SELinux - Bug #12398

Write to /var/run/foreman/pids/dynflow_executor.output is prevented

11/05/2015 03:28 AM - Lukas Zapletal

Status:	Resolved		
Priority:	Normal		
Assignee:			
Category:			
Target version:			
Difficulty:		**Fixed in Releases:**	
Triaged:	No	**Found in Releases:**	
Bugzilla link:	1273371	**Red Hat JIRA:**	
Pull request:			

Description

When users configure for sendmail, we block this.

Related issues:

Related to foreman-tasks - Feature #18635: Redirect stdout to syslog	**Closed**	**02/23/2017**

History

#1 - 11/05/2015 03:37 AM - Lukas Zapletal

- Tracker changed from Feature to Bug

- Subject changed from Create boolean for sendmail to Write to /var/run/foreman/pids/dynflow_executor.output is prevented

Oh we do this already, the error user see is:

SELinux is preventing /usr/sbin/sendmail.postfix from append access on the file /var/run/foreman/pids/dynflow_executor.output

type=AVC msg=audit(1445266684.536:1061): avc: denied { append } for pid=20151 comm="sendmail" path="/var/run/foreman/pids/dynflow_executor.output" dev=dm-1 ino=1711405 scontext=system_u:system_r:system_mail_t:s0 tcontext=system_u:object_r:foreman_var_run_t:s0 tclass=file

type=SYSCALL msg=audit(1445266684.536:1061): arch=x86_64 syscall=execve success=yes exit=0 a0=984aa0 a1=983470 a2=983140 a3=38 items=0 ppid=2893 pid=20151 auid=4294967295 uid=495 gid=494 euid=495 suid=495 fsuid=495 egid=494 sgid=494 fsgid=494 tty=(none) ses=4294967295 comm=sendmail exe=/usr/sbin/sendmail.postfix subj=system_u:system_r:system_mail_t:s0 key=(null)

#2 - 11/05/2015 08:03 AM - Lukas Zapletal

- Category deleted (General Foreman)

This is file descriptor leak in foreman-tasks / daemons gem. It redirects STDOUT/STDERR in this file, so when we change the SELinux domain it is prevented from appending there. We should either log to a safe directory, or better output should be sent to syslog/journald (a patch for daemons gem is needed for that).

#3 - 11/05/2015 08:36 AM - Lukas Zapletal

Attempt to add syslog support into daemons gem: https://github.com/thuehlinger/daemons/pull/43

Then we only need to make sure our policy allows syslog (logging_send_syslog_msg macro).

#4 - 02/23/2017 03:19 AM - Lukas Zapletal

Patch in daemons rubygem was merged, this will be part of 1.2.5+ release.

#5 - 02/23/2017 03:19 AM - Lukas Zapletal

https://github.com/thuehlinger/daemons/commit/5b7e862df59efeb3bbfcba698c00f3d27cbc6cfe

#6 - 02/23/2017 03:25 AM - Lukas Zapletal

- Related to Feature #18635: Redirect stdout to syslog added

#7 - 05/27/2020 08:25 AM - Lukas Zapletal

- Status changed from New to Resolved