CHEAT SHEET

Знай свои log файлы.



Где Linux записывает всё подряд —
и как читать каждый файл.

ЧТО ВНУТРИ

01 /var/log/map
Маппинги логов (куда что пишется)

02 syslog
Общие системные сообщения

03 auth.log
Аутентификация и авторизация

04 kern.log
Сообщения ядра (kernel)

05 journal
Системный журнал (systemd)

06 boot.log
Процесс загрузки системы

07 nginx & apache
Логи веб-серверов

08 cron
Задачи по расписанию

09 wtmp · btmp
Логи входов и выходов
(успешные и неудачные)

10 audit.log
Журнал аудита (auditd)

11 logrotate
Ротация и сжатие логов

+ rotation, zcat, tail -f
Полезные команды для работы с логами

ПОЛЕЗНЫЕ КОМАНДЫ

tail -f файл.log

Смотреть лог в реальном времени (следить за изменениями)

```
tail -f /var/log/syslog
```

zcat файл.log.gz

Читать сжатый лог (.gz) без распаковки

```
zcat /var/log/syslog.1.gz
```

logrotate

Управление ротацией логов (архивация, удаление)

```
logrotate /etc/logrotate.conf
```

СОВЕТ

Начни с syslog, auth.log и journal —
они подскажут, что происходит в системе.

```
May 21  10:15:32 server sshd[1234]: Accepted password
May 21  10:15:33 server CRON[567]: (root) CMD (backup.sh)
May 21  10:15:34 server kernel: [12345.678] USB device...
```

ДЛЯ КОГО

Sysadmins · DevOps · SOC · Blue teams ·
Linux learners

КАТАЛОГ

/var/log

/var/log/ • systemd host'ы тоже используют journald

ls -l /var/log

drwxr-xr-x	syslog		Все системные события
-rw-r-----	auth.log		Входы в систему и команды sudo
-rw-r-----	kern.log		Буфер кольца ядра (kernel ring buffer)
-rw-r--r--	dpkg.log		Изменения пакетов (package changes)
drwxr-xr-x	nginx/		Доступ и ошибки веб-сервера (nginx)
drwxr-xr-x	apache2/		Доступ и ошибки веб-сервера (apache)
drwxr-xr-x	audit/		Журналы аудита (auditd records)
-rw-rw-r--	wtmp		История входов в систему (бинарный файл)
-rw-r--r--	boot.log		Последний вывод при загрузке системы

ЧТО ОЗНАЧАЕТ КАЖДАЯ СТРОКА

text logs	Обычные текстовые логи, которые можно читать командами: `cat`, `less`, `tail`, `grep`
binary logs	Бинарные журналы: wtmp, btmp, journal* нужен инструмент для чтения
per-app dirs	Сервисы ведут свои логи в собственных папках (например: `nginx/`)
permissions	Логи с чувствительной информацией (например: `auth.log`) доступны только `root`



ОБЗОР

/var/log — это центральное хранилище логов в большинстве Linux-дистрибутивов. Некоторые файлы — обычный текст, другие — бинарные и требуют специального инструмента. Зная, какой файл за что отвечает, вы экономите минуты при поиске проблем.

ПРИМЕРЫ ПОЛЕЗНЫХ КОМАНД

tail -f файл.log
Смотреть лог в реальном времени (следить за изменениями)

```
tail -f /var/log/syslog
```

zcat файл.log.gz
Читать сжатый лог (.gz) без распаковки

```
zcat /var/log/syslog.1.gz
```

logrotate
Управление ротацией (архивацией, удалением) логов

```
logrotate /etc/logrotate.conf
```

ПРИМЕР ВЫВОДА

```
May 21 10:15:32 server sshd[1234]:
 Accepted password

May 21 10:15:33 server CRON[567]:
 (root) CMD (backup.sh)

May 21 10:15:34 server kernel:
 [12345.678] USB device...
```

СОВЕТ

Начни с syslog, auth.log и journal — они подскажут, что происходит в системе.

