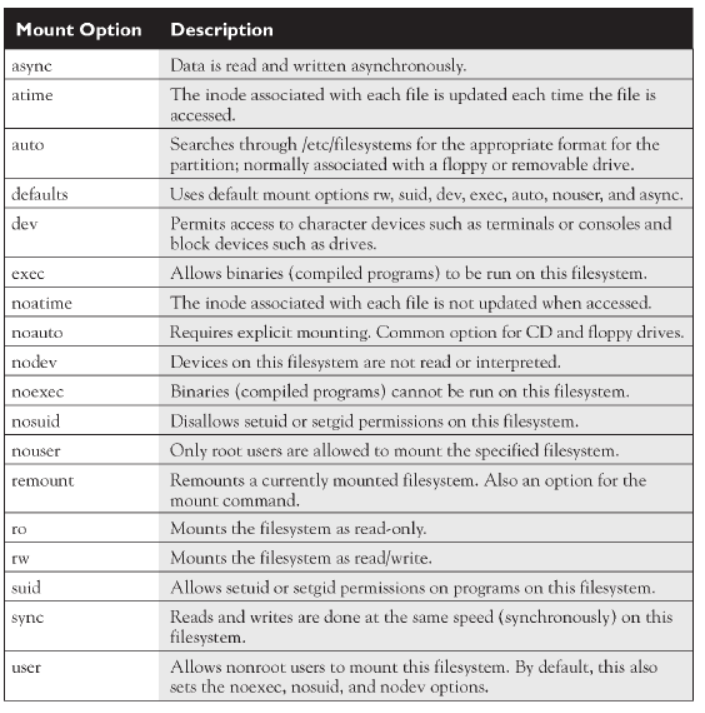
mount -t xfs /dev/sdb1 /storage1

mount -t ext4 /dev/sdb2 /storage2

vi /etc/fstab



/dev/sdb1 /opt ext4 defaults 0 0



/dev/sdb1 /mountdir ext4 defaults 0 0

UUID=b3a913db-8291-472d-b413-024c2f3b7fe4 /mountdir ext4 defaults 0 0

mount -a (fstab dan sonra mount amaclı reboot yapmamak için)

**Finding UUID**

* dumpe2fs /dev/sdb1 | grep UUID
* blkid

SWAP PARTITION

Swap: extension of local RAM especially when Resources runs short

Linux moves infrequently used programs and data to swap space

fdisk /dev/sdc

n (new partition)

p (primary partition)

1 (partition number)

First sector> default

Last sector> +5G

t> 82

w

partprobe /dev/sdc

mkswap /dev/sdc1

swapon /dev/sdc1 (activation)

vi /etc/fstab

/dev/sdc1 swap swap defaults 0 0

mount -a

swapon -s : swap partition’ları görmek

swaponff -v /dev/sdc1 : swap partition’u kaldırmak

free –m: ile swap space in geldiği kontrol edilir

GUI TOOLS

yum install gnome-disk-utility

gnome-disks

! hem partition yapar hemde ext4 file sistemde oluşturur

(disabling swap)

sed -i '/swap/d' /etc/fstab

swapoff -a

CREATING LVM PARTITION

yum install -y lvm2

pvdisplay (physical volume display)

vgdisplay (volume group display)

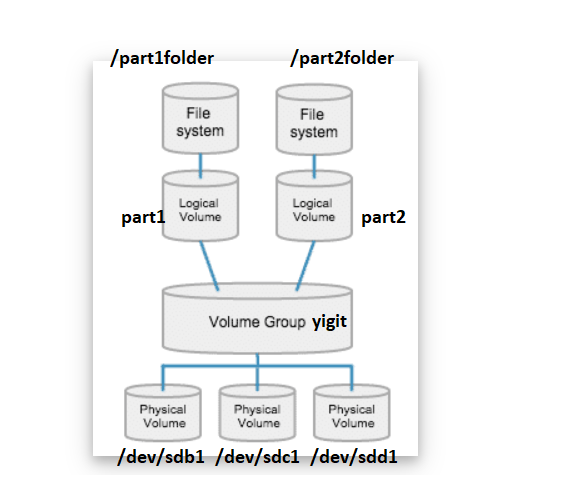
lvdisplay (logical volume display)

PHYSICAL VOLUME(PV) /dev/sdb1 “pvcreate /dev/sdb1”

VOLUME GROUP(VG) vgcreate “vgname” /dev/sdb1

LOGICAL VOLUME1 (LV1) /dev/vg/lv1 “lvcreate -n part1 -L 6G “vgname”

LOGICAL VOLUME2 (LV2) /dev/vg/lv2 “lvcreate -n part2 -L 6G “vgname”



fdisk /dev/sdb

n (new partition)

p (primary partition)

1 (partition number)

First sector> default

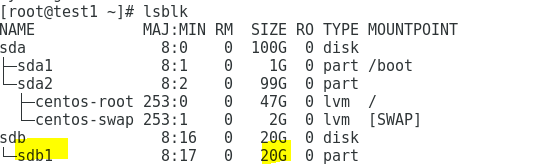
Last sector> +20G

t> 8e

w

partprobe /dev/sdb

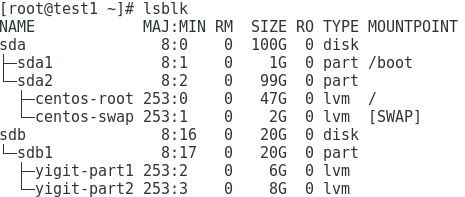
pvcreate /dev/sdb1



vgcreate yigit /dev/sdb1 (Volume group "yigit" successfully created)

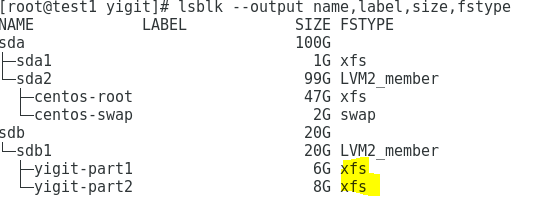
lvcreate -l “physicalextendnumber” -n part1 -L 6G yigit

lvcreate -l “physicalextendnumber” -n part2 -L 8G yigit



mkfs.xfs /dev/yigit/part1 (or mkfs.ext4 /dev/yigit/part1)

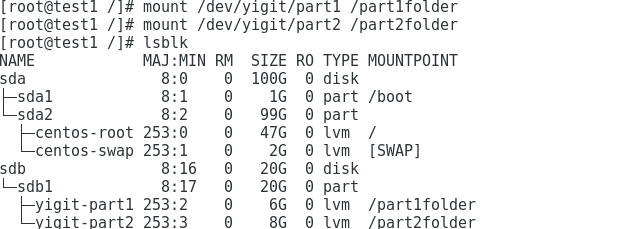
mkfs.xfs /dev/yigit/part2 (or mkfs.ext4 /dev/yigit/part2)



cd /

mkdir part1folder

mkdir part2folder



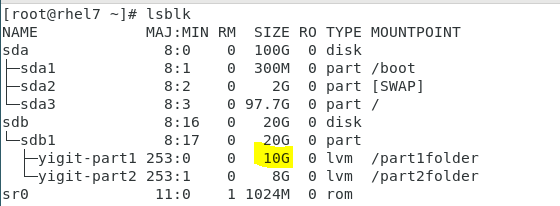
vi /etc/fstab

/dev/yigit/part1 /part1folder xfs defaults 0 0

/dev/yigit/part2 /part2folder xfs defaults 0 0

Increasing size of LVM disk df>>/dev/mapper/yigit-part1

lvextend --size +4G --resizefs yigit/part1



Lowering size of LVM disk

umount /part1folder

lvreduce --size -1G --resizefs yigit/part1

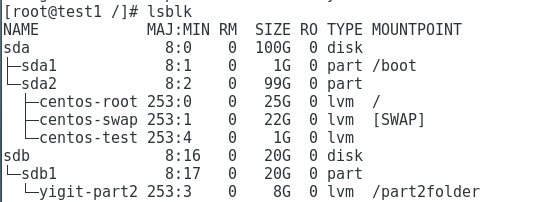
mount /part1folder

Disable lvm volume

umount /dev/yigit/part1

lvchange -an /dev/yigit/part1 (disable)

lvremove /dev/yigit/part1 (remove)



Daha sonrasında fstab tan kaldırılır

vgremove yigit

pvremove /dev/sdb1

**GUI TOOL**

yum install system-storage-manager -y

**TROUBLESHOOT FILE SYSTEM PROBLEMS**

mount -t xfs /dev/sdb1 /storage1

mount -t ext4 /dev/sdb2 /storage2

xfs repair

umount /storage1

xfs\_repair /dev/sdb1

mount -t xfs /dev/sdb1 /storage1

ext4 repair

umount /storage2

e2fsck /dev/sdb2

e2fsck /dev/sdb2 -b <SUPERBLOCK>

mount -t ext4 /dev/sdb2 /storage2

**ENCRYPTION WITH LUKS**

lsblk --output name,size,fstype,mountpoint

You need to enter passphrase at boot to mount

Encrpytion should be done when there is no data, data will be lost during encryption

During boot process there will be luksopen process(de encryption)

yum install -y cryptsetup-luks

modprobe dm\_crypt (activate LUKS modüle)

lsmod | grep dm\_crypt (check if module is running)

/dev/sdb > format ext4 or xfs

cryptsetup luksFormat /dev/sdb (encryption)

and enter passphrase

cryptsetup luksOpen /dev/sdb luks1 (de encryption)

(enter passphrase)

(/dev/mapper/ and luks1 created)

mkdir /data

mkfs.ext4 /dev/mapper/luks1

mount -t ext4 /dev/mapper/luks1 /data

cryptsetup -v status luks1 (status check)

vi /etc/crypttab

luks1 /dev/sdb

chown root:root /etc/crypttab

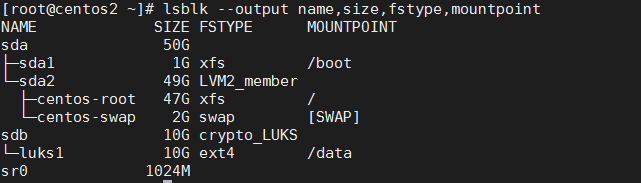
chmod 0744 /etc/crypttab

echo "/dev/mapper/luks1 /data ext4 defaults 0 2" >> /etc/fstab

(re encrypt)

umount /data

cryptsetup luksClose luks1



(changing passphrase)

cryptsetup luksChangeKey /dev/sdb

(adding extra key)

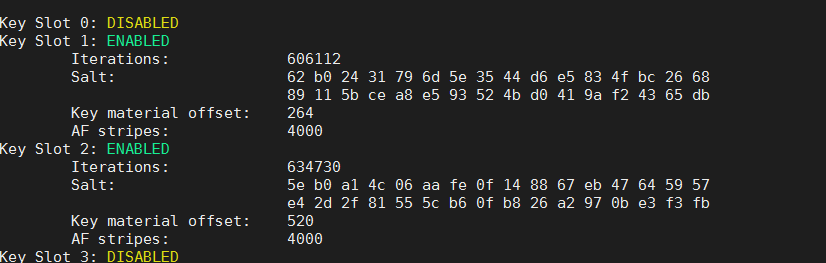
Find next available slot

cryptsetup luksDump /dev/sdb

cryptsetup luksAddKey --key-slot 2 /dev/sdb

(enter initial passphrase)

(then enter second key)



(backup luks header)

cryptsetup luksHeaderBackup /dev/sdb --header-backup-file /root/luks.backup

(restore)

cryptsetup luksHeaderRestore /dev/sdb --header-backup-file /root/luks.backup

-secondary passphrases should be recreated

**FILESYSTEM QUOTAS**

vi /etc/fstab >>>

/dev/sdb1 /mountdir ext4 defaults,usrjquota=aquota.user,grpjquota=aquota.group,jqfmt=vfsv0 0 0

quotacheck -avugm

quotaon -avug (turn on user and group quotas)

repquota /mountdir (kullanıcıların /mountdir üzerindeki kotalarını gösterir)

setquota -u "username" -F vfsv0 0 "quotainkbytes" 0 0 /dev/sdb1

edquota "username"> conf ile kullanıcı kotasını değiştirmek

setquota -g "groupname" -F vfsv0 0 "quotainkbytes" 0 0 /dev/sdb1

edquota -g "groupname"> conf ile kullanıcı kotasını değiştirmek

quotaoff -avug (turn off user and group quotas)

**FSFREEZE – DISABLING ACCESS TO FILE SYSTEM**

**/sbin/fsfreeze -f /data**

**/sbin/fsfreeze -u /data**

Wget options

wget -O “downloadname” “link” > link’teki dosyayı farklı isimle indirir

wget –i “file.txt” > file.txt ‘deki linklerden indirme yapar

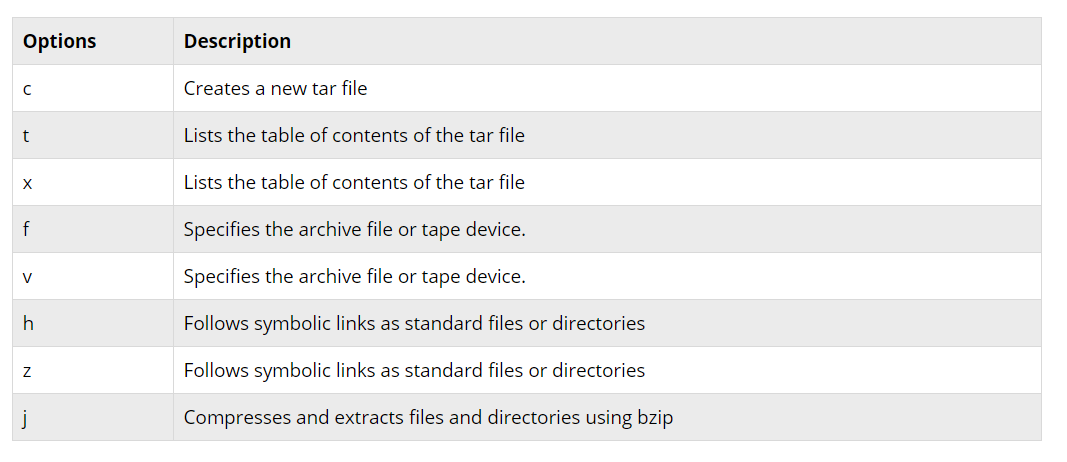
wget –c “link.iso” > büyük dosyaları indirirken kullanılır

wget –b “link” > linkdeki dosyayı background’da indirir /wget/log.txt’ye log’u atar

wget –c –limitrate=100k /wget/log.txt “link”

wget --http-user=username --http-password=password “link”

TAR



https://www.tecmint.com/18-tar-command-examples-in-linux/

tar -cvf /home/yaydog/Newfoldername.tar /etc : /etc klasörünü /home/yaydog altına newfolder isimiyle backup’lar

tar -xvf “Newfoldername.tar” -C /home/yaydog : backup’lanmış dosyayı farklı lokasyona cıkar

tar –tvf “Newfoldername.tar” : backup’lanmış dosyanın içeriğini gösterir

tar –xvf “Newfoldername.tar” –wildcards ‘\*.php’ : backup tan php uzantılı dosyaları çıkartır

tar –xvf “Newfoldername.tar” “file1” “file2” : backup’tan belirtilen dosyaları çıkartır

tar –rvf “Newfoldername.tar” file1.txt : backup a dosya eklemek

gzip format

tar -cvf /home/yaydog/Newfoldername.tgz /etc : /etc klasörünü /home/yaydog altına newfolder isimiyle backup’lar

**bzip2 Compression Format**

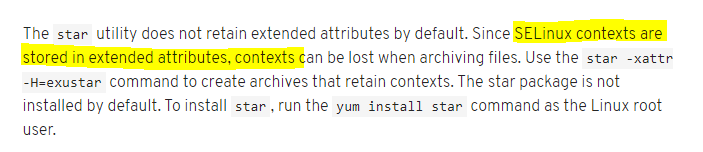
yum install bzip2

bzip2 -zk filename (compress file)

bzip2 -zk backup.tar (compress archive)

bzip2 -d filename.bz2 (decompress file)

**STAR**



star -xattr -H=exustar -c -f=test.star filename (archieve)

star -x -f=test.star (de-archieve)

**ZIP/UNZIP**

zip –r zipname.zip foldername/filename > archiving and compressing foldername folder to zipname (creates zip folder)

unzip> unzip zipname.zip

**GETTING SERVER SPEC**

uname -p: to identify atchitecture of the system (32bit or 64bit)

lscpu > cpu bilgileri

Architecture: x86\_64

CPU op-mode(s): 32-bit, 64-bit

Model name: Intel(R) Core(TM) i7-6700HQ CPU @ 2.60GHz

CPU MHz: 2591.607

CPU: 1

Core(s) per socket: 1

Socket(s): 1

Lsblk > disk information

free -m >

total used free shared buff/cache available

Mem: 1823 769 71 9 982 832

cat /etc/\*release\* > OS info (centos7)

cat /etc/redhat-release > OS info (centos6)

(hardware specs)

dmidecode –t system,baseboard,chassis,processor,memory,cache,connector,slot

dmidecode –t “number”

dmidecode | less

yum install pciutils -y

lspci (shows pci devices)

yum install usbutils -y

lsusb (shows attached usb devices)

(sending hardware errors to journalctl-machine check exception logging)

yum install mcelog -y

systemctl enable mcelog && systemctl start mcelog

journalctl -f -u mcelog.service

**PERFORMACE CO-PILOT** (COLLECT SYSTEM INFORMATION WITH METRICS)

yum install -y pcp pcp-system-tools

systemctl enable pmcd && systemctl start pmcd

showing all metrics: pminfo

metric values: pmval “value” (e.x pmval network.tcpconn.established)

(reading performance metrics in time)

systemctl enable pmlogger && systemctl start pmlogger

pmval network.tcpconn.established –a /var/log/pcp/pmlogger/$HOSTNAME/file

**Collecting Report About Server (SYSSTAT)**

yum install sysstat

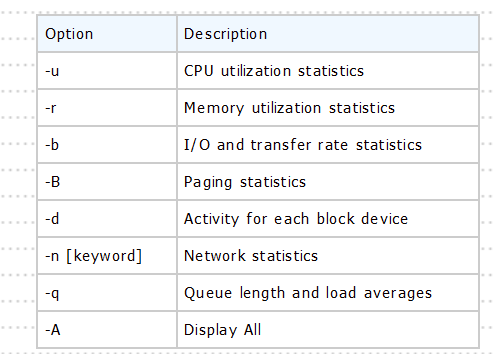
systemctl start sysstat

systemctl enable sysstat

config : vi /etc/sysconfig/sysstat AND /etc/cron.d/sysstat

Sysstat will log resource usage data into files in the /var/log/sa directory,

Sysstat will log resource usage data into files in the /var/log/sa directory, with new data being written every 10 minutes



Real-time statistics

sar -u 1 5 (1sec interval 5times)

sar -u -s 14:00:00 -e 15:00:00 -f /var/log/sa/sa27 >> cpureport.txt

sar -P ALL -s 14:00:00 -e 15:00:00 -f /var/log/sa/sa27 >>allcorecpureport.txt

sar -r -s 14:00:00 -e 15:00:00 -f /var/log/sa/sa27 sed memoryreport.txt

sar -b -s 14:00:00 -e 15:00:00 -f /var/log/sa/sa27 >> ioreport.txt

sar -q -s 14:00:00 -e 15:00:00 -f /var/log/sa/sa27 >> loadreport.txt

sar -S -s 14:00:00 -e 15:00:00 -f /var/log/sa/sa27 >> swapreport.txt

sar -W -s 14:00:00 -e 15:00:00 -f /var/log/sa/sa27 >> swapstats.txt

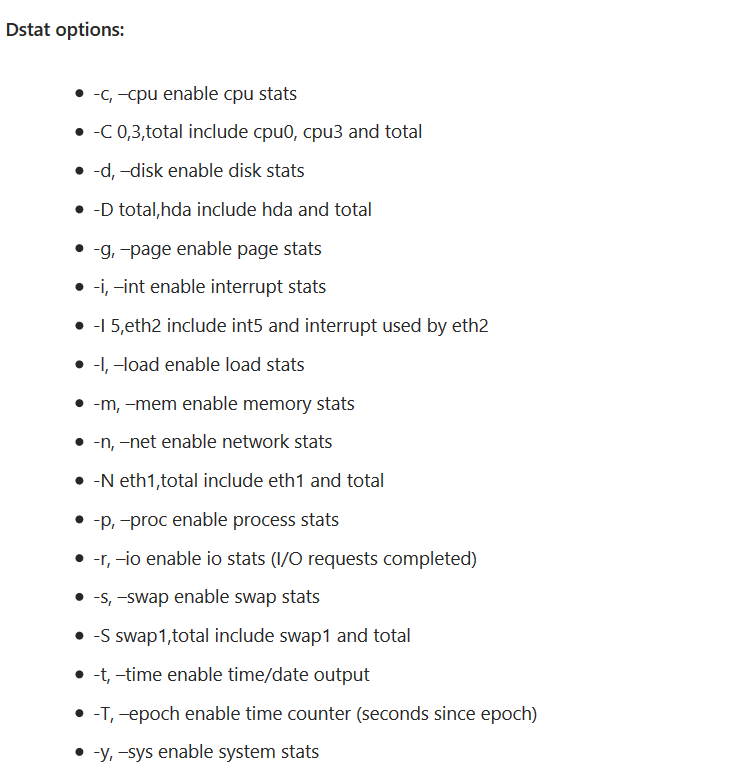
sar -n DEV -s 14:00:00 -e 15:00:00 -f /var/log/sa/sa27 >> networkstats.txt

sar -A -s 14:00:00 -e 15:00:00 -f /var/log/sa/sa27 >> allreport.txt

**Collecting Report About Server (DSTAT)**

yum install -y dstat

dstat --help



dstat -tcdm --output dstat.csv (ON REAL TIME REPORTING)

**OTHER UTILIZATION TOOLS**

htop

iostat : input/output statistics for devices and partitions

pidstat:

yum install nmon : all statistics (realtime)

yum install -y gnome-system-monitor : GUI tool like task manager

**SOSREPORT**

Sosreport is required when you have open a case with redhat for technical support. Redhat support Engineers will require sosreport of your server for troubleshooting purpose.

yum install sos -y

(listing modules) sosreport -l

sosreport -n module1 module2 --tmp-dir /var/log

**REPO**

yum list installed (shows all installed packages and from which repo)

yum list installed | grep @epel >> rpms installed from epel repo

yum list available | grep epel>> shows all packages from repo

**download all packages from repo**

rpm -ivh yum-repo-sync-2.0-0.noarch.rpm

mkdir /root/repo

(examples)

reposync -r epel -p /root/repo &

reposync -r remi -p /root/repo &

reposync -r remi-php70 -p /root/repo &

reposync -r percona-release-noarch -p /root/repo &

(giving priority to repos)

/etc/yum.repos.d/reponame1

Priority=1

/etc/yum.repos.d/reponame2

Priority=2

**CREATING CUSTOM REPO**

**.repo file format**

vi /etc/yum.repos.d/test.repo

[test]

name=

baseurl=

mirrorlist=

failovermethod=priority

enabled=1

gpgkey=

gpgcheck=0

yum clean all

yum repolist all (shows enabled and disabled repos)

yum repolist enabled (shows only enabled repos)

**show packages from only one repo**

yum search --disablerepo=\* --enablerepo=”reponame” “packagename”

**download only from one repo**

yum install --enablerepo=”reponame” “packname”

**SELINUX**

Sestatus> selinux status

Setting Selinux=disabled

vi /etc/sysconfig/selinux : disabled

SELINUX=disabled

reboot

sestatus

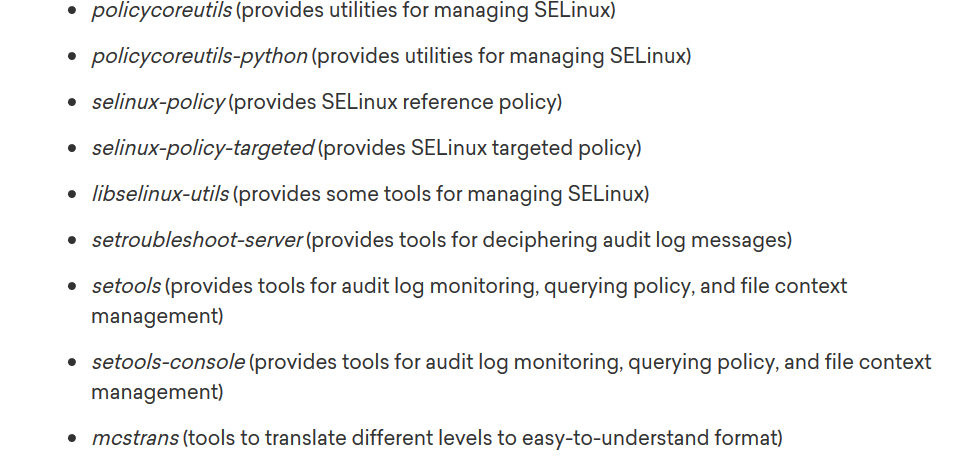
Setting Selinux=permisive

vi /etc/sysconfig/selinux : permissive

setenforce 0

reboot

**SELINUX ADVANCED**



yum install policycoreutils policycoreutils-python selinux-policy selinux-policy-targeted libselinux-utils setroubleshoot-server setools setools-console mcstran

Selinux logs : cat /var/log/messages | grep "SELinux"

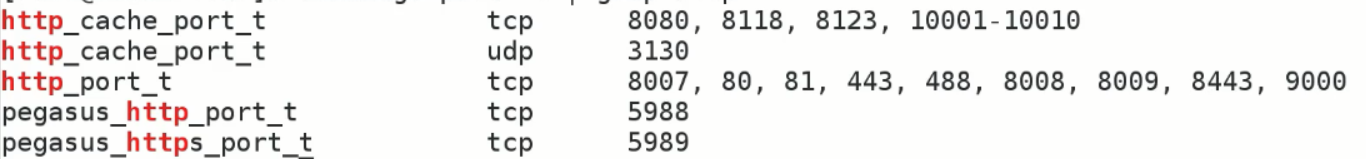
**Selinux Gui**

yum install policycoreutils-gui

system-config-selinux

Selinux-services and ports

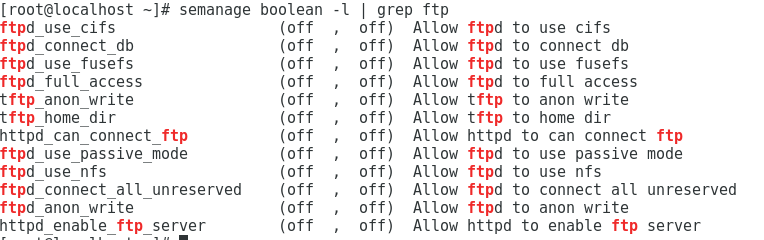
semanage port -l |grep “servicename” > shows which ports are enable in selinux



semanage port -a -t http\_port\_t -p tcp “portnumber” : enable port in selinux

Boolean values

semanage boolean -l | grep “servicename”



setsebool -P “parameter” on/off

security context

ls -lZ “filename”

(example)

-rw-r--r--. root root system\_u:object\_r:etc\_t:s0 /etc/yum.conf

Highlighted is security context seperated by :

1st part: user context

2nd part: selinux role

3rd part: type of file

4th part: sensitivity of resource

Security context of service

ps -efZ | grep “servicename”

Restoring security context

restorecon -vRF /test/\*

Permissive domain

semanage permissive -a mysqld\_t

SELINUX POLICY VIOLATIONS DIAGNOSE

yum install -y setroubleshoot-server

sealert -a /var/log/audit/audit.log

**grep “auditnumber” /var/log/audit/audit.log | audit2why**

GRUB BOOTLOADER

Load OS core

(configuration)

/boot/grub/grub.conf

file “document” > shows format of a file

which cmd> komutun tam yol bilgisini verir

w,who,whoami> logged on users

who -m(ip and terminal info) –r(user run level)

write “username” “terminal name” (sending message from terminal)

uptime> system uptime and under which users

locate filename > find where is the file

/etc/cron.daily/mlocate>> manual indexing

LS (ls –lah)

File:/// browser (finding file from browser)

-l >> list with details

-a >> show also hidden files

-R>> recursively search

-S>> dosya buyuklugune göre sırala

-F>> dosya türüne göre işaret vererek sıralar

-d >> kritere göre dosyaları sıralar

-o >> dosya izinlerini göstermez

-h >> dosya boyutlarının mb,kb cinsinden ayırır

(detailed info about sub folders)

yum install tree

cat -n “filename” : satır numaraları ile gormek

Cat text1.txt text2.txt > newfile.txt (merge files)

head -n 2 filename.txt > shows top 2 of the file (default:10)

tail -n 2 filename.txt > shows top 2 of the file

split –l 5 originalfile.txt newfile (divide original file into 5)

wc -l filename> prints number of lines

wc -m filename> prints number of characters

string search

grep <parametre> searchname “içinde aranılan dosya”

grep -i:not sensitive to upper or lower case

grep –r: checks subfiles as well

grep -n: shows row line

grep -c: shows repat time

touch> create empty file, update timestamp

File remove: rm file1 file2

File move: mv filelocation folderlocation

Directory remove: rm –rf dir1(without prompt)

