



RUDN
university

РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук
Кафедра прикладной информатики и теории вероятностей

Презентация №7

Журналы событий в SystemD (journald)

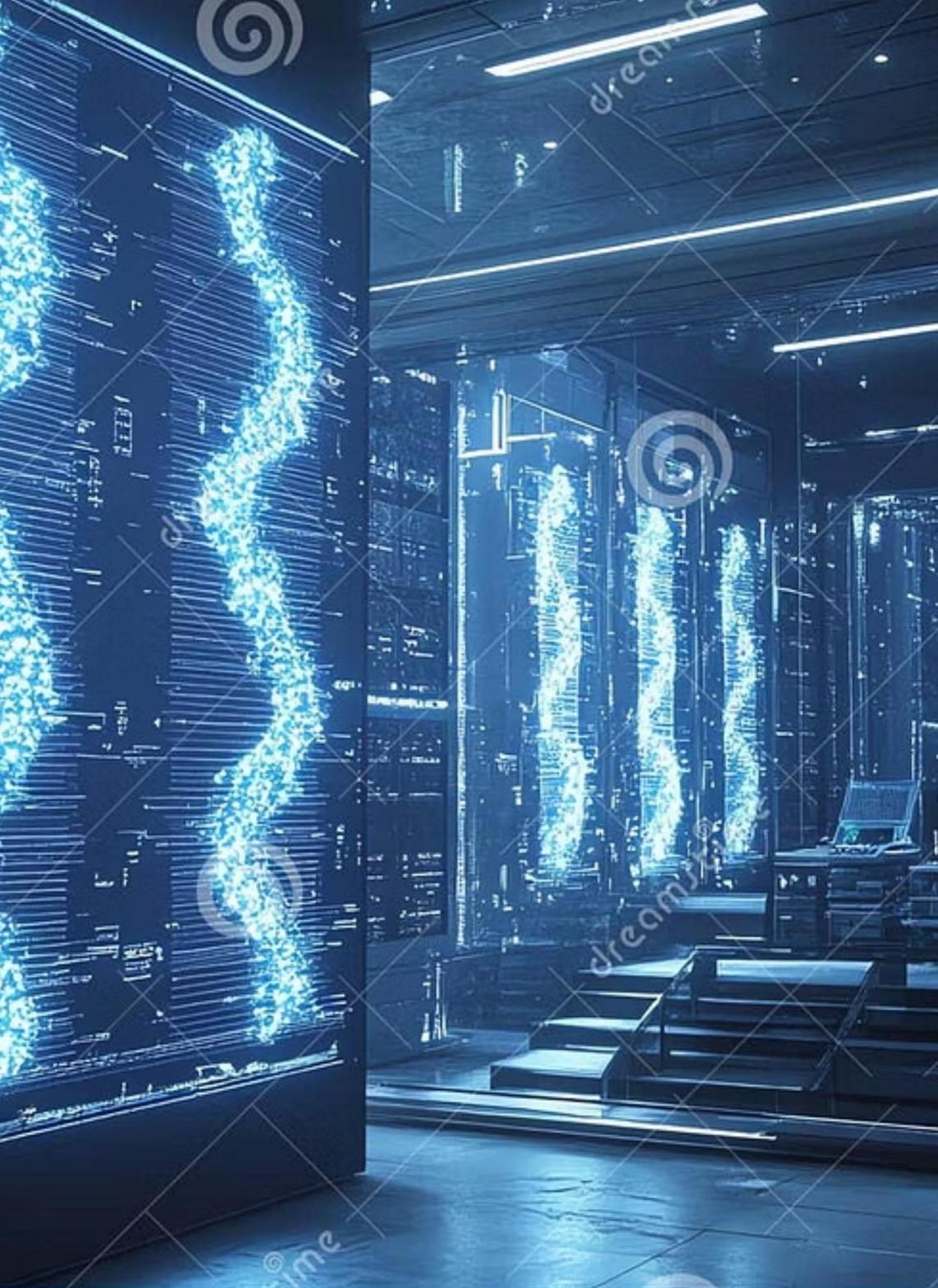
Студент: Эйвази Мани

Группа: НПИбд-03-24

Студенческий билет №: 1032245107

Журналы событий в SystemD (journald)

