РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

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

Презентация №7

Журналы событий в SystemD (journald)

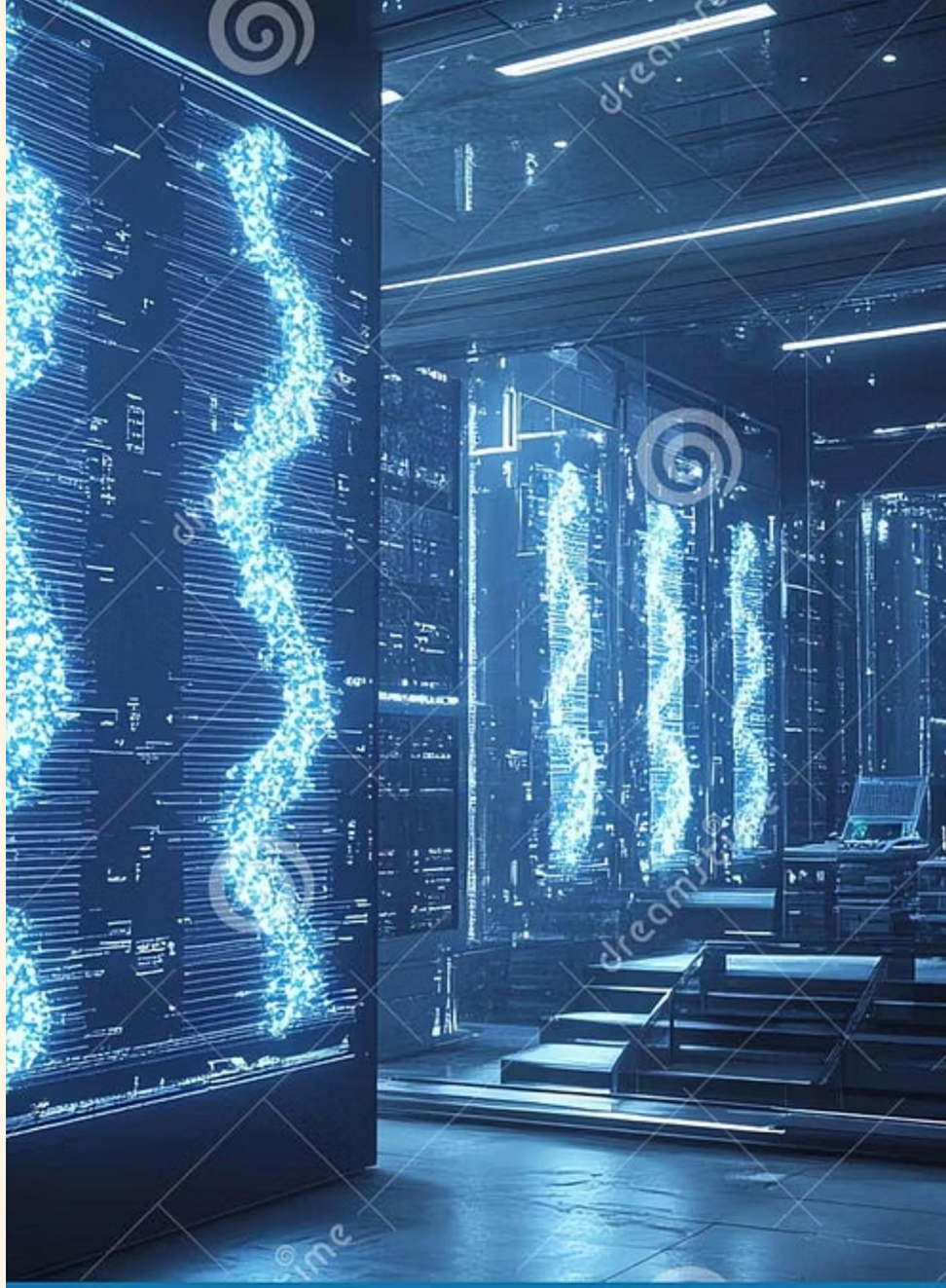
