SELinux - Bug #7719

Selinux prevents console from starting/connecting

09/27/2014 08:11 AM - Andreas Pfaffeneder

Status:	Closed		
Priority:	Normal		
Assignee:			
Category:	Compute resources		
Target version:	1.6.3		
Difficulty:		**Fixed in Releases:**	
Triaged:		**Found in Releases:**	1.6.0
Bugzilla link:	1151048	**Red Hat JIRA:**	
Pull request:	https://github.com/theforeman/foreman-selinux/pull/36		

Description

When setting selinux to enforcing, the console via websocket does not work any more.

Putting selinux into permissive, the connection works:

type=AVC msg=audit(1411818342.258:1286): avc: denied { getattr } for pid=5360 comm="ruby" path="/usr/bin/ssh" dev=dm-0 ino=403231 scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:object_r:ssh_exec_t:s0 tclass=file
type=AVC msg=audit(1411818342.266:1287): avc: denied { getcap } for pid=8868 comm="ruby" scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:system_r:passenger_t:s0 tclass=process
type=AVC msg=audit(1411818342.266:1288): avc: denied { setcap } for pid=8868 comm="ruby" scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:system_r:passenger_t:s0 tclass=process
type=AVC msg=audit(1411818342.266:1289): avc: denied { execute } for pid=8868 comm="ruby" name="ssh" dev=dm-0 ino=403231 scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:object_r:ssh_exec_t:s0 tclass=file
type=AVC msg=audit(1411818342.266:1289): avc: denied { read open } for pid=8868 comm="ruby" name="ssh" dev=dm-0 ino=403231 scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:object_r:ssh_exec_t:s0 tclass=file
type=AVC msg=audit(1411818342.266:1289): avc: denied { execute_no_trans } for pid=8868 comm="ruby" path="/usr/bin/ssh" dev=dm-0 ino=403231 scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:object_r:ssh_exec_t:s0 tclass=file
type=AVC msg=audit(1411818376.883:1290): avc: denied { name_bind } for pid=5382 comm="ruby" src=12276 scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:object_r:port_t:s0 tclass=udp_socket

[root@katello2 ~]# semodule -l|egrep -i 'foreman|katello|candlepin|pulp'
candlepin 1.0.0
foreman 1.6.0.1
pulp-server 2.4.0

abrt-daemon was uninstalled for testing purposes. This did not fix the problem.

Related issues:

Related to SELinux - Bug #7727: Ssh finish script does not work under Enforcing	**Rejected**	**09/29/2014**
Is duplicate of SELinux - Bug #7524: Adding libvirt compute resource ersults ...	**Duplicate**	**09/18/2014**

Associated revisions

Revision b696bcf7 - 10/21/2014 03:51 AM - Lukas Zapletal

Fixes #7719 - added ssh rules for libvirt CR

Revision 9fb84170 - 10/21/2014 03:51 AM - Lukas Zapletal

Refs #7719 - added websockify rules for VNC console

Revision 016e15c5 - 10/21/2014 04:26 AM - Lukas Zapletal

Refs #7719 - explicitly create .ssh dir in home

History

#1 - 09/27/2014 06:20 PM - Anonymous

- Category set to 56

#2 - 09/27/2014 06:56 PM - Stephen Benjamin

Is there any more in the audit log? That looks like passenger is using ssh there (maybe for a finish script?) I'm not 100% sure.

I ask if there's more in the audit log, because if this is Katello, I do see an issue that we've now enabled encrypted websockets but not given access to the Katello cert and keys -- I see denials for that on my instance.

#3 - 09/27/2014 07:16 PM - The Foreman Bot

- Status changed from New to Ready For Testing

- Target version set to 1.7.3

- Pull request https://github.com/theforeman/foreman-selinux/pull/34 added

- Pull request deleted ()

#4 - 09/28/2014 02:30 PM - Andreas Pfaffeneder

I modified the /usr/share/doc/foreman-selinux-1.6.0/foreman.te and added the line in the pull at 283:

apache_search_config(websockify_t)
corenet_tcp_bind_generic_node(websockify_t)
corenet_tcp_connect_vnc_port(websockify_t)
corenet_tcp_bind_vnc_port(websockify_t)
dev_read_urand(websockify_t)
kernel_read_system_state(websockify_t)
logging_send_syslog_msg(websockify_t)
miscfiles_read_localization(websockify_t)
miscfiles_read_certs(websockify_t)
sysnet_read_config(websockify_t)
abrt_stream_connect(websockify_t)
read_files_pattern(websockify_t, puppet_var_lib_t, puppet_var_lib_t)