ДЛЯ КОГО

Sysadmins • DevOps • SOC
Blue teams • Linux learners

GENERAL SYSTEM LOG

syslog

/var/log/syslog · RHEL: /var/log/messages



syslog — это общий системный журнал (лог),
куда пишут большинство системных служб и демонов.

```
tail /var/log/syslog

1  Feb 14 09:01:22  web01  systemd[1]:
       Started Daily apt download activity
2  Feb 14 09:01:25  web01  CRON[2210]:
       (root) CMD (/usr/bin/backup.sh)
3  Feb 14 09:02:03  web01  kernel:
       [ 4021.5] usb 1-1: new high-speed device
4  Feb 14 09:02:31  web01  dhclient[889]:
       bound to 10.0.2.15 renewal in 1800s
```

ЧТО ОЗНАЧАЕТ КАЖДАЯ ЧАСТЬ СТРОКИ?

Feb 14 09:01:22	web01	systemd[1]:	Started Daily apt download activity
Дата и время события	Имя хоста	Программа и PID процесса	Текст сообщения

ЧТО ОЗНАЧАЕТ КАЖДАЯ ЧАСТЬ (КЛЮЧЕВЫЕ ПОНЯТИЯ)

systemd	Сообщения менеджера служб (systemd): запуск, остановка сервисов и т.д.
CRON	Запланированные задания (cron): пары с /var/log/cron.
kernel	Сообщения ядра Linux: также дублируются из /var/log/kern.log.
facility (программа)	Каждая строка помечена программой-источником. Можно отфильтровать: grep systemd

ОБЗОР

syslog — это единый поток сообщений, где разные службы (systemd, cron, kernel, сеть и др.) записывают события в хронологическом порядке. Это лучший один файл, чтобы быстро понять, что происходило в системе.

ПОЛЕЗНЫЕ КОМАНДЫ

`tail -f /var/log/syslog`
Смотреть лог в реальном времени

`grep "error" /var/log/syslog`
Найти ошибки (error) в логах

`grep systemd /var/log/syslog`
Показать только сообщения от systemd

СОВЕТ Часто полезно смотреть syslog вместе с `dmesg`, `journalctl` и `kern.log` для полной картины.

АУТЕНТИФИКАЦИЯ И ДОСТУП

auth.log

/var/log/auth.log • RHEL: /var/log/secure



auth.log — журнал, где записываются все события аутентификации и использования sudo/PAM.

tail /var/log/auth.log

```
1  Feb 14 08:21:03 web01 sshd[1492]:
     Accepted publickey for kerem from 10.0.2.7
2  Feb 14 08:23:48 web01 sshd[1551]:
     Failed password for root from 203.0.113.9
3  Feb 14 08:23:51 web01 sshd[1551]:
     Invalid user admin from 203.0.113.9
4  Feb 14 08:30:12 web01 sudo:
     kerem : TTY=pts/0 ; PWD=/home
     USER=root ; COMMAND=/usr/bin/apt update
5  Feb 14 08:30:12 web01 sudo:
     pam_unix(sudo:session): session opened
```

1. Успешный вход (public key)
2. Неверный пароль
3. Пользователь не существует
4. Команда sudo
5. PAM-сессия открыта

ЧТО ОЗНАЧАЕТ КАЖДАЯ СТРОКА

Accepted	Успешный вход · показывает способ входа и IP-адрес источника
Failed password	Неверный пароль · повторяющиеся строки указывают на подбор пароля (brute-force)
Invalid user	Попытка входа с несуществующим именем пользователя
sudo:	Выполнение команды от другого пользователя · записывает `COMMAND`

ОБЗОР

auth.log фиксирует каждое событие аутентификации: SSH-входы, использование sudo и PAM-сессии.
Каждая строка содержит: `время (timestamp)` · `хост` · `сервис[PID]` · `сообщение`.
Это лучшее место, чтобы узнать, кто заходил на сервер и какие команды выполнял.

ПОЛЕЗНЫЕ КОМАНДЫ

tail -f /var/log/auth.log
Следить за логом в реальном времени

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

grep "Failed password" /var/log/auth.log
Найти неудачные попытки входа

```
grep "Failed password" /var/log/auth.log
```

grep "sudo" /var/log/auth.log
Показать использованные команды sudo

```
grep "sudo" /var/log/auth.log
```

СОВЕТ Часто полезно смотреть auth.log вместе с syslog и /var/log/secure (на RHEL/CentOS) для полной картины событий входа.