Студент: Эйвази Мани

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

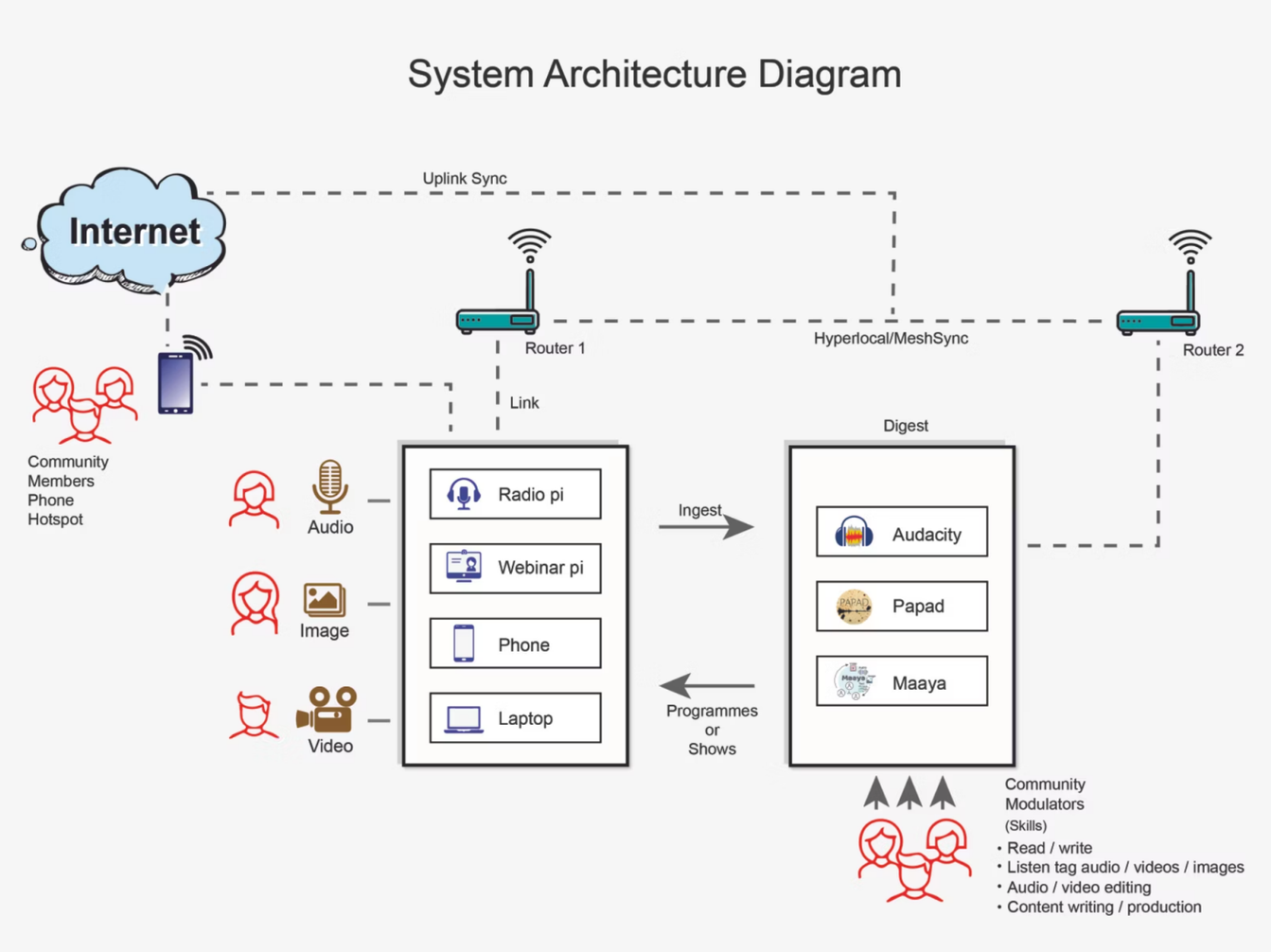
Долгое время стандартом были текстовые логи в `/var/log/`.

