

TCPDUMP

#01

TCPDUMP

TCPDUMP ?

)
TCP/IP

Wireshark

가

가

(**Basic / Expression / Header Flag**)

Basic ()

-i : 가
-c :
-v : -vv
-n : IP . -nn Port
-w : .pcap . -r TXT

(-i) 100 (-c) .pcap
(-w) txt 가 Binary -r wireshark

```
tcpdump -i ens33 -vv -c 100 -w ttt.pcap
tcpdump: listening on ens33, link-type EN10MB (Ethernet),
capture size 262144 bytes
100 packets captured
100 packets received by filter
```

0 packets dropped by kernel

```
#          (-i)          5  (-c) DNS/PORT          IP
          (-nn)          .
tcpdump -i br0 -n -c 5
tcpdump: verbose output suppressed, use -v or -vv for full
protocol decode
listening on br0, link-type EN10MB (Ethernet), capture size
262144 bytes
14:08:14.531606 ARP, Request who-has 8.8.8.8 tell
10.10.10.200, length 28
14:08:15.533556 ARP, Request who-has 8.8.8.8 tell
10.10.10.200, length 28
14:08:16.535615 ARP, Request who-has 8.8.8.8 tell
10.10.10.200, length 28
14:08:18.531679 ARP, Request who-has 8.8.8.8 tell
10.10.10.200, length 28
14:08:19.533632 ARP, Request who-has 8.8.8.8 tell
10.10.10.200, length 28
5 packets captured
5 packets received by filter
0 packets dropped by kernel
```

```
#          ( -v , -vv )          .
tcpdump -i br0 -n -vv -c 5
tcpdump: listening on br0, link-type EN10MB (Ethernet),
capture size 262144 bytes
14:10:46.548613 ARP, Ethernet (len 6), IPv4 (len 4), Request
who-has 8.8.8.8 tell 10.10.10.200, length 28
14:10:47.549640 ARP, Ethernet (len 6), IPv4 (len 4), Request
who-has 8.8.8.8 tell 10.10.10.200, length 28
14:10:48.551557 ARP, Ethernet (len 6), IPv4 (len 4), Request
who-has 8.8.8.8 tell 10.10.10.200, length 28
14:10:50.548614 ARP, Ethernet (len 6), IPv4 (len 4), Request
who-has 8.8.8.8 tell 10.10.10.200, length 28
14:10:51.549621 ARP, Ethernet (len 6), IPv4 (len 4), Request
who-has 8.8.8.8 tell 10.10.10.200, length 28
5 packets captured
5 packets received by filter
0 packets dropped by kernel
```

(-i) IP 가 (-nn, grep)

tcpdump -i ens33 -nn | grep "1.2.3.4"

```
tcpdump: verbose output suppressed, use -v or -vv for full
protocol decode
listening on ens33, link-type EN10MB (Ethernet), capture size
262144 bytes
5 packets captured
6 packets received by filter
0 packets dropped by kernel
14:28:31.524052 IP 1.2.3.4.22 > 5.6.7.8.53707: Flags [P.], seq
4138122029:4138122237, ack 1068364849, win 1432, length 208
14:28:31.525940 IP 5.6.7.8.53707 > 1.2.3.4.22: Flags [.], ack
208, win 509, length 0
```

Expression ()

. 가 .

1) Type ()

- host , net , port

2) Dir ()

- src, dst , src or dst, src and dst

3) Proto ()

- ether, fddi, ip, arp, rarp, decnet, lat, sca, moprc, mopdl,
tcp, udp

4)

- ('and(&&)', 'or(||)', 'not(!)')

- gateway, broadcast, less, greater

(-i) tcp Destination Port 가 22

IP (-nn)

