**Как посмотреть логи Linux**

Большинство логов в [**Linux**](https://ravesli.com/chto-takoe-linux-ego-struktura-i-preimushhestva/) генерируются системными демонами **syslogd** или **rsyslogd**и хранятся в обычном текстовом файле ASCII в [**каталоге**](https://ravesli.com/struktura-katalogov-v-linux/) */var/log.*Этот каталог содержит лог-файлы самой ОС, служб и различных приложений, запущенных в системе

**ls -l /var/log/**

**Основные логи**

В основных логах, необходимых для работы Linux, содержится наиболее значительный объем информации о текущем состоянии системы. Их можно условно разделить на четыре категории:

* системные лог-файлы;
* лог-файлы событий;
* лог-файлы служб;
* лог-файлы приложений.

Многие из этих лог-файлов располагаются в каталоге ***var/log***. Наиболее распространенными логами являются:

**The main log file:**

***/var/log/syslog*** или ***/var/log/messages*** — журналы, в которых хранится информация об общей активности в системе (включая сообщения этапа загрузки);

**Access and authentication**

***/var/log/auth.log***или ***/var/log/secure*** — журналы аутентификации и безопасности (в них хранятся записи обо всех попытках входа в систему, включая как успешные, так и неудачные);

***/var/log/faillog*** — информация о неудачных входах в систему. Журнал полезен для изучения потенциальных нарушений безопасности, таких как: взломы учетных записей, попытки перебора паролей и пр.;

***/var/log/lastlog***— журнал с информацией о последних входах пользователей. Для просмотра сообщений применяется команда lastlog

***/var/log/utmp***и***/var/log/utmp***— журналы учета входов пользователей в систему. Для просмотра сообщений применяется команда utmpdump, например:

# utmpdump /var/log/wtmp

**Package install/uninstall**

***/var/log/dpkg.log*** — журнал пакетов, установленных через утилиту *dpkg* в системах на основе **[Debian Linux](https://ravesli.com/obzor-distributivov-linux-kakoj-vybrat/" \l "toc-8" \t "_blank)**.

***/var/log/yum.log*** — журнал пакетов, установленных через утилиту *yum* в системах на основе [**Red Hat Linux**](https://ravesli.com/obzor-distributivov-linux-kakoj-vybrat/#toc-11).

***/var/log/emerge.log*** — журнал пакетов (ebuild), установленных через утилиту *emerge* в Gentoo Linux.

**System**

***/var/log/boot.log*** — журнал загрузки системы (в нем хранится вся информация, связанная с этапами загрузки ОС

***/var/log/kern.log*** — журнал ядра (в нем хранятся сообщения и предупреждения, поступающие непосредственно из [**ядра Linux**](https://ravesli.com/chto-takoe-linux-ego-struktura-i-preimushhestva/#toc-6));

***/var/log/debug*** — журнал отладки (в нем хранится подробная отладочная информация системы и приложений);

***/var/log/daemon.log*** — журнал демонов (содержит информацию о событиях, связанных с различными запущенными в системе демонами/службами);

***/var/log/cron***— журнал, в котором хранится информация о запланированных задачах (заданиях *cron*);

***/var/log/cups*** – логи связанные с принтером и со всеми задачами по печать

***/var/log/dmesg*** — журнал сообщений драйверов устройств. Просмотреть содержимое данного журнала можно с помощью команды dmesg. Стоит заметить, что при достижении своего предела, старые сообщения перезаписываются более новыми.

