Внешний курс

Часть 2 - Анастасия Мазуркевич

17 ноября 2025

Российский университет дружбы народов, Москва, Россия

Цель работы

Цель курса

Освоить системное администрирвоание

Ход выполнения

Урок 4.2. Поиск справочной информации в Linux

В работе с Linux системный администратор постоянно сталкивается с новыми утилитами, командами и конфигурациями. Даже знакомые программы могут содержать десятки неопробованных параметров и опций — запомнить их все практически невозможно.

Умение быстро находить нужную справку помогает сэкономить время и избежать ошибок. В уроке рассмотрим основные способы получить информацию о командах и их использовании в Linux.

Рис. 1: основные способы получить информацию о командах

Задания по теме «Работа с текстовыми файлами в Linux»

Выполните задачи самостоятельно, а затем сверьтесь с готовыми решениями ниже.

Задание №1

Откройте файл /etc/os-release с помощью less и найдите название дистрибу

Задание №2

Используйте grep, чтобы найти строки, содержащие «error» в файле /var/log/

Урок 4.4. Анализ системных логов

В уроке разберем, где хранятся логи в Linux и как с ними работать. Цель — научиться находить, фильтровать и анализировать системные логи для диагностики проблем и мониторинга работы сервисов.

Где хранятся логи

Основное хранилище логов — каталог /var/log/. Здесь находятся как системные, так и лог-файлы различных приложений. Рассмотрим некоторые важные файлы логов:

- /var/log/syslog — общий системный лог (все события системы);
- /var/log/auth.log — логи аутентификации (входы в систему, sudo и т. д.);
- /var/log/kern.log — сообщения ядра Linux;
- /var/log/dmesg — логи загрузки и работы драйверов.

Помимо прочего, различные приложения могут создать в /var/log/ свои папки для хранения логов, например, Nginx или MySQL/MariaDB:

Урок 4.5. Автоматизация анализа логов и работы с текстом

В прошлом уроке мы научились вручную анализировать логи с помощью journalctl. Это удобно, но не всегда эффективно: при возникновении ошибок важна максимально быстрая реакция, особенно если речь о безопасности. Здесь на помощь приходит автоматизация обработки.

В этом уроке мы рассмотрим, как отслеживать логи в реальном времени, выполнять команды по расписанию, а также автоматически сохранять и фильтровать ошибки.

Отслеживание логов в реальном времени

Однако логи могут обновляться каждую долю секунды, а постоянно прописывать команду в терминале неэффективно. Для отслеживания изменений в реальном времени можно использовать утилиту tail с параметром -f:

Урок 5.2. Основы управления пользователями и группами

В этом уроке рассмотрим, как создавать учетные записи пользователей и управлять ими. Разберем зачем нужны группы и как они работают. Не останутся без внимания и технические особенности — например, где хранятся данные о пользователях.

Работа с пользователями

В большинстве Unix-подобных системах, включая Linux и macOS, пользователь — это учетная запись, соотнесенная с человеком или процессом, который имеет определенный доступ к ресурсам системы. С пользователем связано несколько атрибутов. Обязательные из них — имя и уникальный идентификатор (UID). Опциональные — домашний каталог, основная группа, командная оболочка, а также электронная почта и другие привычные записи.

Урок 5.3. Основы управления доступом и разрешениями

В этом уроке вы узнаете о том, как управлять доступом групп и пользователей к файлам. Мы рассмотрим все способы задания доступа — как буквенную, так и цифровую форму записи. Также познакомимся с командами для управления разрешениями.

Проверка доступов

Для того чтобы проверить права доступа к файлу или файлам, используем уже известную нам команду ls с ключом -l (от англ. long listing):

```
ls -l /etc
```

Результат выполнения выглядит примерно так:

Урок 5.4. Повышение безопасности работы с учетными записями

Есть множество аспектов безопасности, про которые надо знать. В этом уроке мы рассмотрим как ограничивать доступ пользователей, какую команду лучше использовать для повышения привилегий. Дадим практических советов, как предотвращать атаки грубой силы на сервер.

Почему лучше использовать sudo вместо su

Часто возникает необходимость выполнить некоторые действия от имени root. В некоторых случаях — от лица другого, обычного пользователя. Эти действия можно выполнить как с помощью команды su, так и sudo. Рассмотрим их особенности.

Безопасность root-пароля

Урок 6.2. Основные принципы прав доступа в Linux

Сначала вспомним «базу», которую рассматривали в предыдущих модулях. Права доступа в Linux — это возможность пользователя системы выполнять одно из следующих действий или любую их комбинацию над файлами:

- чтение (r, read);
- запись (w, write);
- выполнение / запуск программ (x, execute).

Зачем нужно разграничивать права в Linux

Вспоминаем: основная концепция в Linux — «все есть файл». Даже каталоги, программы, носители информации и т. д. И если кто-то из обычных пользователей получит доступ, например, к файлам с конфигурацией системы или важных утилит нечаянно что-то изменит, то это может негативно сказаться на системе — вплоть до полной поломки. Более того, это может остановить работу и других пользователей в ОС.

Урок 7.1. Введение в модуль

В мире Linux-систем процессы — это основа всего. Каждая запущенная программа служба или скрипт работают как отдельный процесс, потребляя ресурсы CPU, памяти и диска. Умение эффективно управлять этими процессами — ключевой навык для администратора, DevOps-инженера или разработчика, который хочет обеспечить стабильность и производительность сервера.

Почему это важно

- Производительность системы. Неоптимизированные процессы могут перегружать сервер, вызывая замедление работы или полный отказ.
- Контроль ресурсов. Вы должны уметь распределять приоритеты между задачами: например, фоновое резервное копирование не должно мешать работ веб-сервера.
- Автоматизация. Современные системы работают на сотнях служб и демонов, которые нужно запускать, останавливать и перезапускать без простоев.

Выводы по проделанной работе

Вывод

В ходе прохождения курса:
- изучили поиск правочной информации в Linux;
- освоили базовые команды.

Полученные навыки позволяют администрировать системы