tcpdump -i ens33 tcp dst port 22 -nn

```
tcpdump: verbose output suppressed, use -v or -vv for full
protocol decode
listening on ens33, link-type EN10MB (Ethernet), capture size
262144 bytes
16:50:25.964928 IP 211.115.223.215.53707 > 211.239.150.48.22:
Flags [.], ack 4194846013, win 511, length 0
```

```
16:50:26.016014 IP 211.115.223.215.53707 > 211.239.150.48.22:
Flags [.], ack 161, win 511, length 0
16:50:26.060903 IP 211.115.223.215.53707 > 211.239.150.48.22:
Flags [.], ack 321, win 510, length 0
```

```
#          (-i)      tcp      "      " Destination Port 가 80 "
" 443      IP      (-nn)
```

```
tcpdump -i ens33 -nn tcp and dst port 80 or dst port 443
```

```
16:59:12.840778 IP 211.239.150.48.49514 > 8.8.8.8.443: Flags
[F.], seq 5, ack 9, win 229, options [nop,nop,TS val
3924566459 ecr 3515313672], length 0
16:59:14.863982 IP 211.239.150.48.47286 > 8.8.8.8.80: Flags
[S], seq 873533324, win 29200, options [mss 1460,sackOK,TS val
3924568482 ecr 0,nop,wscale 7], length 0
16:59:15.865581 IP 211.239.150.48.47286 > 8.8.8.8.80: Flags
[S], seq 873533324, win 29200, options [mss 1460,sackOK,TS val
3924569484 ecr 0,nop,wscale 7], length 0
```

Header Flag

```
#
□ SYN : Client 가 Server ( ) 가
IN/OUT Port .
```

TCP Header

Interesting Parts	TCP header
tcp[0:2]	source port
tcp[2:2]	destination port
tcp[4:4]	sequence number
tcp[8:4]	acknowledgement number
tcp[12]	header length
tcp[13]	tcp flags
tcp[14:2]	window size
tcp[16:2]	checksum
tcp[18:2]	urgent pointer
tcp[20..60]	options or data

UDP Header

Interesting Parts	UDP Header
udp[0:2]	source port
udp[2:2]	destination port
udp[4:2]	datagram length
udp[6:2]	UDP checksum

Flags

Flags	Numerically	Meaning
---- --S- 0000 0010	0x02	normal syn
---A --S- 0001 0010	0x12	normal syn-ack
---A ---- 0001 0000	0x10	normal ack
--UA P--- 0011 1000	0x38	psh-urg-ack.
---A -R-- 0001 0100	0x14	rst-ack
---- --SF 0000 0011	0x03	syn-fin scan
--U- P--F 0010 1001	0x29	urg-psh-fin
-Y-- ---- 0100 0000	0x40	anything >= 0x40
XY-- ---- 1100 0000	0xC0	both reserved bits set
XYUA PRSF 1111 1111	0xFF	FULL_XMAS scan

SYN

```
= TCP Flag( tcp[13] )      SYN ( 0x02 )   IP ( -nn )      10
(-c) txt      result.log      ( > )
```

```
tcpdump -i ens33 -c 10 "tcp[13] == 0x02" -n -nn > result.log
```

```
tcpdump: verbose output suppressed, use -v or -vv for full
protocol decode
```

```
listening on ens33, link-type EN10MB (Ethernet), capture size
262144 bytes
```

```
10 packets captured
```

```
10 packets received by filter
```

```
0 packets dropped by kernel
```

cat resule.log

```
16:16:15.308872 IP 211.239.150.48.43192 > 61.100.13.230.10051:
Flags [S], seq 3596242163, win 29200, options [mss
1460,sackOK,TS val 3921988927 ecr 0,nop,wscale 7], length 0
```

```
16:16:17.048128 IP 121.40.192.14.41265 > 211.239.150.48.4244:
Flags [S], seq 3887030721, win 1024, length 0
```

[S] = SYN Flag

json , .

Unskilled Attackers Pester Real Security Folks

=====

TCPDUMP FLAGS

Unskilled = URG = (Not Displayed in Flag Field, Displayed elsewhere)

Attackers = ACK = (Not Displayed in Flag Field, Displayed elsewhere)

Pester = PSH = [P] (Push Data)

Real = RST = [R] (Reset Connection)

Security = SYN = [S] (Start Connection)

Folks = FIN = [F] (Finish Connection)

SYN-ACK = [S.] (SynAck Packet)

[.] (No Flag Set)

JSON

```
result.log
```

```
IP: 211.239.150.48
```

JSON:

```
[ { ipaddr1: '221.239.150.48',
  ipaddr2: '61.100.13.230',
  type: 'Outbound',
  port: '10051' },
  { ipaddr1: '121.40.192.14',
  ipaddr2: '221.239.150.48',
  type: 'Inbound',
  port: '4244' } ]
```

