Ранее я неоднократно рассказывал, как настроить файловый сервер samba для совместной работы с файлами. При совместной работе часто бывает нужно знать, кто и когда что-то сделал с тем или иным файлом, а конкретно, кто удалил файл. По-умолчанию, такой лог не ведется, нужно настраивать отдельно. Займемся настройкой логирования операций с файлами в данной статье.

Содержание:

Введение

У меня есть две статьи по настройке файлового сервера samba:

1. Настройка Samba с интеграцией в Active Directory.
2. Быстрая настройка самбы с доступом по паролю или ip.

В обоих случаях будет не лишним настроить логирование всех обращений к файлам на сервере. Делается это штатными возможностями самой самбы. Она будет отправлять логи в syslog, а в нем мы уже настроим их хранение и ротацию с помощью logrotate. На нагруженных серверах логи будут очень объемными. Нужно обязательно позаботиться об их хранении и удалении.

Я буду настраивать логи в samba на сервере CentOS 7. В других случаях отличий почти не будет. Сами настройки самбы везде одинаковые. Syslog и Logrotate тоже примерно одинаковые во всех дистрибутивах Linux.

Включаем логирование операций в samba

Для логирования действий пользователей на файловом сервере будем использовать модуль самбы **full_audit**. Если вы хотите выполнять логирование операций с файлами в один лог файл по всем доступным шарам, то добавляйте настройки аудита в глобальную секцию. Если же захотите разделить по шарам, то отдельно в каждую шару с небольшими изменениями. Я рассмотрю оба варианта. Для начала, настроим аудит по всем шарам в один общий файл. Добавляем в */etc/samba/smb.conf* в секцию **[global]** следующие строки:

```
log level = 1 vfs:1
full_audit:prefix = %u|%I|%S
full_audit:success = connect, open, mkdir, rmdir, unlink, write, rename
full_audit:failure = connect, open, mkdir, rmdir, unlink, write, rename
full_audit:facility = local5
full_audit:priority = notice
vfs objects = full_audit
```

Поясню каждый параметр.

full_audit:prefix	В каком формате будет выводиться информация о подключении: %u - имя пользователя, %I - его ip адрес, %S - название шары.
full_audit:success	Какие удачные события будут логироваться. В приведенном примере по смыслу и так понятно, о чем речь. Полный список событий такой: chdir, chflags, chmod, chmod_acl, chown, close, closedir, connect, disconnect, disk_free, fchmod, fchmod_acl, fchown, fget_nt_acl, fgetxattr, flistxattr, fremovexattr, fset_nt_acl, fsetxattr, fstat, fsync, ftruncate, get_nt_acl, get_quota, get_shadow_copy_data, getlock, getwd, getxattr, kernel_flock, link, linux_setlease, listxattr, lock, lseek, lstat, mkdir, mknod, open, opendir, pread, pwrite, read, readdir, readlink, realpath, removexattr, rename, rewinddir, rmdir, seekdir, sendfile, set_nt_acl, set_quota, setxattr, stat, statvfs, symlink, sys_acl_delete_def_file, sys_acl_get_fd, sys_acl_get_file, sys_acl_set_fd, sys_acl_set_file, telldir, unlink, utime, write.
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.

Если вы хотите настроить вывод лога доступа с разных шар в отдельные файлы, то указанные выше параметры поместите не в глобальную, а отдельно в каждую секцию с шарой, изменив категории событий, сделав их в каждой шаре уникальными, например local5 и local6. Так же нужно будет в каждую шару отдельно добавить еще один параметр:

```
vfs objects = full_audit
```

После изменения конфигурации, не забудьте перезапустить самбу. Если больше ничего не делать, то логи посещений самбы польются в стандартный поток вывода для системных логов. В Centos в */var/log/messages*. Это очень неудобно, поэтому далее настроим вывод логов в отдельный файл.

Вывод лога доступа к файлам samba в отдельный файл

Нам нужно отредактировать файл конфигурации **rsyslog** для направления вывода лога самбы в отдельный файл. В CentOS 7 открываем файл */etc/rsyslog.conf* и добавляем в самый конец такую строку:

```
# mcedit /etc/rsyslog.conf
```

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

Этим параметром мы направили вывод логов аудита посещений в отдельный файл *audit.log*. Если все оставить как есть, то информация о посещениях будет писаться как в отдельный файл, так и в общий системный. Чтобы в общий не писалось, редактируем еще одну строку, добавляя туда выделенный фрагмент:

```
*.info;mail.none;authpriv.none;cron.none;local5.none /var/log/messages
```

Сохраняем файл и перезапускаем rsyslog.

```
# systemctl restart rsyslog
```

Теперь все нормально. Все логи посещений шары на samba будут складываться в отдельный файл и только туда. Если у вас есть желание хранить логи на удаленном сервере, то воспользуйтесь моей статье на эту тему - настройка syslog-ng для удаленного сбора логов. Это сделать быстро и просто. Зачастую это может быть оправданно и удобно, особенно с точки зрения безопасности и не только логов от самбы.

