

---

# FreeBSD

---

Korea FreeBSD Users Group – <http://www.kr.FreeBSD.org/>

## Chapter 15 :

<rick@rickinc.com> .

<nobreak@kr.FreeBSD.org> .

: 2004 8 7

: 2005 3 8

: 1.0

FreeBSD Documentation Project FreeBSD Handbook 2004 8

7 . FreeBSD Handbook ,  
, CVS Repository  
,  
,  
가  
가 . KFUG(Korea FreeBSD Users Group)  
KFUG

“FreeBSD Handbook” “FreeBSD Documentation Project” , “ FreeBSD  
” “ (Young-oak Lee)” .

*Copyright © 1995, 1996, 1997, 1998, 1999, 2000, 2001, 2002, 2003, 2004 The FreeBSD Documentation Project.*

# 15

## 15.1

가 . TrustedBSD 가 .  
 TrustedBSD POSIX@.1e  
 FreeBSD 5.X .  
 (MAC) (ACLs)  
 MAC 가? (Mandatory Access Controls)  
 ;  
 (object) (subject) .  
 .  
 MAC , (Mandatory Access  
 Control) FreeBSD 5.X 가  
 가 가 .  
 :  
 • FreeBSD MAC .  
 • MAC  
 가  
 • MAC 가  
 • MAC 가  
 • MAC 가

- MAC 가

:

- FreeBSD (3 ).

- FreeBSD / (8 ).

- FreeBSD (14 ).

:

Xfree86 . MAC

. MAC

가 :

## 15.1.1

## 가?

MAC . MAC

MAC

mac\_test(4),

mac\_stub(4) mac\_none(4) /



- *(sensitivity):* MLS 가  
가
- :  
*(multilabel)*
- *(subject):* :

## 15.3 MAC

MAC 가  
MAC 가 , ,  
가  
(multi-layer) 가 가  
가  
MAC 가  
MAC 가  
가 ; mac\_portacl(4), mac\_ifoff(4)

mac\_biba(4)

. mac\_bsdxextended(4) mac\_mls(4)

ssh(1)가

. mac\_portacl(4)

가?

가

가?

가?

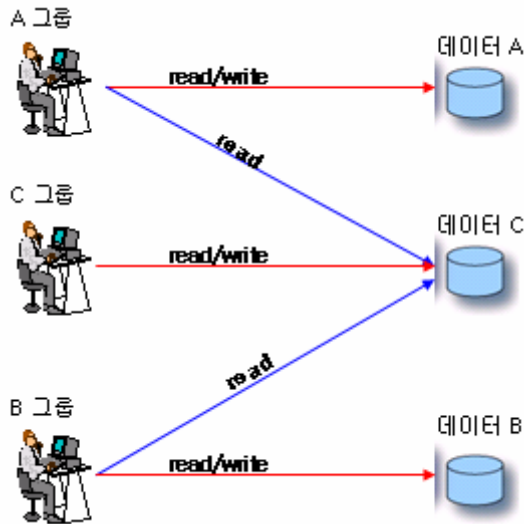
A

B

C

MAC

가



[15-1.bmp]

가

. MAC

가

가

FreeBSD

MAC

;

가 :

options    MAC
----------------

:    MAC

. MAC

MAC

가 .

## 15.4 MAC

MAC

가 ;

*biba/low*

"low"    Biba

FreeBSD    (low, high    equal    ) 3

가 가    low    가

, equal

high    가    가

```

가
가
가
tunefs(8)
Biba  MLS
가
;
DAC . MAC . root
/
root
root
Biba  MLS
/

```

## 15.4.1

4

```

setfmac(8) setpmac(8) . setfmac
MAC
setpmac . :
# setfmac biba/high test
가 가 가 ;
chmod(1) chwon(8)
"Permission denied"가
:

```







login.conf                    cap\_mkdb

가

가

가

### 15.4.1.2

*biba*

MAC

*maclabel* ifconfig

# ifconfig bge0 maclabel *biba/equal*

bge(4)

*biba/equal* MAC

*biba/high*(low - high)

가

MAC

tunable 가

*equal*

가 . sysctl

tunables

### 15.4.2

가?

