SELinux - Bug #6162

"WebSock error: [object Event]"

06/11/2014 12:25 PM - Jorick Astrego

Status:	Closed		
Priority:	High		
Assignee:	Lukas Zapletal		
Category:	Packaging		
Target version:	1.5.2		
Difficulty:	easy	**Fixed in Releases:**	
Triaged:		**Found in Releases:**	1.5.0
Bugzilla link:	1111592	**Red Hat JIRA:**	
Pull request:			

Description

After hooking up a libvirt server to foreman I'm unable to access the VNC console. I already checked everything from http://theforeman.org/manuals/1.5/index.html#7.1NoVNC but I still get the "WebSock error: [object Event]" error.

`grep AVC /var/log/audit/audit.log`

type=AVC msg=audit(1399456510.010:428): avc: denied { relabelto } for pid=5010 comm="ruby" name="yaml" dev=dm-0 ino=394367 scontext=unconfined_u:system_r:passenger_t:s0 tcontext=system_u:object_r:puppet_var_lib_t:s0 tclass=dir
type=AVC msg=audit(1399456510.053:429): avc: denied { relabelto } for pid=5010 comm="ruby" name="masterhttp.log" dev=dm-0 ino=264319 scontext=unconfined_u:system_r:passenger_t:s0 tcontext=system_u:object_r:puppet_log_t:s0 tclass=file
type=AVC msg=audit(1399456510.396:430): avc: denied { relabelto } for pid=5010 comm="ruby" name="ca_crt.pem" dev=dm-0 ino=395701 scontext=unconfined_u:system_r:passenger_t:s0 tcontext=system_u:object_r:puppet_var_lib_t:s0 tclass=file
type=AVC msg=audit(1399456511.688:433): avc: denied { execute } for pid=5216 comm="ruby" name="node.rb" dev=dm-0 ino=2364347 scontext=unconfined_u:system_r:passenger_t:s0 tcontext=system_u:object_r:puppet_etc_t:s0 tclass=file
type=AVC msg=audit(1399456511.688:433): avc: denied { execute_no_trans } for pid=5216 comm="ruby" path="/etc/puppet/node.rb" dev=dm-0 ino=2364347 scontext=unconfined_u:system_r:passenger_t:s0 tcontext=system_u:object_r:puppet_etc_t:s0 tclass=file
type=AVC msg=audit(1399458317.549:459): avc: denied { execute } for pid=6379 comm="ruby" name="node.rb" dev=dm-0 ino=2364347 scontext=unconfined_u:system_r:passenger_t:s0 tcontext=system_u:object_r:puppet_etc_t:s0 tclass=file
type=AVC msg=audit(1399458317.549:459): avc: denied { execute_no_trans } for pid=6379 comm="ruby" path="/etc/puppet/node.rb" dev=dm-0 ino=2364347 scontext=unconfined_u:system_r:passenger_t:s0 tcontext=system_u:object_r:puppet_etc_t:s0 tclass=file
type=AVC msg=audit(1399460122.486:479): avc: denied { execute } for pid=7554 comm="ruby" name="node.rb" dev=dm-0 ino=2364347 scontext=unconfined_u:system_r:passenger_t:s0 tcontext=system_u:object_r:puppet_etc_t:s0 tclass=file
type=AVC msg=audit(1399460122.486:479): avc: denied { execute_no_trans } for pid=7554 comm="ruby" path="/etc/puppet/node.rb" dev=dm-0 ino=2364347 scontext=unconfined_u:system_r:passenger_t:s0 tcontext=system_u:object_r:puppet_etc_t:s0 tclass=file
type=AVC msg=audit(1399462327.629:514): avc: denied { name_bind } for pid=6998 comm="ruby" src=18882 scontext=unconfined_u:system_r:passenger_t:s0 tcontext=system_u:object_r:port_t:s0 tclass=udp_socket
type=AVC msg=audit(1399620146.796:1033): avc: denied { getattr } for pid=3890 comm="ruby" path="/usr/bin/ssh" dev=dm-0 ino=2100741 scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:object_r:ssh_exec_t:s0 tclass=file
type=AVC msg=audit(1399620146.803:1034): avc: denied { getcap } for pid=18897 comm="ruby" scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:system_r:passenger_t:s0 tclass=process
type=AVC msg=audit(1399620146.803:1035): avc: denied { setcap } for pid=18897 comm="ruby" scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:system_r:passenger_t:s0 tclass=process
type=AVC msg=audit(1399620146.803:1036): avc: denied { execute } for pid=18897 comm="ruby" name="ssh" dev=dm-0 ino=2100741 scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:object_r:ssh_exec_t:s0 tclass=file
type=AVC msg=audit(1399620146.803:1036): avc: denied { read open } for pid=18897 comm="ruby" name="ssh" dev=dm-0 ino=2100741 scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:object_r:ssh_exec_t:s0 tclass=file
type=AVC msg=audit(1399620146.803:1036): avc: denied { execute_no_trans } for pid=18897 comm="ruby" path="/usr/bin/ssh" dev=dm-0 ino=2100741 scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:object_r:ssh_exec_t:s0 tclass=file
type=AVC msg=audit(1399898437.528:33): avc: denied { name_bind } for pid=1610 comm="ruby" src=26907 scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:object_r:port_t:s0 tclass=udp_socket