Ограничения

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

ГЛАВА 1

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*

ГЛАВА 2

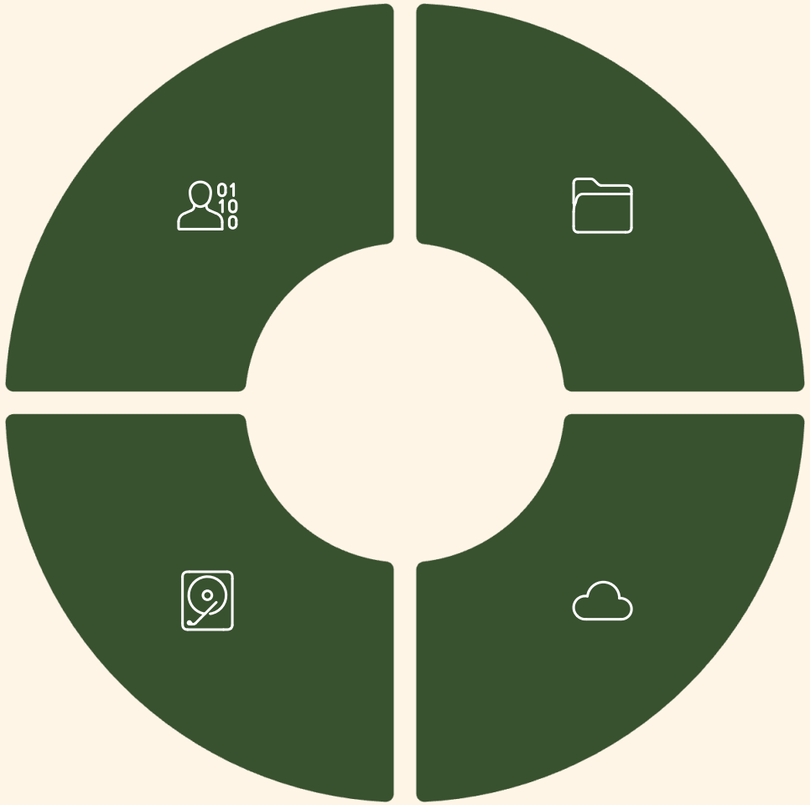
Структура журнала journald

Бинарный формат

Эффективное хранение, индексация и быстрый поиск.

