СИНЕРГИЯ АКАДЕМИЯ

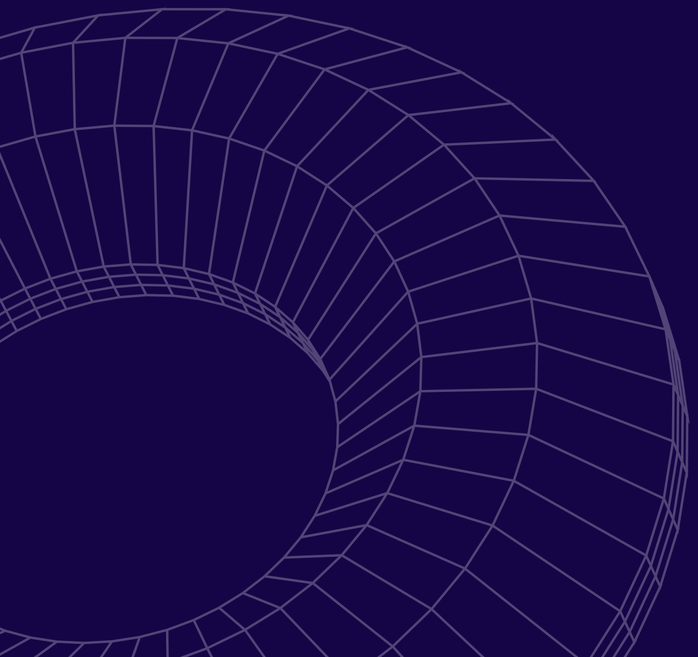
Linux: основы процессов и потоков

МОНИТОРИНГ СИСТЕМЫ, ЛОГИ И ЛУЧШИЕ ПРАКТИКИ

Спикер: Немков Максим

Мониторинг системы, логи и лучшие практики

В ЭТОЙ ТЕМЕ



Как следить
за производительностью системы

01

Как анализировать логи для
выявления и устранения проблем

02

Лучшие практики системного
администрирования, которые
помогают поддерживать стабильность
и безопасность системы

03

Мониторинг производительности

Зачем нужен мониторинг

Выявление узких мест в производительности системы. Оптимизация использования ресурсов: процессора, памяти, дисков и сети

`top и htop`	Показывают загрузку процессора, использование памяти и активные процессы
`free -h`	Отображает информацию об использовании оперативной памяти
`df -h`	Анализ использования дискового пространства

Мониторинг производительности

Мониторинг сети

`iftop` Показывает активность сети в реальном времени

`netstat или ss` Отображают активные подключения ss -tuln

`tar -cvf архив.tar /путь/к/данным` Создание архива

`tar -czvf архив.tar.gz /путь/к/данным` Сжатие архива

Работа с логами

Логи содержат информацию о событиях в системе, таких как ошибки, успешные операции, входы пользователей

Анализ логов помогает находить и устранять неисправности

Основные логи и их местоположение

/var/log/syslog

общий системный лог

/var/log/auth.log

информация о попытках входа в систему

/var/log/dmesg

сообщения ядра, связанные с оборудованием

/var/log/apache2/access.log

запросы к веб-серверу Apache

Работа с логами

`cat /var/log/syslog` Просмотр содержимого лога

`tail -n 20 /var/log/syslog` Просмотр последних строк

`tail -f /var/log/syslog` Просмотр в реальном времени

Очистка логов

`sudo truncate -s 0 /var/log/syslog` Используйте truncate, чтобы очистить файл без удаления

Сохранение логов

Для сохранения логов на удалённом сервере настройте rsyslog

Лучшие практики системного администрирования

Мониторинг безопасности

Следите за логами входов в систему

```
sudo cat /var/log/auth.log
```

Настройте брандмауэр с помощью ufw

```
sudo ufw enable
```

Автоматизация задач

Настройте автоматическое резервное копирование и обновления

Используйте cron для выполнения регулярных задач

Регулярное обновление системы

Устанавливайте обновления, чтобы закрывать уязвимости и повышать стабильность

```
sudo apt update && sudo apt upgrade
```

Очистка системы

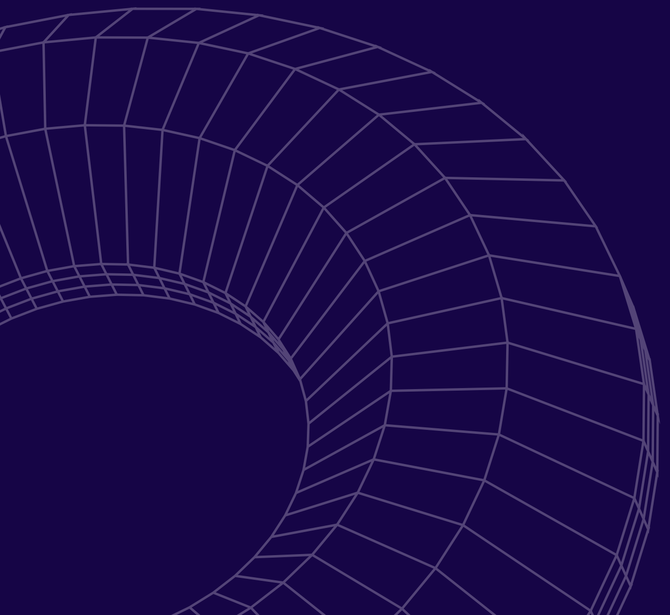
Удаляйте ненужные пакеты

```
sudo apt autoremove && sudo apt clean
```

Следите за заполнением диска с помощью df и освобождайте место

Мониторинг системы, логи и лучшие практики

ИТОГИ



Методы мониторинга производительности системы позволяют отслеживать использование ресурсов, таких как память и дисковое пространство, что помогает выявлять узкие места и оптимизировать работу системы

Анализ логов позволяет быстро обнаруживать ошибки, сбои или необычное поведение системы, что значительно упрощает процесс устранения неполадок и предотвращает их повторение

Знание практик системного администрирования помогает поддерживать стабильность и безопасность системы, минимизирует риски и обеспечивает надежную работу для пользователей и приложений