Осталось малось - настроить ротацию логов. Сделать это надо обязательно, так как файл аудита будет расти очень быстро. Здесь ничего особенного, используем logrotate. Скорее всего у вас уже есть фал конфигурации logrotate для самбы. Он создается в момент установки. Отредактируем его, добавив новые параметры.

```
# mcedit /etc/logrotate.d/samba
```

```
/var/log/samba/audit.log {
 daily
 notifempty
 olddir /var/log/samba/old
 missingok
 sharedscripts
 copytruncate
 rotate 90
 compress
}
```

Я храню логи за последние 90 дней, ротацию делаю раз в день и складываю старые логи в отдельную папку. Если у вас в конфигурации есть параметр с маской, который захватывает сразу все файлы в директории */var/log/samba*, например вот так:

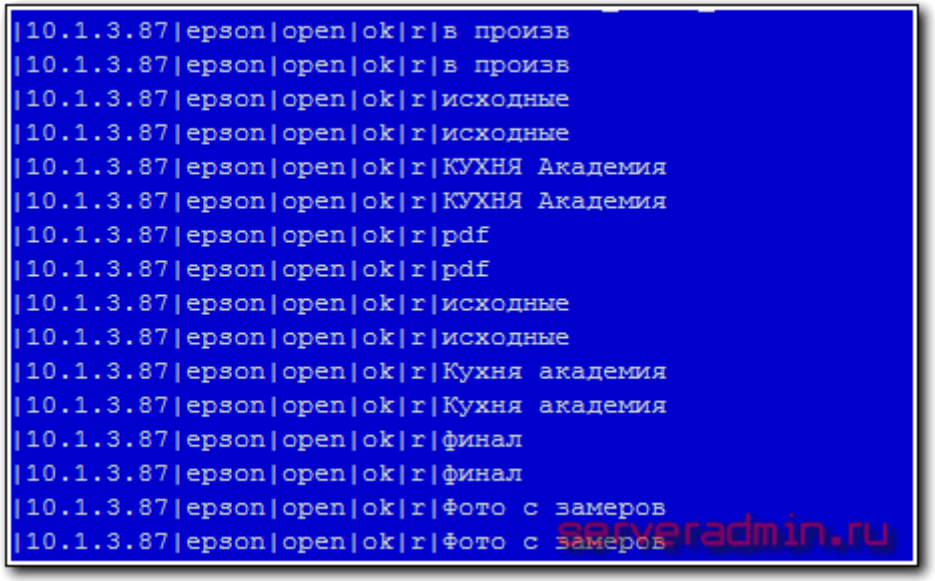
```
/var/log/samba/*
```

То либо вынесите лог-файл с аудитом в отдельную директорию, либо измените маску.

Заключение

Я уже давно заметил один неприятный баг в самбе 4-й версии. Привожу пример того, как выглядит лог посещений файловой шары самбы с русскими названиями в именах на 3 и 4-й версии. В данном случае сначала версия 3.6.3, потом 4.6.2

```
|10.1.3.14|epson|open|ok|r|Дизайнеры/Ro     a/!Общая/В Перегеше на горе Зеленая выпал первый снег_files/s.js.Без названия
|10.1.3.14|epson|open|ok|r|Дизайнеры/Ro     a/!Общая/В Перегеше на горе Зеленая выпал первый снег_files/saved_resource(1).html
|10.1.3.14|epson|open|ok|r|Дизайнеры/Ro     a/!Общая/В Перегеше на горе Зеленая выпал первый снег_files/saved_resource(10).html
|10.1.3.14|epson|open|ok|r|Дизайнеры/Ro     a/!Общая/В Перегеше на горе Зеленая выпал первый снег_files/saved_resource(11).html
|10.1.3.14|epson|open|ok|r|Дизайнеры/Ro     a/!Общая/В Перегеше на горе Зеленая выпал первый снег_files/saved_resource(12).html
|10.1.3.14|epson|open|ok|r|Дизайнеры/Ro     a/!Общая/В Перегеше на горе Зеленая выпал первый снег_files/saved_resource(13).html
|10.1.3.14|epson|open|ok|r|Дизайнеры/Ro     a/!Общая/В Перегеше на горе Зеленая выпал первый снег_files/saved_resource(2).html
|10.1.3.14|epson|open|ok|r|Дизайнеры/Ro     a/!Общая/В Перегеше на горе Зеленая выпал первый снег_files/saved_resource(3).html
|10.1.3.14|epson|open|ok|r|Дизайнеры/Ro     a/!Общая/В Перегеше на горе Зеленая выпал первый снег_files/saved_resource(4).html
|10.1.3.14|epson|open|ok|r|Дизайнеры/Ro     a/!Общая/В Перегеше на горе Зеленая выпал первый снег_files/saved_resource(5).html
|10.1.3.14|epson|open|ok|r|Дизайнеры/Ro     a/!Общая/В Перегеше на горе Зеленая выпал первый снег_files/saved_resource(6).html
|10.1.3.14|epson|open|ok|r|Дизайнеры/Ro     a/!Общая/В Перегеше на горе Зеленая выпал первый снег_files/saved_resource(7).html
|10.1.3.14|epson|open|ok|r|Дизайнеры/Ro     a/!Общая/В Перегеше на горе Зеленая выпал первый снег_files/saved_resource(8).html
|10.1.3.14|epson|open|ok|r|Дизайнеры/Ro     a/!Общая/В Перегеше на горе Зеленая выпал первый снег_files/saved_resource(9).html
```



В первом случае отображаются полные корректные пути. Во втором случае на события типа **open** идут только обрывки названий директорий, по которым не понятен полный путь. Делаю важный акцент - только на события open. Если идут события создания, удаления, изменения, то пути уже корректны, даже если они русские. В принципе, события на доступ лично для меня обычно не важны. Интерес представляет только создание, изменение и особенно удаление файлов. С этим все в порядке. Аудит показывает корректный лог удаления файлов. Но все равно не приятно смотреть на неинформативный лог.

Возможно, дело не в 3-1 и 4-й версии. Я не проверял различные изменения в рамках одной и той же ветки. Просто посмотрел на имеющиеся у меня сервера. Там где 3-я версия все в порядке, там где 4-я везде такой бардак в логах. Если кто-то знает, как от него избавиться, прошу поделиться.