Linux

Table of Contents

Linux
Linux

Linux Linux
Linux Linux

Linux

URL
http://list.ospn.jp/mailman/listinfo/linux-text

1 3

Linux systemd
Linux systemd

4 6

Linux OS

7

Linux Linux

Linux

OS Red Hat
OS

PDF　EPUB

PDF　EPUB

LPI-Japan

106-0041 1-11-9 CR 7F

TEL 03-3568-4482

FAX 03-3568-4483

E-Mail info@lpi.or.jp

LPIC Linux
Web

1

1

Windows Linux Windows

IP

IP
Linux

OS

Linux CentOS 6.6 64
CentOS 7 7 CentOS 7

OS DVD

Linux

1 IP

OS

CentOS 6.6 64 Desktop
yum

IP

	server.example.com
IP	192.168.0.10
	24 255.255.255.0
	192.168.0.1
DNS	192.168.0.1

UTC

sato

- 1
- 2
- 3

- 4
- 5
- 6
- 7　CentOS 7

iptables　SELinux

6

- Linux　1　root　#
- Linux　2
- ⇒

```
# command ※root□□□□□□□□□
$ command ※□□□□□□□□□
[root@server ~]# command ※□□□□□root□□□□□□□□□
[sshuser@client ~]$ command ※□□□□□□□□□□□sshuser□□□□□
$ id
uid=500(sato) gid=500(sato) □□□□□□=500(sato) context=unconfined_u:unconfin
```

Windows macOS OS 1 1

Linux OS

root (

)

root ( )

id OS sato

id

```
$ id
uid=500(sato) gid=500(sato) □□□□□□=500(sato) context=unconfined_u:unconfin
```

uid ID gid ID groups

ID ID

uid CentOS 6 500 65535

root

uid 0

root

Linux root

Linux root

su

root su su -

```
$ su -
Password: ※root□□□□□□□□□□□□
#
```

root #
id

```
# id
uid=0(root) gid=0(root) □□□□□□=0(root) context=unconfined_u:unconfined_r:u
```

root uid 0

root

root

AlmaLinux uid 1
499

SSH sshd sshd root
id sshd

```
# id sshd
uid=74(sshd) gid=74(sshd) □□□□□□=74(sshd)
```

useradd

root useradd passwd

useradd

-c

```
# useradd -c "Ichiro Suzuki" suzuki
# id suzuki
uid=501(suzuki) gid=501(suzuki) □□□□□□=501(suzuki)
```

useradd

-u ID

-g ID

-G (,)

-s shell

-c

-d

-e YYYY-MM-DD

passwd

```
# passwd suzuki
□□□□ suzuki □□□□□□□□□□
□□□□□□□□: □□□□suzuki□□□□□□□□□□□□
□□□□□□□□□□□□□□□□□□□: □□□□suzuki□□□□□□□□□□□□□□
passwd: □□□□□□□□□□□□□□□□□□□□□□□□
```

root

suzuki

```
$ passwd
□□□□ suzuki □□□□□□□□□□
suzuki □□□□□□□□□□□
□□□UNIX□□□□□□: □□□□suzuki□□□□□□□□□□□□
□□□□□□□□: □□□□suzuki□□□□□□□□□□□□
□□□□□□□□□□□□□□□□□□□: □□□□suzuki□□□□□□□□□□□□□□
passwd: □□□□□□□□□□□□□□□□□□□□□□□□
```

/etc/passwd

cat /etc/passwd

```
# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
□□□
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
tcpdump:x:72:72::/:/sbin/nologin
sato:x:500:500::/home/sato:/bin/bash
suzuki:x:501:501:Ichiro Suzuki:/home/suzuki:/bin/bash
```

/etc/passwd (:)

x

ID ID

ID ID

UNIX /etc/passwd
/etc/passwd

root (/etc/shadow)

/etc/passwd

x

/etc/shadow 000
400 root

```
# ls -l /etc/shadow
----------. 1 root root 1164  1□  6 06:48 2015 /etc/shadow
```

root suzuki

```
# grep suzuki /etc/shadow
suzuki:$6$Tq1q9Ztw$8sh1KFpEGFAmU68P8hYLuGjIml01omSdTELmhGNFLWdielH8CzmLLrI
```

1

( )

```
# id suzuki
uid=501(suzuki) gid=501(suzuki) □□□□□□=501(suzuki)
```

gid

/etc/group

/etc/group

```
# cat /etc/group
root:x:0:
bin:x:1:bin,daemon
□□□
sato:x:500:
suzuki:x:501:
```

useradd
ID uid

groupadd ID -g
ID

groupadd

```
groupadd [-g □□□□ID] □□□□□
```

ID 5000 grouptest

```
# groupadd -g 5000 grouptest
```

/etc/group

```
# grep grouptest /etc/group
grouptest:x:5000:
```

groupmod

groupmod

```
groupmod [-n □□□□□□□□] □□□□□
```

grouptest eigyou

```
# groupmod -n eigyou grouptest
```

/etc/group

```
# grep eigyou /etc/group
eigyou:x:5000:
```

usermod -G

gpasswd

usermod

```
usermod [-G □□□□□□□ [,...]] □□□□
```

suzuki eigyou

```
# usermod -G eigyou suzuki
```

id

```
# id suzuki
uid=501(suzuki) gid=501(suzuki) □□□□□□=501(suzuki),5000(eigyou)
```

eigyou

/etc/group

```
# grep eigyou /etc/group
eigyou:x:5000:suzuki
```

suzuki eigyou

gpasswd

gpasswd gpasswd
1

gpasswd

```
gpasswd -a □□□□□□□□ □□□□□
gpasswd -d □□□□□□□□ □□□□□
```

suzuki eigyou

```
# gpasswd -d suzuki eigyou
Removing user suzuki from group eigyou
# id suzuki
uid=501(suzuki) gid=501(suzuki) □□□□□□=501(suzuki)
```

/etc/group　　eigyou　　suzuki

```
# grep eigyou /etc/group
eigyou:x:5000:
```

eigyou　　suzuki

suzuki　　eigyou

```
# gpasswd -a suzuki eigyou
Adding user suzuki to group eigyou
# id suzuki
uid=501(suzuki) gid=501(suzuki) □□□□□□=501(suzuki),5000(eigyou)
```

suzuki　　eigyou

(permission)

cd

pwd

```
$ cd
$ pwd
/home/suzuki
```

touch

```
touch test.txt
```

ls　　-l

```
$ ls -l
□□ 0
-rw-rw-r--. 1 suzuki suzuki 0  1□  6 07:34 2015 test.txt
```

rw-rw-r--

AlmaLinux ll ls -l ll ls -l

```
$ ll
□□ 0
-rw-rw-r--. 1 suzuki suzuki 0  1□  6 07:34 2015 test.txt
```

alias

```
$ alias
alias l.='ls -d .* --color=auto'
alias ll='ls -l --color=auto'
alias ls='ls --color=auto'
alias vi='vim'
alias which='alias | /usr/bin/which --tty-only --read-alias --show-dot --s
```

rwx 3

chmod

(Readable)	r	4
(Writable)	w	2
(eXecutable)	x	1
	-	0

test.txt

user	**(group)**	**(other)**
rw-	rw-	r--
4+2+0=6	4+2+0=6	4+0+0=4

- rw- suzuki
- rw- suzuki
- r--

3

rw-rw-r-- 664

mkdir testdir

```
$ mkdir testdir
$ ls -l
□□ 4
-rw-rw-r--. 1 suzuki suzuki    0  1□  6 07:34 2015 test.txt
drwxrwxr-x. 2 suzuki suzuki 4096  1□  6 07:42 2015 testdir
```

testdir d

rwx(4+2+1) rwx(4+2+1) r-x(4+1) 775

chmod chmod

```
chmod □□□ □□□□
```

+ -

ug+x

a+x

g-w

chmod

```
$ chmod u-x testdir
$ ls -l
□□ 4
-rw-rw-r--. 1 suzuki suzuki    0  1□  6 07:34 2015 test.txt
drw-rwxr-x. 2 suzuki suzuki 4096  1□  6 07:42 2015 testdir
$ cd testdir
-bash: cd: testdir: □□□□□□□□
$ chmod u+x testdir
$ cd testdir
$ pwd
/home/suzuki/testdir
```

useradd usermod -e

```
useradd -e YYYY-MM-DD □□□□
usermod -e YYYY-MM-DD □□□□
```

usermod

```
# usermod -e 2015-1-6 suzuki
```

chage

```
# chage -l suzuki
Last password change    : Jan 05, 2015
Password expires     : never
Password inactive     : never
Account expires      : ※Jan 06, 2015
Minimum number of days between password change  : 0
Maximum number of days between password change  : 99999
Number of days of warning before password expires : 7
```

Your account has expired

```
login: suzuki
Password: ※□□□suzuki□□□□□□□□□
Your account has expired; please contact your system administrator
```

" 2

Account expires never

```
# usermod -e '' suzuki
# chage -l suzuki
Last password change    : Jan 05, 2015
Password expires     : never
Password inactive     : never
Account expires      : ※never
Minimum number of days between password change  : 0
```

```
Maximum number of days between password change  : 99999
Number of days of warning before password expires : 7
```

chage -M

30 30

```
# chage -M 30 suzuki
```

Password expires

```
# chage -l suzuki
Last password change    : Jan 05, 2015
Password expires     : ※Feb 04, 2015
Password inactive     : never
Account expires      : never
Minimum number of days between password change  : 0
Maximum number of days between password change  : 30
Number of days of warning before password expires : 7
```

-d 0

1970 1 1

```
# chage -d 0 suzuki
```

chage Last password change Password expires Password inactive password must be changed

```
# chage -l suzuki
Last password change    : ※password must be changed
Password expires     : ※password must be changed
Password inactive     : ※password must be changed
Account expires      : never
Minimum number of days between password change  : 0
Maximum number of days between password change  : 30
Number of days of warning before password expires : 7
```

```
login: suzuki
Password: ※□□□suzuki□□□□□□□□□□□□
You are required to change your password immediately (root enforced)
Changing password for suzuki.
```

```
(current) UNIX password: ※□□□suzuki□□□□□□□□□□□□
New password: ※□□□suzuki□□□□□□□□□□□□
Retype new password: ※□□□suzuki□□□□□□□□□□□□
```

cron

cron

cron cron 3

testuser

```
# useradd testuser
# id testuser
uid=502(testuser) gid=502(testuser) □□□□□□=502(testuser)
# userdel testuser
# id testuser
id: testuser: □□□□□□□□□□□□□□□
```

userdel

userdel

-r

```
# ls -l /home
□□ 28
drwx------.  2 root   root   16384  1□  6 06:07 2015 lost+found
drwx------. 26 sato   sato    4096  1□  6 06:49 2015 sato
drwx------.  5 suzuki suzuki  4096  1□  6 09:00 2015 suzuki
drwx------.  4   ※502    502※  4096  1□  6 09:56 2015 testuser
# ls -l /var/spool/mail
□□ 0
□□ 0
-rw-rw----. 1 rpc    mail 0  1□  6 06:11 2015 rpc
-rw-rw----. 1 sato   mail 0  1□  6 06:23 2015 sato
-rw-rw----. 1 suzuki mail 0  1□  6 06:48 2015 suzuki
-rw-rw----. 1   ※502※ mail 0  1□  6 09:56 2015 testuser
```

ID

testuser

```
# useradd testuser
useradd: □□: □□□□□□□□□□□□□□□□□□□
skel □□□□□□□□□□□□□□□□□□□□
□□□□□□□□□□□□□□□□□□: □□□□□□□□□□□
```

```
# ls -l /home
□□ 28
drwx------.  2 root     root     16384  1□  6 06:07 2015 lost+found
drwx------. 26 sato     sato      4096  1□  6 06:49 2015 sato
drwx------.  5 suzuki   suzuki    4096  1□  6 09:00 2015 suzuki
drwx------.  4 ※testuser testuser※  4096  1□  6 09:56 2015 testuser
# ls -l /var/spool/mail
□□ 0
-rw-rw----. 1 rpc      mail 0  1□  6 06:11 2015 rpc
-rw-rw----. 1 sato     mail 0  1□  6 06:23 2015 sato
-rw-rw----. 1 suzuki   mail 0  1□  6 06:48 2015 suzuki
-rw-rw----. 1 ※testuser※ mail 0  1□  6 09:56 2015 testuser
```

ID 502
testuser ID 502

userdel -r testuser

```
# userdel -r testuser
# ls -l /home
□□ 24
drwx------.  2 root   root   16384  1□  6 06:07 2015 lost+found
drwx------. 26 sato   sato    4096  1□  6 06:49 2015 sato
drwx------.  5 suzuki suzuki  4096  1□  6 09:00 2015 suzuki
# ls -l /var/spool/mail
□□ 0
-rw-rw----. 1 rpc    mail 0  1□  6 06:11 2015 rpc
-rw-rw----. 1 sato   mail 0  1□  6 06:23 2015 sato
-rw-rw----. 1 suzuki mail 0  1□  6 06:48 2015 suzuki
```

groupdel
/etc/group

testuser testuser testgroup

```
# useradd testuser
# groupadd testgroup
# gpasswd -a testuser testgroup
Adding user testuser to group testgroup
# id testuser
uid=502(testuser) gid=502(testuser) □□□□□□=502(testuser),5001(testgroup)
# groupdel testuser
```

```
groupdel: □□□ 'testuser' □□□□□□□□□□□□□□□□□□□□
# groupdel testgroup
# id testuser
uid=502(testuser) gid=502(testuser) □□□□□□=502(testuser)
```

SSH

SSH (Secure Shell) ( )
SSH

Linux OpenSSH Linux Windows
SSH

※1
2 Linux SSH SSH SSH
SSH

2 Linux

	IP
server.example.com	192.168.0.10
client.example.com	192.168.0.101

Linux /etc/hosts

```
192.168.0.10 server.example.com server
192.168.0.101 client.example.com client
```

SSH

CentOS OpenSSH sshd

SSH 22

```
[root@server ~]# lsof -i:22
COMMAND   PID   USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
sshd     1718   root    3u  IPv4  13399      0t0  TCP *:ssh (LISTEN)
sshd     1718   root    4u  IPv6  13401      0t0  TCP *:ssh (LISTEN)
```

SSH

SSH

SSH

SSH

sshuser

```
[root@server ~]# useradd sshuser
[root@server ~]# passwd sshuser
□□□ sshuser □□□□□□□□□□
□□□□□□□□: □□□□sshuser□□□□□□□□□□□□
□□□□□□□□□□□□□□□□□□□: □□□□sshuser□□□□□□□□□□□□□
passwd: □□□□□□□□□□□□□□□□□□□□□□
```

sshuser SSH

sshuser SSH ssh
ssh

ssh

```
ssh [□□□□@]□□□
```

IP

```
[sshuser@client ~]$ ssh sshuser@server
```

SSH SSH
yes sshuser

```
[sshuser@client ~]$ ssh sshuser@server
The authenticity of host 'server (192.168.0.10)' can't be established.
RSA key fingerprint is b6:95:54:92:62:cb:c8:f7:17:97:88:8e:69:f9:2a:dd.
Are you sure you want to continue connecting (yes/no)? ※yes ←yes□□□
Warning: Permanently added 'server,192.168.0.10' (RSA) to the list of know
```

```
sshuser@server's password: ※□□□□□□□□□□□sshuser□□□□□□□□□
[sshuser@server ~]$
```

ifconfig IP IP
192.168.0.10

```
[sshuser@server ~]$ ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:1C:42:65:AF:C4
          inet addr:192.168.0.10  Bcast:10.0.0.255  Mask:255.255.255.0
          inet6 addr: fe80::21c:42ff:fe65:afc4/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:19972 errors:0 dropped:0 overruns:0 frame:0
          TX packets:11094 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:15984761 (15.2 MiB)  TX bytes:992110 (968.8 KiB)
```

exit

```
[sshuser@server ~]$ exit
logout
Connection to server closed.
[sshuser@client ~]$
```

ssh

ssh -v ( )

```
[sshuser@client ~]$ ssh -v sshuser@server
OpenSSH_5.3p1, OpenSSL 1.0.1e-fips 11 Feb 2013
debug1: Reading configuration data /etc/ssh/ssh_config
debug1: Applying options for *
debug1: Connecting to server [192.168.0.10] port 22.
debug1: Connection established.
□□□□□
```

SSH

SSH .ssh
known_hosts
2

```
[sshuser@client ~]$ ssh sshuser@server
sshuser@server's password:
```

cat ~/.ssh/known_hosts

```
[sshuser@client ~]$ cat ~/.ssh/known_hosts
server,192.168.0.10 ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEA0xULiTzWSingpALtma
```

SSH SSH
~/.ssh/known_hosts SSH
yes ~/.ssh/known_hosts

2 SSH known_hosts SSH
SSH
ssh

SSH
SSH
SSH 2

SSH
~/.ssh/known_hosts SSH
~/.ssh/known_hosts vi SSH
1

SSH

1.
2.
3.