*biba/high* 가



**Note:** root 가 .  
(15.16)

### 15.4.3 Tunables MAC

sysctl MAC :

- *security.mac.enforce\_fs* MAC
- *security.mac.enforce\_kld* MAC  
([kld\(4\)](#)).
- *security.mac.enforce\_network* MAC
- *security.mac.enforce\_pipe* (pipe) MAC
- *security.mac.enforce\_process* MAC
- *security.mac.enforce\_socket* MAC  
([socket\(2\)](#)).
- *security.mac.enforce\_system* accounting  
MAC
- *security.mac.enforce\_vm* 가 MAC

**Note:** MAC tunables .  
*security.mac.<policyname>* . MAC tunables  
:

# sysctl -da | grep mac

MAC

sysctl

가

## 15.5

MAC

/boot/loader.conf

가

MAC

“ ”

가

tunefs

### 15.5.1 MAC seeotheruids

: mac\_seeotheruids.ko

: *options MAC\_SEEOTHERUIDS*

: *mac\_seeotheruids\_load="YES"*

mac\_seeotheruids(4)      *security.bsd.see\_other\_uids*      *security.bsd.see\_other\_gids*  
sysctl tunables

sysctl tunables

:

- *security.mac.seeotheruids.enabled*

- *security.mac.seeotheruids.specificgid\_enabled*

*security.mac.seeotheruids.specificgid=XXX* sysctl tunable  
XXX ID

- *security.mac.seeotheruids.primarygroup\_enabled*

tunable  
*security.mac.seeotheruids.specificgid\_enabled*

root MAC  
*security.bsd.seeotheruids* tunable 가

## 15.6 MAC bsdextended

: *mac\_bsdextended.ko*

: *options MAC\_BSDEXTENDED*

: *mac\_bsdextended\_load="YES"*

mac\_bsdextended(4)

가

ipfw(8) 가 ugidfw(8)  
libugidfw(3)

## 15.6.1

mac\_bsdextended(4)

:

```
# ugidfw list
0 slots, 0 rules
```

. root

:

```
# ugidfw add subject not uid root new object not uid root mode n
```

**Note:** FreeBSD 5.3 add 가 . set

ls 가 .

:

```
# ugidfw set 2 subject uid user object uid trhodes mode n
# ugidfw set 3 subject uid user object gid trhodes mode n
```

user trhodes

user *not uid trhodes*

**Note:** root

mac\_bsdextended(4)

mac\_bsdextended(4) ugidfw(8)



## 15.7 MAC ifoff

: mac\_ifoff.ko

: options MAC\_IFOFF

: mac\_ifoff\_load="YES"

mac\_ifoff(4)

MAC

sysctl tunables

- *security.mac.ifoff.lo\_enabled* (lo(4)) /
- *security.mac.ifoff.bpfrecv\_enabled* (bpf(4)) /
- *security.mac.ifoff.other\_enabled* /

mac\_ifoff(4) 가

[security/aide](#)

## 15.8 MAC portacl

: mac\_portacl.ko

: *MAC\_PORTACL*

: *mac\_portacl\_load="YES"*

mac\_portacl(4) sysctl TCP UDP  
 mac\_portacl(4) root 가 가  
 (1024 )  
 MAC tunables

- *security.mac.portacl.enabled* / ( *security.mac.portacl.enabled* sysctl FreeBSD 5.2.1 )

- *security.mac.portacl.port\_high* mac\_portacl(4)가 가

- *security.mac.portacl.suser\_exempt* 0 root

- *security.mac.portacl.rules* mac\_portacl ;

*security.mac.portacl.rules* sysctl *mac\_portacl*  
*rule[,rule,...]*  
*idtype:id:protocol:port* . *ldtype* id id 가  
*uid gid* 가 *id* . *protocol* *tcp*  
*udp* TCP UDP  
*port*

**Note:** ID, ID,

```

1024
. root 가 . mac_portacl(4)
1024
sysctl(8) net.inet.ip.portrange.reservedlow net.inet.ip.portrange.reservedhigh 0
.
mac_portacl(4)

```

## 15.8.1

```

# sysctl security.mac.portacl.port_high=1023
# sysctl net.inet.ip.portrange.reservedlow=0 net.inet.ip.portrange.reservedhigh=0

