ЛОГИ (ЖУРНАЛ СЕРВЕРА) В LINUX.

ЧТО ТАКОЕ ЛОГИ

Все системы Linux создают и хранят файлы логов информации для процессов загрузки, приложений и других событий. Эти файлы могут быть полезным ресурсом для устранения неполадок системы. Логи (журнал сервера, англ. server log) – это записываемые фрагменты данных, описывающие то, что в конкретный момент времени делает сервер, ядро, службы и приложения.
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.

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.

Поддерживаемые уровни журналирования (приоритеты):

```
  emerg - система неиспользуемая
  alert - действие должно быть произведено немедленно
   crit - условия критичности
    err - условия ошибок
   warn - условия предупреждений
 notice - обычные, но значимые условия
   info - информационный
  debug - отладочные сообщения

(5:520)$ dmesg -l err
[1131424.604352] usb 1-1.1: 2:1: cannot get freq at ep 0x1
[1131424.666013] usb 1-1.1: 1:1: cannot get freq at ep 0x81
```

```
[1131424.749378] usb 1-1.1: 1:1: cannot get freq at ep 0x81
```

- **/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.

```
(5:535)$ sudo utmpdump /var/log/wtmp
[5] [02187] [l0  ] [        ] [4.0.5-gentoo     ] [0.0.0.0     ] [Вт авг 11 16:50:07 2015]
[1] [00000] [~~  ] [shutdown] [4.0.5-gentoo     ] [0.0.0.0     ] [Вт авг 11 16:50:08 2015]
[2] [00000] [~~  ] [reboot  ] [3.18.12-gentoo   ] [0.0.0.0     ] [Вт авг 11 16:50:57 2015]
[8] [00368] [rc  ] [        ] [3.18.12-gentoo   ] [0.0.0.0     ] [Вт авг 11 16:50:57 2015]
[1] [20019] [~~  ] [runlevel] [3.18.12-gentoo   ] [0.0.0.0     ] [Вт авг 11 16:50:57 2015]
```

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.

```
Initializing  "kcm_input" :  "kcminit_mouse"
Initializing  "kcm_access" :  "kcminit_access"
Initializing  "kcm_kgamma" :  "kcminit_kgamma"
QXcbConnection: XCB error: 3 (BadWindow), sequence: 181, resource id: 10486050, major code: 20 (GetProperty), minor code: 0
kf5.kcoreaddons.kaboutdata: Could not initialize the equivalent properties of Q*Application: no instance (yet) existing.
QXcbConnection: XCB error: 3 (BadWindow), sequence: 181, resource id: 10486050, major code: 20 (GetProperty), minor code: 0
Qt: Session management error: networkIdsList argument is NULL
```

- **~/.xfce4-session.verbose-log** — Сообщения рабочего стола XFCE4.

ХРАНЕНИЕ И СОЗДАНИЕ ЛОГОВ

Большинство файлов логов Linux хранятся в простом текстовом файле ASCII и находятся в каталоге и подкаталоге /var/log. Логи создаются системным демоном логов Linux, syslogd или rsyslogd.

Используйте следующий пример строковой команды для доступа к соответствующему файлу:

```
sudo less [log name here].log
```

Эта команда отображает временную шкалу всей информации, относящейся к этой операции.

Обратите внимание, что файлы логов хранятся в виде обычного текста, поэтому их можно просматривать с помощью следующих стандартных команд:

- zcat - Отображает все содержимое logfile.gz
- zmore - Просмотр файла по страницам, не распаковывая файлы
- zgrep - Поиск внутри сжатого файла
- grep - Найти все вхождения поискового запроса в файле или отфильтровать файл логов
- tail - Выводит последние несколько строк файлов
- head - Просмотр самого начала текстовых файлов
- vim - Просмотр при помощи текстового редактора vim
- nano - Просмотр при помощи текстового редактора nano

ВАЖНЫЕ СИСТЕМНЫЕ ЛОГИ LINUX

Логи могут многое рассказать о работе системы. Хорошее понимание каждого типа файла поможет различать соответствующие логи.

Большинство каталогов можно сгруппировать в одну из четырех категорий:

- Системные логи (System Logs)
- Логи событий (Event Logs)
- Логи приложений (Application Logs)
- Логи обслуживания (Service Logs)

Многие из этих логов могут быть расположены в подкаталоге var/log.

СИСТЕМНЫЕ ЛОГИ

Файлы логов необходимы для работы Linux. Они содержат значительный объем информации о функциональности системы.

КАК ПОСМОТРЕТЬ ЛОГИ В LINUX

Системные администраторы, да и обычные пользователи Linux, часто должны смотреть лог файлы для устранения неполадок. На самом деле, это первое, что должен сделать любой сисадмин при возникновении любой ошибки в системе.