type=AVC msg=audit(1399902097.497:69): avc: denied { name_bind } for pid=3556 comm="ruby" src=27353 scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:object_r:port_t:s0 tclass=udp_socket
type=AVC msg=audit(1400484735.815:3319): avc: denied { name_bind } for pid=17619 comm="ruby" src=63129 scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:object_r:port_t:s0 tclass=udp_socket
type=AVC msg=audit(1400485968.143:3325): avc: denied { name_bind } for pid=8275 comm="ruby" src=61873 scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:object_r:port_t:s0 tclass=udp_socket
type=AVC msg=audit(1400486560.039:3356): avc: denied { name_bind } for pid=8956 comm="ruby" src=63357 scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:object_r:port_t:s0 tclass=udp_socket
type=AVC msg=audit(1400492728.366:3395): avc: denied { name_bind } for pid=8275 comm="ruby" src=18297 scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:object_r:port_t:s0 tclass=udp_socket
type=AVC msg=audit(1400495975.598:3414): avc: denied { name_bind } for pid=8275 comm="ruby" src=27615 scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:object_r:port_t:s0 tclass=udp_socket
type=AVC msg=audit(1400500022.536:3433): avc: denied { name_bind } for pid=14744 comm="ruby" src=8309 scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:object_r:port_t:s0 tclass=udp_socket
type=AVC msg=audit(1400662325.649:4356): avc: denied { name_bind } for pid=16953 comm="ruby" src=15183 scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:object_r:port_t:s0 tclass=udp_socket
type=AVC msg=audit(1400686537.521:4667): avc: denied { getattr } for pid=16953 comm="ruby" path="/usr/bin/ssh" dev=dm-0 ino=2100741 scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:object_r:ssh_exec_t:s0 tclass=file
type=AVC msg=audit(1400686537.529:4668): avc: denied { getcap } for pid=14945 comm="ruby" scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:system_r:passenger_t:s0 tclass=process
type=AVC msg=audit(1400686537.529:4669): avc: denied { setcap } for pid=14945 comm="ruby" scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:system_r:passenger_t:s0 tclass=process
type=AVC msg=audit(1400686537.531:4670): avc: denied { execute } for pid=14945 comm="ruby" name="ssh" dev=dm-0 ino=2100741 scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:object_r:ssh_exec_t:s0 tclass=file
type=AVC msg=audit(1400686537.531:4670): avc: denied { read open } for pid=14945 comm="ruby" name="ssh" dev=dm-0 ino=2100741 scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:object_r:ssh_exec_t:s0 tclass=file
type=AVC msg=audit(1400686537.531:4670): avc: denied { execute_no_trans } for pid=14945 comm="ruby" path="/usr/bin/ssh" dev=dm-0 ino=2100741 scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:object_r:ssh_exec_t:s0 tclass=file
type=AVC msg=audit(1402388176.141:13989): avc: denied { name_bind } for pid=16564 comm="ruby" src=62901 scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:object_r:port_t:s0 tclass=udp_socket
type=AVC msg=audit(1402482860.316:14646): avc: denied { getattr } for pid=16564 comm="ruby" path="/usr/bin/ssh" dev=dm-0 ino=2100741 scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:object_r:ssh_exec_t:s0 tclass=file
type=AVC msg=audit(1402482860.323:14647): avc: denied { getcap } for pid=1827 comm="ruby" scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:system_r:passenger_t:s0 tclass=process
type=AVC msg=audit(1402482860.324:14648): avc: denied { setcap } for pid=1827 comm="ruby" scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:system_r:passenger_t:s0 tclass=process
type=AVC msg=audit(1402482860.325:14649): avc: denied { execute } for pid=1827 comm="ruby" name="ssh" dev=dm-0 ino=2100741 scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:object_r:ssh_exec_t:s0 tclass=file
type=AVC msg=audit(1402482860.325:14649): avc: denied { read open } for pid=1827 comm="ruby" name="ssh" dev=dm-0 ino=2100741 scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:object_r:ssh_exec_t:s0 tclass=file
type=AVC msg=audit(1402482860.325:14649): avc: denied { execute_no_trans } for pid=1827 comm="ruby" path="/usr/bin/ssh" dev=dm-0 ino=2100741 scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:object_r:ssh_exec_t:s0 tclass=file
type=AVC msg=audit(1402483172.553:14650): avc: denied { name_bind } for pid=16564 comm="ruby" src=7772 scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:object_r:port_t:s0 tclass=udp_socket
type=AVC msg=audit(1402483332.186:14651): avc: denied { getcap } for pid=2212 comm="ruby" scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:system_r:passenger_t:s0 tclass=process
type=AVC msg=audit(1402483332.186:14652): avc: denied { setcap } for pid=2212 comm="ruby" scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:system_r:passenger_t:s0 tclass=process
type=AVC msg=audit(1402484542.323:14698): avc: denied { getattr } for pid=1957 comm="ruby" path="/usr/bin/ssh" dev=dm-0 ino=2100741 scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:object_r:ssh_exec_t:s0 tclass=file
type=AVC msg=audit(1402484542.332:14699): avc: denied { getcap } for pid=2893 comm="ruby" scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:system_r:passenger_t:s0 tclass=process
type=AVC msg=audit(1402484542.332:14700): avc: denied { setcap } for pid=2893 comm="ruby" scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:system_r:passenger_t:s0 tclass=process
type=AVC msg=audit(1402484542.334:14701): avc: denied { execute } for pid=2893 comm="ruby" name="ssh" dev=dm-0 ino=2100741 scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:object_r:ssh_exec_t:s0 tclass=file
type=AVC msg=audit(1402484542.334:14701): avc: denied { read open } for pid=2893 comm="ruby" name="ssh" dev=dm-0 ino=2100741 scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:object_r:ssh_exec_t:s0 tclass=file
type=AVC msg=audit(1402484542.334:14701): avc: denied { execute_no_trans } for pid=2893 comm="ruby" path="/usr/bin/ssh" dev=dm-0 ino=2100741 scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:object_r:ssh_exec_t:s0 tclass=file
type=AVC msg=audit(1402484588.441:14702): avc: denied { name_bind } for pid=1957 comm="ruby" src=25223 scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:object_r:port_t:s0 tclass=udp_socket
type=AVC msg=audit(1402488995.098:14726): avc: denied { getattr } for pid=5393 comm="ruby" path="/usr/bin/ssh" dev=dm-0 ino=2100741 scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:object_r:ssh_exec_t:s0 tclass=file