The version was incrimented to 1.6.0.2:
[root@katello2 foreman-selinux-1.6.0]# semodule -l|egrep -i 'foreman|katello|candlepin|pulp'
candlepin 1.0.0
foreman 1.6.0.2
pulp-server 2.4.0

Same result as earlier, no connection possible, when setting to enforcing. But also no newer logs indicating selinux problems (AVC).

Just to make sure: I am talking about an qemu+ssh-connection to libvirt.

#5 - 09/29/2014 03:51 AM - Dominic Cleal

- Project changed from Foreman to SELinux

- Category changed from 56 to Compute resources

- Status changed from Ready For Testing to New

- Target version deleted (1.7.3)

#6 - 09/29/2014 04:41 AM - Stephen Benjamin

Have you trusted the Katello CA certificate in your browser? That should fix the encrypted web sockets.

If you're using the latest 2.0 installer, you should see a copy in the /pub directory on the web server:

http://katello.example.com/pub/katello-default-ca.crt

Otherwise it's also in /etc/pki/katello.

Try trusting that and then viewing the console.

For qemu+ssh, I think the only ssh connection it will make is on the initial host pages when it's loading the power buttons -- I think that's where those denials came from and might be a separate issue to look at.

#7 - 09/29/2014 04:42 AM - Lukas Zapletal

This looks really like issue for the ssh finish script, because websockify runs in its own domain.

I think we need to define our own ssh domain from policy/modules/services/ssh.if: ssh_basic_client_template and backport this for RHEL6 where there is no such an interface (I suppose).

#8 - 09/29/2014 04:45 AM - Lukas Zapletal

Andreas, can you paste us the denials when you run in Enforcing and the console does not work? The output above does not refer to the websockets at all. It looks like a different issue.

#9 - 09/29/2014 04:45 AM - Andreas Pfaffeneder

Trusting the /etc/pki/katello/certs/katello-default-ca.crt in my browser (FF32.0.3/Windows 7) did not change the behavior.

#10 - 09/29/2014 04:47 AM - Lukas Zapletal

- Related to Bug #7727: Ssh finish script does not work under Enforcing added

#11 - 09/29/2014 04:51 AM - Stephen Benjamin

I created #7729 for the websockets Katello issue

#12 - 09/29/2014 04:52 AM - The Foreman Bot

- Status changed from New to Ready For Testing

- Target version set to 1.7.3

#13 - 09/29/2014 05:00 AM - Andreas Pfaffeneder

type=AVC msg=audit(1411981245.749:98): avc: denied { getattr } for pid=2169 comm="ruby" path="/usr/bin/ssh" dev=dm-0 ino=403231 scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:object_r:ssh_exec_t:s0 tclass=file
type=AVC msg=audit(1411981245.754:99): avc: denied { getcap } for pid=3023 comm="ruby" scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:system_r:passenger_t:s0 tclass=process
type=AVC msg=audit(1411981245.755:100): avc: denied { setcap } for pid=3023 comm="ruby" scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:system_r:passenger_t:s0 tclass=process
type=AVC msg=audit(1411981245.755:101): avc: denied { execute } for pid=3023 comm="ruby" name="ssh" dev=dm-0 ino=403231 scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:object_r:ssh_exec_t:s0 tclass=file
type=AVC msg=audit(1411981245.755:101): avc: denied { read open } for pid=3023 comm="ruby" name="ssh" dev=dm-0 ino=403231 scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:object_r:ssh_exec_t:s0 tclass=file
type=AVC msg=audit(1411981245.755:101): avc: denied { execute_no_trans } for pid=3023 comm="ruby" path="/usr/bin/ssh" dev=dm-0 ino=403231 scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:object_r:ssh_exec_t:s0 tclass=file
type=AVC msg=audit(1411981245.849:102): avc: denied { search } for pid=3023 comm="ssh" name=".ssh" dev=dm-0 ino=2740965 scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:object_r:ssh_home_t:s0 tclass=dir
type=AVC msg=audit(1411981245.863:103): avc: denied { getattr } for pid=3023 comm="ssh" path="/usr/share/foreman/.ssh" dev=dm-0 ino=2740965 scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:object_r:ssh_home_t:s0 tclass=dir
type=AVC msg=audit(1411981245.863:104): avc: denied { read } for pid=3023 comm="ssh" name="id_rsa" dev=dm-0 ino=2741223 scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:object_r:ssh_home_t:s0 tclass=file
type=AVC msg=audit(1411981245.863:104): avc: denied { open } for pid=3023 comm="ssh" name="id_rsa" dev=dm-0 ino=2741223 scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:object_r:ssh_home_t:s0 tclass=file
type=AVC msg=audit(1411981245.864:105): avc: denied { getattr } for pid=3023 comm="ssh" path="/usr/share/foreman/.ssh/id_rsa" dev=dm-0 ino=2741223 scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:object_r:ssh_home_t:s0 tclass=file