SSH

SSH Linux ssh-keygen

ssh-keygen
ssh-keygen
.ssh

SSH

```
[sshuser@client ~]$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/sshuser/.ssh/id_rsa): ※Enter□□□
Enter passphrase (empty for no passphrase): ※□□□□□□□□□□□□□□
Enter same passphrase again: ※□□□□□□□□□□□□□□
Your identification has been saved in /home/sshuser/.ssh/id_rsa.
Your public key has been saved in /home/sshuser/.ssh/id_rsa.pub.
The key fingerprint is:
91:47:d4:85:39:58:59:7e:d4:0b:50:7c:56:f7:28:45 sshuser@client
The key's randomart image is:
+--[ RSA 2048]----+
|         .o==OE *|
|         o. *= =+|
|        o . ..* +|
|         o   . o |
|        S        |
|                 |
|                 |
|                 |
|                 |
+-----------------+
```

~/.ssh id_rsa.pub (id_rsa) .ssh ssh ssh-keygen

```
[sshuser@client ~]$ ls -ld .ssh
drwx------. 2 sshuser sshuser 4096  1□  7 14:17 2015 .ssh
[sshuser@client ~]$ ls -l .ssh
□□ 8
-rw-------. 1 sshuser sshuser 1743  1□  7 14:17 2015 id_rsa
-rw-r--r--. 1 sshuser sshuser  396  1□  7 14:17 2015 id_rsa.pub
```

cat

```
[sshuser@client ~]$ cat .ssh/id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAxaKrCiK5rrJBqtjG3NbWoRlGJMGEqkND6WYTfL
```

1

```
[sshuser@client .ssh]$ cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,9A3828879701873A

kSkjcd/9+VWwk2NR8CuET4CXKu7ZIAOkNmvHwUZVMpUlnDwqxeznXP4NVGEq5uFD
□□□
Jw6FruKNyjl8mqLtrj+eltCUh6N4Z+NPVzlAHMQ9IQmBjdpArj0SLQ==
-----END RSA PRIVATE KEY-----
```

.ssh

.ssh

ssh-keygen

ssh
root root

~/.ssh	rwx------(700)
id_rsa.pub	rw-r--r--(644)
id_rsa	rw-------(600)

SSH (id_rsa.pub)

1.
2. ~/.ssh
3. ~/.ssh/authorized_keys
4. ~/.ssh/authorized_keys
5.

1

1.

id_rsa.pub SSH
scp

scp

```
scp □□□□□□□□ □□□□@□□□:□□□□□□□□
```

scp ~/.ssh/id_rsa.pub sshuser

```
[sshuser@client ~]$ scp ~/.ssh/id_rsa.pub sshuser@server:~
sshuser@server's password: ※□□□□□□□□□□□□sshuser□□□□□□□□□
id_rsa.pub                                    100%  396     0.4KB/s   00:0
```

2

1. ~/.ssh

ssh

```
[sshuser@client ~]$ ssh sshuser@server
sshuser@server's password: ※□□□□□□□□□□□sshuser□□□□□□□□□
Last login: Tue Jan  6 10:58:42 2015 from client
[sshuser@server ~]$
```

id_rsa.pub

```
[sshuser@server ~]$ ls -l
□□ 4
-rw-r--r--. 1 sshuser sshuser 396  1□  6 10:56 2015 id_rsa.pub
[sshuser@server ~]$ cat id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAxaKrCiK5rrJBqtjG3NbWoRlGJMGEqkND6WYTfL
```

.ssh chmod

```
[sshuser@server ~]$ mkdir .ssh
[sshuser@server ~]$ chmod 700 .ssh
[sshuser@server ~]$ ls -ld .ssh
drwx------. 2 sshuser sshuser 4096  1□  6 10:59 2015 .ssh
```

3

1. ~/.ssh/authorized_keys

.ssh authorized_keys

```
[sshuser@server ~]$ touch .ssh/authorized_keys
[sshuser@server ~]$ chmod 600 .ssh/authorized_keys
[sshuser@server ~]$ ls -l .ssh
□□ 0
-rw-------. 1 sshuser sshuser 0  1□  6 10:59 2015 authorized_keys
```

4

1. ~/.ssh/authorized_keys

authorized_keys cat “>>” authorized_keys
authorized_keys cp mv
authorized_keys SELinux

```
[sshuser@server ~]$ cat id_rsa.pub >> .ssh/authorized_keys
[sshuser@server ~]$ cat .ssh/authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAxaKrCiK5rrJBqtjG3NbWoRlGJMGEqkND6WYTfL
```

5

1.

```
[sshuser@server ~]$ exit
logout
Connection to server closed.
[sshuser@client ~]$ ssh sshuser@server
Enter passphrase for key '/home/sshuser/.ssh/id_rsa': ※□□□□□□□□□□□□□□
Last login: Tue Jan  6 10:59:03 2015 from client
[sshuser@server ~]$
```

ssh-copy-id

SSH ssh-copy-id
ssh-copy-id authorized_keys

ssh-copy-id

```
ssh-copy-id □□□□@□□□
```

ssh-copy-id

```
[sshuser@client ~]$ ssh-copy-id sshuser@server
sshuser@server's password:
Now try logging into the machine, with "ssh 'sshuser@server'", and check i

  .ssh/authorized_keys

to make sure we haven't added extra keys that you weren't expecting.
```

SSH

```
[sshuser@client ~]$ ssh sshuser@server
Enter passphrase for key '/home/sshuser/.ssh/id_rsa': ※□□□□□□□□□□□□□□
Last login: Tue Jan  6 11:01:52 2015 from client
[sshuser@server ~]$
```

OpenSSH

scp

scp SSH

testdir

scp -r

```
[sshuser@client ~]$ mkdir testdir
[sshuser@client ~]$ cd testdir
[sshuser@client testdir]$ touch testfile1 testfile2
[sshuser@client testdir]$ ls
testfile1  testfile2
[sshuser@client testdir]$ cd
[sshuser@client ~]$ scp -r testdir sshuser@server:~
Enter passphrase for key '/home/sshuser/.ssh/id_rsa': ※□□□□□□□□□□□□□□
testfile1                                     100%    0     0.0KB/s   00:0
testfile2                                     100%    0     0.0KB/s   00:0
```

```
[sshuser@client ~]$ ssh sshuser@server
Enter passphrase for key '/home/sshuser/.ssh/id_rsa': ※□□□□□□□□□□□□□□
Last login: Tue Jan  6 11:02:46 2015 from client
[sshuser@server ~]$ ls
id_rsa.pub  testdir
[sshuser@server ~]$ ls -l testdir
□□ 0
-rw-rw-r--. 1 sshuser sshuser 0  1□  6 11:04 2015 testfile1
-rw-rw-r--. 1 sshuser sshuser 0  1□  6 11:04 2015 testfile2
```

sftp

SFTP (SSH File Transfer Protocol) SSH FTP

sftp

”sftp>”

```
[sshuser@client ~]$ touch sftptestfile
[sshuser@client ~]$ ls
sftptestfile  testdir
[sshuser@client ~]$ sftp sshuser@server
Connecting to server...
Enter passphrase for key '/home/sshuser/.ssh/id_rsa': ※□□□□□□□□□□□□□□
sftp>
```

“put ”

```
sftp> put sftptestfile
Uploading sftptestfile to /home/sshuser/sftptestfile
sftptestfile                                  100%    0     0.0KB/s   00:0
```

ls

```
sftp> ls
id_rsa.pub      sftptestfile    testdir
sftp> ls -l
-rw-r--r--    1 sshuser  sshuser       396 Jan  6 10:56 id_rsa.pub
-rw-rw-r--    1 sshuser  sshuser         0 Jan  6 11:20 sftptestfile
drwxrwxr-x    2 sshuser  sshuser      4096 Jan  6 11:04 testdir
sftp> exit
[sshuser@client ~]$
```

SFTP

pwd

ls

cd [ ]

put [-P] [-P]

get [-P] [-P]

rm

mkdir

rmdir

lpwd

lls [ls] [ ]

lcd

lmkdir

Windows SSH

Tera Term Windows

Windows Tera Term SSH OpenSSH Tera Term SSH SCP

Tera Term Tera Term Web .EXE

`http://sourceforge.jp/projects/ttssh2/`

Tera Term

1. Tera Term

   IP IP

IP SSH
OK

2

2.

knows hosts

3

3.

SSH

4

4.

Tera Term

Tera Term

1.

Tera Term SSH

TTSSH:

2

2.

3

3.

Tera Term

Tera Term SSH SCP
id_rsa.pub

1. Secure File Copy

From:
From:

TeraTerm SSH SCP

2

2.
TTSSH: Secure File Copy From: ...
id_rsa.pub

3.
Send

4.

```
[sshuser@server ~]$ ls
id_rsa.pub  sftptestfile  testdir
```

5.
Linux authorized_keys

```
[sshuser@server ~]$ mkdir .ssh
[sshuser@server ~]$ chmod 700 .ssh
[sshuser@server ~]$ touch .ssh/authorized_keys
[sshuser@server ~]$ chmod 600 .ssh/authorized_keys
[sshuser@server ~]$ cat id_rsa.pub >>  .ssh/authorized_keys
```

Tera Term　　Windows

Tera Term

1. Tera Term
2. SSH
3. RSA/DSA/EC DSA
   id_rsa　　OK

   RSA/DSA/EC DSA
   RSA/DSA/EC DSA

   TeraTerm

root

OpenSSH

OpenSSH　　/etc/ssh/sshd_config

```
[root@server ~]# vi /etc/ssh/sshd_config

PasswordAuthentication ※no ←no□□□
```

root　　root
root　　SSH

```
PermitRootLogin ※no ←no□□□
```

service　　sshd

```
[root@server ~]# service sshd restart
sshd □□□□:                                                [  OK  ]
sshd □□□□:                                                [  OK  ]
```

root　　SSH

root

root
root　　3

- root
- su　　root
- sudo　　root

root su
sudo

root

root

root
last root

```
# last
root     ttyS0                          Mon Aug 11 12:56   still logged in
root     ttyS0                          Mon Aug 11 12:23 - 12:56  (00:32)
root     ttyS0                          Mon Aug 11 01:11 - 12:23  (11:11)
```

root
root root

OpenSSH root ( )
SSH SSH
OpenSSH IP

su root

su root root

uid 501 suzuki su

```
$ su -
□□□□□:
# tail /var/log/secure
□□□
Jan  6 11:33:55 server su: pam_unix(su-l:session): session opened for user
```

root root

su

su

su root root
PAM Pluggable Authentication Modules su

wheel su root

PAM /etc/pam.d/su vi 2
wheel su

wheel su

```
#  vi /etc/pam.d/su

#%PAM-1.0
auth            sufficient      pam_rootok.so
# Uncomment the following line to implicitly trust users in the "wheel" gr
auth           sufficient      pam_wheel.so trust use_uid ※←□□□#□□□
# Uncomment the following line to require a user to be in the "wheel" grou
auth           required        pam_wheel.so use_uid ※←□□□#□□□
auth            include         system-auth
account         sufficient      pam_succeed_if.so uid = 0 use_uid quiet
account         include         system-auth
password        include         system-auth
session         include         system-auth
session         optional        pam_xauth.so
```

suzuki su root root

```
$ id suzuki
uid=501(suzuki) gid=501(suzuki) □□□□□□=501(suzuki),5000(eigyou)
$ su -
□□□□□:
su: □□□□□□□□□□
```

root gpasswd suzuki wheel

```
# gpasswd -a suzuki wheel
Adding user suzuki to group wheel
```

suzuki su
root

```
$ id suzuki
uid=501(suzuki) gid=501(suzuki) □□□□□□=501(suzuki),10(wheel),5000(eigyou)
```

```
$ su -
[root@server ~]#
```

sudo

sudo root
su sudo

sudo
root

CentOS sudo

```
$ id suzuki
uid=501(suzuki) gid=501(suzuki) □□□□□□=501(suzuki),10(wheel),5000(eigyou)
$ sudo cat /etc/shadow

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

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

[sudo] password for suzuki: ※□□□suzuki□□□□□□□□□
suzuki □ sudoers □□□□□□□□□□□□□□□□□□□□□□□□□□□□
```

sudo wheel sudo

root visudo /etc/sudoers wheel
sudo

```
# visudo
```

%wheel wheel ALL=(ALL)
ALL

```
%wheel ALL=(ALL)       ALL ※←□□□#□□□
```

visudo vi :wq

sudo useradd

```
$ sudo useradd testuser
[sudo] password for suzuki: ※□□□suzuki□□□□□□□□□
```

```
[suzuki@server ~]$ id testuser
uid=503(testuser) gid=503(testuser) □□□□□□=503(testuser)
```

sudo

sudo

webadm Web httpd
visudo 1

```
$ sudo visudo

%webadm       ALL=NOPASSWD:  /sbin/service httpd start, /sbin/service http
```

webadm useradd -G

```
sudo groupadd webadm
sudo useradd -G webadm httpdtest
```

su - httpdtest

```
$ sudo su - httpdtest
$ id
uid=504(httpdtest) gid=504(httpdtest) □□□□□□=504(httpdtest),5001(webadm)
```

sudo Web

```
$ sudo service httpd start
httpd □□□□: httpd: Could not reliably determine the server's fully qualifi
                                                                  [  OK  ]
```

Web

```
$ ps ax | grep httpd
28608 pts/0    S      0:00 su - httpdtest
31175 ?        Ss     0:00 /usr/sbin/httpd
31176 ?        S      0:00 /usr/sbin/httpd
31177 ?        S      0:00 /usr/sbin/httpd
31179 ?        S      0:00 /usr/sbin/httpd
31180 ?        S      0:00 /usr/sbin/httpd
31181 ?        S      0:00 /usr/sbin/httpd
31182 ?        S      0:00 /usr/sbin/httpd
31183 ?        S      0:00 /usr/sbin/httpd
31184 ?        S      0:00 /usr/sbin/httpd
31198 pts/0    S+     0:00 grep httpd
```

Web

```
$ sudo service httpd stop
httpd □□□□:                                                [  OK  ]
$ ps ax | grep httpd
28608 pts/0    S      0:00 su - httpdtest
31325 pts/0    S+     0:00 grep httpd
```

Web

IP

ip

ip
ARP

IP MAC ip address show

```
# ip address show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state
    link/ether 00:1c:42:dc:25:92 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.10/24 brd 192.168.0.255 scope global eth0
    inet6 fe80::21c:42ff:fedc:2592/64 scope link
       valid_lft forever preferred_lft forever
```

ip route show route

```
# ip route show
192.168.0.0/24 dev eth0  proto kernel  scope link  src 192.168.0.10  metri
default via 192.168.0.1 dev eth0  proto static
```

default 192.168.0.1
eth0

ARP

ARP ip neighbor show neighbor neigh

```
#  ip neigh show
192.168.0.1 dev eth0 lladdr 00:1c:42:00:00:18 STALE
192.168.0.2 dev eth0 lladdr 00:1c:42:00:00:08 REACHABLE
```

netstat

※ss
netstat

-i
-n IP
-a
-l
-t TCP
-u UDP

netstat -i

```
# netstat -i
Kernel Interface table
Iface       MTU Met    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP T
eth0       1500   0    47780      0      0      0    16784      0      0
lo        65536   0     2366      0      0      0     2366      0      0
```

TCP

TCP netstat -nat

```
# netstat -nat
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address               Foreign Address
tcp        0      0 0.0.0.0:22                  0.0.0.0:*
tcp        0      0 127.0.0.1:631               0.0.0.0:*
tcp        0      0 127.0.0.1:25                0.0.0.0:*
tcp        0      0 0.0.0.0:37729               0.0.0.0:*
tcp        0      0 0.0.0.0:111                 0.0.0.0:*
tcp        0      0 :::22                       :::*
tcp        0      0 ::1:631                     :::*
tcp        0      0 ::1:25                      :::*
tcp        0      0 :::37114                    :::*
tcp        0      0 :::111                      :::*
```

TCP

TCP netstat -nlt

```
# netstat -nlt
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address               Foreign Address
tcp        0      0 0.0.0.0:22                  0.0.0.0:*
tcp        0      0 127.0.0.1:631               0.0.0.0:*
tcp        0      0 127.0.0.1:25                0.0.0.0:*
tcp        0      0 0.0.0.0:37729               0.0.0.0:*
tcp        0      0 0.0.0.0:111                 0.0.0.0:*
tcp        0      0 :::22                       :::*
tcp        0      0 ::1:631                     :::*
tcp        0      0 ::1:25                      :::*
tcp        0      0 :::37114                    :::*
tcp        0      0 :::111                      :::*
```