type=AVC msg=audit(1402488995.102:14727): avc: denied { execute } for pid=5535 comm="ruby" name="ssh" dev=dm-0 ino=2100741 scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:object_r:ssh_exec_t:s0 tclass=file
type=AVC msg=audit(1402488995.102:14727): avc: denied { read open } for pid=5535 comm="ruby" name="ssh" dev=dm-0 ino=2100741 scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:object_r:ssh_exec_t:s0 tclass=file
type=AVC msg=audit(1402488995.102:14727): avc: denied { execute_no_trans } for pid=5535 comm="ruby" path="/usr/bin/ssh" dev=dm-0 ino=2100741 scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:object_r:ssh_exec_t:s0 tclass=file

Associated revisions

Revision 93006b82 - 06/19/2014 10:14 AM - Lukas Zapletal

fixes #6162 - fixed websockify hidden denial

History

#1 - 06/11/2014 12:28 PM - Jorick Astrego

Forgot to add that I'm running version "foreman-1.5.0-1.el6.noarch"

#2 - 06/12/2014 07:54 AM - Lukas Zapletal

Hello,

I don't see any denials that have something to do with our VNC proxy. Can you do this for me:

```
ps auxwwwZ
```

and

```
ll -Z /usr/share/foreman/extras/noVNC
```

This is audit2allow:

```
#============= passenger_t ==============
allow passenger_t puppet_etc_t:file { execute execute_no_trans };

#!!!! This avc is allowed in the current policy
allow passenger_t puppet_log_t:file relabelto;

#!!!! This avc is allowed in the current policy
allow passenger_t puppet_var_lib_t:dir relabelto;

#!!!! This avc is allowed in the current policy
allow passenger_t puppet_var_lib_t:file relabelto;

allow passenger_t self:process { getcap setcap };
corenet_udp_bind_generic_port(passenger_t)
ssh_exec(passenger_t)
```

Dom, what is your opinion about last three rules?

The first one - it looks like some passenger magic (execmem soon? :-)

The second one - and we can see this from the audit.log as well - Foreman/Passenger really wants to bind random UDP ports. We've seen this already. Possible solutions - dontaudit, allowing ports (7k-64k), ignoring.

The third one - Foreman obviously uses ssh to do provisioning, but why do we see this denial today? Don't we have this feature for years now?

#3 - 06/12/2014 07:56 AM - Lukas Zapletal

Jorick, can you please tail -f the audit.log and then try to access the console. Paste me those lines which are added after the requrest. I really think this has noting to do with SELinux.

Also try "setenforce 0".

#4 - 06/12/2014 08:06 AM - Jorick Astrego

I updated to 1.6 nightly to get around some other bugs and it works now. I'll revert back to 1.5 stable later in the day and tail the audit.log for you

#5 - 06/12/2014 08:24 AM - Jorick Astrego

- File Selection_214.png added

- File Selection_213.png added

Sorry didn't have my first coffee yet, it worked because I switched of SELinux .... duh!

When I do setenforce 0, the console works... when trying with setenforce 1, it gives the websocket error.