Persistent хранение

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

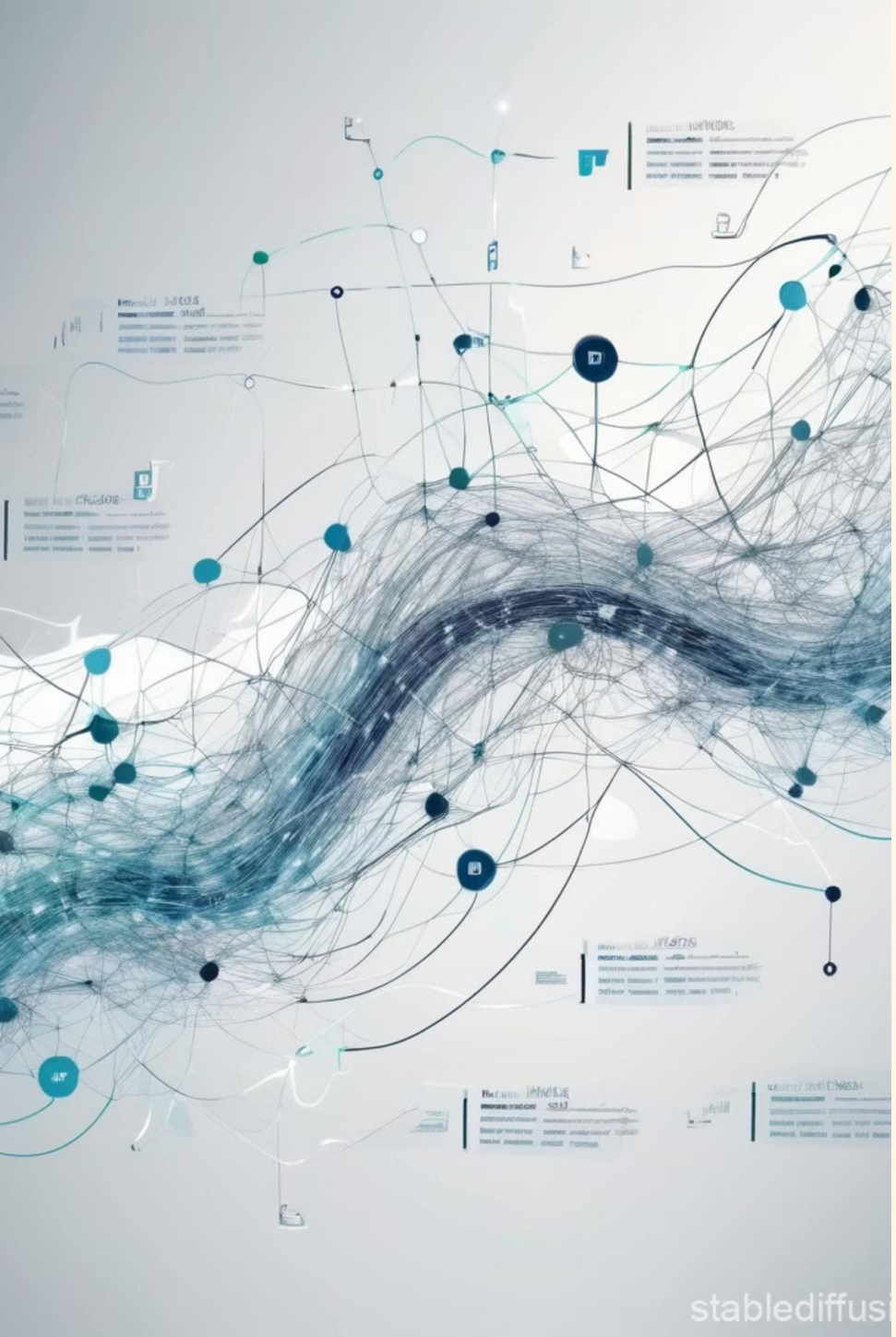


Индексация

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.

ГЛАВА 4

Просмотр журналов: утилита journalctl

Базовые запросы

`journalctl`

Выводит все логи с самого начала.

