Управление журналами событий в системе

Лабораторная работа 7

Основы администрирования операционных систем

Студентка: Симбине Камила Шеймиле

Группа: НПИбд-03-23

Цель работы

- **Цель:**

Получить навыки работы с журналами мониторинга различных событий в системе'.

Задания

- Мониторинг системных журналов в реальном врем
- Настройка мониторинга событий веб-службы
- Использование journalctl для работы с журналами
- Настройка постоянного журнала journald

Мониторинг системных журналов

Что было сделано:

Использовали команду tail -f /var/log/messages для мониторинга системных журналов в реальном времени. Эта команда позволяет видеть новые события, как только они фиксируются в журнале

Результат:

Мы научились отслеживать системные события в реальном времени, что полезно для диагностики и мониторинга безопасности. Также использовали команду logger, чтобы вручную добавлять сообщения в системный журнал.

Настройка логирования веб-службы

Что было сделано:Установили веб-сервер Apache и настроили его для отправки логов в syslog. В конфигурации Apache добавили строку ErrorLog syslog:local1, которая направляет логи об ошибках через syslog. Затем настроили rsyslog для записи этих логов в отдельный файл /var/log/httpd-error.log

Результат:Логи ошибок веб-сервера теперь записываются централизованно в системные журналы. Это позволяет проще управлять логами и анализировать работу веб-сервера.

Использование journalctl

Что было сделано:Использовали команду journalctl для просмотра системных событий. Осуществили фильтрацию сообщений по времени, пользователю и приоритету сообщений. Также использовали команду journalctl -f для мониторинга в реальном времени.

Результат:Мы научились эффективно работать с журналами с помощью journalctl, фильтровать логи по различным параметрам и отслеживать только те события, которые важны для анализа. Это помогает сужать область поиска и быстрее находить проблемы.

Настройка постоянного журнала journald

•**Что было сделано:**
Настроили систему для сохранения логов после перезагрузки. По умолчанию journald хранит логи в оперативной памяти, что означает их потерю после перезагрузки. Мы создали каталог /var/log/journal и настроили права доступа, чтобы система могла записывать постоянные логи.

•**Результат:**
Теперь все логи сохраняются на диске, и они не теряются при перезагрузке системы. Это позволяет анализировать события, которые происходили до перезагрузки, и отслеживать проблемы, возникающие после

Заключение

•В ходе выполнения лабораторной работы мы научились управлять системными журналами в Unix-подобных системах, используя tail, logger, journalctl, и rsyslog.

•Мы освоили мониторинг системных событий в реальном времени, настройку логирования веб-серверов, а также фильтрацию журналов для получения важных сообщений.

•Настроили постоянное хранение журналов, что улучшает возможность отслеживания системных событий и диагностики ошибок после перезагрузки системы.

•Эти навыки помогут в администрировании систем, улучшении безопасности и эффективности управления журналами событий.

Результат:

•Мы уверенно применяем инструменты для работы с журналами, можем быстро находить проблемы в системе, анализировать логи веб-сервера и настраивать долгосрочное хранение логов для лучшей диагностики в будущем.