But the strange part is there are no entries in audit.log except my setenforce

type=MAC_STATUS msg=audit(1402560931.564:71): enforcing=1 old_enforcing=0 auid=0 ses=4
type=SYSCALL msg=audit(1402560931.564:71): arch=c000003e syscall=1 success=yes exit=1 a0=3 a1=7fffda90ae60 a2=1 a3=7fffda909be0 items=0 ppid=2460 pid=2487 auid=0 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts1 ses=4 comm="setenforce" exe="/usr/sbin/setenforce" subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key=(null)
type=MAC_STATUS msg=audit(1402560954.603:72): enforcing=0 old_enforcing=1 auid=0 ses=4
type=SYSCALL msg=audit(1402560954.603:72): arch=c000003e syscall=1 success=yes exit=1 a0=3 a1=7fff3bd93d20 a2=1 a3=7fff3bd92aa0 items=0 ppid=2460 pid=2510 auid=0 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts1 ses=4 comm="setenforce" exe="/usr/sbin/setenforce" subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key=(null)
type=MAC_STATUS msg=audit(1402561131.706:73): enforcing=1 old_enforcing=0 auid=0 ses=4
type=SYSCALL msg=audit(1402561131.706:73): arch=c000003e syscall=1 success=yes exit=1 a0=3 a1=7fffa3775550 a2=1 a3=7fffa37742d0 items=0 ppid=2460 pid=2775 auid=0 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts1 ses=4 comm="setenforce" exe="/usr/sbin/setenforce" subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key=(null)
type=MAC_STATUS msg=audit(1402561141.312:74): enforcing=0 old_enforcing=1 auid=0 ses=4
type=SYSCALL msg=audit(1402561141.312:74): arch=c000003e syscall=1 success=yes exit=1 a0=3 a1=7fff8f976530 a2=1 a3=7fff8f9752b0 items=0 ppid=2460 pid=2780 auid=0 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts1 ses=4 comm="setenforce" exe="/usr/sbin/setenforce" subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key=(null)
type=MAC_STATUS msg=audit(1402561157.918:75): enforcing=1 old_enforcing=0 auid=0 ses=4
type=SYSCALL msg=audit(1402561157.918:75): arch=c000003e syscall=1 success=yes exit=1 a0=3 a1=7fff2ccfb700 a2=1 a3=7fff2ccfa480 items=0 ppid=2460 pid=2793 auid=0 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts1 ses=4 comm="setenforce" exe="/usr/sbin/setenforce" subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key=(null)

#6 - 06/12/2014 11:30 AM - Lukas Zapletal

Hello,

thanks for testing. Can you install foreman-selinux from nightly repo (you can mix and match this package without any issue), set Permissive (setenforce 0), then restart Foreman and try to tail audit log while trying to connect?

There is no denial in the listing you pasted above and SELinux should not hurt in this case. Also send me your "ps auxwwwZ" output.

Ping me on irc (FreeNode) my nick is "lzap".

#7 - 06/12/2014 11:47 AM - Jorick Astrego

I already have the latest foreman-selinux installed and "setenforce 0" works and "setenforce 1" fails consistently without anything in audit.log..... This makes no sense to me but I can reproduce everytime....

rpm -qa|grep foreman-selinux
foreman-selinux-1.6.0-0.develop.201405301314git8ad6a63.el6.noarch

There are only some lines added to audit.log when I restart the foreman service and try it the first time:

type=AVC msg=audit(1402573453.803:63): avc: denied { getattr } for pid=1843 comm="ruby" path="/usr/bin/ssh" dev=dm-0 ino=2100741 scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:object_r:ssh_exec_t:s0 tclass=file
type=SYSCALL msg=audit(1402573453.803:63): arch=c000003e syscall=4 success=yes exit=0 a0=7f0728195ed0 a1=7f0742e43e90 a2=7f0742e43e90 a3=d items=0 ppid=1815 pid=1843 auid=4294967295 uid=497 gid=497 euid=497 suid=497 fsuid=497 egid=497 sgid=497 fsgid=497 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(1402573453.807:64): avc: denied { getcap } for pid=1846 comm="ruby" scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:system_r:passenger_t:s0 tclass=process
type=SYSCALL msg=audit(1402573453.807:64): arch=c000003e syscall=125 success=yes exit=0 a0=7f07287244b4 a1=7f07287244bc a2=4 a3=7f0742e43cc0 items=0 ppid=1838 pid=1846 auid=4294967295 uid=497 gid=497 euid=497 suid=497 fsuid=497 egid=497 sgid=497 fsgid=497 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(1402573453.807:65): avc: denied { setcap } for pid=1846 comm="ruby" scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:system_r:passenger_t:s0 tclass=process
type=SYSCALL msg=audit(1402573453.807:65): arch=c000003e syscall=126 success=yes exit=0 a0=7f07287244b4 a1=7f07287244bc a2=4 a3=7f0742e43cc0 items=0 ppid=1838 pid=1846 auid=4294967295 uid=497 gid=497 euid=497 suid=497 fsuid=497 egid=497 sgid=497 fsgid=497 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(1402573453.807:66): avc: denied { execute } for pid=1846 comm="ruby" name="ssh" dev=dm-0 ino=2100741 scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:object_r:ssh_exec_t:s0 tclass=file
type=AVC msg=audit(1402573453.807:66): avc: denied { read open } for pid=1846 comm="ruby" name="ssh" dev=dm-0 ino=2100741 scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:object_r:ssh_exec_t:s0 tclass=file
type=AVC msg=audit(1402573453.807:66): avc: denied { execute_no_trans } for pid=1846 comm="ruby" path="/usr/bin/ssh" dev=dm-0 ino=2100741 scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:object_r:ssh_exec_t:s0 tclass=file
type=SYSCALL msg=audit(1402573453.807:66): arch=c000003e syscall=59 success=yes exit=0 a0=7f0728195ed0 a1=7f07289012b0 a2=7f07288f7060 a3=7f0742e43cf0 items=0 ppid=1838 pid=1846 auid=4294967295 uid=497 gid=497 euid=497 suid=497 fsuid=497 egid=497 sgid=497 fsgid=497 tty=(none) ses=4294967295 comm="ssh" exe="/usr/bin/ssh" subj=system_u:system_r:passenger_t:s0 key=(null)

```
ps auxwwwZ
LABEL                          USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
system_u:system_r:init_t:s0    root         1  0.1  0.0  19232  1516 ?        Ss   13:39   0:00 /sbin/init
system_u:system_r:kernel_t:s0  root         2  0.0  0.0      0     0 ?        S    13:39   0:00 [kthreadd]
system_u:system_r:kernel_t:s0  root         3  0.0  0.0      0     0 ?        S    13:39   0:00 [migration/0]
system_u:system_r:kernel_t:s0  root         4  0.0  0.0      0     0 ?        S    13:39   0:00 [ksoftirqd/0]
system_u:system_r:kernel_t:s0  root         5  0.0  0.0      0     0 ?        S    13:39   0:00 [migration/0]
system_u:system_r:kernel_t:s0  root         6  0.0  0.0      0     0 ?        S    13:39   0:00 [watchdog/0]
system_u:system_r:kernel_t:s0  root         7  0.0  0.0      0     0 ?        S    13:39   0:00 [events/0]
system_u:system_r:kernel_t:s0  root         8  0.0  0.0      0     0 ?        S    13:39   0:00 [cgroup]
system_u:system_r:kernel_t:s0  root         9  0.0  0.0      0     0 ?        S    13:39   0:00 [khelper]
system_u:system_r:kernel_t:s0  root        10  0.0  0.0      0     0 ?        S    13:39   0:00 [netns]
system_u:system_r:kernel_t:s0  root        11  0.0  0.0      0     0 ?        S    13:39   0:00 [async/mgr]
system_u:system_r:kernel_t:s0  root        12  0.0  0.0      0     0 ?        S    13:39   0:00 [pm]
system_u:system_r:kernel_t:s0  root        13  0.0  0.0      0     0 ?        S    13:39   0:00 [sync_supers]
system_u:system_r:kernel_t:s0  root        14  0.0  0.0      0     0 ?        S    13:39   0:00 [bdi-default]
system_u:system_r:kernel_t:s0  root        15  0.0  0.0      0     0 ?        S    13:39   0:00 [kintegrityd/0]
system_u:system_r:kernel_t:s0  root        16  0.0  0.0      0     0 ?        S    13:39   0:00 [kblockd/0]
system_u:system_r:kernel_t:s0  root        17  0.0  0.0      0     0 ?        S    13:39   0:00 [kacpid]
system_u:system_r:kernel_t:s0  root        18  0.0  0.0      0     0 ?        S    13:39   0:00 [kacpi_notify]
system_u:system_r:kernel_t:s0  root        19  0.0  0.0      0     0 ?        S    13:39   0:00 [kacpi_hotplug]
system_u:system_r:kernel_t:s0  root        20  0.0  0.0      0     0 ?        S    13:39   0:00 [ata_aux]
system_u:system_r:kernel_t:s0  root        21  0.0  0.0      0     0 ?        S    13:39   0:00 [ata_sff/0]
system_u:system_r:kernel_t:s0  root        22  0.0  0.0      0     0 ?        S    13:39   0:00 [ksuspend_usbd]
system_u:system_r:kernel_t:s0  root        23  0.0  0.0      0     0 ?        S    13:39   0:00 [khubd]
system_u:system_r:kernel_t:s0  root        24  0.0  0.0      0     0 ?        S    13:39   0:00 [kseriod]
system_u:system_r:kernel_t:s0  root        25  0.0  0.0      0     0 ?        S    13:39   0:00 [md/0]
system_u:system_r:kernel_t:s0  root        26  0.0  0.0      0     0 ?        S    13:39   0:00 [md_misc/0]
