

NAME

mac_test - MAC framework testing policy

SYNOPSIS

To compile the testing policy into your kernel, place the following lines in your kernel configuration file:

```
options MAC
options MAC_TEST
```

Alternately, to load the testing module at boot time, place the following line in your kernel configuration file:

```
options MAC
```

and in loader.conf(5):

```
mac_test_load="YES"
```

DESCRIPTION

The **mac_test** policy module implements a testing facility for the MAC framework. Among other things, **mac_test** will try to catch corrupt labels the system is attempting to destroy and drop to the debugger. Additionally, a set of statistics regarding the number of times various MAC framework entry points have been called is stored in the *security.mac.test* sysctl(8) tree.

Label Format

No labels are defined for **mac_test**.

SEE ALSO

mac(4), mac_biba(4), mac_bsextended(4), mac_ddb(4), mac_ifoff(4), mac_lomac(4), mac_mls(4), mac_none(4), mac_partition(4), mac_portacl(4), mac_seeotheruids(4), mac(9)

HISTORY

The **mac_test** policy module first appeared in FreeBSD 5.0 and was developed by the TrustedBSD Project.

AUTHORS

This software was contributed to the FreeBSD Project by Network Associates Labs, the Security Research Division of Network Associates Inc. under DARPA/SPAWAR contract N66001-01-C-8035 ("CBOSS"), as part of the DARPA CHATS research program.

BUGS

While the MAC Framework design is intended to support the containment of the root user, not all attack channels are currently protected by entry point checks. As such, MAC Framework policies should not be relied on, in isolation, to protect against a malicious privileged user.