**Application**

***/var/log/maillog***или***/var/log/mail.log*** — журналы почтовых серверов (в них хранится информация, относящаяся к почтовым серверам и архивированию электронных писем);

***/var/log/Xorg.x.log*** — журнал сообщений X-сервера.

***/var/log/*<Application\_Name>**— журнал сообщений отдельного приложения

**Ротация лог-файлов**

Если учесть, что информация в лог-файлы поступает регулярно и по любому поводу, то в скором времени они должны были бы стать просто гигантскими, занимая при этом огромную кучу места на диске. А работать с ними было бы просто невозможно. Но этого не происходит благодаря **ротации лог-файлов***.*

Цель ротации заключается в сжатии устаревших лог-файлов, которые занимают много места. Лог-файлы, в конце имен которых добавлены нули, являются *ротируемыми* (их имена были автоматически изменены системой). Ротацию лог-файлов можно выполнить с помощью **команды logrotate**, например:

# **logrotate /var/log/daemon.log**

Настройки ротации лог-файлов хранятся в соответствующем файле конфигурации */etc/logrotate.conf*:

var/log/имя\_журнала.log {  
Missingok  
Notifempty  
Compress  
Size 20k  
Daily  
Create 0600 root root  
}

Разберем детально каждую строку вышеприведенного фрагмента:

* Missingok — указывает команде logrotate не выводить ошибку, если лог-файл отсутствует.
* Notifempty — если лог-файл пуст, то ротации не будет.
* Compress — лог-файл необходимо сжать.
* Size 20k — гарантирует, что лог-файл не превышает заданного размера, в противном случае производится его ротация.
* Daily — ротация лог-файлов по ежедневному расписанию. Также можно задавать ежечасный (Hourly), еженедельный (Weekly), ежемесячный (Monthly) или ежегодный (Yearly) график.
* Create 0600 root root — создает экземпляр лог-файла, владельцем и группой которого является *root*.

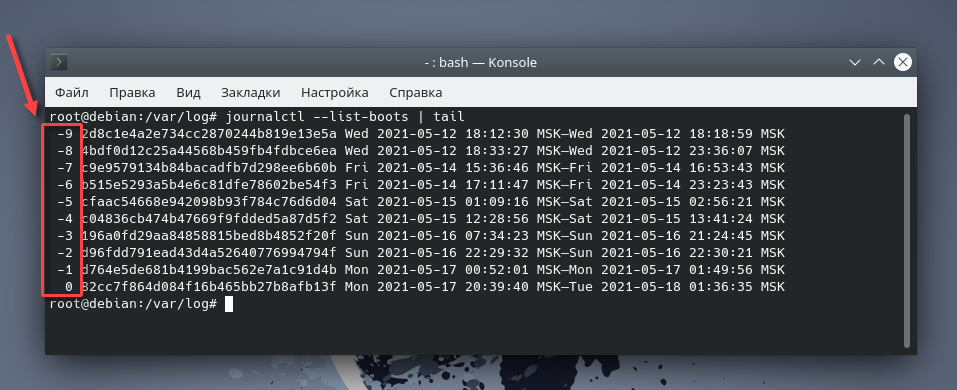
Теперь, разобравшись с тем, что означает каждый параметр, можно каждому лог-файлу задавать соответствующий индивидуальный параметр ротации.

**systemd и journald**

**systemd**— это подсистема инициализации и управления службами в Linux, фактически вытеснившая в 2010-е годы традиционную подсистему *init*. В связке с ней работает и **journald** — демон сбора логов, являющийся частью *systemd*. Он собирает логи со всей системы и хранит их в бинарном виде в каталоге */var/log/journal*. Для того чтобы их просмотреть, создана специальная **утилита journalctl**. Рассмотрим несколько примеров её применения.