system_u:system_r:kernel_t:s0  root        27  0.0  0.0      0     0 ?        S    13:39   0:00 [linkwatch]
system_u:system_r:kernel_t:s0  root        28  0.0  0.0      0     0 ?        S    13:39   0:00 [khungtaskd]
system_u:system_r:kernel_t:s0  root        29  0.0  0.0      0     0 ?        S    13:39   0:00 [kswapd0]
system_u:system_r:kernel_t:s0  root        30  0.0  0.0      0     0 ?        SN   13:39   0:00 [ksmd]
system_u:system_r:kernel_t:s0  root        31  0.0  0.0      0     0 ?        SN   13:39   0:00 [khugepaged]
system_u:system_r:kernel_t:s0  root        32  0.0  0.0      0     0 ?        S    13:39   0:00 [aio/0]
system_u:system_r:kernel_t:s0  root        33  0.0  0.0      0     0 ?        S    13:39   0:00 [crypto/0]
system_u:system_r:kernel_t:s0  root        38  0.0  0.0      0     0 ?        S    13:39   0:00 [kthrotld/0]
system_u:system_r:kernel_t:s0  root        40  0.0  0.0      0     0 ?        S    13:39   0:00 [kpsmoused]
system_u:system_r:kernel_t:s0  root        41  0.0  0.0      0     0 ?        S    13:39   0:00 [usbhid_resumer]
system_u:system_r:kernel_t:s0  root        72  0.0  0.0      0     0 ?        S    13:39   0:00 [kstriped]
system_u:system_r:kernel_t:s0  root       142  0.0  0.0      0     0 ?        S    13:39   0:00 [scsi_eh_0]
system_u:system_r:kernel_t:s0  root       143  0.0  0.0      0     0 ?        S    13:39   0:00 [scsi_eh_1]
system_u:system_r:kernel_t:s0  root       260  0.0  0.0      0     0 ?        S    13:39   0:00 [virtio-blk]
system_u:system_r:kernel_t:s0  root       294  0.0  0.0      0     0 ?        S    13:39   0:00 [kdmflush]
system_u:system_r:kernel_t:s0  root       296  0.0  0.0      0     0 ?        S    13:39   0:00 [kdmflush]
system_u:system_r:kernel_t:s0  root       313  0.0  0.0      0     0 ?        S    13:39   0:00 [jbd2/dm-0-8]
system_u:system_r:kernel_t:s0  root       314  0.0  0.0      0     0 ?        S    13:39   0:00 [ext4-dio-unwrit]
system_u:system_r:udev_t:s0-s0:c0.c1023 root 396 0.0  0.0 11376  1448 ?        S<s  13:39   0:00 /sbin/udevd -d
system_u:system_r:kernel_t:s0  root       434  0.0  0.0      0     0 ?        S    13:39   0:00 [virtio-net]
system_u:system_r:kernel_t:s0  root       436  0.0  0.0      0     0 ?        S    13:39   0:00 [vballoon]
system_u:system_r:kernel_t:s0  root       720  0.0  0.0      0     0 ?        S    13:39   0:00 [jbd2/vda1-8]
system_u:system_r:kernel_t:s0  root       721  0.0  0.0      0     0 ?        S    13:39   0:00 [ext4-dio-unwrit]
system_u:system_r:kernel_t:s0  root       766  0.0  0.0      0     0 ?        S    13:39   0:00 [kauditd]
system_u:system_r:kernel_t:s0  root       778  0.0  0.0      0     0 ?        S    13:39   0:00 [flush-253:0]
system_u:system_r:auditd_t:s0  root       992  0.0  0.0  27640   824 ?        S<sl 13:39   0:00 auditd
system_u:system_r:syslogd_t:s0  root      1017  0.0  0.0 249088  1588 ?        Sl   13:39   0:00 /sbin/rsyslogd -i /var/run/syslogd.pid -c 5
system_u:system_r:named_t:s0    named     1036  0.0  0.2 160032 11676 ?        Ssl  13:39   0:00 /usr/sbin/named -u named
system_u:system_r:system_dbusd_t:s0-s0:c0.c1023 dbus 1056 0.0  0.0 97332 1472 ? Ssl 13:39   0:00 dbus-daemon --system
system_u:system_r:hald_t:s0     68        1086  0.0  0.1  37632  4200 ?        Ssl  13:39   0:00 hald
system_u:system_r:hald_t:s0     root      1087  0.0  0.0  20324  1340 ?        S    13:39   0:00 hald-runner
system_u:system_r:hald_t:s0     root      1119  0.0  0.0  22444  1272 ?        S    13:39   0:00 hald-addon-input: Listening on /dev/input/event2
/dev/input/event0
system_u:system_r:hald_t:s0     68        1134  0.0  0.0  17932  1136 ?        S    13:39   0:00 hald-addon-acpi: listening on acpi kernel interface
/proc/acpi/event
system_u:system_r:sshd_t:s0-s0:c0.c1023 root 1146 0.0  0.0 66608 1232 ?        Ss   13:39   0:00 /usr/sbin/sshd
system_u:system_r:inetd_t:s0-s0:c0.c1023 root 1154 0.0  0.0 22180 964 ?        Ss   13:39   0:00 xinetd -stayalive -pidfile /var/run/xinetd.pid
system_u:system_r:postgresql_t:s0 postgres 1177 0.1  0.1 216272  6372 ?        S    13:39   0:00 /usr/bin/postmaster -p 5432 -D /var/lib/pgsql/data
system_u:system_r:dhcpd_t:s0    dhcpd     1191  0.0  0.1  49048  4300 ?        Ss   13:39   0:00 /usr/sbin/dhcpd -user dhcpd -group dhcpd eth0
system_u:system_r:postfix_master_t:s0 root 1267 0.0  0.0  81284  3412 ?        Ss   13:39   0:00 /usr/libexec/postfix/master
system_u:system_r:postfix_pickup_t:s0 postfix 1273 0.0  0.0 81364 3372 ?        S    13:39   0:00 pickup -l -t fifo -u
system_u:system_r:postfix_qmgr_t:s0 postfix 1274 0.0  0.0 81432  3428 ?        S    13:39   0:00 qmgr -l -t fifo -u
system_u:system_r:postgresql_t:s0 postgres 1279 0.0  0.0 179284  1496 ?        Ss   13:39   0:00 postgres: logger process
system_u:system_r:postgresql_t:s0 postgres 1281 0.0  0.0 216392  2896 ?        Ss   13:39   0:00 postgres: writer process
system_u:system_r:postgresql_t:s0 postgres 1282 0.0  0.0 216272  1752 ?        Ss   13:39   0:00 postgres: wal writer process
system_u:system_r:postgresql_t:s0 postgres 1283 0.0  0.0 216556  1992 ?        Ss   13:39   0:00 postgres: autovacuum launcher process
system_u:system_r:postgresql_t:s0 postgres 1284 0.0  0.0 179556  1736 ?        Ss   13:39   0:00 postgres: stats collector process
```