ЯДРО И ОБОРУДОВАНИЕ

kern.log



/var/log/kern.log · просмотр в реальном времени: dmesg -T

kern.log — журнал сообщений ядра Linux.
Здесь записываются события ядра, драйверов и оборудования.

tail /var/log/kern.log

```
1  Feb 14 10:11:02 web01 kernel:
   [12.3] EXT4-fs (sda1): mounted filesystem

2  Feb 14 10:14:55 web01 kernel:
   [88.7] Out of memory: Kill process 3120
   (java) score 902 or sacrifice child

3  Feb 14 10:15:01 web01 kernel:
   [91.2] eth0: link up 1000 Mbps full

4  Feb 14 10:16:40 web01 kernel:
   [99.9] usb 2-1: device descriptor read failed
```

1. Файловая система смонтирована
2. Недостаток памяти (OOM killer)
3. Сетевой интерфейс активен (link up)
4. Ошибка устройства (USB)
5. Сервисное сообщение ядра

ЧТО ОЗНАЧАЕТ КАЖДАЯ СТРОКА

[time]	Время в секундах с момента загрузки системы. Используйте dmesg -T для вывода реальных дат и времени.
EXT4-fs	Сообщения файловой системы: монтирование, ошибки, переподключение (remount) и др.
Out of memory	OOM killer: ядро завершило процесс из-за нехватки памяти. Указывает PID процесса.
link up / down	Состояние сетевого интерфейса (NIC драйвер): подключение (link up) или отключение (link down).
прочее	Различные сообщения ядра, драйверов и оборудования.

ОБЗОР



kern.log — это буфер кольца ядра (kernel ring buffer), который записывается на диск. Он собирает сообщения от драйверов, файловых систем, OOM killer и оборудования. Если сервер завис или диск работает некорректно — именно здесь находятся улики, которые помогут понять, что произошло.

ПОЛЕЗНЫЕ КОМАНДЫ

dmesg -T
Вывести сообщения ядра с реальным временем

```
dmesg -T
```

grep "error" /var/log/kern.log
Найти ошибки (error) в сообщениях ядра

```
grep "error" /var/log/kern.log
```

grep -i "usb" /var/log/kern.log
Фильтровать сообщения по ключевому слову (usb)

```
grep -i "usb" /var/log/kern.log
```

СОВЕТ При проблемах сначала смотрите: kern.log, dmesg и journalctl -k (на RHEL/CentOS) — это даст полную картину событий ядра.

ЖУРНАЛ У SYSTEMD

journalctl

journalctl · бинарное хранилище логов, запрос с помощью **journalctl**



journalctl — основная система хранения логов в systemd. Логи хранятся в бинарном виде и индексируются для быстрого поиска.

Примеры команд

```
$ journalctl -u ssh -n 5
Feb 14 08:21:03 web01 sshd[1492]:
   Server listening on 0.0.0.0 port 22
Feb 14 08:21:44 web01 sshd[1492]:
   Accepted publickey for kerem

# фильтр по приоритету (только kernel)
$ journalctl -k -p err -b
```

-u unit
Показать логи для одного сервиса (напр. -u nginx)

-b
Только текущая загрузка. -b -1 — предыдущая

-p err
Фильтр по приоритету: emerg, err, warning, info и др.

-f
Режим реального времени (как `tail -f`) по всем юнитам

ЧТО ОЗНАЧАЕТ КАЖДАЯ ОПЦИЯ

-u unit	Показать логи для одного сервиса. Например: `-u nginx`
-b	Только текущая загрузка системы. Используйте `-b -1` для предыдущей загрузки
-p err	Фильтр по приоритету: `emerg`, `err`, `warning`, `info` и другие (по уровню важности)
-f	Следить за логами в реальном времени (режим live), как команда `tail -f`, но для всех юнитов
--since	Показать логи с определённого времени. Например: `--since today`
-n N	Показать последние N строк (напр. `-n 50`)

ОБЗОР



На системах с `systemd` журнал (journal) — это основное хранилище логов. Он бинарный и индексированный, поэтому вместо `grep` вы выполняете поиск через `journalctl` по юнитам (unit), времени, загрузке (boot) или приоритету (priority).
Часто в нём содержится больше информации, чем в текстовых логах.