Table:

ipaddr1	ipaddr2	type	port
221.239.150.48	61.100.13.230	Outbound	10051
121.40.192.14	211.239.150.48	Inbound	4244

TCP 3 way handshark : <https://websecurity.tistory.com/93>

[OS] CentOS 7

iptables

iptables

CentOS 7

SSH

(Pre) CentOS 7

firewalld

iptables

```
firewalld
service
```

```
, iptables
```

```
iptables.target
```

```
# firewalld disable
```

```
systemctl stop firewalld && systemctl disable firewalld
```

```
# firewalld service  
# /etc/sysconfig/iptables
```

```
yum install iptables-services  
service iptables reload  
service iptables status
```

```
#  
service iptables save
```

```
#  
service iptables reload
```

```
# -c ( ALL Rule )  
ROUTE(NAT)  
iptables-save -c > rules.txt
```

```
#  
iptables-restore < rules.txt
```

```
iptables ( IP )
```

```
#  
iptables -F
```

```
# lo ACCEPT  
iptables -A INPUT -i lo -j ACCEPT
```

```
# IP (SSH) -p tcp (-m  
tcp 가 ) --dport 22 가  
iptables -A INPUT -s 1.2.3.4/32 -m comment --comment " " -j  
ACCEPT
```

```
# state ACCEPT.  
iptables -A INPUT -m state --state RELATED,ESTABLISHED -j  
ACCEPT
```

```
# ( ) Ping request 가 . 가
```

```
iptables -A INPUT -j REJECT --reject-with icmp-host-prohibited
```



```

# ( ) Ping request
iptables -A INPUT -p icmp --icmp-type echo-request -j REJECT

# ( ) Ping DROP. ACCEPT
iptables -A INPUT -p icmp -j DROP

# TCP DROP
iptables -A INPUT -p tcp -j DROP

#
service iptables save

```

가 가

```

# -A 가 DROP Line 가 Line
# -I INPUT [DROP Line] DROP 가
iptables -nL --line-number
-----
Chain INPUT (policy ACCEPT)
num target prot opt source destination
1 ACCEPT all -- 1.2.3.4 0.0.0.0/0
/* */
2 DROP tcp -- 0.0.0.0/0 0.0.0.0/0
-----

# 2 DROP 가
iptables -I INPUT 2 -s 5.6.7.8 -j ACCEPT -m comment --comment "
가"
iptables -nL --line-number
-----
Chain INPUT (policy ACCEPT)
num target prot opt source destination
1 ACCEPT all -- 1.2.3.4 0.0.0.0/0
/* */
2 ACCEPT all -- 5.6.7.8 0.0.0.0/0

```

```
/* 가 */
3 DROP tcp -- 0.0.0.0/0 0.0.0.0/0
```

```
# /etc/sysconfig/iptables
reload 가 .
```

```
iptables -D INPUT [Number]
```

CentOS 7 Windows RDP

CentOS 7 Windows RDP

```
# OS
CentOS 7.9 x86_64 minimal
--> XRDP GUI --> GUI Windows
RDP
```

Linux GUI

```
# GUI GroupInstall
root@localhost ~]# yum groups list | grep -i desktop
Cinnamon Desktop
MATE Desktop
GNOME Desktop
```

```
General Purpose Desktop
LXQt Desktop
# GNOME "Server with GUI"
root@localhost ~] yum groupinstall "GNOME Desktop"

# GUI init
[root@localhost ~]# systemctl get-default
multi-user.target
[root@localhost ~]# systemctl set-default graphical.target
[root@localhost ~]# systemctl get-default
graphical.target
# Reboot GUI
[root@localhost ~]# reboot
```

Linux

```
# XRDP Install.
[root@localhost ~]# yum install epel-release
[root@localhost ~]# yum install xrdp
[root@localhost ~]# systemctl enable xrdp && systemctl start
xrdp

# selinux disable iptables -F or tcp/3389 가
```

