

## SELinux Feedback

As discussed on the IRC channel, I have asked a series of my colleagues questions about their knowledge of SELinux. Their Linux knowledge in general I would put as rating from above average to high. I have not specifically put what I believe their knowledge to be because this is going on a mailing list. The respondents names have been omitted to protect the innocent.

It should be well noted the following problems with this survey -

- a) Its about as scientific as a monkey peeling a banana.
- b) The answers may be biased because all the people are in the same company and thus have more or less the same agenda.
- c) The questions that I asked could be wrong.
- d) The sample is far far too small.

Question	Respondent 1	Respondent 2	Respondent 3	Respondent 4
<p><b>If you installed Fedora regarding SELinux would you</b></p> <p><b>a) Disable it on install</b></p> <p><b>b) permissive on install</b></p> <p><b>c) enforcing on install.</b></p>	<p>i would probably have to activley choose to use selinux, so would disable if I didn't plan on definatley using it</p>	<p>I was going to say that I'd leave it disabled because I'd be under the impression that it'd cause niggley problems which I'd like logged in the hope that I'd enable it eventually.</p> <p>In fact, I think if I was going through the install and thinking about the options I'd most likely enable it and deal with the issues now that I now how to (pretty much)</p>	<p>oh right, ha, probably disable because i don't see any necessity for it ever</p>	<p>enforcing</p>
<p><b>Why would you choose that option?</b></p>	<p>haven't had the personal experience with it to fully appreciate what it does, and so tend to find it gets in the way more than it helps.</p>	<p>-- Answered above in some fashion. --</p>	<p>because there are sufficient security measures that can be taken by other means, pam, hosts.deny and .allow, iptables</p>	<p>reasonably familiar with SELinux and happy with what it achieves for my server security</p>

<p><b>Specifically what is SELinux meant to do?</b></p>	<p>I would describe it as an advanced extension of the security infrastruc in linux. It essentially allows you to put more limits in place than on a standard box.</p>	<p>Allow you to control what can be done on the system to a very complex level, allowing nothing by default except for what you specify</p>	<p>it's for setting up system wide security policies</p>	<p>add an extra layer of security between the server and the code running on it.... possibly ;)</p>
<p><b>Out of five, (five being very sufficient, 0 being completely insufficient) where would you put standard UNIX permissions (rwx, setuids and acls) for security on a machine? First for desktops second for servers.</b></p>	<p>4 and 3</p>	<p>5 and 4</p>	<p>4 and 3</p>	<p>3 and 2</p>