Directory move: mv dir folderlocation

File copy:cp filelocation newfilelocation (cp file1 file2 file3 path)

File copy(including hidden file) cp /path/. newlocation

Folder copy: cp -r dir1 dir2 path

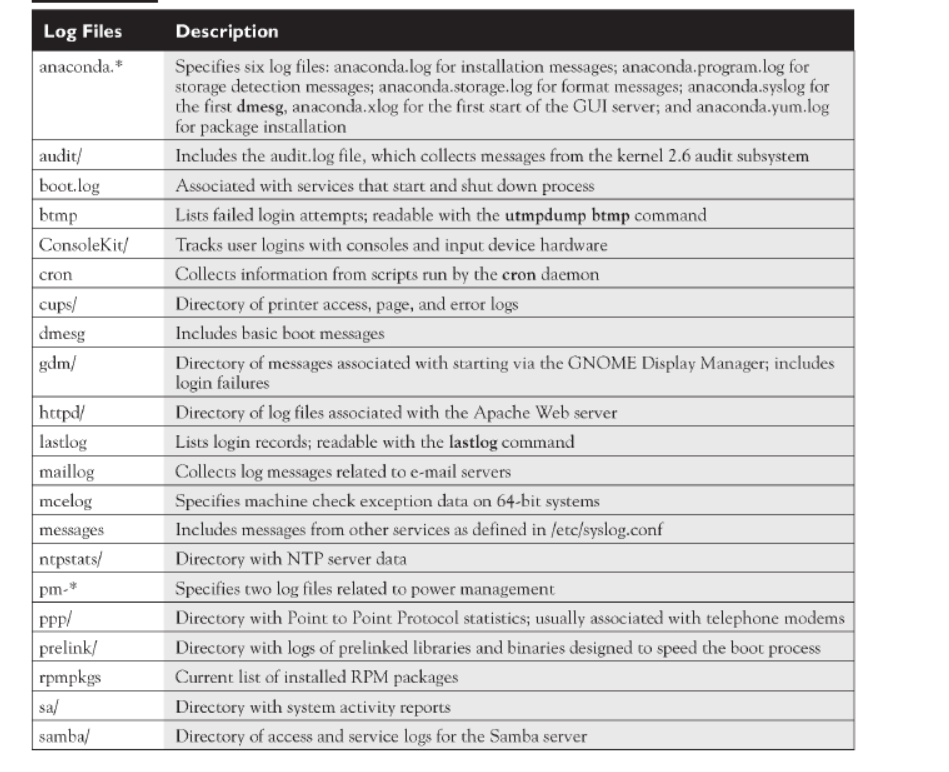
Folder create:Mkdir dir1 dir2

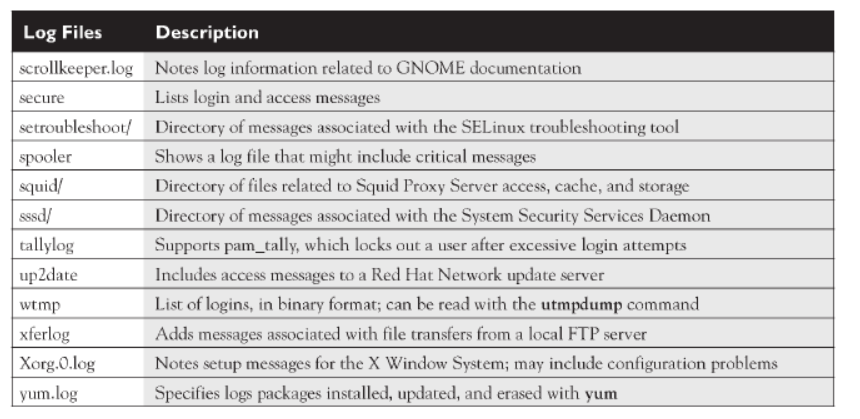
Folder create with extensions: mkdir -p dir1/dir2

**Log files**

/var/log > log files are stored here

/var/log/messages > system logs (tail –f /var/log/messages)





**GUI tools to view log files**

yum install gnome-system-log

gnome-system-log

vi /etc/logrotate.conf log rotate settings

(display which process is accessing to log files)

Lsof +d /var/log

TRACING AND ALERTING LOGFILES (LOGWATCH)

Logwatch is a Perl-based log management tool for analyzing, summarizing, and reporting on a server’s log files. It is most often used to send a short digest of server’s log activity to a system administrator

yum -y install logwatch mailx

(configure mailx)

/usr/share/logwatch/scripts/services>> all services that logwatch cover

/usr/share/logwatch/default.conf/logwatch.conf

LogDir = /var/log

Format = html (report format)

MailTo =

MailFrom =

Range = Today ( alternative: --range 'between 14 days ago and yesterday')

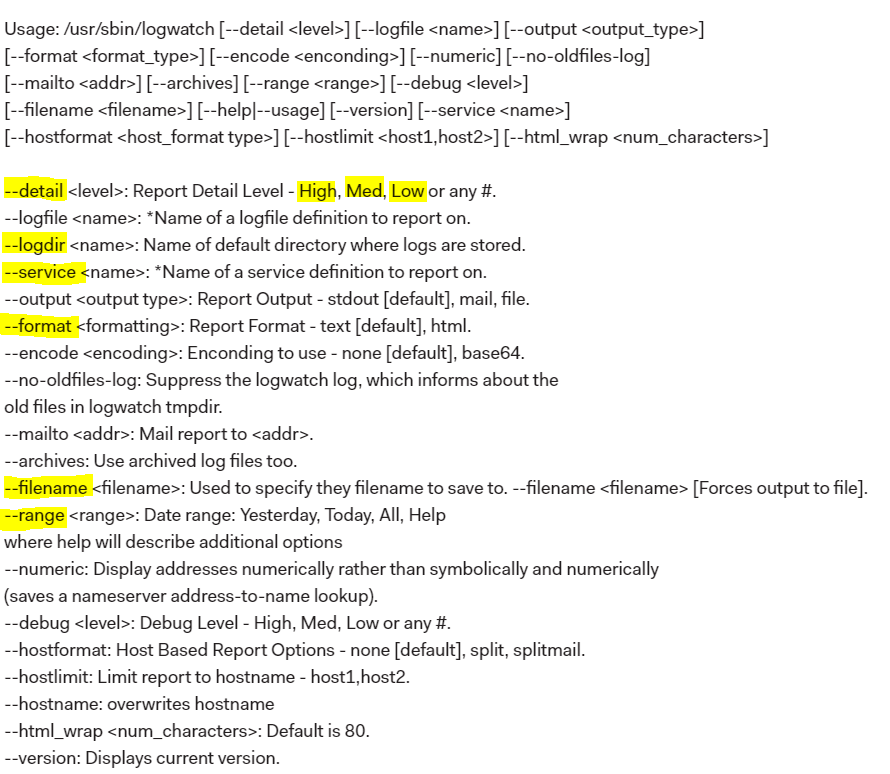
Detail = Low or Medium or High

Service= All or choose from /usr/share/logwatch/scripts/services

DailyReport=No

crontab entry

\* \* \* \* \* /usr/sbin/logwatch



Creating manual reports

/usr/sbin/logwatch --detail Low --filename report.html --service All --range today --format html --logdir /var/log && echo "Daily Log File Report is attached" | mail -a /root/report.html -s "LogFile Analysis" [e-mail@e-mail.com](mailto:e-mail@e-mail.com) && rm -rf /root/report.html

**JOURNALCTL**

journalctl -r : display the newest log entries

journalctl -n [number]: display specific number of most recent log files

journalctl –p debug/info/notice/warning/err/crit/alert/emerg

journalctl -u ntpd,httpd… (systemd unit)

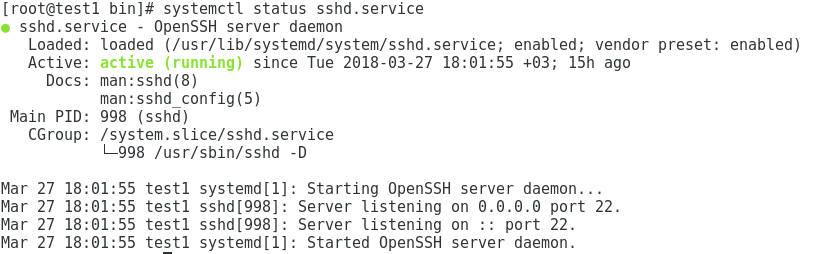
journalctl --since "2015-01-10" --until "2015-01-11 03:00"

journalctl \_PID=8088

journalctl -k (kernel messages)

SERVICES

Finding services and ports



List status of all services> systemctl list-unit-files --type=service

/usr/lib/systemd/system >>> servicename.service

(shows all enabled and disable services)

**MASKING A SERVICE (FOR ACCIDENT START OF SERVICE)**

systemctl mask httpd



**SHOWING DEPENDENCIES OF SERVICE (all possiblities)**

systemctl list-dependencies servicename

**RESTARTING SERVICE WITHOUT AFFECTING CURRENT CONNECTIONS**

systemctl reload servicename

All ports and correspondance

cat /etc/services

yum install lsof

lsof -i :portnumber

lsof –i:range1-range2

lsof –i: shows open connections

**NETWORK SCANNING**

yum install nmap

GUI>>> zenmap

<https://www.linuxhelp.com/how-to-install-zenmap-on-centos-7/>

nc -vz <HOST> <PORT>

SYSTEM VULNERABILITY SCANNING

NESSUS

Processes

Processid numarasını bulmak >> pidof “servicename”

ps

see all processes: ps ax --sort

display processes belongs to user: ps –u “username” ; top –u “username”

ps aux | grep ‘processname’

child processes >> ps -o “servicename”

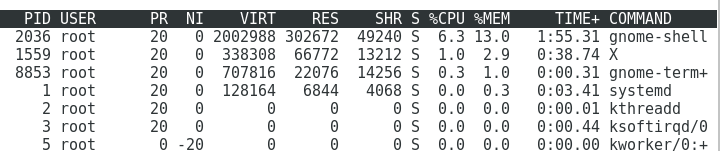
Vmstat> sistemin genel durumunu görmek

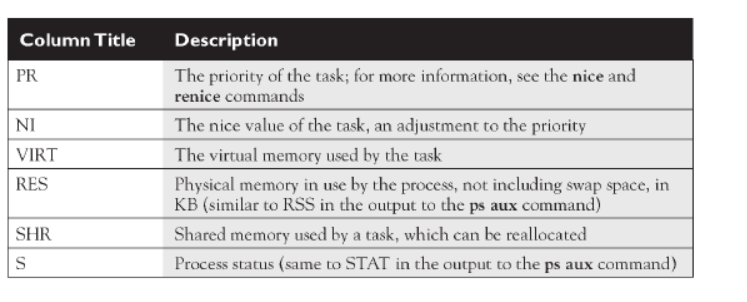
Pstree –p : process tree

/proc/cpuinfo

**Memory segments of processes: Process information can be found in the /proc filesystem. All process IDs get their own directory, so if you want process ID 324, you would go to /proc/324.**

Top>interactive live display of processes (refresh rate 3sec)





PR: kernel priority

NI:nice level (user level)

S:status

R: running

S: suspend

T: stop

Z: zombi

Free> shows free memory

**TOP 10 PROCESSES BY CPU**

ps aux --sort -pcpu | head

**TOP 10 PROCESSES BY MEMORY**

ps aux --sort -rss | head

**Signals**

Sighup number:1 description:Hangup kill -1 processid (restarts service)

Sigint number:2 description:interrupt ctrl+c or kill -2 processid

Sigkill number:9 description:kill kill -9 processid

Sigterm number:15 description:terminate kill -15 processid

Killall –i pid/processname

Killall –signalnumber processname

pgrep –l “process” : Finding PID from process name

pgrep –lu username: kullanıcıya ait olan süreçler

pgrep –af processnameshortcut: finding PID

priority levels (nice level NI)

öncelikli tanımlanmış işleri listelemek : ps -al

-20 0 19

Higher default lower

Renice number –p processnumber > process’in nice level’ını change

**DEBUGGING PROCESS**

yum install strace ltrace -y

strace -p PID

ltrace -p PID

Networking

GUI: nm-connection-editor

ping -c 3 IP > sends 3 ping packages

ping -i “interval” > send ping with interval(seconds)

Yum install whois

yum install -y traceroute

traceroute

İfconfig

**STATIC ROUTING**

yum -y install net-tools

route -n >> routing table of local system

ip route show or ip route list>> routing table of local system

(static)

ip route add 172.16.5.0/24 via 192.168.1.4 dev ens33

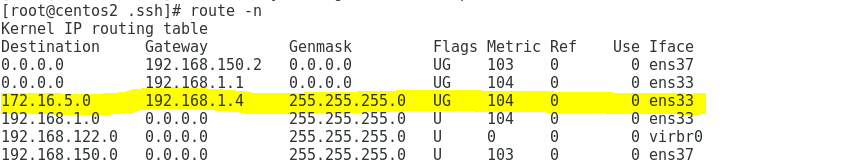
ip route del 172.16.5.0/24 via 192.168.1.4 dev ens33

(persistent)

vi /etc/sysconfig/network-scripts/route-ens33

172.16.5.0/24 via 192.168.1.4 dev ens33

route -n (or netstat -rn)

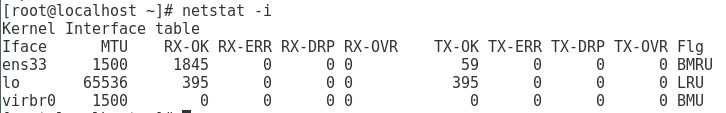


Set IP address> ifconfig eth0 192.168.1.12 netmask 255.255.255.0

Setting DHCP> dhclient eth0

ifconfig “interfacename” up/down

netstat -i



Restart network interface > systemctl restart network

systemctl status network

Host file > /etc/hosts

Creating new connection (Network manager)

nmcli connection add con-name rhcsa ifname DEVICENAME type ethernet

nmcli connection delete id rhcsa

vi /etc/sysconfig/network-scripts/ifcfg-rhcsa

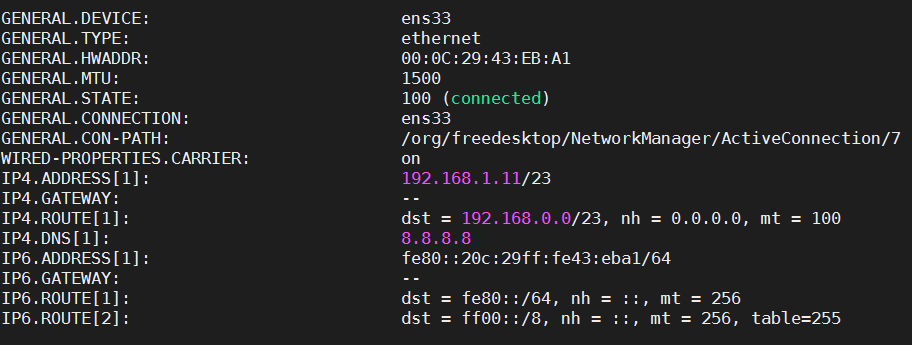
nmcli connection up rhcsa

nmcli connection down rhcsa

nmcli connection show



nmcli d show



systemctl restart NetworkManager

systemctl enable NetworkManager

**CONFIGURING STATIC IP**

vi /etc/sysconfig/network-scripts/ifcfg-\*

TYPE=”Ethernet”

BOOTPROTO=”none”

DEFROUTE=”yes” (binary yes/no directive for default route on defined by route -n)

IPV4\_FAILURE\_FATAL=”no” (binary directive supporting network failure if there is an error)

IPV6INIT=”no”

IPV6\_AUTOCONF=”no”

IPV6\_DEFROUTE=”no”

IPV6\_FAILURE\_FATAL=”no”

IPV6\_ADDR\_GEN\_MODE=”stable-privacy”

NAME=”ens33”

UUID=”ce79746a-d633-4577-a446-e095bb2fb09f”

DEVICE=”ens33”

ONBOOT=”yes”

DNS1=

DNS2=

DOMAIN=

IPADDR=

NETMASK=

GATEWAY=

CONFIGURING DHCP BASED

BOOTPROTO=”DHCP”

No IPADDR and NETMASK

**Defining gateway and hostname**

vi /etc/sysconfig/network

NETWORKING=YES (if it is no /etc/init.d/network script does not activate network devices)

NETOWRKING\_IPV6=YES

network 0:off 1:off 2:on 3:on 4:on 5:on 6:off

**DNS**

/etc/resolv.conf

Search domainname

name server dnsserverIP

**HOSTNAME**

/etc/hostname : holds hostname

systemctl restart systemd-hostnamed (change hostname withuot logout)

Network connections

netstat -tuna

netstat -lntu >> active tcp connections

netstat

-t: tcp only

-u: udp only

-s: active ports

(PORT-APPLICATION MAPPING)

Netstat –ap | grep “uygulamaadı” : uygulama > port

Netstat –an |grep “portnumber” : port> uygulama

IPV4 Forwarding

cat /proc/sys/net/ipv4/ip\_forward : current state

sysctl -w net.ipv4.ip\_forward=1 (enable)

sysctl -w net.ipv4.ip\_forward=0 (disable)

**LOGIN TIMES OF USERS**

yum install psacct -y

systemctl enable psacct

systemctl start psacct

ac -d root : prints the day-wise total login time of user “**root**” in hours.

**CONFIGURING ONLY IPV6 FOR SINGLE INTERFACE**

vim /etc/sysconfig/network

NETWORKING\_IPV6=yes

sysctl -w net.ipv6.conf.default.disable\_ipv6=0

sysctl -w net.ipv6.conf.all.disable\_ipv6=0

vi /etc/sysconfig/network-scripts/ifcfg-ens33

TYPE="Ethernet"

PROXY\_METHOD="none"

BROWSER\_ONLY="no"

BOOTPROTO="static"

DEFROUTE="yes"

IPV4\_FAILURE\_FATAL="no"

IPV6INIT="yes"

IPV6\_AUTOCONF="no"

IPV6\_DEFROUTE="yes"

IPV6\_FAILURE\_FATAL="no"

IPV6\_ADDR\_GEN\_MODE="stable-privacy"

NAME="ens33"

UUID="317a83c8-c584-4772-99e8-6aebba6c33f2"

DEVICE="ens33"

ONBOOT="yes"

DNS1="8.8.8.8"

DNS2="192.168.1.3"

IPV6ADDR=2001:1:1:1443::434/122

IPV6\_DEFAULTGW=2001:1:1:1443::43f

systemctl restart network

(testing)

ping6 -c [Count] -I [Interface] [Destination Address/Hostname]

**CONFIGURING IPV4+IPV6 FOR SINGLE INTERFACE**

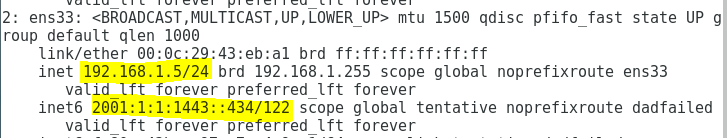
İpv4 on ens33 (available)

nmcli connection modify ens33 ipv6.addresses 2001:1:1:1443::434/122 ipv6.method manual

vi /etc/sysconfig/network-scripts/ifcfg-ens33

IPV6\_DEFAULTGW=2001:1:1:1443::43f

systemctl restart network



**CREATING FOR BEGINING (IPV4+IPV6)**

nmcli con add con-name eth1 type ethernet ifname eth1

nmcli con mod eth1 ipv4.addresses 192.168.1.2/24

nmcli con mod eth1 ipv4.method manual

nmcli con mod eth1 ipv6.addresses 2001:1:1:1443::434/122

nmcli con mod eth1 ipv6.method manual

nmcli con up eth1

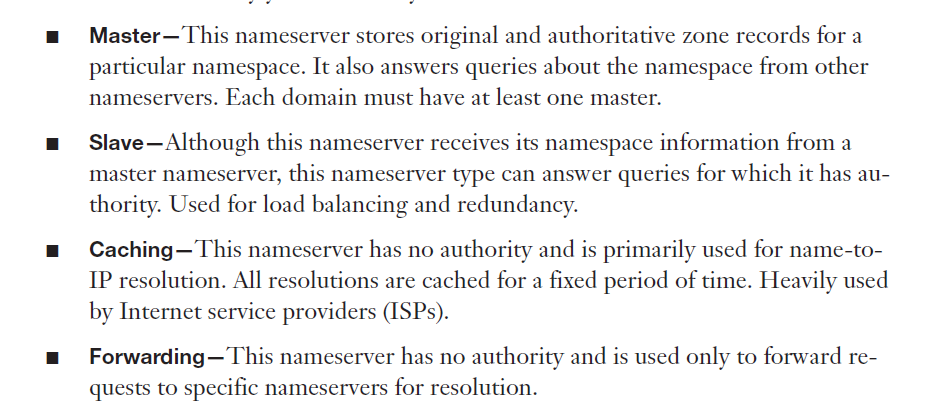
**NETWORK PACKET CAPTURE on port**

yum install tcpdump -y

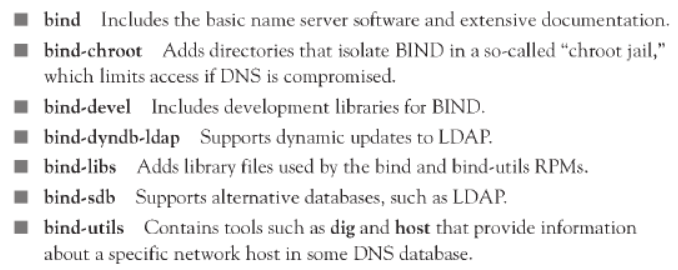
tcpdump -i ens33 -w /root/tcpdump.pcap 'port 80'

tcpdump -r /root/tcpdump.pcap (reading)

**BIND DNS SERVER**



(important packages)



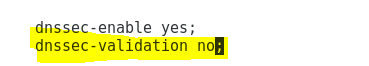
**Caching-Only DNS Server**

**(non authoritive, doesnt hold records for zones)**

yum install bind bind-utils bind-chroot -y

vi /etc/named.conf





named-checkconf (check sytanx)

semanage fcontext -a -t named\_conf\_t /etc/named.conf

semanage fcontext -a -t named\_conf\_t /etc/named.rfc1912.zones

firewall-cmd --permanent --add-port=53/udp

firewall-cmd --reload

systemctl restart named

systemctl enable named

ln -s /etc/named.conf /var/named/chroot/etc/named.conf

(on client)

vi /etc/resolv.conf ve vi /etc/sysconfig/network-scripts/ifcfg-ens33 >> dns sunucu girilir

(testing on server)

nslookup facebook.com 127.0.0.1

(testing on client)

yum install bind-utils

dig facebook.com

dig @DNSSERVERIP facebook.com

nslookup facebook.com DNSSERVERIP

telnet DNSSERVERIP 53

**MASTER DNS SERVER (test5.example.com 192.168.1.175)**

vi /etc/named.conf

options {

listen-on port 53 { 127.0.0.1;192.168.1.175; };

directory "/var/named";

dump-file "/var/named/data/cache\_dump.db";

statistics-file "/var/named/data/named\_stats.txt";

memstatistics-file "/var/named/data/named\_mem\_stats.txt";

allow-query { 127.0.0.1;192.168.1.175; 192.168.1.173; };

recursion yes;

dnssec-enable no;

dnssec-validation no;

/\* Path to ISC DLV key \*/

bindkeys-file "/etc/named.iscdlv.key";

managed-keys-directory "/var/named/dynamic";

pid-file "/run/named/named.pid";

session-keyfile "/run/named/session.key";

};

logging {

channel default\_debug {

file "data/named.run";

severity dynamic;

};

};

Zone "example.com" IN {

type master;

file "example.com.zone";

also-notify {192.168.1.173;};

allow-transfer {192.168.1.173;};

};

Zone "1.168.192.in-addr.arpa" IN {

type master;

file "example.com.revzone";

also-notify {192.168.1.173;};

allow-transfer {192.168.1.173;};

};

include "/etc/named.rfc1912.zones";

include "/etc/named.root.key";

vi /var/named/example.com.zone (Forward LookupZone)

$TTL 86400

@ IN SOA example.com. root.example.com. (

2017092101 ; serial (d. adams)

3H ; refresh

15M ; retry

1W ; expiry

1D ) ; minimum

IN NS test5.example.com.

IN NS test4.example.com.

IN MX 5 smtp.example.com.

test5.example.com. IN A 192.168.1.175

test1.example.com. IN A 192.168.1.170

test3.example.com. IN A 192.168.1.172

test4.example.com. IN A 192.168.1.173

vi /var/named/example.com.revzone (reverse lookup zone)

$TTL 86400

@ IN SOA example.com. root.example.com. (

2017092101 ; Serial

28800 ; Refresh

14400 ; Retry

3600000 ; Expire

86400 ) ; Minimum

NS test5.example.com.