```

```

가 mac_portacl(4)

```

```

# sysctl security.mac.portacl.suser_exempt=1

```

```

root security.mac.portacl.suser_exempt 0
. mac_portacl(4)

```

```

# sysctl security.mac.portacl.rules=uid:80:tcp:80

```

```

UID 80 ( www ) 가 80 . www
가 root

```

```

# sysctl security.mac.portacl.rules=uid:1001:tcp:110,uid:1001:tcp:995

```

```

1001 UID 가 TCP 110("pop3") 995("pop3s")
가 110 995

```

## 15.9 MCA

가 MAC

mac\_biba(4), mac\_lomac(4), mac\_partition(4), mac\_mls(4)

**Note:**

가 가

### 15.9.1

login.conf :

- *insecure* 가 . Insecure ;
- *Insecure* 가 . 가

```

insecure:
    :copyright=/etc/COPYRIGHT:
    :welcome=/etc/motd:
    :setenv=MAIL=/var/mail/$,BLOCKSIZE=K:
    :path=~ /bin:/sbin:/bin:/usr/sbin:/usr/bin:/usr/local/sbin:/usr/local/bin:
    :manpath=/usr/share/man /usr/local/man:
    :nologin=/usr/sbin/nologin:
    :cputime=1h30m:
    :datasize=8M:
    :vmemoryuse=100M:
    :stacksize=2M:
    :memorylocked=4M:
    :memoryuse=8M:
    :filesize=8M:
    :coredumpsize=8M:
    :openfiles=24:
    :maxproc=32:
    :priority=0:
    :requirehome:
    :passwordtime=91d:
    :umask=022:
    :ignoretime@:
    :label=partition/13,mls/5,biba/low:
    
```

가

cap\_mkdb(1)

login.conf(5)

root login  
setpmac

root 가

: login.ocnf

가

- MAC

가



## 15.10.1

:

```
# ps Zax
```

가

:

```
# ps -ZU trhodes
```

**Note:** mac\_seeotheruids(4)

root

/etc/rc.conf

**Note:** 3

## 15.11 MAC

: mac\_mls.ko

: *options MAC\_MLS*

: *mac\_mls\_load="YES"*

mac\_mls(4)

MLS( ) "clearance" . clearance sensibility 6000 ;

3 "instant" .

*mls/low* *mls/equal* *mls/high* .

:

- *mls/low* . *mls/low* clearance 가 가 clearance
- *mls/equal* .
- *mls/high* 가 가 clearace 가 ;

MLS :

- .
- ( ).
- ( ).
- ( ) .

sysctl tunables :





: mac\_biba.ko

: options MAC\_BIBA

: mac\_biba\_load="YES"

```
mac_biba(4)      MAC Biba
                  MLS
                  MLS
                  가
                  ;
```

```
Biba            " "
                  가
                  가
```

*biba/low, biba/equal*      *biba.high* :

- *biba/low*      가      가
- *biba/equal*
- *biba/high*

```
Biba            :
    ●
    ●      (MLS      ).      가
    ;      가
    ●      (      ).
```

- ( MLS ).

sysctl tunables Biba

- *security.mac.biba.enabled* Biba /

- *security.mac.biba.ptys\_equal* pty(4) Biba

- *security.mac.biba.revocation\_enabled*

Biba setfmac getfmac :

```
# setfmac biba/low test
# getfmac test
test: biba/low
```

;

## 15.13 MAC LOMAC

: mac\_lomac.ko

: *options MAC\_LOMAC*

: *mac\_lomac\_load="YES"*

MAC Biba mac\_lomac(4)



## 15.14.1 insecure

/etc/login.conf 가 :

```
insecure:
:copyright=/etc/COPYRIGHT:
:welcome=/etc/motd:
:setenv=MAIL=/var/mail/$,BLOCKSIZE=K:
:path=~:/bin:/sbin:/bin:/usr/sbin:/usr/bin:/usr/local/sbin:/usr/local/bin
:manpath=/usr/share/man /usr/local/man:
:nologin=/usr/sbin/nologin:
:cputime=1h30m:
:datasize=8M:
:vmemoryuse=100M:
:stacksize=2M:
:memorylocked=4M:
:memoryuse=8M:
:filesize=8M:
:coredumpsize=8M:
:openfiles=24:
:maxproc=32:
:priority=0:
:requirehome:
:passwordtime=91d:
:umask=022:
:ignoretime@:
:label=partition/13,mls/5:
```