ПОЛЕЗНЫЕ КОМАНДЫ

journalctl -u nginx
Логи сервиса nginx

journalctl -b -1
Логи предыдущей загрузки

journalctl -p err
Только ошибки и критические события

journalctl -f
Следить за логами в реальном времени

journalctl --since today
Логи с начала сегодняшнего дня

СОВЕТ `journalctl` — мощный инструмент. Используйте комбинации опций (`-u`, `-p`, `-b`, `--since`, `-f` и др.), чтобы быстро находить нужные события!

ЗАГРУЗКА И ЗАПУСК СИСТЕМЫ

boot.log

/var/log/boot.log • см. также: journalctl -b



boot.log — это вывод консоли с последней загрузки системы. Он помогает быстро понять, какие службы стартовали успешно, а какие — нет.

cat /var/log/boot.log

```
[ OK ]   Started Network Manager
[ OK ]   Mounted /boot/efi
[ OK ]   Reached target Multi-User System
[FAILED]  Failed to start Docker daemon
   See 'systemctl status docker' for details
[ OK ]  Started OpenSSH server
[ OK ]  Reached target Graphical Interface
```

[OK]
Блок (unit) запущен успешно при загрузке

[FAILED]
Блок (unit) не запущен — первое, что нужно проверить

Reached target
Достигнута цель загрузки (например, multi-user или сеть)

Mounted
Файловая система смонтирована по указанному пути

ЧТО ОЗНАЧАЕТ КАЖДАЯ СТРОКА

[OK]	Блок (unit) стартовал успешно во время загрузки.
[FAILED]	Блок (unit) не стартовал — это первая вещь, которую нужно проверить.
Reached target	Достигнута цель загрузки (например, multi-user, graphical, network).
Mounted	Файловая система была подключена (смонтирована) по указанному пути.

ОБЗОР



boot.log содержит вывод консоли с последнего старта системы. Зелёные строки OK — успешные действия, красные FAILED — ошибки. Это самый быстрый способ найти сервис, который не запустился после перезагрузки.

ПОЛЕЗНЫЕ КОМАНДЫ

cat /var/log/boot.log
Показать весь лог последней загрузки
`cat /var/log/boot.log`

journalctl -b
Посмотреть логи текущей загрузки (лучше и подробнее)
`journalctl -b`

journalctl -b -1
Посмотреть логи предыдущей загрузки
`journalctl -b -1`

journalctl -p err -b
Показать только ошибки (priority: err) за эту загрузку
`journalctl -p err -b`

СОВЕТ Если что-то пошло не так при загрузке — смотрите сначала boot.log и используйте journalctl -b для изучения деталей.

ЛОГИ ВЕБ-СЕРВЕРА

nginx



/var/log/nginx/ · apache: /var/log/apache2/

Nginx записывает логи запросов и ошибок.
Основные файлы: access.log (запросы) и error.log (ошибки).

Пример содержимого логов

```
# access.log (объединённый формат)
10.0.2.7 - - [14/Feb:08:30:01] "GET /api/login HTTP/1.1" 200 512

203.0.113.9 - - [14/Feb:08:31:14] "GET /admin.php HTTP/1.1" 404 146

# error.log
2025/02/14 08:31 [error] open() failed admin.php
```

- IP клиента
- Дата и время
- Метод и путь
- 200 Статус (2xx = успех)
- 512 Размер ответа (байты)
- 404 Ошибка (4xx = клиент, 5xx = сервер)

ЧТО ОЗНАЧАЕТ КАЖДОЕ ПОЛЕ В access.log

IP	Время	Метод и путь	2xx/4xx/5xx	Размер
IP-адрес клиента	Дата и время запроса	HTTP-метод и запрошенный путь	HTTP-статус ответа	Размер ответа в байтах

ЧТО ОЗНАЧАЕТ КАЖДЫЙ ФАЙЛ

access.log	Лог всех HTTP-запросов. Содержит IP, время, путь, статус, размер и User-Agent. Помогает анализировать трафик, сканирование и поведение пользователей.
error.log	Лог ошибок Nginx и приложений. Показывает проблемы конфигурации, отсутствие файлов, ошибки backend (upstream) и другие сбои на стороне сервера.
user-agent	В объединённом формате access.log также записывается User-Agent клиента — браузер, бот, сканер и т.д.
combined format	Объединённый формат (combined) содержит все важные данные в одной строке: удобно для анализа и парсинга.