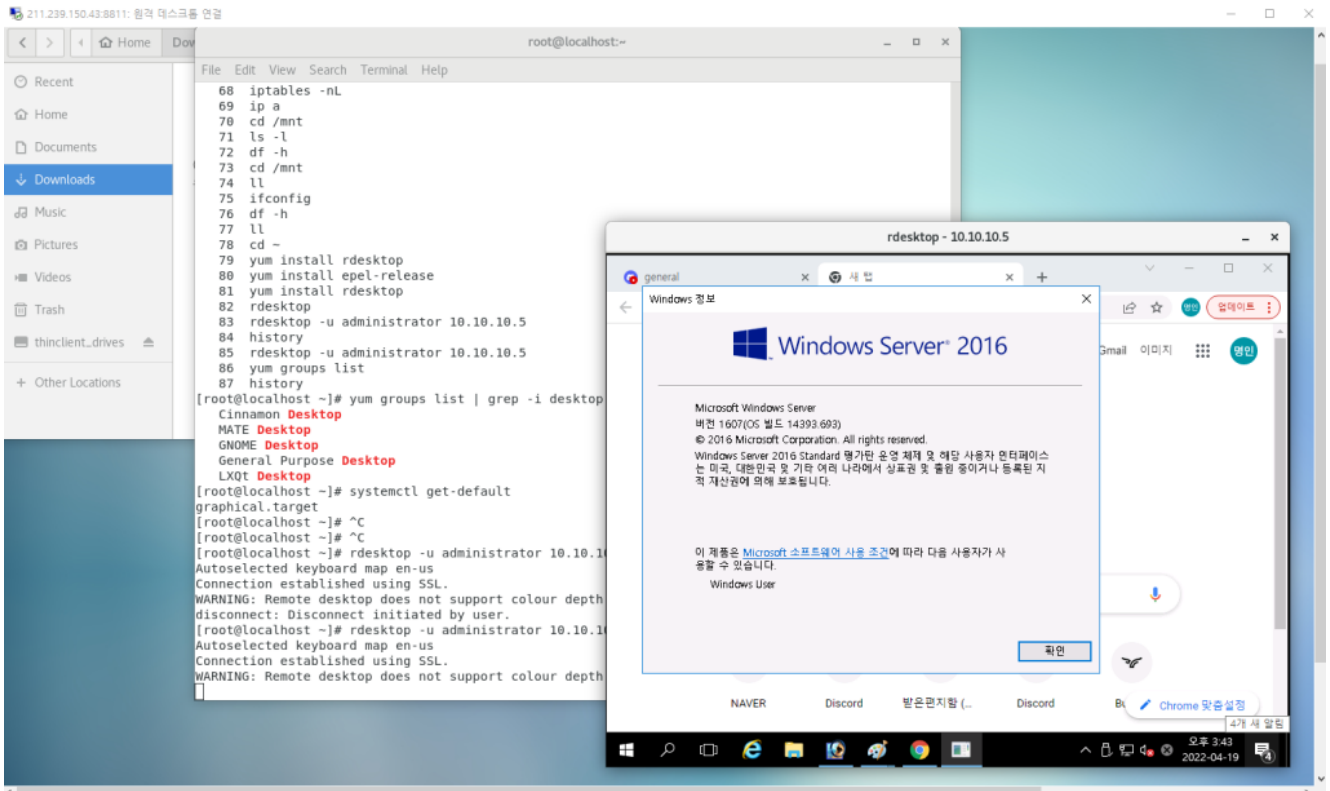
rdesktop

```
# openssl-devel
yum -y install gcc openssl-devel

wget
https://github.com/rdesktop/rdesktop/releases/download/v1.8.6/
rdesktop-1.8.6.tar.gz
tar xvzf rdesktop-1.8.6.tar.gz
cd rdesktop-1.8.6/
./configure --disable-credssp --disable-smartcard
make
make install
```

Check

```
# RDP , rdesktop -u [User] [ip] .  
root@localhost ~]# rdesktop -u administrator 10.10.10.5  
Autoselected keyboard map en-us  
Connection established using SSL.  
WARNING: Remote desktop does not support colour depth 24;  
falling back to 16
```



CentOS 7

(2)