Эффективное управление логами в Linux



Традиционное логирование в Linux

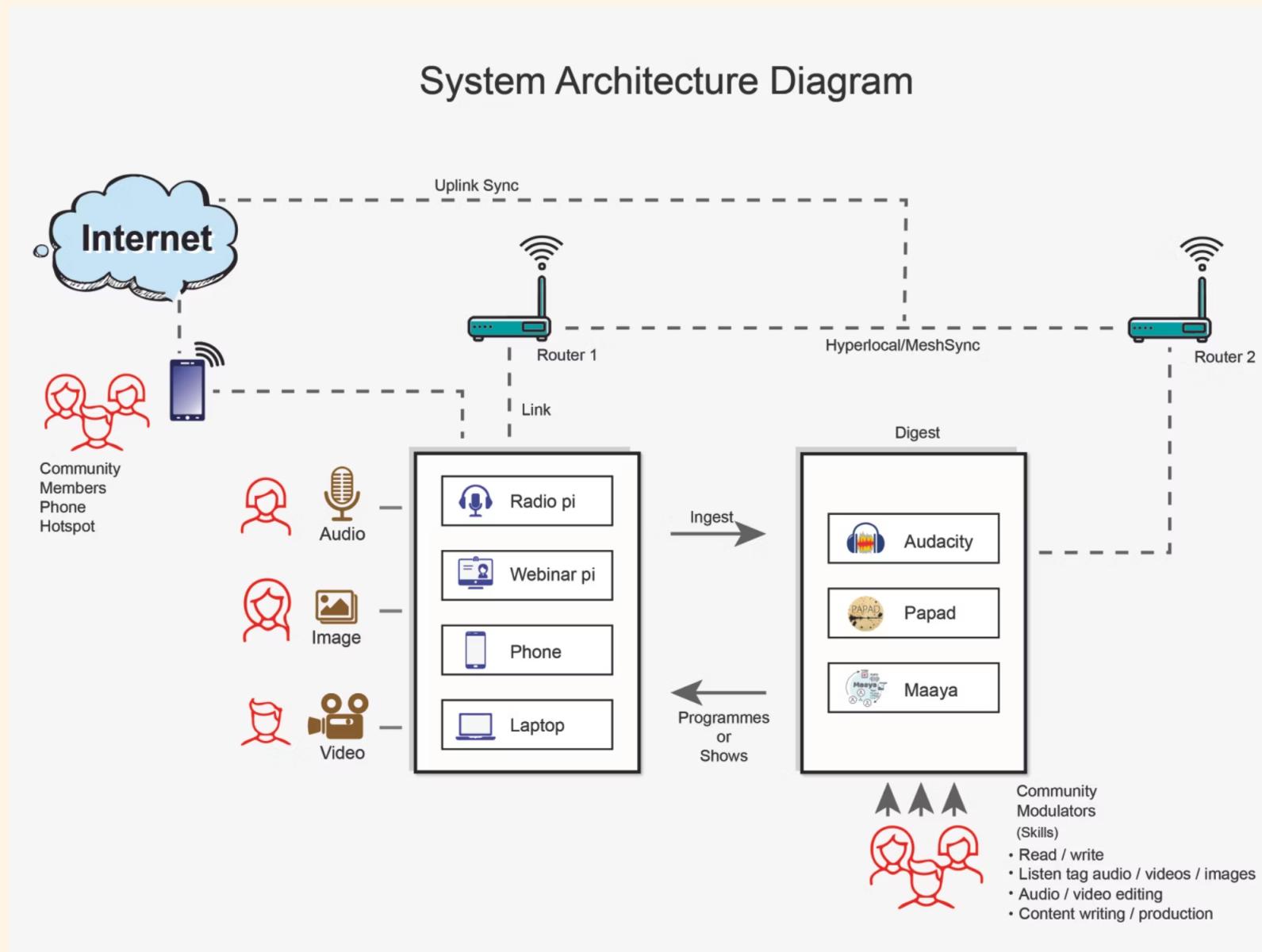
Syslog и текстовые файлы

Долгое время стандартом были текстовые логи в /var/log/.

