SELinux - Feature #5930

Implement policy for Katello plugin

05/26/2014 02:39 PM - Lukas Zapletal

Status:	Closed		
Priority:	High		
Assignee:	Lukas Zapletal		
Category:	Packaging		
Target version:	1.6.0		
Difficulty:		**Fixed in Releases:**	
Triaged:		**Found in Releases:**	
Bugzilla link:	1104251	**Red Hat JIRA:**	
Pull request:			

Description

Some rules can be taken from katello-selinux package.

Related issues:

Related to SELinux - Refactor #6284: Remove Passenger/init_exec_script_files ...	**Closed**

Associated revisions

Revision 0578ccf1 - 06/19/2014 10:14 AM - Lukas Zapletal

fixes #5930 - implement katello selinux policy

Revision 55326848 - 06/24/2014 08:42 AM - Lukas Zapletal

fixes #5930 - fix katello-jobs domain

History

#1 - 05/27/2014 08:24 AM - Dominic Cleal

This should be a layered policy (katello-selinux), not in foreman-selinux.

#2 - 05/27/2014 08:52 AM - Lukas Zapletal

Why? Katello is a plugin, like others. There is no big benefit in splitting those.

Also, I don't expect katello policy to be huge. Yes, there is existing katello-selinux, but most of the rules (I expect more than 95%) will not be necessary and are covered by the foreman policy.

#3 - 05/27/2014 08:53 AM - Dominic Cleal

Ok, see what it involves, but my concern is if changes are needed regularly in a core Foreman project to support a plugin, then we'll get in a mess (better to have the plugin manage their own release schedule, like the installer).

#4 - 05/27/2014 10:27 AM - Lukas Zapletal

I agree, if we find this annoying, I will work on splitting all the policies. But I hope for 5 lines for Katello, there is nothing special at all.

#5 - 06/05/2014 10:26 AM - Lukas Zapletal

- Category set to Packaging

- Assignee set to Lukas Zapletal

- Priority changed from Normal to High

Another set of denials:

```
type=AVC msg=audit(1401810620.485:4502): avc:  denied  { getattr } for  pid=19983 comm="service" path="/etc/rc
.d/init.d/katello-jobs" dev=dm-0 ino=2889442 scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:objec
t_r:initrc_exec_t:s0 tclass=file
type=SYSCALL msg=audit(1401810620.485:4502): arch=c000003e syscall=4 success=yes exit=0 a0=c84290 a1=7fffbcdf5
f20 a2=7fffbcdf5f20 a3=8 items=0 ppid=14901 pid=19983 auid=4294967295 uid=497 gid=498 euid=497 suid=497 fsuid=
497 egid=498 sgid=498 fsgid=498 tty=(none) ses=4294967295 comm="service" exe="/bin/bash" subj=system_u:system_
```

```
r:passenger_t:s0 key=(null)
type=AVC msg=audit(1401810620.486:4503): avc:  denied  { execute } for  pid=19987 comm="env" name="katello-jobs" dev=dm-0 ino=2889442 scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:object_r:initrc_exec_t:s0 tclass=file
type=AVC msg=audit(1401810620.486:4503): avc:  denied  { read open } for  pid=19987 comm="env" name="katello-jobs" dev=dm-0 ino=2889442 scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:object_r:initrc_exec_t:s0 tclass=file
type=AVC msg=audit(1401810620.486:4503): avc:  denied  { execute_no_trans } for  pid=19987 comm="env" path="/etc/rc.d/init.d/katello-jobs" dev=dm-0 ino=2889442 scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:object_r:initrc_exec_t:s0 tclass=file
type=SYSCALL msg=audit(1401810620.486:4503): arch=c000003e syscall=59 success=yes exit=0 a0=7fff90befd53 a1=7fff90beef38 a2=11ad060 a3=ffffff00 items=0 ppid=19983 pid=19987 auid=4294967295 uid=497 gid=498 euid=497 suid=497 fsuid=497 egid=498 sgid=498 fsgid=498 tty=(none) ses=4294967295 comm="katello-jobs" exe="/bin/bash" subj=system_u:system_r:passenger_t:s0 key=(null)
type=AVC msg=audit(1401810620.487:4504): avc:  denied  { ioctl } for  pid=19987 comm="katello-jobs" path="/etc/rc.d/init.d/katello-jobs" dev=dm-0 ino=2889442 scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:object_r:initrc_exec_t:s0 tclass=file
type=SYSCALL msg=audit(1401810620.487:4504): arch=c000003e syscall=16 success=no exit=-25 a0=3 a1=5401 a2=7fffd16d8df0 a3=4 items=0 ppid=19983 pid=19987 auid=4294967295 uid=497 gid=498 euid=497 suid=497 fsuid=497 egid=498 sgid=498 fsgid=498 tty=(none) ses=4294967295 comm="katello-jobs" exe="/bin/bash" subj=system_u:system_r:passenger_t:s0 key=(null)
type=AVC msg=audit(1401810620.487:4505): avc:  denied  { execute } for  pid=19989 comm="katello-jobs" name="consoletype" dev=dm-0 ino=1703944 scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:object_r:consoletype_exec_t:s0 tclass=file
type=AVC msg=audit(1401810620.487:4505): avc:  denied  { read open } for  pid=19989 comm="katello-jobs" name="consoletype" dev=dm-0 ino=1703944 scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:object_r:consoletype_exec_t:s0 tclass=file
type=AVC msg=audit(1401810620.487:4505): avc:  denied  { execute_no_trans } for  pid=19989 comm="katello-jobs" path="/sbin/consoletype" dev=dm-0 ino=1703944 scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:object_r:consoletype_exec_t:s0 tclass=file
type=SYSCALL msg=audit(1401810620.487:4505): arch=c000003e syscall=59 success=yes exit=0 a0=d26990 a1=d269f0 a2=d26a20 a3=10 items=0 ppid=19988 pid=19989 auid=4294967295 uid=497 gid=498 euid=497 suid=497 fsuid=497 egid=498 sgid=498 fsgid=498 tty=(none) ses=4294967295 comm="consoletype" exe="/sbin/consoletype" subj=system_u:system_r:passenger_t:s0 key=(null)
```

https://bugzilla.redhat.com/show_bug.cgi?id=1104251

#6 - 06/05/2014 10:44 AM - Lukas Zapletal

- Bugzilla link set to https://bugzilla.redhat.com/show_bug.cgi?id=1104251

#7 - 06/05/2014 10:58 AM - Lukas Zapletal

Combined two BZs into this ticket: https://bugzilla.redhat.com/show_bug.cgi?id=1084013

#8 - 06/10/2014 10:08 AM - Lukas Zapletal

- Status changed from New to Ready For Testing

- Target version set to 1.8.2

- translation missing: en.field_release set to 10

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

Note for myself: there are two downstream bugzillas for this one.

#9 - 06/11/2014 02:53 PM - Anonymous

- Target version changed from 1.8.2 to 1.8.1

#10 - 06/19/2014 10:12 AM - Dominic Cleal

- Related to Refactor #6284: Remove Passenger/init_exec_script_files policy added

#11 - 06/19/2014 10:47 AM - Anonymous

- Status changed from Ready For Testing to Closed

- % Done changed from 0 to 100

Applied in changeset 0578ccf1ad96640d36849346dea3f0af01f1748a.