175 IN PTR test5.example.com.

170 IN PTR test1.example.com.

172 IN PTR test3.example.com.

173 IN PTR test4.example.com.

**SLAVE DNS SERVER (test4.example.com 192.168.1.173)**

vi /etc/named.conf

options {

listen-on port 53 { 127.0.0.1;192.168.1.173; };

directory "/var/named";

dump-file "/var/named/data/cache\_dump.db";

statistics-file "/var/named/data/named\_stats.txt";

memstatistics-file "/var/named/data/named\_mem\_stats.txt";

allow-query { 192.168.1.0/24; };

recursion yes;

dnssec-enable no;

dnssec-validation no;

/\* Path to ISC DLV key \*/

bindkeys-file "/etc/named.iscdlv.key";

managed-keys-directory "/var/named/dynamic";

pid-file "/run/named/named.pid";

session-keyfile "/run/named/session.key";

};

logging {

channel default\_debug {

file "data/named.run";

severity dynamic;

};

};

Zone "example.com" IN {

type slave;

masters {192.168.1.175;};

file "slaves/db.example.com.zone";

};

Zone "1.168.192.in-addr.arpa" IN {

type slave;

masters {192.168.1.175;};

file "slaves/db.example.com.revzone";

};

include "/etc/named.rfc1912.zones";

include "/etc/named.root.key";

**FORWARDING DNS SERVER**

192.168.1.180: origianal server

options {

listen-on port 53 { 127.0.0.1;192.168.1.180;};

directory "/var/named";

forwarders

{

192.168.1.145;

};

dump-file "/var/named/data/cache\_dump.db";

statistics-file "/var/named/data/named\_stats.txt";

memstatistics-file "/var/named/data/named\_mem\_stats.txt";

recursing-file "/var/named/data/named.recursing";

secroots-file "/var/named/data/named.secroots";

allow-query { localhost;192.168.1.0/24; };

recursion yes;

dnssec-enable yes;

dnssec-validation yes;

/\* Path to ISC DLV key \*/

bindkeys-file "/etc/named.iscdlv.key";

managed-keys-directory "/var/named/dynamic";

pid-file "/run/named/named.pid";

session-keyfile "/run/named/session.key";

};

logging {

channel default\_debug {

file "data/named.run";

severity dynamic;

};

};

zone "." IN {

type hint;

file "named.ca";

};

include "/etc/named.rfc1912.zones";

include "/etc/named.root.key";

Check configuration file syntax

named-checkconf /etc/named.conf (geriye birşey dönmüyorsa ok)

**DHCP**

yum install -y dhcp

chkconfig dhcpd on

service dhcpd start

cat /var/lib/dhcpd/dhcpd.leases (atanan IP adresleri gösterilir)

cp /usr/share/doc/dhcp-4.2.5/dhcpd.conf.example /etc/dhcp/dhcpd.conf

vi /etc/dhcp/dhcpd.conf

# Global Options

ddns-update-style none; #This means that the DHCP server won’t update client DNS

authoritative; #This informs the client that the DHCP server contains legitimate information.

option domain-name "example.com";

option domain-name-servers 192.168.1.175,8.8.8.8;

default-lease-time 600;

max-lease-time 7200;

subnet 192.168.1.0 netmask 255.255.255.0 {

range 192.168.1.200 192.168.1.220;

option routers 192.168.1.1;

}

#fixed ip to client

host client01 {

option host-name "client01.example.com"

hardware ethernet 08:00:07:26:c0:a5;

fixed-address 192.168.1.222;

}

**SSH**

Currently installed ssh version: ssh -V

yum install openssh-server openssh-clients

sytemctl enable sshd

firewall-cmd --permanent --add-port=22/tcp

firewall-cmd –permanent --reload

man sshd

configuration file > vi /etc/ssh/sshd\_config (server)

vi /etc/ssh/ssh\_config (client)

<https://www.ssh.com/ssh/sshd_config/>

vi /etc/ssh/sshd\_config (server)

AllowUsers \*@IP (allow specific people)

DenyUsers \*@IP Port 22 (deny specific people)

ListenAddress (listening IP for ssh)

Protocol 2 (more secured)

**LoginGraceTime** (The time after which the server disconnects if the user has not successfully logged in)

LogLevel INFO

PermitEmptyPassword no

PermitRootLogin yes (is root user allowed to ssh or not)

Banner /root/banner (banner info)

PrintMotd yes (display message in /etc/motd after ssh login)

(full syntax)

ssh root@IP -p “portnumber”

semanage port -a -t ssh\_port\_t -p tcp 1028 (ssh different port set selinux)

**WELCOME MESSAGE**

Scripted welcome message

vi /etc/ssh/sshd\_config

PrintMotd no

vi /etc/profile.d/message.sh

#!/bin/bash

#

echo -e "

###################################

#

# Welcome to `hostname`

# This system is running `cat /etc/redhat-release`

# kernel is `uname -r`

#

# You are logged in as `whoami`

# Company Name

#

############################

"

tail -f /var/log/secure

**Key-based Auth Only**

Password’less SSH

A >> B

userA userB

A: ssh-keygen (root/.ssh/id\_rsa ‘a key’i atar, 2048-bit RSA key pair, id\_rsa ve id\_rsa.pub)

A: ssh-copy-id userB@ipofB id\_rsa.pub’ı karşı makinenin home directorysinde .ssh altında authorized keye’e atar)

(disable password auth)

vi /etc/ssh/sshd\_config

PasswordAuthentication no

File transfer

scp /home/yaydog/file.txt root@targetip:/home/yaydog

Folder transfer

scp -r /home/yaydog/folder root@targetip:/home/yaydog

SFTP connection

Sftp root@destinationip

File transfer from remote host > get remotefilelocation localpath (get –r : folder transfer)

File transfer to remote host> put localfilelocation remotepath

**WEBMIN PANEL**

Webmin installation

wget https://prdownloads.sourceforge.net/webadmin/webmin-1.920.tar.gz

tar -xvf webmin-1.920.tar.gz

cd webmin-1.920

./setup.sh

File permissions

Owned by user, belongs to user

R:read

W:write

X:execute

r(4)w(2)x(1) r(4)w(2)x(1) r(4)w(2)x(1)

user group other

[root@centostest ~]# **getfacl** file2

# file: file2

# owner: root

# group: root

user::rw-

group::r--

other::r--

**COLLABORATIVE GROUP**

chown -R root:groupname foldername

chmod 2770 foldername: bu folder altında oluşturulan her dosyanın ownership’i groupname olur

chmod +t foldername (groupname içerisindeki kullanıcılar birbirlerinin dosyasını gorebilir ama silemez)

chown user:group filename>> changing belongings of file

chown **-R** user:group foldername>> changing belongings of folder recursively

Only user owner of the file and root can change file and folder permissions

chmod ugo+-rwx filename

**FİLE AND FOLDER ATTRIBUTES**

chattr +i filename : file cant be deleted

chattr -i filename : file can be deleted

LSATTR : display file attributes

**ACL FILE PERMISSIONS (-R recursively)**

(user based permissions)

setfacl -m u:testuser:rwx /root

setfacl -m g:testgroup:rwx /root

(removing all acl permissions from user)

setfacl -m u:testuser:--- /root

(remove all acl permission)

setfacl -b /root

id>info about user

sudo>do command with root priviledges

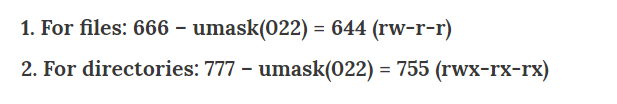
etc/passwd >> user and service accounts

UMASK

UID >200 : umask=002

UID<200: umask: 022 dir.

root umask: 022



Standard user umask: 002

For files: 666-002=664 rw- rw- r--

For directories: 777-002=775 rwx rwx r-x

kullanıcı islemleri

GUI: yum install system-config-users

/etc/passwd : user info

Display all users on system > awk -F':' '{ print $1}' /etc/passwd

/etc/shadow: passwd info

/etc/group : groupların isimleri ve id’leri

User with interactive shell

useradd <username> -d /home/username -m(creates home directory) -s /bin/bash(defines user shell) -c (comment) -e (YYYY-MM-DD:expiry date) -u (user idsi) -g(group id) -G (group1,group2)

user without interactive shell

useradd <username> -d /home/username -m(creates home directory) -s /sbin/nologin -c (comment) -e (YYYY-MM-DD:expiry date) -u (kullanıcı idsi) -g(group id) -G (group1,group2)

chfn “username” : user identification card (Display Name)

DISPLAY LOGGED ON USER TO SYSTEM:

utmpdump /var/log/wtmp

lslogins -u

(creating users directory manually)

sudo mkhomedir\_helper username

userdel -r username : deletes user with home folder

usermod -c(changes comment line) -e (expiry date change) -s (change shell) -L (locks useraccount) -U (unlocks useraccount) -g (grupidsini değiştirir) “username”

gpasswd -a username groupname1 groupname2 >> adding user to groups

gpasswd -d username groupname1 groupname2 >> removing user from groups

Adding superuser(sudoer)= gpasswd -a username wheel

(adding user to wheel group)

Visudo

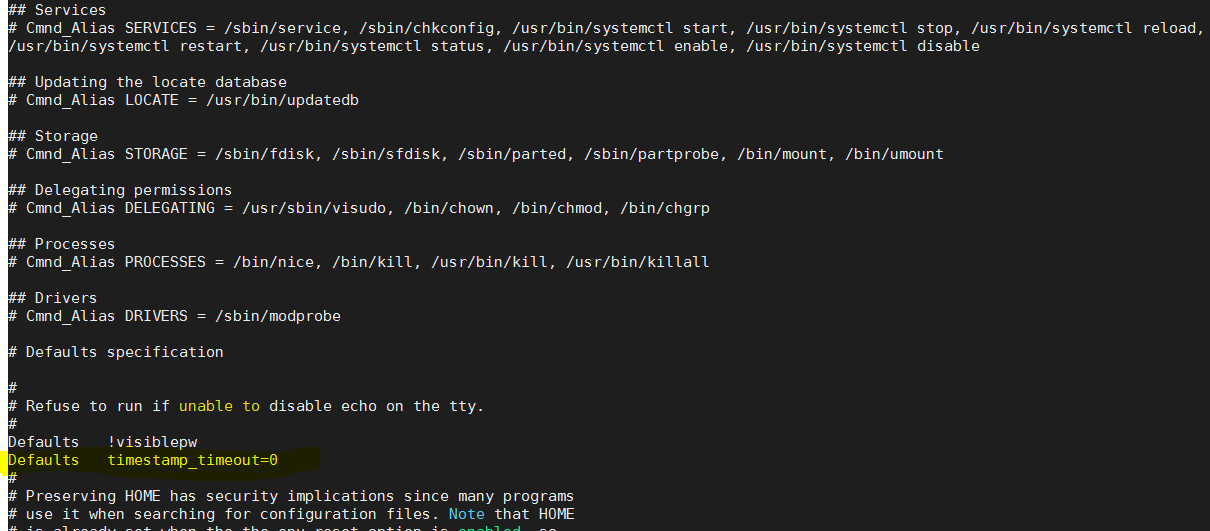
(executing command without password for wheel group users or sudoers)

%wheel ALL=(ALL) ALL

%wheel ALL=(ALL) NOPASSWD: ALL

CHANGING TIME OUT PERIOD OF SUDO (default 5min)

visudo



şifre işlemleri

passwd –l (lock user password) -u(unlock user password) –d (deletes user password) –n (min day of user password before expire) –x (max day of user password before expire) –w(password notification warning duration before expire) “username”

passwd username> change passwords

groupadd -g GUID number “groupname”

groupmod newname oldname : changes group name

cat /etc/group >> shows groups

cat /etc/passwd

USER:x:USERID:GROUPID:DISPLAYNAME:/HOMEFOLDER:/bin/bash

**(user cannot login to system via ssh or console)**

usermod “username”-s /sbin/nologin

**migrate local users and groups from one system to another system**

<https://access.redhat.com/solutions/179753>

**PAM MODULE**

(pam aware applications configuration files are located in)

/etc/pam.d

yum install -y pam-devel

**Account Lockout Policy**

locks after 3 trial for 600 seconds

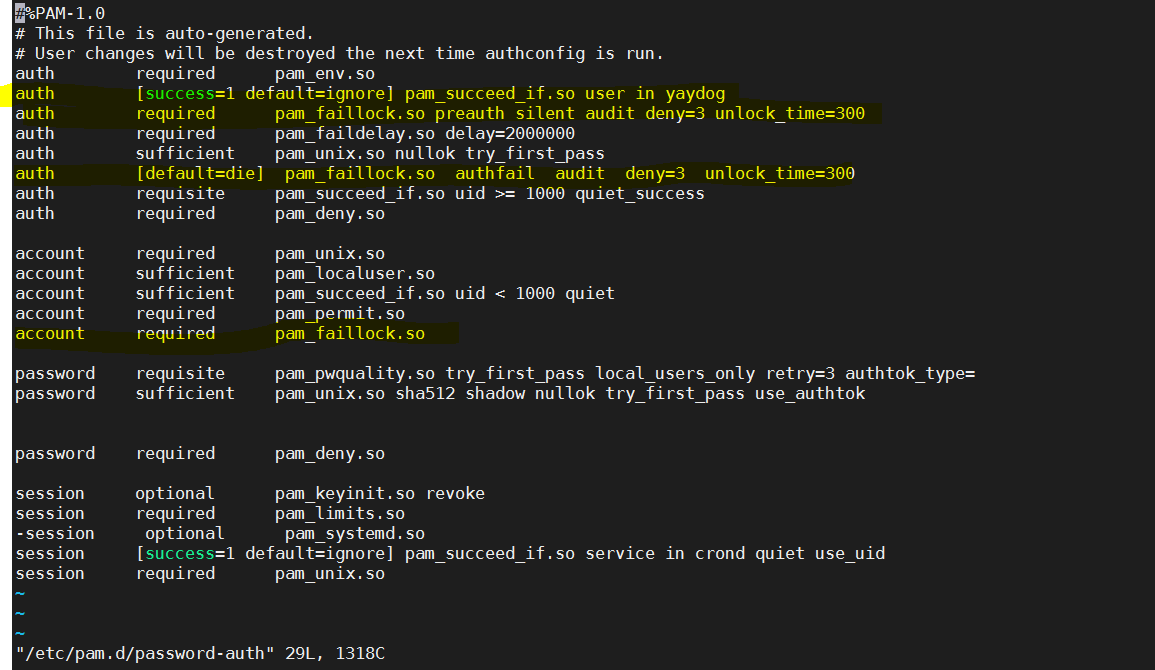
(unlocking useraccount)

faillock --user “username” –reset

(displaying lockedout users)

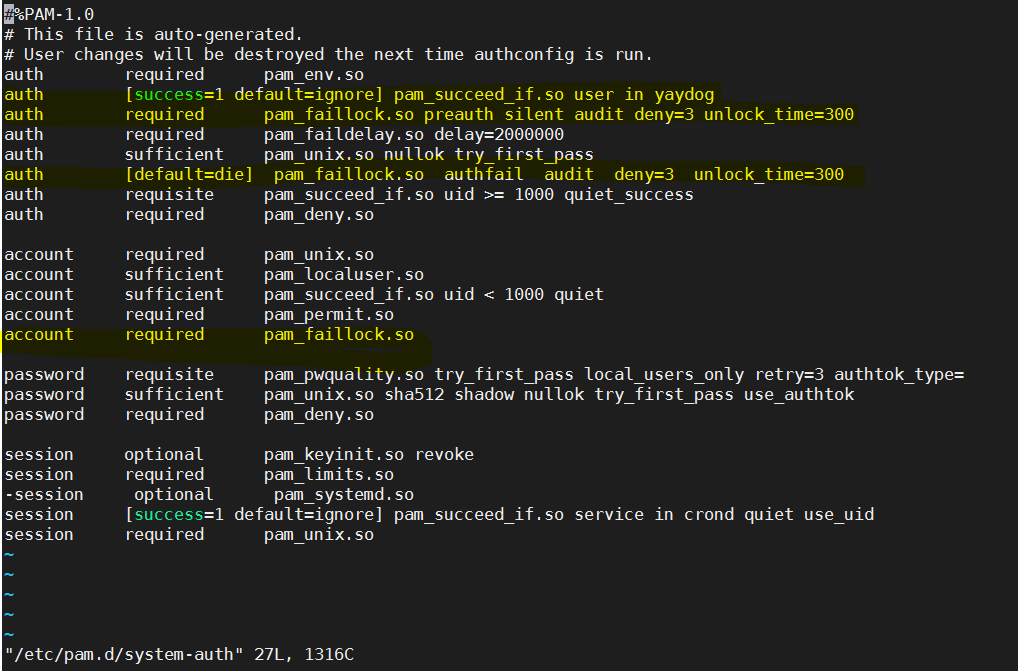
faillock

/etc/pam.d/password-auth



(root and yaydog user is excluded)

/etc/pam.d/system-auth



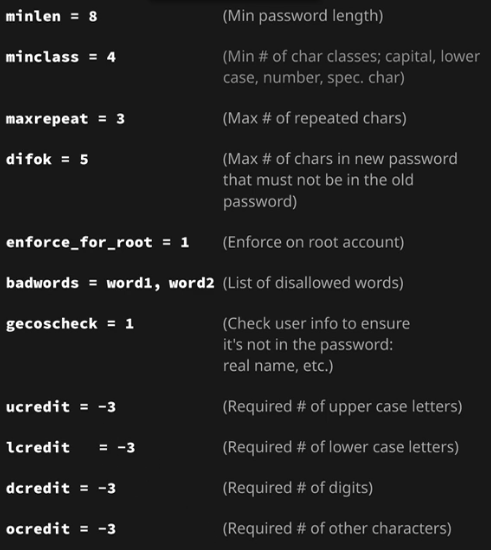
(root and yaydog user is excluded)

systemctl restart sshd

**PASSWORD POLICIES**

/etc/security/pwquality.conf

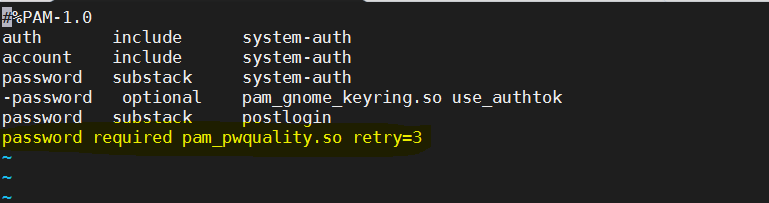
(uncomment necessary parameters)



vi /etc/pam.d/passwd

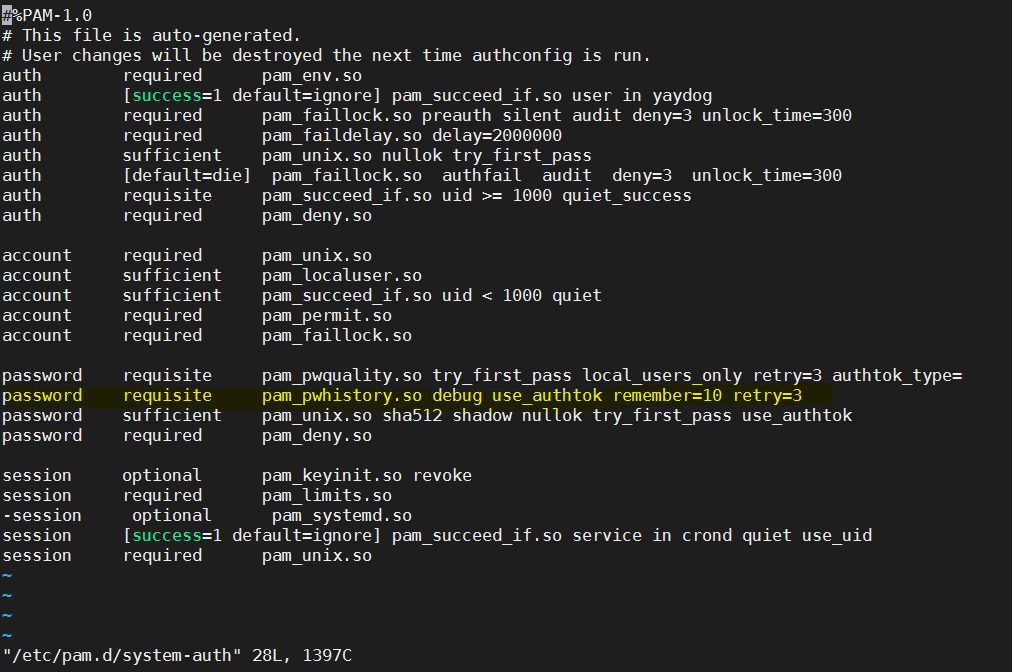
(add following line)

password required pam\_pwquality.so retry=3



(Password history policy)

vi /etc/pam.d/system-auth



Password Aging

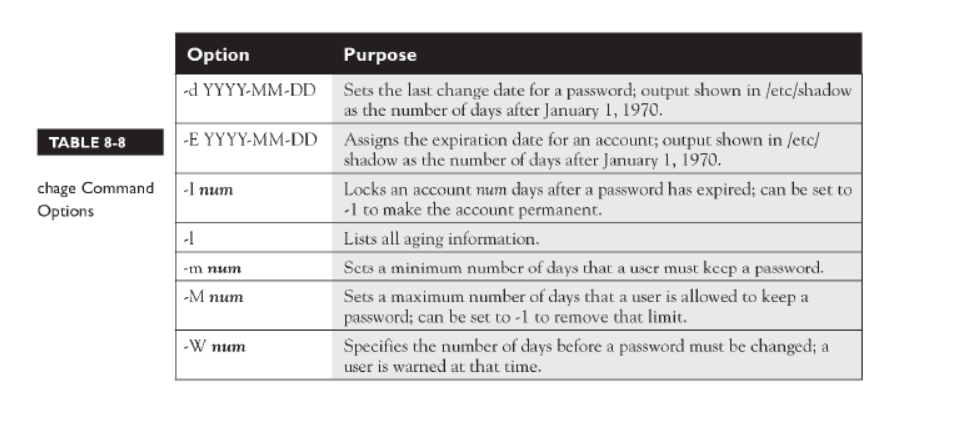
chage –l <username>: password expiry date for user

chage -d 0 <username> : user should change password for next login

chage -M 45 <username> Maximum number of days between password change for user

chage -W 15 <username> Number of days of warning before password expires : 7 (default)

parameters



groupadd> adds group sudo groupadd <groupname>

groupmod –g newid groupname > change group id

groupdel

id <username> : gives info about user

last -number>show recent logins

lastlog – u “username” > from which address user logged in

Last> successful logins

Lasttb> not successful logins

seeing userlimits

ulimit –a (see codes of limits and corresponding number)

ulimit –code limit :session based

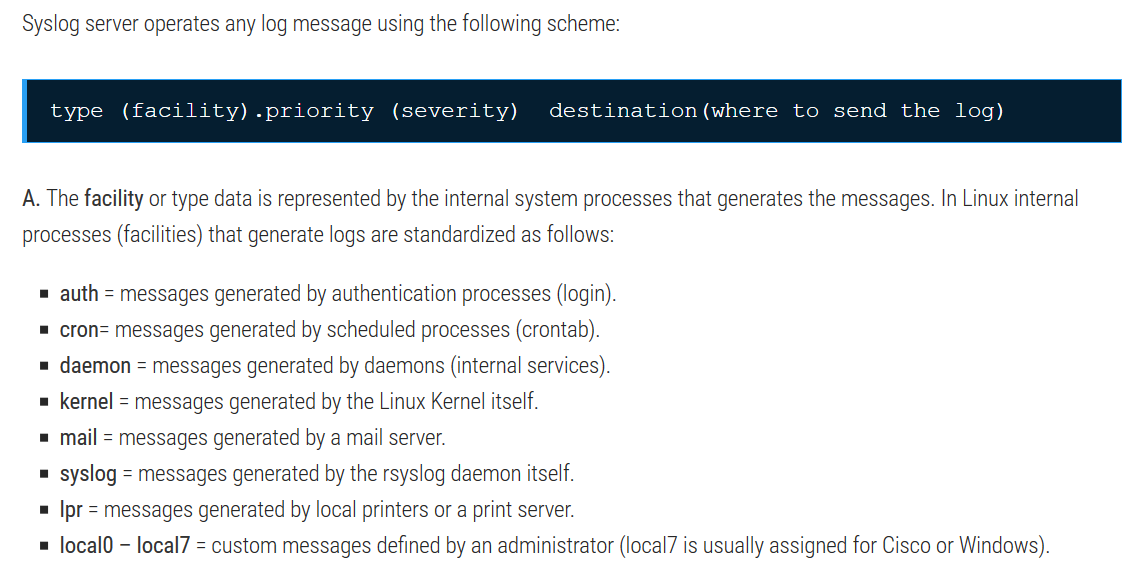
/etc/security/limits.conf

RSYSLOG

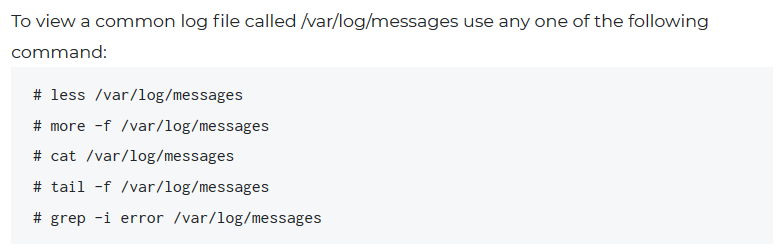
yum install rsyslog

systemctl status rsyslog

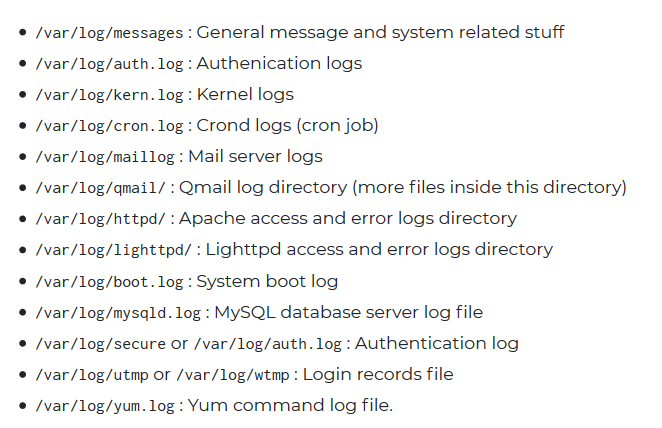
TCP/UDP 514







**LOG FILE MEANING**



**rsyslog server and client configuration**

<https://www.centlinux.com/2018/08/configure-rsyslog-central-logging-server-centos-7.html>

(SENDER)

/etc/rsyslog.conf

(uncomment following)

#$ActionQueueFileName fwdRule1 # unique name prefix for spool files

#$ActionQueueMaxDiskSpace 1g # 1gb space limit (use as much as possible)

#$ActionQueueSaveOnShutdown on # save messages to disk on shutdown

#$ActionQueueType LinkedList # run asynchronously

#$ActionResumeRetryCount -1 # infinite retries if host is down

#\*.\* @@remote-host:514

(RECEIVER)

/etc/rsyslog.conf

(uncomment following)

#$ModLoad imtcp

#$InputTCPServerRun 514

#RULES

$template DynamicFile,“/var/log/hosts/system-%HOSTNAME%-test.log”

\*.\* ?DynamicFile

tail -f /var/log/messages

(SENDER LOGS APPEAR HERE)

**LOG READER GUI TOOLS (on client)**

Yum install glogg (linux+windows)

Working with other users permissions

su -c ‘command’ : execute command with root permissions

sg “groupname” –c ‘command’: execute command with group permissions

standard users cant make su except wheel group

vi /etc/pam.d/su

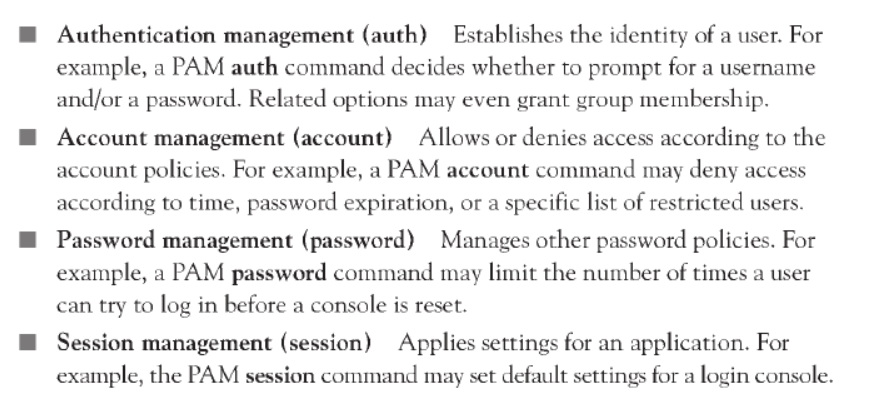
auth required pam\_wheel.so use\_uid

(sadece wheels grubundaki kullanıcılar su komutunu çalıştırabilir)

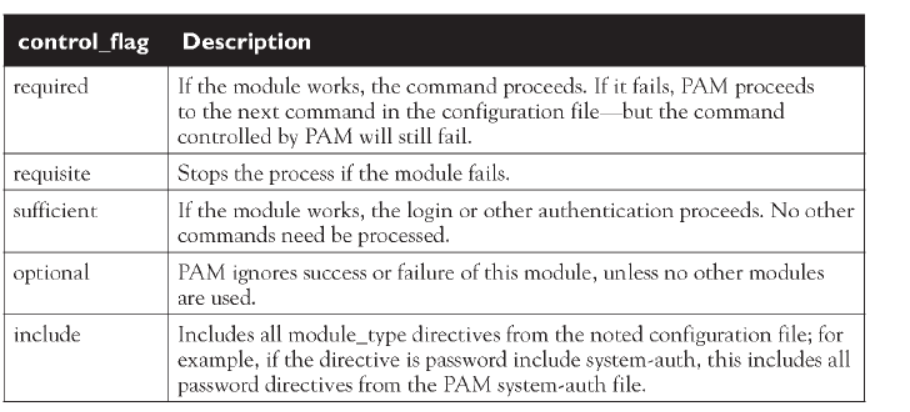
/etc/pam.d syntax

module\_type control\_flag module\_path [arguments]

module types



control\_flags



user profiles

login shell + interactive shell

/etc/profile ; /etc/profile.d

/home/user/bash\_profile

Bash\_login

Profile

/home/user/.bashrc

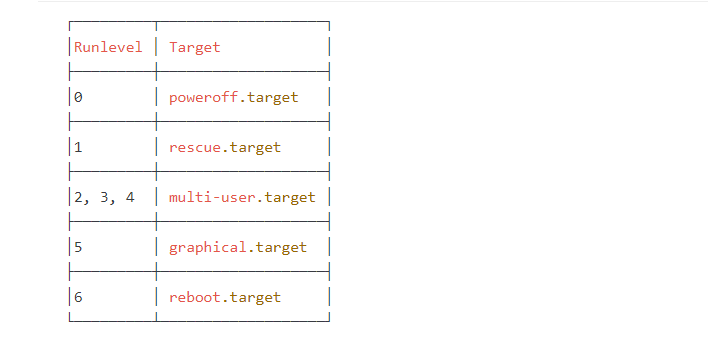
/etc/bashrc

pointer > ln –s “file” pointername

Finding and changing boot target

Run level 3: text mode

Graphical target: GUI mode with X server



systemctl get-default

systemctl enable multi-user.target

systemctl set-default multi-user.target

**GRUB**

GRUB 2 menu-configuration settings are taken from /etc/default/grub when generating grub.cfg

GRUB\_TIMEOUT=5

GRUB\_DISTRIBUTOR="$(sed 's, release .\*$,,g' /etc/system-release)"

GRUB\_DEFAULT=saved

GRUB\_DISABLE\_SUBMENU=true

GRUB\_TERMINAL\_OUTPUT="console"

GRUB\_CMDLINE\_LINUX="crashkernel=auto rhgb quiet"

GRUB\_DISABLE\_RECOVERY="true"

\* the saved\_entry value is set to the name of latest installed kernel of package type kernel

İf you change /etc/default/grub use

grub2-mkconfig > /boot/grub2/grub.cfg (MBR-BIOS)

grub2-mkconfig > /boot/efi/EFI/redhat/grub.cfg (GPT-UEFI)

grep ^menuentry /boot/grub2/grub.cfg >> show which kernels system boots into

awk -F\' /^menuentry/{print\$2} /etc/grub2.cfg >> show which kernels system boots into

Red Hat Enterprise Linux Server (3.10.0-327.10.1.el7.x86\_64) 7.2 (Maipo) ===> entry 0