Ограничения

- *Неструктурированные данные*
- *Сложность парсинга*
- *Отсутствие централизации*
- *Проблемы с безопасностью*

Systemd-journald: новое поколение логов



Назначение и место в SystemD

Systemd-journald – это системный демон, интегрированный в *SystemD*, для сбора и хранения логов.

Он действует как централизованный сборщик событий от ядра, служб, приложений и пользователей.

Принцип работы

- Запускается как демон `systemd-journald.service`
- Перехватывает и индексирует все сообщения
- Бинарный формат для эффективности

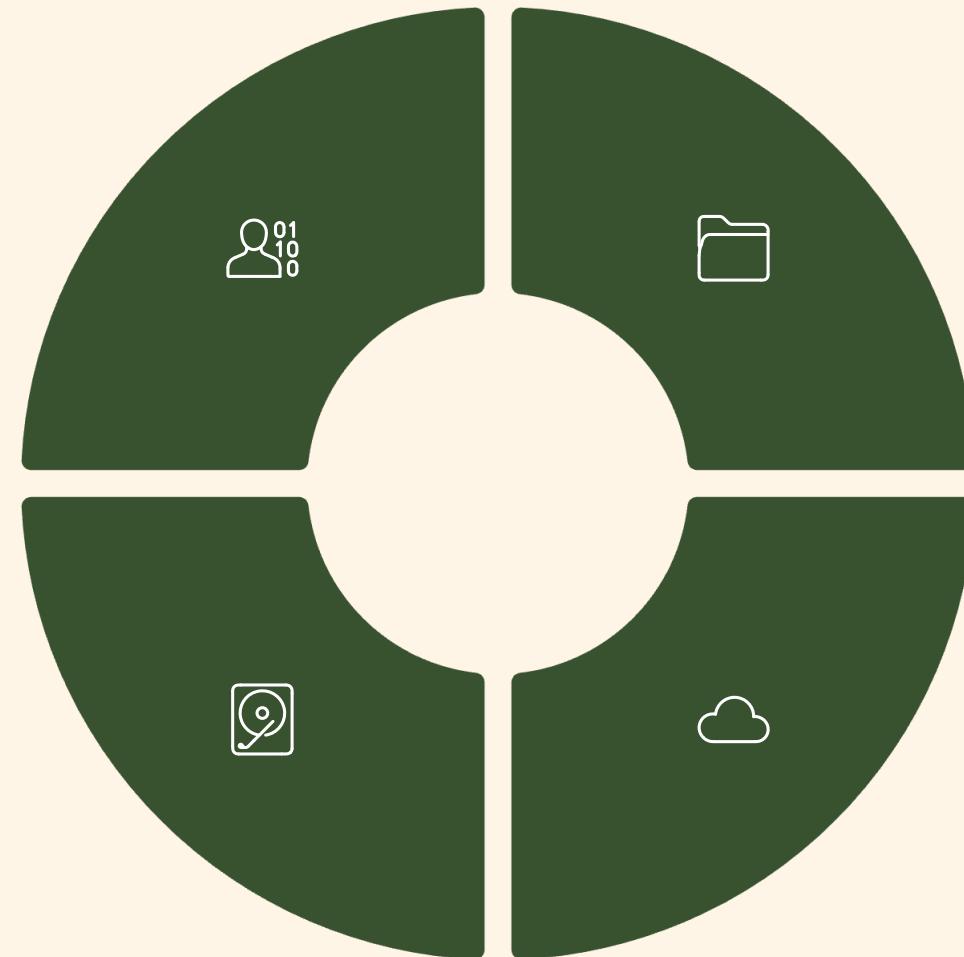
Структура журнала journald

Бинарный формат

*Эффективное хранение, индексация
и быстрый поиск.*

Persistent хранение

*Сохранение между перезагрузками в
`/var/log/journal` (требует
создания каталога).*

