SELinux - Bug #16273
SELinux Preventing Foreman Proxy From Starting
08/24/2016 02:32 PM - Jason Nance

Status: Closed
Priority: Normal
Assignee: Lukas Zapletal
Category: Smart proxy
Target version: 1.22.0
Difficulty:

Pull request: https://github.com/theforeman/foreman-selinux/pull/88

Triaged: No
Bugzilla link:

Fixed in Releases: 1.22.0
Found in Releases: 1.12.2

Description
Using the foreman-installer options below on a CentOS 7 system that is FreeIPA-joined results in a system where the foreman-proxy service will not start due to SELinux denials.

The SELinux denial is (/var/log/audit/audit.log):

type=AVC msg=audit(1472060581.857:571): avc: denied { execmem } for pid=6134 comm="ruby" scontext=system_u:system_r:foreman_proxy_t:s0 tcontext=system_u:system_r:foreman_proxy_t:s0 tclass=process

If I change SELinux to permissive or create a module using the above AVC and audit2allow the the proxy starts up fine.

foreman-prepare-realm was ran prior to foreman-installer and the keytab copied/chowned/chmoded.

/var/log/foreman-proxy/proxy.log says (with log level set to ERROR):


The binary bits on the end change every time you attempt to start.

/var/log/foreman-proxy/proxy.log says (with log level set to DEBUG):

D, [2016-08-24T12:39:18.361200 #5987] DEBUG -- : Rack::Handler::WEBrick is mounted on /.
I, [2016-08-24T12:39:18.361334 #5987] INFO -- : WEBrick::HTTPServer#start: pid=5987 port=9090
I, [2016-08-24T12:40:14.100128 #5987] INFO -- : going to shutdown ...
foreman-installer \
  --scenario katello \
  --enable-foreman-plugin-bootdisk \
  --enable-foreman-plugin-default-hostgroup \
  --enable-foreman-plugin-discovery \
  --enable-foreman-plugin-hooks \
  --enable-foreman-plugin-openscap \
  --enable-foreman-plugin-puppetdb \
  --enable-foreman-plugin-remote-execution \
  --enable-foreman-plugin-setup \
  --enable-foreman-plugin-templates \
  --enable-foreman-proxy-plugin-openscap \
  --enable-foreman-proxy-plugin-remote-execution-ssh \
  --foreman-ipa-authentication true \
  --foreman-ipa-manage-sssd true \
  --foreman-puppetrun true \
  --foreman-plugin-discovery-install-images true \
  --foreman-plugin-openscap-configure-openscap-repo true \
  --foreman-proxy-bmc true \
  --foreman-proxy-logs true \
  --foreman-proxy-realm true \
  --foreman-proxy-realm-principal realm-proxy@DOMAIN.COM \
  --foreman-proxy-templates true \
  --foreman-proxy-tftp true

Related issues:
Related to SELinux - Bug #18409: foreman-proxy does not start in 1.14 with SE... Duplicate
Related to SELinux - Feature #26520: Allow execmem for passenger due to Ruby FFI Closed

Associated revisions
Revision 390a5680 - 04/03/2019 02:50 PM - Lukas Zapletal
Fixes #16273 - allow execmem

History
#1 - 08/24/2016 03:25 PM - Jason Nance
FYI, I did run through the "SELinux denials" section on the Foreman troubleshooting page (without my custom module loaded) including a full relabel of the system.
Results of foreman-debug are at http://debugs.theforeman.org/foreman-debug-1D7Ku.tar.xz.

#2 - 08/25/2016 02:38 AM - Dominic Cleal
- Project changed from Foreman to SELinux
- Category set to Smart proxy

#3 - 08/25/2016 02:45 AM - Lukas Zapletal
Thanks for the report. For the record, the missing rules are:

```
#============= foreman_proxy_t ==============
allow foreman_proxy_t autofs_t:dir { getattr search };
allow foreman_proxy_t cgroup_t:dir getattr;
allow foreman_proxy_t cgroup_t:filesystem getattr;
allow foreman_proxy_t configs_t:dir getattr;
allow foreman_proxy_t configs_t:filesystem getattr;
allow foreman_proxy_t device_t:filesystem getattr;
allow foreman_proxy_t dosfs_t:dir getattr;
allow foreman_proxy_t dosfs_t:filesystemgetattr;
allow foreman_proxy_t efivarfs_t:dir getattr;
allow foreman_proxy_t efivarfs_t:filesystem getattr;
```
allow foreman_proxy_t fs_t:filesystem getattr;
allow foreman_proxy_t httpd_sys_rw_content_t:dir {getattr search};
allow foreman_proxy_t hugetlbfs_t:dir getattr;
allow foreman_proxy_t hugetlbfs_t:filesystem getattr;
allow foreman_proxy_t mongod_var_lib_t:dir getattr;
allow foreman_proxy_t nfsd_fs_t:dir getattr;
allow foreman_proxy_t nfsd_fs_t:filesystem getattr;
allow foreman_proxy_t postfix_etc_t:dir getattr;
allow foreman_proxy_t postfix_etc_t:filesystem getattr;
allow foreman_proxy_t pstore_t:dir getattr;
allow foreman_proxy_t pstore_t:filesystem getattr;
allow foreman_proxy_t self:capability fowner;
allow foreman_proxy_t self:key {write setattr};
allow foreman_proxy_t self:process execmem;
allow foreman_proxy_t sssd_var_lib_t:dir search;
allow foreman_proxy_t sysctl_fs_t:dir search;
allow foreman_proxy_t tmpfs_t:filesystem getattr;
allow foreman_proxy_t var_lib_nfs_t:dir search;

Looks like OpenSCAP plugin's FFI dependency has problems, also something is sniffing around the filesystem, might be also the new inotify capability. We have couple of regressions as SELinux for proxy is turned off by default.

I will fix the bugs and suggest turning it on by default now.

#4 - 04/03/2019 09:34 AM - Lukas Zapletal
For the record, FFI is SELinux unfriendly, turns out most FFI applications won’t start due to execmem.

#5 - 04/03/2019 09:48 AM - Lukas Zapletal
- Related to Bug #18409: foreman-proxy does not start in 1.14 with SELinux activated added

#6 - 04/03/2019 09:49 AM - Lukas Zapletal
- Related to Feature #26520: Allow execmem for passenger due to Ruby FFI added

#7 - 04/03/2019 09:53 AM - The Foreman Bot
- Assignee set to Lukas Zapletal
- Status changed from New to Ready For Testing
- Pull request https://github.com/theforeman/foreman-selinux/pull/88 added

#8 - 04/03/2019 11:56 AM - Tomer Brisker
- Target version set to 1.22.0
#9 - 04/03/2019 03:01 PM - Anonymous

- Status changed from Ready For Testing to Closed

Applied in changeset 390a66806d400b69249af775943787c8741dbcc5.

#10 - 04/22/2019 09:11 AM - Tomer Brisker

- Fixed in Releases 1.22.0 added