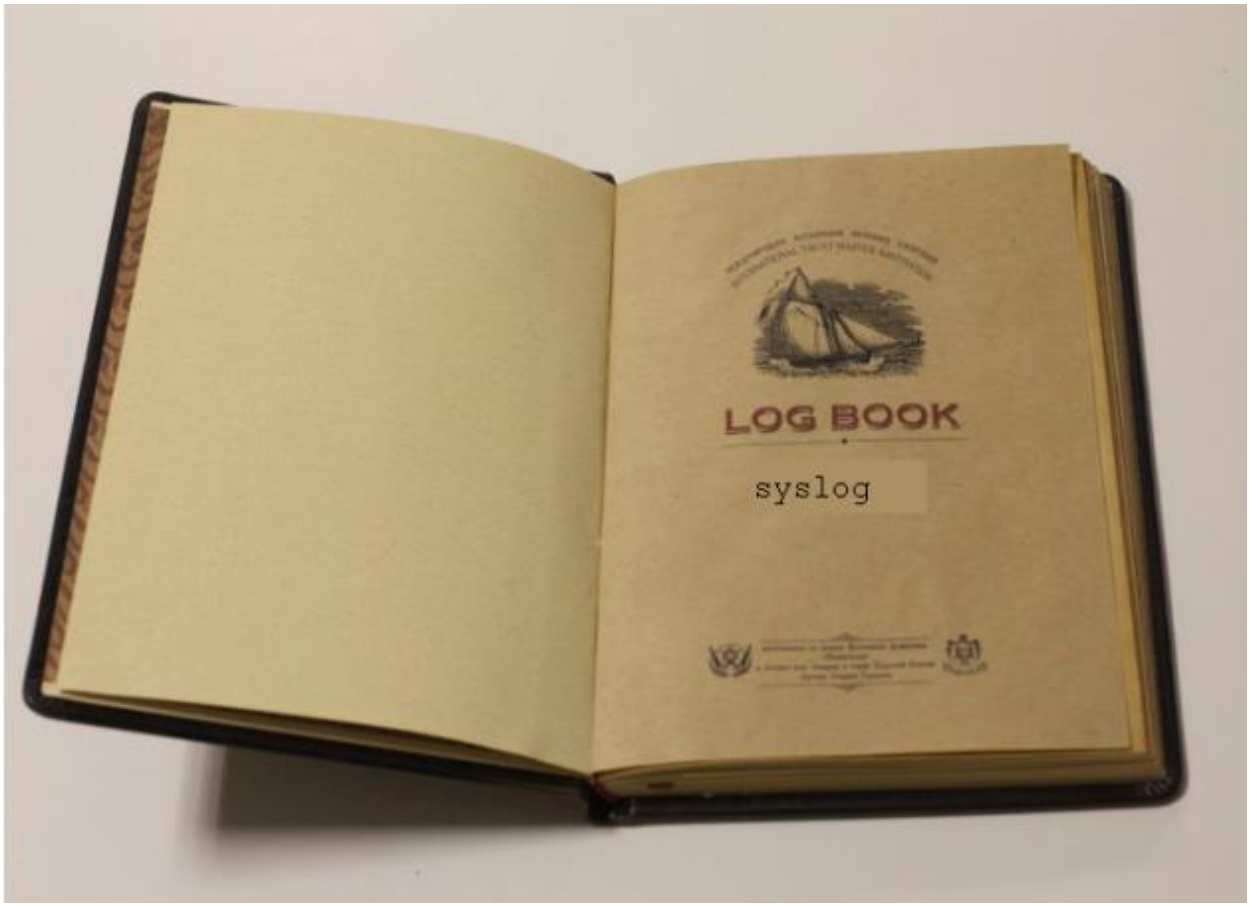

Невозможно представить себе пользователя и администратора сервера, или даже рабочей станции на основе Linux, который никогда не читал лог файлы. Операционная система и работающие приложения постоянно создают различные типы сообщений, которые регистрируются в различных файлах журналов. Умение определить нужный файл журнала и что искать в нем поможет существенно сэкономить время и быстрее устранить ошибку. Журналирование является основным

источником информации о работе системы и ее ошибках. В этом кратком руководстве рассмотрим основные аспекты журналирования операционной системы, структуру каталогов, программы для чтения и обзора логов.

Основные лог файлы

Все файлы журналов, можно отнести к одной из следующих категорий:

- приложения;
- события;
- службы;
- системный.

Большинство же лог файлов содержится в директории /var/log.

- **/var/log/syslog** или **/var/log/messages** содержит глобальный системный журнал, в котором пишутся сообщения с момента запуска системы, от ядра Linux, различных служб, обнаруженных устройствах, сетевых интерфейсов и много другого.
- **/var/log/auth.log** или **/var/log/secure** — информация об авторизации пользователей, включая удачные и неудачные попытки входа в систему, а также задействованные механизмы аутентификации.

- **/var/log/dmesg** — драйвера устройств. Одноименной командой можно просмотреть вывод содержимого файла. Размер журнала ограничен, когда файл достигнет своего предела, старые сообщения будут перезаписаны более новыми. Задав ключ --level= можно отфильтровать вывод по критерию значимости.
- **/var/log/alternatives.log** — Вывод программы update-alternatives, в котором находятся символические ссылки на команды или библиотеки по умолчанию.
- **/var/log/anaconda.log** — Записи, зарегистрированные во время установки системы.
- **/var/log/audit** — Записи, созданные службой аудита auditd.
- **/var/log/boot.log** — Информация, которая пишется при загрузке операционной системы.
- **/var/log/cron** — Отчет службы crond об исполняемых командах и сообщения от самих команд.
- **/var/log/cups** — Все, что связано с печатью и принтерами.
- **/var/log/faillog** — Неудачные попытки входа в систему. Очень полезно при проверке угроз в системе

безопасности, хакерских атаках, попыток взлома методом перебора. Прочитать содержимое можно с помощью команды faillog.

