How to exclude crond from audit logs

SOLUTION VERIFIED - Updated November 17 2015 at 1:57 PM - English ()

Environment

- Red Hat Enterprise Linux 5
- Red Hat Enterprise Linux 6
- Red Hat Enterprise Linux 7

Issue

- How can we disable all the extra PAM-related crond messages from filling up /var/log/audit/audit.log?
- Auditd logs show at least 6 events audit.log every time cron runs a job. In my case that's every 5 minutes cause that's what I have set sar to.

```
type=USER_ACCT msg=audit(1336941301.016:10008): user pid=27266 uid=0
auid=4294967295 msg='PAM: accounting acct="root" : exe="/usr/sbin/crond"
(hostname=?, addr=?, terminal=cron res=success)'
type=CRED_ACQ msg=audit(1336941301.016:10009): user pid=27266 uid=0
auid=4294967295 msg='PAM: setcred acct="root" : exe="/usr/sbin/crond"
(hostname=?, addr=?, terminal=cron res=success)'
type=LOGIN msg=audit(1336941301.016:10010): login pid=27266 uid=0 old
auid=4294967295 new auid=0 old ses=4294967295 new ses=1542
type=USER_START msg=audit(1336941301.046:10011): user pid=27266 uid=0 auid=0
msg='PAM: session open acct="root" : exe="/usr/sbin/crond" (hostname=?, addr=?,
terminal=cron res=success)'
type=CRED_DISP msg=audit(1336941301.076:10012): user pid=27266 uid=0 auid=0
msg='PAM: setcred acct="root" : exe="/usr/sbin/crond" (hostname=?, addr=?,
terminal=cron res=success)'
type=USER_END msg=audit(1336941301.076:10013): user pid=27266 uid=0 auid=0
msg='PAM: session close acct="root" : exe="/usr/sbin/crond" (hostname=?, addr=?,
terminal=cron res=success)'
```

Resolution

- Add an audit rule like the following to minimize audit events triggered by `crond` executing cron jobs


```
-A never,user -F subj_type=crond_t
```

- Notes:
  - This does not work in RHEL 5 (there are no other options there)
  - This does not work if SELinux is disabled (as it relies on filtering by the SELinux context type of the `crond` process)
  - If unable to add the rule, crond-triggered audit events can be minimized by combining cron jobs, e.g., with the following 3 jobs:

```
*/4 * * * * somecommand
*/4 * * * * another-command
*/4 * * * * some-other-command
```

In RHEL 6, that's going to generate 18 audit events every 4 minutes
Instead, they could be combined into a single line that would only generate 6 events every 4 minutes, e.g.:

```
*/4 * * * * somecommand; another-command; some-other-command
```

Private Notes (Red Hat Internal)

- RHEL6 Bugzilla: https://bugzilla.redhat.com/show_bug.cgi?id=634303 (https://bugzilla.redhat.com/show_bug.cgi?id=634303)
  - errata released: http://rhn.redhat.com/errata/RHSA-2011-0542.html (http://rhn.redhat.com/errata/RHSA-2011-0542.html)
- RHEL5 Bugzilla: https://bugzilla.redhat.com/show_bug.cgi?id=667405 (private)
  - no errata

CUSTOMER PORTAL (https://access.redhat.com/)

Product(s) Red Hat Enterprise Linux (/taxonomy/products/red-hat-enterprise-linux)

Component audit (/components/audit) **Category** Configure (/category/configure)

Tags audit (/tags/audit) rhel_5 (/tags/rhel_5) rhel_6 (/tags/rhel_6) rhel_7 (/taxonomy/tags/rhel7) selinux (/tags/selinux)

This solution is part of Red Hat's fast-track publication program, providing a huge library of solutions that Red Hat engineers have created while supporting our customers. To give you the knowledge you need the instant it becomes available, these articles may be presented in a raw and unedited form.

People who viewed this solution also viewed

auid doesn't display user id while connected via ssh

Solution - May 17, 2012

Why running /etc/init.d/crond status displays "crond dead but pid file exists" ?

Solution - Jun 6, 2013

How to change time stamp recorded in the audit log to normal format ?

Solution - Sep 22, 2015

Case Links (Red Hat Internal)

01518226 (/support/cases/#/case/01518226) - rhn-support-rahranja

CUSTOMER PORTAL (https://access.redhat.com/)

01541823 (/support/cases/#/case/01541823) - rhn-support-ryamamot

01070692 (/support/cases/#/case/01070692) - rhn-support-fjayalat

01446757 (/support/cases/#/case/01446757) - rhn-support-nparmar

01460306 (/support/cases/#/case/01460306) - rhn-support-jiazhang

01624116 (/support/cases/#/case/01624116) - rhn-support-santony

01588167 (/support/cases/#/case/01588167) - rhn-support-santony

01942310 (/support/cases/#/case/01942310) - rhn-support-ryamamot

01737326 (/support/cases/#/case/01737326) - rhn-support-dbodnarc

01983959 (/support/cases/#/case/01983959) - rhn-support-mezhu

Show More

Comments