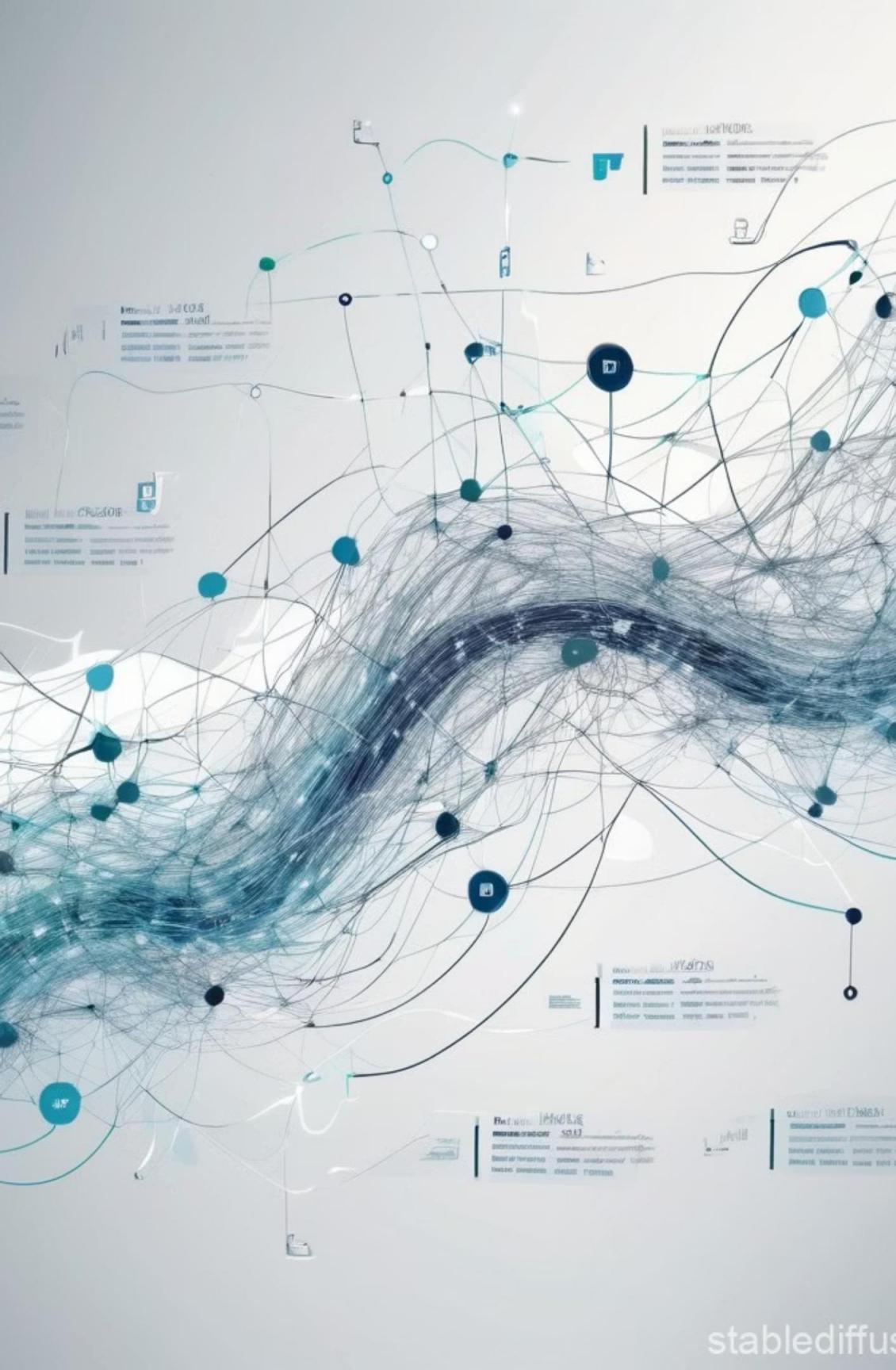


Индексация

*Все поля событий индексируются
для мгновенной фильтрации.*

Volatile хранение

*По умолчанию логи хранятся в ОЗУ
`(/run/log/journal)` до
перезагрузки.*



ГЛАВА 3

Сбор данных: поля и метаданные



Приоритет

Важность события (*от Emergency до Debug*).



