How to exclude specific users, groups, or services when using auditd to audit syscalls

SOLUTION VERIFIED - Updated August 2 2016 at 12:48 PM - English ()

Environment

- Red Hat Enterprise Linux
- auditd

Issue

- How to exclude services from triggering syscall rules with audit?
- We're using standard STIG rules to audit time-changes by syscall (e.g., in the same way as what can be seen with `grep ^-a.*time-change /usr/share/doc/audit-*/stig.rules`) but unfortunately `ntpd` (or `chronyd` on newer servers) is constantly triggering new audit events as it makes changes to the time. How can we exclude ntpd or chronyd from triggering these audit rules?

Resolution

See also: How to exclude specific users or groups when using auditd to watch files (https://access.redhat.com/solutions/2482221)

- Take a simple syscall rule like:

```
-a always,exit -F arch=b64 -S clock_settime
```

- The above rule can be extended with conditions to restrict when it will be triggered
  For example:
    - `-F subj_type!=ntpd_t`
      Adding this to the above rule effectively "*whitelists*" the use of `clock_settime()` by any processes running under the `ntpd_t` SELinux domain

We use cookies on our websites to deliver our online services. Details about how we use cookies and how you may disable them are set out in our Privacy Statement (//www.redhat.com/en/about/privacy-policy#cookies). By using this website you agree to our use of cookies.

- `-F auid!=timekeeper`
  Adding this to the above rule effectively *"whitelists"* the use of `clock_settime()` by any processes owned by a user (probably root) who originally logged in as the "timekeeper" user

- Note that there are many more rule field names to allow more specificity with users, groups, and the different components of the subject & object SELinux context
  (See the **auditctl(8)** man page for more details)

- Note that it is *not* possible to add executable path (e.g., `-F path!=/usr/sbin/ntpd`) or command/process name to a syscall-auditing rule
  For more detail on this, see: How to exclude specific processes when using auditd to audit syscalls (https://access.redhat.com/solutions/2482361)

Final example

- The standard STIG rules audit time-changes

```
~]# grep ^-a.*time-change /usr/share/doc/audit-*/stig.rules
-a always,exit -F arch=b32 -S adjtimex,settimeofday,stime -F key=time-change
-a always,exit -F arch=b64 -S adjtimex,settimeofday -F key=time-change
-a always,exit -F arch=b32 -S clock_settime -F a0=0x0 -F key=time-change
-a always,exit -F arch=b64 -S clock_settime -F a0=0x0 -F key=time-change
```

- To allow the `ntpd` and `chronyd` services to change time without triggering audit events on a system where SELinux is in enforcing or permissive, add `-F subj_type!=ntpd_t` to each line, resulting in:

```
-a always,exit -F arch=b32 -S adjtimex,settimeofday,stime -F subj_type!=ntpd_t -F key=time-change
-a always,exit -F arch=b64 -S adjtimex,settimeofday -F subj_type!=ntpd_t -F key=time-change
-a always,exit -F arch=b32 -S clock_settime -F a0=0x0 -F subj_type!=ntpd_t -F key=time-change
-a always,exit -F arch=b64 -S clock_settime -F a0=0x0 -F subj_type!=ntpd_t -F key=time-change
```

SBR **Services (/sbr/services)**

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

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

We use cookies on our websites to deliver our online services. Details about how we use cookies and how you may disable them are set out in our Privacy Statement (//www.redhat.com/en/about/privacy-policy#cookies). By using this website you agree to our use of cookies.

Tags audit (/tags/audit) how-to (/tags/how-to) logging (/tags/logging) rhel (/tags/rhel) rhel_5 (/tags/rhel_5) rhel_6 (/tags/rhel_6) rhel_7 (/taxonomy/tags/rhel7) security (/tags/security)

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

auditd rule "-F auid>=500" produces "missing operation for auid" error.

Solution - Jun 12, 2014

Warning - entry rules deprecated, changing to exit rule in line xx

Solution - Mar 18, 2013

Why audit daemon logging ntp events continously after adding audit rule for system time change

Solution - Dec 29, 2016

Case Links (Red Hat Internal)

01666987 (/support/cases/#/case/01666987) - rhn-support-rsawhill

01676617 (/support/cases/#/case/01676617) - rhn-support-rsawhill

We use cookies on our websites to deliver our online services. Details about how we use cookies and how you may disable them are set out in our Privacy Statement (//www.redhat.com/en/about/privacy-policy#cookies). By using this website you agree to our use of cookies.

01674995 (/support/cases/#/case/01674995) - rhn-support-rsawhill

01841758 (/support/cases/#/case/01841758) - rhn-support-bpowers

01943678 (/support/cases/#/case/01943678) - rhn-support-ysoni

01727334 (/support/cases/#/case/01727334) - rhn-support-thgardne

02013637 (/support/cases/#/case/02013637) - rhn-support-bpowers

01828247 (/support/cases/#/case/01828247) - rhn-support-akjain

01920040 (/support/cases/#/case/01920040) - rhn-support-apmukher

01879769 (/support/cases/#/case/01879769) - rhn-support-nparmar

Show More

Comments

All systems operational (https://status.redhat.com)

Privacy Statement (http://www.redhat.com/en/about/privacy-policy)
Customer Portal Terms of Use (https://access.redhat.com/help/terms/)
All Policies and Guidelines (http://www.redhat.com/en/about/all-policies-guidelines)

Copyright © 2018 Red Hat, Inc.

We use cookies on our websites to deliver our online services. Details about how we use cookies and how you may disable them are set out in our Privacy Statement (//www.redhat.com/en/about/privacy-policy#cookies). By using this website you agree to our use of cookies.