SELinux - Bug #6192

Policy prevents from libvirt qemu+ssh connection

06/12/2014 01:47 PM - Lukas Zapletal

Status:	Closed		
Priority:	Normal		
Assignee:			
Category:			
Target version:			
Difficulty:		**Fixed in Releases:**	
Triaged:		**Found in Releases:**	
Bugzilla link:		**Red Hat JIRA:**	
Pull request:			

Description

With SELinux turned on in Enforcing, one is not able to reach qemu+ssh libvirt instance.

```
type=AVC msg=audit(1402580749.159:279): avc:  denied  { getattr } for  pid=13036 comm="ruby" path=
"/usr/bin/ssh" dev=vda3 ino=144958 scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:obj
ect_r:ssh_exec_t:s0 tclass=file
type=SYSCALL msg=audit(1402580749.159:279): arch=c000003e syscall=4 success=yes exit=0 a0=7ff7602b
20b0 a1=7ff77bd56e90 a2=7ff77bd56e90 a3=d items=0 ppid=1 pid=13036 auid=4294967295 uid=497 gid=498
 euid=497 suid=497 fsuid=497 egid=498 sgid=498 fsgid=498 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(1402580749.162:280): avc:  denied  { getcap } for  pid=15391 comm="ruby" sconte
xt=system_u:system_r:passenger_t:s0 tcontext=system_u:system_r:passenger_t:s0 tclass=process
type=SYSCALL msg=audit(1402580749.162:280): arch=c000003e syscall=125 success=yes exit=0 a0=7ff760
7fb2c4 a1=7ff7607fb2cc a2=4 a3=7ff77bd56cc0 items=0 ppid=13031 pid=15391 auid=4294967295 uid=497 g
id=498 euid=497 suid=497 fsuid=497 egid=498 sgid=498 fsgid=498 tty=(none) ses=4294967295 comm="rub
y" exe="/opt/rh/ruby193/root/usr/bin/ruby" subj=system_u:system_r:passenger_t:s0 key=(null)
type=AVC msg=audit(1402580749.162:281): avc:  denied  { setcap } for  pid=15391 comm="ruby" sconte
xt=system_u:system_r:passenger_t:s0 tcontext=system_u:system_r:passenger_t:s0 tclass=process
type=SYSCALL msg=audit(1402580749.162:281): arch=c000003e syscall=126 success=yes exit=0 a0=7ff760
7fb2c4 a1=7ff7607fb2cc a2=4 a3=7ff77bd56cc0 items=0 ppid=13031 pid=15391 auid=4294967295 uid=497 g
id=498 euid=497 suid=497 fsuid=497 egid=498 sgid=498 fsgid=498 tty=(none) ses=4294967295 comm="rub
y" exe="/opt/rh/ruby193/root/usr/bin/ruby" subj=system_u:system_r:passenger_t:s0 key=(null)
type=AVC msg=audit(1402580749.163:282): avc:  denied  { execute } for  pid=15391 comm="ruby" name=
"ssh" dev=vda3 ino=144958 scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:object_r:ssh
_exec_t:s0 tclass=file
type=AVC msg=audit(1402580749.163:282): avc:  denied  { read open } for  pid=15391 comm="ruby" nam
e="ssh" dev=vda3 ino=144958 scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:object_r:s
sh_exec_t:s0 tclass=file
type=AVC msg=audit(1402580749.163:282): avc:  denied  { execute_no_trans } for  pid=15391 comm="ru
by" path="/usr/bin/ssh" dev=vda3 ino=144958 scontext=system_u:system_r:passenger_t:s0 tcontext=sys
tem_u:object_r:ssh_exec_t:s0 tclass=file
type=SYSCALL msg=audit(1402580749.163:282): arch=c000003e syscall=59 success=yes exit=0 a0=7ff7602
b20b0 a1=7ff7603049c0 a2=7ff76033a610 a3=7ff77bd56cf0 items=0 ppid=13031 pid=15391 auid=4294967295
 uid=497 gid=498 euid=497 suid=497 fsuid=497 egid=498 sgid=498 fsgid=498 tty=(none) ses=4294967295