Идентификация

PID, UID, GID, CODE_FILE, PID_COMM.



Метка времени

Точное время и дата события.



Источник

Ядро, служба, приложение, пользователь.

Просмотр журналов: утилита journalctl

Базовые запросы

```
journalctl
```

Выводит все логи с самого начала.

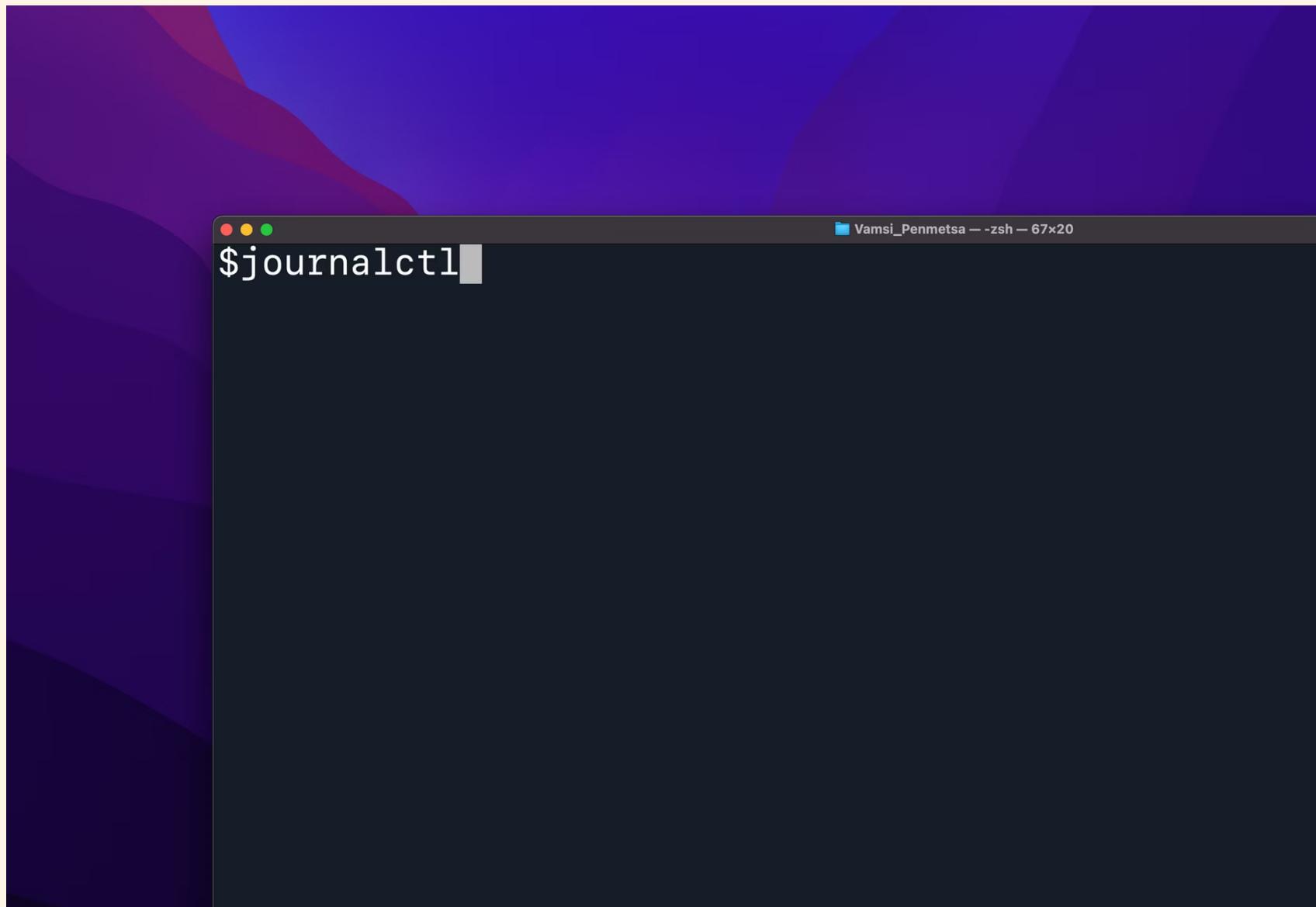
Фильтрация по времени

```
journalctl --since "2 hours ago"
```