Сама операционная система Linux и работающие приложения генерируют различные типы сообщений, которые регистрируются в различных файлах журналов. В Linux используются специальное программное обеспечение, файлы и директории для хранения лог файлов. Знание в каких файлах находятся логи каких программ поможет вам сэкономить время и быстрее решить проблему. В этой статье мы рассмотрим основные части системы логирования в Linux, файлы логов, а также утилиты, с помощью которых можно посмотреть логи Linux.

РАСПОЛОЖЕНИЕ ЛОГОВ ПО УМОЛЧАНИЮ

Большинство файлов логов Linux находятся в папке **/var/log/** вы можете список файлов логов для вашей системы с помощью команды ls:

```
ls -l /var/log/
```

Ниже мы рассмотрим 20 различных файлов логов Linux, размещенных в каталоге **/var/log/**. Некоторые из этих логов встречаются только в определенных дистрибутивах, например, **dpkg.log** встречается только в системах, основанных на Debian.

- **/var/log/messages** - содержит глобальные системные логи Linux, в том числе те, которые регистрируются при запуске системы. В этот лог записываются несколько типов сообщений: это почта, cron, различные сервисы, ядро, аутентификация и другие.
- **/var/log/dmesg** - содержит сообщения, полученные от ядра. Регистрирует много сообщений еще на этапе загрузки, в них отображается информация об аппаратных устройствах, которые инициализируются в процессе загрузки. Можно сказать это еще один лог системы Linux. Количество сообщений в логе ограничено, и когда файл будет переполнен, с каждым новым сообщением старые будут перезаписаны. Вы также можете посмотреть сообщения из этого лога с помощью команды dmseg.
- **/var/log/auth.log** - содержит информацию об авторизации пользователей в системе, включая пользовательские логины и механизмы аутентификации, которые были использованы.
- **/var/log/boot.log** - Содержит информацию, которая регистрируется при загрузке системы.
- **/var/log/daemon.log** - Включает сообщения от различных фоновых демонов
- **/var/log/kern.log** - Тоже содержит сообщения от ядра, полезны при устранении ошибок пользовательских модулей, встроенных в ядро.
- **/var/log/lastlog** - Отображает информацию о последней сессии всех пользователей. Это нетекстовый файл, для его просмотра необходимо использовать команду lastlog.
- **/var/log/maillog /var/log/mail.log** - журналы сервера электронной почты, запущенного в системе.
- **/var/log/user.log** - Информация из всех журналов на уровне пользователей.
- **/var/log/Xorg.x.log** - Лог сообщений X сервера.
- **/var/log/alternatives.log** - Информация о работе программы update-alternatives. Это символические ссылки на команды или библиотеки по умолчанию.
- **/var/log/btmp** - лог файл Linux содержит информацию о неудачных попытках входа. Для просмотра файла удобно использовать команду last -f /var/log/btmp
- **/var/log/cups** - Все сообщения, связанные с печатью и принтерами.
- **/var/log/anaconda.log** - все сообщения, зарегистрированные при установке сохраняются в этом файле
- **/var/log/yum.log** - регистрирует всю информацию об установке пакетов с помощью Yum.
- **/var/log/cron** - Всякий раз когда демон Cron запускает выполнения программы, он записывает отчет и сообщения самой программы в этом файле.
- **/var/log/secure** - содержит информацию, относящуюся к аутентификации и авторизации. Например, SSHd регистрирует здесь все, в том числе неудачные попытки входа в систему.
- **/var/log/wtmp или /var/log/utmp -** системные логи Linux**,** содержат журнал входов пользователей в систему. С помощью команды wtmp вы можете узнать кто и когда вошел в систему.
- **/var/log/faillog** - лог системы linux, содержит неудачные попытки входа в систему. Используйте команду faillog, чтобы отобразить содержимое этого файла.
- **/var/log/mysqld.log** - файлы логов Linux от сервера баз данных MySQL.

- **/var/log/httpd/ или /var/log/apache2** - лог файлы linux11 веб-сервера Apache. Логи доступа находятся в файле access_log, а ошибок в error_log
- **/var/log/lighttpd/** - логи linux веб-сервера lighttpd
- **/var/log/conman/** - файлы логов клиента ConMan,
- **/var/log/mail/** - в этом каталоге содержатся дополнительные логи почтового сервера
- **/var/log/prelink/** - Программа Prelink связывает библиотеки и исполняемые файлы, чтобы ускорить процесс их загрузки. /var/log/prelink/prelink.log содержит информацию о .so файлах, которые были изменены программой.
- **/var/log/audit/**- Содержит информацию, созданную демоном аудита auditd.
- **/var/log/setroubleshoot/ -** SE Linux использует демон setroubleshootd (SE Trouble Shoot Daemon) для уведомления о проблемах с безопасностью. В этом журнале находятся сообщения этой программы.
- **/var/log/samba/** - содержит информацию и журналы файлового сервера Samba, который используется для подключения к общим папкам Windows.
- **/var/log/sa/** - Содержит .cap файлы, собранные пакетом Sysstat.
- **/var/log/sssd/** - Используется системным демоном безопасности, который управляет удаленным доступом к каталогам и механизмами аутентификации.