 comm="ssh" exe="/usr/bin/ssh" subj=system_u:system_r:passenger_t:s0 key=(null)
type=AVC msg=audit(1402580749.170:283): avc:  denied  { search } for  pid=15391 comm="ssh" name="s
elinux" dev=vda3 ino=138549 scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:object_r:s
elinux_config_t:s0 tclass=dir
type=AVC msg=audit(1402580749.170:283): avc:  denied  { read } for  pid=15391 comm="ssh" name="con
fig" dev=vda3 ino=142973 scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:object_r:seli
nux_config_t:s0 tclass=file
type=AVC msg=audit(1402580749.170:283): avc:  denied  { open } for  pid=15391 comm="ssh" name="con
fig" dev=vda3 ino=142973 scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:object_r:seli
nux_config_t:s0 tclass=file
type=SYSCALL msg=audit(1402580749.170:283): arch=c000003e syscall=2 success=yes exit=4 a0=7f0d2686
af9d a1=0 a2=1b6 a3=0 items=0 ppid=13031 pid=15391 auid=4294967295 uid=497 gid=498 euid=497 suid=4
97 fsuid=497 egid=498 sgid=498 fsgid=498 tty=(none) ses=4294967295 comm="ssh" exe="/usr/bin/ssh" s
```

```
ubj=system_u:system_r:passenger_t:s0 key=(null)
type=AVC msg=audit(1402580749.170:284): avc:  denied  { getattr } for  pid=15391 comm="ssh" path="
/etc/selinux/config" dev=vda3 ino=142973 scontext=system_u:system_r:passenger_t:s0 tcontext=system
_u:object_r:selinux_config_t:s0 tclass=file
type=SYSCALL msg=audit(1402580749.170:284): arch=c000003e syscall=5 success=yes exit=0 a0=4 a1=7ff
fcadd2eb0 a2=7fffcadd2eb0 a3=78 items=0 ppid=13031 pid=15391 auid=4294967295 uid=497 gid=498 euid=
497 suid=497 fsuid=497 egid=498 sgid=498 fsgid=498 tty=(none) ses=4294967295 comm="ssh" exe="/usr/
bin/ssh" subj=system_u:system_r:passenger_t:s0 key=(null)
type=AVC msg=audit(1402580749.170:285): avc:  denied  { search } for  pid=15391 comm="ssh" name="c
ontexts" dev=vda3 ino=143864 scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:object_r:
default_context_t:s0 tclass=dir
type=AVC msg=audit(1402580749.170:285): avc:  denied  { search } for  pid=15391 comm="ssh" name="f
iles" dev=vda3 ino=147540 scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:object_r:fil
e_context_t:s0 tclass=dir
type=SYSCALL msg=audit(1402580749.170:285): arch=c000003e syscall=2 success=no exit=-2 a0=7f0d27d9
4060 a1=0 a2=1b6 a3=0 items=0 ppid=13031 pid=15391 auid=4294967295 uid=497 gid=498 euid=497 suid=4
97 fsuid=497 egid=498 sgid=498 fsgid=498 tty=(none) ses=4294967295 comm="ssh" exe="/usr/bin/ssh" s
ubj=system_u:system_r:passenger_t:s0 key=(null)
type=AVC msg=audit(1402580749.170:286): avc:  denied  { read } for  pid=15391 comm="ssh" name="fil
e_contexts" dev=vda3 ino=150216 scontext=system_u:system_r:passenger_t:s0 tcontext=unconfined_u:ob
ject_r:file_context_t:s0 tclass=file
type=AVC msg=audit(1402580749.170:286): avc:  denied  { open } for  pid=15391 comm="ssh" name="fil
e_contexts" dev=vda3 ino=150216 scontext=system_u:system_r:passenger_t:s0 tcontext=unconfined_u:ob
ject_r:file_context_t:s0 tclass=file
type=SYSCALL msg=audit(1402580749.170:286): arch=c000003e syscall=2 success=yes exit=4 a0=7f0d27d8
eb40 a1=0 a2=1b6 a3=0 items=0 ppid=13031 pid=15391 auid=4294967295 uid=497 gid=498 euid=497 suid=4
