Subject: [RFC][patch 0/3] Network container subsystem - bind filtering
Posted by Daniel Lezcano on Tue, 04 Sep 2007 17:00:22 GMT
View Forum Message <> Reply to Message

Paul Menage mentionned, a few weeks ago, he wanted a bind filtering
for containers. Here it is :)

The following patches are a proposition to bring IP isolation to a container.

After looking more closely at the code I found that security hooks are
at the right place to catch socket calls. The IP isolation relies on the
security hooks and that has the advantage of not having the kernel code modified,
(expect container.h and makefile/kconfig), the patchset provide just a new
file container_network.c

Roughly, a container has a subsystem for the network (only ipv4).
This subsystem contains the list of the addresses allowed to be used by the
container. If a container tries to bind to an address not contained into
this list, the bind will fail with EPERM. Of course the bind is allowed to
INADDR_ANY.

If this approach is ok for everyone, I can extend the bind filtering to
consolidate the IP isolation.

Regards.

--
____
Containers mailing list
Containers@lists.linux-foundation.org
https://lists.linux-foundation.org/mailman/listinfo/containers