Red Hat Enterprise Linux Server (3.10.0-229.el7.x86\_64) 7.2 (Maipo) ===> entry 1

Red Hat Enterprise Linux Server (0-rescue-0cb6313ed65e4b36ba5daace11f3ad50) 7.2 (Maipo) ===> entry 2

grub2-set-default [number] :

FIXING BOOT ISSUE ON EFI SYSTEM

Boot into rescue target

grub2-mkconfig -o /boot/

grub2-mkconfig -o /boot/efi/EFI/centos/grub.cfg

reboot

password protect grub

grub2-setpassword

vi /boot/grub2/grub.cfg > delete --unrestricted

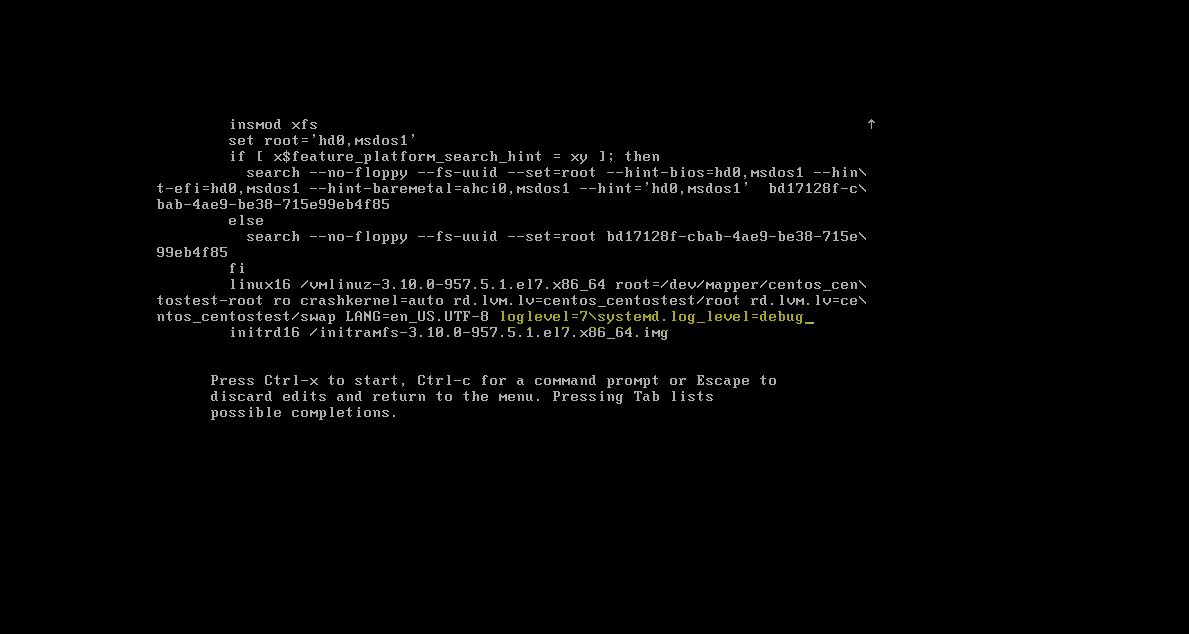
when you enter ‘e’ or ‘c’ it ask user(root) and password to edit configuration

finding kernel command line

cat /proc/cmdline

BOOT\_IMAGE=/vmlinuz-3.10.0-957.el7.x86\_64 root=UUID=7384f15e-bdb7-4d29-b37d-dc44a4367c2d ro crashkernel=auto rhgb quiet LANG=en\_US.UTF-8

Starting system with debug mode:



Power opitions

halt

Poweroff

Reboot (init 6)

Shutdown –r now “message”

Shutdown –h +2(min)

Shutdown –h now

Shutdown –h 05:21 “message”

Shutdown –F : forces a file system check on reboot

reboot

Share libraries>> for programs to share common part (where programs look)

/etc/ld.so.conf

/etc/ld.so.cache

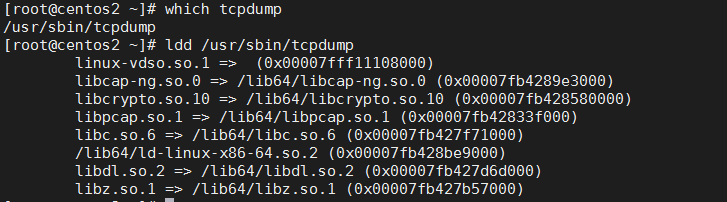
/etc/ld.so.conf.d

To find which program needs which libraries >

which cmd : gives full execution path

ldd path

(example)



(finding library path)

ldconfig -p | grep library name

(example)



yum whatprovides '\*/LIBRARYNAME.so\*' : it will shows needed package to install

Links

Hardlink (copy) : Ln file1 file2 (file1 and file2 are linked) (same inode)

(file is protected even one link is deleted)

Symbolic link (shortcut) (different inode) ln –s file1 file2 (file2 is copy of file1)

(file is not protected even one link is deleted)

See inode numbers : ls –li

**RPM CMDS**

rpm –qa : shows all installed packages

rpm –qi “packagename.rpm” : get info about installed package

rpm –iv “packagename.rpm” : verbose package install

rpm –U “packagename.rpm” : update package

rpm -e “packagename.rpm” : remove package

rpm –qR “packagename.rpm” :shows package dependencies

**CONTROLLING PACKAGE SIGNATURE**

rpm --checksig epel-release-7-11.noarch.rpm

rpm –verify -a : verify all system packages

yum repolist >> see installed repos

(DOWNLOAD ONLY RPM PACKAGE): yumdownloader “packagename”

(INSTALL PACKAGE WITHOUT DEPENDENCIES) yum localinstall packagename.rpm

Downloading packages with dependencies

(option1-dependency’ler de iner)

yum install yum-plugin-downloadonly

yum install --downloadonly --downloaddir=/tmp httpd

yum update : system update

yum check-update : check system updates

GUI: gpk-update-viewer

(finding out libarary dependencies error when installing package)

Error failed dependencies

(shows library dependencies of package)

yum deplist httpd

**YUM VERSION LOCKING (when we dont want package upgrade)**

yum install yum-plugin-versionlock -y

yum versionlock add/delete <package>

yum versionlock status

(rebuild rpm database)

rpm -vv --rebuilddb

(finding out which conf file correspons to which package)

rpm -qf httpd.conf

(how to find corrupted systemd services files, modified package files)

yum install yum-plugin-verify

yum verify <packagename> (diagnose problem)

rpm --setperms <packagename>

rpm --setugids <packagename>

yum reinstall <packagename>

**ENABLING AUTOMATIC UPDATES SECURITY UPDATES**

Yum -y install yum-cron

systemctl start yum-cron

systemctl enable yum-cron

vi /etc/yum/yum-cron.conf

update\_cmd = security (sadece security update’leri yapar)

emit\_via = email

email\_from =

email\_to =

email\_host =

service yum-cron status

service yum-cron restart

update edilen paketleri görmek : cat /var/log/yum.log | grep Updated

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*KERNELUPDATE\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

vi /etc/yum.repos.d/kernel.repo

[kernelrepo]

name=this is for kernel repo

baseurl=urllink

gpgcheck=0

enabled=1

Learning kernel version: uname -r

Updating kernel: yum install kernel (+reboot)

awk -F\' '$1=="menuentry " {print $2}' /etc/grub2.cfg : kernel options during reboot

CentOS Linux (3.10.0-957.27.2.el7.x86\_64) 7 (Core) >> grub2-set-default 0

CentOS Linux (3.10.0-862.el7.x86\_64) 7 (Core) >> grub2-set-default 1

CentOS Linux (0-rescue-e2675603581b4f64a2c3bbc83d1d550b) 7 (Core) >> grub2-set-default 2

**Blacklist kernel module**

vi /etc/modprobe.d/local-blacklist.conf

blacklist [module name]

**\*\*\*\*\*\*\*SECURITY UPDATES AND PATCHING\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

* List erratas without installing them

yum updateinfo list available | grep RHSA-2019:0368

* To list all security updates without installing them

yum updateinfo list security all

* Errata updates only

yum update-minimal --security

* System update according to CVE number

yum update --cve <CVE>

* System update according to advisory

yum update --advisory=RHSA-2014:0159

* Display CVE info for system

yum updateinfo list cve

**INSTALLATION FROM THE BUİLD (MUST HAVE PACKAGES)**

Yum install gcc make

Vim editör

Changing default editor

export EDITOR=/bin/vim

export EDITOR=/bin/nano

vim -R filename > read-only open

vim -x filename > put password

:q> editorden çıkar, çalışma kaydedilmezse uyarı verir

:q! > kaydetmeden çıkar

:w ! > write for read only files

:$ > last line

:1 > first line

:3 > 3rd line

:/searchword : find word in editor

:set nu > shows line number

**Gedit Text Editor**

Yum install gedit

Gedit <filename>

\*\*\*

BackgroundJobs

Seeing background jobs

cmd & > putting job in background

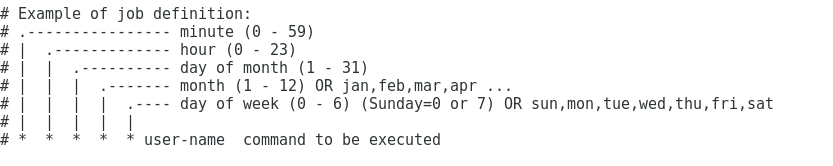
Job background’a > bg %jobnumber

Job foreground’a > fg %jobnumber

CRON

(/etc/crontab)

* yum install cronie
* systemctl enable crond
* systemctl start crond
* service crond start/restart



* user crontab display

Crontab –u “username” –l

* editing crontab for user

Crontab –eu useraneme

Other parameters: @yearly, @hourly,@daily,@weekly,@reboot

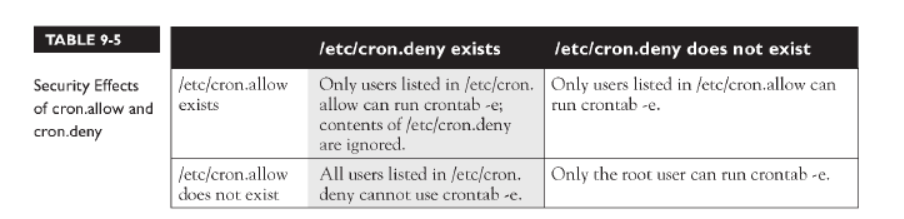
cronjob log> /var/log/cron

dont let cmd to be in cron logs >/dev/null/ 2>&1

crontab –r: deletes all cronjobs

/etc/cron.deny : users that are not allowed access

/etc/cron.allow: users that are allowed to schedule jobs



ONE TIME JOBS (to execute a command or a script at a specified date and hour, or after a given interval of time)

yum install at

systemctl enable atd

at now+ 2 minutes,3days

at 4pm

to exit at prompt CTRL+D command is used

at 4pm -f script .sh

atq>show scheduled jobs

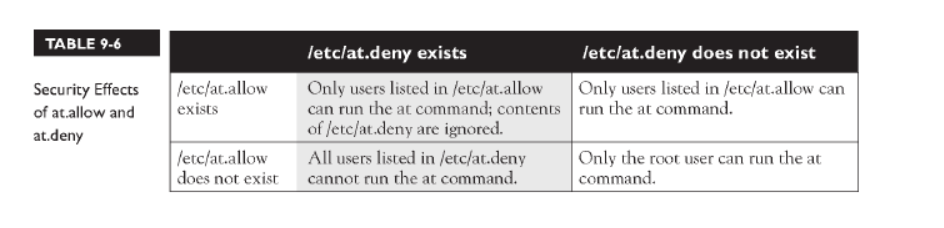


Atrm “jobid” > remove job id

/etc/at.deny contains a list of users that can not use at

/etc/at.allow contains a list of users that can use at

/var/spool/at > scheduled jobs



LANGUAGE AND KEYBOARD SETTINGS

Klavye dilini değiştirmek

yum -y install system-config-keyboard

system-config-keyboard

localectl status

localectl set-keymap tr

change system language

yum -y install system-config-language

system-config-language

**NTP**

Port:123 UDP

Installing NTP service > yum install ntp ntpdate -y

systemctl enable ntpd

systemctl start ntpd

firewall-cmd --permanent –add-service=ntp

firewall-cmd –reload

GUI TOOL: yum install system-config-date

system-config-date

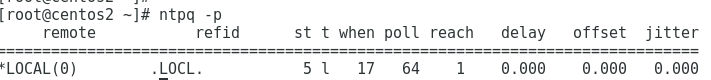
NTP SERVER CONFIGURATION (192.168.1.5)

vi /etc/ntp.conf

server 127.127.1.0

ntpstat : hangi ntp server’ın kullanıldıgını gosterir

ntpq -p : where comes from ntp information



NTP CLIENT(PEER) CONFIGURATION

yum install ntp ntpdate -y

systemctl enable ntpd

vi /etc/ntp.conf

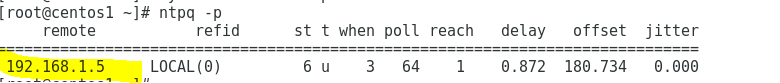
server NTPSERVERIP

firewall-cmd --permanent –add-service=ntp

firewall-cmd –reload

systemctl start ntpd

ntpq -p



**timedatectl set-ntp yes**

SETTING TIMEZONE

s

to see time zone> timedatectl

timedatectl set-timezone UTC

**ALTERNATIVES**

yum install chrony

vi /etc/chrony.conf

server example.com iburst

systemctl restart chronyd

check:chronyc tracking

check: chronyc sources

**FIREWALLD**

Systemctl disable iptables

Systemctl stop iptables

Yum install firewalld –y

Start firewall > systemctl start/restart firewalld.service

Check firewall is running > firewall-cmd --state

Viewing currently selected zone> firewall-cmd --get-default-zone

Setting default zone> firewall-cmd –set-default-zone=”internal” (2)

Viewing currently active zones> firewall-cmd --get-active-zones

Rules associated with the zone> firewall-cmd --list-all

\*Rules associated with all zones> firewall-cmd --list-all-zones

List all available zones> firewall-cmd --get-zones (1)

Create new zone> firewall-cmd --permanent --new-zone=publicweb

Get firewall rules related to specific zone> firewall-cmd --zone=”zonename” --list-all

Assign zone to interface> firewall-cmd --zone=home --change-interface=”interfacename”

Firewall’a eklenebilecek servisleri listelemek> firewall-cmd --get-services

firewall-cmd --permanent --zone=public --add-service “SERVICENAME” (ex.http)

firewall-cmd --permanent --zone=public --remove-service “SERVICENAME” (ex.http)

Belirli zone’da firewall’da izin verilmiş servisleri listelemek> firewall-cmd --zone=public --permanent --list-services

\*Allow source IP on firewall> firewall-cmd --zone=public --permanent --add-source IP

Allow port on firewall> firewall-cmd --zone=public --add-port=”portnumber”/tcp (3)

Remove port on firewall> firewall-cmd --permanent --zone=public --remove-port=4990-4999/udp

Allow port ranges on firewall> firewall-cmd --permanent --zone=public --add-port=4990-4999/udp

List open ports> firewall-cmd --list-ports (4)

Reload firewall > firewall-cmd --reload

Enable firewall at boot time> systemctl enable firewalld

Block all incoming and outgoing connections> firewall-cmd –panic-on/off

Block/Accept IP Address> firewall-cmd –zone=”zonename” –add-rich-rule=’rule family=”ipv4” source address=”192.168.1.4” accept/reject’

**Restart firewalld service**

firewall-cmd --reload

**BLOCK ALL OUTGOING TRAFFIC**

# firewall-cmd --permanent --direct --add-rule ipv4 filter OUTPUT 0 -p tcp -m tcp --dport=22 -j ACCEPT

success

# firewall-cmd --permanent --direct --add-rule ipv4 filter OUTPUT 1 -p tcp -m tcp --sport=22 -j ACCEPT

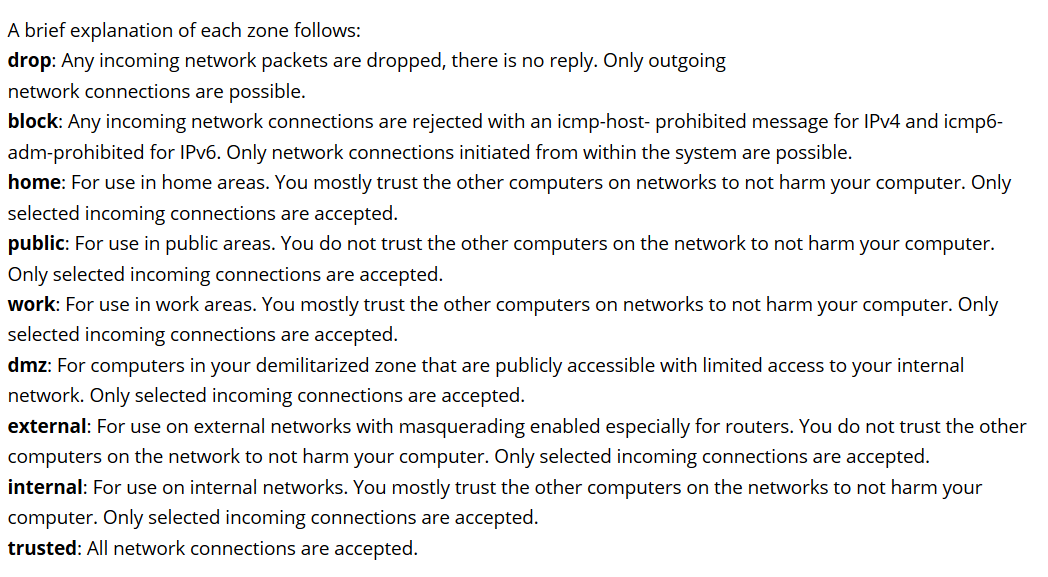
success

# firewall-cmd --permanent --direct --add-rule ipv4 filter OUTPUT 9 -j DROP

success

firewall-cmd --permanent --direct --remove-rule ipv4 filter OUTPUT 9 -j DROP

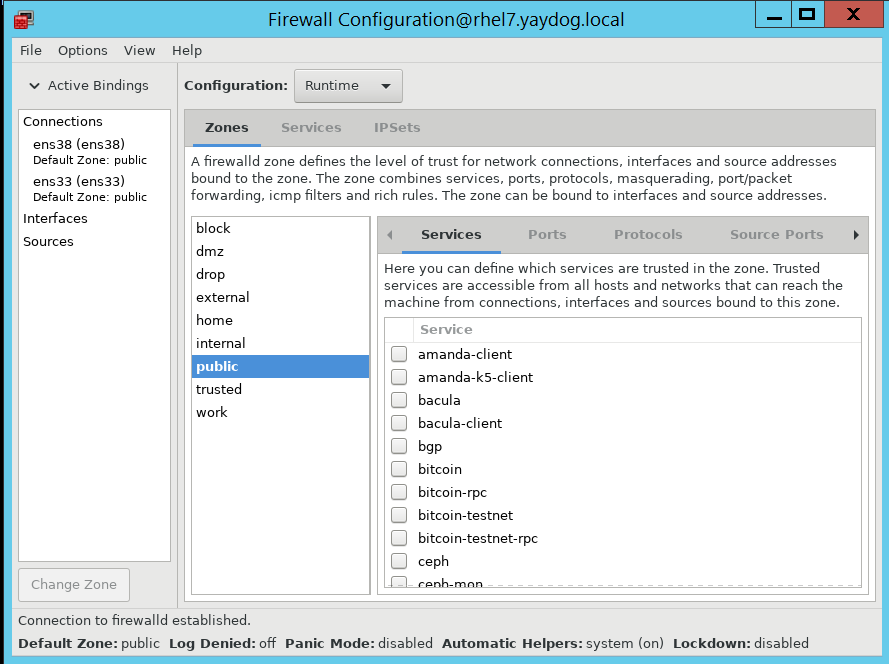
**ZONES**



**GUI**

yum install firewall-config

firewall-config



**PORT FORWARDING**

**firewall-cmd --permanent --zone="public" --add-forward-port=port=80:proto=tcp:toport=12345**

aynı sunucu üzerinde 80 portuna gelen trafik 12345’e yönlendirilir

[root@rhel7 ~]# firewall-cmd --list-all

public (active)

target: default

icmp-block-inversion: no

interfaces: ens33

sources:

services: ssh dhcpv6-client http

ports:

protocols:

masquerade: no

forward-ports: port=80:proto=tcp:toport=12345:toaddr=

source-ports:

icmp-blocks:

rich rules:

firewall-cmd --zone="public" --remove-forward-port=port=80:proto=tcp:toport=12345

**(başka bir sunucuya port yönlendirmesi)**

firewall-cmd –permanent --zone=public --add-masquerade

firewall-cmd --zone="public" --add-forward-port=port=80:proto=tcp:toport=80:toaddr=192.168.1.211

**(port forwarding with source address)**

firewall-cmd --permanent --zone="public" --add-rich-rule 'rule family=ipv4 source address=192.168.1.5 forward-port port=8080 protocol=tcp to-port=80'

firewall-cmd --reload

192.168.1.5 den 8080 e gelen istekler 80 portuna yönlensin

**ENABLING NAT**

sysctl -w net.ipv4.ip\_forward=1

public IP Private IP

eth0 123.111.0.1 eth1 192.168.1.1

firewall-cmd --zone=external --add-interface=eth0 --permanent

firewall-cmd --zone=internal --add-interface=eth1 --permanent

firewall-cmd --complete-reload

firewall-cmd --zone=external --add-masquerade –permanent

firewall-cmd --permanent --direct --passthrough ipv4 -t nat -I POSTROUTING -o eth0 -j MASQUERADE -s 192.168.1.0/24

firewall-cmd --complete-reload

**RICH-RULE SYNTAX**

--add-rich-rule

rule family= ipv4

service name=

protocol= tcp

source address=

destination address=

forward-port port=

to-port=

accept/reject/drop

limit value= "100/s" (100 connections per second)

log level=notice

(example)

firewall-cmd --permanent --zone=public --add-rich-rule='rule family=ipv4 service name=http source address=192.168.1.3/24 accept'

**ICMP FILTER**

**List icmp types**: firewall-cmd --get-icmptypes

**Check if icmp type is blocked**: firewall-cmd --query-icmp-block=<icmptypes> no:notblocked

**Belirli bir icmptype bloklamak**: firewall-cmd --permanent --add-icmp-block=<icmptypes>

**Bloklamayı kaldırmak:** firewall-cmd –permanent --remove-icmp-block=<icmptypes>

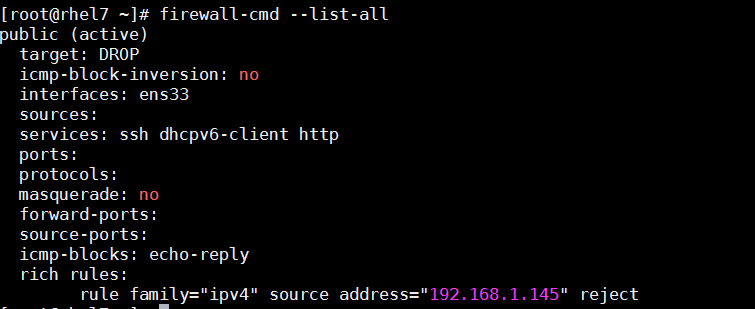
closing ping from kernel runtime parameters

echo 1 > /proc/sys/net/ipv4/icmp\_echo\_ignore\_all

**FILTERING IP**

Blocking ip

firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" source address="192.168.1.145" reject'



firewall-cmd --zone=public --remove-rich-rule='rule family="ipv4" source address="192.168.1.145" reject'

**TCP WRAPPERS**

(HOST BASED ACL)

Check if a daemon supports tcp wrappers

ldd $(which sshd) | grep libwrap.so

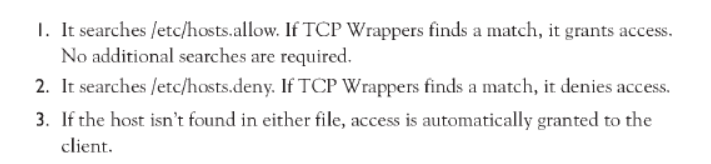
**libwrap.so**.0 => /lib64/**libwrap.so**.0 (0x00007f023f3dd000)

means it supports

 is a library that provides simple access control and standardized logging for supported applications that accept connections over a network.

vi /etc/hosts.allow

vi /etc/hosts.deny



daemon list: client list

sshd : IP (client IP)

sshd: .yaydog.local (all clients on this domain)

ALL: ALL (all service and client)

Sshd: user@IP (specific user from clientIP)

Sshd: IP1 IP2 EXCEPT IP3

ALL EXCEPT: IP

sshd:192.168.1.0/24

**TELNET**

İnstall telnet server: yum install telnet-server -y

systemctl start telnet.socket

systemctl status telnet.socket

Ss –tnlp | grep 23 (checklisteningport)

install telnet client: yum install telnet -y

**WEBSERVER (APACHE)**

(cmd browser)

yum install -y elinks

yum install -y httpd mod\_ssl mod\_security openssl

systemctl start httpd

systemctl reload httpd (servisi durdurmadan değişien config file’ı okumayı sağlar)

versiyon: httpd -v

syntax check: httpd -t

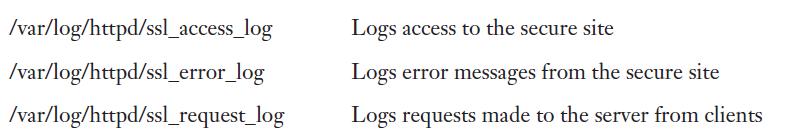
security modules: yum install mod\_evasive

Log files: vi /var/log/httpd/access\_log vi /var/log/httpd/error\_log

Dosyaların bulundugu lokasyon: vi /var/www

Apache modules: cd /usr/lib64/httpd/modules or /etc/httpd/modules

apachectl -M : installed apache modules



firewall-cmd --permanent –add-service=http

firewall-cmd --permanent –add-service=https

firewall-cmd –reload

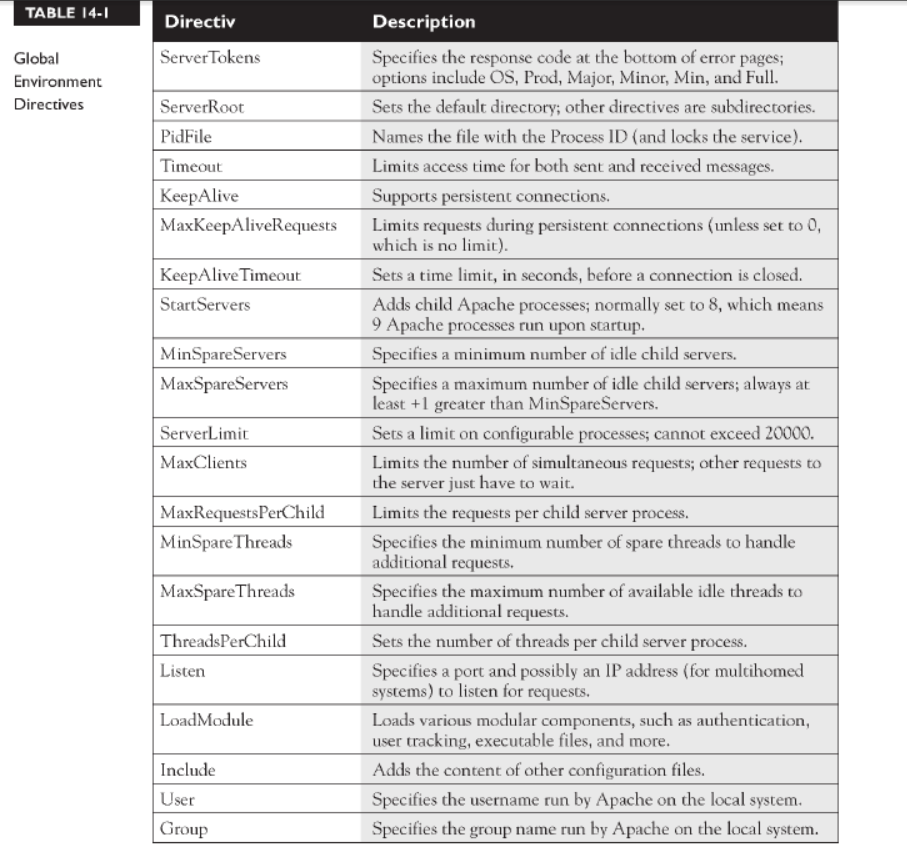
Test Configuration: apachectl configtest