ПРОСМОТР ЛОГОВ В LINUX

Чтобы посмотреть логи на Linux удобно использовать несколько утилит командной строки Linux. Это может быть любой текстовый редактор, или специальная утилита. Скорее всего, вам понадобятся права суперпользователя для того чтобы посмотреть логи в Linux. Вот команды, которые чаще всего используются для этих целей:

- less;
- more;
- cat;
- head;
- grep;
- tail;
- zcat;
- zgrep;
- zmore;
- vi;
- nano.

ЛОГИ ПРИЛОЖЕНИЙ

Логи приложений хранят информацию, относящуюся к любому запускаемому приложению. Это может включать сообщения об ошибках, признаки взлома системы и строку идентификации браузера.

Файлы логов, которые попадают в эту категорию, включают логи системы печати CUPS, лог Rootkit Hunter, логи HTTP-сервера Apache, логи SMB-сервера Samba и лог сервера X11.

ЛОГИ НЕ В УДОБОЧИТАЕМОМ ФОРМАТЕ

Не все логи созданы в удобочитаемом формате. Некоторые предназначены только для чтения системными приложениями. Такие файлы часто связаны с информацией для входа. Они включают логи сбоев входа в систему, логи последних входов в систему и записи входа в систему.

Существуют инструменты и программное обеспечение для чтения файлов логов Linux. Они не нужны для чтения файлов, так как большинство из них можно прочитать непосредственно с терминала Linux.

ГРАФИЧЕСКИЕ ИНТЕРФЕЙСЫ ДЛЯ ПРОСМОТРА ФАЙЛОВ ЛОГОВ LINUX

System Log Viewer - это графический интерфейс, который можно использовать для отслеживания системных логов.
Интерфейс предоставляет несколько функций для управления логами, включая отображение статистики лога. Это удобный графический интерфейс для мониторинга логов.

В качестве альтернативы можно использовать **Xlogmaster**, который может отслеживать значительное количество файлов логов.
Xlogmaster полезен для повышения безопасности. Он переводит все данные для выделения и скрытия строк и отображает эту информацию для выполнения действий, запрошенных пользователем.

КАК НАСТРОИТЬ ФАЙЛЫ ЛОГОВ В UBUNTU И CENTOS

Начнем с примера CentOS. Чтобы просмотреть пользователей, которые в настоящее время вошли на сервер Linux, введите команду who от имени пользователя root:

```
[root@localhost ~]# who
sofija   :0           2020-03-11 05:41 (:0)
sofija   pts/0        2020-03-11 05:41 (:0)
```

Здесь также отображается история входа в систему пользователей. Для просмотра истории входа системного администратора введите следующую команду:

```
last reboot
```

```
[root@localhost ~]# last reboot
reboot   system boot  3.10.0-1062.12.1 Wed Mar 11 05:28 - 05:45  (00:16)
reboot   system boot  3.10.0-1062.12.1 Thu Feb 27 05:22 - 05:45 (13+00:22)
reboot   system boot  3.10.0-1062.9.1. Tue Feb 25 06:25 - 05:45 (14+23:19)
reboot   system boot  3.10.0-1062.9.1. Mon Feb 24 05:52 - 05:45 (15+23:52)
reboot   system boot  3.10.0-1062.9.1. Tue Jan 28 08:47 - 05:45 (42+20:58)
reboot   system boot  3.10.0-1062.9.1. Mon Jan 27 08:18 - 05:45 (43+21:26)
reboot   system boot  3.10.0-1062.9.1. Wed Jan 15 05:24 - 05:45 (56+00:20)
reboot   system boot  3.10.0-1062.9.1. Wed Jan  8 05:18 - 05:45 (63+00:26)
reboot   system boot  3.10.0-1062.9.1. Wed Jan  8 03:20 - 05:45 (63+02:24)
```

Чтобы просмотреть информацию о последнем входе в систему, введите:

```
lastlog
```

```
[root@localhost ~]# lastlog
Username         Port     From             Latest
root             pts/0                     Wed Mar 11 05:41:59 -0400 2020
bin                                        **Never logged in**
daemon                                     **Never logged in**
adm                                        **Never logged in**
lp                                         **Never logged in**
sync                                       **Never logged in**
shutdown                                   **Never logged in**
halt                                       **Never logged in**
mail                                       **Never logged in**
operator                                   **Never logged in**
games                                      **Never logged in**
ftp                                        **Never logged in**
nobody                                     **Never logged in**
systemd-network                            **Never logged in**
```

ВЫПОЛНИТЬ РОТАЦИЮ ЛОГА

Файлы логов, в конце которых добавлены нули, являются повернутыми файлами. Это означает, что имена файлов логов были автоматически изменены в системе.