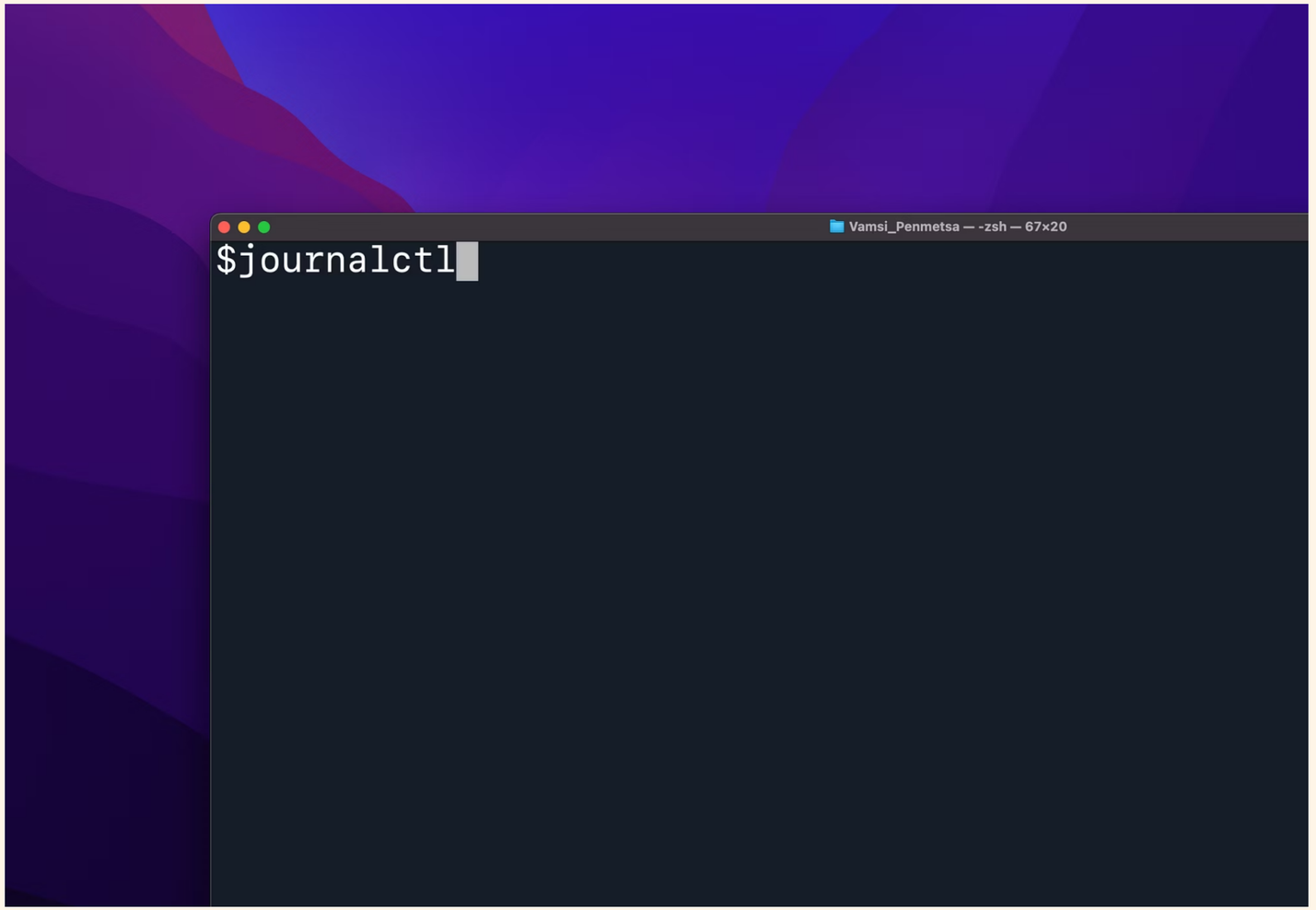
Фильтрация по времени

`journalctl --since "2 hours ago"`

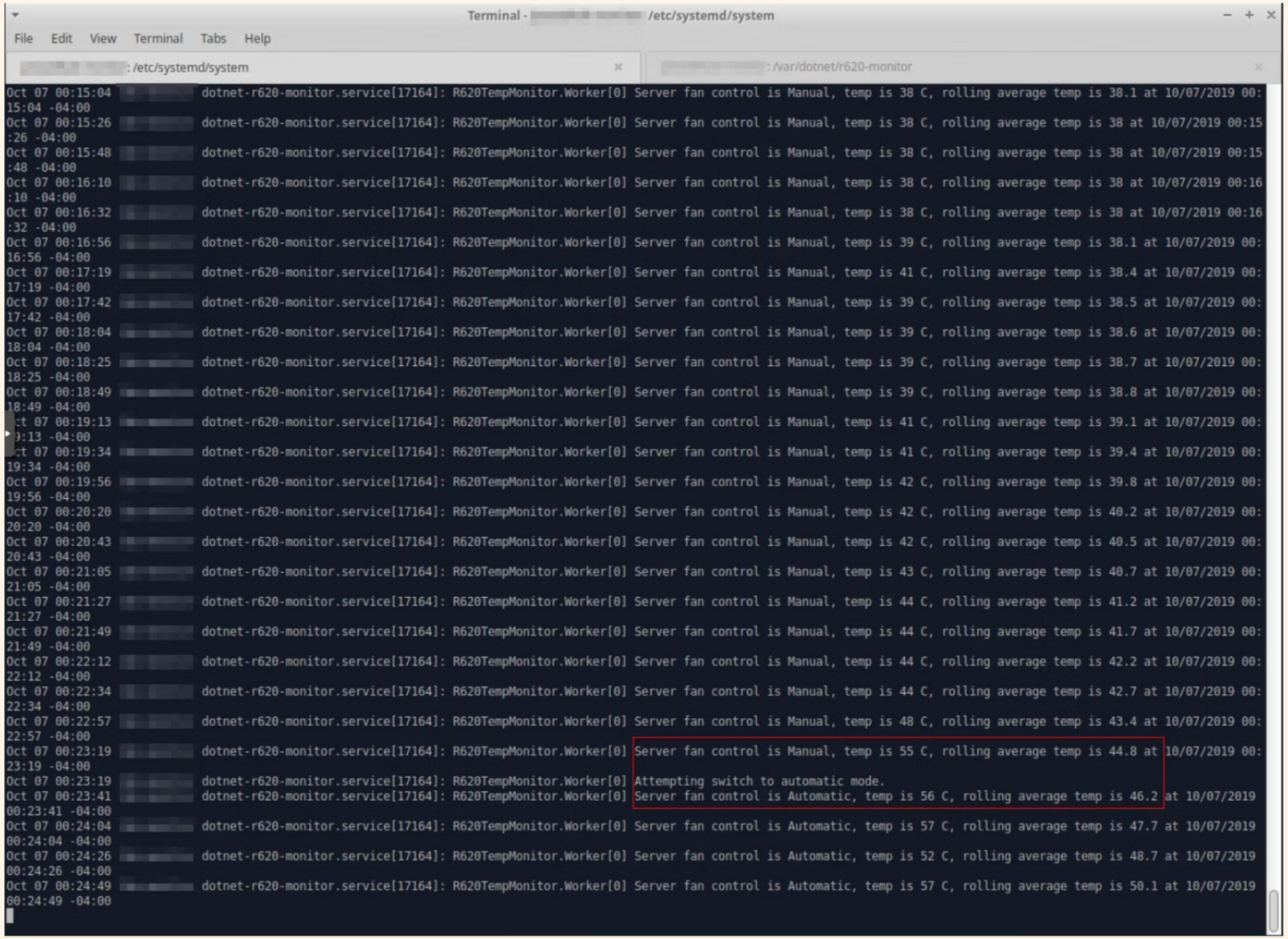
Логи за последние 2 часа.