가 :

```
:label=mls/equal,biba/equal,partition/equal:
```

:

```
# cap_mkdb /etc/login.conf
```

## 15.14.2

```
/boot/loader.conf 가
```

```
:
```

```
mac_biba_load="YES"
mac_mls_load="YES"
mac_seeotheruids_load="YES"
mac_partition_load="YES"
```

## 15.14.3 Insecure

```
root 가 가 .
가 vi(1) .
sh :
```

```
# for x in `awk -F: '($3 >= 1001) && ($3 != 65534) { print $1 }'
/etc/passwd`; do pw usermod $x -L insecure; done;
```

```
/etc/master.passwd cap_mkdb .
```

## 15.14.4

```
contexts ; Robert Watson
/etc/policy.contexts
```

```
# This is the default BIBA/MLS policy for this system.

.*                biba/high,mls/high
/sbin/dhclient    biba/high(low),mls/high(low)
/dev(/.*)?       biba/equal,mls/equal
# This is not an exhaustive list of all "privileged" devices.
/dev/mdctl        biba/high,mls/high
/dev/pci          biba/high,mls/high
/dev/k?mem        biba/high,mls/high
/dev/io           biba/high,mls/high
/dev/agp.*        biba/high,mls/high
(/var)?/tmp(/.*)? biba/equal,mls/equal
/tmp/ .X11-unix   biba/high(equal),mls/high(equal)
/tmp/ .X11-unix/.* biba/equal,mls/equal
/proc(/.*)?      biba/equal,mls/equal
/mnt.*           biba/low,mls/low
(/usr)?/home     biba/high(low),mls/high(low)
(/usr)?/home/.*  biba/low,mls/low
/var/mail(/.*)?  biba/low,mls/low
/var/spool/mqueue(/.*)? biba/low,mls/low
(/mnt)?/cdrom(/.*)? biba/high,mls/high
(/usr)?/home/(ftp|samba)(/.)? biba/high,mls/high
/var/log/sendmail .st biba/low,mls/low
/var/run/utmp     biba/equal,mls/equal
/var/log/(lastlog|wtmp) biba/equal,mls/equal
```

가

:

```
# setfsmac -ef /etc/policy.contexts /
# setfsmac -ef /etc/policy.contexts /usr
```

**Note:**

/etc/mac.conf :

```
default_labels file ?biba,?mls
default_labels ifnet ?biba,?mls
default_labels process ?biba,?mls,?partition
default_labels socket ?biba,?mls
```

## 15.14.5

adduser 가 insecure .

root ;

### 15.14.5.1

```
% getpmac
biba/15(15-15),mls/15(15-15),partition/15
# setpmac partition/15,mls/equal top
```

**Note:** top top .

### 15.14.5.2 MAC Seeotheruids

```
% ps Zax
biba/15(15-15),mls/15(15-15),partition/15 1096 #C: S 0:00.03 -su (bash)
biba/15(15-15),mls/15(15-15),partition/15 1101 #C: R+ 0:00.01 ps Zax
```



### 15.14.5.3 MAC Partition

MAC *seeotheruids* :

```
# sysctl security.mac.seeotheruids.enabled=0
% ps Zax
LABEL                                PID  TT  STAT    TIME
COMMAND
  biba/equal(low - high),mls/equal(low - high),partition/15  1122 #C:  S+    0:00.02
top
  biba/15(15 - 15),mls/15(15 - 15),partition/15            1096 #C:  S     0:00.05
-su (bash)
  biba/15(15 - 15),mls/15(15 - 15),partition/15            1123 #C:  R+    0:00.01
ps Zax
```

Biba .

```
# setpmac partition/15,mls/equal,biba/low top
% ps Zax
LABEL                                PID  TT  STAT    TIME COMMAND
  biba/15(15 - 15),mls/15(15 - 15),partition/15  1096 #C:  S     0:00.07 -su (bash)
  biba/15(15 - 15),mls/15(15 - 15),partition/15  1226 #C:  R+    0:00.01 ps Zax
```

Biba MLS .

```
% ifconfig bge0 | grep maclabel
maclabel biba/low(low - low),mls/low(low - low)
% ping -c 1 192.0.34.166
PING 192.0.34.166 (192.0.34.166): 56 data bytes
ping: sendto: Permission denied
```

example.com .

