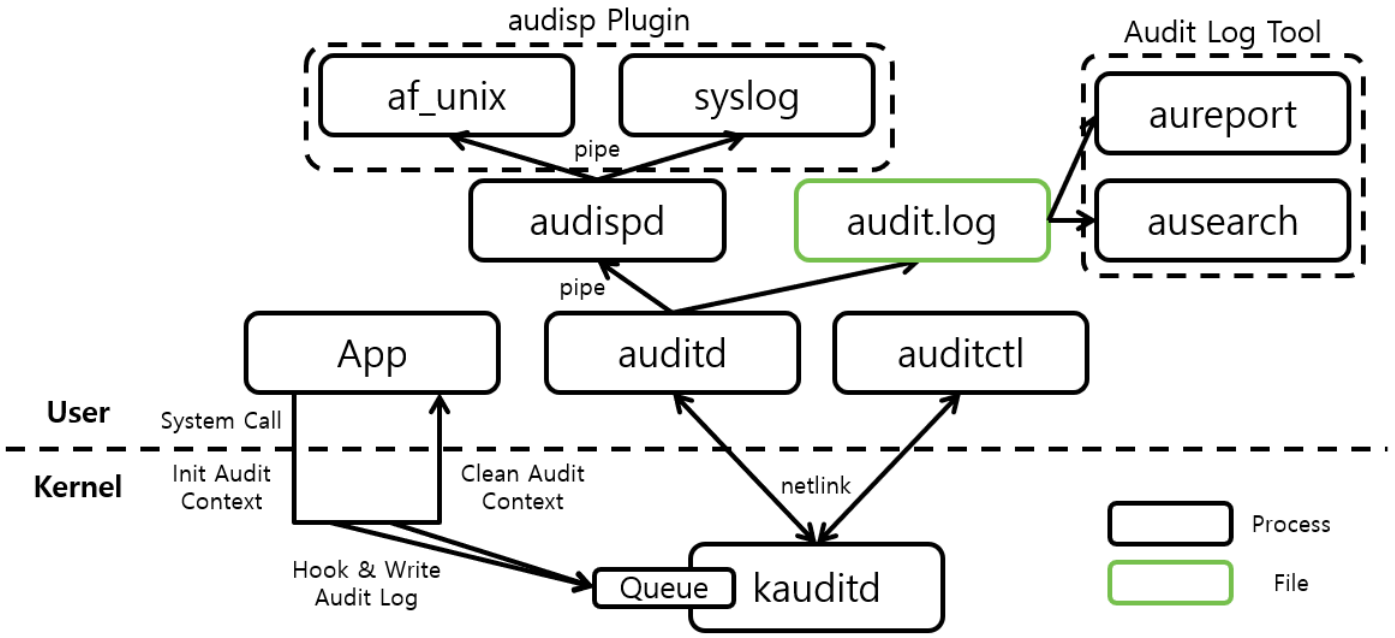
# Настройка AuditD на Unix системах

> Информация, приведенная на данной странице, является разработкой команды pre-sales и/или community KUMA и **НЕ** является официальной рекомендацией вендора.

## Архитектура Auditd




## Настройка AuditD

Для начала необходимо проврить установлена нужная служба auditd, посмотрим активные правила:

```
auditctl -l
```

В случае наличия подобной ошибки:


Необходимо установить следующие пакеты:

```
apt-get install auditd audispd-plugins
```

Либо (если RHEL подобные ОС):

```
yum install audit audispd-plugins
```

Рекомендуем использовать следующие правила для аудита:

```
wget -O audit.rules https://raw.githubusercontent.com/Neo23x0/auditd/master/audit.rules
```

Загрузить файл с правилами аудита с портала box.kaspersky.com - **тут**.