97 fsuid=497 egid=498 sgid=498 fsgid=498 tty=(none) ses=4294967295 comm="ssh" exe="/usr/bin/ssh" s
ubj=system_u:system_r:passenger_t:s0 key=(null)
type=AVC msg=audit(1402580749.170:287): avc:  denied  { getattr } for  pid=15391 comm="ssh" path="
/etc/selinux/targeted/contexts/files/file_contexts" dev=vda3 ino=150216 scontext=system_u:system_r
:passenger_t:s0 tcontext=unconfined_u:object_r:file_context_t:s0 tclass=file
type=SYSCALL msg=audit(1402580749.170:287): arch=c000003e syscall=5 success=yes exit=0 a0=4 a1=7ff
fcadd13e0 a2=7fffcadd13e0 a3=7fffcadd10e0 items=0 ppid=13031 pid=15391 auid=4294967295 uid=497 gid
=498 euid=497 suid=497 fsuid=497 egid=498 sgid=498 fsgid=498 tty=(none) ses=4294967295 comm="ssh"
exe="/usr/bin/ssh" subj=system_u:system_r:passenger_t:s0 key=(null)
type=AVC msg=audit(1402580749.277:288): avc:  denied  { read write } for  pid=15391 comm="ssh" nam
e="context" dev=selinuxfs ino=5 scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:object
_r:security_t:s0 tclass=file
type=AVC msg=audit(1402580749.277:288): avc:  denied  { open } for  pid=15391 comm="ssh" name="con
text" dev=selinuxfs ino=5 scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:object_r:sec
urity_t:s0 tclass=file
type=SYSCALL msg=audit(1402580749.277:288): arch=c000003e syscall=2 success=yes exit=4 a0=7fffcadd
2450 a1=2 a2=7fffcadd2460 a3=7fffcadd21d0 items=0 ppid=13031 pid=15391 auid=4294967295 uid=497 gid
=498 euid=497 suid=497 fsuid=497 egid=498 sgid=498 fsgid=498 tty=(none) ses=4294967295 comm="ssh"
exe="/usr/bin/ssh" subj=system_u:system_r:passenger_t:s0 key=(null)
type=AVC msg=audit(1402580749.277:289): avc:  denied  { check_context } for  pid=15391 comm="ssh"
scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:object_r:security_t:s0 tclass=security
type=SYSCALL msg=audit(1402580749.277:289): arch=c000003e syscall=1 success=yes exit=27 a0=4 a1=7f
0d2929d800 a2=1b a3=7fffcadd21d0 items=0 ppid=13031 pid=15391 auid=4294967295 uid=497 gid=498 euid
=497 suid=497 fsuid=497 egid=498 sgid=498 fsgid=498 tty=(none) ses=4294967295 comm="ssh" exe="/usr
/bin/ssh" subj=system_u:system_r:passenger_t:s0 key=(null)
type=AVC msg=audit(1402580749.277:290): avc:  denied  { setfscreate } for  pid=15391 comm="ssh" sc
ontext=system_u:system_r:passenger_t:s0 tcontext=system_u:system_r:passenger_t:s0 tclass=process
type=SYSCALL msg=audit(1402580749.277:290): arch=c000003e syscall=1 success=yes exit=27 a0=4 a1=7f
0d2929a4d0 a2=1b a3=7fffcadd3270 items=0 ppid=13031 pid=15391 auid=4294967295 uid=497 gid=498 euid
=497 suid=497 fsuid=497 egid=498 sgid=498 fsgid=498 tty=(none) ses=4294967295 comm="ssh" exe="/usr
/bin/ssh" subj=system_u:system_r:passenger_t:s0 key=(null)
```

History

#1 - 06/12/2014 03:29 PM - Lukas Zapletal

Warning for myself - I had semanage -DB enabled.

#2 - 06/28/2018 12:30 PM - Dirk Götz

I could not reproduce this with selinux in enforcing mode on RHEL 7.5 and current Foreman SELinux Policy.

#3 - 06/28/2018 03:38 PM - Lukas Zapletal

- Status changed from New to Closed

Thanks for help! My TODO is shrinking, oh yeah.