Логи за последние 2 часа.

```
journalctl --since "YYYY-MM-DD HH:MM:SS"
```

Логи с определенной даты/времени.



Расширенные возможности journalctl

```
File Edit View Terminal Tabs Help
Terminal - /etc/systemd/system
File Edit View Terminal Tabs Help
Terminal - /var/dotnet/r620-monitor

Oct 07 00:15:04 dotnet-r620-monitor.service[17164]: R620TempMonitor.Worker[0] Server fan control is Manual, temp is 38 C, rolling average temp is 38.1 at 10/07/2019 00:15:04 -04:00
Oct 07 00:15:26 dotnet-r620-monitor.service[17164]: R620TempMonitor.Worker[0] Server fan control is Manual, temp is 38 C, rolling average temp is 38 at 10/07/2019 00:15:26 -04:00
Oct 07 00:15:48 dotnet-r620-monitor.service[17164]: R620TempMonitor.Worker[0] Server fan control is Manual, temp is 38 C, rolling average temp is 38 at 10/07/2019 00:15:48 -04:00
Oct 07 00:16:10 dotnet-r620-monitor.service[17164]: R620TempMonitor.Worker[0] Server fan control is Manual, temp is 38 C, rolling average temp is 38 at 10/07/2019 00:16:10 -04:00
Oct 07 00:16:32 dotnet-r620-monitor.service[17164]: R620TempMonitor.Worker[0] Server fan control is Manual, temp is 38 C, rolling average temp is 38 at 10/07/2019 00:16:32 -04:00
Oct 07 00:16:56 dotnet-r620-monitor.service[17164]: R620TempMonitor.Worker[0] Server fan control is Manual, temp is 39 C, rolling average temp is 38.1 at 10/07/2019 00:16:56 -04:00
Oct 07 00:17:19 dotnet-r620-monitor.service[17164]: R620TempMonitor.Worker[0] Server fan control is Manual, temp is 41 C, rolling average temp is 38.4 at 10/07/2019 00:17:19 -04:00
Oct 07 00:17:42 dotnet-r620-monitor.service[17164]: R620TempMonitor.Worker[0] Server fan control is Manual, temp is 39 C, rolling average temp is 38.5 at 10/07/2019 00:17:42 -04:00
Oct 07 00:18:04 dotnet-r620-monitor.service[17164]: R620TempMonitor.Worker[0] Server fan control is Manual, temp is 39 C, rolling average temp is 38.6 at 10/07/2019 00:18:04 -04:00
Oct 07 00:18:25 dotnet-r620-monitor.service[17164]: R620TempMonitor.Worker[0] Server fan control is Manual, temp is 39 C, rolling average temp is 38.7 at 10/07/2019 00:18:25 -04:00
Oct 07 00:18:49 dotnet-r620-monitor.service[17164]: R620TempMonitor.Worker[0] Server fan control is Manual, temp is 39 C, rolling average temp is 38.8 at 10/07/2019 00:18:49 -04:00
Oct 07 00:19:13 dotnet-r620-monitor.service[17164]: R620TempMonitor.Worker[0] Server fan control is Manual, temp is 41 C, rolling average temp is 39.1 at 10/07/2019 00:19:13 -04:00
Oct 07 00:19:34 dotnet-r620-monitor.service[17164]: R620TempMonitor.Worker[0] Server fan control is Manual, temp is 41 C, rolling average temp is 39.4 at 10/07/2019 00:19:34 -04:00