#14 - 09/29/2014 05:11 AM - Lukas Zapletal

Thanks, Andreas. Now, can you describe what actually does not work? The issue is named "Selinux prevents console from starting/connecting" but here I see different scenario. This really looks like you try to spawn a libvirt instance via qemu+ssh?

#15 - 09/29/2014 06:11 AM - Andreas Pfaffeneder

- File foreman-debug-Ko4Ty.tar.xz added

Added foreman-debug-outfile.

#16 - 09/29/2014 06:22 AM - Andreas Pfaffeneder

Lukas Zapletal wrote:

> Thanks, Andreas. Now, can you describe what actually does not work? The issue is named "Selinux prevents console from starting/connecting" but here I see different scenario. This really looks like you try to spawn a libvirt instance via qemu+ssh?

Whats really not working:

Seting up a new VM via Katello2/Foreman1.6 works, but I can not connect to the console via web-ui.

#17 - 09/30/2014 11:14 AM - Dominic Cleal

- Target version changed from 1.7.3 to 1.7.2

#18 - 10/09/2014 07:42 AM - Lukas Zapletal

Unfortunately, I have NO idea why this runs ssh binary. From what I've seen the ruby ssh client library is pure ruby. It should definitely not try to spawn a ssh binary. I have the very same version of the rubygem-net-ssh and I don't get this behavior at all.