UDP

UDP netstat -nlu

```
# netstat -nlu
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address               Foreign Address
udp        0      0 0.0.0.0:68                  0.0.0.0:*
udp        0      0 127.0.0.1:708               0.0.0.0:*
udp        0      0 0.0.0.0:111                 0.0.0.0:*
udp        0      0 0.0.0.0:631                 0.0.0.0:*
udp        0      0 192.168.0.10:123            0.0.0.0:*
udp        0      0 127.0.0.1:123               0.0.0.0:*
udp        0      0 0.0.0.0:123                 0.0.0.0:*
udp        0      0 0.0.0.0:44415               0.0.0.0:*
udp        0      0 0.0.0.0:655                 0.0.0.0:*
udp        0      0 :::111                      :::*
udp        0      0 fe80::21c:42ff:fedc:2592:123 :::*
udp        0      0 ::1:123                     :::*
udp        0      0 :::123                      :::*
udp        0      0 :::39182                    :::*
udp        0      0 :::655                      :::*
```

ping

IP ping Ctrl+C

```
# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=128 time=6.26 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=128 time=3.28 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=128 time=2.85 ms
※^C Ctrl+C□□□□□□□
--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 62.780/64.980/66.416/1.579 ms
```

-c 5

```
# ping -c 5 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=128 time=3.39 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=128 time=3.12 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=128 time=3.44 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=128 time=2.85 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=128 time=3.10 ms

--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4012ms
rtt min/avg/max/mdev = 2.856/3.185/3.440/0.225 ms
```

ping ICMP
ICMP ping
ping

(RTT) 1ms( )
10ms 30ms 500ms

ethtool

ethtool

ethtool

```
# ethtool eth0
Settings for eth0:
   Supported ports: [ TP ]
   Supported link modes:   10baseT/Half 10baseT/Full
                           100baseT/Half 100baseT/Full
                           1000baseT/Full
   Supported pause frame use: No
   Supports auto-negotiation: Yes
   Advertised link modes:  10baseT/Half 10baseT/Full
                           100baseT/Half 100baseT/Full
```

```
                        1000baseT/Full
   Advertised pause frame use: No
   Advertised auto-negotiation: Yes
   Speed: 1000Mb/s
   Duplex: Full
   Port: Twisted Pair
   PHYAD: 1
   Transceiver: internal
   Auto-negotiation: on
   MDI-X: Unknown
   Supports Wake-on: g
   Wake-on: g
   Link detected: yes
```

ethtool -i

```
# ethtool -i eth0
driver: bnx2
version: 2.2.3
firmware-version: bc 4.6.4 NCSI 1.0.3
bus-info: 0000:02:00.0
supports-statistics: yes
supports-test: yes
supports-eeprom-access: yes
supports-register-dump: yes
supports-priv-flags: no
```

```
# ethtool eth0
Settings for eth0:
 Link detected: yes
```

```
# ethtool -i eth0
driver: virtio_net
version:
firmware-version:
bus-info: virtio0
supports-statistics: no
supports-test: no
supports-eeprom-access: no
supports-register-dump: no
supports-priv-flags: no
```

Linux

/etc/sysconfig/network

/etc/sysconfig/network

```
# cat /etc/sysconfig/network
NETWORKING=yes
HOSTNAME=server.example.com
NTPSERVERARGS=iburst
```

HOSTNAME

/etc/hosts

/etc/hosts IP

```
# cat /etc/hosts
127.0.0.1   localhost localhost.localdomain localhost4 localhost4.localdom
::1         localhost localhost.localdomain localhost6 localhost6.localdom

192.168.0.10 server.example.com server
192.168.0.101 client.example.com client
```

DNS /etc/resolv.conf

/etc/resolv.conf DNS DNS
DNS DNS DNS
DNS

```
# cat /etc/resolv.conf
# Generated by NetworkManager
search example.com
nameserver 192.168.0.1
```

/etc/resolv.conf

/etc/resolv.conf DNS
NetworkManager network DHCP
/etc/resolv.conf /etc/resolv.conf
/etc/resolv.conf

DNS
/etc/resolv.conf

/etc/sysconfig/network-scripts/ifcfg-eth0 DNS1 DNS DNS2
DNS

```
DNS1=192.168.0.1
DNS2=192.168.0.2
```

NetworkManager network
/etc/resolv.conf

/etc/nsswitch.conf

/etc/nsswitch.conf
/etc/hosts DNS NIS

```
# cat /etc/nsswitch.conf
□□□
#hosts:     db files nisplus nis dns
hosts:      files dns
□□□
```

files dns /etc/hosts
DNS

/etc/services

/etc/services TCP/UDP

HTTP

```
http          80/tcp        www www-http # WorldWideWeb HTTP
```

TCP 80
http
netstat -n -n

```
# netstat -nat | grep 80
tcp        0      0 :::80                         :::*
# netstat -at | grep http
tcp        0      0 *:http                        *:*
```

80 http
/etc/services
1 IPv6 IPv6 Apache Web
IPv4

/etc/protocols

/etc/protocols

```
ip 0 IP  # internet protocol, pseudo protocol number
icmp 1 ICMP  # internet control message protocol
tcp 6 TCP  # transmission control protocol
udp 17 UDP  # user datagram protocol
```

iptables

iptables　Linux

iptables　NF(netfilter)
iptables

iptables　NAT

iptables　NAT(Network Address Translation)
IP
NAT　IP　LAN
IP

NAT

IP　IP　1　1
IP　IP　IP
IP

NAT

IP　IP　N　N
IP　IP　IP
IP
IP　IP
IP
IP　NAPT

NAPT(IP)

IP 1 IP IP
IP NAPT
65535 1 IP

iptables

service iptables

```
# service iptables start
iptables: □□□□□□□□□ ACCEPT □□□□filter          [  OK  ]
iptables: □□□□□□□□□□□□□□□□:                   [  OK  ]
iptables: □□□□□□□□□□□□:                          [  OK  ]
iptables: □□□□□□□□□□□□□□□□:                   [  OK  ]
```

service iptables

```
# service iptables stop
iptables: □□□□□□□□□ ACCEPT □□□□filter          [  OK  ]
iptables: □□□□□□□□□□□□□□□□:                   [  OK  ]
iptables: □□□□□□□□□□□□:                          [  OK  ]
```

iptables

service iptables

```
# service iptables start
iptables: □□□□□□□□□□□□□□□□:                   [  OK  ]
# service iptables status
□□□□: filter
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination
1    ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0           state RE
2    ACCEPT     icmp --  0.0.0.0/0            0.0.0.0/0
3    ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
4    ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NE
5    REJECT     all  --  0.0.0.0/0            0.0.0.0/0           reject-w

Chain FORWARD (policy ACCEPT)
num  target     prot opt source               destination
1    REJECT     all  --  0.0.0.0/0            0.0.0.0/0           reject-w

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination
```

iptables -L iptables

```
# iptables -L
```

iptables-save　　iptables　　iptables

```
# iptables-save
# Generated by iptables-save v1.4.7 on Fri Jan  9 16:51:47 2015
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [33:4180]
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
# Completed on Fri Jan  9 16:51:47 2015
```

iptables-A

```
iptables -A □□□□ □□ -j □□□□□
```

INPUT
OUTPUT
FORWARD
PREROUTING
POSTROUTING

ACCEPT
DROP
REJECT [--reject-with]　　ICMP
LOG　　syslog

iptables

INPUT

```
iptables -A INPUT -m tcp -p tcp --dport □□□□□ -j ACCEPT
```

TCP 80 (HTTP) iptables REJECT

/etc/sysconfig/iptables iptables

```
# iptables -A INPUT -m tcp -p tcp --dport 80 -j ACCEPT
# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere            state RELATED
ACCEPT     icmp --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere
ACCEPT     tcp  --  anywhere             anywhere            state NEW tcp
REJECT     all  --  anywhere             anywhere            reject-with i
ACCEPT     tcp  --  anywhere             anywhere            tcp dpt:http
□□□
```

iptables

iptables

```
# service iptables save
iptables: Saving firewall rules to /etc/sysconfig/iptables: [  OK  ]
```

iptables /etc/sysconfig/iptables iptables

iptables iptables

iptables

/etc/sysconfig/iptables ( )
service iptables reload

iptables service iptables restart
iptables restart
reload

```
# service iptables reload
iptables: Trying to reload firewall rules:                  [  OK  ]
```

system-config-firewall-tui iptables

system-config-firewall-tui iptable CUI

```
# yum install system-config-firewall-tui
```

1. system-config-firewall-tui

```
# system-config-firewall-tui
```

2

2.

system-config-firewall-tui
Enter TAB

3

3.

WWW
(HTTP)

4.

OK iptables

5

5.

system-config-firewall-tui /etc/sysconfig/iptables
iptables

WWW(HTTP) 80

```
# cat /etc/sysconfig/iptables
# Firewall configuration written by system-config-firewall
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
```

```
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

AlmaLinux firewalld firewalld firewalld firewall-cmd

```
$ sudo firewall-cmd --list-services
cockpit dhcpv6-client http ssh
```

HTTP SSH

imap

```
$ sudo firewall-cmd --add-service=imap
success
```

```
sudo firewall-cmd --add-service=imap --zone=public --permanent
sudo firewall-cmd --reload
```

```
$ sudo firewall-cmd --get-services
RH-Satellite-6 amanda-client amanda-k5-client bacula bacula-client bgp bit
```

```
$ sudo firewall-cmd --remove-service=imap
success
```

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

OS

OS

1.
2. BIOS
3. GRUB
4. Linux
5. init
6.
7. OS

GRUB

BIOS
GRUB

GRUB Linux

GRUB
GRUB

Linux GRUB
GRUB Enter

GRUB
grubby --info=ALL

GRUB
grubby --default-kernel

GRUB
grubby --default-index

GRUB
grubby --set-default /boot/vmlinuz-5.14.0-503.11.1.el9_5.x86_64

GRUB
grubby --set-default 1

GRUB

$ sudo grubby --info=ALL
[sudo] linuc :

```
index=0
kernel="/boot/vmlinuz-5.14.0-570.25.1.el9_6.aarch64"
args="ro crashkernel=1G-4G:256M,4G-64G:320M,64G-:576M rd.lvm.lv=almalinux_vbox/root
rd.lvm.lv=almalinux_vbox/swap rhgb quiet $tuned_params"
root="/dev/mapper/almalinux_vbox-root"
initrd="/boot/initramfs-5.14.0-570.25.1.el9_6.aarch64.img $tuned_initrd"
title="AlmaLinux (5.14.0-570.25.1.el9_6.aarch64) 9.6 (Sage Margay)"
id="9e034831eddf4bbb9525d8a0f6676c28-5.14.0-570.25.1.el9_6.aarch64"
index=1
kernel="/boot/vmlinuz-5.14.0-570.12.1.el9_6.aarch64"
args="ro crashkernel=1G-4G:256M,4G-64G:320M,64G-:576M rd.lvm.lv=almalinux_vbox/root
rd.lvm.lv=almalinux_vbox/swap rhgb quiet $tuned_params"
root="/dev/mapper/almalinux_vbox-root"
initrd="/boot/initramfs-5.14.0-570.12.1.el9_6.aarch64.img $tuned_initrd"
title="AlmaLinux (5.14.0-570.12.1.el9_6.aarch64) 9.6 (Sage Margay)"
id="9e034831eddf4bbb9525d8a0f6676c28-5.14.0-570.12.1.el9_6.aarch64"
index=2
kernel="/boot/vmlinuz-0-rescue-9e034831eddf4bbb9525d8a0f6676c28"
args="ro crashkernel=1G-4G:256M,4G-64G:320M,64G-:576M rd.lvm.lv=almalinux_vbox/root
rd.lvm.lv=almalinux_vbox/swap rhgb quiet"
root="/dev/mapper/almalinux_vbox-root"
initrd="/boot/initramfs-0-rescue-9e034831eddf4bbb9525d8a0f6676c28.img"
title="AlmaLinux (0-rescue-9e034831eddf4bbb9525d8a0f6676c28) 9.6 (Sage Margay)"
id="9e034831eddf4bbb9525d8a0f6676c28-0-rescue"
```

index

kernel

args

root

initrd

RAM

title

id

ID

GRUB Linux

RAM initramfs
RAM

dmesg

dmesg

```
# dmesg
Initializing cgroup subsys cpuset
Initializing cgroup subsys cpu
Linux version 2.6.32-504.el6.x86_64 (mockbuild@c6b9.bsys.dev.centos.org) (
Command line: ro root=/dev/mapper/vg_server-lv_root rd_LVM_LV=vg_server/lv
KERNEL supported cpus:
  Intel GenuineIntel
  AMD AuthenticAMD
  Centaur CentaurHauls
Disabled fast string operations
BIOS-provided physical RAM map:
 BIOS-e820: 0000000000000000 - 000000000009ec00 (usable)
```

systemd

systemd

systemd

service
target
mount
swap

device

systemd systemctl

Web systemctl

systemctl start

```
# systemctl start httpd
```

systemctl status

systemd cgroup Linux
cgroup CPU

```
# systemctl status httpd
httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled)
   Active: active (running) since □ 2015-01-28 15:23:50 JST; 33s ago
 Main PID: 2926 (httpd)
   Status: "Total requests: 0; Current requests/sec: 0; Current traffic:
   CGroup: /system.slice/httpd.service
           ├─2926 /usr/sbin/httpd -DFOREGROUND
           ├─2927 /usr/sbin/httpd -DFOREGROUND
           ├─2928 /usr/sbin/httpd -DFOREGROUND
           ├─2929 /usr/sbin/httpd -DFOREGROUND
           ├─2930 /usr/sbin/httpd -DFOREGROUND
           └─2931 /usr/sbin/httpd -DFOREGROUND

 1□ 28 15:23:50 centos7.example.com httpd[2926]: AH00557: httpd: apr_socka
 1□ 28 15:23:50 centos7.example.com httpd[2926]: AH00558: httpd: Could not
 1□ 28 15:23:50 centos7.example.com systemd[1]: Started The Apache HTTP Se
Hint: Some lines were ellipsized, use -l to show in full.
```

systemctl restart

```
# systemctl restart httpd
# systemctl status httpd
httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled)
   Active: active (running) since □ 2015-01-28 15:24:40 JST; 2s ago
  Process: 2945 ExecStop=/bin/kill -WINCH ${MAINPID} (code=exited, status=
 Main PID: 2950 (httpd)
□□□
```

systemctl stop

```
# systemctl stop httpd
# systemctl status httpd
httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled)
   Active: inactive (dead)
```

systemd systemctl list-unit-files

```
# systemctl list-unit-files
```

-t

service systemctl

```
# systemctl list-unit-files -t service
```

STATE

enabled
disabled
static

systemctl list-units systemctl

```
# systemctl list-units
# systemctl
```

-t service

```
# systemctl -t service
UNIT                          LOAD   ACTIVE SUB     DESCRIPTION
abrt-ccpp.service             loaded active exited  Install ABRT coredump h
abrt-oops.service             loaded active running ABRT kernel log watcher
abrt-xorg.service             loaded active running ABRT Xorg log watcher
abrtd.service                 loaded active running ABRT Automated Bug Repo
alsa-state.service            loaded active running Manage Sound Card State
atd.service                   loaded active running Job spooling tools
□□□
kdump.service                 loaded failed failed  Crash recovery kernel a
□□□
```

UNIT

LOAD systemd

ACTIVE active inactive

SUB running exited

DESCRIPTION

ACTIVE active inactive
--all

LOAD systemctl mask masked

ACTIVE failed
kdump

-t device

```
# systemctl list-units -t device
UNIT
sys-devices-pci0000:00-0000:00:05.0-virtio0-net-eth0.device
sys-devices-pci0000:00-0000:00:1f.2-ata3-host2-target2:0:0-2:0:0:0-block-s
□□□
```

-t mount

```
# systemctl list-units -t mount
UNIT                          LOAD   ACTIVE SUB     DESCRIPTION
```

```
-.mount                      loaded active mounted /
boot.mount                   loaded active mounted /boot
dev-hugepages.mount          loaded active mounted Huge Pages File System
dev-mqueue.mount             loaded active mounted POSIX Message Queue Fil
home.mount                   loaded active mounted /home
□□□
```

-t swap

```
# systemctl list-units -t swap
UNIT             LOAD   ACTIVE SUB    DESCRIPTION
dev-dm¥x2d0.swap loaded active active /dev/dm-0
□□□
```

systemctl enable

Web /usr/lib/systemd/system/httpd.service Web systemctl enable /etc/systemd/system/multi-user.target.wants

multi-user.target

```
# systemctl enable httpd
ln -s '/usr/lib/systemd/system/httpd.service' '/etc/systemd/system/multi-u
```

systemctl disable