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

Логи с определенной даты/времени.



Расширенные возможности journalctl



Фильтрация по службе

```
journalctl -u sshd
```

Логи для службы SSH.

По приоритету

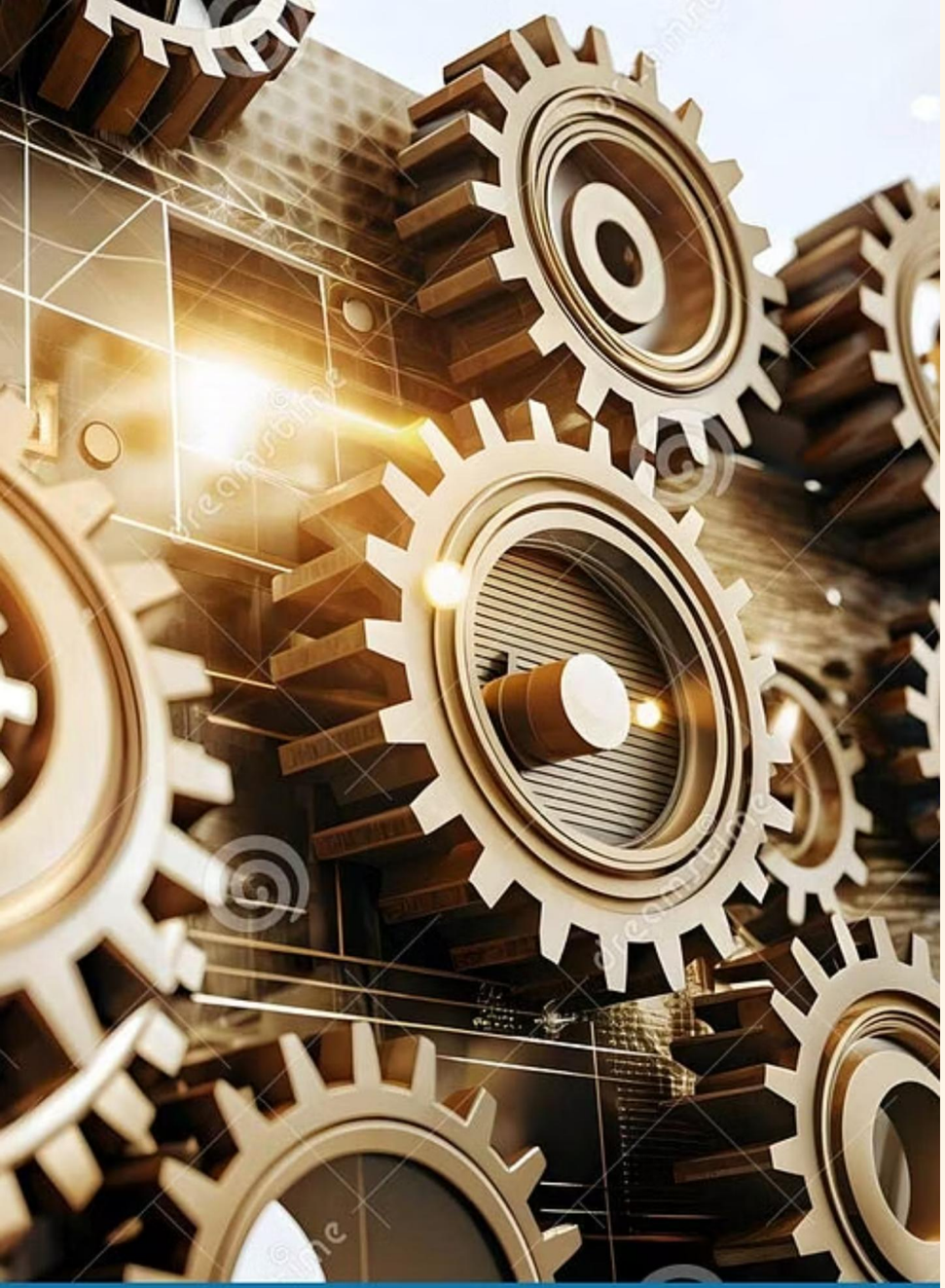
```
journalctl -p err -b
```

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