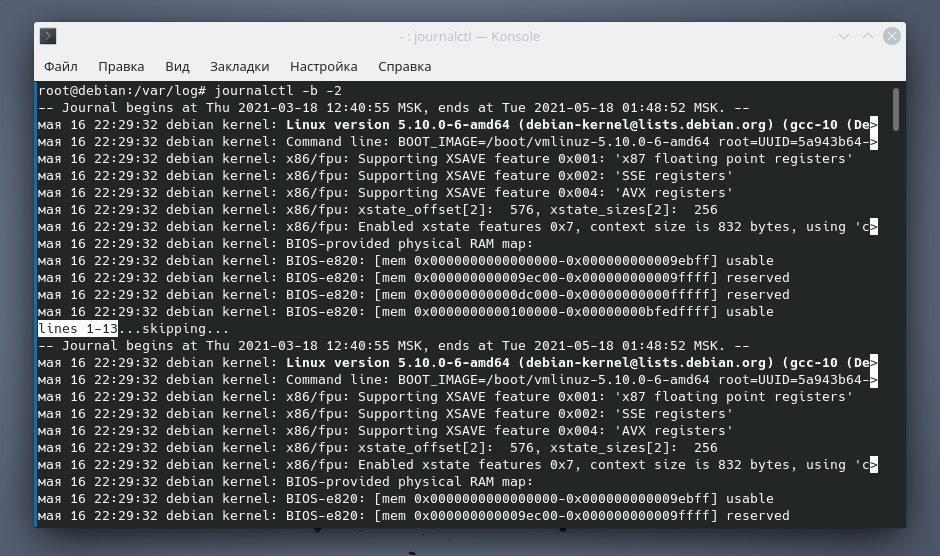
Чтобы просмотреть последние 10 строк логов всех запусков системы, достаточно выполнить следующую команду:

# **journalctl --list-boots | tail**



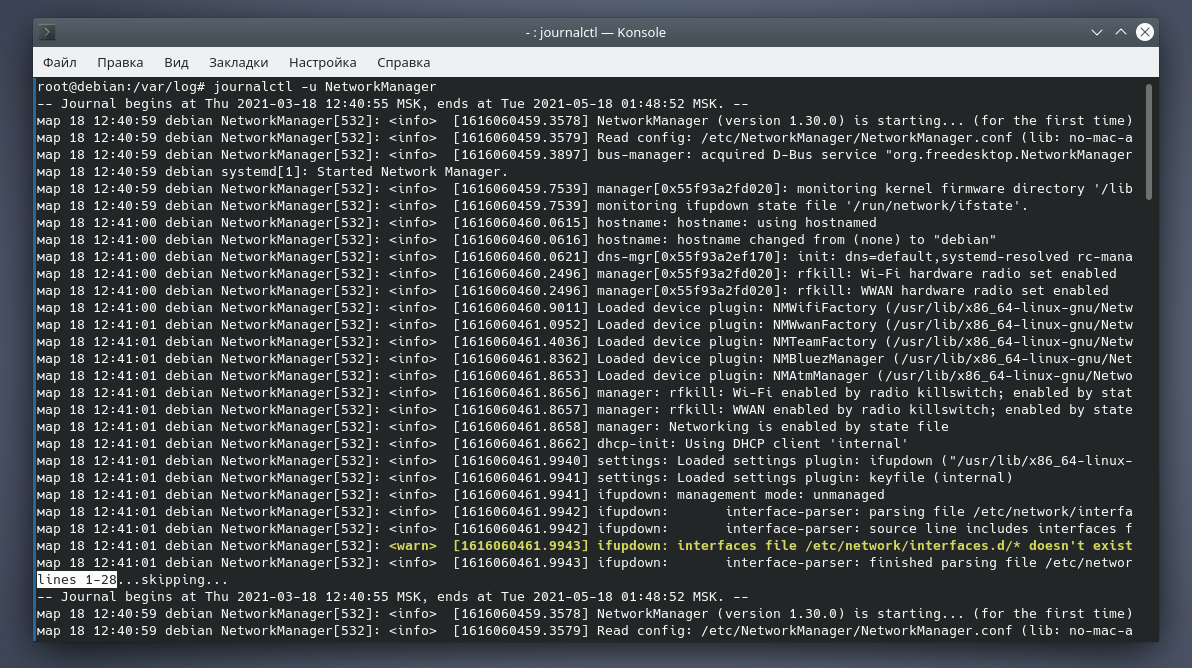
Видите столбец, который я обвел красным? Цифрой 0 в нем обозначена текущая загрузка системы, цифрой -1 — предыдущая и т.д. Если вы хотите просмотреть логи какой-то конкретной загрузки, например, позапрошлой, то достаточно ввести:

# journalctl -b -2



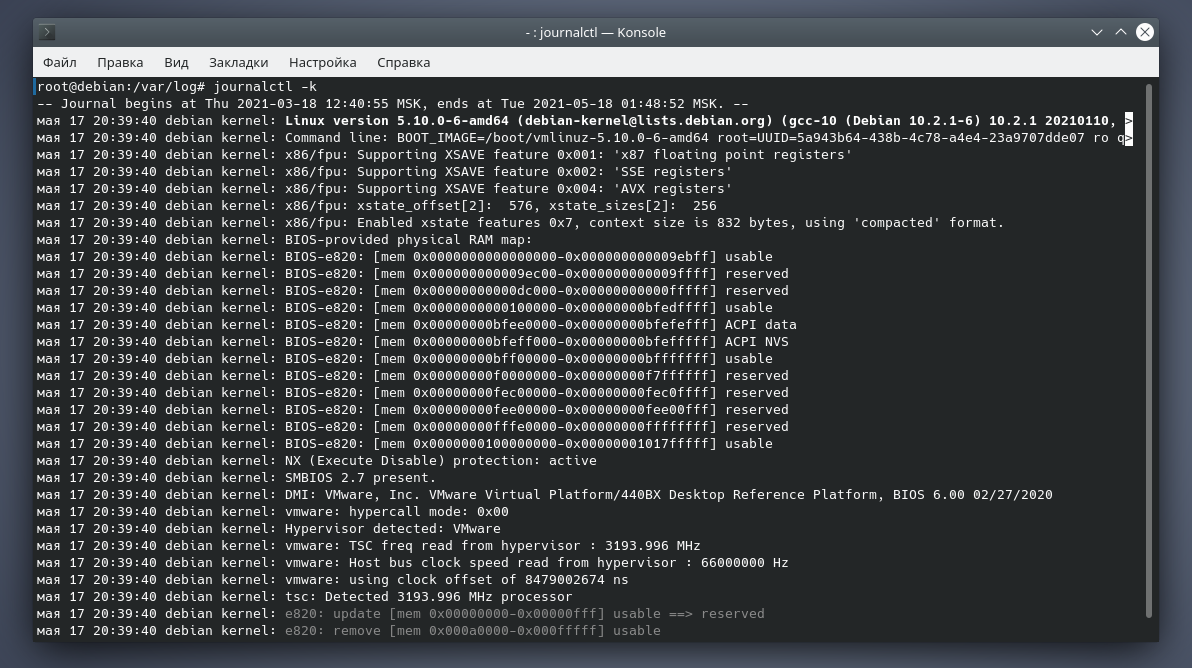
Также можно просмотреть информацию по выбранной службе, например, по *NetworkManager*:

# journalctl -u NetworkManager



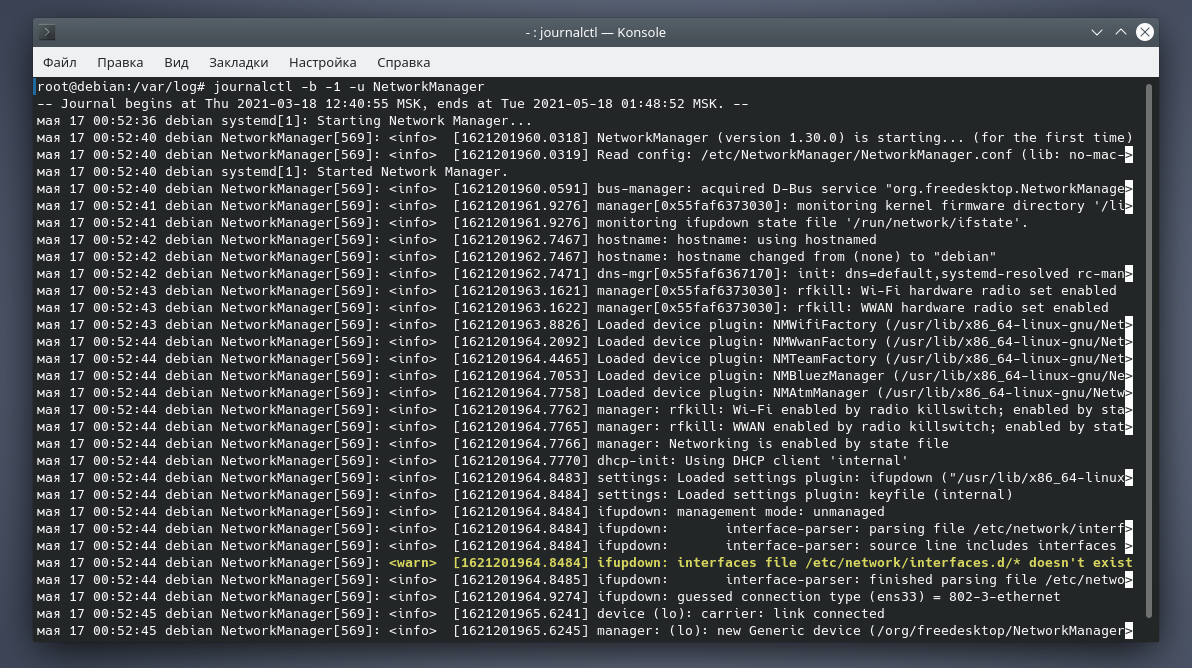
Или же вывести сообщения ядра ОС:

# journalctl -k



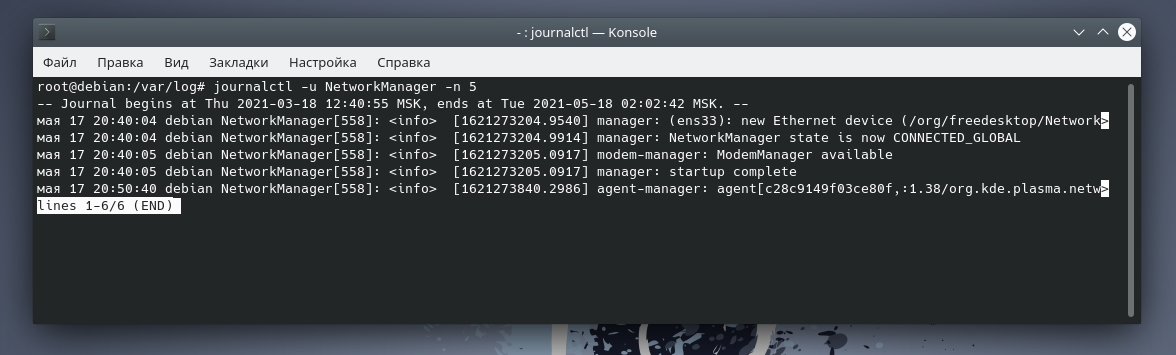
Для получения своих, каких-то более конкретных результатов, допускается комбинировать опции и параметры команды journalctl:

# journalctl -b -1 -u NetworkManager



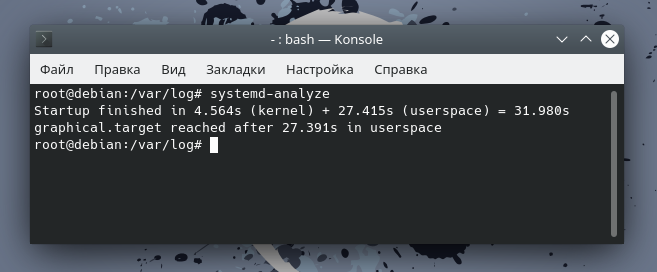
Для вывода информации только по нескольким последним записям, применяется опция -n, задающая их количество:

# journalctl -u NetworkManager -n 5



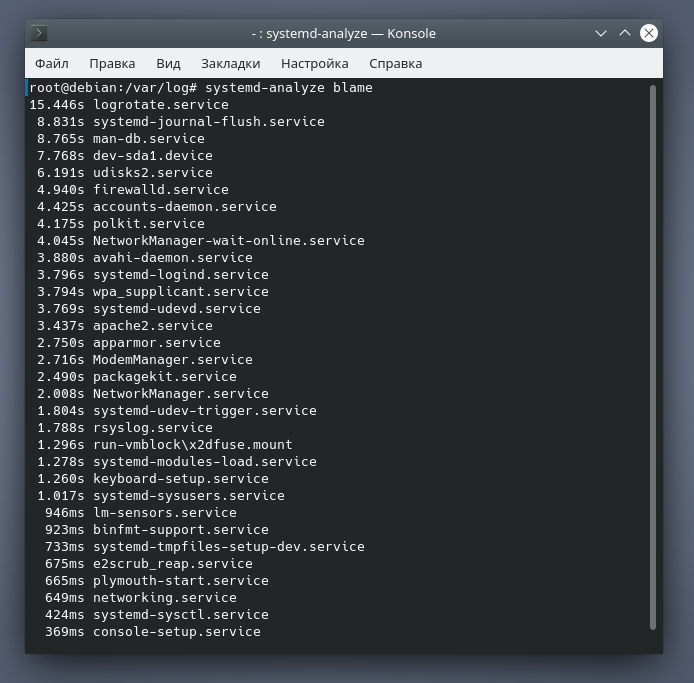
Если говорить про *systemd*, то, наверное, стоит упомянуть и про **команду systemd-analyze**, которая отвечает за сбор статистики загрузки системы. Применение данной команды без параметров отобразит общее время загрузки системы:

# systemd-analyze

****

С помощью параметра blame можно увидеть, сколько времени понадобилось для загрузки каждой конкретной службы (при этом сверху отобразятся самые медленные):

# systemd-analyze blame



**Приоритет сообщений в лог-файлах**

Сообщения в лог-файлах создаются в зависимости от типа событий. В свою очередь, событие имеет определенную степень важности. В зависимости от этой важности **событию присваивается определенный приоритет**:

**emerg** — наивысший приоритет, что-то сломалось, повод паниковать;

**alert** — тревога, стоит волноваться;

**crit** — критическое событие, стоит насторожиться;

**err** — ошибка;

**warning** — предупреждение;

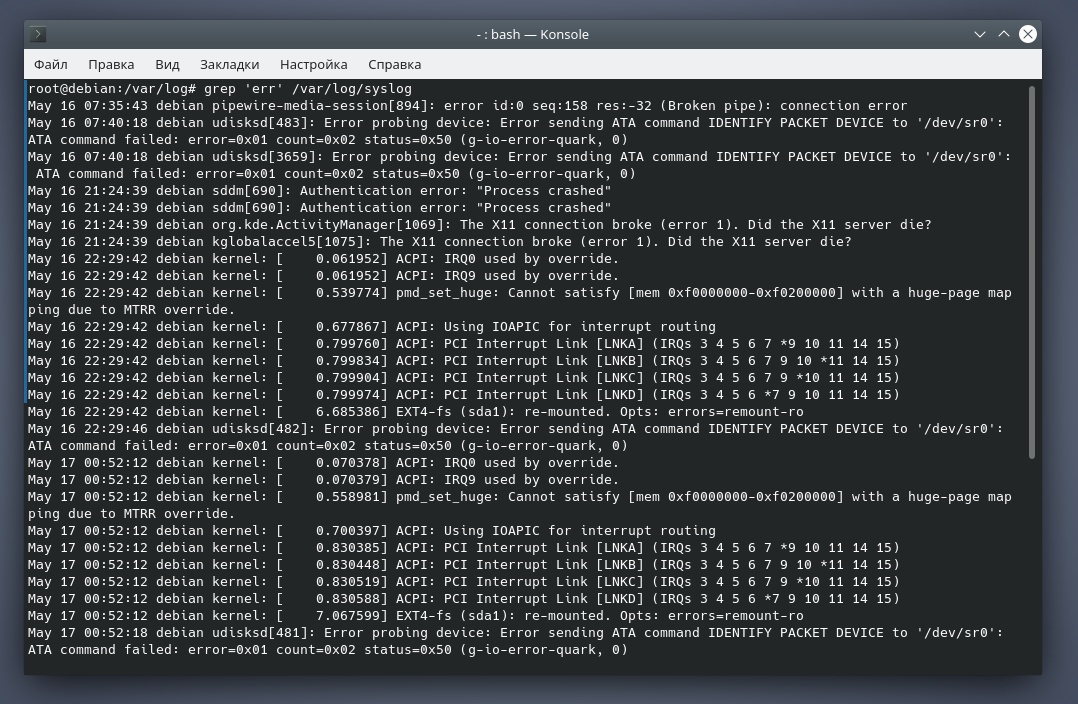
**notice** — уведомление, можно не заморачиваться;

