Foreman - Bug #11560

foreman-debug to skip USER_AVC SELinux audit "denials"

08/25/2015 02:48 PM - Bryan Kearney

Status:	Closed		
Priority:	Normal		
Assignee:	Lukas Zapletal		
Category:	foreman-debug		
Target version:	1.10.0		
Difficulty:		**Fixed in Releases:**	
Triaged:		**Found in Releases:**	
Bugzilla link:	1209794	**Red Hat JIRA:**	
Pull request:	https://github.com/theforeman/foreman/pull/2637		

Description

Cloned from https://bugzilla.redhat.com/show_bug.cgi?id=1209794
Description of problem:
foreman-debug checking for SELinux denials wrongly reports also USER_AVC records like below example. Those are logs of policy load and not real denials. foreman-debug then wrongly reports "DENIALS: 12" to stdout.

Version-Release number of selected component (if applicable):
foreman-debug-1.7.2.15-1.el7sat.noarch

How reproducible:
100%

Steps to Reproduce:
1. e.g. on freshly installed RHEL7.1 and Sat6.1 (most probably reproducible anywhere), run foreman-debug
2. Check it's output and selinux_denials.log it generates

Actual results:
foreman-debug output having:

```
HOSTNAME: pmoravec-sat61.gsslab.brq.redhat.com
      OS: redhat
 RELEASE: Red Hat Enterprise Linux Server release 7.1 (Maipo)
 FOREMAN: 1.7.2
    RUBY: ruby 2.0.0p598 (2014-11-13) [x86_64-linux]
  PUPPET: 3.6.2
 DENIALS: 12
```

selinux_denials.log having 12 records like:
time->Wed Apr 8 09:31:02 2015
type=USER_AVC msg=audit(1428478262.651:1213): pid=1 uid=0 auid=4294967295 ses=4294967295
subj=system_u:system_r:init_t:s0 msg='avc: received policyload notice (seqno=11) exe="/usr/lib/systemd/systemd" sauid=0
hostname=? addr=? terminal=?'

Expected results:
foreman-debug output to have "DENIALS: 0"
selinux_denials.log without the USER_AVC logs

Additional info:
/me not sure what all audit logs could be of USER_AVC type, or if there could be also real denials. But definitely the above logs are not SELinux denials and should not be reported as such by foreman-debug.

Associated revisions

Revision ee2d45d0 - 08/27/2015 03:23 PM - Lukas Zapletal

Fixes #11560 - foreman-debug counts denials correctly

History

#1 - 08/25/2015 02:49 PM - Bryan Kearney

- Category set to foreman-debug

#2 - 08/26/2015 03:15 AM - Lukas Zapletal

We can use

```
ausearch -m avc -r
```

instead

#3 - 08/26/2015 08:19 AM - The Foreman Bot

- Status changed from New to Ready For Testing

- Pull request https://github.com/theforeman/foreman/pull/2637 added

- Pull request deleted ()

#4 - 08/27/2015 04:03 PM - Lukas Zapletal

- Status changed from Ready For Testing to Closed

- % Done changed from 0 to 100

Applied in changeset ee2d45d090b81b00586fcccfcb524ea3bc272839.

#5 - 08/28/2015 02:58 AM - Dominic Cleal

- translation missing: en.field_release set to 63

- Assignee set to Lukas Zapletal