NAME

ugidfw - firewall-like access controls for file system objects

SYNOPSIS

ugidfw add subject [**not**] [[**!**] **uid** *uid* | *minuid:maxuid*] [[**!**] **gid** *gid* | *mingid:maxgid*] [[**!**] **jailid** *jailid*] **object** [**not**] [[**!**] **uid** *uid* | *minuid:maxuid*] [[**!**] **gid** *gid* | *mingid:maxgid*] [[**!**] **filesys** *path*] [[**!**] **suid**] [[**!**] **sgid**] [[**!**] **uid_of_subject**] [[**!**] **gid_of_subject**] [[**!**] **type** *ardbclsp*] **mode** *arswxn*

ugidfw list

ugidfw set *rulenum* **subject** [**not**] [[**!**] **uid** *uid* | *minuid:maxuid*] [[**!**] **gid** *gid* | *mingid:maxgid*] [[**!**] **jailid** *jailid*] **object** [**not**] [[**!**] **uid** *uid* | *minuid:maxuid*] [[**!**] **gid** *gid* | *mingid:maxgid*] [[**!**] **filesys** *path*] [[**!**] **suid**] [[**!**] **sgid**] [[**!**] **uid_of_subject**] [[**!**] **gid_of_subject**] [[**!**] **type** *ardbclsp*] **mode** *arswxn*

ugidfw remove *rulenum*

DESCRIPTION

The **ugidfw** utility provides an ipfw(8)-like interface to manage access to file system objects by UID and GID, supported by the mac_bsdextended(4) mac(9) policy.

The arguments are as follows:

add subject ... **object** ... **mode** *arswxn*

Add a new rule, automatically selecting the rule number. See the description of **set** for syntax information.

list Produces a list of all the current **ugidfw** rules in the system.

set *rulenum* **subject** ... **object** ... **mode** *arswxn*

Add a new rule or modify an existing rule. The arguments are as follows:

rulenum Rule number. Entries with a lower rule number are applied first; placing the most frequently-matched rules at the beginning of the list (i.e., lower-numbered) will yield a slight performance increase.

subject [**not**] [[**!**] **uid** *uid* | *minuid:maxuid*] [[**!**] **gid** *gid* | *mingid:maxgid*] [[**!**] **jailid** *jailid*]

Subjects performing an operation must match all the conditions given. A leading **not** means that the subject should not match the remainder of the specification. A condition may be prefixed by **!** to indicate that particular condition must not match the subject. The subject can be required to have a particular *uid* and/or *gid*. A range of uids/gids can be specified, separated by a colon. The subject can be required to be in a particular jail with the *jailid*.

object [**not**] [[**!**] **uid** *uid* | *minuid:maxuid*] [[**!**] **gid** *gid* | *mingid:maxgid*] [[**!**] **filesys** *path*] [[**!**] **suid**] [[**!**] **sgid**] [[**!**] **uid_of_subject**] [[**!**] **gid_of_subject**] [[**!**] **type** *ardbclsp*]

The rule will apply only to objects matching all the specified conditions. A leading **not** means that the object should not match all the remaining conditions. A condition may be prefixed by **!** to indicate that particular condition must not match the object. Objects can be required to be owned by the user and/or group specified by *uid* and/or *gid*. A range of uids/gids can be specified, separated by a colon. The object can be required to be in a particular filesystem by specifying the filesystem using **filesys**. Note, if the filesystem is unmounted and remounted, then the rule may need to be reapplied to ensure the correct filesystem id is used. The object can be required to have the **suid** or **sgid** bits set. The owner of the object can be required to match the **uid_of_subject** or the **gid_of_subject** attempting the operation. The type of the object can be restricted to a subset of the following types.

a	any file type
r	a regular file
d	a directory
b	a block special device
c	a character special device
l	a symbolic link
s	a unix domain socket
p	a named pipe (FIFO)

mode *arswxn*

Similar to chmod(1), each character represents an access mode. If the rule applies, the specified access permissions are enforced for the object. When a character is specified in the rule, the rule will allow for the operation. Conversely, not including it will cause the operation to be denied. The definitions of each character are as follows:

a	administrative operations
r	read access
s	access to file attributes
w	write access
x	execute access
n	none

remove *rulenum*

Disable and remove the rule with the specified rule number.

SEE ALSO

mac_bsdextended(4), mac(9)

HISTORY

The **ugidfw** utility first appeared in FreeBSD 5.0.

AUTHORS

This software was contributed to the FreeBSD Project by NAI 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.