CentOS 7

CentOS 7

가

/

1.

```
##
```

```
yum update [ ]
```

```
##
```

```
yum list updates
```

2.

```
# epel-release :
```

```
disable
```

```
enablerepo
```

```
vi /etc/yum.repos.d/epel.repo
```

```
enabled=1 0
```

```
[epel]
```

```
...
```

```
enabled=0
```

```
...
```

```
yum repolist
yum --enablerepo=epel install [      ]
```

```
# net-tools :                               IP
ifconfig,                                   netstat
```

```
<ifconfig>
ifconfig -a
ifconfig [interface] up
ifconfig [interface] down
```

```
<netstat>
netstat -nap
netstat -an | grep [Port]
netstat -nlpt
```

```
# unzip : zip
```

```
unzip [file_name].zip
unzip -l [file_name].zip
unzip -t [file_name].zip
```

```
# wget :                                     가                               HTTP, HTTPS, FTP
```

```
wget -O [      ] [URL      ]
wget --no-check-certificate [URL      ]
```

```
# curl :                                     HTTP, FTP
```

```
Web                                         wget
```

```
curl -o [      ] [URL      ]
curl -T [      ] [      IP]
curl -L [URL      ]
```

```
# chrony : NTP Server/Client ntpd
```

```
## NTP IP 가
```

```
vi /etc/chrony.conf
```

```
server [NTP server IP] iburst <iburst =  
>
```

```
systemctl restart chronyd  
chronyc sources
```

```
# gcc, gcc-c++ : C , C++
```

```
# openssl-devel : openssl openssl
```

```
# htop : (  
)
```

```
PID  
USER  
PR  
NI  
VIRT  
RES  
SHR  
S  
%CPU  
%MEM  
TIMR+  
COMMAND
```

iftop :

```
iftop -i eno1  
iftop -f "dst port 22"
```

dstat : I/O
가 .

```
dstat -tcdml
```

sysstat : sar, iostat

<iostat> : CPU , .
iostat -d 3
iostat -c 3

<sar> : /var/log/sa sa
. .
sar -u
sar -r
sar -dp
sar -n DEV

lsof :

```
lsof -u [ ]  
lsof -i  
lsof -c [ ]
```

psmisc : proc fuser,
killall, pstree

<fuser> : umount
, kill
fuser -v []
fuser -ck []
<killall> :
killall -i []


```
killall -v [      ]
killall -w [      ]
```

```
<pstree> :                Tree
pstree -anp
```

3.

```
# mlocate :                find
```

```
updatedb
locate [      ]
locate -n [    ] [      ]
```

```
# ncat :                가
```

```
<      >
ncat -l [Port]
ncat -lk [Port]
```

```
<          >
ncat [Server IP] [Port]
```

```
# whois :                IP
```

```
whois [      ]
whois [IP    ]
```

```
# cloud-utils-growpart : LVM                root
가
```

```
growpart [      ] [      ]
resize2fs [      ]
```

```
# tcping :                TCP                ping
```

```
tcping [Server IP] [Port]
```

About OOM Killer ?

Kernel 5.4.0-104-generic

OOM(Out Of Memory) ?

Linux swap , 가 가
Over Commit 가 .

OOM(Out Of Memory) Killer ?

Linux Out Of Memory가 , OOM Score
가 Kill Linux Kernel

OOM Killer /var/log/

oom_killer Log

```
$ cat /var/log/syslog | grep oom
Mar  7 19:14:00 zabbix-node01 kernel: [1132818.054201]
ib_log_writer invoked oom-killer:
gfp_mask=0x100cca(GFP_HIGHUSER_MOVABLE), order=0,
oom_score_adj=0
OOM Score OOM Killer
```

1. + fork()
- 2.
3. 가 , root (super user)

```

4.      nice      1      Score      2      가
5. /proc/[PID]/oom_score_adj ( 가      가 )
6. /proc/[PID]/oom_adj ( 가      가 )
      OOM Score      .

```

```

# oom_score
$ cat /proc/890081/oom_score
1048
# 890081 PID , OOM Score 1048 .
oom_adj / oom_score_adj
      가 OOM Score 가 OOM Killer
가 , oom_adj /oom_score_adj , OOM
Score 가 .
oom_adj -17 ~ 15 , -17 OOM Killer Disable
      가 .
oom_score_adj -1000 ~ 1000 , OOM Score
oom_score_adj 가 .(oom_score_adj -1000 oom_adj
-17 .)
oom_adj / oom_score_adj
oom_score
      OOM Score oom_score_adj OOM Score
      .