- **var/log/kern.log** — Журнал содержит сообщения от ядра и предупреждения, которые могут быть полезны при устранении ошибок пользовательских модулей встроенных в ядро.
- **/var/log/maillog/** или **/var/log/mail.log** — Журнал почтового сервера, используемого на ОС.
- **/var/log/pm-powersave.log** — Сообщения службы экономии заряда батареи.
- **/var/log/samba/** — Логи файлового сервера Samba, который используется для доступа к общим папкам Windows и предоставления доступа пользователям Windows к общим папкам Linux.
- **/var/log/spooler** — Для представителей старой школы, содержит сообщения USENET. Чаще всего бывает пустым и заброшенным.
- **/var/log/Xorg.0.log** — Логи X сервера. Чаще всего бесполезны, но если в них есть строки начинающиеся с EE, то следует обратить на них внимание.

Для каждого дистрибутива будет отдельный журнал менеджера пакетов.

- **/var/log/yum.log** — Для программ установленных с помощью Yum в RedHat Linux.
- **/var/log/emerge.log** — Для ebuild-ов установленных из Portage с помощью emerge в Gentoo Linux.
- **/var/log/dpkg.log** — Для программ установленных с помощью dpkg в Debian Linux и всем семействе родственных дистрибутивах.

И немного бинарных журналов учета пользовательских сессий.

- **/var/log/lastlog** — Последняя сессия пользователей. Прочитать можно командой last.
- **/var/log/tallylog** — Аудит неудачных попыток входа в систему. Вывод на экран с помощью утилиты pam_tally2.
- **/var/log/btmp** — Еже один журнал записи неудачных попыток входа в систему. Просто так, на всякий случай, если вы еще не догадались где следует искать следы активности взломщиков.

- **/var/log/utmp** — Список входов пользователей в систему на данный момент.
- **/var/log/wtmp** — Еще один журнал записи входа пользователей в систему. Вывод на экран командой utmpdump.

И другие журналы

Так как операционная система, даже такая замечательная как Linux, сама по себе никакой ощутимой пользы не несет в себе, то скорее всего на сервере или рабочей станции будет крутится база данных, веб сервер, разнообразные приложения. Каждое приложения или служба может иметь свой собственный файл или каталог журналов событий и ошибок. Всех их естественно невозможно перечислить, лишь некоторые.

- **/var/log/mysql/** — Лог базы данных MySQL.
- **/var/log/httpd/** или **/var/log/apache2/** — Лог веб сервера Apache, журнал доступа находится в access_log, а ошибки — в error_log.
- **/var/log/lighthttpd/** — Лог веб сервера lighttpd.

В домашнем каталоге пользователя могут находится журналы графических приложений, DE.

- **~/.xsession-errors** — Вывод stderr графических приложений X11.
- **~/.xfce4-session.verbose-log** — Сообщения рабочего стола XFCE4.

Чем просматривать — lnav

Почти все знают об утилите less и команде tail -f. Также для этих целей сгодится редактор vim и файловый менеджер Midnight Commander. У всех есть свои недостатки: less неважно обрабатывает журналы с длинными строками, принимая их за бинарники. Midnight Commander годится только для беглого просмотра, когда нет необходимости искать по сложному шаблону и переходить помногу взад и вперед между совпадениями. Редактор vim понимает и подсвечивает синтаксис множества форматов, но если журнал часто обновляется, то появляются отвлекающие внимания сообщения об изменениях в файле. Впрочем это легко можно обойти с помощью <:view /path/to/file>.

еще есть утилитаНавигатор журналов *lnav* понимает ряд форматов файлов.

- Access_log веб сервера.
- CUPS page_log
- Syslog

- glog
- dpkg.log
- strace
- Произвольные записи с временными отметками
- gzip, bzip
- Журнал VMWare ESXi/vCenter

Что в данном случае означает понимание форматов файлов- *lnav* больше чем утилита для просмотра текстовых файлов. Программа умеет кое что еще. Можно открывать несколько файлов сразу и переключаться между ними. Кроме этого поддерживается подсветка синтаксиса, дополнение по табу и разные полезности в статусной строке. К недостаткам можно отнести нестабильность поведения и зависания.

вопрос	ответ
Какой файл логов поможет при проверке безопасности при авторизации в систему	/var/log/faillog
в каком файле смотреть логи неудачных попыток авторизации	/var/log/auth.log или /var/log/secure
Что делает команда ls /var/log	Команда **ls** –наиболее используемая команда в любой **UNIX**-системе. Её предназначение – вывод

	информации о файлах и каталогах. Дополнительные опции команды позволяют получить более подробную информацию и сортировать её определённым образом.
Какой командой посмотреть логи журнала сообщений от ядра в реальном времени?	/var/log/syslog **или** /var/log/messages
Какая команда покажет, кто из пользователей сейчас залогинен в системе и когда он зашел?	/var/log/utmp
Какая команда дает понять, когда пользователь заходил в систему и сколько времени в ней находился?	/var/log/wtmp /var/log/lastlog
Какой самый простой способ посмотреть логи (открыть лог файл) syslog?	Команда “tail -f /var/log/syslog” позволит наблюдать запись логов в реальном времени.