SELinux - Bug #11608

Selinux prevents Console from working

08/28/2015 01:47 PM - Chris Edester

Status:	Closed		
Priority:	Normal		
Assignee:	Dominic Cleal		
Category:	General Foreman		
Target version:	1.9.2		
Difficulty:		**Fixed in Releases:**	
Triaged:		**Found in Releases:**	1.9.0
Bugzilla link:		**Red Hat JIRA:**	
Pull request:	https://github.com/theforeman/foreman-selinux/pull/52		

Description

After upgrading to Foreman 1.9 vnc consoles no longer work.
When I disable selinux the console works again.

With selinux on I get this error in foreman web ui:
Failed to set console: Permission denied - bind(2)

and this in the audit log:
type=SYSCALL msg=audit(1440783828.777:124): arch=c000003e syscall=49 success=no exit=-13 a0=10 a1=7f6bf0f27a08 a2=10 a3=1 items=0 ppid=1 pid=2784 auid=4294967295 uid=997 gid=995 euid=997 suid=997 fsuid=997 egid=995 sgid=995 fsgid=995 tty=(none) ses=4294967295 comm="ruby" exe="/opt/rh/ruby193/root/usr/bin/ruby" subj=system_u:system_r:passenger_t:s0 key=(null)

Could this be related to this recent change:
http://projects.theforeman.org/issues/10703

Does the selinx policy need to be updated to reflect the new random port binding?

Related issues:

Related to Foreman - Feature #10703: Randomize websockify port	**Closed**	**06/04/2015**

Associated revisions

Revision d3a9081b - 09/21/2015 04:25 AM - Dominic Cleal

fixes #11608 - permit Foreman/passenger_t to bind to VNC ports

During initialisation of the websockify process for consoles, Foreman
now binds to the VNC ports to check if they're free first.

History

#1 - 09/01/2015 04:36 AM - Dominic Cleal

If you're seeing the error in the web UI then it's more likely to be Foreman unable to talk to the compute resource as for the console, websockify runs in a separate process. If it was unable to bind then you'd not see the error in Foreman.

Can you try again to retrieve the AVC from the audit log? The line pasted is just a syscall and doesn't show precisely what's happening.

If you're using OpenStack then you're probably hitting #10443.

#2 - 09/01/2015 09:10 PM - Chris Edester

IT works when I turn off selinux:
setenforce 0

Then stops working again when selinux is enabled:
setenforce 1

Which makes me think its all selinux related.
Besides that, it all worked when I was on 1.8.x and only started acting up after the upgrade to 1.9.

I'm using the foreman installer, so there should be no abnormalities. Two systems with the same results:
One is OEL 7.1 and the other is CentOS 7.1

How can I better retrieve the audit log? I tail it and get that line only added when I click the console button.
I'm not using Openstack. I'm using VMware vsphere.

#3 - 09/01/2015 09:13 PM - Chris Edester

I also never see the websockify process spawned with ps...
This makes me think Foreman is denied to spawn it on the random port.

#4 - 09/02/2015 04:44 AM - Dominic Cleal

It could be a "dontaudit" rule if you're not getting an actual AVC message in the audit log (https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Security-Enhanced_Linux/sect-Security-Enhanced_Linux-Fixing_Problems-Possible_Causes_of_Silent_Denials.html shows how to re-enable auditing).

#5 - 09/16/2015 03:21 PM - Nicolas BOUCHARD

I have the same issue :
type=AVC msg=audit(1442430096.649:4670): avc: denied { name_bind } for pid=11869 comm="ruby" src=5919
scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:object_r:vnc_port_t:s0 tclass=tcp_socket

#6 - 09/16/2015 04:09 PM - Nicolas BOUCHARD

Adding this custom SELinux module solve the issue :

yum install -y selinux-policy-devel

cd /tmp/
cat <<EOF > foreman_addition.te
module foreman_addition 1.0;

require {
type passenger_t;
type vnc_port_t;
class tcp_socket { name_bind };
}

#============= passenger_t ==============
allow passenger_t vnc_port_t:tcp_socket name_bind;
EOF

make -f /usr/share/selinux/devel/Makefile foreman_addition.pp
semodule -i foreman_addition.pp

#7 - 09/17/2015 06:37 AM - Dominic Cleal

Thanks, that's useful data. Could you check the context of the websockify process? It's meant to be in a separate domain, websockify_t, which should have this rule already: https://github.com/theforeman/foreman-selinux/blob/develop/foreman.te#L352

```
[root@foreman ~]# ll -Z /usr/share/foreman/extras/noVNC/websockify.py
-rwxr-xr-x. root root system_u:object_r:websockify_exec_t:s0 /usr/share/foreman/extras/noVNC/websockify.py
```

That file should be websockify_exec_t. Run restorecon against it if not.

Next, when you load the console, the process should also be websockify_t. Run ps -efZ | grep websockify to check that.

#8 - 09/18/2015 04:24 AM - Nicolas BOUCHARD

[root@foreman ~]# ll -Z /usr/share/foreman/extras/noVNC/websockify.py
-rwxr-xr-x. root root system_u:object_r:websockify_exec_t:s0 /usr/share/foreman/extras/noVNC/websockify.py

[root@foreman ~]# ps -efZ | grep webso
system_u:system_r:websockify_t:s0 foreman 5600   1 0 10:20 ?   00:00:00 /usr/bin/python /usr/share/foreman/extras/noVNC/websockify.py --daem
on --idle-timeout=120 --timeout=120 5917 vmware-host:5925 --cert /var/lib/puppet/ssl/certs/foreman.xx.pem --key /var/lib

#9 - 09/18/2015 04:27 AM - Dominic Cleal

- Related to Feature #10703: Randomize websockify port added

#10 - 09/18/2015 04:28 AM - Dominic Cleal

- translation missing: en.field_release set to 88

Ah, I now see why is happening, there was a behaviour change in Foreman that I missed in #10703. Apologies!

The code now checks from the Foreman app whether the port is in use before trying to launch websockify, so both Foreman (passenger_t) and websockify need to be able to bind to the range of ports.

https://github.com/theforeman/foreman/blob/develop/lib/ws_proxy.rb#L28

#11 - 09/18/2015 04:32 AM - Dominic Cleal

- Status changed from New to Assigned

- Assignee set to Dominic Cleal

#12 - 09/18/2015 04:45 AM - The Foreman Bot

- Status changed from Assigned to Ready For Testing

- Pull request https://github.com/theforeman/foreman-selinux/pull/52 added

- Pull request deleted ()

#13 - 09/21/2015 05:01 AM - Dominic Cleal

- Status changed from Ready For Testing to Closed

- % Done changed from 0 to 100

Applied in changeset d3a9081be5811873bf7b0e4ca84a1adf6a5c946a.