```

```

# oom_score
$ cat /proc/890081/oom_score
1048
# 890081 PID , OOM Score 1048 .

# oom_score_adj OOM Score
$ echo -1000 > /proc/890081/oom_score_adj

```

```

$ cat /proc/890081/oom_score_adj
-1000
# oom_score_adj 가 -1000

```

```

# oom_score / oom_adj
$ cat /proc/890081/oom_score
0
$ cat /proc/890081/oom_adj
-17
# oom_score_adj , oom_adj -17 (OOM Killer
Disable)

```

```
# oom_score 1048 -> 0
가 , overcommit . over commit
```

over commit

```
$ cat /etc/sysctl.conf | grep overcommit_memory
vm.overcommit_memory = 1 # 0~2 가 .
# 0 = Heuristic overcommit. Default , (
) over commit .
# 1 = over commit . OOM Killer가 ,
# 2 = vm.overcommit_ratio over commit
```

```
# 가
$ cat /etc/sysctl.conf | grep overcommit_ratio
vm.overcommit_ratio = 90
# vm.overcommit_memory가 2 가 .
# 90% + swap OOM Killer
가 .
```

```
#
$ systemctl -w
, commit 가 over commit
?
/proc/meminfo sysstat . .
```

```
# commit
$ cat /proc/meminfo | grep Commit
CommitLimit: 30229156 kB
# vm.overcommit_memory 2 vm.overcommit_ratio
commit 가
Committed_AS: 64267776 kB
# commit
```

sysstat

commit

```
$ apt install -y sysstat
# sysstat
```

```
# sar
$ sar -r 1
Linux 5.4.0-104-generic (zabbix-node02) 04/14/2022
_x86_64_ (16 CPU)
```

```
09:25:17 AM kbmemfree kbavail kbmemused %memused kbbuffers
kbcached kbcommit %commit kbactive kbinact kbdirty
09:25:18 AM 208884 2446760 20804112 85.73 990436
1441416 64262056 196.79 19538260 3304352 1508
```

```
# %commit commit
# 100% commit , over commit
# sar (CPU, Memory, I/O)
```

```
# -r Memory , 1 1
```

```
Linux Memory Commit / Memory Over Commit ?
Memory Commit
가 가
```

```
A 가 가 A 가 ,
A ,
Memory Commit ( ) . ,가
? ,
가
```

1. A 가 .
2. .
- , 가
3. (Fragmentation)가 .
- : RAM 가
- 가 가
-
- .

```
Memory Over Commit
, Memory Over( ) Commit
```

over commit 가
, over commit 가 oom killer
가
가

CentOS 7 APM yum

가 yum

Image OS : CentOS 7.6.1810 Minimal

```
#  
가  
yum install -y epel-release  
  
# Apache 2.4.52  
RPMs  
(codeit)  
  
cd /etc/yum.repos.d/ && wget  
https://repo.codeit.guru/codeit.el`rpm -q --qf "%{VERSION}"  
$(rpm -q --whatprovides redhat-release)` .repo  
  
# 가  
yum info httpd
```

```
Loaded plugins: fastestmirror  
Loading mirror speeds from cached hostfile  
* base: mirror.kakao.com  
* epel: hk.mirrors.thegigabit.com  
* extras: mirror.kakao.com  
* remi-safe: mirror.bebout.net  
* updates: mirror.navercorp.com
```

Installed Packages

Name : httpd
Arch : x86_64
Version : 2.4.52
Release : 1.codeit.el7
Size : 4.3 M
Repo : installed
From repo : CodeIT
Summary : Apache HTTP Server
URL : <https://httpd.apache.org/>
License : ASL 2.0
Description : The Apache HTTP Server is a powerful, efficient,
and extensible
: web server.

Apache

```
yum --enablerepo=CodeIT install httpd mod_ssl
```

PHP 7.4 Remi Repository .

```
yum install  
https://rpms.remirepo.net/enterprise/remi-release-7.rpm
```

PHP 7.4

```
yum repolist all | grep -i php
```

```
yum --enablerepo=remi-php74 install php php-opcache php-gd  
php-mysql php-xml
```

MariaDB 10.3

```
cat << EOF | tee /etc/yum.repos.d/MariaDB.repo
```

```
[mariadb]
```

```
name = MariaDB
```

```
baseurl = http://yum.mariadb.org/10.3/centos7-amd64
```

```
gpgkey=https://yum.mariadb.org/RPM-GPG-KEY-MariaDB
```

```
gpgcheck=1
```

```
enabled=0
```

```
EOF
```

