Конспект к теме

МОНИТОРИНГ СИСТЕМЫ, ЛОГИ И ЛУЧШИЕ ПРАКТИКИ

Введение

Эффективное администрирование системы требует постоянного контроля её состояния, анализа логов и следования проверенным методам управления

В этой теме вы изучите

- Как следить за производительностью системы
- Как анализировать логи для выявления и устранения проблем
- Лучшие практики системного администрирования, которые помогают поддерживать стабильность и безопасность системы

Мониторинг производительности

Зачем нужен мониторинг

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

Основные инструменты мониторинга

top и htop

Показывают загрузку процессора, использование памяти и активные процессы

iotop

Показывает загрузку дисков ввода-вывода

free

Отображает информацию об использовании оперативной памяти

```
free -h
```

df

Анализ использования дискового пространства

```
df -h
```

Мониторинг сети

iftop

Показывает активность сети в реальном времени

netstat или ss

Отображают активные подключения

```
ss -tuln
```

Графический мониторинг

Используйте инструменты, такие как Grafana и Prometheus, для более глубокого анализа и визуализации данных

Мониторинг помогает выявлять проблемы на ранних стадиях и поддерживать оптимальную работу системы

Работа с логами

Зачем нужны логи

- 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
`grep "error" /var/log/syslog`	Поиск ошибок в логах

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

> Логи — это важный источник информации, который помогает анализировать работу системы и устранять проблемы

Лучшие практики системного администрирования

Регулярное обновление системы

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

Устанавливайте обновления, чтобы закрывать уязвимости и повышать стабильность

Автоматизация задач

- Настройте автоматическое резервное копирование и обновления
- Используйте cron для выполнения регулярных задач

Мониторинг безопасности

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

Следите за логами входов в систему

```
sudo ufw enable
```

Настройте брандмауэр с помощью ufw

Очистка системы

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

Удаляйте ненужные пакеты

Следите за заполнением диска с помощью df и освобождайте место

Документация изменений

Ведите записи обо всех изменениях конфигурации системы и обновлениях

Резервное копирование

Настройте автоматическое создание резервных копий с использованием утилит, таких как rsync или tar

Планирование проверок

Регулярно проверяйте журналы, состояние сети и использование ресурсов

Следование лучшим практикам помогает поддерживать систему в стабильном, безопасном и оптимизированном состоянии

ИТОГ

На этом уроке вы узнали, как мониторить производительность системы, работать с логами и следовать лучшим практикам системного администрирования. Эти навыки помогут вам эффективно управлять системой, предотвращать сбои и поддерживать её безопасность