NAME

auditd.conf − time-based rotation of audit logs

DESCRIPTION

By default, the audit daemon (auditd) supports size-based log rotation, where logs are rotated once they reach a specified size, as configured in */etc/audit/auditd.conf*. This manual describes an alternative method: time-based log rotation using **cron.** Using this approach, audit logs can be rotated at specified intervals (hourly, daily, weekly or on a custom date), regardless of their size.

CONFIGURATION

1.Disable Size-Based Rotation:

To enable time-based log rotation, first disable **auditd's** built-in size-based rotation by setting the following parameter in */etc/audit/auditd.conf:*

max_log_file_action = ignore

2. Configure Log Retention:

The **num_logs** parameter determines the number of rotated log files to keep. For daily rotation, setting

num_logs = 7

ensures that logs from the last seven days are retained. However, on busy systems, audit logs may grow rapidly, potentially leading to a lack of disk space. To prevent this, ensure that the **space_left_action** parameter is configured to handle low-disk-space situations appropriately.

3. Apply Configuration Changes:

After modifying the main auditd configuration file, reload auditd to apply the changes:

auditctl --signal reload

4. Deploy the Rotation Script:

Copy the provided **auditd.cron** script to the appropriate cron directory (*cron.daily* or *cron.hourly* or *cron.weekly* , depending on your rotation preference). Then, ensure the file has the correct SELinux labels:

cp /usr/share/doc/audit/auditd.cron /etc/cron.daily

SEE ALSO

auditd.conf(5), **auditd**(8), **cron(8).**

AUTHOR

Attila Lakatos