

## Re: Jailed sysvipc implementation.

**Source:** <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/arch/2003-06/0306.html>

---

**From:** Dmitry Sivachenko (*demon\_at\_FreeBSD.org*)

**Date:** 06/25/03

Date: Wed, 25 Jun 2003 19:46:27 +0400

To: Pawel Jakub Dawidek <nick@garage.freebsd.pl>

On Wed, Jun 25, 2003 at 05:31:53PM +0200, Pawel Jakub Dawidek wrote:

> *On Wed, Jun 25, 2003 at 07:21:19PM +0400, Dmitry Sivachenko wrote:*

> > > > *But you got still \*one\* memory zones for every jail and main host.*

> > > >

> > > > *Yes, that is exactly what I want.*

> > > > *This is similar to separate IP stack for each jail: this is more powerful*

> > > > *solution, but more expensive (uses more kernel memory).*

> > >

> > > *But note that my implementation allocates memory "on demand".*

> > >

> > > *This is part of the problem: with single memory zone for all jails,*

> > > *less memory is allocated. With private memory zones, if  $m$  jails use IPC,*

> > > *you need to allocate  $m * M$  kbytes (for some value of  $M$  you consider*

> > > *sufficient for one jail).*

> > >

> > > *With one memory zone for all jails, it is enough to allocate  $N$  kbytes where*

> > >  *$M < N < m * M$ , because every jail will not use all  $M$  kbytes at the same time.*

>

> *Of course, but please. We could start wondering if struct prison in every*

> *ucred struct don't consume to much memory. Of course we allocate more memory,*

Common sence is your friend.

> *but if we want to run for example two instants of postgresql in two*

> *diffrent jails?*

I propose to add additional checks for `p->p_prison`. If two different users (with different UIDs) can use IPC, then it is simple to allow processes from different jails to use it too (and do not interfere with each other).

>

> *But ok, it will be good compromise to add `sysctl security.jail.privipc` IMHO.*

> *So we could turn this feature on if it is needed. What is your opinion?*

>

My point of view is that allowing jailed processes to safely use single

freebsd-arch: Re: Jailed sysvipc implementation.

memory zone is simple and sufficient solution.

---

freebsd-arch@freebsd.org mailing list

<http://lists.freebsd.org/mailman/listinfo/freebsd-arch>

To unsubscribe, send any mail to "freebsd-arch-unsubscribe@freebsd.org"