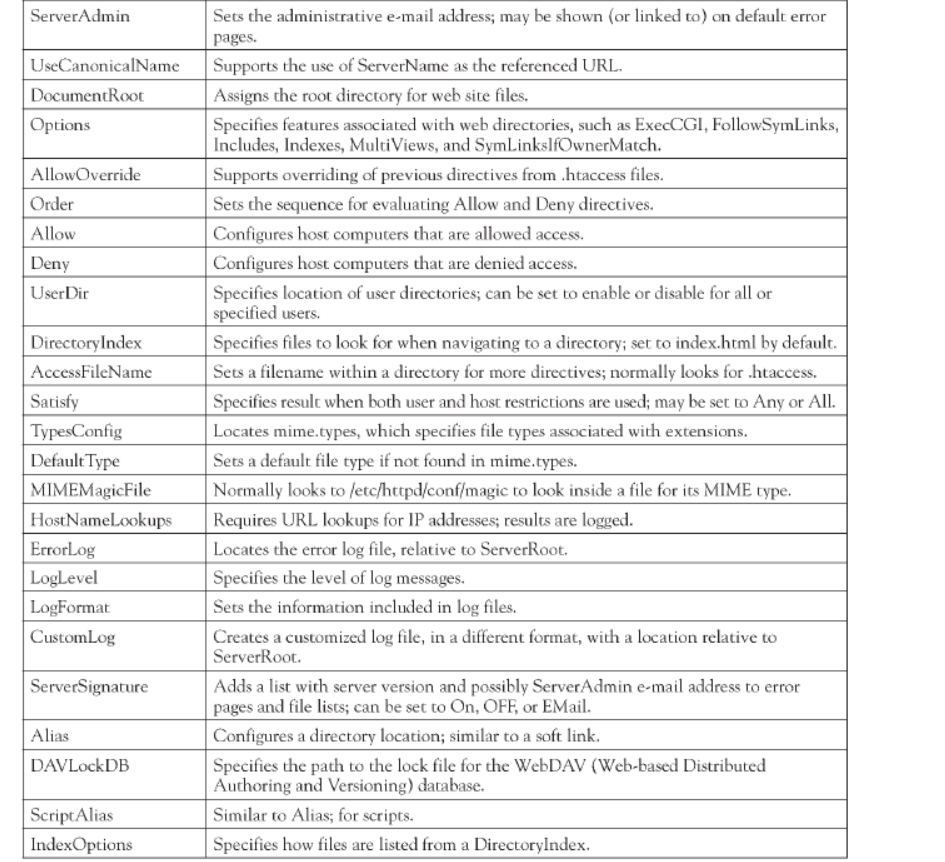
ll -Z /var/www

drwxr-xr-x. root root system\_u:object\_r:httpd\_sys\_script\_exec\_t:s0 cgi-bin

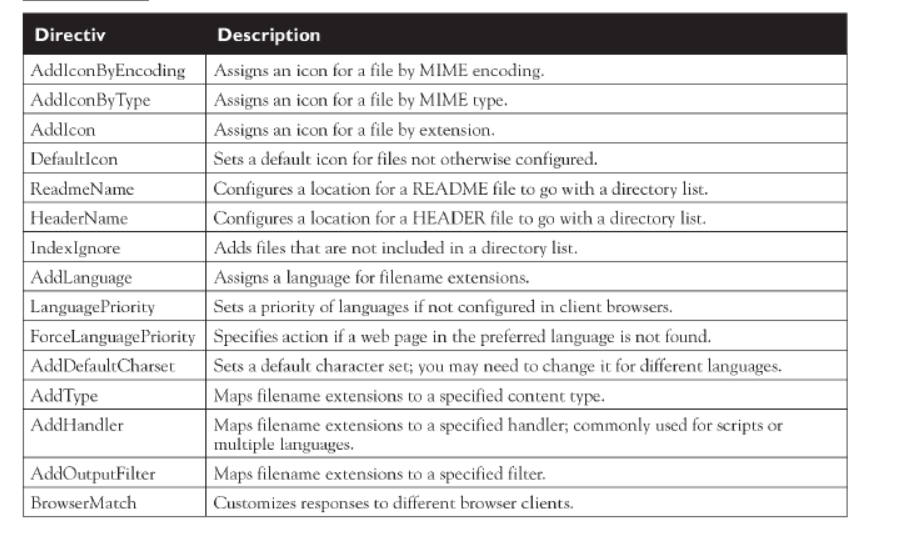
drwxr-xr-x. root root system\_u:object\_r:httpd\_sys\_content\_t:s0 html

Main Config file: vi /etc/httpd/conf/httpd.conf





AllowOverride None: for security



**HIDING APACHE VERSION BANNER**

[root@rhel7 modules]# curl -I http://192.168.1.180/

HTTP/1.1 403 Forbidden

Date: Thu, 04 Apr 2019 13:43:23 GMT

Server: Apache/2.4.6 (Red Hat Enterprise Linux) OpenSSL/1.0.2k-fips

Last-Modified: Fri, 22 Jun 2018 05:17:35 GMT

ETag: "f91-56f34264b39c0"

Accept-Ranges: bytes

Content-Length: 3985

Content-Type: text/html; charset=UTF-8

vi /etc/httpd/conf/httpd.conf

ServerTokens Prod

ServerSignature Off

service httpd restart

[root@rhel7 modules]# curl -I http://192.168.1.180/

HTTP/1.1 403 Forbidden

Date: Thu, 04 Apr 2019 13:51:01 GMT

Server: Apache

Last-Modified: Fri, 22 Jun 2018 05:17:35 GMT

ETag: "f91-56f34264b39c0"

Accept-Ranges: bytes

Content-Length: 3985

Content-Type: text/html; charset=UTF-8

**IMAGE HOSTING WITH APACHE**

<https://access.redhat.com/solutions/67298>

Configure Virtual Host and user authentication (PRIVATE DIRECTORY)

mkdir -p /wwwroot/app1

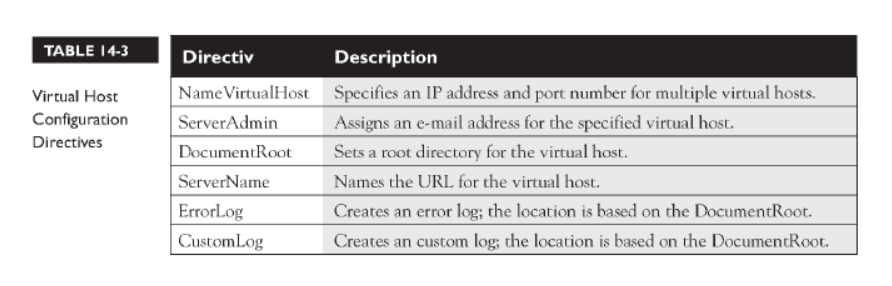
semanage fcontext -at httpd\_sys\_content\_t "/wwwroot/app1(/.\*)?"

restorecon -Rv /wwwroot/app1

vi /etc/hosts

192.168.1.15 centos3.yaydog.local

echo "user1 index page" > /wwwroot/app1/index.html



httpd -D DUMP\_VHOSTS (virtual host’ları gösterir)

htpasswd -c /etc/httpd/.htpasswd user1

cat /etc/httpd/.htpasswd (hangi kullanıcıların basic auth ile bağlandığını gösterir)

vim /etc/httpd/conf.d/app1.conf

<VirtualHost \*:80>

ServerAdmin yaydog@gmail.com

DocumentRoot /wwwroot

ServerName centos3.yaydog.local

ErrorLog /var/log/app1\_error\_log

CustomLog /var/log/app1\_access\_log combined

</VirtualHost>

<Directory "/wwwroot/app1">

LogLevel warn

AuthType Basic

AuthName "Authentication Required"

AuthUserFile /etc/httpd/.htpasswd

Require user user1

</Directory>

<http://centos3.yaydog.local/app1>

Configure Virtual Host and group authentication (PRIVATE DIRECTORY)

mkdir -p /wwwroot/app2

groupadd admins

useradd user2 -m -d /home/user2

useradd user3 -m -d /home/user3

usermod -G admins user2

usermod -G admins user3

chgrp admins /wwwroot/app2

chmod 0771 /wwwroot/app2

echo "Group index page" > /wwwroot/app2/index.html

semanage fcontext -at httpd\_sys\_content\_t "/wwwroot/app2(/.\*)?"

restorecon -Rv /wwwroot/app2

vim /etc/httpd/conf.d/app2.conf

<VirtualHost \*:80>

ServerAdmin yaydog@gmail.com

DocumentRoot /wwwroot

ServerName centos3.yaydog.local

ErrorLog /var/log/app2\_error\_log

CustomLog /var/log/app2\_access\_log combined

</VirtualHost>

<Directory "/wwwroot/app2">

LogLevel warn

AuthType Basic

AuthName "Authentication Required"

AuthUserFile /etc/httpd/.uhtpasswd

AuthGroupFile /etc/httpd/.ghtpasswd

Require group admins

</Directory>

vi /etc/httpd/.ghtpasswd

admins:user2 user3

htpasswd -c /etc/httpd/.uhtpasswd user2

htpasswd -c /etc/httpd/.uhtpasswd user3

<http://centos3.yaydog.local/app2>

Configure Virtual Host only

vi /etc/hosts

192.168.1.4 app3.yaydog.local

mkdir -p /var/www/html/app3

echo "Virtualhost only index page" > /var/www/html/app3/index.html

vim /etc/httpd/conf.d/app3.conf

<VirtualHost \*:80>

ServerAdmin yaydog@gmail.com

DocumentRoot /wwwroot/app3

ServerName app3.yaydog.local

ErrorLog /var/log/app3\_error\_log

CustomLog /var/log/app3\_access\_log combined

</VirtualHost>

<http://app3.yaydog.local>

Configure Virtual Host and user authentication+SelfSignedSSL

yum install openssl

yum install mod\_ssl

(mod\_ssl.so library needed )

LoadModule ssl\_module modules/mod\_ssl.so

cd /etc/pki/tls/certs

openssl genpkey -algorithm rsa -pkeyopt rsa\_keygen\_bits:2048 -out test1.yaydog.local.key

openssl req -new -key test1.yaydog.local.key -out test1.yaydog.local.csr

openssl x509 -req -days 365 -signkey test1.yaydog.local.key -in test1.yaydog.local.csr -out test1.yaydog.local.crt

vim /etc/httpd/conf.d/app2.conf

<VirtualHost \*:443>

ServerAdmin yaydog@gmail.com

DocumentRoot /wwwroot

ServerName test1.yaydog.local

ErrorLog /var/log/app2\_error\_log

CustomLog /var/log/app2\_access\_log combined

SSLEngine on

SSLCertificateFile /etc/pki/tls/certs/test1.yaydog.local.crt

SSLCertificateKeyFile /etc/pki/tls/certs/test1.yaydog.local.key

SSLCertificateChainFile /etc/pki/tls/certs/test1.yaydog.local.csr

<Directory "/wwwroot/app2">

LogLevel warn

AuthType Basic

AuthName "Authentication Required"

AuthUserFile /etc/httpd/.htpasswd

Require valid-user

</Directory>

</VirtualHost>

https://test1.yaydog.local/app2

CGI Application

setsebool -P httpd\_enable\_cgi 1

semanage fcontext -at httpd\_sys\_script\_exec\_t "/var/webscripts(/.\*)?"

restorecon -Rv /var/webscripts

mkdir -p /var/webscripts

vi /var/webscripts/hello.pl

chmod +x /var/webscripts/hello.pl

vi /etc/httpd/conf/httpd.conf

ScriptAlias /cgi-bin/ "/var/webscripts"

<Directory "/var/webscripts">

AllowOverride None

Options None

Require all granted

</Directory>

systemctl restart httpd

<http://centos3.yaydog.local/cgi-bin/hello.pl>

**WSGI APPLICATION**

yum install mod\_wsgi

vi /etc/httpd/conf.d/webapp.conf

<VirtualHost \*:80>  
ServerAdmin root@localhost  
ServerName [wwww.tech.com](http://wwww.tech.com)  
WSGIScriptAlias / /var/www/html/webapp.wsgi  
</VirtualHost>

vi /var/www/html/webapp.wsgi >> Script buraya girilir

systemctl restart httpd

mysql-php connection

mysql veritabanının apache sunucusu üzerinden kontrol edilmesi

(php eklentileri)

yum install php php-mysql php-gd php-imap php-ldap php-mbstring php-odbc php-pear php-xml php-xmlrpc php-pecl-apc

service httpd restart

mySQL

sample databases: https://dev.mysql.com/doc/index-other.html

to install mysql

wget http://repo.mysql.com/mysql-community-release-el7-5.noarch.rpm

rpm -ivh mysql-community-release-el7-5.noarch.rpm

yum install mysql-server

config : /etc/my.cnf

log-error=/var/log/mysqld.log

general\_log\_file= “filepath”

[mysqld]

bind-address= “ip address of sql server”

[client]

Port=”portnumber”

[mysqld]

Port=”portnumber”

(datadir): /var/lib/mysql

/usr/bin/mysql\_secure\_installation >> secure root password

Set root password

Remove anonymous users? y / n

Disallow root login remotely? y/n

Remove test database and access to it? y/ n

Reload priviledge tables now? y/ n

mysql –h “hostname” –u ‘username’ –p

mysql –h “hostname” –u ‘username’ –p databasename

over socket:

mysql -u root -p -S /var/lib/mysql.sock

SHOW TABLES

SELECT \* FROM tablename WHERE condition ORDERBY

INSERT INTO tablename (columnname1,columnanme2...) VALUES (value1,value2,...)

DELETE FROM tablename WHERE condition (deleting rows wit condition)

UPDATE tablename SET column condition where condition

**GRANT ALL PRIVILEGES ON \*.\* TO 'user'@'%';**

FLUSH PRIVILEGES;

User create and priviledges

create user 'esh'@'%' identified by ‘rootdb23’;

grant all privileges on \*.\* to 'esh'@’%’;

mysql> FLUSH PRIVILEGES

show grants for 'esh'@'%';

priviledges

<https://dev.mysql.com/doc/refman/5.7/en/privileges-provided.html>

deleting user

DROP USER 'testuser'@'localhost';

running .sql script

select db

mysql> /source/script.sql

ENABLE AUDIT LOGGIN

msql> install plugin audit\_log soname 'audit\_log.so';

[mysqld]

audit\_log=ON

audit\_log\_file='/var/log/mysql/audit.log'

Parola degişikliği:

UPDATE mysql.user SET password= PASSWORD(‘password’) WHERE user ='username’;

FLUSH PRIVILEGES

BACKUPS (stop mysql service)

/var/lib/mysql ‘deki dosyalar kopyalanmalıdır

Make tables read only

mysql -u root -p -e "FLUSH TABLES WITH READ LOCK;"

remove read only after backup

mysql -u root -p -e "UNLOCK TABLES"

**FTP SERVER**

yum install -y vsftpd

service vsftpd start

chkconfig vsftpd on

/var/ftp/pub altındaki dosyalara <ftp://192.168.1.211/pub/>

ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin

/var/log/xferlog : upload transfers

/etc/vsftpd/vsftpd.conf > config file

<http://vsftpd.beasts.org/vsftpd_conf.html>

Listen: aktif hale getirilirse servis xinedt daemon’u yerine stand-alone modda çalışır

anonymous\_enable=YES (kullanıcı ve şifresi olmadan girişe izin verir)

local\_enable: yes (/etc/passwd içerisinde saklanan normakl kullanıcıların sisteme girip giremeyecekleri)

download\_enable: istemciden gelen indirme isteklerine izin verilip verilmeyeceği

anon\_mkdir\_write\_enable=YES (anonymous FTP user to be able to create new directories)

userlist\_enable=YES (/etc/vsftpd/userlist\_deny) deki kullanıcılar ftp yapamaz

write\_enable:YES/NO kullanıcıların sunucu dosya sistemi üzerinde değişiklik yapıp yapmamasını sağlar

anon\_root= path (anonim bağlantıların kök dizinleri)

anon\_max\_rate= (download sınırı)

listen\_address= IP

listen\_port: bağlantıların kullanacağı port

chroot\_local\_user=YES (kullanıcılar sadece kendi home folder’larını görebilir)

local\_root= a directory which vsftpd will try to change into after a local (i.e. non-anonymous) login

xferlog\_file=/var/log/xferlog

idle\_session\_timeout=10

data\_connection\_timeout=300

listen=YES

#listen\_ipv6=YES (ipv6 dan dinlemez)

tcp\_wrappers=YES (/etc7host.allow ve /etc/host.deny’ı kullanmayı sağlar)

/etc/vsftpd/user\_list> allowed and not allowed ftp users

# If userlist\_deny=NO, only allow users in this file

# If userlist\_deny=YES (default), never allow users in this file, and do not even prompt for a password.

Enable anon users to upload

mkdir /var/ftp/pub/upload

chmod 733 /var/ftp/pub/upload

/etc/vsftpd/vsftpd.conf > anon\_upload\_enable=YES

Adding ftpusers conf

<https://www.unixmen.com/install-configure-ftp-server-centos-7/>

yum install xinetd

/etc/xinetd.conf

Yum install lftp

Lftp ftp://user@IP:port

lftp sftp://cxi\_user@nas.corendonairlines.com.mt:22

pget

put

**BACKUP**

Yum install epel-release

yum -y install rsync

Yereldeki etc dosyasını 192.168.1.60 ip’li sunucunun backup dosyasının altına kopyalamak

rsync –av ssh /etc root@192.168.1.60:/backup

192.168.1.60 ip’sindeki /etc yi yerelde /backup’a almak

rsync -av root@192.168.1.60:/etc /backup

rsync from GUI

grsync

RSNAPSHOT (DAİLY,WEEKLY PROGRAM)

<https://www.cyberciti.biz/faq/redhat-cetos-linux-remote-backup-snapshot-server/>

<https://www.pontikis.net/blog/howto-rsnapshot-backup>

Apache Directory Server (ApacheDS)

wget <https://archive.apache.org/dist/directory/apacheds/dist/2.0.0-M24/apacheds-2.0.0-M24-x86_64.rpm>

rpm -ivh apacheds-2.0.0-M24-x86\_64.rpm

/etc/init.d/apacheds-2.0.0\_M24-default start

/etc/init.d/apacheds-2.0.0\_M24-default status

DN uid=admin,ou=system and the current password (default is "secret") port 10389

Create user> inetorg person uid=username

chkconfig apacheds-2.0.0\_M24-default on

Apache Directory Studio (Windows)

Java 8 Update 162 (64bit) JRE gerekli

Apache Directory Studio (Linux)

java install > yum install java-1.8.0-openjdk

java-1.7.0-openjdk

java -version

wget <http://archive.apache.org/dist/directory/studio/2.0.0.v20170904-M13/ApacheDirectoryStudio-2.0.0.v20170904-M13-linux.gtk.x86_64.tar.gz>

tar -xf ApacheDirectoryStudio-2.0.0.v20170904-M13-linux.gtk.x86\_64.tar.gz

cd ApacheDirectoryStudio

./ApacheDirectoryStudio

**UNISON**

192.168.1.170 192.168.1.171

(enable passwordless ssh)

Yum install -y unison

Script: unison -batch /var/www/ ssh://192.168.1.171//var/www

Crontab –e > \*/5 \* \* \* \* /script.sh

**/root/.unison/default.prf**

Unison -version

Check unison connects remote server :

unison -testServer /home/www ssh://server2//home/www

**INOTIFY**

yum install –y unison

(passwordless ssh)

yum install gcc make

wget <http://jensd.be/download/inotify-tools-3.14.tar.gz>

tar -xvzf inotify-tools-3.14.tar.gz

cd /root/inotify-tools-3.14

./configure

make

make install



Create script

while inotifywait -r -e create,modify,delete,move /var/www ; do

> unison -batch /var/www/ ssh://192.168.1.171//var/www

>done

**FSNIPER & UNISON**

<https://tecadmin.net/fsniper-directory-monitor-setup-in-centos-linux/>

<http://blog.secaserver.com/2011/06/fsniper-monitor-newly-created-files-in-directory/>

[**http://g33kinfo.com/info/archives/4245**](http://g33kinfo.com/info/archives/4245)

**test1 test2**

**192.168.1.171 192.168.1.170**

Şifresiz root ssh’a izin ver

Yum install –y epel-release

yum install -y unison

**cd /root**

**mkdir .unison**

**vi /root/.unison/default.prf**(test1de)

# Unison preferences file

root=/var/www

root=ssh://192.168.1.170//var/www

batch=true

confirmbigdel=false (klasor icerisindeki tum dosyalar silindiğinde bile karsı tarafa replike eder)

**vi /root/.unison/default.prf**(test2de)

# Unison preferences file

root=/var/www

root=ssh://192.168.1.171//var/www

batch=true

confirmbigdel=false (klasor icerisindeki tum dosyalar silindiğinde bile karsı tarafa replike eder)

unison default

**OPENVPN**

Wget <http://swupdate.openvpn.org/as/openvpn-as-2.5-CentOS7.x86_64.rpm>

rpm -i openvpn-as-2.5-CentOS7.x86\_64.rpm

Access Server Web UIs are available here:

Admin UI: https://<server\_ip>:943/admin

Client UI: https://<server\_ip>:943

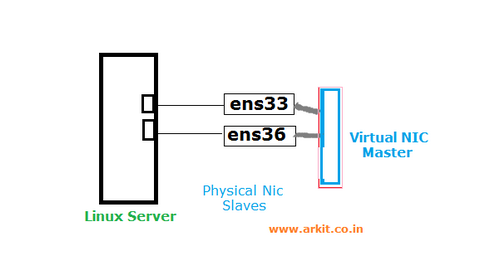
passwd openvpn

**how to install vpn client on centos7**

yum install openvpn

openvpn --config client.ovpn

**NIC TEAMING**



Activebackup: one NIC active while another NIC is asleep. If the active NIC goes down, another NIC becomes active. only supported in x86 environments.

yum install NetworkManager -y

nmcli con add type team con-name nicteam ifname nicteam config '{"runner":{"name":"activebackup"}}'

(options:loadbalance,broadcast,roundrobin,activebackup)

(active backup: if primary port gets down, other will automatically start)

nmcli con mod nicteam ipv4.addresses 192.168.1.55/24 ipv4.gateway 192.168.1.1 ipv4.dns 8.8.8.8 ipv4.method manual connection.autoconnect yes

nmcli con add type team-slave con-name nicteam-port1 ifname ens38 master nicteam

nmcli con add type team-slave con-name nicteam-port2 ifname ens39 master nicteam

nmcli con up nicteam-port1

nmcli con up nicteam-port2

nmcli con up nicteam

teamdctl nicteam state (shows active port)

**MARIADB**

yum groupinstall mariadb mariadb-client -y (hem server hem client için kurulmalıdır)

systemctl enable mariadb

firewall-cmd --permanent --add-service=mysql

firewall-cmd --reload

vim /etc/my.cnf

bind-address=192.168.1.171

systemctl start mariadb

mysql\_secure\_installation (set root password)

systemctl restart mariadb

Operations

(entering database) mysql -u root –p

show databases;

create database **contacts**;

drop database contacts;

use contacts;

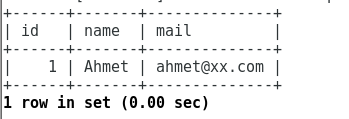
show tables;

DESCRIBE tablename;

(create table) create table **employees** (**id** int(10),**name** varchar(70),**mail** varchar(12));

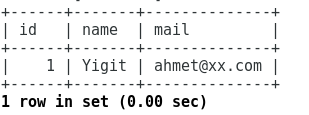
insert into employees (id,name,mail) values("1","Ahmet","ahmet@xx.com");

select \* from employees whre id=’1’;



delete from employees where id=1;

update employees set name='Yigit' where name='Ahmet';



exit

creating user and give priviledges

create user 'esh'@'localhost' identified by ‘lapland23’;

grant all privileges on contacts.\* to esh;

flush privileges;

mysql -u esh -p (then login to database)

Enabling Remote access (IP BASED)

GRANT ALL ON \*.\* TO root@192.168.1.4 IDENTIFIED BY 'lapland23';

FLUSH PRIVILEGES;

mysql -h 192.168.1.5 -u root -p

Disabling Remote access (socket based)

vim /etc/my.cnf

skip-networking=1 (only local client can connect to mariadb)

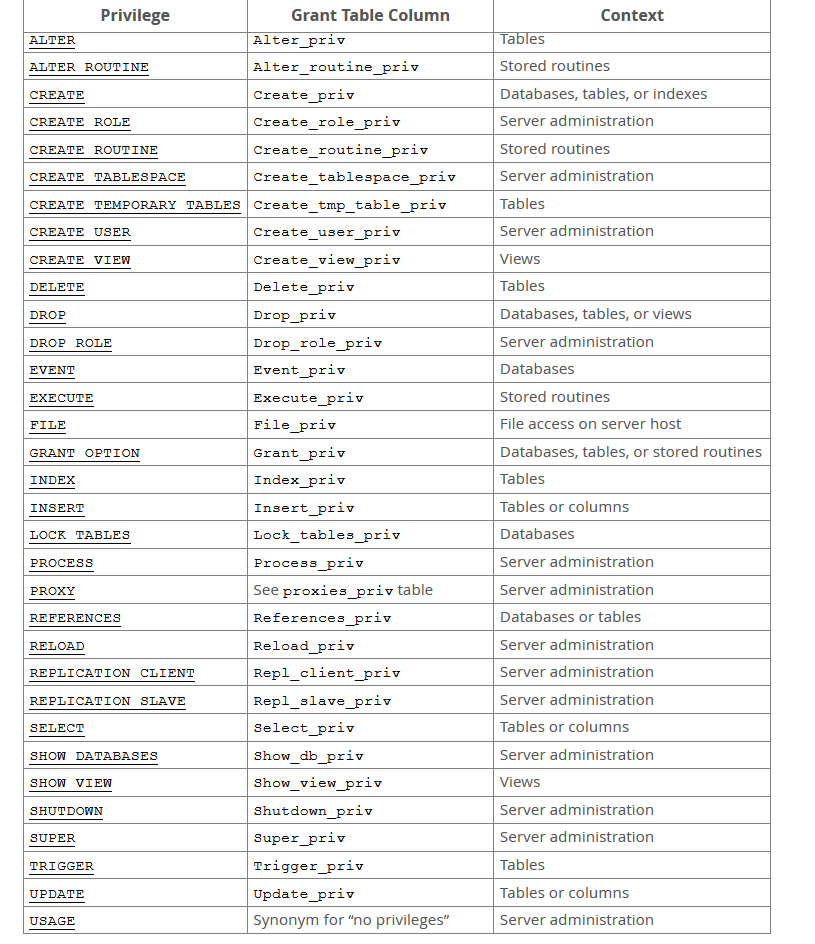
systemctl restart mariadb

Showing all db users

SELECT host, user FROM mysql.user;

**ALL PRIVILEGES**

grant privilegename on databasename.\* to esh'@'localhost



Backup MSQL

mkdir /backup

cd /backup

mysqldump -u root -p --all-databases > allbackup.sql

(with date stamp)

mysqldump -u root -p --all-databases > /data/backup/backup$(date +%Y-%m-%d-%H.%M.%S).sql

(crontab command )

vi /root/.mylogin.cnf

[client]

user = root

password = $meetcai19

/usr/bin/mysqldump --defaults-extra-file=/root/.mylogin.cnf -u root --all-databases > /data/backup/backup$(date +%Y-%m-%d).sql

Restore MSQL

mysql -u root -p < allbackup.sql

**SPEEDTEST ON LINUX**

yum install python

wget -O speedtest-cli <https://raw.githubusercontent.com/sivel/speedtest-cli/master/speedtest.py>

chmod +x speedtest-cli

./speedtest-cli

**LOAD BALANCING (HAPROXY)**

DNS Round Robin: no monitoring

LVS (linux virtual server): kernel level load balancing

Ldirectord

Haproxy (proxy and load balanced)

Algorithms

* Roundrobin: each new connection is handled by the next backend server
* Lastconn: A new connnection is handled by the backend server with the least amount of current connections
* Source: the client ip is hashed and same backend server is taking care of this IP

LB1 (test3 192.168.1.172) > yum install -y haproxy

vi /etc/haproxy/haproxy.cfg

#---------------------------------------------------------------------

# Global settings

#---------------------------------------------------------------------

global

log 127.0.0.1 local2 #Log configuration

chroot /var/lib/haproxy

pidfile /var/run/haproxy.pid

maxconn 4000

user haproxy #Haproxy running under user and group "haproxy"

group haproxy

daemon

# turn on stats unix socket

stats socket /var/lib/haproxy/stats

#---------------------------------------------------------------------

# common defaults that all the 'listen' and 'backend' sections will

# use if not designated in their block

#---------------------------------------------------------------------

defaults

mode http

log global

option httplog

option dontlognull

option http-server-close

option forwardfor except 127.0.0.0/8

option redispatch

retries 3

timeout http-request 10s

timeout queue 1m

timeout connect 10s

timeout client 1m

timeout server 1m

timeout http-keep-alive 10s

timeout check 10s

maxconn 3000

#---------------------------------------------------------------------

#HAProxy Monitoring Config

#---------------------------------------------------------------------

listen haproxy3-monitoring \*:8080 #Haproxy Monitoring run on port 8080

mode http

option forwardfor

option httpclose

stats enable

stats show-legends

stats refresh 5s

stats uri /stats #URL for HAProxy monitoring

stats realm Haproxy\ Statistics

stats auth howtoforge:howtoforge #User and Password for login to the monitoring dashboard

stats admin if TRUE

default\_backend app-main #This is optionally for monitoring backend

#---------------------------------------------------------------------

# FrontEnd Configuration

#---------------------------------------------------------------------

frontend main

bind \*:80

option http-server-close

option forwardfor

default\_backend app-main

#---------------------------------------------------------------------

# BackEnd roundrobin as balance algorithm

#---------------------------------------------------------------------

backend app-main

balance roundrobin #Balance algorithm

option httpchk HEAD / HTTP/1.1\r\nHost:\ localhost #Check the server application is up and healty - 200 status code

server test1 192.168.1.170:80 check

server test2 192.168.1.171:80 check

systemctl enable haproxy

systemctl start haproxy

App1> httpd kurulu (test1>192.168.1.170)