system_u:system_r:initrc_t:s0 498 1290 0.0 0.8 132788 34228 ? S 13:39 0:00 /usr/bin/ruby /usr/share/foreman-proxy/bin/smart-proxy
system_u:system_r:httpd_t:s0 root 1317 0.0 0.1 155644 6052 ? Ss 13:39 0:00 /usr/sbin/httpd
system_u:system_r:passenger_t:s0 root 1321 0.0 0.0 214048 1836 ? Ssl 13:39 0:00 PassengerWatchdog
system_u:system_r:passenger_t:s0 root 1325 0.1 0.1 575788 5756 ? Sl 13:39 0:00 PassengerHelperAgent
system_u:system_r:passenger_t:s0 nobody 1331 0.0 0.0 214128 3872 ? Sl 13:39 0:00 PassengerLoggingAgent
system_u:system_r:crond_t:s0-s0:c0.c1023 root 1343 0.1 0.0 117300 1392 ? Ss 13:39 0:00 crond
system_u:system_r:httpd_t:s0 apache 1347 0.0 0.1 155992 6160 ? S 13:39 0:00 /usr/sbin/httpd
system_u:system_r:httpd_t:s0 apache 1348 0.0 0.1 155928 5940 ? S 13:39 0:00 /usr/sbin/httpd
system_u:system_r:httpd_t:s0 apache 1349 0.0 0.1 156064 6140 ? S 13:39 0:00 /usr/sbin/httpd
system_u:system_r:httpd_t:s0 apache 1350 0.0 0.1 155928 5952 ? S 13:39 0:00 /usr/sbin/httpd
system_u:system_r:httpd_t:s0 apache 1351 0.0 0.1 155848 6004 ? S 13:39 0:00 /usr/sbin/httpd
system_u:system_r:httpd_t:s0 apache 1352 0.0 0.1 155972 6032 ? S 13:39 0:00 /usr/sbin/httpd
system_u:system_r:httpd_t:s0 apache 1353 0.0 0.1 155784 5868 ? S 13:39 0:00 /usr/sbin/httpd
system_u:system_r:httpd_t:s0 apache 1354 0.0 0.1 156092 5856 ? S 13:39 0:00 /usr/sbin/httpd
system_u:system_r:puppet_t:s0 root 1364 0.1 1.7 178224 68696 ? Ss 13:39 0:00 /usr/bin/ruby /usr/sbin/puppetd
system_u:system_r:getty_t:s0 root 1385 0.0 0.0 4064 580 tty1 Ss+ 13:39 0:00 /sbin/mingetty /dev/tty1
system_u:system_r:getty_t:s0 root 1387 0.0 0.0 4064 580 tty2 Ss+ 13:39 0:00 /sbin/mingetty /dev/tty2
system_u:system_r:getty_t:s0 root 1389 0.0 0.0 4064 580 tty3 Ss+ 13:39 0:00 /sbin/mingetty /dev/tty3
system_u:system_r:getty_t:s0 root 1391 0.0 0.0 4064 580 tty4 Ss+ 13:39 0:00 /sbin/mingetty /dev/tty4
system_u:system_r:getty_t:s0 root 1393 0.0 0.0 4064 580 tty5 Ss+ 13:39 0:00 /sbin/mingetty /dev/tty5
system_u:system_r:udev_t:s0-s0:c0.c1023 root 1395 0.0 0.0 12296 2592 ? S< 13:39 0:00 /sbin/udevd -d
system_u:system_r:udev_t:s0-s0:c0.c1023 root 1396 0.0 0.0 12296 2584 ? S< 13:39 0:00 /sbin/udevd -d
system_u:system_r:getty_t:s0 root 1398 0.0 0.0 4064 576 tty6 Ss+ 13:39 0:00 /sbin/mingetty /dev/tty6
system_u:system_r:passenger_t:s0 puppet 1429 0.2 1.7 173052 66776 ? Sl 13:39 0:00 Passenger RackApp: /etc/puppet/rack
system_u:system_r:sshd_t:s0-s0:c0.c1023 root 1577 0.0 0.1 100360 4112 ? Ss 13:40 0:00 sshd: root@pts/0
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 1584 0.0 0.0 108432 1988 pts/0 Ss 13:40 0:00 -bash
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 1610 0.0 0.0 100944 648 pts/0 S+ 13:40 0:00 tail -200f /var/log/audit/audit.log
system_u:system_r:sshd_t:s0-s0:c0.c1023 root 1652 0.0 0.1 100356 4056 ? Ss 13:40 0:00 sshd: root@pts/1
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 1660 0.0 0.0 108432 1968 pts/1 Ss 13:40 0:00 -bash
system_u:system_r:passenger_t:s0 foreman 1802 0.0 0.0 9196 1244 ? S 13:43 0:00 /bin/bash /usr/bin/ruby193-ruby
/usr/lib/ruby/gems/1.8/gems/passenger-4.0.18/helper-scripts/rack-preloader.rb
system_u:system_r:passenger_t:s0 foreman 1811 0.0 0.0 4060 548 ? S 13:43 0:00 scl enable ruby193 ruby
/usr/lib/ruby/gems/1.8/gems/passenger-4.0.18/helper-scripts/rack-preloader.rb
system_u:system_r:passenger_t:s0 foreman 1812 0.0 0.0 9196 1304 ? S 13:43 0:00 /bin/bash /var/tmp/scl2VSOqz
system_u:system_r:passenger_t:s0 foreman 1815 11.2 3.7 341764 147052 ? Sl 13:43 0:13 Passenger AppPreloader: /usr/share/foreman
system_u:system_r:passenger_t:s0 foreman 1838 1.2 4.0 543984 159688 ? Sl 13:44 0:01 Passenger RackApp: /usr/share/foreman
system_u:system_r:postgresql_t:s0 postgres 1845 0.0 0.2 218452 8008 ? Ss 13:44 0:00 postgres: foreman foreman [local] idle
system_u:system_r:passenger_t:s0 foreman 1846 0.0 0.0 60364 3392 ? S 13:44 0:00 ssh xx.xxx.xxx.xxx sh -c 'if 'nc' -q 2>&1 | grep
"requires an argument" >/dev/null 2>&1; then ARG=-q0;else ARG=;fi;'nc' $ARG -U /var/run/libvirt/libvirt-sock'
system_u:system_r:websockify_t:s0 foreman 1850 0.0 0.2 99228 7892 ? S 13:44 0:00 /usr/bin/python
/usr/share/foreman/extras/noVNC/websockify.py --daemon --idle-timeout=120 --timeout=120 5910 yyyyy.yyyyy.yyyy:5902
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 1897 4.0 0.0 110236 1196 pts/1 R+ 13:45 0:00 ps auxwwwZ