Oct 07 00:19:56 dotnet-r620-monitor.service[17164]: R620TempMonitor.Worker[0] Server fan control is Manual, temp is 42 C, rolling average temp is 39.8 at 10/07/2019 00:19:56 -04:00
Oct 07 00:20:20 dotnet-r620-monitor.service[17164]: R620TempMonitor.Worker[0] Server fan control is Manual, temp is 42 C, rolling average temp is 40.2 at 10/07/2019 00:20:20 -04:00
Oct 07 00:20:43 dotnet-r620-monitor.service[17164]: R620TempMonitor.Worker[0] Server fan control is Manual, temp is 42 C, rolling average temp is 40.5 at 10/07/2019 00:20:43 -04:00
Oct 07 00:21:05 dotnet-r620-monitor.service[17164]: R620TempMonitor.Worker[0] Server fan control is Manual, temp is 43 C, rolling average temp is 40.7 at 10/07/2019 00:21:05 -04:00
Oct 07 00:21:27 dotnet-r620-monitor.service[17164]: R620TempMonitor.Worker[0] Server fan control is Manual, temp is 44 C, rolling average temp is 41.2 at 10/07/2019 00:21:27 -04:00
Oct 07 00:21:49 dotnet-r620-monitor.service[17164]: R620TempMonitor.Worker[0] Server fan control is Manual, temp is 44 C, rolling average temp is 41.7 at 10/07/2019 00:21:49 -04:00
Oct 07 00:22:12 dotnet-r620-monitor.service[17164]: R620TempMonitor.Worker[0] Server fan control is Manual, temp is 44 C, rolling average temp is 42.2 at 10/07/2019 00:22:12 -04:00
Oct 07 00:22:34 dotnet-r620-monitor.service[17164]: R620TempMonitor.Worker[0] Server fan control is Manual, temp is 44 C, rolling average temp is 42.7 at 10/07/2019 00:22:34 -04:00
Oct 07 00:22:57 dotnet-r620-monitor.service[17164]: R620TempMonitor.Worker[0] Server fan control is Manual, temp is 48 C, rolling average temp is 43.4 at 10/07/2019 00:22:57 -04:00
Oct 07 00:23:19 dotnet-r620-monitor.service[17164]: R620TempMonitor.Worker[0] Server fan control is Manual, temp is 55 C, rolling average temp is 44.8 at 10/07/2019 00:23:19 -04:00
Oct 07 00:23:39 dotnet-r620-monitor.service[17164]: R620TempMonitor.Worker[0] Attempting switch to automatic mode.
Oct 07 00:23:41 dotnet-r620-monitor.service[17164]: R620TempMonitor.Worker[0] Server fan control is Automatic, temp is 56 C, rolling average temp is 46.2 at 10/07/2019 00:23:41 -04:00
Oct 07 00:24:04 dotnet-r620-monitor.service[17164]: R620TempMonitor.Worker[0] Server fan control is Automatic, temp is 57 C, rolling average temp is 47.7 at 10/07/2019 00:24:04 -04:00
Oct 07 00:24:26 dotnet-r620-monitor.service[17164]: R620TempMonitor.Worker[0] Server fan control is Automatic, temp is 52 C, rolling average temp is 48.7 at 10/07/2019 00:24:26 -04:00
Oct 07 00:24:49 dotnet-r620-monitor.service[17164]: R620TempMonitor.Worker[0] Server fan control is Automatic, temp is 57 C, rolling average temp is 50.1 at 10/07/2019 00:24:49 -04:00
```

Фильтрация по службе

`journalctl -u sshd`

Логи для службы SSH.

