Subject: Why is SELinux incompatible with OpenVZ?
Posted by cwebster on Sun, 09 Jan 2011 20:27:57 GMT
View Forum Message <> Reply to Message

I've got a CentOS 5 development server where several developers need to periodically run instances of a real-time application. Each instance expects to be the only one running on the machine. Multiple instances will collide.

Since this is a low-end server and target archtecture is identical to development host, OpenVZ would seem to be the most resource-efficient virtualization tool.

The problem is that this development server is required by security policy to run SELinux. I don't need to run SELinux within the containers, only on the develoment server host.

I've done a lot of googling and searching various forums but I can find no specific reasons why OpenVZ is incompatible with SELinux.

Please explain the impact of setting up SELinux in an OpenVZ kernel. Why can't I re-build an OpenVZ kernel with support for SELinux and enable it to use our required policies?

Thanks in advance for any information, suggestions, useful links, etc.

Subject: Re: Why is SELinux incompatible with OpenVZ?
Posted by thewanderer on Tue, 11 Jan 2011 21:26:33 GMT
View Forum Message <> Reply to Message

OpenVZ introduces many hacks to the kernel. If you read the code, you'll know what this is about. However, Linux Containers are compatible with SELinux. I'd suggest trying that - you do not have to use OpenVZ for separation when you secure LXC with SELinux (as described in an IBM tutorial: search the web for "secure linux containers cookbook"), and you make it available for the host as well.
I would not recommend running LXC without SELinux-secured containers, though - it's too easy to break out with CAP_SYS_ADMIN and init seems to need it on most distros.

Subject: Re: Why is SELinux incompatible with OpenVZ?
Posted by cwebster on Wed, 12 Jan 2011 16:48:41 GMT
View Forum Message <> Reply to Message

Forgive me if this reply gets posted more than once. My first [Submit Reply] did not seem to post anything but a rather vague message told me to "check my inbox for instructions". After 10 min. without an email I resubmitted this reply:

thewanderer wrote on Tue, 11 January 2011 16:26OpenVZ introduces many hacks to the kernel.

If you read the code, you'll know what this is about.

Thank you. I will look at the source. I just found it odd that there is no mention of this in docs or on the forum, only that it must be disabled. With network/system security being such a vital part of any connected system these days I'm surprised that this project has not found a way to work within SELinux constraints. Maybe it will be more clear to me after looking at the OpenVZ source, but it seems to me someone should be able to develop a policy module allowing it to function without breaking security.

Quote:However, Linux Containers are compatible with SELinux. I'd suggest trying that - you do not have to use OpenVZ for separation when you secure LXC with SELinux (as described in an IBM tutorial: search the web for "secure linux containers cookbook"), and you make it available for the host as well.
I would not recommend running LXC without SELinux-secured containers, though - it's too easy to break out with CAP_SYS_ADMIN and init seems to need it on most distros.

Thank you for your candor and the excellent suggestion and reference. I am reading through the "Secure Linux containers cookbook" now. This sounds like it will meet our development and security requirements better than OpenVZ.

Now that I'm aware of OpenVZ, however, I will feel compelled to revisit this question later. I find it difficult to tolerate unsolved mysteries.

Many thanks!