```
# systemctl disable httpd
rm '/etc/systemd/system/multi-user.target.wants/httpd.service'
```

systemd

systemctl mask systemd

/etc/systemd/system/httpd.service /dev/null

Web systemd

```
# systemctl mask httpd
ln -s '/dev/null' '/etc/systemd/system/httpd.service'
```

```
# systemctl start httpd
Failed to issue method call: Unit httpd.service is masked.
```

systemctl is-enabled httpd masked

```
# systemctl is-enabled httpd
masked
```

systemctl unmask systemd httpd disabled

```
# systemctl unmask httpd
rm '/etc/systemd/system/httpd.service'
# systemctl is-enabled httpd
disabled
```

systemd

systemd

systemctl enable systemd 2

/usr/lib/systemd/system

/etc/rc.d/init.d

/etc/systemd/system

/etc/rc.d

systemd /etc/systemd/system

1. /etc/systemd/system/sysinit.target.wants/

rc.sysinit

2. /etc/systemd/system/basic.target.wants/

3. /etc/systemd/system/multi-user.target.wants/

3 CUI

4. /etc/systemd/system/graphical.target.wants/

5 GUI

systemd multi-user.target graphical.target

systemd

CUI GUI

systemctl set-default

systemctl get-default

```
# systemctl get-default
graphical.target
```

CUI

multi-user.target CUI

```
# systemctl set-default multi-user.target
# reboot
```

GUI

GUI systemctl set-default

```
# systemctl set-default graphical.target
# reboot
```

systemd systemctl isolate

GUI CUI GUI

```
# systemctl isolate multi-user.target
```

CUI　GUI

```
# systemctl isolate graphical.target
```

anacron

cron　　cron
　　cron　　CPU　　I/O

　anacron

anacron

1	/etc/cron.daily
1	/etc/cron.weekly
1	/etc/cron.monthly

anacron

anacron　1　crond　　/etc/anacrontab

```
# cat /etc/anacrontab
# /etc/anacrontab: configuration file for anacron

# See anacron(8) and anacrontab(5) for details.

SHELL=/bin/sh
PATH=/sbin:/bin:/usr/sbin:/usr/bin
MAILTO=root
# the maximal random delay added to the base delay of the jobs
RANDOM_DELAY=45
# the jobs will be started during the following hours only
START_HOURS_RANGE=3-22

#period in days   delay in minutes   job-identifier   command
1       5       cron.daily              nice run-parts /etc/cron.daily
7       25      cron.weekly             nice run-parts /etc/cron.weekly
@monthly 45     cron.monthly            nice run-parts /etc/cron.monthly
```

1 7
1

@daily 1 1
@weekly 7 1
@monthly 1

45 RANDOM_DELAY
2 1
5 1 25 1 45

anacron START_HOURS_RANGE 3 22
anacron

/etc/anacrontab 23 6

```
START_HOURS_RANGE=23-6
```

NTP

1 OFF

NTP Network Time Protocol NTP
NTP

NTP

NTP NTP NTP
NTP NTP NTP NTP

NTP yum

```
# yum install ntp
```

NTP

NTP ntpd

```
# service ntpd start
```

chkconfig

```
# chkconfig ntpd on
# chkconfig --list ntpd
ntpd            0:off   1:off   2:off   3:on    4:off   5:off   6:off
```

NTP NTP

NTP

NTP /etc/ntp.conf
CentOS pool.ntp.org NTP
pool.ntp.org NTP

```
server 0.centos.pool.ntp.org iburst
server 1.centos.pool.ntp.org iburst
server 2.centos.pool.ntp.org iburst
server 3.centos.pool.ntp.org iburst
```

ntpq NTP

```
# ntpq -p
     remote           refid      st t when poll reach   delay   offset  ji
==============================================================================
*219x123x70x91.a 192.168.7.123    2 u  424 1024  377    2.296   -0.851   1
-balthasar.gimas 65.32.162.194    3 u  764 1024  377    4.574    3.282   1
+ntp-v6.chobi.pa 61.114.187.55    2 u  960 1024  337    1.012    0.546   1
+the.platformnin 22.42.17.250     3 u   46 1024  377    3.686    0.123   2
```

*

+

x

NTP

NTP NTP

NTP /etc/ntp.conf 192.168.0.0/255.255.255.0
NTP

```
# vi /etc/ntp.conf
```

```
# Hosts on local network are less restricted.
#restrict 192.168.1.0 mask 255.255.255.0 nomodify notrap
※restrict 192.168.0.0 mask 255.255.255.0 nomodify notrap ←□□□□□□
```

ntp

```
# service ntpd restart
ntpd □□□□:                                                [  OK  ]
ntpd □□□□:                                                [  OK  ]
```

NTP UDP 123 NTP
iptables

/etc/sysconfig/iptables iptables

```
# vi /etc/sysconfig/iptables

# Firewall configuration written by system-config-firewall
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT
※-A INPUT -m state --state NEW -m udp -p udp --dport 123 -j ACCEPT ←□□□□□□
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

service iptables

```
# service iptables reload
iptables: Trying to reload firewall rules:                [  OK  ]
# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
□□□
ACCEPT     udp  --  anywhere             anywhere            state NEW udp
REJECT     all  --  anywhere             anywhere            reject-with i
□□□
```

NTP　　NTP　　NTP

NTP　　/etc/ntp.conf　server　　NTP

pool.ntp.org　server　　NTP
192.168.0.10

NTP　　yum

```
[root@client ~]# yum install ntp
[root@client ~]# vi /etc/ntp.conf

※#※server 0.centos.pool.ntp.org iburst ※←□□□□□□□□□□
※#※server 1.centos.pool.ntp.org iburst ※←□□□□□□□□□□
※#※server 2.centos.pool.ntp.org iburst ※←□□□□□□□□□□
※#※server 3.centos.pool.ntp.org iburst ※←□□□□□□□□□□
※server 192.168.0.10 iburst ←□□□□□□
```

NTP

```
# service ntpd restart
ntpd □□□□:                                                [  OK  ]
ntpd □□□□:                                                [  OK  ]
```

ntpq

```
[root@client ~]# ntpq -p
     remote           refid      st t when poll reach   delay   offset  ji
==========================================================================
*server          157.7.154.29     3 u    2   64    1    0.152    0.108   0
```

Linux POSIX POSIX Portable Operating System Interface for UNIX IEEE UNIX OS ID uid / ID gid

UID GID

ID uid User Identifier) Linux Linux uid
uid 0 65535 0 ID root

ID gid: Group Identifier Linux
1
gid 0 65535

1
useradd grooupadd

sato suzuki suzuki wheel eigyou

```
# id sato
uid=500(sato) gid=500(sato) □□□□□□=500(sato)
# id suzuki
uid=501(suzuki) gid=501(suzuki) □□□□□□=501(suzuki),10(wheel),5000(eigyou)
```

sato suzuki

Linux

Linux X Window System root
su

A sato

```
[root@server ~]# su - sato
[sato@server ~]$ id
uid=500(sato) gid=500(sato) □□□□□□=500(sato) context=unconfined_u:unconfin
```

B suzuki

```
[root@server ~]# su - suzuki
[suzuki@server ~]$ id
uid=501(suzuki) gid=501(suzuki) □□□□□□=501(suzuki),10(wheel),5000(eigyou)
```

Linux root

sato vi vim /tmp
suzuki kill

sato vi /tmp/sato

```
[sato@server ~]$ vi /tmp/sato
```

suzuki vim

```
[suzuki@server ~]$ ps aux | grep vim
sato      6456  0.1  0.3 148100  3692 pts/2    S+   19:46   0:00 vim /tmp/
suzuki    6462  0.0  0.0 107464   916 pts/3    S+   19:46   0:00 grep vim
```

suzuki sato vim kill
ID ps 2

```
[suzuki@server ~]$ kill 6456
-bash: kill: (6456) - □□□□□□□□□□□□
```

sato :q! vim

sato /tmp/sato

sato /tmp/sato

```
[sato@server ~]$ ls -l /tmp/sato
-rw-rw-r--. 1 sato sato 5 12□  9 17:51 2014 /tmp/sato
```

suzuki cat /tmp/sato

```
[suzuki@server ~]$ cat /tmp/sato
sato
```

suzuki /tmp/sato

```
[suzuki@server ~]$ echo "suzuki" >> /tmp/sato
-bash: /tmp/sato: □□□□□□□□
```

umask

umask
umask

```
[sato@server ~]$ umask
0002
```

umask 8

	r	w	x
8	4	2	1

umask

(eXecute) 0666(rw-rw-rw-) umask

umask 0002 w
-rw-rw-r-- 0664

```
[sato@server ~]$ umask
0002
[sato@server ~]$ touch testfile
[sato@server ~]$ ls -l testfile
-rw-rw-r--. 1 sato sato 0  1□ 14 19:51 2015 testfile
```

umask

(eXecute) 0777(rwxrwxrwx) umask 1

umask 0002 w
-rwxrwxr-x 0775

```
[sato@server ~]$ umask
0002
[sato@server ~]$ mkdir testdir
```

```
[sato@server ~]$ ls -ld testdir
drwxrwxr-x. 2 sato sato 4096  1□ 14 19:52 2015 testdir
```

umask　4

3
umask　4　setUID/setGID/
setUID
setUID　umask
3
umask　022　3　umask　0022

```
[sato@server ~]$ umask 022
[sato@server ~]$ umask
0022
```

umask

umask　umask　umask
umask　0022　644(-rw-r--r--)

```
[sato@server ~]$ umask 0022
[sato@server ~]$ touch umasktest
[sato@server ~]$ ls -l umasktest
-rw-r--r--. 1 sato sato 0  1□ 14 19:53 2015 umasktest
```

root　umask　umask

umask　0002　root　umask　0022

```
[root@server ~]# umask
0022
```

bash　/etc/bashrc　umask
uid　200　uid　gid　umask　0002
002　3　0022

/etc/profile

```
# cat /etc/bashrc
□□□
    # By default, we want umask to get set. This sets it for non-login she
    # Current threshold for system reserved uid/gids is 200
    # You could check uidgid reservation validity in
    # /usr/share/doc/setup-*/uidgid file
    if [ $UID -gt 199 ] && [ "`id -gn`" = "`id -un`" ]; then
       umask 002
```

```
    else
       umask 022
    fi
□□□
```

uid　gid　　useradd
　　uid　gid
　uid　gid　　useradd

setUID

setUID　　setUID
　　ls　　s

setUID　　passwd
root　　/etc/shadow　　passwd
　　root　　setUID　　passwd
　root　　/etc/shadow

　　setUID

　　passwd　　ps

setUID

```
[sato@server ~]$ ls -l /usr/bin/passwd
-rwsr-xr-x. 1 root root 30768  2□ 22 20:48 2012 /usr/bin/passwd
```

passwd　　Ctrl+Z　　Enter

```
[sato@server ~]$ passwd
□□□□ sato □□□□□□□□□□
sato □□□□□□□□□□□
□□□UNIX□□□□□: □Ctrl+Z□□□□□□□Enter□□□□□
[1]+  □□                  passwd
```

ps　　passwd　　root

```
[sato@server ~]$ ps aux | grep passwd
root     15052  0.0  0.2 164012  2068 pts/1    T    10:47   0:00 passwd
sato     15178  0.0  0.0 107464   916 pts/1    S+   10:48   0:00 grep pass
```

fg　　passwd　　Ctrl+C

```
[sato@server ~]$ fg
passwd
```

```
※^C ←Ctrl+C□□□□□
[sato@server ~]$
```

setGID

setGID setGID
s

setGID write slocate

```
$ ls -l /usr/bin/write
-rwxr-sr-x  1 root tty 10124 2□ 18□  2011 /usr/bin/write
$ ls -l /usr/bin/slocate
-rwxr-sr-x  1 root slocate 38516 11□ 17□  2007 /usr/bin/slocate
```

write write
ps

2
write Ctrl+Z

```
[sato@server ~]$ write suzuki
※^Z ←Ctrl+Z□□□□□
[1]+  □□                write suzuki
```

ps

```
[sato@server ~]$ ps a -eo "%p %u %g %G %y %c" | grep write
23400 sato     sato     ※tty※      pts/1    write
```

ID %p %u %g %G
%y %c sato setGID tty

tty Tele-TYpewriter write
setGID tty

/tmp /tmp

/tmp 777 rwxrwxrwx
/tmp

ls t

```
[sato@server ~]$ ls -ld /tmp
drwxrwxrwt. 16 root root 4096  1□ 14 20:26 2015 /tmp
```

sato /tmp/sbittest 666

```
[sato@server ~]$ touch /tmp/sbittest
[sato@server ~]$ chmod 666 /tmp/sbittest
[sato@server ~]$ ls -l /tmp/sbittest
-rw-rw-rw-. 1 sato sato 0  1□ 14 20:28 2015 /tmp/sbittest
```

suzuki /tmp/sbittest

```
[suzuki@server ~]$ echo "suzuki" >> /tmp/sbittest
[suzuki@server ~]$ cat /tmp/sbittest
suzuki
```

suzuki /tmp/sbittest

```
[suzuki@server ~]$ rm /tmp/sbittest
rm: cannot remove `/tmp/sbittest': □□□□□□□□□□□□
```

sato /tmp/sbittest

```
[sato@server ~]$ rm /tmp/sbittest
```

POSIX ACL

ACL(Access Control List POSIX ACL POSIX ACL) Linux 2.6 Linux
Linux OS Windows ACL
Linux Windows Samba
ACL

ACL

ACL
ext3 ext4 XFS

mount acl
CentOS 6 ext4 ACL acl

ACL ls "."

"." ACL ACL "+"

ACL

ACL getfacl ACL setfacl ACL

sato /tmp/acltest

```
[sato@server ~]$ touch /tmp/acltest
```

getfacl /tmp/acltest ACL

```
[sato@server ~]$ getfacl /tmp/acltest
getfacl: Removing leading '/' from absolute path names
# file: tmp/acltest
# owner: sato
# group: sato
user::rw-
group::r--
other::r--
```

suzuki /tmp/acltest

```
[suzuki@server ~]$ echo "suzuki" >> /tmp/acltest
-bash: /var/tmp/acltest: □□□□□□□□
```

sato setfacl suzuki /tmp/acltest ACL

```
[sato@server ~]$ setfacl -m u:suzuki:rw /tmp/acltest
[sato@server ~]$ getfacl /tmp/acltest
getfacl: Removing leading '/' from absolute path names
# file: tmp/acltest
# owner: sato
# group: sato
user::rw-
※user:suzuki:rw- □□□suzuki□□□□ACL□□□□□□□□
group::rw-
mask::rw-
other::r--
```

suzuki /tmp/acltest ACL

```
[suzuki@server ~]$ echo "suzuki" >> /tmp/acltest
[suzuki@server ~]$ cat /tmp/acltest
suzuki
```

sato　setfacl　　suzuki　/tmp/acltest　　ACL

```
[sato@server ~]$ setfacl -x u:suzuki /tmp/acltest
[sato@server ~]$ getfacl /tmp/acltest
getfacl: Removing leading '/' from absolute path names
# file: tmp/acltest
# owner: sato
# group: sato
user::rw-
group::rw-
mask::rw-
other::r--
```

suzuki　/tmp/acltest　　ACL

```
[suzuki@server ~]$ echo "suzuki" >> /tmp/acltest
-bash: /var/tmp/acltest: □□□□□□□□
```

Samba　ACL

Samba　Windows　　Windows
Linux　　ACL

/home/sato　　samba_ACL_test　　ACL

Samba

Samba

```
# yum install samba
```

Samba　　/etc/samba/smb.conf　workgroup
Windows　　Windows
　　WORKGROUP

```
vi /etc/samba/smb.conf

        workgroup = ※WORKGROUP ←□□□□□□□□□□□□
```

Samba　　smb　　nmb

```
# service smb start
SMB □□□□□□□□:                                          [  OK  ]
# service nmb start
NMB □□□□□□□□:                                          [  OK  ]
```

iptables

iptables system-config-firewall-tui Samba /etc/sysconfig/iptables 4 iptables reload Samba SMB/CIFS TCP UDP 2

```
-A INPUT -m state --state NEW -m udp -p udp --dport 137 -j ACCEPT
-A INPUT -m state --state NEW -m udp -p udp --dport 138 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 139 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 445 -j ACCEPT
```

SELinux

SELinux SELinux setsebool Samba SELinux

```
# setsebool -P samba_enable_home_dirs on
```

Samba

smbpasswd Samba Linux sato Windows

```
# smbpasswd -a sato
New SMB password: ※□□□□□□□□
Retype new SMB password: ※□□□□□□□□□
Added user sato.
```

Windows Samba

Windows Samba

1. Samba

   Samba
   Samba

→ \server\ \192.168.0.10

2

2.