App2> httpd kurulu (test2>192.168.1.171)

Bütün sunucuların /etc/hosts dosyasında birbirlerinin IP’lerini yaz

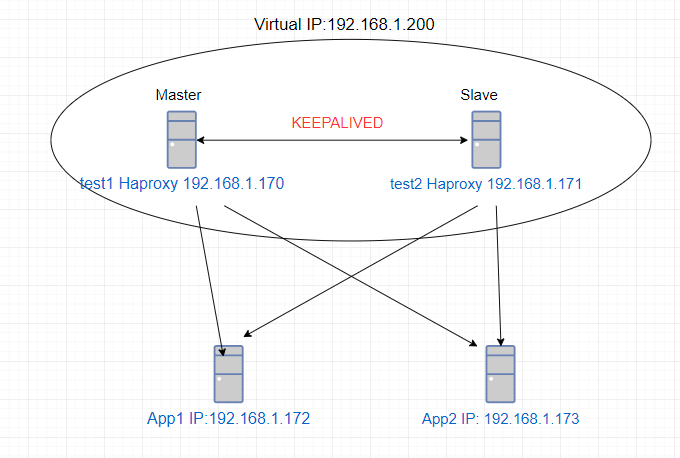
Web Monitoring

<http://192.168.1.172:8080/stats>

username: howtoforge

password: howtoforge

Keepalived



LB1(192.168.1.170-ens33 interface test1-haproxy) +keepalived

LB2(192.168.1.171-ens33 interface test2-haproxy) +keepalived

yum install gcc kernel-headers kernel-devel

yum install keepalived

LB1> /etc/keepalived/keepalived.conf

global\_defs {

notification\_email {

sysadmin@mydomain.com

support@mydomain.com

}

notification\_email\_from lb1@mydomain.com

smtp\_server localhost

smtp\_connect\_timeout 30

}

vrrp\_instance VI\_1 {

state MASTER

interface ens33

virtual\_router\_id 51

priority 101

advert\_int 1

authentication {

auth\_type PASS

auth\_pass 1111

}

virtual\_ipaddress {

192.168.1.200

}

}

LB2> /etc/keepalived/keepalived.conf

global\_defs {

notification\_email {

sysadmin@mydomain.com

support@mydomain.com

}

notification\_email\_from lb1@mydomain.com

smtp\_server localhost

smtp\_connect\_timeout 30

}

vrrp\_instance VI\_1 {

state MASTER

interface ens33

virtual\_router\_id 51

priority 100

advert\_int 1

authentication {

auth\_type PASS

auth\_pass 1111

}

virtual\_ipaddress {

192.168.1.200

}

}

App1 (192.168.1.172 test3) > httpd installed

App2 (192.168.1.173 test4)> httpd installed

**HIGH AVAILABILTY (HA)**

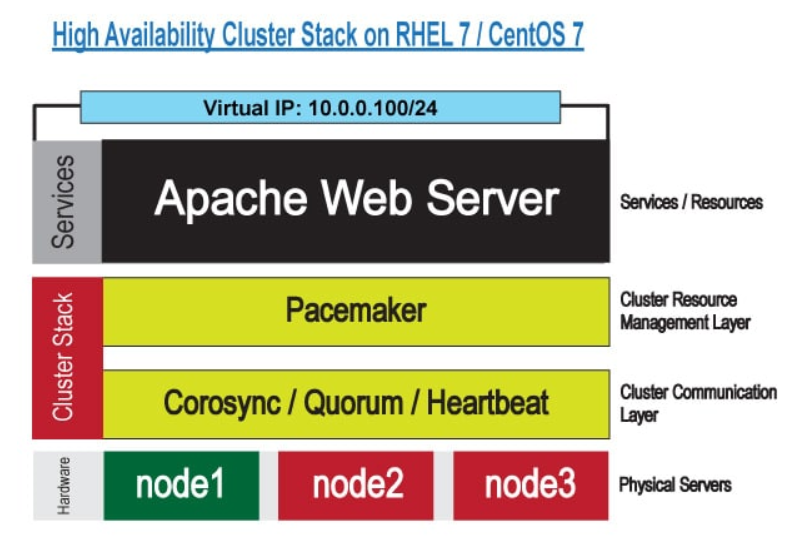
Common storage

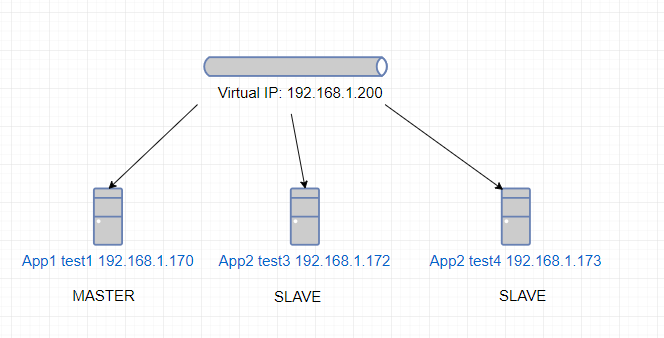
**Drbd:** every server has local storage (block level synch between storages)

Active-passive

**İscsi:** Seperate iscsi target, servers has access to target (serverların sdb si iscsi storage kullanır)

Clustered file systems: GFS





Corosync > cluster engine

Pacemaker> cluster resource manager

Active-Passive Cluster > The web cluster will get addressed by its virtual IP address and will automatically fail over if a node fails.

users will access your web application by the virtual IP address

Nodes should have fixed IP address

/etc/hosts file should be filled with node IP address

Test2: 192.168.1.171 web server (not necessary to start service)

Test3:192.168.1.172 web server (not necessary to start service)

Test4:192.168.1.173 web server (not necessary to start service)

Apache resource agent uses the Apache server status page for checking the health of the Apache service.

@ Test2,test3,test4

yum install epel-release

yum -y install corosync pacemaker pcs

systemctl enable pcsd ; systemctl enable corosync ; systemctl enable pacemaker

systemctl start pcsd

passwd hacluster

@ test2

pcs cluster auth test2 test3 test4

username: hacluster

pcs cluster setup --name yigitcluster test2 test3 test4

firewall-cmd --permanent --add-service=high-availability

firewall-cmd –reload

pcs cluster start --all

pcs cluster stop test2,test3,test4

pcs cluster enable --all

pcs status cluster

pcs status

Configuration file: vi /etc/corosync/corosync.conf

On test2

pcs property set no-quorum-policy=ignore

pcs property set stonith-enabled=false

pcs property set default-resource-stickiness="INFINITY" (disable autofailback)

pcs property list

vi /etc/httpd/conf.d/server\_status.conf

ExtendedStatus On

<Location /server-status>

SetHandler server-status

Require local

</Location>

Set Virtual IP address (on test2)

pcs resource create Virtual\_IP ocf:heartbeat:IPaddr2 ip=192.168.1.200 cidr\_netmask=24 op monitor interval=30s

Add httpd resources

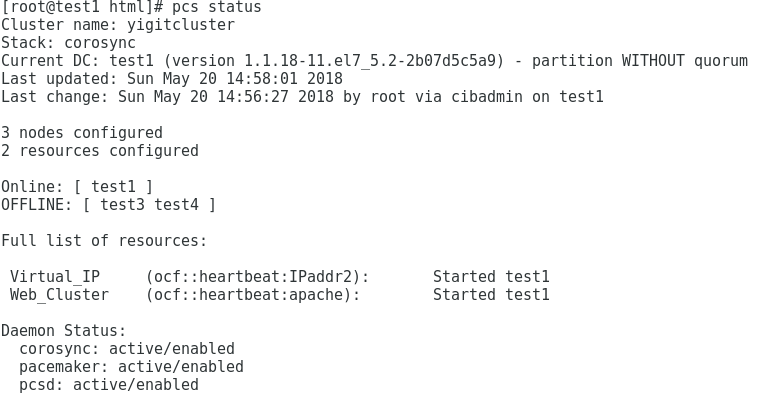
pcs resource create Web\_Cluster ocf:heartbeat:apache configfile=/etc/httpd/conf/httpd.conf statusurl="http://127.0.0.1/server-status" op monitor interval=1min

pcs constraint colocation add Web\_Cluster with Virtual\_IP INFINITY (two resource are on same host)

pcs constraint order Virtual\_IP then Web\_Cluster

pcs status resources





**OPENLDAP**

Ldap 389 ldaps 636

Distinguished name example

dn: o=”Organization name” c=”Country” postalAddress=”postaddress”

Attributes (are not case insensitive)

1. Organization Name (o)

2. Mailing address (postalAddress)

3. Locality (l), which may be the name of a city, town, village, and so forth

4. State or Province (st)

5. Postal Code or ZIP Code (postalCode)

6. Country (c,CountryName)

7. Telephone Number (telephoneNumber)

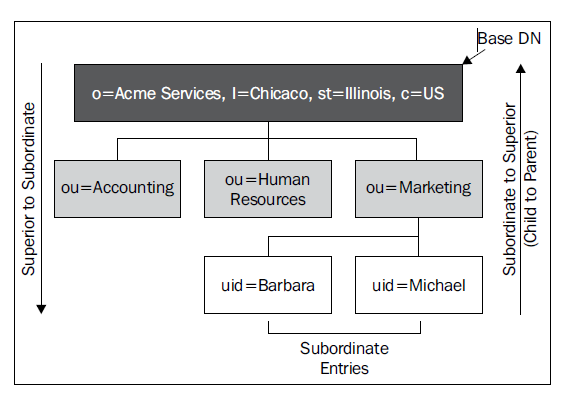
8. Object Class (objectclass), which specifies what type (or types) of record this entry is

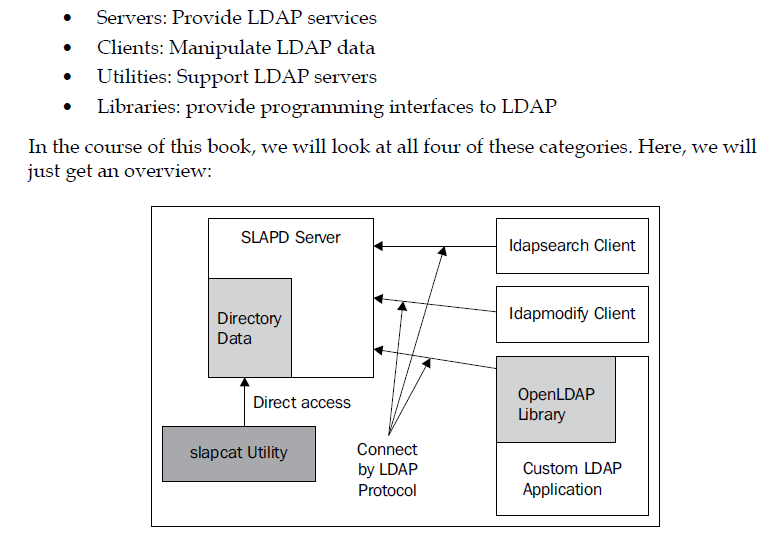
9. Givenname

\* Attributes can have more than one value

\* Attributes are defined in attribute definitions(in schema)

DIT= Directory information tree (organized collection of entries)





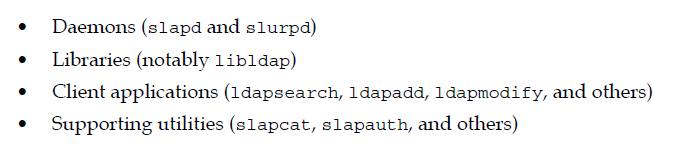
SLAPD- Standalone LDAP Daemon

slapd> handles client requests and directory management

slurpd> manages replicating changes to other directories

Client> ldap-utils

Client connects to directory server and then bind(authenticate) and then perform operations



Centos7 OPENLDAP SERVER Installation and Configuration

yum -y install openldap compat-openldap openldap-clients openldap-servers openldap-servers-sql openldap-devel

systemctl start slapd

systemctl enable slapd

(getting version) /usr/sbin/slapd -V

nmap ile 389/tcp open ldap açık olduğu kontrol edilir

creating root password:

slappasswd -h {SSHA} -s lapland23

output: {SSHA}sPWy6xNxsPm7T8tYkf1fYkbYix0Opb8A

Configuration File: /etc/openldap/slapd.d/

cd /etc/openldap

vi db.ldif

dn: olcDatabase={2}hdb,cn=config

changetype: modify

replace: olcSuffix

olcSuffix: dc=yaydog,dc=local

dn: olcDatabase={2}hdb,cn=config

changetype: modify

replace: olcRootDN

olcRootDN: cn=ldapadmin,dc=yaydog,dc=local

dn: olcDatabase={2}hdb,cn=config

changetype: modify

replace: olcRootPW

olcRootPW: {SSHA}sPWy6xNxsPm7T8tYkf1fYkbYix0Opb8A

ldapmodify -Y EXTERNAL -H ldapi:/// -f db.ldif

vi monitor.ldif

olcAccess

olcAccess: {0}to \* by dn.base="gidNumber=0+uidNumber=0,cn=peercred,cn=external, cn=auth" read by dn.base="cn=ldapadmin,dc=yaydog,dc=local" read by \* none

ldapmodify -Y EXTERNAL -H ldapi:/// -f monitor.ldif

cp /usr/share/openldap-servers/DB\_CONFIG.example /var/lib/ldap/DB\_CONFIG

cd /etc/openldap

ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/cosine.ldif

ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/nis.ldif

ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/inetorgperson.ldif

ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/ppolicy.ldif

vi base.ldif

dn: dc=yaydog,dc=local

dc: yaydog

objectClass: top

objectClass: domain

dn: cn=ldapadmin ,dc=yaydog,dc=local

objectClass: organizationalRole

cn: ldapadmin

description: LDAP Manager

dn: ou=ActivePeople,dc=yaydog,dc=local

objectClass: organizationalUnit

ou: ActivePeople

dn: ou=DisaledPeople,dc=yaydog,dc=local

objectClass: organizationalUnit

ou: DisaledPeople

ldapadd -x -W -D "cn=ldapadmin,dc=yaydog,dc=local" -f base.ldif

creating user (LDIF Format)

cd /etc/openldap

vi ldapuser1.ldif

dn: uid=ldapuser1,ou=ActivePeople,dc=yaydog,dc=local

objectClass: top

objectClass: account

objectClass: posixAccount

objectClass: shadowAccount

cn: ldapuser1

uid: ldapuser1

uidNumber: 9999

gidNumber: 100

homeDirectory: /home/ldapuser1

loginShell: /bin/bash

gecos: standarduser

userPassword: {crypt}x

shadowLastChange: 17058

shadowMin: 0

shadowMax: 99999

shadowWarning: 7

userPassword: {SSHA}71xEB2E59cuoPEQLErY44bYMHwCCgbtR (slappasswd ile üretilen şifre girilir)

(creating user)

ldapadd -x -W -D "cn=ldapadmin,dc=yaydog,dc=local" -f ldapuser1.ldif

(changing password of the user)

ldappasswd -s lapland23 -W -D "cn=ldapadmin,dc=yaydog,dc=local" -x "uid=ldapuser11,ou=ActivePeople,dc=yaydog,dc=local"

QUERY

Simple Bind(clients provide full DN), and through an SASL(simple authentication and security layer) Bind

Binding process Flags

-D: the full DN of the user who will bind to the directory server (this is used for simple binding).

-W: user should provide password interactively

-w : takes password as string from command line

-x : simple bind

-H : ldap url ldap://<ip>:389

-h : ldap hostname

-b :base DN

-f : take filename as parameter

(var olan kullanıcıyı sorgulamak)

slapcat -a '(uid=ldapuser1)'

ldapsearch -x -W -D 'cn=ldapadmin,dc=yaydog,dc=local' -b 'ou=ActivePeople,dc=yaydog,dc=local' '(uid=ldapuser1)'

(kullanıcıya ait sadace belirli parametreleri sorgular)

ldapsearch -x -W -D 'cn=ldapadmin,dc=yaydog,dc=local' -b 'ou=ActivePeople,dc=yaydog,dc=local' -LLL '(uid=ldapuser11)' gecos uidNumber

ldapsearch -x cn=ldapadmin -b dc=yaydog,dc=local (privledge user)

(tüm directory’i export etmek)

slapcat -l basics-out.ldif

(deleting user)

ldapdelete -W -D "cn=ldapadmin,dc=yaydog,dc=local" "uid=ldapuser1,ou= ActivePeople,dc=yaydog,dc=local"

(checking user attribute if it is true or false)

ldapcompare -x -W -D 'cn=ldapadmin,dc=yaydog,dc=local' 'uid=ldapuser1,ou=ActivePeople,dc=yaydog,dc=local' 'loginShell: /bin/bash'

ldapuser1 kullanıcısının login shell inin /bin/bash olurp olmadığını sorgular

(kullanıcının attr.lerini değiştirmek)

ldapmodrdn -x -W -D 'cn=ldapadmin,dc=yaydog,dc=local' -r 'uid=ldapuser1,ou=ActivePeople,dc=yaydog,dc=local' 'uid=ldapuser11'

(kullanıcının şifresini değiştirmek)

ldappasswd -x -D "cn=ldapadmin,dc=yaydog,dc=local" -W -S "uid=ldapuser11,ou=ActivePeople,dc=yaydog,dc=local"

Password Policy

* pwdMinAge= how much time must pass (in seconds) between the last time the password was changed and the next time SLAPD will allow the password to be changed.
* pwdMaxAge= how long (in seconds) a password will be considered good, calculated from the time when the password was last changed. After the elapsed time, the password will be marked as expired
* pwdInHistory
* pwdMinLength
* pwdExpireWarning: provide a warning to the user when the user logs in. takes the time, in seconds, prior to when the password expires that it should start warning the user
* pwdGraceAuthNLimit: specify how many grace logins a user with an expired password will be allowed before the account is locked.
* pwdLockout: this is turned on, then when a user fails to bind a certain number of times (pwdMaxFailures) in a row, then the account will be locked for some duration of time (pwdLockoutDuration). To turn on pwdLockout, which is off by default, set the value of this attribute to TRUE.
* pwdMustChange: determines whether or not a user must change their password after an administrator sets it.

**LDAP CLIENT**

yum install openldap-clients nss-pam-ldap nscd -y

yum install auth\* sssd\* krb5-workstation -y

yum install authconfig-gtk

yum install libsss\_autofs

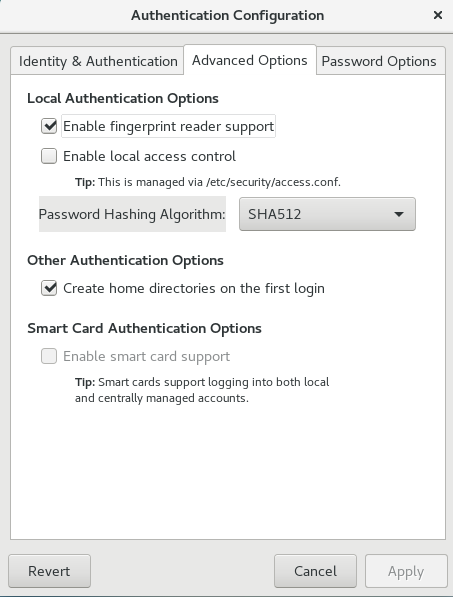
yum install nf-utils autofs

Arayüzden LDAP Client ayarları:

system-config-authentication OR authconfig-tui

Ldap search Base DN

dc=yaydog,dc=local



systemctl enable sssd.service

systemctl start sssd.service

LDAP kullanıcısını sorgulamak getent passwd “username”

**ONLINE TEST LDAP SERVER**

<https://www.forumsys.com/tutorials/integration-how-to/ldap/online-ldap-test-server/>

Automount ldap user directories

yum install autofs

vi /etc/auto.master.d/home.autofs

/home/guests /etc/auto.home

vi /etc/auto.home

ldapuser0 -rw,sync example.com:/home/guests/&

systemctl enable autofs.service

Client(Centos) makinesini AD ye bağlamak

Backup /etc/nsswitch.conf

Open port 88

yum install sssd realmd oddjob oddjob-mkhomedir adcli samba-common samba-common-tools krb5-workstation openldap-clients policycoreutils-python -y

vi /etc/resolv.conf

search yaydog.local

nameserver AD DC IP

realm join --user=administrator yaydog.local (bu işlem sonrası DC de bilgisayar ismi çıkar ve dns kaydı gelir)

systemctl restart sssd

bu işlemden sonra linux sunucuya yaydog\administrator hesabıyla sunucuya girilir

visudo

administrator@yaydog.local ALL=(ALL) ALL

(bu işlem ile DC deki domain admin hesabının linux sunucuda root yetkisi sağlanır)

(Leaving the domain)

realm leave yaydog.local

PHP LDAP ADMIN

yum install epel-release

yum install -y phpldapadmin

vi /etc/httpd/conf.d/phpldapadmin.conf

#

# Web-based tool for managing LDAP servers

#

Alias /phpldapadmin /usr/share/phpldapadmin/htdocs

Alias /ldapadmin /usr/share/phpldapadmin/htdocs

<Directory /usr/share/phpldapadmin/htdocs>

<IfModule mod\_authz\_core.c>

# Apache 2.4

Require all granted

</IfModule>

<IfModule !mod\_authz\_core.c>

# Apache 2.2

Order Deny,Allow

Deny from all

Allow from 127.0.0.1

Allow from ::1

</IfModule>

</Directory>

systemctl restart httpd.service

vi /etc/phpldapadmin/config.php

$servers->setValue('server','name','YIGITAYDOG LDAP SERVER');

$servers->setValue('server','host','127.0.0.1');

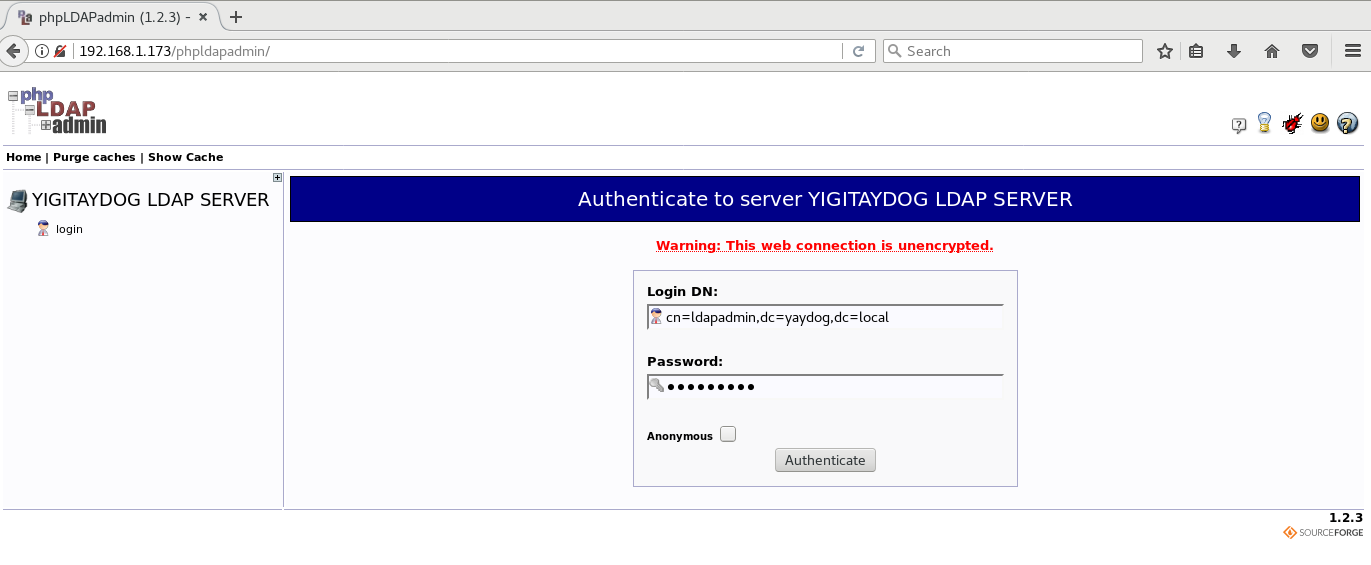
$servers->setValue('login','attr','dn');

// $servers->setValue('login','attr','uid');

systemctl restart httpd.service

<http://ipaddress_of_ldap_server/phpldapadmin/>

cn=ldapadmin ,dc=yaydog,dc=local



Creating Password Policy

ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/ppolicy.ldif

vi passpol.ldif

dn: cn=module,cn=config

objectClass: olcModuleList

cn: module

olcModulePath: /usr/lib64/openldap

olcModuleLoad: ppolicy.la

dn: olcOverlay=ppolicy,olcDatabase={2}hdb,cn=config

objectClass: olcPPolicyConfig

olcPPolicyDefault: cn=ppolicy,ou=Policies,dc=yaydog,dc=local

ldapadd -Y EXTERNAL -H ldapi:/// -f passpol.ldif

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

vi defaultpasspol.ldif

# Creates a Policy object in Policies OU (Organizational Unit)

dn: cn=defaultpasswordpolicy,dc=yaydog,dc=local

objectClass: top

objectClass: device

objectClass: pwdPolicy

cn: default

pwdAttribute: userPassword

pwdMaxAge: 3888000

pwdExpireWarning: 604800

pwdInHistory: 3

pwdCheckQuality: 1

pwdMinLength: 8

pwdMaxFailure: 5

pwdLockout: TRUE

pwdLockoutDuration: 86400

pwdGraceAuthNLimit: 0

pwdFailureCountInterval: 0

pwdMustChange: TRUE

pwdAllowUserChange: TRUE

pwdSafeModify: FALSE

**ACTIVATING LDAPS WITH SELF SIGNED CERT**

cd /etc/pki/tls/certs

echo "03" >> file.srl

openssl req -out ca.pem -new -x509

openssl genrsa -out server.key 1024

openssl req -key server.key -new -out server.req

openssl x509 -req -in server.req -CA ca.pem -CAkey privkey.pem -CAserial file.srl -out server.pem

/etc/pki/tls/certs altına ca.pem, server.pem, server.key dosyaları gelir

vim /etc/sysconfig/slapd

SLAPD\_URLS="ldapi:/// ldap:/// ldaps:///"

vim /root/ldif/mod\_ssl.ldif

dn: cn=config

changetype: modify

replace: olcTLSVerifyClient

olcTLSVerifyClient: allow

-

replace: olcTLSCACertificateFile

olcTLSCACertificateFile: /etc/pki/tls/certs/ca.pem

-

replace: olcTLSCertificateFile

olcTLSCertificateFile: /etc/pki/tls/certs/server.pem

-

replace: olcTLSCertificateKeyFile

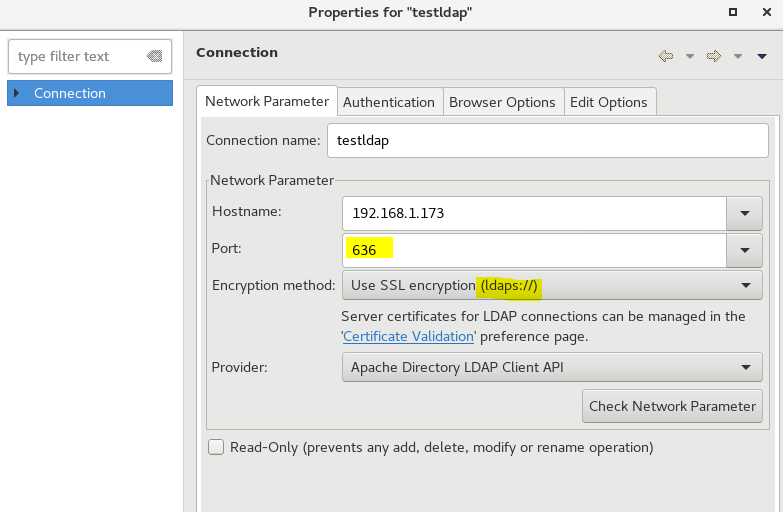
olcTLSCertificateKeyFile: /etc/pki/tls/certs/server.key

ldapmodify -Y EXTERNAL -H ldapi:/// -f mod\_ssl.ldif

vi /etc/openldap/ldap.conf

TLS\_REQCERT allow

systemctl restart slapd



**AUDITING**

* Monitoring file access
* Monitoring system changes
* Recording commands run by user
* Monitoring network access rules

(audit log files)

/var/log/audit/audit.log

yum install audit audit-libs

systemctl enable auditd

service auditd start

service auditd rotate (forces log rotation)

(configuration file)

vi /etc/audit/auditd.conf

num\_logs = 10 (number of audit log files kept in server)

max\_log\_file = 30 (maximum log file size in MB)

max\_log\_file\_action = ROTATE

(persistent rules should be created)

/etc/audit/rules.d/audit.rules

(file system and file monitoring)

-w “path” -p “permission” -k “keyname”

-w /etc/hosts -p wa -k hostsfile\_change

-w /etc/passwd -p wa -k passwd\_change

-w /etc/selinux -p wa -k selinux\_rule

-a always,exit -F path=/root/file.txt -F perm=wa -k filetxt\_change

-a always,exit -F arch=b64 -F -F auid=1001 -S open -k userfileaccess

(precreated rules)

/usr/share/doc/audit-2.8.5/rules

(creating audit reports)

ausearch -k hostsfile\_change

ausearch -a "eventidno" (event idsi girilen olaylari sorgular)

aureport -f -i (auditctl'e girilen path'lerle ilgili degisimleri gözlemler)

ausearch -f /etc/httpd/conf.d/php.conf -i (spesifik path ile ilgili yapilan tüm isleri gösterir)

ausearch -ts 03/04/2014 -k hostsfile\_change

**COMPLIANCE MONITORING (OPENSCAP)**

Ensure that hosts fits compliances

yum install scap-workbench openscap-scanner scap-security-guide -y (install it on remote and local machine)

running: scap-workbench

**POSTFIX CONFIGURATION**

yum remove sendmail

yum install cyrus-sasl-plain

yum install postfix -y

systemctl enable postfix

firewall-cmd --permanent --add-service=smtp

firewall-cmd --reload

vi /etc/postfix/main.cf

:99 myorigin = $myhostname

:116 inet\_interfaces = loopback-only

:164 mydestination =

:165 local\_transport= error: local delivery disabled

:264 mynetworks = 127.0.0.0/8 [::1]/128

:316 relayhost = [smtp.example.com]:587

#smtp\_use\_tls=no

smtp\_sasl\_auth\_enable=yes

smtp\_sasl\_password\_maps=hash:/etc/postfix/sasl\_password

#smtp\_tls\_CAfile= /etc/ssl/certs/ca-bundle.crt

smtp\_sasl\_security\_options= noanonymous

#smtp\_sasl\_tls\_security\_options= noanonymous

vi /etc/postfix/sasl\_password

[smtp.example.com]:587 [example@example.com:password](mailto:example@example.com:password)

postmap /etc/postfix/sasl\_password

chown root:postfix /etc/postfix/sasl\_password

chmod 640 /etc/postfix/sasl\_password

systemctl restart postfix

(client settings)

yum install mailx

echo "Your message" | mail -s "Message Subject" example@example.com

postqueue -p : Mail queue is empty

tail -f /var/log/maillog

**NGINX**

vi /etc/yum.repos.d/nginx.repo

[nginx]

name=nginx repo

baseurl=http://nginx.org/packages/mainline/centos/7/$basearch/

gpgcheck=0

enabled=1

yum update

yum install -y nginx

systemctl start-stop-resart nginx

nginx -s reload (reloads config files)

configuration file syntax check: /usr/sbin/nginx -t

/usr/sbin/nginx -t -c /etc/nginx/conf.d/default.conf

/usr/sbin/nginx -v

Main configuration file: vi /etc/nginx/nginx.conf

Worker process= implies that the execution is delegated to core of your CPU.

worker\_processes X worker\_connections = server will threat this number of total connections

**sendfile** > If this directive is enabled, Nginx uses the sendfile kernel call to handle file transmission. If disabled, Nginx handles the file transfer by itself.