> Другие правила аудита можно найти в этой статье - https://kb.kuma-community.ru/link/14#bkmrk-linux

Рекомендуем добавить записи в конец файла `audit.rules`, для быстрого добавления используйте команду ниже (после выполните `systemctl restart auditd.service`):

```
cat << EOF >> /etc/audit/rules.d/audit.rules
# root authorized_keys
-w /root/.ssh/authorized_keys -p wa -k rootkey

# motd audit
-w /etc/update-motd.d/ -p wa -k motd

# udev audit
-w /etc/udev/rules.d/ -p wa -k udev

# xdg audit
-w /etc/xdg/autostart/ -p wa -k xdg
-w /usr/share/autostart/ -p wa -k xdg

# Package Manager (APT/YUM/DNF)
-w /etc/yum/pluginconf.d/ -p wa -k package_man
-w /etc/apt/apt.conf.d/ -p wa -k package_man
```

```
-w /etc/dnf/plugins/dnfcon.conf -p wa -k package_man

# exta systemd
-w /usr/lib/systemd/ -p wa -k systemd
-w /lib/systemd/ -p wa -k systemd
-w /usr/local/lib/systemd/ -p wa -k systemd
-w /usr/local/share/systemd/user -p wa -k systemd_user
-w /usr/share/systemd/user  -p wa -k systemd_user

# setcap audit
-w /usr/sbin/setcap -p x -k setcap

# rc audit
-w /etc/rc.local -p wa -k rclocal

## extra Shell/profile configurations
-w /etc/bash.bashrc -p wa -k shell_profiles
-w /etc/bash.bash_logout -p wa -k shell_profiles
-w /root/.profile -p wa -k shell_profiles
-w /root/.bashrc -p wa -k shell_profiles
-w /root/.bash_logout -p wa -k shell_profiles
-w /root/.bash_profile -p wa -k shell_profiles
-w /root/.bash_login -p wa -k shell_profiles

# extra search files
-w /usr/bin/find -p x -k T1083_File_And_DIrectory_Discovery

## Kernel Related Events
-w /usr/sbin/modprobe -p x -k T1547_Boot_or_Logon_Autostart_Execution
-w /usr/sbin/insmod -p x -k T1547_Boot_or_Logon_Autostart_Execution
-w /usr/sbin/lsmod -p x -k T1547_Boot_or_Logon_Autostart_Execution
-w /usr/sbin/rmmod -p x -k T1547_Boot_or_Logon_Autostart_Execution
-w /usr/sbin/modinfo -p x -k T1547_Boot_or_Logon_Autostart_Execution
-w /etc/modprobe.conf -p wa -k T1547.006_6
-w /etc/sysctl.conf -p wa -k sysctl

# extra file manipulation
-w /usr/bin/ftp -p x -k T1105_remote_file_copy
-w /usr/bin/sftp -p x -k T1105_remote_file_copy
-w /usr/bin/rsync -p x -k T1105_remote_file_copy
```

```
-w /usr/bin/cp -p x -k T1005_Data_from_Local_System
-w /usr/bin/dd -p x -k T1005_Data_from_Local_System
-a always,exit -F arch=b32 -S execve -S execveat -F exe=/usr/bin/shred -F -k T1070.004_1
-a always,exit -F arch=b64 -S execve -S execveat -F exe=/usr/bin/shred -F -k T1070.004_2

EOF
```

Другие  правила аудита и полезные материалы по AuditD можно найти - **тут**.

Далее нужно переместить правила в директорию по умолчанию и применить правила перезапуском сервиса:

```
cp audit.rules /etc/audit/rules.d/
systemctl restart auditd.service
systemctl enable auditd.service
```

**В случае ошибки рестарта службы auditd (Failed to restart auditd.service)**

На RHEL подобных ОС, может встретиться следующая ошибка:

*Failed to restart auditd.service: Operation refused, unit auditd.service may be requested by dependency only (it is configured to refuse manual start/stop).*
*See system logs and 'systemctl status auditd.service' for details.*

```
nano /usr/lib/systemd/system/auditd.service
```