3

3.

sato Samba

4

4.

samba_acl_test
samba_acl_test

samba_acl_test

5

5.

Windows samba_acl_test

6

6.

Everyone 5 OK
OK

Linux ACL

1. sato samba_acl_test ACL

```
[sato@server ~]$ getfacl samba_acl_test/
# file: samba_acl_test/
# owner: sato
# group: sato
```

```
user::rwx
group::r-x
other::r-x
```

2

2. setfacl samba_acl_test
   ACL

```
[sato@server ~]$ setfacl -m o::rwx samba_acl_test
[sato@server ~]$ getfacl samba_acl_test/
# file: samba_acl_test/
# owner: sato
# group: sato
user::rwx
group::r-x
other::r※w※x ※←□□□□□□□□□□□□□□
```

3

3. Windows

Windows Everyone

SELinux

SELinux Linux 2.6 root
MAC Mandatory Access Control

SELinux SELinux
Linux

SELinux

SELinux Linux contexts
subject object

SELinux
Linux

SELinux

SELinux getenforce

```
[root@server ~]# getenforce
Enforcing
```

getenforce

Enforcing SELinux
Permissive SELinux
Disabled SELinux

SELinux setenforce /etc/selinux/config

setenforce SELinux

setenforce SELinux root

Enforcing Permissive SELinux
Disabled

```
setenforce [ Enforcing | Permissive | 1 | 0 ]
```

SELinux
Permissive SELinux
SELinux
SELinux Permissive SELinux

```
# setenforce permissive
# getenforce
Permissive
```

SELinux

SELinux SELinux /etc/selinux/config

/etc/selinux/config SELINUX disabled

```
# vi /etc/selinux/config

※#※SELINUX=enforcing ※←□□□#□□□
※SELINUX=disabled ←□□□□□
```

```
# reboot
```

getenforce SELinux Disabled

```
# getenforce
Disabled
```

/etc/selinux/config SELINUX enforcing

```
# vi /etc/selinux/config

SELINUX=enforcing ※←□□□#□□□
※#※SELINUX=disabled ※←□□□#□□□
```

```
# reboot
```

getenforce SELinux Enforcing

```
# getenforce
Enforcing
```

4

- (user)
- (role)
- (type)
- MLS Multi Level Security

```
□□□:□□□:□□□:MLS□□□
```

SELinux

Apache Web

httpd httpd_t

SELinux -Z

ls -lZ

Apache Web httpd

```
# ls -lZ /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 error
drwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0 html
drwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0 icons
```

/var/www/html /var/www/icons Web
httpd_sys_content_t /var/www/html

/var/www/html index.html
index.html httpd_sys_content_t

```
# touch /var/www/html/index.html
# ls -lZ /var/www/html/index.html
-rw-r--r--. root root unconfined_u:object_r:※httpd_sys_content_t※:s0 /var/
```

ps axZ

httpd httpd_t

```
[root@server ~]# service httpd start
httpd □□□□:                                                [  OK  ]
[root@server ~]# ps axZ | grep httpd
unconfined_u:system_r:httpd_t:s0 27104 ?       Ss     0:00 /usr/sbin/httpd
unconfined_u:system_r:httpd_t:s0 27106 ?       S      0:00 /usr/sbin/httpd
□□□
```

SELinux httpd httpd_t httpd_sys_content_t
read

Boolean SELinux

SELinux SELinux
SELinux

Boolean Boolean
CentOS 6 200

Linux

Apache Web (httpd)

getsebool Boolean Boolean
grep httpd

```
# getsebool -a | grep httpd
allow_httpd_anon_write --> off
allow_httpd_mod_auth_ntlm_winbind --> off
□□□
httpd_enable_homedirs --> off
□□□
```

httpd_enable_homedirs Boolean Boolean Apache Web

public_html Web

Apache Web /etc/httpd/conf/httpd.conf UserDir

```
# vi /etc/httpd/conf/httpd.conf

□□□
<IfModule mod_userdir.c>
    #
    # UserDir is disabled by default since it can confirm the presence
    # of a username on the system (depending on home directory
    # permissions).
    #
    ※#※UserDir disabled ※←□□□#□□□

    #
    # To enable requests to /~user/ to serve the user's public_html
    # directory, remove the "UserDir disabled" line above, and uncomment
    # the following line instead:
    #
    UserDir public_html ※←□□□#□□□
□□□
```

httpd

```
# service httpd restart
httpd □□□□:                                                [  OK  ]
httpd □□□□:                                                [  OK  ]
```

sato public_html

```
$ pwd
/home/sato
$ mkdir public_html
```

/home/sato /home/sato/public_html 711

```
chmod 711 /home/sato
chmod 711 /home/sato/public_html/
```

public_html index.html

```
[sato@server ~]$ echo "SELinux test" > /home/sato/public_html/index.html
```

http://192.168.0.10/~sato/ SELinux Forbidden

Forbidden
Forbidden

root /var/log/audit/audit.log httpd(httpd_t) (user_home_dir_t)

```
[root@server ~]# tail /var/log/audit/audit.log
□□□
type=AVC msg=audit(1421241819.317:804): avc:  ※denied  { search }※ for  p
type=SYSCALL msg=audit(1421241819.317:804): arch=c000003e syscall=4 succes
type=AVC msg=audit(1421241819.317:805): avc:  ※denied  { getattr }※ for  p
type=SYSCALL msg=audit(1421241819.317:805): arch=c000003e syscall=6 succes
```

setsebool Boolean httpd_enable_homedirs

```
[root@server ~]# getsebool httpd_enable_homedirs
httpd_enable_homedirs --> off
[root@server ~]# setsebool httpd_enable_homedirs on
[root@server ~]# getsebool httpd_enable_homedirs
httpd_enable_homedirs --> on
```

http://192.168.0.10/~sato/ Boolean

LVM

LVM Logical Volume Manager

LVM

HDD HDD

Linux LVM
CentOS LVM

LVM

LVM PV: Physical Volume VG: Volume Group
LV: Logical Volume 3

PV

(PV)
PV
PV

PV 8E

Linux /dev/sdb LVM
fdisk PV

```
# fdisk /dev/sdb
□□□□□□□□□ DOS □□□□□□□□□Sun, SGI □ OSF □□□□□□□□□
□□□□□□□□
□□□

□□□□ (m □□□□): □n ←□□□□□□□□□□□□□n□□□
□□□□□□□□□□
   e   □□
   p   □□□□□□□□□□ (1-4)
※p ←□□□□□□□□□□□p□□□
□□□□□□□□□□ (1-4): □1 ←□□□□□□□□□□1□□□
□□ □□□□□ (1-8354, □□□ 1): □1 ←□□□□□□□□□□1□□□
Last □□□□, +□□□□□ or +size{K,M,G} (1-8354, □□□ 8354): ※+2G ←□□□□□+2GB□□□

□□□□ (m □□□□): □n ←□□□□□□□□□□□□□n□□□
□□□□□□□□□□
   e   □□
   p   □□□□□□□□□□ (1-4)
※p ←□□□□□□□□□□□p□□□
□□□□□□□□□□ (1-4): □2 ←□□□□□□□□□□2□□□
□□ □□□□□ (263-8354, □□□ 263): □Enter□□□□□
□□□ 263 □□□□□
Last □□□□, +□□□□□ or +size{K,M,G} (263-8354, □□□ 8354): ※+2G ←□□□□□+2GB□□□

□□□□ (m □□□□): □t ←□□□□□□□□□□□□□t□□□
□□□□□□□□□□ (1-4): □1 ←□□□□□□□□□□1□□□
16□□□□□ (L □□□□□□□□□□□□□□): □8e ←LVM□□8e□□□
□□□□□□□□□□□□ 1 □□ 8e (Linux LVM) □□□□□□□

□□□□ (m □□□□): □t ←□□□□□□□□□□□□□t□□□
□□□□□□□□□□ (1-4): □2 ←□□□□□□□□□□2□□□
16□□□□□ (L □□□□□□□□□□□□□□): □8e ←LVM□□8e□□□
□□□□□□□□□□□□ 2 □□ 8e (Linux LVM) □□□□□□□
```

□□□□ (m □□□□): □w ←□□□□□□□□□□□□□□□w□□□
□□□□□□□□□□□□□□□□□□□□□

ioctl() □□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□□□□□□□□□□□□□□

VG

(VG) 1 PV

vgcreate

```
vgcreate □□□□□□□ PV□□□□□□ [PV□□□□□□ ...]
```

PV /dev/sdb1 Volume00
vgcreate

```
# vgcreate Volume00 /dev/sdb1
  Physical volume "/dev/sdb1" successfully created
  Volume group "Volume00" successfully created
```

vgscan

```
# vgscan
  Reading all physical volumes.  This may take a while...
  Found volume group "Volume00" using metadata type lvm2
  Found volume group "vg_server" using metadata type lvm2
```

LV

LV VG Linux

lvcreate

```
lvcreate -L □□□□ -n □□□□□□□□□ □□□□□□□□□□□□
```

Volume00 1GB LogVol01
lvcreate

```
# lvcreate -L 1024M -n LogVol01 Volume00
```

/dev/□□□□□□□□□□/□□□□□□□□

/dev/Volume00/LogVol01　ext4　mkfs

```
# mkfs -t ext4 /dev/Volume00/LogVol01
mke2fs 1.41.12 (17-May-2010)
Discarding device blocks: done
Filesystem label=
OS type: Linux
□□□
This filesystem will be automatically checked every 33 mounts or
180 days, whichever comes first.  Use tune2fs -c or -i to override.
```

mount　/dev/Volume00/LogVol01

```
# mkdir /mnt/LVMtest
# mount -t ext4 /dev/Volume00/LogVol01 /mnt/LVMtest/
# mount /mnt/LVMtest/
mount: /dev/mapper/Volume00-LogVol01 □ □□□□□□ /mnt/LVMtest □□□□□□
mount: mtab □□□□□/dev/mapper/Volume00-LogVol01 □ /mnt/LVMtest □□□□□□□□
```

Volume00　/dev/sdb2

vgextend　/dev/sdb2　Volume00

```
# vgextend Volume00 /dev/sdb2
  Physical volume "/dev/sdb2" successfully created
  Volume group "Volume00" successfully extended
```

vgdisplay　Volume00　PV　Physical volume　2　/dev/sdb2

```
# vgdisplay Volume00
  --- Volume group ---
  VG Name               Volume00
  System ID
  Format                lvm2
  Metadata Areas        2
  Metadata Sequence No  3
  VG Access             read/write
  VG Status             resizable
  MAX LV                0
  Cur LV                1
  Open LV               1
  Max PV                0
  Cur PV                ※2
  Act PV                ※2
```

```
  VG Size               4.01 GiB
  PE Size               4.00 MiB
  Total PE              1026
  Alloc PE / Size       256 / 1.00 GiB
  Free  PE / Size       770 / 3.01 GiB
  VG UUID               yTTwWd-G5tb-FzNb-Ow0L-ebvr-1n9I-ikLWo2
```

LVM LVM ext4

df 1GB

```
# df /mnt/LVMtest/
Filesystem           1K-blocks  Used Available Use% Mounted on
/dev/mapper/Volume00-LogVol01
                        999320  1284    945608   1% /mnt/LVMtest
```

lvextend LogVol01 2G

```
# lvextend -L 2G /dev/Volume00/LogVol01
 Size of logical volume Volume00/LogVol01 changed from 1.00 GiB (256 exten
  Logical volume LogVol01 successfully resized
```

resize2fs

```
# resize2fs /dev/Volume00/LogVol01
resize2fs 1.41.12 (17-May-2010)
Filesystem at /dev/Volume00/LogVol01 is mounted on /mnt/LVMtest; on-line r
old desc_blocks = 1, new_desc_blocks = 1
Performing an on-line resize of /dev/Volume00/LogVol01 to 524288 (4k) bloc
The filesystem on /dev/Volume00/LogVol01 is now 524288 blocks long.
```

df 2GB

```
# df /mnt/LVMtest/
Filesystem           1K-blocks  Used Available Use% Mounted on
/dev/mapper/Volume00-LogVol01
                       2031440  1536   1925060   1% /mnt/LVMtest
```

umount /mnt/LVMtest

```
# umount /mnt/LVMtest/
```

/dev/Volume00/LogVol01 fsck
-f

```
# fsck -f /dev/Volume00/LogVol01
fsck from util-linux-ng 2.17.2
e2fsck 1.41.12 (17-May-2010)
Pass 1: Checking inodes, blocks, and sizes
Pass 2: Checking directory structure
Pass 3: Checking directory connectivity
Pass 4: Checking reference counts
Pass 5: Checking group summary information
/dev/mapper/Volume00-LogVol01: 11/131072 files (0.0% non-contiguous), 1681
```

resize2fs 1GB

```
# resize2fs /dev/Volume00/LogVol01 1G
resize2fs 1.41.12 (17-May-2010)
Resizing the filesystem on /dev/Volume00/LogVol01 to 262144 (4k) blocks.
The filesystem on /dev/Volume00/LogVol01 is now 262144 blocks long.
```

lvreduce /dev/Volume00/LogVol01

```
# lvreduce -L 1G /dev/Volume00/LogVol01
  WARNING: Reducing active logical volume to 1.00 GiB
  THIS MAY DESTROY YOUR DATA (filesystem etc.)
Do you really want to reduce LogVol01? [y/n]: ※y ←y□□□
  Size of logical volume Volume00/LogVol01 changed from 2.00 GiB (512 exte
  Logical volume LogVol01 successfully resized
```

/mnt/LVMtest

```
# mount -t ext4 /dev/Volume00/LogVol01 /mnt/LVMtest/
# df /mnt/LVMtest/
Filesystem           1K-blocks  Used Available Use% Mounted on
/dev/mapper/Volume00-LogVol01
                        999320  1284    945616   1% /mnt/LVMtest
```

CD　DVD

Linux

- dd
- dump
- tar
- rsync

dd

dd

dd

- MBR(Master Boot Record)
- i　atime　ctime
-

dd

-
-

dump

dump

-
-
-
- i　atime　ctime

-
-

dump

-
-
-
- ext2/3/4 XFS xfsdump

tar

Tape Archiver

tar

-
-
-
-

tar

-
- i i

rsync

remote sync

rsync

-
- tar
-

rsync

- dd dump
- i i

/mnt/backup_test /dev/sdb1 /mnt/restore_test /dev/sdc1

2 /dev/sdb
/dev/sdc OS

2 1 2
/dev/sdb1 /dev/sdb2

LVM /dev/sdb
fdisk

fdisk /dev/sdb /dev/sdb1 mkfs.ext4 ext4
/mnt/backup_test LVM
LVM

```
# fdisk /dev/sdb
※□□□□□□□□□□
# mkfs.ext4 /dev/sdb1
# mkdir /mnt/backup_test
# mount -t ext4 /dev/sdb1 /mnt/backup_test/
```

/mnt/backup_test

```
# mkdir /mnt/backup_test/test_dir
# touch /mnt/backup_test/test_dir/test_file
```

dd

dd /dev/sdb

/dev/sdc dd /dev/sdb /dev/sdc

```
#  dd if=/dev/sdb of=/dev/sdc
208896+0 records in
208896+0 records out
106954752 bytes (107 MB) copied, 1.29132 s, 82.8 MB/s
```

fdisk /dev/sdc1 /dev/sdc
OS OS

```
# reboot
※□□□□□□□□□□□
```

```
# fdisk /dev/sdc
□□□
□□□□ (m □□□□): □p ←□□□□□□□□□□□□p□□□

□□□□ /dev/sdc: 106 MB, 106954752 □□□
□□□ 255, □□□ 63, □□□□ 13
Units = □□□□□ of 16065 * 512 = 8225280 □□□
□□□□□□ (□□ / □□): 512 □□□ / 4096 □□□
I/O size (minimum/optimal): 4096 bytes / 4096 bytes
□□□□□□□: 0x43b56949

□□□□ □□□      □□        □□     □□□□   Id  □□□□
/dev/sdc1               1          13      104391   83  Linux
Partition 1 does not start on physical sector boundary.

□□□□ (m □□□□): □q ←□□□q□□□
```