Целью ротации логов является сжатие устаревших логов, занимающих место. Ротацию лога можно выполнить с помощью команды logrotate. Эта команда вращает, сжимает и отправляет системные логи по почте.
logrotate обрабатывает системы, которые создают значительные объемы файлов логов. Эта команда используется планировщиком cron и считывает файл конфигурации logrotate /etc/logrotate.conf. Он также используется для чтения файлов в каталоге конфигурации logrotate.
Чтобы включить дополнительные функции для logrotate, начните с ввода следующей команды:

```
var/log/log name here].log {
Missingok
Notifempty
Compress
Size 20k
Daily
Create 0600 root root
}
```

Он сжимает и изменяет размер желаемого файла логов.

Команды выполняют следующие действия:

- missingok - сообщает logrotate не выводить ошибку, если файл логов отсутствует.
- notifempty - не выполняет ротацию файла логов, если он пуст. Уменьшает размер файла лога с помощью gzip
- size - гарантирует, что файл логов не превышает указанный размер, и поворачивает его в противном случае
- daily - меняет файлы журналов по ежедневному расписанию. Это также можно делать по недельному или ежемесячному расписанию.
- create - создает файл логов, в котором владелец и группа являются пользователем root

Тщательное понимание того, как просматривать и читать логи Linux, необходимо для устранения неполадок в системе Linux. Использование правильных команд и инструментов может упростить этот процесс.

ТАБЛИЦА «Вопрос – ответ»:

Чек-лист

- документ «server_log» содержит описание журнала сервера Linux (Это записываемые фрагменты данных, описывающие то, что в конкретный момент времени делает сервер, ядро, службы и прил ожения);
- документ «server_log» содержит вопрос и ответ о проверке безопасности при авторизации в сист ему (Логи авторизации /var/log/auth.log или /var/log/secure и логи неудачных попыток /var/log/faill og);
- документ «server_log» содержит вопрос и ответ о команде ls /var/log (команда ls /var/log отображ ает все файлы логов Linux);
- документ «server_log» содержит вопрос и ответ о команде для просмотра логов журнала сообще ний от ядра в реальном времени (команда tail –f /var/log/kern.log или cat /var/log/kern.log);
- документ «server_log» содержит вопрос и ответ о команде для просмотра информации о залогин еных пользователях (команда who покажет, кто из пользователей сейчас залогинен в системе и к огда он зашел);
- документ «server_log» содержит вопрос и ответ о команде для просмотра информации о конкрет ном пользователе (команда last <имя пользователя в системе> покажет, когда пользователь заход ил в систему и сколько времени в ней находился);
- документ «server_log» содержит вопрос и ответ о команде для просмотра логов syslog (открыть л ог файл syslog можно командой cat var/log/syslog).

Вариант 1

вопрос	ответ
Какой файл логов поможет при проверке безопасности при авторизации в систему?	/var/log/avth.log или /var/log/secure /var/log/faillog
в каком файле смотреть логи неудачных попыток авторизации?	/var/log/auth.log или /var/log/secure /var/log/faillog
Какой самый простой способ посмотреть логи (открыть лог файл) syslog?	cat var/log/syslog
Какой командой посмотреть логи журнала сообщений от ядра в реальном времени?	tail-f var/log/kern/log или car/var/log/kern.log
Какая команда покажет, кто из пользователей сейчас залогинен в системе и когда он зашел?	/var/log/who
Какая команда дает понять, когда пользователь заходил в систему и сколько времени в ней находился?	/var/log/wtmp
Что делает команда ls /var/log?	Отображает все файлы логов linux

Вариант 2

вопрос	ответ
Какой файл логов поможет при проверке безопасности при авторизации в систему в каком файле смотреть логи неудачных попыток авторизации?	/var/log/auth.log или /var/log/secure /var/log/faillog
Какой самый простой способ посмотреть логи (открыть лог файл) syslog?	cat var/log/syslog
Какой командой посмотреть логи журнала сообщений от ядра в реальном времени?	tail f var/log/kern.log и cat var/log/kern.log
Какая команда покажет, кто из пользователей сейчас залогинен в системе и когда он зашел?	/var/log/who и w
Какая команда дает понять, когда пользователь заходил в систему и сколько времени в ней находился?	/var/log/last
Что делает команда ls /var/log?	Отображает все файлы логов Linux