#19 - 10/09/2014 09:02 AM - Lukas Zapletal

Ok finally, thank to Jason Montleon, we managed to reproduce. Those are thrown when passenger is being restarted, not when you try to access the console!

```
type=AVC msg=audit(1412859490.009:2650): avc:  denied  { getattr } for  pid=97840 comm="ruby" path="/usr/bin/s
sh" dev="dm-0" ino=268713866 scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:object_r:ssh_exec_t:s
0 tclass=file
type=SYSCALL msg=audit(1412859490.009:2650): arch=c000003e syscall=4 success=no exit=-13 a0=7f051c2a4c60 a1=7f
052420d8d0 a2=7f052420d8d0 a3=3 items=0 ppid=97752 pid=97840 auid=4294967295 uid=996 gid=995 euid=996 suid=996
 fsuid=996 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)
type=AVC msg=audit(1412859491.662:2651): avc:  denied  { getattr } for  pid=97819 comm="ruby" path="/usr/bin/s
sh" dev="dm-0" ino=268713866 scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:object_r:ssh_exec_t:s
0 tclass=file
type=SYSCALL msg=audit(1412859491.662:2651): arch=c000003e syscall=4 success=no exit=-13 a0=7f051c2aff30 a1=7f
052420d8d0 a2=7f052420d8d0 a3=3 items=0 ppid=97752 pid=97819 auid=4294967295 uid=996 gid=995 euid=996 suid=996
 fsuid=996 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)
type=AVC msg=audit(1412859499.030:2652): avc:  denied  { getattr } for  pid=97819 comm="ruby" path="/usr/bin/s
sh" dev="dm-0" ino=268713866 scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:object_r:ssh_exec_t:s
0 tclass=file
type=SYSCALL msg=audit(1412859499.030:2652): arch=c000003e syscall=4 success=no exit=-13 a0=7f051c41cfa0 a1=7f
052420d8d0 a2=7f052420d8d0 a3=3 items=0 ppid=97752 pid=97819 auid=4294967295 uid=996 gid=995 euid=996 suid=996
 fsuid=996 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)
type=AVC msg=audit(1412859499.376:2653): avc:  denied  { getattr } for  pid=97819 comm="ruby" path="/usr/bin/s
sh" dev="dm-0" ino=268713866 scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:object_r:ssh_exec_t:s
0 tclass=file
type=SYSCALL msg=audit(1412859499.376:2653): arch=c000003e syscall=4 success=no exit=-13 a0=7f051c38ba40 a1=7f
052420d8d0 a2=7f052420d8d0 a3=3 items=0 ppid=97752 pid=97819 auid=4294967295 uid=996 gid=995 euid=996 suid=996
 fsuid=996 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)
type=USER_ACCT msg=audit(1412859601.738:2654): pid=97908 uid=0 auid=4294967295 ses=4294967295 subj=system_u:sy
stem_r:crond_t:s0-s0:c0.c1023 msg='op=PAM:accounting acct="foreman" exe="/usr/sbin/crond" hostname=? addr=? te
rminal=cron res=success'
type=CRED_ACQ msg=audit(1412859601.739:2655): pid=97908 uid=0 auid=4294967295 ses=4294967295 subj=system_u:sys
tem_r:crond_t:s0-s0:c0.c1023 msg='op=PAM:setcred acct="foreman" exe="/usr/sbin/crond" hostname=? addr=? termin
al=cron res=success'
type=LOGIN msg=audit(1412859601.742:2656): pid=97908 uid=0 subj=system_u:system_r:crond_t:s0-s0:c0.c1023 old-a
uid=4294967295 auid=996 old-ses=4294967295 ses=219 res=1
```

```
require {
        type ssh_exec_t;
        type passenger_t;
        class process setcap;
        class file { read getattr open execute execute_no_trans };
}

#============= passenger_t ==============
allow passenger_t self:process setcap;
allow passenger_t ssh_exec_t:file { read getattr open execute execute_no_trans };
```

#20 - 10/09/2014 09:27 AM - Lukas Zapletal

- Is duplicate of Bug #7524: Adding libvirt compute resource ersults in error added

#21 - 10/09/2014 09:28 AM - Lukas Zapletal

Ok problem solved I think, it was during restart because I had my noVNC console opened. It's the libvirt who is spawning the ssh directly (tunneling). I will create new rules for this. Thanks for the report, it was really helpful.

#22 - 10/09/2014 09:36 AM - Lukas Zapletal

- Status changed from Ready For Testing to Assigned

- Bugzilla link set to 1151048

- Pull request added

- Pull request deleted (https://github.com/theforeman/foreman-selinux/pull/34)

#23 - 10/09/2014 10:14 AM - The Foreman Bot

- Status changed from Assigned to Ready For Testing

- Pull request https://github.com/theforeman/foreman-selinux/pull/36 added

- Pull request deleted ()

#24 - 10/10/2014 04:13 AM - Andreas Pfaffeneder

Tried with the latest foreman-selinux-branch (libvirt-ssh-7719):

[root@katello2 ~]# #git clone https://github.com/lzap/foreman-selinux.git -b libvirt-ssh-7719
[root@katello2 ~]# #cd foreman-selinux/
[root@katello2 ~]# #rake pkg:load host=katello2.zuhause-local.de distro=rhel6
[root@katello2 ~]# #reboot

[root@katello2 ~]# semodule -l|egrep -i 'foreman|katello|candlepin|pulp'
candlepin 1.0.0
foreman 99.9
katello 1.0
pulp-server 2.4.0

Problem still the same: opening a console with selinux=enforcing yields a "WebSock error: [object Event]", setting selinux=permissive makes it work.

No recent AVCs in audit.log.

#25 - 10/10/2014 09:59 AM - Lukas Zapletal

Andreas,

I get the very same error: WebSock error: [object Event].

But when I try to set Permissive, I still have the error. I saw several denials in the log in regard to websockify, passenger and ssh. Can you rebuild the policy without dontaudit:

semodule -DB

and then refresh the console and then

audit2allow -Ral || audit2allow -al

(paste me the output ^^^)

and put back the dontaudit mode:

semodule -B

I am not able to tell what is wrong.