/dev/sdc1 /mnt/restore_test /mnt/backup_test

```
# mount /dev/sdc1 /mnt/restore_test
# cd /mnt/restore_test
# ls -l
□□ 14
drwx------. 2 root root 12288 12□ 22 13:16 2014 lost+found
drwxr-xr-x. 3 root root  1024 12□ 22 13:16 2014 test_dir
[root@server restore_test]# ls -l test_dir/
□□ 0
-rw-r--r--. 1 root root 0  12□ 22 13:16 2014 test_file
```

dump

dump
/etc/fstab

/boot /boot /
/boot
/boot dump

CentOS 6 dump dump

```
# yum install dump
```

dump /etc/fstab /etc/fstab 5 2
1 dump /boot
dump /proc /sys

```
# vi /etc/fstab

/dev/mapper/vg_cent65-lv_root /                       ext4    defaults
1 1
UUID=fe4d3f56-a570-44b4-a863-418b789b42bc /boot                   ext4
defaults        ※1※ 2
/dev/mapper/vg_cent65-lv_swap swap                    swap    defaults
0 0
tmpfs                   /dev/shm                tmpfs   defaults        0 
devpts                  /dev/pts                devpts  gid=5,mode=620  0 
sysfs                   /sys                    sysfs   defaults        0 
proc                    /proc                   proc    defaults        0 
```

dump /boot
dump dd

-

-0 0 0
-u /etc/dumpdates
-a
-n operator
-f

```
# dump -0uan -f - /boot | dd of=/tmp/boot.dump
  DUMP: No group entry for operator.
  DUMP: Date of this level 0 dump: Thu Jan 15 00:07:19 2015
  DUMP: Dumping /dev/sda1 (/boot) to standard output
□□□
  DUMP: Date this dump completed:  Thu Jan 15 00:07:20 2015
  DUMP: Average transfer rate: 26570 kB/s
  DUMP: DUMP IS DONE
53140+0 records in
53140+0 records out
27207680 bytes (27 MB) copied, 0.202273 s, 135 MB/s

# ls -l /tmp/boot.dump
-rw-r--r--. 1 root root 27207680  1□ 15 00:07 2015 /tmp/boot.dump
```

restore /tmp/restore_test -r
-f -
dump cat
restore

```
# mkdir /tmp/restore_test
# cd /tmp/restore_test
# cat /tmp/boot.dump | restore -rf -
# ls
System.map-2.6.32-504.el6.x86_64  initramfs-2.6.32-504.el6.x86_64.img
config-2.6.32-504.el6.x86_64      lost+found
efi                               symvers-2.6.32-504.el6.x86_64.gz
grub                              vmlinuz-2.6.32-504.el6.x86_64
```

/tmp/restore_test

```
# rm -rf /tmp/restore_test/*
```

tar

tar
Linux

/boot
/tmp/boot_backup.tar tar -c

```
# tar -cvf /tmp/boot_backup.tar /boot
tar: □□□□□□□□□ `/' □□□□□□□
/boot/
/boot/grub/
□□□
/boot/System.map-2.6.32-504.el6.x86_64
/boot/.vmlinuz-2.6.32-504.el6.x86_64.hmac

# ls -l /tmp/boot_backup.tar
-rw-r--r--. 1 root root 26982400  1□ 15 00:15 2015 /tmp/boot_backup.tar
```

/tmp/restore_test tar
-x

```
# cd /tmp/restore_test
# tar -xvf /tmp/boot_backup.tar
boot/
boot/grub/
□□□
boot/System.map-2.6.32-504.el6.x86_64
boot/.vmlinuz-2.6.32-504.el6.x86_64.hmac
# ls -l
□□ 4
dr-xr-xr-x. 5 root root 4096  1□  6 06:20 2015 boot
# ls boot/
System.map-2.6.32-504.el6.x86_64  initramfs-2.6.32-504.el6.x86_64.img
config-2.6.32-504.el6.x86_64      lost+found
```

```
efi                                     symvers-2.6.32-504.el6.x86_64.gz
grub                                    vmlinuz-2.6.32-504.el6.x86_64
```

/tmp/restore_test

```
# rm -rf /tmp/restore_test/*
```

rsync

rsync

/boot

rsync /boot /tmp/restore_test

```
# rsync -av /boot /tmp/restore_test
sending incremental file list
boot/
boot/.vmlinuz-2.6.32-504.el6.x86_64.hmac
□□□
boot/grub/xfs_stage1_5
boot/lost+found/

sent 26964672 bytes  received 457 bytes  53930258.00 bytes/sec
total size is 26959690  speedup is 1.00
```

/tmp/restore_test

```
# ls -l /tmp/restore_test
□□ 4
dr-xr-xr-x. 5 root root 4096  1□  6 06:20 2015 boot
# ls -l /tmp/restore_test/boot
□□ 25848
-rw-r--r--. 1 root root  2544748 10□ 15 13:54 2014 System.map-2.6.32-504.el
-rw-r--r--. 1 root root   106308 10□ 15 13:54 2014 config-2.6.32-504.el6.x
□□□
-rw-r--r--. 1 root root   200191 10□ 15 13:55 2014 symvers-2.6.32-504.el6.
-rwxr-xr-x. 1 root root  4152336 10□ 15 13:54 2014 vmlinuz-2.6.32-504.el6.
```

/boot/rsync_test

```
# touch /boot/rsync_test
# ls -l /boot/rsync_test
-rw-r--r--. 1 root root 0  1□ 15 00:23 2015 /boot/rsync_test
```

rsync

```
# rsync -av /boot /tmp/restore_test
sending incremental file list
boot/
boot/rsync_test

sent 832 bytes  received 40 bytes  1744.00 bytes/sec
total size is 26959690  speedup is 30917.08



# ls -l /tmp/restore_test/boot/rsync_test
-rw-r--r--. 1 root root 0  1□ 15 00:23 2015 /tmp/restore_test/boot/rsync_t
```

tmp/restore_test

```
# rm -rf /tmp/restore_test/*
```

Linux Linux

Linux 1

Red Hat Enterprise Linux CentOS SUSE Linux RPM(Red Hat Package Manager)
Yum Yellowdog Updater Modified

Debian GNU/Linux Ubuntu Debian
deb APT Advanced Package Tool

CentOS 6 yum

Yum

RPM rpm

Yum yum

Yum

Yum RPM
RPM

/etc/yum.repos.d

```
# ls /etc/yum.repos.d
CentOS-Base.repo       CentOS-Media.repo  CentOS-fasttrack.repo
CentOS-Debuginfo.repo  CentOS-Vault.repo
```

CentOS-Base.repo

```
# cat /etc/yum.repos.d/CentOS-Base.repo
□□□
```

```
[base]
name=CentOS-$releasever - Base
mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearc
#baseurl=http://mirror.centos.org/centos/$releasever/os/$basearch/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-6
□□□

#additional packages that extend functionality of existing packages
[centosplus]
name=CentOS-$releasever - Plus
mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearc
#baseurl=http://mirror.centos.org/centos/$releasever/centosplus/$basearch/
gpgcheck=1
enabled=0
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-6
□□□
```

mirrorlist mirror.centos.org

enabled 0 yum --enablerepo

yum HTTP PROXY yum /etc/yum.conf PROXY

proxy PROXY URL
proxy_username PROXY
proxy_password PROXY

DVD

yum

yum

```
yum install □□□□□□
```

```
yum remove □□□□□□
```

```
yum check-update
```

```
yum update [□□□□□□]
```

```
yum grouplist
```

```
yum groupinstall □□□□□□□□□□
```

```
yum groupremove □□□□□□□□□□
```

yum dump

Emacs

```
# yum grouplist
□□□□□□□□□□□:fastestmirror, refresh-packagekit, security
□□□□□□□□□□□□□□□□
Loading mirror speeds from cached hostfile
 * base: ftp.nara.wide.ad.jp
 * extras: ftp.nara.wide.ad.jp
 * updates: ftp.nara.wide.ad.jp
□□□□□□□□□□□□□:
   CIFS □□□□□□□□□
   Java □□□□□□□□□
□□□
□□□□□□□□□□
   Eclipse
   ※Emacs
□□□
```

Emacs

```
# yum groupinstall Emacs
□□□□□□□□□□□:fastestmirror, refresh-packagekit, security
□□□□□□□□□□□□□□□□
Loading mirror speeds from cached hostfile
 * base: ftp.riken.jp
 * extras: ftp.riken.jp
 * updates: ftp.riken.jp
□□□□□□□□□□□□□□
--> □□□□□□□□□□□□□□□□□□□□□□□□
---> Package emacs.x86_64 1:23.1-25.el6 will be □□□□□□□
--> □□□□□□□□□□□□□□: emacs-common = 1:23.1-25.el6 □□□□□□□: 1:emacs-23.1-25.el6
□□□

□□□□□□□□□□□

=============================================================================
 □□□□□□                □□□□□□□□
                                            □□□□□□            □□□□□□□

=============================================================================
□□□□□□□□□□□□□:
 emacs                    x86_64        1:23.1-25.el6         base        2
□□□□□□□□□□□□□□□□□□□□□□□:
 emacs-common             x86_64        1:23.1-25.el6         base
 libXaw                   x86_64        1.0.11-2.el6          base
 libXpm                   x86_64        3.5.10-2.el6          base
 libotf                   x86_64        0.9.9-3.1.el6         base
 m17n-db-datafiles        noarch        1.5.5-1.1.el6         base        1

□□□□□□□□□□□□□
```

```
================================================================================
□□□□□□□         6 □□□□□□

□□□□□□□□□□□: 21 M
□□□□□□□□□□□: 73 M
□□□□□□□□□? [y/N]※y ←y□□□
□□□□□□□□□□□□□□□□□□□:
(1/6): emacs-23.1-25.el6.x86_64.rpm                       | 2.2 MB     00:0
□□□

□□□□□□□:
  emacs.x86_64 1:23.1-25.el6

□□□□□□□□□□□□□□□□□□□:
  emacs-common.x86_64 1:23.1-25.el6            libXaw.x86_64 0:1.0.11-2.el
  libXpm.x86_64 0:3.5.10-2.el6                 libotf.x86_64 0:0.9.9-3.1.e
  m17n-db-datafiles.noarch 0:1.5.5-1.1.el6

□□□□□□□!
```

Emacs

```
# emacs
```

Emacs Ctrl+X Ctrl+C

yum Locale LANG
yum groupinstall

yum LANG=C
LANG
yum

```
# LANG=C yum grouplist
□□□
Installed Groups:
   Additional Development
   Base
   CIFS file server
□□□
```

"

Development tools

```
# yum groupinstall "Development tools"
```

DVD

yum DVD

/etc/yum.repos.d/CentOS-Media.repo

```
# cat /etc/yum.repos.d/CentOS-Media.repo
# CentOS-Media.repo
#
#  This repo can be used with mounted DVD media, verify the mount point fo
#  CentOS-6.  You can use this repo and yum to install items directly off
#  DVD ISO that we release.
#
# To use this repo, put in your DVD and use it with the other repos too:
#  yum --enablerepo=c6-media [command]
#
# or for ONLY the media repo, do this:
#
#  yum --disablerepo=\* --enablerepo=c6-media [command]

[c6-media]
name=CentOS-$releasever - Media
baseurl=file:///media/CentOS/
        file:///media/cdrom/
        file:///media/cdrecorder/
gpgcheck=1
enabled=0
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-6
```

DVD /media/CentOS yum

DVD

1. CentOS root
2. DVD DVD ISO DVD
3.
4. mount DVD /media/CentOS_6.6_Final

```
# mount
□□□
/dev/sr0 on /media/CentOS_6.6_Final type iso9660 (ro,nosuid,nodev,uhelper=
```

5

1. /media/CentOS

```
# ln -s /media/CentOS_6.6_Final/ /media/CentOS
# ls -l /media
□□ 4
lrwxrwxrwx. 1 root root   24  1□ 15 02:47 2015 CentOS -> /media/CentOS_6.6
dr-xr-xr-x. 7 root root 4096 10□ 24 23:17 2014 CentOS_6.6_Final
```

1. yum --disablerepo --enablerepo c6-media

```
# yum --disablerepo=\* --enablerepo=c6-media grouplist
```

stress

stress stress CentOS 6 RPMforge yum

RPMforge
rpmforge-release

```
http://pkgs.repoforge.org/rpmforge-release/
```

64 CentOS 6

```
http://pkgs.repoforge.org/rpmforge-release/rpmforge-release-0.5.3-1.el6.rf
```

wget

```
# wget http://pkgs.repoforge.org/rpmforge-release/rpmforge-release-0.5.3-1
□□□

2014-12-24 11:19:30 (19.2 KB/s) - `rpmforge-release-0.5.3-1.el6.rf.x86_64.
```

rpm rpmforge-release

```
# ls -l rpmforge-release-0.5.3-1.el6.rf.x86_64.rpm
-rw-r--r--. 1 root root 12640  3□ 21 00:59 2013 rpmforge-release-0.5.3-1.e
# rpm -ivh rpmforge-release-0.5.3-1.el6.rf.x86_64.rpm
```

yum stress

```
# yum install stress
```

RPM

URL RPM

```
http://pkgs.repoforge.org/stress/
http://pkgs.repoforge.org/stress/stress-1.0.2-1.el6.rf.x86_64.rpm
```

top

top CPU

top

```
top - 03:11:49 up 16:28,  4 users,  load average: 0.08, 0.03, 0.01
Tasks: 188 total,   1 running, 187 sleeping,   0 stopped,   0 zombie
Cpu(s):  0.0%us,  0.0%sy,  0.0%ni, 99.8%id,  0.2%wa,  0.0%hi,  0.0%si,  0.
Mem:   1016372k total,   811796k used,   204576k free,    24736k buffers
Swap:  2064380k total,    41640k used,  2022740k free,   295652k cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
    1 root      20   0 19364 1304 1036 S  0.0  0.1   0:01.24 init
    2 root      20   0     0    0    0 S  0.0  0.0   0:00.03 kthreadd
    3 root      RT   0     0    0    0 S  0.0  0.0   0:00.03 migration/0
    4 root      20   0     0    0    0 S  0.0  0.0   0:00.09 ksoftirqd/0
    5 root      RT   0     0    0    0 S  0.0  0.0   0:00.00 stopper/0
    6 root      RT   0     0    0    0 S  0.0  0.0   0:00.08 watchdog/0
    7 root      RT   0     0    0    0 S  0.0  0.0   0:00.04 migration/1
    8 root      RT   0     0    0    0 S  0.0  0.0   0:00.00 stopper/1
    9 root      20   0     0    0    0 S  0.0  0.0   0:00.07 ksoftirqd/1
   10 root      RT   0     0    0    0 S  0.0  0.0   0:00.06 watchdog/1
   11 root      20   0     0    0    0 S  0.0  0.0   0:03.16 events/0
   12 root      20   0     0    0    0 S  0.0  0.0   0:02.79 events/1
   13 root      20   0     0    0    0 S  0.0  0.0   0:00.00 cgroup
   14 root      20   0     0    0    0 S  0.0  0.0   0:00.01 khelper
   15 root      20   0     0    0    0 S  0.0  0.0   0:00.00 netns
   16 root      20   0     0    0    0 S  0.0  0.0   0:00.00 async/mgr
   17 root      20   0     0    0    0 S  0.0  0.0   0:00.00 pm
```

5

1
2
3 CPU
4
5

stress top

stress
stress Enter

```
# stress --cpu 3 --io 4 --vm 2 --vm-bytes 128M &
[1] 9747
# stress: info: [9747] dispatching hogs: 3 cpu, 4 io, 2 vm, 0 hdd
※Enter□□□□□
#
```

top stress CPU

```
# top

top - 03:28:09 up 16:44,  3 users,  load average: 16.85, 14.44, 7.86
Tasks: 208 total,  13 running, 195 sleeping,   0 stopped,   0 zombie
Cpu(s): 55.5%us, 44.5%sy,  0.0%ni,  0.0%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0
Mem:   1016372k total,   718440k used,   297932k free,     1528k buffers
Swap:  2064380k total,   116124k used,  1948256k free,    39532k cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
 9692 sato      20   0  6516  176   92 R 17.0  0.0   2:02.20 stress
 9698 sato      20   0  6516  176   92 R 17.0  0.0   2:03.52 stress
 9748 root      20   0  6516  188  104 R 17.0  0.0   0:04.95 stress
 9750 root      20   0  134m 125m  184 R 17.0 12.6   0:05.11 stress
 9754 root      20   0  6516  188  104 R 17.0  0.0   0:05.11 stress
 9694 sato      20   0  134m  24m  168 R 16.6  2.4   2:00.22 stress
 9695 sato      20   0  6516  176   92 R 16.6  0.0   2:02.48 stress
 9751 root      20   0  6516  188  104 R 16.6  0.0   0:04.88 stress
 9697 sato      20   0  134m  59m  168 R 16.3  6.0   2:00.31 stress
 9753 root      20   0  134m  55m  184 R 16.3  5.6   0:04.87 stress
 9755 root      20   0  6516  184  100 D  4.7  0.0   0:01.50 stress
 9756 root      20   0  6516  184  100 D  4.7  0.0   0:01.49 stress
 9696 sato      20   0  6516  172   88 R  4.0  0.0   0:54.59 stress
 9699 sato      20   0  6516  172   88 D  4.0  0.0   0:59.14 stress
```

```
 9693 sato      20   0  6516  172   88 D  2.0  0.0   0:57.48 stress
 9700 sato      20   0  6516  172   88 D  2.0  0.0   0:59.43 stress
 9749 root      20   0  6516  184  100 D  2.0  0.0   0:01.60 stress
```

q　　top　　stress　　fg

```
# fg
stress --cpu 3 --io 4 --vm 2 --vm-bytes 128M
※^C ←Ctrl+C□□□□□
```

vmstat

vmstat　　CPU

vmstat　　CPU

```
# vmstat
procs -----------memory---------- ---swap-- -----io---- --system-- -----cpu
 r  b   swpd   free   buff  cache   si   so    bi    bo   in   cs us sy id
 8  0 116104 408536  58692  71292    0    1    10    11  251   66  2  2 97
```

r
b
swpd
free
buff
cache
si　1
so　1
bi　1
bo　1
in　1
cs　1
us　CPU
sy　CPU
id　CPU

vmstat
　Ctrl+C

```
# vmstat 5
procs -----------memory---------- ---swap-- -----io---- --system-- -----cpu
 r  b   swpd   free   buff  cache   si   so    bi    bo   in   cs us sy id
10  0 116104 261708  65040  79460    0    1    11    11  253   70  2  2 97
 9  0 116104 358068  65712  80356    0    0   189   242 5411 8564 42 58  0
 7  0 116104 301924  66184  81372    0    0   202   308 4610 7441 41 59  0
※^C Ctrl+C□□□□□□□
```

sysstat

Linux sysstat iostat sar

sysstat

```
# yum install sysstat
```

sysstat 10
cron

```
# cat /etc/cron.d/sysstat
# Run system activity accounting tool every 10 minutes
*/10 * * * * root /usr/lib64/sa/sa1 1 1
# 0 * * * * root /usr/lib64/sa/sa1 600 6 &
# Generate a daily summary of process accounting at 23:53
53 23 * * * root /usr/lib64/sa/sa2 -A
```

