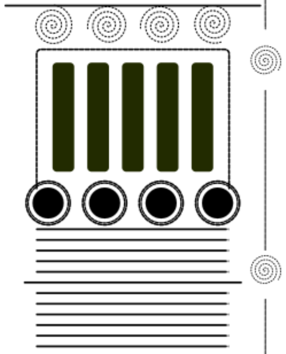
FreeBSD Jails - Part III

Man Pages
jail.conf(5) zfs-jail, zfs-unjail(8)
jail(8) jexec(8)

Core Parameters, Continued from Part II

allow.* -> **some restrictions of the jail environment may be set on per jail basis.**



allow.set_hostname

by default is off and when set, jails hostname can be changed via hostname(1) or sethostname(3).

allow.raw_sockets

settings this parameter allows utilities like ping(8) and traceroute(8) to operate inside jail, **be cautious with this one.**

allow.chflags

chflags treats privileged users inside jail as unprivileged, when this parameter is set, such users treated as privileged users, and may manipulate system file flags.

allow.mount

when set privileged users will be able to mount and unmount file system types marked as jail-friendly, read lsvfs(1) for available file system, enforce_statfs should be lowered than 2

allow.mount.devfs

privileged users inside jails can mount & unmount devfs file system, this permission only effective together with allow.mount and enforce_statfs is set to lower than 2

allow.quotas

The jail root may administer quotas on the jails filesystem.

allow.read_msgbuf

Jails users may read kernel message buffer, if the security.bsd.unprivileged_read_msgbuf MIB entry is zero.

allow.socket_af

sockets within jail are normally restricted to IPv4, Ipv6, local(UNIX) and route. this allows access to other protocol stacks that have not jail functionality added to them

allow.mlock

locking or unlocking physical pages in memory are not availble in jail, when this is set user may mlock(2) or munlock(2) memory, make sure to verify security.bsd.unprivileged_mlock

allow.reserved_ports

Jail root may bind to ports lower than 1024

allow.unprivileged_proc_debug

unprivileged process in the jail may use debugging facilities

allow.suser

The super-user will be disabled automatically if it's parent system has it disabled, by default is enabled.