#26 - 10/13/2014 02:57 AM - Andreas Pfaffeneder

semodule -DB, try to access console:

/var/log/audit/audit.log
type=AVC msg=audit(1413182319.822:4621): avc: denied { read } for pid=28531 comm="id" name="mls" dev=selinuxfs ino=12
scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:object_r:security_t:s0 tclass=file
type=AVC msg=audit(1413182319.822:4621): avc: denied { open } for pid=28531 comm="id" name="mls" dev=selinuxfs ino=12
scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:object_r:security_t:s0 tclass=file
type=SYSCALL msg=audit(1413182319.822:4621): arch=c000003e syscall=2 success=yes exit=4 a0=7fff74d67670 a1=0 a2=7fff74d6767c a3=0
items=0 ppid=28528 pid=28531 auid=4294967295 uid=498 gid=498 euid=498 suid=498 fsuid=498 egid=498 sgid=498 fsgid=498 tty=(none)
ses=4294967295 comm="id" exe="/usr/bin/id" subj=system_u:system_r:passenger_t:s0 key=(null)
type=AVC msg=audit(1413182327.505:4622): avc: denied { rlimitinh } for pid=28552 comm="websockify.py"
scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:system_r:websockify_t:s0 tclass=process
type=AVC msg=audit(1413182327.505:4622): avc: denied { siginh } for pid=28552 comm="websockify.py"
scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:system_r:websockify_t:s0 tclass=process
type=AVC msg=audit(1413182327.505:4622): avc: denied { noatsecure } for pid=28552 comm="websockify.py"
scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:system_r:websockify_t:s0 tclass=process
type=SYSCALL msg=audit(1413182327.505:4622): arch=c000003e syscall=59 success=yes exit=0 a0=7f481d55af58 a1=7f481d55ab50
a2=585d620 a3=7f4826a59f30 items=0 ppid=24049 pid=28552 auid=4294967295 uid=498 gid=498 euid=498 suid=498 fsuid=498 egid=498 sgid=498
fsgid=498 tty=(none) ses=4294967295 comm="websockify.py" exe="/usr/bin/python" subj=system_u:system_r:websockify_t:s0 key=(null)
type=AVC msg=audit(1413182329.175:4623): avc: denied { search } for pid=28552 comm="websockify.py" name="lib" dev=dm-0 ino=781826
scontext=system_u:system_r:websockify_t:s0 tcontext=system_u:object_r:var_lib_t:s0 tclass=dir
type=SYSCALL msg=audit(1413182329.175:4623): arch=c000003e syscall=4 success=yes exit=0 a0=1a46150 a1=7fffca8dcda0 a2=7fffca8dcda0
a3=7a2e326f6c6c6574 items=0 ppid=24049 pid=28552 auid=4294967295 uid=498 gid=498 euid=498 suid=498 fsuid=498 egid=498 sgid=498
fsgid=498 tty=(none) ses=4294967295 comm="websockify.py" exe="/usr/bin/python" subj=system_u:system_r:websockify_t:s0 key=(null)

audit2allow -Ral || audit2allow -al-Output:

```
require {
type sysstat_t;
type passenger_t;
type websockify_t;
class process { siginh rlimitinh noatsecure };
}

#============= passenger_t ==============
allow passenger_t websockify_t:process { siginh noatsecure rlimitinh };
selinux_get_enforce_mode(passenger_t)

#============= sysstat_t ==============
userdom_search_admin_dir(sysstat_t)

#============= websockify_t ==============
files_search_var_lib(websockify_t)
```

#27 - 10/13/2014 03:30 AM - Andreas Pfaffeneder

Adding above rules to the git df4d9d88afb6edc74c37072b3a15cb517eaa3547 makes my console work! :)

#28 - 10/13/2014 05:16 AM - Lukas Zapletal

I saw the exact denials on my host. I've added these to the patch, thanks.

#29 - 10/21/2014 04:22 AM - Dominic Cleal

- translation missing: en.field_release set to 27

#30 - 10/21/2014 05:01 AM - Anonymous

- Status changed from Ready For Testing to Closed

- % Done changed from 0 to 100

Applied in changeset b696bcf7fe8041d0ad950d41be0a65bd4f186e75.

Files

foreman-debug-Ko4Ty.tar.xz	628 KB	09/29/2014	Andreas Pfaffeneder