FreeBSD - Jails *Part-I*

/jail — Choose jail path

- completejail
- servicejail

Ways to install Jail

- From Internet
- From ISO
- From Source

jail.conf

Jails config file

Man Pages

jail(8), jexec(8), jls(8), jail.conf(5) jail(2)
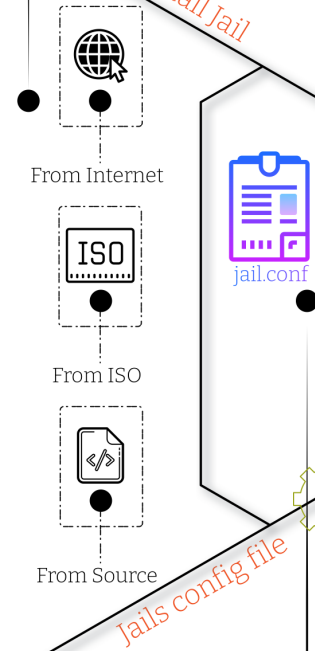
jail(8)

Use this utility to create new jails or modify or remove existing jails

jail is specified using parameters either on command line or in jail.conf(5) file

Parameters

True jail parameters
Passed to kernel when jail is created

Pseudo-parameters
Only used by jail itself

Core parameters and kernel modules can add their own parameters

To view use
"sysctl –d security.jail.param"

Parameters not set will be given default value

Core parameters

jid
Jail identifier, assigned automatically to new jail, or can be explicitly set

name
Jail name, arbitrary string that identifies jail, may not contain '.'

path
Root directory of jail, any command run inside jail either by jail(8) or jexec(8) are run from this directory

ipv4.addr
List of ip addresses assigned to jail, set this to restrict jail to use only these addresses. For ipv4 first ip address given will be used as source address

ipv4.saddrsel
Boolean option to disable ipv4 source address selection for the jail which is enabled by default for all jails

ipv4
Control the availability of ipv4 addresses, possible values are "inhirit", "new" and "disable"

ipv6.addr, ipv6.saddrsel, ip6
Counterparts of ip4.addr, ip4.saddrsel and ip4

vnet
Create jail with it's own virtual network stack, kernel must compiled with VIMAGE option, possible values are "inherit", "new" to create new network stack

host.hostname
Hostname of jail, similar parameters are, host.domainname, host.hostuuid and host.hostid

host
Set the origin of hostname and related information, possible values "inherit" and "new"

securelevel
Value of jails kern.securelevel systel, jail never has lower securelevel than its parent, but can set to higher level

devfs_ruleset
The number of the devfs ruleset that is enforced for mounting devfs in jail, value 0 is default means no ruleset is enforced

General syntax of jail definition In jail.conf

```
jailname {
        parameter = "value";
        …
}

ip4.addr = 192.168.10.10;
path = "/jail/firstjail"

// basics of C programming
// will help with syntax guide
```
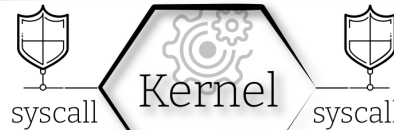
jail()
This system call sets up jail and locks process in it

jail_set()
This system call create new jail or modify existing one and optionally lock process in it

Kernel
syscall   syscall

jail_get()
This system call retrieves jail parameters

jail_attach()
This system call attaches current process to an existing jail, identified by jail id

jail_remove()
This system call removes jail, identified by jail id