Subject: selinux mini-summit sub-policy topic
Posted by serue on Thu, 17 Apr 2008 17:55:30 GMT
View Forum Message <> Reply to Message

Hi,

It appears many of us have a related policy issue.

The Fedora folks want to be able to create distro images under a chroot or namespace with selinux enforcing, but with the distro images having different policy from the host. I don't know whether they want to be able to run tests under that image, or only be able to write down potentially unknown labels so as to be able to lay the image down on disk.

The fmac (opensolaris) folks may want to be able to load different policies in different zones.

The linux containers folks (and I) want basically the same thing as zones folks, that, is to support container administrators loading their own policy. My plan had been to pull together what I can to propose a LISA paper, so I was hoping to really get geared up this week after finishing other papers. (This is free time stuff, and has been on the back burner for a year now.) In the containers case, I am starting to use the type namespace (container1.subtype1) to confine a container policy, where subtype1 in container1 is known to the host as container1.subtype1. This leaves MLS and MCS unsupported ATM.

Dan Walsh is working policy for xen/qemu images, however that is not really related as the vm has its own OS. I'm mentioning it here in case I'm wrong.

Are there other projects needing similar support? There used to be a problem with rpms being able to create files with not-yet-defined types, which may be more similar to the fedora problem above, and I have no idea whether/how that ended up being resolved.

Is it worth proposing a joint topic for discussion at the selinux mini-summit? It could take several formats, from a meeting amongst ourselves followd by a panel discussion, to a set of lightning talks, to a 30 minute joint presentation where we present what we talk about in emails before OLS.

thanks,
-serge

_____
Containers mailing list
Containers@lists.linux-foundation.org