Samba – подробное логирование

Включение модуля full_audit, позволяет увидеть кто и к какому файлу обращался, кто создал, удалил или переименовал конкретный файл или каталог.

Количество сообщений, записываемых в лог-файлы, для всех VFS модулей может быть задано следующим параметром в секции [global]:

log level = 0 vfs:2

Если планируется сохранять лог-файлы длительное время, может быть полезным указание параметра

max log size = 0

Размер лог-файла задается в килобайтах. При достижении указанного значения файл будет переименован, путем добавления к имени файла расширения *.old*. Значение 0 отключает проверку размера (в этом случае необходимо самостоятельно позаботиться о размере лог-файла, к примеру, настроив соответсвующим образом logrotate).

Для активации модуля аудита, в секции, которая описывает расшаренный ресурс, добавляется строка

vfs objects = full_audit

В результате данные о доступе к файлам будут записываться в syslog, либо в лог-файл по умолчанию (log.smbd). Здесь же, *через пробел*, могут быть заданы *другие* VFS модули.

Можно указать дополнительные параметры модулю full_audit. Префикс, сообщений в лог-файле:

full_audit:prefix = %u|%I

(каждая строка будет начинаться с user|ip_adress)

Какие ошибки должны отображаться в лог-файле:

full_audit:failure = none

(не протоколируем ошибки)

Действия пользователей, которые записываются в лог-файл

full_audit:success = connect disconnect opendir mkdir rmdir closedir open close read pread write pwrite sendfile rename unlink chmod fchmod chown fchown chdir ftruncate lock symlink readlink link mknod realpath

Параметры, позволяющие управлять записью в журналы демоном syslogd:

full_audit:facility = local5
full_audit:priority = notice

Пример, в секции [global]:

```
# Подробный лог
log level = 0 vfs:2
max log size = 0

vfs objects = full_audit recycle
full_audit:prefix = %u|%I|%S
full_audit:failure = none
full_audit:success = mkdir rmdir open read pread write pwrite sendfile rename unlink lock
full_audit:facility = local5
full_audit:priority = notice
```

- full_audit:prefix – %u – имя пользователя, %I – его IP, %S – имя расшареного ресурса (если ресурс один смысла в нем нет)
- full_audit:success – какие удачные события будут логироваться
- full_audit:failure – то же самое, что выше, только для ошибок
- full_audit:facility – категория событий syslog, в которую будут попадать записи
- full_audit:priority – приоритет записей для syslog. Для самбы будет достаточно приоритета notice, чем ее записи

по сути и являются

Чтобы сообщения записывались в заданный файл, нужно добавить в

```
# vi /etc/rsyslog.conf

## SAMBA
local5.notice -/var/log/samba/audit.log
```

- mkdir – создание директории;
- rmdir – удаление директории;
- open – в какую папку заходили или открывали файл;
- close – с какой папки вышли или закрыли файл;
- read, pread – чтение(открытие) файла;
- write,pwrite – запись (изменение) файла/папки;
- rename – переименование файла/папки;
- unlink – удаление.

В логах, будут в зависимости от действий такие записи:

Создание файла

```
Jan 5 13:57:29 sdata smbd_audit: lera|192.168.113.11|open|ok|w|Новый текстовый документ.txt
```

Создание директории

```
Jan 5 13:58:03 sdata smbd_audit: lera|192.168.113.11|mkdir|ok|Новая папка
```

Открытие директории

```
Jan 5 13:58:03 sdata smbd_audit: lera|192.168.113.11|open|ok|r|Новая папка
```

Открытие файла

```
Jan 5 13:59:32 sdata smbd_audit: lera|192.168.113.11|open|ok|r|Новый текстовый документ.txt
```

Сохранение файла

```
Jan 5 14:00:05 sdata smbd_audit: lera|192.168.113.11|open|ok|w|Новый текстовый документ.txt
```

Копирование файла на сетовой диск

```
Jan       5       13:54:52       sdata       smbd_audit:
lera|192.168.113.11|open|ok|w|200628876x7vPywJ5wrJsY5NUCXC_NVk
HQbMrzQlv.pdf
```

Удаление файла

```
Jan       5       13:55:07       sdata       smbd_audit:
lera|192.168.113.11|unlink|ok|200628876x7vPywJ5wrJsY5NUCXC_NVk
HQbMrzQlv.pdf
```

Удаление директории

```
Jan       5       14:00:58       sdata       smbd_audit:
lera|192.168.113.11|rmdir|ok|Новая папка
```

Прцесс копирование на диск каталога “stat” с файлами

```
Jan       5       14:01:56       sdata       smbd_audit:
lera|192.168.113.11|mkdir|ok|stat
Jan       5       14:01:56       sdata       smbd_audit:
lera|192.168.113.11|open|ok|r|stat
Jan       5       14:01:56       sdata       smbd_audit:
lera|192.168.113.11|open|ok|w|stat/proxystat.l
Jan       5       14:01:56       sdata       smbd_audit:
lera|192.168.113.11|open|ok|w|stat/sborka.sh
Jan       5       14:01:56       sdata       smbd_audit:
lera|192.168.113.11|open|ok|w|stat/traflogans.l
Jan       5       14:01:56       sdata       smbd_audit:
lera|192.168.113.11|open|ok|w|stat/z.pl
```

Настроим ротацию логов, для этого отредактируем /etc/logrotate.d/samba

```
/var/log/samba/* {
   daily
   notifempty
   olddir /var/log/samba/old
   missingok
   sharedscripts
   copytruncate
   rotate 90
```

```
    compress
}
```

Хранить логи за последние 90 дней, ротацию делать раз в день.