**Настройка журнала мониторинга в Linux Ubuntu**

Журналирование (логирование) — важная часть администрирования системы. В Ubuntu для этого используются:

- systemd-journald (бинарные журналы, `journalctl`)

- rsyslog(традиционные текстовые логи, `/var/log/`)

---

1. Настройка systemd-journald

journald— компонент systemd, собирающий логи ядра, служб и приложений.

Основные команды

bash

Просмотр всех логов

sudo journalctl

Логи за последний час

sudo journalctl --since "1 hour ago"

Логи конкретной службы (например, ssh)

sudo journalctl -u ssh

Логи с фильтром по уровню (emerg, alert, crit, err, warning, info, debug)

sudo journalctl -p err

Настройка хранения журналов

Файлы журналов хранятся в `/var/log/journal/`.

1. Увеличим размер журнала(по умолчанию — 10% от размера раздела `/var/log`):

sudo mkdir -p /etc/systemd/journald.conf.d/

sudo nano /etc/systemd/journald.conf.d/custom.conf

```

Добавляем:

SystemMaxUse=1G # Максимальный размер журнала

RuntimeMaxUse=500M # Максимальный размер в /run (для временных журналов)

MaxRetentionSec=1month # Хранить логи не более 1 месяца

2. Применяем изменения:

sudo systemctl restart systemd-journald

---

2. Настройка rsyslog

rsyslog — стандартный демон журналирования, пишущий логи в `/var/log/`.

Основные файлы конфигурации

- `/etc/rsyslog.conf` — главный конфиг

- `/etc/rsyslog.d/\*.conf` — дополнительные настройки

Пример настройки ротации логов

1. Редактируем конфиг:

sudo nano /etc/rsyslog.conf

2. Добавляем правило для сохранения логов в отдельный файл (например, для SSH):

if $programname == 'sshd' then /var/log/sshd.log

& stop

3. Применяем изменения:

sudo systemctl restart rsyslog

Проверка работы logrotate:

sudo logrotate -f /etc/logrotate.conf

---

Вывод

Теперь система Ubuntu настроена на:

✅ Хранение логов (`journald`, `rsyslog`)

Для более сложных сценариев можно использовать \*\*ELK Stack (Elasticsearch + Logstash + Kibana)\*\* или \*\*Prometheus + Grafana\*\*.