가 :

```
# sysctl security.mac.biba.trust_all_interfaces=1
```

insecure Biba

```
# ifconfig bge0 maclabel biba/equal (low-high ),mls/equal (low-high )
% ping -c 1 192.0.34.166
PING 192.0.34.166 (192.0.34.166): 56 data bytes
 64 bytes from 192.0.34.166: icmp_seq=0 ttl=50 time=204.455 ms
 --- 192.0.34.166 ping statistics ---
 1 packets transmitted, 1 packets received, 0% packet loss
 round-trip min/avg/max/stddev = 204.455/204.455/204.455/0.000 ms
```

ping .

가 :

```
# touch test1 test2 test3 test4 test5
# getfmac test1
test1: biba/equal,mls/equal
# setfmac biba/low test1 test2; setfmac biba/high test4 test5;
  setfmac mls/low test1 test3; setfmac mls/high test2 test4
# setfmac mls/equal,biba/equal test3 && getfmac test?
test1: biba/low,mls/low
  test2: biba/low,mls/high
  test3: biba/equal,mls/equal
  test4: biba/high,mls/high
  test5: biba/high,mls/equal
# chown testuser:testuser test?
```

testuser 가 :

```
% ls
test1 test2 test3 test4 test5
% ls test?
ls: test1: Permission denied
ls: test2: Permission denied
ls: test4: Permission denied
test3 test5
```

;  
(biba/high,mls/high) .

```
% for i in `echo test*`; do echo 1 > $i; done
-su: test1: Permission denied
-su: test4: Permission denied
-su: test5: Permission denied
```

;  
(biba/equal,mls/equal).

```
% cat test?
cat: test1: Permission denied
cat: test2: Permission denied
1
cat: test4: Permission denied
```

root :

```
# cat test2
1
```

**15.15** :

**MAC**

가 . biba/high  
가 .

```
# mkdir /usr/home/cvs
```

cvs :

```
# cvs -d /usr/home/cvs init
```

*biba* /boot/loader.conf  
*mac\_biba\_enable="YES"* . MAC 가

*biba/high* .

login.conf :

```
:ignoretime@:  
:umask=022:  
:label=biba/high:
```

```
# for x in `awk -F: '($3 >= 1001) && ($3 != 65534) { print $1 }'  
/etc/passwd`; do pw usermod $x -L default; done;
```

*biba/low* web .

cvs .

web .

```

biba/high 가
가 ; biba/high 가
.
FreeBSD sh(1) cron(8)
가 :
```

```

PATH=/bin:/usr/bin:/usr/local/bin; export PATH;
CVSROOT=/home/repo; export CVSROOT;
cd /home/web;
cvs -qR checkout -P htdocs;
exit;
```

**Note:** cvs ID

```

web crontab(1) 가 :
```

```

# Check out the web data as biba/low every twelve hours:
0 */12 * * * web /home/web/checkout.sh
```

```

12 HTML
```

```

biba/low
/usr/local/etc/rc.d/apache.sh :
```

```

command="setpmac biba/low /usr/local/sbin/httpd"
```

```

Apache biba/low biba/low
가 "access
denied"
```

**Note:** docroot 가 /home/web/htdocs  
Apache

PID, Scoreboardfile, DocumentRoot, log

. *biba* *biba/low*가

## 15.16 MAC

가

:

### 15.16.1 / *multilabel*

*mltilabel* 가 root(/)

50 가

root /etc/fstab *ro*

/ tunefs -*l enable*

mount -*urw* / /etc/fstab *ro rw*

root mount

### 15.16.2 MAC

### Xfree86

MAC

Xfree86

MAC :  
; 가 *insecure* 가  
*default* cap\_mkdb  
. , XFree86 /dev

TrustedBSD (<http://www.trustedbsd.org/>) TrustedBSD  
FreeBSD  
(<http://lists.freebsd.org/mailman/listinfo/freebsd-questions>)