**keepalive\_requests>** This specifies the maximum number of requests served over a single keep-aliveconnection.

**keepalive\_timeout** > number of seconds the server will wait before closing a keep-alive connection.

The intended effect is to let the client browser close the connection itself after this period has elapsed.

**send\_timeout >**This specifies the amount of time after which Nginx closes an inactiveconnection. A connection becomes inactive the moment a client stopstransmitting data.

Real Time Statistics of a page

yum install epel-release

yum install python-pip

pip install ngxtop

ngxtop -l /var/log/nginx/access.log

**SSL**

cd /wwwroot

openssl req -x509 -new -newkey rsa:2048 -nodes -keyout private.key -out public.pem -days 600

vi /etc/nginx/conf.d/default.conf

server {

listen 443 ssl ;

server\_name test1.yaydog.local;

ssl\_certificate /wwwroot/public.pem;

ssl\_certificate\_key /wwwroot/private.key;

ssl\_protocols TLSv1 TLSv1.1 TLSv1.2;

ssl\_ciphers HIGH:!aNULL:!MD5;

access\_log /var/log/nginx/ssl.access.log combined;

root /wwwroot/app1;

index index.html; #This defines the default page that Nginx will serve if no filename is specified in the request

error\_page 404 /404.html;

error\_page 500 502 503 504 /50x.html;

location = /50x.html {

root /usr/share/nginx/html;

}

}

<https://test1.yaydog.local/app1.html>

Performance Tests

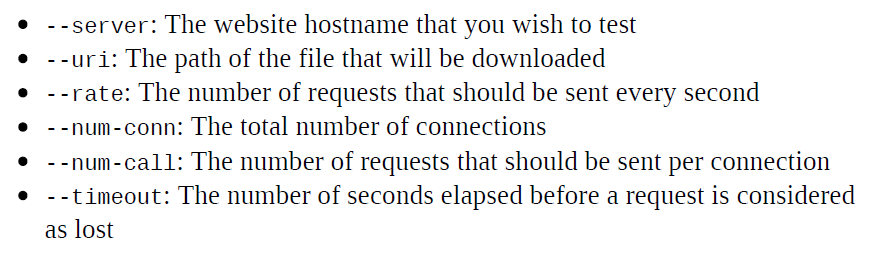
HTTPPERF

wget <http://ftp.tu-chemnitz.de/pub/linux/dag/redhat/el7/en/x86_64/rpmforge/RPMS/rpmforge-release-0.5.3-1.el7.rf.x86_64.rpm>

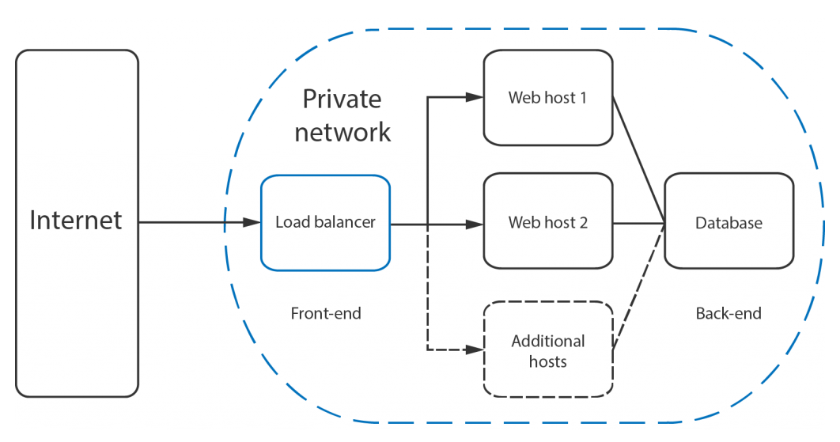
rpm -Uvh rpmforge-release-0.5.3-1.el7.rf.x86\_64.rpm

yum install httperf

httperf --server 192.168.1.100 --port 80 --uri /app1.html --rate 300 --num-conn 30000 --num-call 1 --timeout 5



**LOAD BALANCING**



**RoundRobin**

*Does not consider server loads and response times*

192.168.1.100 test1.yaydog.local (LoadBalancer)

192.168.1.101 test2.yaydog.local

192.168.1.102 test3.yaydog.local

@test1

rm /etc/nginx/conf.d/default.conf

vi /etc/nginx/conf.d/load-balancer.conf

upstream backend {

server test1.yaydog.local;

server test2.yaydog.local weight=2;

server test3.yaydog.local;

}

server {

listen 80;

server\_name test1.yaydog.local;

access\_log /var/log/nginx/load-access.log combined;

location / {

proxy\_pass http://backend;

}

}

@test2

@test3

vi /etc/nginx/conf.d/default.conf

server {

listen 80;

server\_name test2.yaydog.local;

#charset koi8-r;

#access\_log /var/log/nginx/host.access.log main;

location / {

root /wwwroot;

index index.html index.htm;

}

error\_page 404 /404.html;

error\_page 500 502 503 504 /50x.html;

location = /50x.html {

root /usr/share/nginx/html;

}

}

**LeastConnections**

*As new requests comes in, loadbalancer directs requests according to connections that backends have*

@test1

vi /etc/nginx/conf.d/load-balancer.conf

upstream backend {

least\_conn; #sadece bu satır eklenir

server test1.yaydog.local;

server test2.yaydog.local;

server test3.yaydog.local;

}

**Hash Based**

IP hashing uses the visitors IP address as a key to determine which host should be selected to server the request. This allows the visitors to be each time directed to the same server

@test1

vi /etc/nginx/conf.d/load-balancer.conf

upstream backend {

ip\_hash; #sadece bu satır eklenir

server test1.yaydog.local;

server test2.yaydog.local;

server test3.yaydog.local;

}

Health checks

@test1

vi /etc/nginx/conf.d/load-balancer.conf

upstream backend {

server test1.yaydog.local;

server test2.yaydog.local weight=2 max\_fails=3 fail\_timeout=30s;

server test3.yaydog.local;

}

Max fails= number of health check attempts

Fail timeout=defines how long the server should be considered failed

PHPv7+Nginx

yum install epel-release -y

yum install -y wget

wget http://rpms.famillecollet.com/enterprise/remi-release-7.rpm

rpm -Uvh remi-release-7.rpm

rm -rf remi-release-7

yum install -y yum-utils

yum-config-manager --enable remi-php70

yum-config-manager --enable remi

yum install php (remi-php70)

yum install php-fpm

systemctl enable php-fpm

yum install -y php-mysql php-pdo php-mcrypt php-mbstring php-xml php-soap php-imap php-pear php-ioncube-loader php-ldap php-bcmath (optional)

rm /etc/nginx/conf.d/default.conf

vi /etc/nginx/conf.d/default.conf

server {

listen 80;

server\_name test2.yaydog.local;

access\_log /var/log/nginx/host.access.log main;

root /wwwroot;

index index.php index.html index.htm; #sıralaması önemli

location / {

try\_files $uri $uri/ =404;

}

error\_page 404 /404.html;

error\_page 500 502 503 504 /50x.html;

location = /50x.html {

root /usr/share/nginx/html;

}

location ~ \.php$ {

try\_files $uri =404;

fastcgi\_pass unix:/var/run/php-fpm/php-fpm.sock;

fastcgi\_index index.php;

fastcgi\_param SCRIPT\_FILENAME $document\_root$fastcgi\_script\_name;

include fastcgi\_params;

}

}

vi /etc/php-fpm.d/www.conf

listen = /var/run/php-fpm/php-fpm.sock

listen.owner = nginx

listen.group = nginx

user = nginx

group = nginx

systemctl restart nginx

systemctl restart php-fpm.service

/wwwroot altına index.php

<?php

phpinfo();

?>

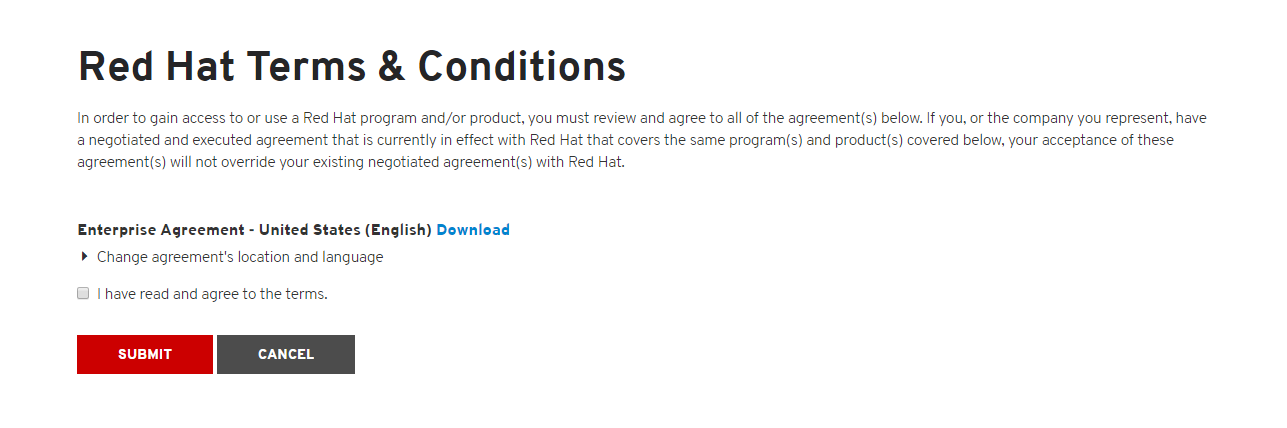
**REDHAT REGISTIRATION-**Red Hat Subscription Manager (RHSM)-

subscription-manager clean

subscription-manager register --username “username” --password “password” --auto-attach --force

(enable extra repository)

subscription-manager repos --enable rhel-7-server-extras-rpms



<https://access.redhat.com/solutions/253273>

subscription-manager status

subscription-manager subscribe>> daha onceden kayıtlı olmus cihazları subscribe eder

**SENDING MAIL FROM CENTOS 7**

yum install -y mailx

ln -s /bin/mailx /bin/email

vi /etc/mail.rc

set smtp=smtp.example.com:587

set smtp-auth=login

set smtp-auth-user=example@example.com

set smtp-auth-password=password

set ssl-verify=ignore

set nss-config-dir=/etc/pki/nssdb/

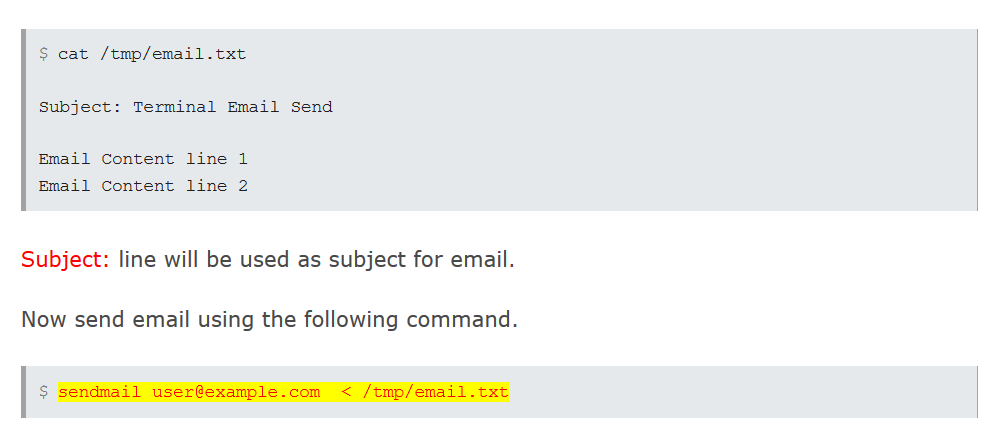
set from=example@example.com

echo "Your message" | mail -a /root/testfile.txt -s "Message Subject" example@example.com

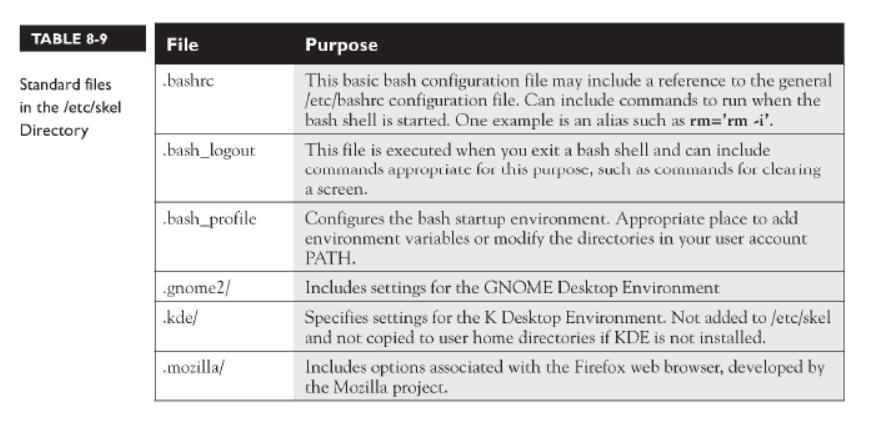
echo "Your message" | mail -s "Message Subject" example@example.com

**SENDMAIL CLIENT**

echo "Your message" | sendmail -s "Message Subject" example@example.com



**ENVIRONMENT VARIABLES**



Printenv :displays all environment variables

echo $environmentvariable : sadece belirtilen environment variable’ı gösterir

export environmentvariable=value

persistent

echo 'export environmentvariable="value"' >> $HOME/.bashrc

**INTRUSION DETECTION WITH AIDE**

(file and folders integrity checker)

* Permissions
* Size
* Access time
* Hash

yum install aide

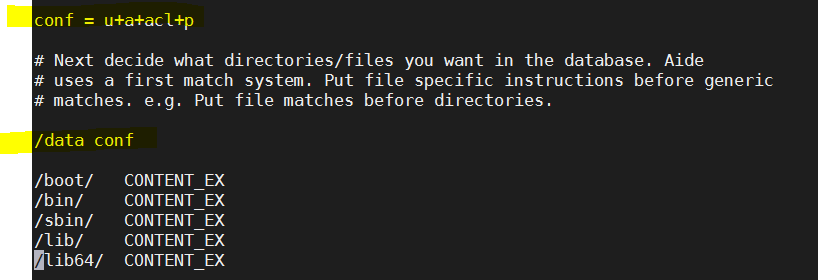
(do it for one time then use script)

/usr/sbin/aide --init

mv /var/lib/aide/aide.db.new.gz /var/lib/aide/aide.db.gz

Configuration file: /etc/aide.conf

(custom add monitoring rule)



access timestamp (atime), the modified timestamp (mtime), and the changed timestamp (ctime).

Daily intrusion analysis script

NOW=$( date '+%F\_%H:%M:%S' )

aide --check >> /var/lib/aide/"AideReport-"$NOW.txt

rm -rf /var/lib/aide/aide.db.gz

aide --init

mv /var/lib/aide/aide.db.new.gz /var/lib/aide/aide.db.gz

crontab>daily

**RESTRICTING USB ACCESS WITH USBGUARD**

Blacklist and whitelisting according to

* Device name
* Device hash
* Device serial
* Port id

Actions:

* Allow
* Reject
* Block

yum install usbguard –y

systemctl start usbguard.service

systemctl enable usbguard.service

Config file: vi /etc/usbguard/usbguard-daemon.conf

IPCAllowedUsers=root

IPCAllowedGroups= root

ImplicitPolicyTarget=block (block all devices that are not match rule)

(generate initial policy-allow currently plugged devices)

usbguard generate-policy /etc/usbguard/rules.conf

usbguard list-devices (shows connected usb devices)



(allowing device)

usbguard allow-device 1

(blocking device)

usbguard block-device 1

cd /root

vi rules.conf

allow name “nameofdevice”

install -m 600 -o root -g root rules.conf /etc/usbguard/rules.conf

systemctl restart usbguard.service

**RKHUNTER**

scanning tool. It helps you to scan out many exploits like backdoors, common exploits like – E-mail injection, Buffer overflows, format string bugs, and rootkits where the name originates from. Rkhunter is a UNIX based tool. The way of working, for rkhunter goes like that it compares SHA-1 hashes for important files with the known good files in an online database. It searches for hidden files, doubtful strings in kernel modules, default directories for rootkits,

yum install -y epel-release

yum install -y rkhunter

check latest version : rkhunter --versioncheck

$ sudo rkhunter --update

$ sudo rkhunter --propupd

rkhunter -c -sk (performs scan)

vi /etc/rkhunter.conf

[MAIL-ON-WARNING=yaydog@corendon-airlines.com](mailto:MAIL-ON-WARNING=yaydog@corendon-airlines.com)

MAIL\_CMD=mail -s "[rkhunter] Warnings found for ${HOST\_NAME}"

SCRIPTWHITELIST=/usr/bin/whatis (safe scripts)

**TIGER VNC**

IP: 192.168.1.211 >> örnekte iki farklı kullanıcı için VNC ayarları yapıldı

yum install tigervnc-server

su - yaydog

vncpasswd

cp /lib/systemd/system/vncserver@.service [/etc/systemd/system/vncserver@:1.service](mailto:/etc/systemd/system/vncserver@:1.service)

vi [/etc/systemd/system/vncserver@\:1.service](mailto:/etc/systemd/system/vncserver@\:1.service)

ExecStartPre=/bin/sh -c '/usr/bin/vncserver -kill %i > /dev/null 2>&1 || :'

ExecStart=/usr/sbin/runuser -l yaydog -c "/usr/bin/vncserver %i"

PIDFile=/home/yaydog/.vnc/%H%i.pid

ExecStop=/bin/sh -c '/usr/bin/vncserver -kill %i > /dev/null 2>&1 || :'

[Install]

WantedBy=multi-user.target

systemctl start vncserver@:1

systemctl status vncserver@:1

systemctl enable vncserver@:1





VNC Client for RHEL

yum install vinagre

vinagre

Remote Desktop Viewer

**KERNEL RUNTIME PARAMETERS**

sysctl -p : re-reads kernel parameters

sysctl -a: shows all kernel runtime parameters

/proc/sys/





(temporary)

sysctl -w net.ipv4.icmp\_echo\_ignore\_all=1 (default value=0)

sysctl net.ipv4.icmp\_echo\_ignore\_all (reading value)

(persistent)

vi /etc/sysctl.conf

net.ipv4.icmp\_echo\_ignore\_all=1

list loaded modules: lsmod

list loadable modules: find /lib/modules/$(uname -r) -type f -name \*.ko\*

load module: modprobe <MODULE>

remove module: modprobe -r <MODULE>

get info about module: modinfo <MODULE>

**SETTING ULIMIT VALUES PERMANENT**

/etc/security/limits.conf

Temporary e.x: ulimit -u “value”

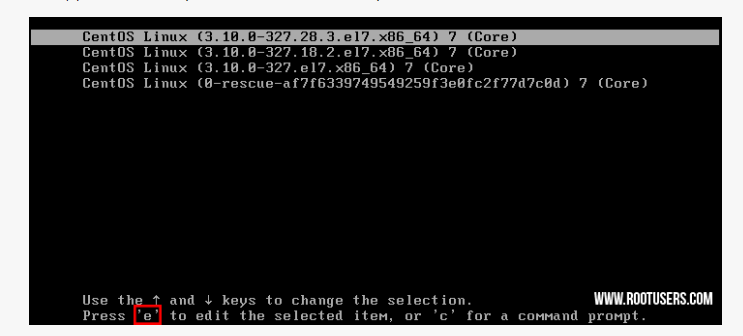
Show all ulimit values: ulimit -a

**KERNEL CRASHDUMPS REPORTS**

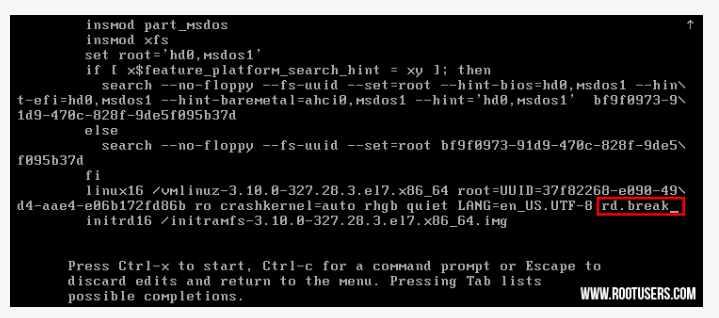
systemctl enable kdump && systemctl start kdump

Send crash dumps to Vendor on path /var/crash

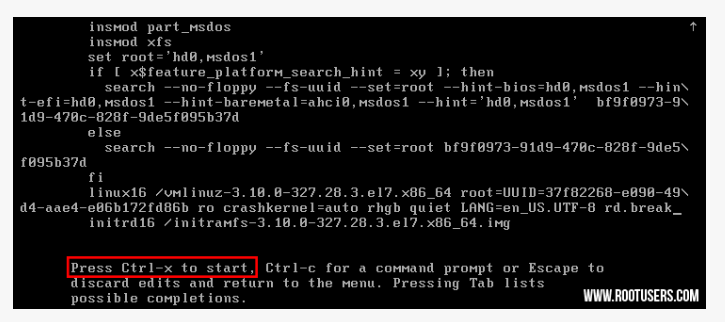
**HOW TO RECOVER ROOT PASSWORD**



1. rd.break

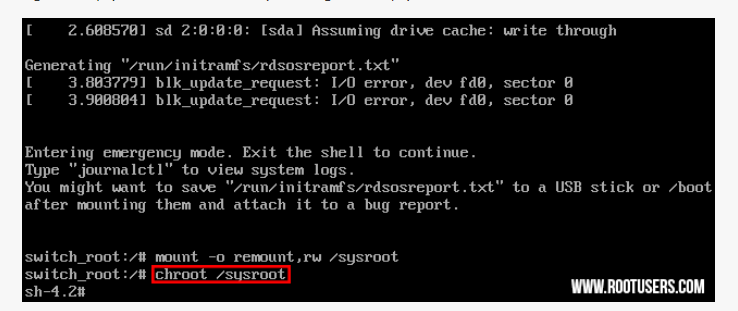


1. Ctrl+x yazılır

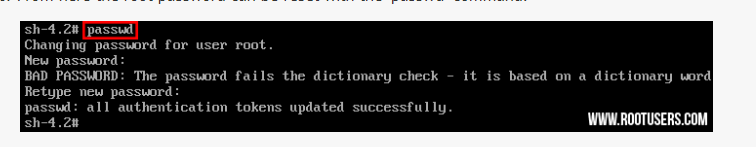


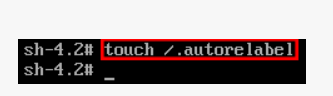
1. mount -o remount,rw /sysroot

chroot /sysroot



(4)Passwd ile yeni şifre belirlenir





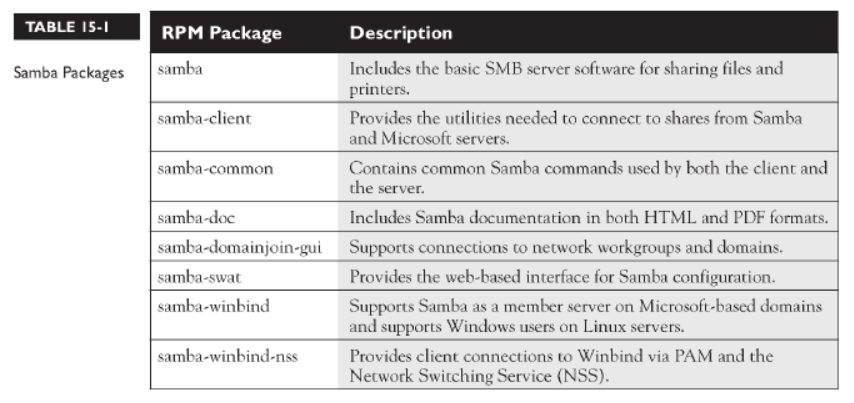


System reboots with new password

**SAMBA FILE SERVER**

Ports:137,138,139,445,901 tcp,udp

139/tcp open netbios-ssn



yum install samba samba-client samba-common -y

systemctl enable smb.service

systemctl enable nmb.service

systemctl restart smb.service

systemctl restart nmb.service

firewall-cmd --permanent --add-service=samba

firewall-cmd --permanent –add-port=137/udp

firewall-cmd --permanent –add-port=138/udp

firewall-cmd --reload

testparm> syntax check

smbstatus

smbstatus –shares (paylaşımları gosterir)

[root@centostest ~]# netstat -tp | grep smbd

tcp 0 0 centostest:microsoft-ds 192.168.1.132:49215 ESTABLISHED 18363/smbd

tcp 0 0 centostest:microsoft-ds 192.168.1.145:57313 ESTABLISHED 18346/smbd

smbd: dosya aktarımı ve kimlik dogrulamasını yönetir

nmbd: ad desteği ve tarama desteği sağlar

winbind: AD üyeliği için kullanılır

setsebool -P samba\_enable\_home\_dirs on

setsebool -P samba\_export\_all\_ro on

setsebool -P samba\_export\_all\_rw on

setsebool -P use\_samba\_home\_dirs on

setsebool -P samba\_share\_nfs on

mkdir /groupdir

semanage fcontext -a -t samba\_share\_t '/groupdir(/.\*)?'