Измените параметр `RefuseManualStop` на:

```
RefuseManualStop=no
```

Затем обновите параметры службы:

```
systemctl daemon-reload
```

Для проверки убедитесь что следующий лог наполняется информацией:

```
tail -f /var/log/audit/audit.log
```

> Рекомендуемый парсер (без агрегации/склейки событий) для правил корреляции Community - **[2024-09-23] Unix AuditD (REGEX)** (из Community-Pack)

# Известные проблемы

Бывают случаи, когда из-за ротации самого себя auditd (собственная ротация) падает в статусе сервиса:
*Sep 24 00:11:42 example.org auditd[756]: Audit daemon rotating log files*

В таком статусе лог файл не пополняется, рекомендуется использовать системную ротацию logrotate.

Сначала отключается собственная ротация auditd, правим конфиг:

```
nano /etc/audit/auditd.conf
```

Правим занчение (выделено жирным): `max_log_file_action = **ignore**`

Затем настраивается системная ротация logrotate.

```
touch /etc/logrotate.d/auditd
chmod 644 /etc/logrotate.d/auditd; chown root:root /etc/logrotate.d/auditd
nano /etc/logrotate.d/auditd
```

Пишем в файле auditd:

```
# daily rotation keep last 2 days and compress old
/var/log/audit/audit.log {
    daily
    missingok
    notifempty
    sharedscripts
    rotate 2
    compress
    delaycompress
    postrotate
        /usr/bin/systemctl kill -s USR1 auditd.service >/dev/null 2>&1 || true
    endscript
}
```

Перезапускаем службы logrotate и auditd:

```
systemctl restart logrotate.service; systemctl restart auditd.service
```

# Удаленная отправка логов auditd

Иногда место на сервере ограничено и хранить объемный лог audutd нет возможности, для этого можно настроить отправку логов сразу на удаленный сервер, для этого будем использовать плагин audispd-plugins, который мы загружали выше.

Отключим локальное ведение логов аудита в файле /etc/audit/auditd.conf выставляем значение write_logs = no:

```
root@kuma# nano /etc/audit/auditd.conf


local_events = yes
write_logs = no
name_format = HOSTNAME
```

Теперь нам нужно исправить файл по примеру ниже для отправки логов на удаленный сервер:

```
root@kuma# nano /etc/audit/plugins.d/au-remote.conf


active = yes
direction = out
path = /sbin/audisp-remote
type = always
#args =
format = string
```

Далее нужно отредактировать файл /etc/audit/audisp-remote.conf следующим образом:

```
root@kuma# nano /etc/audit/audisp-remote.conf


#
# This file controls the configuration of the audit remote
# logging subsystem, audisp-remote.
#

remote_server = 192.168.0.100
port = 16666
transport = tcp
```

```
queue_file = /var/spool/audit/remote.log
mode = immediate
queue_depth = 10240
format = ascii
network_retry_time = 2
max_tries_per_record = 3
max_time_per_record = 5
heartbeat_timeout = 0

network_failure_action = stop
disk_low_action = ignore
disk_full_action = warn_once
disk_error_action = warn_once
remote_ending_action = reconnect
generic_error_action = syslog
generic_warning_action = syslog
queue_error_action = stop
overflow_action = syslog
startup_failure_action = warn_once_continue

##krb5_principal =
##krb5_client_name = auditd
##krb5_key_file = /etc/audisp/audisp-remote.key
```

Теперь нужно перезапустить сервис auditd для применения обновленных конфигураций :

```
systemctl restart auditd.service
```

Сырые события будут без заголовка syslog, парсер Unix из персейл-пака обработает корректно такие логи:

```
node=kuma-aio.local type=PROCTITLE msg=audit(1704808440.087:50482):
proctitle=2F7362696E2F617564697463746C002D52002F6574632F61756469742F61756469742E72756C6573
```

---

Revision #25
Created 14 August 2023 07:31:00 by Boris Rzr
Updated 22 November 2024 12:22:32 by Boris Rzr