ОБЗОР

Веб-серверы ведут два основных лога: access.log (все запросы) и error.log (ошибки). Чтение status code и путей помогает увидеть паттерны трафика, попытки доступа к админ-панелям и проблемы с backend. Эти логи — ваш главный источник для диагностики веб-приложений и безопасности.

ПОЛЕЗНЫЕ КОМАНДЫ

- `tail -f /var/log/nginx/access.log` — Смотреть лог запросов в реальном времени
- `tail -f /var/log/nginx/error.log` — Смотреть лог ошибок в реальном времени
- `grep "404" /var/log/nginx/access.log` — Найти 404 ошибки в логах запросов
- `grep "POST" /var/log/nginx/access.log` — Найти все POST запросы
- `awk '{print $1}' /var/log/nginx/access.log | sort | uniq -c` — Топ IP-адресов по количеству запросов
- `gzip -c /var/log/nginx/access.log > access.log.gz` — Сжать лог-файл

СОВЕТ Регулярно проверяйте error.log и ищите частые 4xx/5xx ошибки в access.log. Это помогает быстро находить и решать проблемы до того, как их заметят пользователи.

ПЛАНИРОВЩИК ЗАДАЧ

cron

`/var/log/cron` · `Debian: grep CRON /var/log/syslog`



cron — планировщик заданий в Linux.
Логи cron записываются в `/var/log/cron`
(на Debian в `/var/log/syslog` с пометкой CRON).

Примеры записей из лога

1. `Feb 14 09:00:01 web01 CRON[2210]: (root) CMD (/usr/bin/backup.sh)`
2. `Feb 14 09:05:01 web01 CRON[2298]: (www-data) CMD (php /var/www/cron.php)`
3. `Feb 14 09:17:01 web01 CRON[2401]: (root) CMD ( cd / && run-parts /etc/cron.hourly )`
4. `Feb 14 09:30:01 web01 CRON[2510]: (mysql) CMD (/usr/bin/mysqlcheck --all)`

(user)
Пользователь, от имени которого выполнено задание

CMD
Команда, которую запустил cron

run-parts
Запуск всех скриптов из папки (cron.hourly, daily и т.д.)

(mysql)
Другой пользователь или служба (например, mysql)

ЧТО ОЗНАЧАЕТ КАЖДОЕ ПОЛЕ

(user)	Какой пользователь (account) запустил задание
CMD	Точная команда, которую выполнил cron
run-parts	cron запускает все скрипты в папках: /etc/cron.hourly, /etc/cron.daily, /etc/cron.weekly и т.д.
missing run	Пропуск: задание должно было запуститься, но не запустилось

ОБЗОР



Лог cron показывает, какие запланированные задачи действительно выполнились, от какого пользователя и когда. Это полезно для:

- отладки бэкапов, которые не запустились
- поиска пропущенных заданий
- выявления подозрительных задач (когда добавил злоумышленник)

ПОЛЕЗНЫЕ КОМАНДЫ

tail -f /var/log/cron
Смотреть лог cron в реальном времени
`tail -f /var/log/cron`

grep CRON /var/log/syslog
Искать записи cron в логах syslog (Debian)
`grep CRON /var/log/syslog`

grep "run-parts" /var/log/cron
Показать запуски папок (hourly, daily и т.д.)
`grep "run-parts" /var/log/cron`

grep "(user)" /var/log/cron
Все задания от конкретного пользователя
`grep "(www-data)" /var/log/cron`

grep "backup" /var/log/cron
Найти задания, связанные с бэкапами
`grep "backup" /var/log/cron`

grep "mysql" /var/log/cron
Найти задания от службы (mysql и др.)
`grep "mysql" /var/log/cron`

СОВЕТ Если задание не сработало — сначала смотрите `/var/log/cron` и ищите пропуски (`missing run`) или ошибки в командах.