restorecon -RFv /groupdir

smbpasswd -x: yaratılan kullanıcıları smb database’inden siler

SETTING READONLY SAMBA SHARE

useradd read-only-user

setfacl -m u: read-only-user:rx /groupdir

smbpasswd -a read-only-user

vi /etc/samba/smb.conf

Workgroup= STAFF

[read-only-share]

comment= this is read-only file share

hosts allow= 192.168.1.

browseable=yes

writeable=no

guest ok= no

valid users= read-only-user

read list= read-only-user

path=/groupdir

logfile=/var/log/samba/%m.log

max log size =5000

systemctl restart smb nmb

check: smbclient -L //localhost -U barney

SETTING READ-WRITE SAMBA SHARE

mkdir /data

chmod 2775 /data

setfacl -m u:user1:rwx /data

setfaclt -m u:user2:rx /data

vi /etc/samba/smb.conf

Workgroup= STAFF

[common]

browseable=yes

path=/data

hosts allow=192.168.1.

valid users=user1,user2

read list=user1,user2

write list=user1

systemctl restart smb nmb

SETTING READ-WRITE SAMBA GROUP SHARE (smbgrp’a dahil olan kullanıcılar bu konumdaki tüm dosyalarda read+write çalışır)

groupadd smbgrp

usermod -aG smbgrp test1

smbpasswd -a test1

usermod -aG smbgrp test2

smbpasswd -a test2

mkdir -p /samba/secured

chgrp smbgrp /samba/secured

chmod -R 0770 /samba/secured

vi /etc/samba/smb.conf

[secured]

hosts allow= 192.168.1.

path = /samba/secured

valid users = @smbgrp

write-list=@smbgrp

guest ok = no

writable = yes

browsable = yes

public=no

force group= +smbgrp

create mask= 0770

systemctl restart smb nmb

(on client)

groupadd smbgrp

usermod -aG smbgrp test1

usermod -aG smbgrp test2

smbclient -L //serverip -U test1

Anonymous Samba Share

Workgroup= STAFF

vi /etc/samba/smb.conf

[Anonymous]

path = /samba/anonymous

browsable =yes

writable = yes

guest ok = yes

read only = no

mkdir -p /samba/anonymous

(paylaşımı read/write yapar)

chmod -R 0755 /samba/anonymous/

chown -R nobody:nobody /samba/anonymous/

CLIENT settings (mounting Linux Samba Share)

yum -y install samba samba-client cifs-utils

smbclient -L //192.168.1.4/sharename -U user

mount -t cifs -o username=user //192.168.1.211/sharename /home/mount (temporary)

(then it asks user password)

mounting samba share on fstab

//192.168.1.4/sharename /home/mount cifs multiuser,sec=ntlmssp,credentials=/etc/smbuser 0 0

vi /etc/smbuser

username=barney

password=123456

(mounting guest samba share)

//192.168.1.4/sharename /home/mount cifs guest 0 0

**NFS SERVER** 192.168.1.180

Ports needed: 2049,111 tcp and udp

Server configuration

vi /etc/sysconfig/nfs

yum install nfs-utils -y

systemctl enable rpcbind

systemctl enable nfs-server

systemctl enable nfs-lock

systemctl enable nfs-idmap

systemctl start rpcbind

systemctl start nfs-server

systemctl start nfs-lock

systemctl start nfs-idmap

firewall-cmd --permanent --add-service nfs

firewall-cmd --permanent --add-service rpc-bind

firewall-cmd --permanent --add-service mountd

firewall-cmd --reload

mkdir /test1

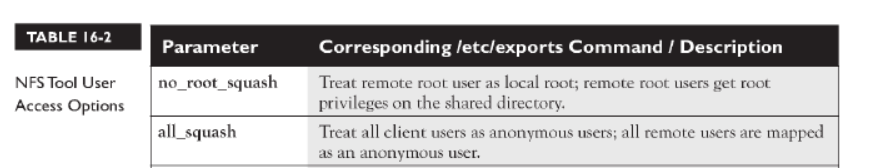
mkdir /test2

setsebool -P nfs\_export\_all\_ro=1 nfs\_export\_all\_rw=1

vi /etc/exports

/test1 192.168.1.211(rw,no\_root\_squash)

/test2 192.168.1.211(sync)



exportfs -avr : activates /etc/exports file

exportfs -ua: disactivates /etc/exports file

systemctl restart rpcbind

systemctl restart nfs-server

**NFS CLIENT**: 192.168.1.211

yum install nfs-utils -y

systemctl enable rpcbind

systemctl start rpcbind

firewall-cmd --permanent –add-port=111/tcp

firewall-cmd --permanent –add-port=111/udp

mkdir /test1

mkdir /test2

vi /etc/fstab (permanent)

192.168.1.180:/test1 /test1 nfs \_netdev,rw 0 0

192.168.1.180:/test2 /test2 nfs \_netdev,ro 0 0

Options:

<https://linoxide.com/file-system/example-linux-nfs-mount-entry-in-fstab-etcfstab/>

Using autofs

<https://www.lisenet.com/2016/setup-nfs-server-on-centos-7-and-configure-client-automount/>

Administration

(on server) exportfs,showmount -e

/nfsshare 192.168.1.211

(on client) nfsiostat : input-output statistics of existing mounting point

(on client) showmount -e 192.168.1.180

(on client and server) nfsstat:

**NFS WITH GROUP COLLABORATION**

NFS Server

groupadd -g 7654 nfsdatagrp

adduser user1

adduser user2

usermod -G nfsdatagrp user1

usermod -G nfsdatagrp user2

mkdir /nfsdata

chown -R nfsnobody:nfsdatagrp /nfsdata

chmod -R 2770 /nfsdata

vi /etc/exports

/nfsdata CLIENTIP(rw,no\_root\_squash)

exportfs -avr

NFS Client

groupadd -g 7654 nfsdatagrp

adduser user1

adduser user2

passwd user1

passwd user2

usermod -G nfsdatagrp user1

usermod -G nfsdatagrp user2

mkdir /nfsdata

vi /etc/fstab

SERVERIP:/nfsdata /nfsdata nfs \_netdev,rw 0 0

**NFS SERVER WITH KERBEROS**

vi /etc/hosts

192.168.1.5 centos2.yaydog.local >KDC SERVER +NFS SERVER

192.168.1.4 centos1.yaydog.local > KDC CLIENT

(on kdc+ nfs server)

yum groupinstall file-server

mkdir /krbdata

chmod 0777 /krbdata

semanage fcontext -a -t public\_content\_rw\_t "/krbdata(/.\*)?"

restorecon -R /krbdata

setsebool -P nfs\_export\_all\_ro=1 nfs\_export\_all\_rw=1

vi /etc/exports

/krbdata centos1.yaydog.local(rw,no\_root\_squash,sec=krb5)

systemctl restart nfs-server

exportfs -avr

kadmin: ktadd host/centos2.yaydog.local

authconfig --enablekrb5 --update

kadmin: addprinc -randkey nfs/centos2.yaydog.local

kadmin: ktadd nfs/centos2.yaydog.local

authconfig --enablekrb5 --update

reboot

(on kdc client)

kadmin: addprinc -randkey nfs/centos1.yaydog.local

kadmin: ktadd nfs/centos1.yaydog.local

yum install nfs-utils -y

sytemctl enable rpcbind

systemctl start rpcbind

systemctl enable nfs-client.target

systemctl start nfs-client.target

mkdir -p /mnt/krbtest

mount -t nfs4 -o sec=krb5 centos2.yaydog.local:/krbdata /mnt/krbtest

su - krbtest

kinit

**INSTALL VMWARE TOOLS ON RHEL7**

yum remove open-vm-tools

yum install policycoreutils-python

yum groupinstall “Development Tools”

(vmware mediası kopyalanır)

cd /media

cd vmware-tools-distrib

perl vmware-install.pl –d –f

systemctl status vmware-tools

systemctl enable vmware-tools

**KVM**

Make sure virtualization technology is enabled

[root@rhel7 ~]# lscpu | grep Virtualization

Virtualization: VT-x

yum install qemu-kvm qemu-img virt-manager libvirt libvirt-python libvirt-client virt-install virt-viewer bridge-utils

systemctl start libvirtd

systemctl enable libvirtd

iso dosyaları host üzerinde

/var/lib/libvirt/images

Sanal makinelerin disk konumu

/var/lib/libvirt/images/”VM Name”.qcow2

GUI>> virt-manager

virsh list --all : lists all VMs

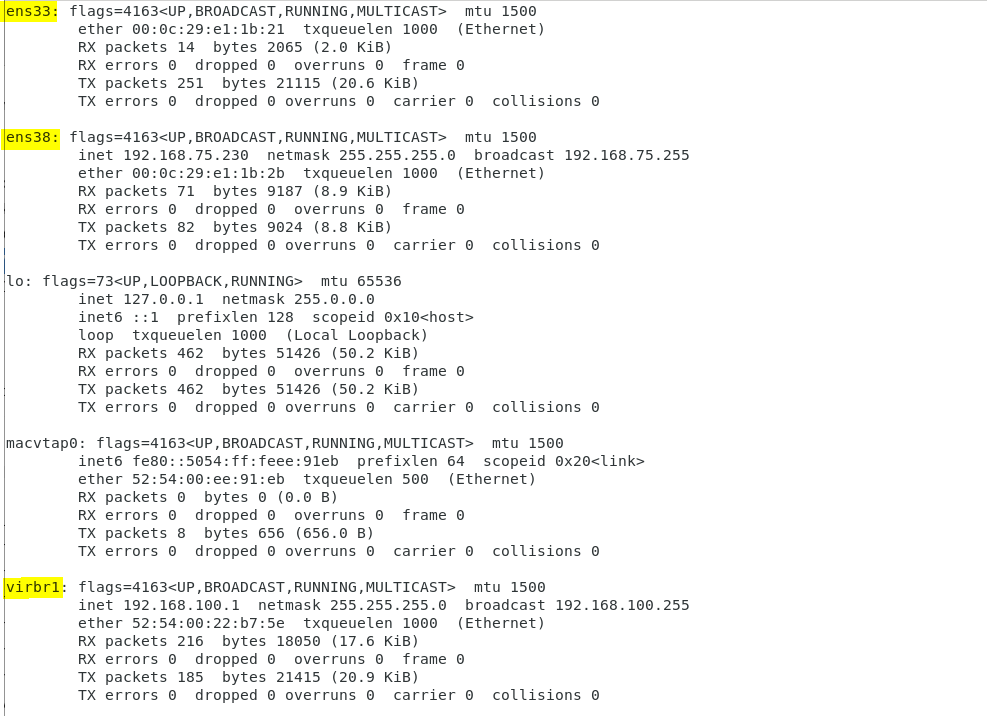
virsh dominfo vmname : get info about VM

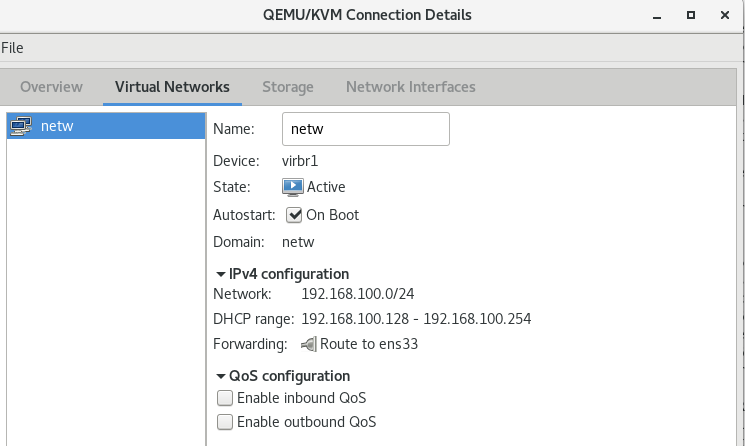
virsh autostart vmname: make vm boot when host boots

virsh reboot/shutdown vmname

Networking

Host





**COCKPIT WEB ADMINISTRATION**

yum install -y cockpit

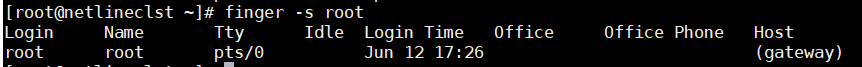
systemctl start cockpit

<https://192.168.1.111:9090>

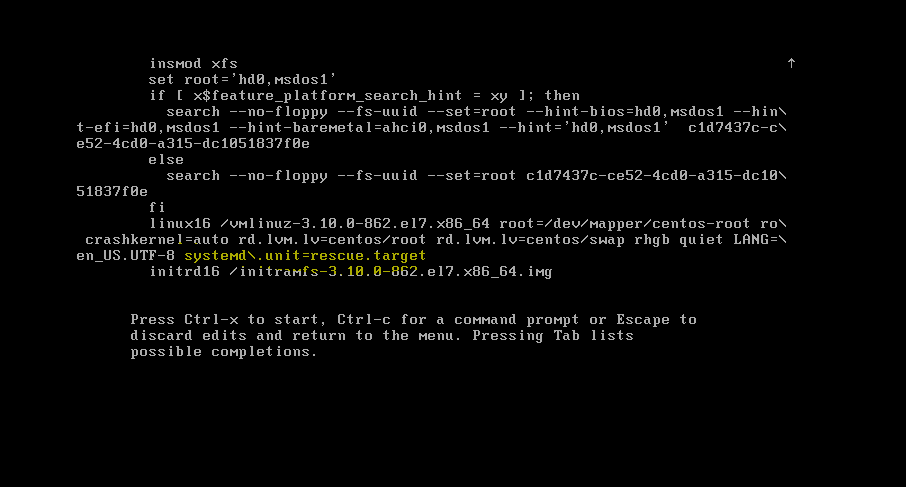
**FINGER COMMAND**

Looks up and display information about users

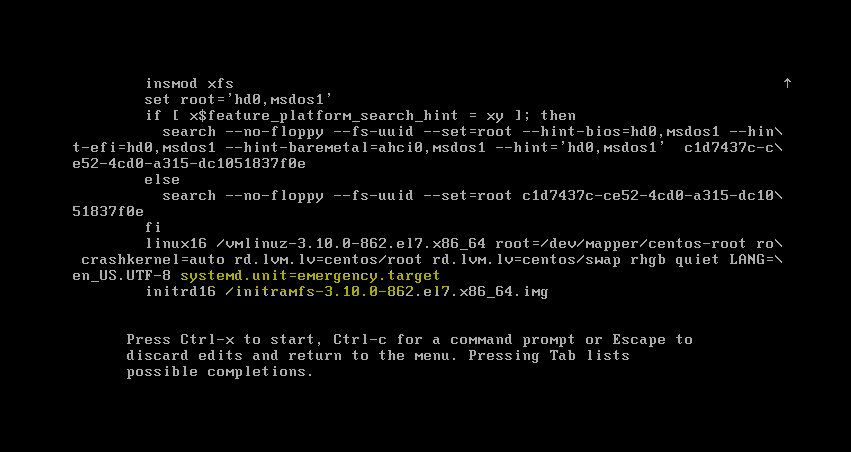
yum install finger\* -y



**RESCUE TARGET**



**EMERGENCY TARGET**

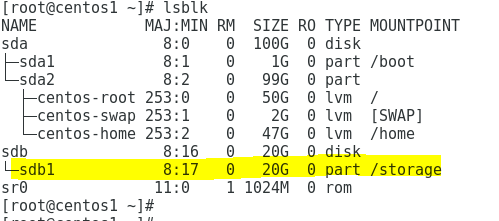


**ISCSI**

Creating iscsi target (192.168.1.4)

mkdir /storage

create sdb1 partion and mount on /storage



yum install targetcli\* -y

firewall-cmd --permanent –add-port=3260/tcp

firewall-cmd --reload

systemctl enable target

systemctl start target

(OPTION2: BLOCKIO)

yum install targetcli\* -y

firewall-cmd --permanent –add-port=3260/tcp

firewall-cmd --reload

systemctl enable target ; systemctl start target

backstores

block

mynew1/dev/sdb

iscsi

iqn.2019-11.local.yaydog:t1 (target)

tpg1

acls

iqn.2019-11.local.yaydog:client (initiator)

set auth userid,password

luns

/backstores/block/mynew1

sdb diski eklenir

targetcli

> backstores/block create mynew1/dev/sdb

> iscsi/ create iqn.2019-10.local.yaydog:t1

> cd iscsi/iqn.2019-10.local.yaydog:t1/tpg1

> luns/ create /backstores/block/mynew1

> acls/ create **iqn.2019-10.local.yaydog:client**

> cd acls/iqn.2019-10.local.yaydog:client/

> set auth userid=lunuser

> set auth password=123456

> cd ../..

> exit

configuration is written to : vi /etc/target/saveconfig.json

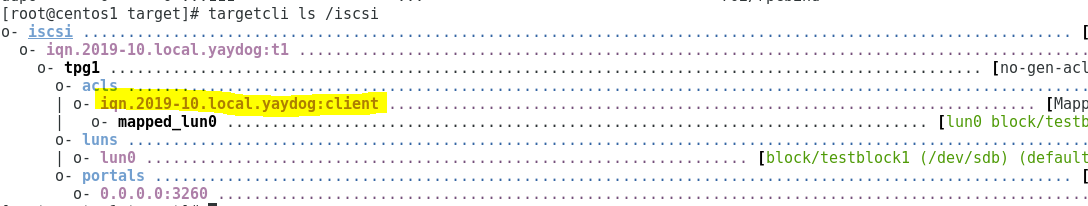
systemctl enable target

systemctl start target



To list created targets

targetcli ls /iscsi



creating iscsi client-initiator (192.168.1.5)-BLOCK IO’A GORE hazırlandı

yum install iscsi-initiator-utils\* lsscsi -y

systemctl enable iscsid

firewall-cmd --permanent –add-port=3260/tcp

firewall-cmd --reload

vim /etc/iscsi/initiatorname.iscsi

InitiatorName= **iqn.2019-10.local.yaydog:client**

vim /etc/iscsi/iscsid.conf

node.session.auth.authmethod = CHAP

node.session.auth.username = lunuser

node.session.auth.password = 123456

systemctl start iscsid

iscsiadm --mode discovery --type sendtargets --portal 192.168.1.4 >> check target

>>192.168.1.4:3260,1 **iqn.2019-10.local.yaydog:t1**

iscsiadm --mode node --targetname **iqn.2019-10.local.yaydog:t1** --portal 192.168.1.4 --login

iscsiadm -m session : shows connected sessions

reboot

mkfs.ext4 /dev/sdb

vi /etc/fstab

/dev/sdb /mnt ext4 \_netdev 0 0

mount -a

systemctl restart iscsid

how to disable iscsi target on client

iscsiadm -m node -T **iqn.2019-10.local.yaydog:t1** --portal 192.168.14:3260 -u

iscsiadm -m node -o delete -T **iqn.2019-10.local.yaydog:t1** --portal 192.168.1.4:3260

1. CREATING USERS FROM LIST

#!/bin/bash

for i in $( cat userlist ); do

useradd $i -m -s /bin/bash -d /home/$i

echo "user $i added successfully!"

done

1. COMMAND ARGUMENT (scriptname: create.sh)

#!/bin/bash

if [ "$1" = x ] ; then

echo argument x

elif [ "$1" = y ] ; then

echo argument y

else

echo "N/A"

fi

[root@centos2 /]# ./create.sh y

argument y

**RHEL7: Configure a system to authenticate using Kerberos**

JOIN ACTIVE DIRECTOR AND ENABLE SSH WITH AD KERBEROS

Kerberos Client

Hostname: centos2.yaydog.local

IP: 192.168.1.5

DNS: dc1.yaydog.local

vi /etc/hosts

192.168.1.100 dc1.yaydog.local

Vi /etc/sysconfig/network-scripts/ifcfg-ens33

DNS1=192.168.1.100

yum install -y realmd oddjob oddjob-mkhomedir sssd adcli openldap-clients policycoreutils-python samba-common samba-common-tools krb5-workstation

realm discover dc1.yaydog.local

realm join dc1.yaydog.local

chown root:root /etc/sssd/sssd.conf

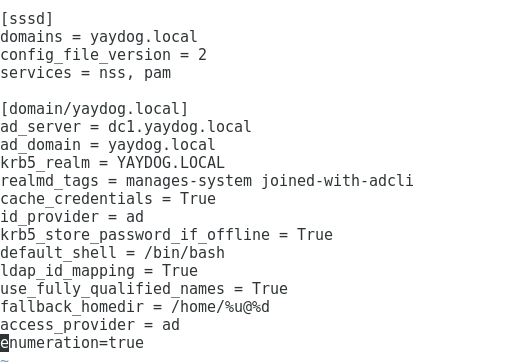
chmod 0600 /etc/sssd/sssd.conf

authconfig --enablesssd --enablesssdauth --enablemkhomedir –update

systemctl start sssd

systemctl enable sssd

vi /etc/sssd/sssd.conf



test: id [user1@yaydog.local](mailto:user1@yaydog.local)

vi /etc/ssh/sshd\_config

KerberosAuthentication yes

KerberosTicketCleanup yes

KerberosOrLocalPasswd yes

GSSAPIAuthentication yes

GSSAPICleanupCredentials yes

UseDNS yes

Systemctl restart sshd

ssh [user1@yaydog.local@127.0.0.1](mailto:user1@yaydog.local@127.0.0.1)

Server Hostname : centos2.yaydog.local

Client Hosname: centos1.yaydog.local

/etc/hosts dosyaları düzenlenir

KDC SERVER SETUP

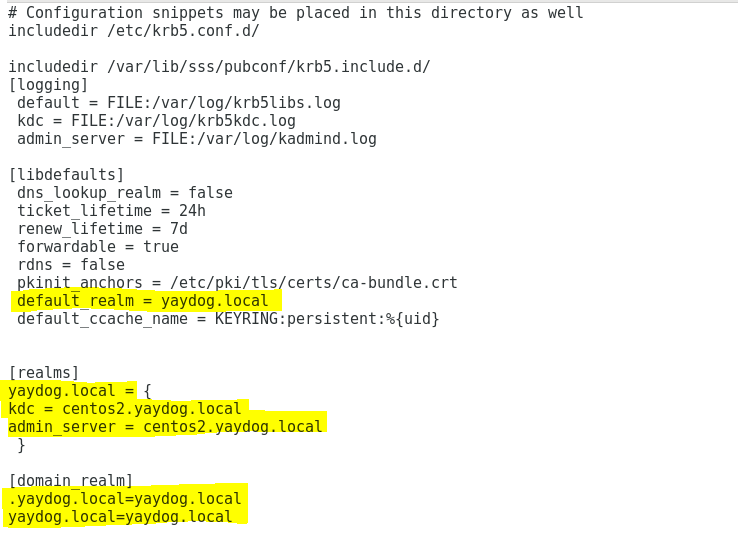
yum install -y krb5-server krb5-workstation pam\_krb5

vi /var/kerberos/krb5kdc/kdc.conf



Sadece krb5 istenirse commentlerden çıkart

vi /etc/krb5.conf



vi /var/kerberos/krb5kdc/kadm5.acl

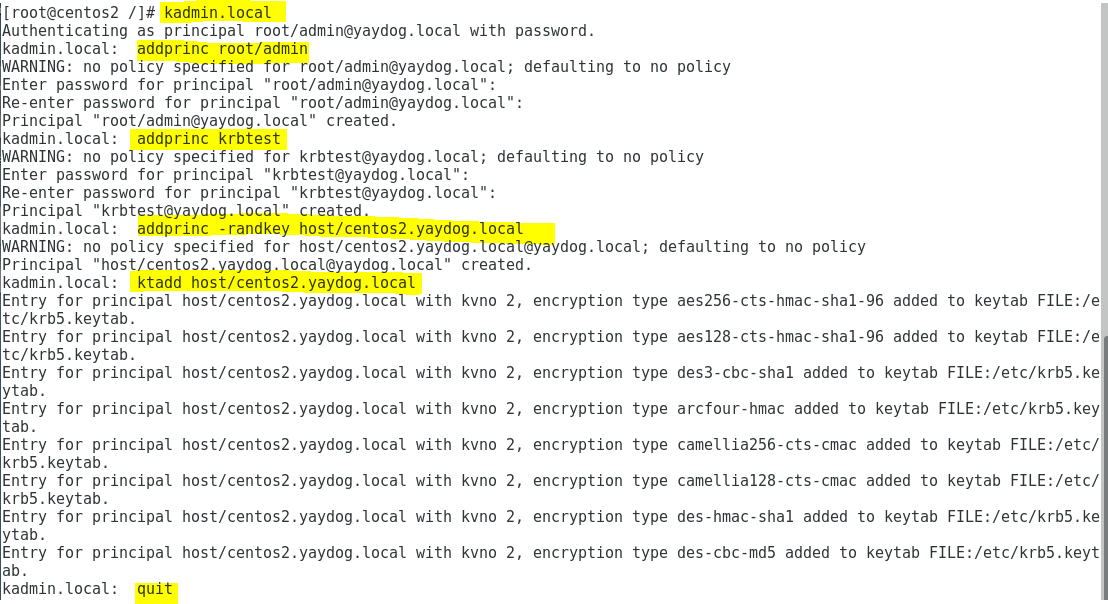
\*/admin@yaydog.local \*

kdb5\_util create -s -r yaydog.local

Enter KDC database master key:

systemctl enable krb5kdc kadmin

systemctl start krb5kdc kadmin



/etc/krb5.keytab is created

vi /etc/ssh/ssh\_config

GSSAPIAuthentication yes

GSSAPIDelegateCredentials yes

systemctl reload sshd

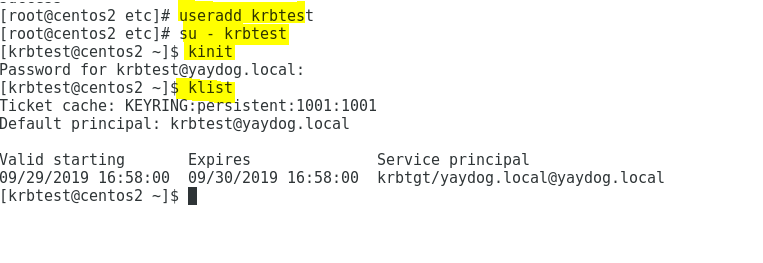
authconfig --enablekrb5 –update

firewall-cmd --permanent --add-port=88/tcp

firewall-cmd --permanent --add-port=88/udp

firewall-cmd --permanent --add-port=749/tcp

firewall-cmd --reload

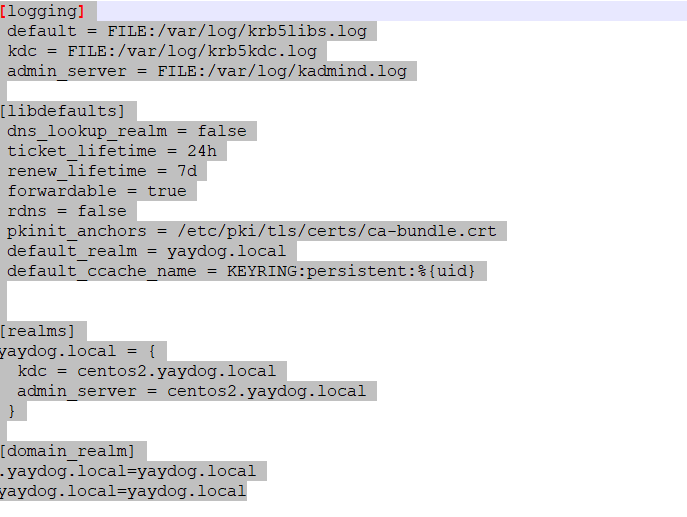


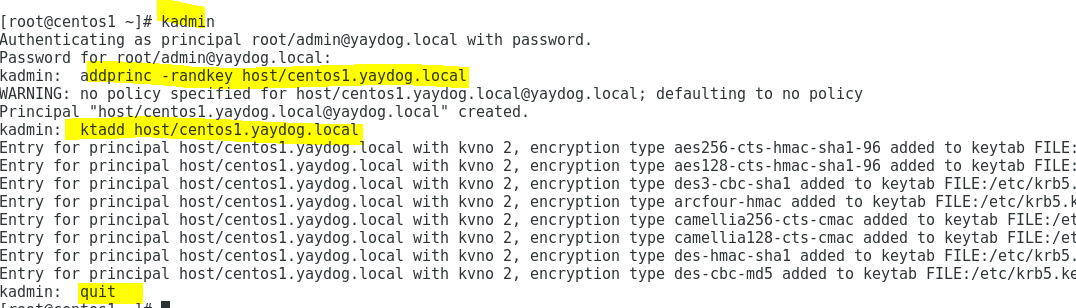
ssh krbtest@localhost ...OK

KDC CLIENT

yum install -y krb5-workstation pam\_krb5

vi /etc/krb5.conf





vi /etc/ssh/ssh\_config

GSSAPIAuthentication yes

GSSAPIDelegateCredentials yes

systemctl reload sshd

authconfig --enablekrb5 --update