MariaDB 10.3

```
yum -y install --enablerepo=mariadb MariaDB-server MariaDB-  
client MariaDB-backup
```

APM

```
[root@localhost ~]# php -v
PHP 7.4.28 (cli) (built: Feb 15 2022 13:23:10) ( NTS )
Copyright (c) The PHP Group
Zend Engine v3.4.0, Copyright (c) Zend Technologies
    with Zend OPcache v7.4.28, Copyright (c), by Zend
Technologies
[root@localhost ~]# mysql --version
mysql Ver 15.1 Distrib 10.3.34-MariaDB, for Linux (x86_64)
using readline 5.1
[root@localhost ~]# httpd -v
Server version: Apache/2.4.52 (codeit)
Server built:   Dec 20 2021 11:29:54
```

CentOS 7

(1)

CentOS 7

가

, ,

.

, ,

()

가

.

LVM : Default

가 ,

가

:

LVM

가 ,

xfs

1.

(OS)

```
# ip addr
# vi /etc/sysconfig/network-scripts/ifcfg-eth0

. . .
BOOTPROTO=none
. . .
IPV6INIT=no
IPV6_AUTOCONF=no
IPV6_DEFROUTE=no
IPV6_FAILURE_FATAL=no
IPV6_ADDR_GEN_MODE=stable-privacy
. . .
ONBOOT=yes # /
yes
IPV6_PRIVACY=no
IPADDR=192.168.122.243
NETMASK=255.255.255.0
GATEWAY=192.168.122.1
DNS1=8.8.8.8
DNS2=8.8.4.4

# systemctl restart network
# ip addr
eth0 IP

# ping -c 4 google.com #
--- google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3094ms
rtt min/avg/max/mdev = 82.692/83.010/83.554/0.492 ms
```

2.

CentOS 7 timedatectl , .

```
# timedatectl
```

```
RTC time :  
NTP enabled : NTP  
NTP synchronized : NTP  
RTC in local TZ : RTC      Time zone
```

```
# timedatectl list-timezones | grep -i Asia*
```

```
# timedatectl set-timezone Asia/Seoul
```

```
# timedatectl
```

3. Hostname

CentOS 7 hostname localhost.localdomain

```
# hostnamectl  
Static hostname: localhost.localdomain
```

```
# hostnamectl set-hostname newhostname
```

```
# hostnamectl  
Static hostname: newhostname
```

4. SELinux

SELinux , disabled(=)

```
# vi /etc/sysconfig/selinux
```

```
. . .  
SELINUX=disabled . . .
```

```
# shutdown -r now
```

```
# getenforce  
Disabled
```

5. root 가

```
root
```

```
su
```

```
.  
# ps -ef | grep sshd  
# systemctl enable sshd
```

```
# vi /etc/ssh/sshd_config
```

```
. . .  
PermitRootLogin=no
```

```
. . .
```

```
# systemctl restart sshd
```

6.

```
# vi /etc/profile.d/timeout.sh
```

```
TMOUT=600
```

```
export TMOUT
```

```
chmod +x /etc/profile.d/timeout.sh
```

```
# source /etc/profile
```

```
# echo $TMOUT
```

600

7.

history

```
# vi /etc/profile.d/history.sh
```

```
HISTTIMEFORMAT="%F %T -- "  
export HISTTIMEFORMAT
```

```
# chmod 644 /etc/profile.d/history.sh  
# source /etc/profile.d/history.sh
```

```
# hisotry
```

```
999 2022-04-06 14:50:10 -- vi /etc/profile.d/history.sh  
1000      2022-04-06 14:50:19 -- chmod 644  
/etc/profile.d/history.sh  
1001 2022-04-06 14:50:28 -- source /etc/profile.d/history.sh  
1002 2022-04-06 14:50:30 -- history
```

8.

```
# localectl
```

```
System Locale: LANG=en_US.UTF-8  
VC Keymap: us  
X11 Layout: us
```

```
# localectl list-locales | grep -i kr  
ko_KR  
ko_KR.euckr  
ko_KR.utf8
```

```
# localectl set-locales LANG=ko_KR.UTF-8
# localectl set-keymap kr
# localectl set-x11-keymap kr
```

```
# localectl
  System Locale: LANG=ko_KR.UTF-8
    VC Keymap: kr
    X11 Layout: kr
```