По приоритету

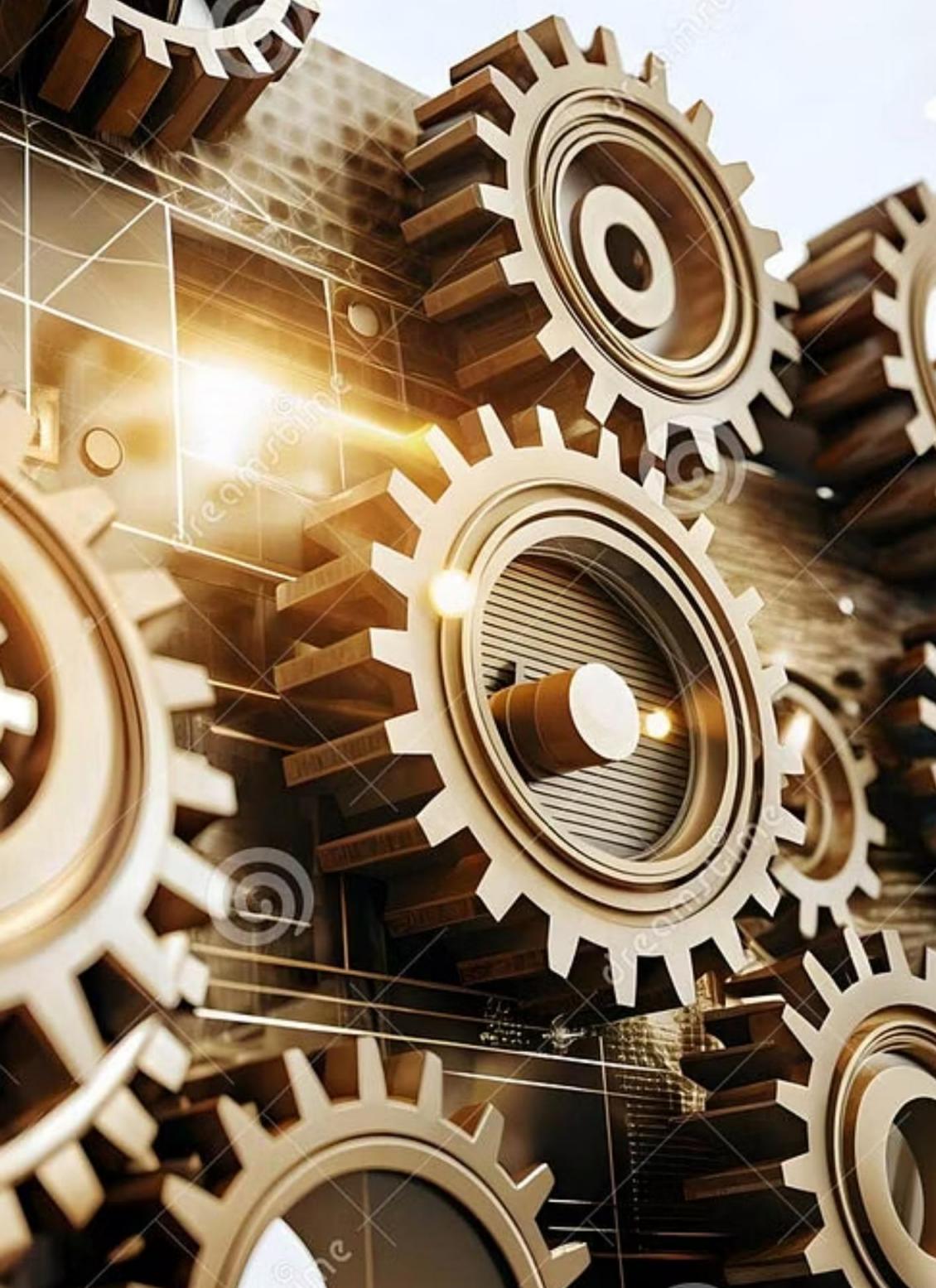
`journalctl -p err -b`

Ошибки текущей загрузки.

Мониторинг в реальном времени

`journalctl -f`

Следование за новыми записями.



ГЛАВА 5

Заключение: journald в современном администрировании

Централизованный сбор

Единая точка входа для всех системных сообщений.

Бинарный формат

Повышенная производительность, безопасность и структурированность.

Мощные инструменты

journalctl для глубокой фильтрации и анализа.

Интеграция

Совместимость с классическим syslog для плавного перехода.

Спасибо за внимание