ЛОГИ ВХОДОВ (БИНАРНЫЕ)

wtmp · btmp

/var/log/wtmp · читаются через last, lastb, lastlog



wtmp, btmp и lastlog — бинарные файлы.
Их нельзя смотреть через cat, используйте специальные команды: last, lastb, lastlog.

last -a | head

```
$ last -a      # успешные входы
kerem   pts/0   Fri 08:21   still logged in  10.0.2.7
kerem   pts/1   Thu 19:03 - 21:40  (02:37)  10.0.2.7
reboot  system  Thu 18:55   6.1.0-amd64
```

УСПЕШНЫЕ ВХОДЫ

- kerem — пользователь
- pts/0 — терминал (tty)
- Fri 08:21 — дата и время
- 10.0.2.7 — IP клиента

```
$ lastb | head   # неудачные входы
admin   ssh:notty   Fri 08:23   203.0.113.9
root    ssh:notty   Fri 08:23   203.0.113.9
```

НЕУДАЧНЫЕ ВХОДЫ (btmp)

Полытки входа, выполненные от имени root

ЧТО ОЗНАЧАЕТ КАЖДОЕ ПОЛЕ

(user)	Пользователь, от имени которого выполнен вход или попытка входа.
CMD	Точная команда/сессия, через которую выполнен вход. Напр.: ssh:notty, pts/0, system.
run-parts	cron запускает все скрипты из папок: /etc/cron.hourly, /etc/cron.daily, /etc/cron.weekly и т.д.
missing run	Задание должно было выполниться, но не запустилось. Это «пробел» в расписании cron.
still logged in	Сессия открыта и ещё не завершена.

ОБЗОР



Файлы wtmp, btmp и lastlog — бинарные, поэтому их нельзя смотреть через cat.
Используйте команды last, lastb и lastlog.
Вместе они отвечают на важные вопросы:

- кто входил в систему
- кто пытался, но не смог
- когда последний раз была перезагрузка

ВАЖНО
Эти логи не редактируются вручную и служат важным источником расследования инцидентов.

ПОЛЕЗНЫЕ КОМАНДЫ

last -a
Показать все входы (включая перезагрузки)
`last -a | head`

lastb
Показать неудачные попытки входа
`lastb | head`

lastlog
Когда каждый пользователь входил последний раз
`lastlog`

grep CRON /var/log/syslog
Найти записи cron в syslog (Debian)
`grep CRON /var/log/syslog`

СОВЕТ При расследовании инцидентов всегда проверяйте:
last, lastb и lastlog — они покажут полную картину входов и событий!

АУДИТ СИСТЕМЫ

audit.log

`/var/log/audit/audit.log` · читается через **ausearch** или **aureport**



audit.log — журнал аудита (**audit trail**).
В нём фиксируются системные вызовы (**syscalls**) и доступ к файлам согласно заданным правилам (**rules**).

Пример записи из audit.log

```
ausearch -m EXECVE

type=SYSCALL msg=audit(1739521203):
  arch=x86_64 syscall=execve success=yes
  uid=1000 auid=1000 comm="passwd"

type=PATH name=/etc/shadow
  nametype=NORMAL mode=0640

type=USER_AUTH acct="kerem" res=success
```

1. **SYSCALL** — информация о системном вызове
2. **PATH** — какой файл был затронут
3. **USER_AUTH** — пользователь и результат аутентификации

ЧТО ОЗНАЧАЮТ ПОЛЯ

type=SYSCALL	Какой системный вызов (system call) был выполнен, каким uid, и успешен он был или нет.
auid	Исходный пользователь (original user), даже если он использовал **su** или **sudo**.
type=PATH	Какой файл попал под правило слежения, например `/etc/shadow`.
ausearch	Команда для поиска записей по типу сообщения, пользователю, времени или ключу (**key**).

ОБЗОР



auditd записывает доказательства (tamper-evident) системных вызовов и доступа к файлам в соответствии с вашими правилами. Журнал очень подробный, не предназначен для чтения командой `cat`. Используйте **ausearch** и **aureport** — они превращают данные в понятные ответы для анализа, соответствия и расследований.

ВАЖНО

audit.log нельзя просматривать через `cat`! Используйте специальные утилиты: **ausearch**, **aureport**.