**info** — информационное сообщение, принять к сведению и забыть;

**debug** — отладочная информация.

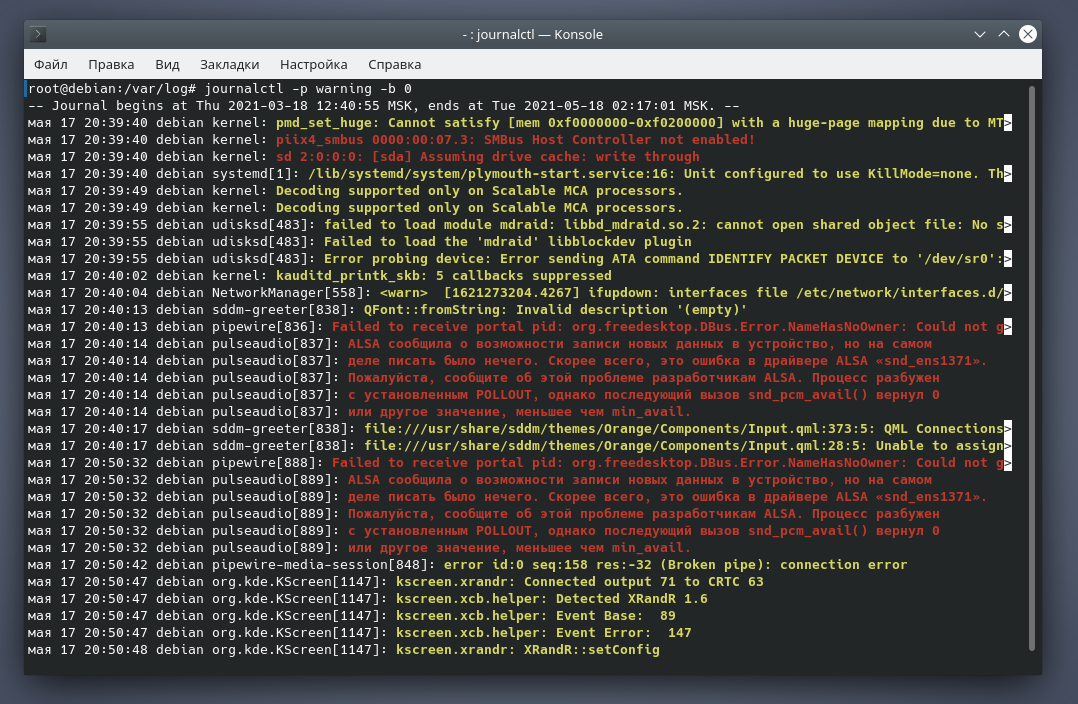
Применяя вышеописанные значения приоритетов, можно просматривать сообщения лог-файлов, фильтруя их по заданному приоритету:

# grep 'err' /var/log/syslog



Или же для *journalctl*:

# journalctl -p warning -b 0



**Просмотр логов Linux**

Просмотр логов Linux, в реальном времени:

**tail -f /var/log/dmesg**

Открываем лог файл dmesg:

**cat /var/log/dmesg**

Первые строки dmesg:

**head /var/log/dmesg**

Выводим только ошибки из /var/log/messages:

**grep -i error /var/log/dmesg**