

Re: Spamassassin emails have wrong perms -- CC'ed to selinux list]

Source: <http://linux.derkeiler.com/Mailing-Lists/Fedora/2006-01/msg05035.html>

- *From:* "Justin Willmert" <justin@xxxxxxxxxxx>
 - *Date:* Tue, 31 Jan 2006 12:20:49 -0600 (CST)
-

Justin Willmert wrote:

> Paul Howarth wrote:

>> On Sun, 2006-01-29 at 22:52 -0600, Justin Willmert wrote:

>>> Ivan Gyurdiev wrote:

>>>> I'm cc-ing this to the fedora-selinux-list. I think some of the
>>>> problems may be applicable there.

>>>>

>>>> OK, after some more testing, when I disable SELinux, many of the
>>>> errors go away. First of all, I get rid of the error message

>>>> saying user can not be found and with it the 'still running as

>>>> root' error. Second, it is able to access the bayes_journal file

>>>> (as long as normal unix permissions are right, which I've figured

>>>> out). So I guess the problem is an SELinux issue which I can't

>>>> solve. I'd attach some avc error messages, but I can't seem to

>>>> find any. I've looked in maillog, secure, and messages, but nothing.

>>>> Have you looked in the audit log, where all such messages are

>>>> usually found ?

>>>> /var/log/audit.log

>>>>

>>> Below is what showed up in audit/audit.log when I sent a message

>>> through

>>> spamassassin. I'm **really** rusty on SELinux...it's the one thing I

>>> have to deal with quite often that I haven't been able to learn how to

>>> use...it's so foreign to me. I've never looked in audit.log before: the

>>> avc messages used to show up in messages, but now as far back as my

>>> logs

>>> go, I don't have a single avc message. This all looks like jibberish to

>>> me, so I need your guy's help.

>>>

>>> Thanks,

>>> Justin

>>>

>>> type=AVC msg=audit(1138596151.681:104174): avc: denied {

>>> name_connect } for pid=23796 comm="spamd" dest=389

>>> scontext=root:system_r:spamd_t

>>> tcontext=system_u:object_r:ldap_port_t tclass=tcp_socket

>>> < clipped >

>>>

Re: Spamassassin emails have wrong perms -- CC'ed to selinux list]

>> Are you using LDAP for authentication or to handle mail accounts?

>>

>> Paul.

> No, I am not using LDAP in spamassassin itself (there are ldap
> arguments to spamd and I'm not using those), but my system uses LDAP
> authentication through nsswitch/pam (whatever the distinction is).
> Does spamd need to know my ldap server's information?

>

> I believe I found a temporary work around for the bayes files: I put
> them in a non-standard location (/etc/mail/bayes/) because I wanted a
> system-wide database (some users don't get enough spam to warrant
> their own database). I found if I set /etc/mail/bayes/ to
> user_home_dir_t and /etc/mail/bayes/* to user_home_t that the denied
> messages for files are gone (if I'm reading the logs right). I don't
> see the file denial messages in the log output I put above, but they
> are in audit.log and in the latest test, they aren't there so I'm
> hoping I'm looking into all of this right. If you want me to confirm
> all of this, I can reset the directory context and do some tests, then
> set up the directory context again and compare that result, somebody
> just has to ask.
> Now I've just got to solve the LDAP messages. I'll try to look into
> this a bit, but I'm probably going to need the help, so thanks to all
> those who take time to reply.

>

> Justin

>

> --

> fedora-selinux-list mailing list

> fedora-selinux-list@xxxxxxxxxxx

> <https://www.redhat.com/mailman/listinfo/fedora-selinux-list>

>

I've got a question about how SELinux works underneath. I'm doing a lot of speculating based on the few things I think I know, so correct me when I'm wrong.

When SpamAssassin wants to get the user information, it probably uses a system call that is controlled through /etc/nsswitch.conf (I've seen the call before, but can't think of it off the top of my head). That in turn would connect to my LDAP server and authenticate the user and download its profile information. The nsswitch libraries would be in SpamAssassin's process space (if I understand linux programming correctly), so that would mean that if SpamAssassin is under an SELinux context, then the nsswitch libraries would be too. Would this be where I'm getting denied messages for ldap_port_t messages from?

If I've thought this through correctly and this is a problem, would somebody tell me so that I can post a bugzilla report? I'll search bugzilla later to make sure that it's not already in there (I've got to go to school so I don't really have time to do it right now).

Thanks to all those who've helped!

Re: Spamassassin emails have wrong perms -- CC'ed to selinux list]

Re: Spamassassin emails have wrong perms -- CC'ed to selinux list]

Justin

--

fedora-list mailing list

fedora-list@xxxxxxxxxxx

To unsubscribe: <https://www.redhat.com/mailman/listinfo/fedora-list>

- Prev by Date: [*DVD on Fedora 2*](#)
- Next by Date: [*slimserver and firewall*](#)
- Previous by thread: [*DVD on Fedora 2*](#)
- Next by thread: [*Dovecot problem ?!*](#)
- Index(es):
 - ◆ [*Date*](#)
 - ◆ [*Thread*](#)