ПОЛЕЗНЫЕ КОМАНДЫ

ausearch -m EXECVE
Найти запуск программ (execve)
`ausearch -m EXECVE`

ausearch -ua <user>
Найти действия конкретного пользователя
`ausearch -ua kerem`

ausearch -ts today
Найти события за сегодня
`ausearch -ts today`

ausearch -k <key>
Найти события по ключу (key в правиле)
`ausearch -k login`

aureport -f
Показать сводку по пользователям, syscalls, файлам и др.
`aureport -f`

aureport --login
Отчёт по входам пользователей (успешные / неудачные)
`aureport --login`

СОВЕТ: Настройте правила audit (в `/etc/audit/rules.d/`), чтобы журналировать только важные события и не перегружать систему.

РОТАЦИЯ и ЧТЕНИЕ ЛОГОВ

logrotate



/etc/logrotate.conf · архивы: *.1, *.2.gz

logrotate управляет размером логов: переименовывает старые, сжимает их и удаляет по расписанию.
Это **не команда** для чтения логов!

ПОЛЕЗНЫЕ КОМАНДЫ

Список логов в /var/log

```
$ ls /var/log/
syslog   syslog.1   syslog.2.gz   syslog.3.gz
```

покажет текущий лог и архивы: .1, .2.gz и т.д.

Поиск текста внутри сжатого архива

```
$ zcat syslog.2.gz | grep error
```

читаем архив логов без распаковки

Чтение лога в реальном времени

```
$ tail -f /var/log/syslog
```

вывод новых строк по мере их появления

ЧТО ОЗНАЧАЕТ КАЖДОЕ ПОЛЕ

.1 .2.gz	Архивы логов после ротации. **.1** — самый новый, **.2.gz** — старее и сжатый.
logrotate	Утилита, которая по расписанию переименовывает, сжимает и удаляет старые логи.
zcat / zgrep	Чтение или поиск по сжатым логам без распаковки.
tail -f	Показывает новые строки лога в реальном времени (режим "следить за файлом").

ОБЗОР



01 Ротация
logrotate переименовывает текущий лог в syslog.1, сжимает старые в syslog.2.gz, syslog.3.gz и т.д.

02 Хранение
Старые архивы хранятся сжатые для экономии места.

03 Удаление
Очень старые архивы удаляются согласно настройкам (чтобы не занимать место).

ВАЖНО
Логи не растут бесконечно! logrotate следит за этим.
Для поиска используйте zcat или zgrep.
Для наблюдения в реальном времени — tail -f.

ПОЛЕЗНЫЕ КОМАНДЫ

ls /var/log/
Показать все логи и архивы в каталоге

```
ls /var/log/
```

zcat file.log.2.gz | grep error
Найти текст в сжатом архиве (читаем без распаковки)

```
zcat file.log.2.gz | grep error
```

zgrep error file.log.2.gz
Поиск по сжатому архиву (удобная альтернатива)

```
zgrep error file.log.2.gz
```

tail -f /var/log/syslog
Следить за логом в реальном времени

```
tail -f /var/log/syslog
```

logrotate -d /etc/logrotate.conf
Проверить конфигурацию logrotate (без выполнения)

```
logrotate -d /etc/logrotate.conf
```

man logrotate
Показать справку по logrotate

```
man logrotate
```

СОВЕТ: Чтобы найти что-то в истории — используйте zcat или zgrep по архивам. Чтобы наблюдать за текущими событиями — tail -f.

ты разобрал логи linux.

вот твой краткий чек-лист:

/var/log	–	главная папка с логами
syslog	–	основной системный лог
auth.log	–	лог аутентификации (логины, sudo)
kern.log	–	сообщения ядра
journalctl	–	системный журнал (systemd journal)
boot.log	–	логи загрузки системы
nginx	–	веб-сервер и доступы
cron	–	запланированные задачи
wtmp / btmp	–	история входов / неудачных входов
audit.log	–	аудит действий пользователей
logrotate	–	ротация и архивирование логов

теперь ты знаешь:

- где искать ошибки
- кто входил в систему
- что запускалось через cron
- почему упал сервис
- кто менял систему
- как расследовать инциденты

ЛЕГИОН

ЛОГИ НЕ ЛГУТ.

@lionsoulbatyshchikov