10 /usr/lib64/sa/sa1 /usr/lib64/sa/sadc
/var/log/sa/saDD DD 2
23:53 /usr/lib64/sa/sa2 sa1
/var/log/sa/sarDD DD 2
28 /etc/sysconfig/sysstat
HISTORY

sar

iostat

sysstat iostat CPU I/O
I/O

iostat iostat CPU
I/O

```
# iostat
Linux 2.6.32-504.el6.x86_64 (server.example.com)  2015□01□15□  _x86_64(2 C

avg-cpu:  %user   %nice %system %iowait  %steal   %idle
```

```
           1.72    0.00    1.95    0.03    0.00   96.30

Device:            tps   Blk_read/s   Blk_wrtn/s   Blk_read   Blk_wrtn
sda               1.89        44.06       117.04    2720068    7224884
scd0              0.01         0.18         0.00      11204          0
dm-0              6.51        41.98        42.57    2591466    2627904
dm-1              0.49         0.17        74.44      10552    4595040
dm-2              0.01         0.06         0.03       3522       1856
```

%user CPU

%nice nice CPU

%system CPU

%iowait I/O CPU

%steal CPU CPU

%idle CPU (I/O

tps 1 I/O

Blk_read/s 1 ( )

Blk_wrtn/s 1 ( )

Blk_read ( )

Blk_wrtn ( )

iostat -x KB

kB_read/s 1 (KB)

kB_wrtn/s 1 (KB)

kB_read (KB)

kB_wrtn (KB)

iostat 1 iostat

I/O

Ctrl+C

```
# iostat 5
Linux 2.6.32-504.el6.x86_64 (server.example.com)  2015□01□15□  _x86_64(2 C

avg-cpu:  %user   %nice %system %iowait  %steal   %idle
           1.76    0.00    2.01    0.03    0.00   96.20

Device:            tps   Blk_read/s   Blk_wrtn/s   Blk_read   Blk_wrtn
sda               1.89        44.02       116.93    2720092    7225892
scd0              0.01         0.18         0.00      11204          0
```

```
dm-0              6.51        41.94        42.54    2591474    2628888
dm-1              0.49         0.17        74.36      10552    4595040
dm-2              0.01         0.06         0.03       3522       1856

avg-cpu:  %user   %nice %system %iowait  %steal   %idle
          44.30    0.00   55.70    0.00    0.00    0.00

Device:            tps   Blk_read/s   Blk_wrtn/s   Blk_read   Blk_wrtn
sda               0.00         0.00         0.00          0          0
scd0              0.00         0.00         0.00          0          0
dm-0              0.00         0.00         0.00          0          0
dm-1              0.00         0.00         0.00          0          0
dm-2              0.00         0.00         0.00          0          0
```

※^C ←Ctrl+C□□□□□□□

iostat -x

```
# iostat -x
Linux 2.6.32-504.el6.x86_64 (server.example.com)  2015□01□15□  _x86_64(2 C

avg-cpu:  %user   %nice %system %iowait  %steal   %idle
           1.78    0.00    2.04    0.03    0.00   96.16

Device:         rrqm/s   wrqm/s     r/s     w/s   rsec/s   wsec/s avgrq-sz
sda               0.83     4.90    0.83    1.06    44.00   116.88    85.16
scd0              0.04     0.00    0.01    0.00     0.18     0.00    27.00
dm-0              0.00     0.00    1.17    5.33    41.92    42.52    12.98
dm-1              0.00     0.00    0.02    0.47     0.17    74.33   150.83
dm-2              0.00     0.00    0.01    0.00     0.06     0.03     7.97
```

rrqm/s	1		
wrqm/s	1		
r/s	1		
w/s	1		
rsec/s	1		
wsec/s	1		
rkB/s	1		KB
wkB/s	1		KB
avgrq-sz		IO	
avgqu-sz		IO	
await		IO	
svctm		IO	

%util IO CPU

sar System Admin Reporter

sar CPU
sar

sar sadc
sysstat cron
sar

sar 1 3 CPU

```
# sar 1 3
Linux 2.6.32-504.el6.x86_64 (server.example.com)  2015□01□23□  _x86_64(2 C

18□25□47□     CPU     %user     %nice   %system   %iowait    %steal     %i
18□25□48□     all     38.00      0.00     62.00      0.00      0.00      0
18□25□49□     all     38.50      0.00     61.50      0.00      0.00      0
18□25□50□     all     39.80      0.00     60.20      0.00      0.00      0
□□□:      all     38.77      0.00     61.23      0.00      0.00      0.00
```

sar -b I/O

```
# sar -b 1 3
Linux 2.6.32-504.el6.x86_64 (server.example.com)  2015□01□23□  _x86_64(2 C

18□26□15□       tps      rtps      wtps   bread/s   bwrtn/s
18□26□16□      0.00      0.00      0.00      0.00      0.00
18□26□17□      0.00      0.00      0.00      0.00      0.00
18□26□18□    352.00    142.00    210.00   5648.00   1904.00
□□□:     117.73     47.49     70.23   1888.96    636.79
```

sar -r

```
# sar -r 1 3
Linux 2.6.32-504.el6.x86_64 (server.example.com)  2015□01□23□  _x86_64(2 C

18□26□32□ kbmemfree kbmemused  %memused kbbuffers  kbcached  kbcommit   %c
18□26□33□    233684    782688     77.01     81008    152872   1562412
18□26□34□    101404    914968     90.02     81008    152872   1562412
18□26□35□    112552    903820     88.93     81008    152872   1562412
□□□:     149213    867159     85.32     81008    152872   1562412     50.7
```

sar sysstat

```
# sar
Linux 2.6.32-504.el6.x86_64 (server.example.com)  2015□01□23□  _x86_64(2 C

11□10□01□     CPU     %user     %nice   %system   %iowait    %steal     %i
11□20□01□     all      0.39      0.00      0.36      0.01      0.00     99
11□30□02□     all      9.34      0.00     12.22      0.04      0.00     78
11□40□01□     all     43.10      0.00     56.90      0.00      0.00      0
□□□
```

sar -f /var/log/sa/saDD

```
# sar -f /var/log/sa/sa22
Linux 2.6.32-504.el6.x86_64 (server.example.com)  2015□01□22□  _x86_64(2 C

12□10□02□     CPU     %user     %nice   %system   %iowait    %steal     %i
12□20□01□     all      0.33      0.00      0.34      0.01      0.00     99
12□30□01□     all      0.39      0.00      0.34      0.02      0.00     99
□□□:      all      0.36      0.00      0.34      0.01      0.00     99.29
□□□
```

/var/log/sa/sarDD 1 less
23 53 sarDD
root sarDD

```
# /usr/lib64/sa/sa2 -A
# cat /var/log/sa/sar24
Linux 2.6.32-504.el6.x86_64 (server.example.com)  2015-01-23  _x86_64(2 CP

11□10□01□     CPU      %usr     %nice      %sys   %iowait    %steal      %
11□20□01□     all      0.39      0.00      0.35      0.01      0.00      0
11□20□01□       0      0.44      0.00      0.36      0.02      0.00      0
□□□
```

logwatch

logwatch

logwatch

```
# yum install logwatch
```

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

LogDir

TmpDir

MailTo

MailFrom

Print

STDOUT Yes MailTo No

Save

Archives

Yes

Range

All Today Yesterday

Detail

Low 0 Med 5 High 10

Service

LogWatch
/usr/share/logwatch/scripts/services

LogFile

mailer

HostLimit

hostname

MailTo Detail

```
# cp /usr/share/logwatch/default.conf/logwatch.conf /etc/logwatch/conf/logw
cp: `/etc/logwatch/conf/logwatch.conf' □□□□□□□□□□□□□□□(yes/no)? ※y y□□□
```

```
MailTo = root
Range = yesterday
Detail = Low
Service = All
```

root
/usr/share/logwatch/scripts/services

```
# ls /usr/share/logwatch/scripts/services
afpd            eximstats         pam_unix          sendmail-largeboxes
amavis          extreme-networks  php               shaperd
arpwatch        fail2ban          pix               slon
audit           ftpd-messages     pluto             smartd
automount       ftpd-xferlog      pop3              sonicwall
autorpm         http              portsentry        sshd
bfd             identd            postfix           sshd2
cisco           imapd             pound             stunnel
clam-update     in.qpopper        proftpd-messages  sudo
clamav          init              pureftpd          syslogd
clamav-milter   ipop3d            qmail             tac_acc
courier         iptables          qmail-pop3d       up2date
```

```
cron            kernel            qmail-pop3ds      vpopmail
denyhosts       mailscanner       qmail-send        vsftpd
dhcpd           modprobe          qmail-smtpd       windows
dnssec          mountd            raid              xntpd
dovecot         named             resolver          yum
dpkg            netopia           rt314             zz-disk_space
emerge          netscreen         samba             zz-fortune
evtapplication  oidentd           saslauthd         zz-network
evtsecurity     openvpn           scsi              zz-runtime
evtsystem       pam               secure            zz-sys
exim            pam_pwdb          sendmail
```

/etc/logwatch/conf/logwatch.conf

```
# vi /etc/logwatch/conf/logwatch.conf

※#※Range = yesterday ※←□□□#□□□
※Range = All ←□□□□□
```

logwatch logwatch --print

```
# logwatch --print


 ################### Logwatch 7.3.6 (05/19/07) ####################
        Processing Initiated: Tue Jan 27 11:53:04 2015
        Date Range Processed: all
      Detail Level of Output: 0
              Type of Output: unformatted
           Logfiles for Host: server.example.com
  ##################################################################

 --------------------- Selinux Audit Begin ------------------------

  Number of audit daemon stops: 1

 ---------------------- Selinux Audit End -------------------------
□□□
 --------------------- Disk Space Begin ------------------------

 Filesystem            Size  Used Avail Use% Mounted on
 /dev/mapper/vg_server-lv_root
                        50G  3.8G   43G   9% /
 /dev/sda1             477M   28M  424M   7% /boot
 /dev/mapper/vg_server-lv_home
                        12G   31M   11G   1% /home
```

```
 ---------------------- Disk Space End -------------------------


 ###################### Logwatch End #########################
```

□□□/etc/logwatch/conf/logwatch.conf□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

~~~
```shell-session
# vi /etc/logwatch/conf/logwatch.conf

Range = Today
~~~

logwatch --print

OS

CentOS /var/log

messages
secure
maillog
dmesg

- /var/log/messages
- /var/log/secure
- /var/log/maillog
- Web /var/log/httpd/error_log

dmesg

dmesg display message Linux

dmesg

```
# dmesg
Initializing cgroup subsys cpuset
Initializing cgroup subsys cpu
Linux version 2.6.32-504.el6.x86_64 (mockbuild@c6b9.bsys.dev.centos.org) (
```

```
Command line: ro root=/dev/mapper/vg_server-lv_root rd_LVM_LV=vg_server/lv
KERNEL supported cpus:
  Intel GenuineIntel
  AMD AuthenticAMD
  Centaur CentaurHauls
Disabled fast string operations
□□□
```

syslog

syslog syslog syslog

CentOS 6 syslog rsyslog

rsyslog syslog syslogd syslog
rsyslog Reliable syslog
TCP
syslogd

syslog facility
priority

auth	login su
authpriv	
cron	cron at
daemon	
kern	
lpr	
mail	
news	NetNews
security	auth
syslog	syslogd
user	

uucp uucp
local0 local7 facility

debug
info
notice
warning
warn warning
err
error err
crit
alert
emerg
panic emerg
none

syslog

syslog /etc/rsyslog.conf

□□□□□□.□□□□□□□□ □□□□□

syslog ,
UUCP

```
uucp,news.crit /var/log/spooler
```

syslog

```
mail.warning
```

mail warning err crit alert emerg

=

```
mail.=warning
```

mail warning

none

-

\

*****

@ IP

UDP syslog

@@ IP

TCP syslog

syslog

/etc/rsyslog.conf

```
authpriv.* /var/log/secure
```

authpriv * /var/log/secure

```
*.info;mail.none;authpriv.none;cron.none  /var/log/messages
```

info /var/log/messages
mail authpriv cron 3 none

mail -

```
authpriv.*      /var/log/secure
mail.*       -/var/log/maillog
cron.*       /var/log/cron
```

syslog

iptables

iptables /etc/sysconfig/iptables 22 ACCEPT
REJECT

```
# Firewall configuration written by system-config-firewall
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
※-A INPUT -j LOG --log-level debug --log-prefix '[iptables_test]:' ←□□□□□
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

iptables reload

```
# service iptables reload
iptables: Trying to reload firewall rules:                [  OK  ]
```

/etc/rsyslog.conf kern /var/log/kern.log

```
# vi /etc/rsyslog.conf

# Log all kernel messages to the console.
# Logging much else clutters up the screen.
```

```
#kern.*                                                    /dev/console
※kern.*                                                    /var/log/kern.log
```

rsyslog

```
# service rsyslog restart
□□□□□□□□□□□□:                                    [  OK  ]
□□□□□□□□□□□□:                                    [  OK  ]
```

iptables 80 Web

/var/log/kern.log 80

```
# tail /var/log/kern.log
Dec 25 14:54:16 server kernel: imklog 5.8.10, log source = /proc/kmsg star
Dec 25 14:54:50 server kernel: ※'[iptables_test]:'※IN=eth0 OUT= MAC=00:1c
```

UDP

syslog syslog
UDP

/etc/rsyslog.conf 2

$ModLoad\ \ UDP$ UDPServerRun UDP

```
[root@server ~]## vi /etc/rsyslog.conf

□□□
# Provides UDP syslog reception
$ModLoad imudp ※←□□□#□□□
$UDPServerRun 514 ※←□□□#□□□
```

rsyslog rsyslogd UDP 514

```
[root@server ~]# service rsyslog restart
□□□□□□□□□□□□:                                    [  OK  ]
□□□□□□□□□□□□:                                    [  OK  ]
[root@server ~]# lsof -i:514
COMMAND   PID USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
rsyslogd 9282 root    3u  IPv4 134339      0t0  UDP *:syslog
rsyslogd 9282 root    4u  IPv6 134340      0t0  UDP *:syslog
```

iptables UDP 514

TCP

TCP UDP
UDP

TCP UDP
syslog

TCP
syslog UDP

/etc/rsyslog.conf 2

ModLoad TCP InputTCPServerRun
TCP

```
[root@server ~]# vi /etc/rsyslog.conf

□□□
# Provides TCP syslog reception
$ModLoad imtcp ※←□□□#□□□
$InputTCPServerRun 514 ※←□□□#□□□
```

rsyslog rsyslogd TCP 514

```
[root@server ~]# service rsyslog restart
□□□□□□□□□□□:                                    [  OK  ]
□□□□□□□□□□□:                                    [  OK  ]
[root@server ~]# lsof -i:514
COMMAND    PID USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
rsyslogd 24138 root    1u  IPv4 107209      0t0  TCP *:shell (LISTEN)
rsyslogd 24138 root    3u  IPv4 107202      0t0  UDP *:syslog
rsyslogd 24138 root    4u  IPv6 107203      0t0  UDP *:syslog
rsyslogd 24138 root    8u  IPv6 107210      0t0  TCP *:shell (LISTEN)
```

shell /etc/services

```
# grep 514 /etc/services
shell           514/tcp         cmd             # no passwords used
syslog          514/udp
□□□
```

iptables TCP 514

syslog　　iptables

syslog　　iptables　　TCP　　UDP　　514
　　iptables

```
[root@server ~]# service iptables stop
iptables: □□□□□□□□□ ACCEPT □□□□filter          [  OK  ]
iptables: □□□□□□□□□□□□□□□□:                   [  OK  ]
iptables: □□□□□□□□□□□□:                          [  OK  ]
```

