Journalctl - ??????????

Journalctl — это утилита для работы с системным журналом **systemd**.
Она объединяет логи всех сервисов и ядра в единое хранилище, доступное через команды фильтрации.
В отличие от классических /var/log/syslog и /var/log/messages, journalctl позволяет быстро находить ошибки, фильтровать логи по времени, сервисам, приоритетам.

???????? ???? ?????

Простая команда для просмотра системного журнала:

```
journalctl
```

Обычно логи будут длинные, поэтому часто используют `-e` (сразу перейти к концу).

```
journalctl -e
```

???????? ????????? ??????? ? ???????? ???????

```
journalctl -f
```

Аналогично `tail -f /var/log/syslog`. Удобно использовать при отладке сервисов.

?????????? ?? ???????

Посмотреть логи конкретного сервиса:

```
journalctl -u nginx
```

В реальном времени:

```
journalctl -u nginx -f
```

?????????? ?? ???????

Примеры:

```
journalctl --since "2025-10-01" --until "2025-10-05"   # за указанный период
journalctl --since "2 hours ago"                        # за последние 2 часа
journalctl --since yesterday                            # за вчерашний день
```

?????????? ?? ??????????? (???????)

Приоритеты: **emerg, alert, crit, err, warning, notice, info, debug**.

```
journalctl -p err        # только ошибки
journalctl -p warning    # предупреждения
journalctl -p info       # информационные сообщения
```

???????? ????? ????????

```
journalctl -b      # текущая загрузка
journalctl -b -1   # предыдущая загрузка
journalctl -b -2   # позапрошлая загрузка
```

Очень полезно для анализа причин падения системы или kernel panic.

???????? ????? ????

```
journalctl -k             # сообщения ядра
journalctl -k -p err      # только ошибки ядра
```

???????????? ?????????? ?????

```
journalctl -n 50          # последние 50 строк
journalctl -n 100 -u ssh  # последние 100 строк сервиса ssh
```

????? ? ????????????? ??? ???????? ???????

```
journalctl -o short       # стандартный вывод
journalctl -o json-pretty # JSON-формат, удобно для анализа
journalctl -o cat         # только текст сообщения
```

???????? ???????? ? ??????? ?????????????

- Сервис не запускается — смотрим причину:
  `journalctl -u имя_сервиса -xe`
- Отслеживание ошибок SSH-подключений:
  `journalctl -u ssh -p err -f`
- Анализ падения Nginx:
  `journalctl -u nginx --since "10 min ago"`
- Поиск "OOM-killer" (система убила процесс из-за нехватки памяти):
  `journalctl -k | grep -i oom`
- Выяснить, кто перезагружал систему:
  `journalctl _COMM=systemd-logind | grep "Power key pressed"`

???????? ?????? ? ???????

- **Ошибка:** логи не сохраняются после перезагрузки.
  Решение: включить постоянное хранение:

```
sudo mkdir -p /var/log/journal
sudo systemctl restart systemd-journald
```

- **Ошибка:** слишком большой размер логов.
  Решение: очистка и настройка лимита:

```
sudo journalctl --vacuum-time=7d      # оставить только 7 дней
sudo journalctl --vacuum-size=500M    # ограничить размер 500 МБ
```

Revision #2
Created 5 October 2025 12:41:31 by Admin
Updated 5 October 2025 12:44:29 by Admin