How to exclude specific users or groups when using auditd to watch files

SOLUTION VERIFIED - Updated August 2 2016 at 12:24 PM - English ()

Environment

- Red Hat Enterprise Linux
- auditd

Issue

- How to exclude users when auditing directories and files with auditd?

- We want to put a filesystem watch on a directory and can do this with the simple `-w PATH -p wa` rule (for write & attribute changes) but unfortunately there's a particular user that needs to be able to make regular changes to this directory and it's files (and subdirs) and we don't want their actions to trigger audit events. How can we make a filesystem watch rule that audits all access *except* for access by a particular user or group?

Resolution

See also: How to exclude specific users, groups, or services when using auditd to audit syscalls (https://access.redhat.com/solutions/2477471)

- The following audit rule essentially audits all writes & attribute-changes to `/opt/application` and everything beneath it

```
-w /opt/application -p wa
```

- If the goal is to ignore changes made to this directory by a particular user or group, the simple rule will first need to be converted to the more expressive format, e.g.:

```
-a always,exit -F dir=/opt/application -F perm=wa
```

- In this more expressive format, conditions can now be added, e.g.:
  - `-F uid!=USER`
    (Where `USER` is some user or user ID)
    Adding this to the above rule would effectively *"whitelist"* `USER`, preventing their actions from triggering the rule

  - `-F uid>=1000`
    Adding this to the above rule would effectively *"whitelist"* all actions by system users

  - `-F success=1`
    Adding this to the above rule would prevent logging of unsuccessful write attempts

  - Note that there are many more rule field names to allow more specificity with users and groups, e.g., `auid`, `egid`, `euid`, `fsgid`, `fsuid`, `gid`
    (See the **auditctl(8)** man page for more details)

Final example

- Consider the following:

```
-a always,exit -F dir=/opt/application -F perm=w -F uid!=bob -F uid!=alice -F
auid!=root -F uid>=1000 -F gid!=admins -F success=1
```

- The above example rule will effectively audit all *successful* writes to `/opt/application`, except those executed by processes which are:

  - owned by the user "bob"
  - owned by the user "alice"
  - owned by a user who originally logged in as root
  - owned by a user with a UID less than 1000
  - owned by a process where the primary group is "admins"

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

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

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

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

auditd: auditing syscall with flags

Solution - Oct 12, 2018

How to configure audit rules to capture user activity for grep or egrep commands.

Solution - Jul 22, 2014

Case Links (Red Hat Internal)

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

01714692 (/support/cases/#/case/01714692) - rhn-support-ryamamot

01734975 (/support/cases/#/case/01734975) - rhn-support-arajendr

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

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

02196219 (/support/cases/#/case/02196219) - rhn-support-lgrunewa

02159662 (/support/cases/#/case/02159662) - rhn-gps-canderso

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)