#8 - 06/12/2014 02:01 PM - Lukas Zapletal

- Category set to Packaging

- Status changed from New to Assigned

- Assignee set to Lukas Zapletal

- Priority changed from Normal to High

- Target version set to 1.8.1

- Difficulty set to easy

I was able to identify the ssh_exec issue and reported it under http://projects.theforeman.org/issues/6192

Now, turning dontaudit rules off with semodule -DB helped us to indentify some denials on websockify:

http://pastebin.com/vTS7xu5s

which translates to:

```
#============= passenger_t ==============
allow passenger_t self:capability sys_tty_config;
allow passenger_t self:process { getcap setcap };
allow passenger_t websockify_t:process { siginh rlimitinh noatsecure };
corenet_udp_bind_generic_port(passenger_t)
ssh_exec(passenger_t)

#============= tftpd_t ==============
userdom_read_admin_home_files(tftpd_t)

#============= websockify_t ==============
allow websockify_t self:netlink_route_socket { read write };
```

```
allow websockify_t self:tcp_socket { read write };
allow websockify_t self:udp_socket { write read };
apache_search_config(websockify_t)
```

As a workaround, run in PERMISSIVE mode until this is fixed.

@Dom - I think this is backport candidate (we can just rebase).

#9 - 06/12/2014 02:39 PM - Lukas Zapletal

Reproduced with:

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

#============= websockify_t ==============
allow websockify_t self:netlink_route_socket { write read };
allow websockify_t self:tcp_socket { read write };
allow websockify_t self:udp_socket { write read };
apache_search_config(websockify_t)
```

#10 - 06/13/2014 03:22 PM - Lukas Zapletal

- Status changed from Assigned to Ready For Testing

Jorick,

can you test with this patch please and selinux in Enforcing if that works?

https://github.com/theforeman/foreman-selinux/pull/21

I made this scratchbuild, just force install it (wont hurt):

http://koji.katello.org/koji/taskinfo?taskID=119386

Thanks for testing this!

#11 - 06/16/2014 11:13 AM - Jorick Astrego

Trying to test it but I don't see your foreman-selinux build in the nightly repo. Do I need to get it from somewhere else?

#12 - 06/16/2014 11:16 AM - Dominic Cleal

Jorick Astrego wrote:

> Trying to test it but I don't see your foreman-selinux build in the nightly repo. Do I need to get it from somewhere else?

It's a test/scratch build, direct link:
http://koji.katello.org/koji/getfile?taskID=119387&name=foreman-selinux-1.6.0-0.develop.el6.noarch.rpm

#13 - 06/16/2014 11:28 AM - Jorick Astrego

Sorry, I'm only the Ops in DevOps. Still learning the rest ;-)

The patch works as intended, I now can use the console while enforcing selinux.

#14 - 06/18/2014 07:56 AM - Lukas Zapletal

Oh, right. I apologize for that, it was not clear for you.

#15 - 06/19/2014 10:13 AM - Dominic Cleal

- translation missing: en.field_release set to 18

Thanks for your testing Jorick, it's a great help!

#16 - 06/19/2014 10:47 AM - Anonymous

- Status changed from Ready For Testing to Closed

- % Done changed from 0 to 100

Applied in changeset 93006b8248357354474b288610da5fb4a17f3dcb.

#17 - 06/20/2014 01:29 PM - Bryan Kearney

- Bugzilla link set to https://bugzilla.redhat.com/show_bug.cgi?id=1111592

Files

Selection_214.png	20.2 KB	06/12/2014	Jorick Astrego
Selection_213.png	16.6 KB	06/12/2014	Jorick Astrego