/etc/sysconfig/iptables　　iptables　　Reject
　　iptables　　reload

```
[root@server ~]# vi /etc/sysconfig/iptables
□□□
※-A INPUT -m state --state NEW -m udp -p udp --dport 514 -j ACCEPT ←□□□□□
※-A INPUT -m state --state NEW -m tcp -p tcp --dport 514 -j ACCEPT ←□□□□□
-A INPUT -j REJECT --reject-with icmp-host-prohibited
```

syslog

　　syslog　　syslog

syslog　　rsyslog　　syslog

syslog　　/etc/rsyslog.conf

authpriv　　syslog　　@
　　UDP

　　mail　　syslog　　@@
　　TCP

```
# vi /etc/rsyslog.conf

# The authpriv file has restricted access.
authpriv.*                                                  /var/log/secure
※authpriv.*                                                 @192.168.0.10 ←□□

# Log all the mail messages in one place.
mail.*                                                      -/var/log/maillog
※mail.*                                                     @@192.168.0.10 ←□

syslog□□□□□□□rsyslog□□□□□□□□□□□□□

```shell-session
[root@client ~]# service rsyslog restart
```
```

```
□□□□□□□□□□□□:                                          [  OK  ]
□□□□□□□□□□□□:                                          [  OK  ]
```

UDP

syslog logger authpriv.debug

```
[root@client ~]# logger -p authpriv.debug "This is auth log over UDP"
```

syslog /var/log/secure

```
[root@server ~]# tail -f /var/log/secure
□□□
Dec 25 17:16:50 client root: This is auth log over UDP
```

TCP

syslog logger mail.debug

```
[root@client ~]# logger -p mail.debug "This is mail log over TCP"
```

syslog /var/log/maillog

```
[root@server ~]# tail /var/log/secure
□□□
Dec 25 17:18:03 client root: This is mail log over TCP
```

logrotate

logrotate

logrotate cron 1 1 /etc/cron.daily/logrotate
/etc/logrotate.conf logrotate

/etc/logrotate.d

logrotate

create [ ] [ ] [ ]

0755

nocreate

create create

copy/nocopy

copytruncate/nocopytruncate

copy create Oracle 10g R1/R2 alert alert_xx.log.1

rotate

a.log num 2 a.log→a.log.1→a.log.2→ 0 a.log→

start

1 num 5 a.log→a.log.5→a.log.6

extension

.bak some.log some.log.1.bak

compress/nocompress

nocompress

compresscmd

gzip

uncompresscmd

gunzip

compressoptions

gzip -9 -9 -s

compressext

delaycompress/nodelaycompress

olddir /noolddir

mail address/nomail

address maillast

maillast

mailfirst

daily/weekly/monthly

/ / daily weekly
1

size [K/M]

daily,weekly
K M

ifempty/notifempty

missingok/nomissingok

firstaction

prerotete

prerotate

firstaction

postrotate

lastaction

lastaction

postrotate

sharedscripts

prerotate postrotate

nosharedscripts

prerotate postrotate

include

include

tabooext [+] [, ,...]

include
.rpmorig .rpmsave ,v .swp .rpmnew ~ .cfsaved .rhn-cfg-tmp-*
+ +

/etc/logrotate.d/httpd

```
# cat /etc/logrotate.d/httpd
/var/log/httpd/*log {
    missingok
    notifempty
    sharedscripts
    delaycompress
    postrotate
        /sbin/service httpd reload > /dev/null 2>/dev/null || true
    endscript
}
```

/var/log/httpd log
access_log error_log

- 1 missingok
- 2 notifempty
- 3 sharedscripts prerotate,postrotate
- 4 delaycompress
- 5 "postrotate" "endscript"
  service httpd reload

- ping
- traceroute
- netstat
- tcpdump
- Wireshark

1.
2. ping IP
3. telnet TCP
4. netstat
5.

ping IP

ping ping ICMP
IP ping

IP iptables
ICMP
ping

traceroute traceroute
ICMP ICMP

telnet TCP

telnet 2 TCP

```
telnet □□□IP□□□□ □□□□□
```

telnet

```
# yum install telnet
```

iptables
iptables

Listen
127.0.0.1 Listen IP
netstat lsof

netstat

netstat IP

netstat -p

```
# netstat -anp | grep sshd
tcp        0      0 0.0.0.0:22     0.0.0.0:*  LISTEN   1493/sshd
```

- sshd ID 1493
- TCP 22 LISTEN
- 22 IP 0.0.0.0:22
- 0.0.0.0:*

tcpdump GUI
Wireshark

tcpdump

tcpdump
tcpdump

-i eth0

tcpdump tcpdump.out

```
# tcpdump -i eth0 > tcpdump.out
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
```

SSH

Ctrl+C tcpdump

```
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
※^C※216 packets captured ※←Ctrl+C□□□□□
216 packets received by filter
0 packets dropped by kernel
```

tcpdump.out

```
# grep ssh tcpdump.out
13:17:06.041096 IP client.example.com.43880 > server.example.com.ssh: ※Fla
13:17:06.041125 IP server.example.com.ssh > client.example.com.43880: ※Fla
13:17:06.041240 IP client.example.com.43880 > server.example.com.ssh: ※Fla
```

) IP . .
SYN)

1

43880 22 ssh SYN TCP

2

1 SYN+ACK TCP

3

ACK TCP TCP

Wireshark

tcpdump

GUI Wireshark

Wireshark GUI wireshark-gnome

```
# yum install wireshark-gnome
```

1. Wireshark
   CentOS GUI wireshark
   → → Wireshark Network Analyzer

```
# wireshark &
```

2

2.

Capture → Interfaces
Capture → Interfaces

Capture → Interfaces

3

3.

eth0
eth0

eth0 Start

4

4. Web
Web
Web

5

5.
Capture → Stop

6

6.

http
http

Filter: http Enter
Hypertext Transfer Protocol
HTTP

OS

Linux 1
root
3 5

GRUB

1. 5
GRUB
2. e kernel e
single 1
3. Enter
4. b

5

5. root
fsck

6. exit

DVD

OS
DVD

1. CentOS DVD BIOS
DVD

2. Rescue installed system

3

1. Language

Language

4

1. /mnt/sysimage Read-Only
Continue

Continue
Continue

5

1. /mnt/sysimage

   /mnt/sysimage
   /mnt/sysimage

6

1. shell fakd First Aid Kit reboot shell

   shell
   shell

7

1. bash /mnt/sysimage

8

1. fsck exit

2. reboot DVD DVD

   reboot
   reboot

CentOS 7

CentOS 7

CentOS 6 CentOS 7

CentOS 7 CentOS 7

- SysV init systemd
- journald
- firewalld

NetworkManager CentOS 6
CUI NetworkManager nmtui

SysV init systemd

CentOS 7 SysV init Upstart Linux
systemd /etc/rc.d

systemd

systemd

SysV init
1

systemd

service
target
mount

swap
device

systemd systemctl service

Web systemctl

systemctl start

```
# systemctl start httpd
```

systemctl status

systemd cgroup Linux
cgroup CPU

```
# systemctl status httpd
httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled)
   Active: active (running) since □ 2015-01-28 15:23:50 JST; 33s ago
 Main PID: 2926 (httpd)
   Status: "Total requests: 0; Current requests/sec: 0; Current traffic:
   CGroup: /system.slice/httpd.service
           ├─2926 /usr/sbin/httpd -DFOREGROUND
           ├─2927 /usr/sbin/httpd -DFOREGROUND
           ├─2928 /usr/sbin/httpd -DFOREGROUND
           ├─2929 /usr/sbin/httpd -DFOREGROUND
           ├─2930 /usr/sbin/httpd -DFOREGROUND
           └─2931 /usr/sbin/httpd -DFOREGROUND

 1□ 28 15:23:50 centos7.example.com httpd[2926]: AH00557: httpd: apr_socka
 1□ 28 15:23:50 centos7.example.com httpd[2926]: AH00558: httpd: Could not
 1□ 28 15:23:50 centos7.example.com systemd[1]: Started The Apache HTTP Se
Hint: Some lines were ellipsized, use -l to show in full.
```

systemctl restart

```
# systemctl restart httpd
# systemctl status httpd
httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled)
   Active: active (running) since □ 2015-01-28 15:24:40 JST; 2s ago
  Process: 2945 ExecStop=/bin/kill -WINCH ${MAINPID} (code=exited, status=
 Main PID: 2950 (httpd)
□□□
```

systemctl stop

```
# systemctl stop httpd
# systemctl status httpd
httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled)
   Active: inactive (dead)
```

systemd systemctl list-unit-files

```
# systemctl list-unit-files
```

-t

service systemctl
chkconfig --list

```
# systemctl list-unit-files -t service
```

STATE

enabled
disabled
static

systemctl list-units systemctl

```
# systemctl list-units
# systemctl
```

-t service

```
# systemctl -t service
UNIT                          LOAD   ACTIVE SUB     DESCRIPTION
abrt-ccpp.service             loaded active exited  Install ABRT coredump h
abrt-oops.service             loaded active running ABRT kernel log watcher
abrt-xorg.service             loaded active running ABRT Xorg log watcher
abrtd.service                 loaded active running ABRT Automated Bug Repo
alsa-state.service            loaded active running Manage Sound Card State
atd.service                   loaded active running Job spooling tools
□□□
kdump.service                 loaded failed failed  Crash recovery kernel a
□□□
```

UNIT

LOAD systemd

ACTIVE active inactive

SUB running exited

DESCRIPTION

ACTIVE active inactive
--all

LOAD systemctl mask masked

ACTIVE failed
kdump

-t device

```
# systemctl list-units -t device
UNIT
sys-devices-pci0000:00-0000:00:05.0-virtio0-net-eth0.device
sys-devices-pci0000:00-0000:00:1f.2-ata3-host2-target2:0:0-2:0:0:0-block-s
□□□
```

-t mount

```
# systemctl list-units -t mount
UNIT                          LOAD   ACTIVE SUB     DESCRIPTION
-.mount                       loaded active mounted /
boot.mount                    loaded active mounted /boot
dev-hugepages.mount           loaded active mounted Huge Pages File System
dev-mqueue.mount              loaded active mounted POSIX Message Queue Fil
home.mount                    loaded active mounted /home
□□□
```

-t swap

```
# systemctl list-units -t swap
UNIT              LOAD   ACTIVE SUB    DESCRIPTION
dev-dm\x2d0.swap loaded active active /dev/dm-0
□□□
```

systemctl enable
chkconfig

Web
/usr/lib/systemd/system/httpd.service Web systemctl enable
/etc/systemd/system/multi-user.target.wants

multi-user.target
SysV init /etc/init.d
/etc/rc.d

```
# systemctl enable httpd
ln -s '/usr/lib/systemd/system/httpd.service' '/etc/systemd/system/multi-u
```

systemctl disable

```
# systemctl disable httpd
rm '/etc/systemd/system/multi-user.target.wants/httpd.service'
```

systemd

systemctl mask systemd

/etc/systemd/system/httpd.service /dev/null

Web systemd

```
# systemctl mask httpd
ln -s '/dev/null' '/etc/systemd/system/httpd.service'
# systemctl start httpd
Failed to issue method call: Unit httpd.service is masked.
```

systemctl is-enabled httpd masked

```
# systemctl is-enabled httpd
masked
```

systemctl unmask systemd
httpd disabled

```
# systemctl unmask httpd
rm '/etc/systemd/system/httpd.service'
# systemctl is-enabled httpd
disabled
```

systemd

systemd

systemctl enable systemd
2

/usr/lib/systemd/system

/etc/rc.d/init.d

/etc/systemd/system

/etc/rc.d

systemd /etc/systemd/system

1. /etc/systemd/system/sysinit.target.wants/

rc.sysinit

2. /etc/systemd/system/basic.target.wants/

3. /etc/systemd/system/multi-user.target.wants/

3 CUI

4. /etc/systemd/system/graphical.target.wants/

5 GUI

SysV init 3 5 systemd multi-user.target graphical.target

systemd CUI GUI

systemctl set-default SysV init /etc/inittab initdefault

systemctl get-default

```
# systemctl get-default
graphical.target
```

CUI

multi-user.target CUI

```
# systemctl set-default multi-user.target
# reboot
```

GUI

GUI systemctl set-default

```
# systemctl set-default graphical.target
# reboot
```

systemd systemctl isolate
SysV init telinit

GUI CUI GUI

```
# systemctl isolate multi-user.target
```

CUI GUI

```
# systemctl isolate graphical.target
```

journald

systemd journald syslog

journald

journald journalctl

dmesg Linux

```
# journalctl
-- Logs begin at □ 2015-01-28 17:29:04 JST, end at □ 2015-01-28 17:29:38 J
 1□ 28 17:29:04 centos7.example.com systemd-journal[149]: Runtime journal
 1□ 28 17:29:04 centos7.example.com systemd-journal[149]: Runtime journal
□□□
```

-u

httpd

```
# journalctl -u httpd
-- Logs begin at □ 2015-01-28 17:29:04 JST, end at □ 2015-01-28 17:31:34 J
 1□ 28 17:31:28 centos7.example.com systemd[1]: Starting The Apache HTTP S
 1□ 28 17:31:34 centos7.example.com httpd[2232]: AH00557: httpd: apr_socka
 1□ 28 17:31:34 centos7.example.com httpd[2232]: AH00558: httpd: Could not
 1□ 28 17:31:34 centos7.example.com systemd[1]: Started The Apache HTTP Se
```

journald

journald journald
/etc/systemd/journald.conf Storage auto

1. /var/log/journal
2. /var/log/journal /run/log/journal

/var/log/journal /run/log/journal
/run/log/journal tmpfs

journald /var/log/journal

```
# mkdir /var/log/journal
# chmod 700 /var/log/journal
# reboot
```

```
# ls -l /var/log/journal/
□□ 0
drwxr-sr-x. 2 root systemd-journal 49  1□ 28 14:53 3b71b9857a284561a345099
# ls -l /var/log/journal/3b71b9857a284561a3450996bf78a306/
□□ 16392
-rw-r-----. 1 root root            8388608  1□ 28 14:56 system.journal
-rw-r-----+ 1 root systemd-journal 8388608  1□ 28 14:55 user-42.journal
```

firewalld

CentOS 7 Linux iptables firewalld
firewalld

iptables

firewalld

firewalld

firewall-cmd --get-default-zone public

```
# firewall-cmd --get-default-zone
public
```

public DHCP SSH

```
# firewall-cmd --list-all
public (default, active)
  interfaces: eth0
```

```
  sources:
  services: dhcpv6-client ssh
  ports:
  masquerade: no
  forward-ports:
  icmp-blocks:
  rich rules:
```

--list-services

```
# firewall-cmd --list-services
dhcpv6-client ssh
```

```
# firewall-cmd --get-services
amanda-client bacula bacula-client dhcp dhcpv6 dhcpv6-client dns ftp high-
```

firewalld HTTP

firewalld HTTP

--add-service

--permanent /etc/firewalld/zones/public.xml
HTTP

```
# firewall-cmd --add-service=http  --permanent
success
# firewall-cmd --list-services
dhcpv6-client http ssh
# cat /etc/firewalld/zones/public.xml
<?xml version="1.0" encoding="utf-8"?>
<zone>
  <short>Public</short>
  <description>For use in public areas. You do not trust the other compute
  <service name="dhcpv6-client"/>
  <service name="http"/>
  <service name="ssh"/>
</zone>
```

Web Web

```
# systemctl start httpd
```

iptables

firewalld iptables

```
# systemctl stop firewalld
# systemctl disable firewalld
# systemctl enable iptables
# systemctl start iptables
```

firewalld

```
# systemctl stop iptables
# systemctl disable iptables
# systemctl enable firewalld
# systemctl start firewalld
```

*NetworkManager nmtui
CentOS 7 NetworkManager

NetworkManager GUI CUI

GUI NetworkManager
GUI NetworkManager

GUI

CUI NetworkManager
CUI NetworkManager

CUI nmtui IP