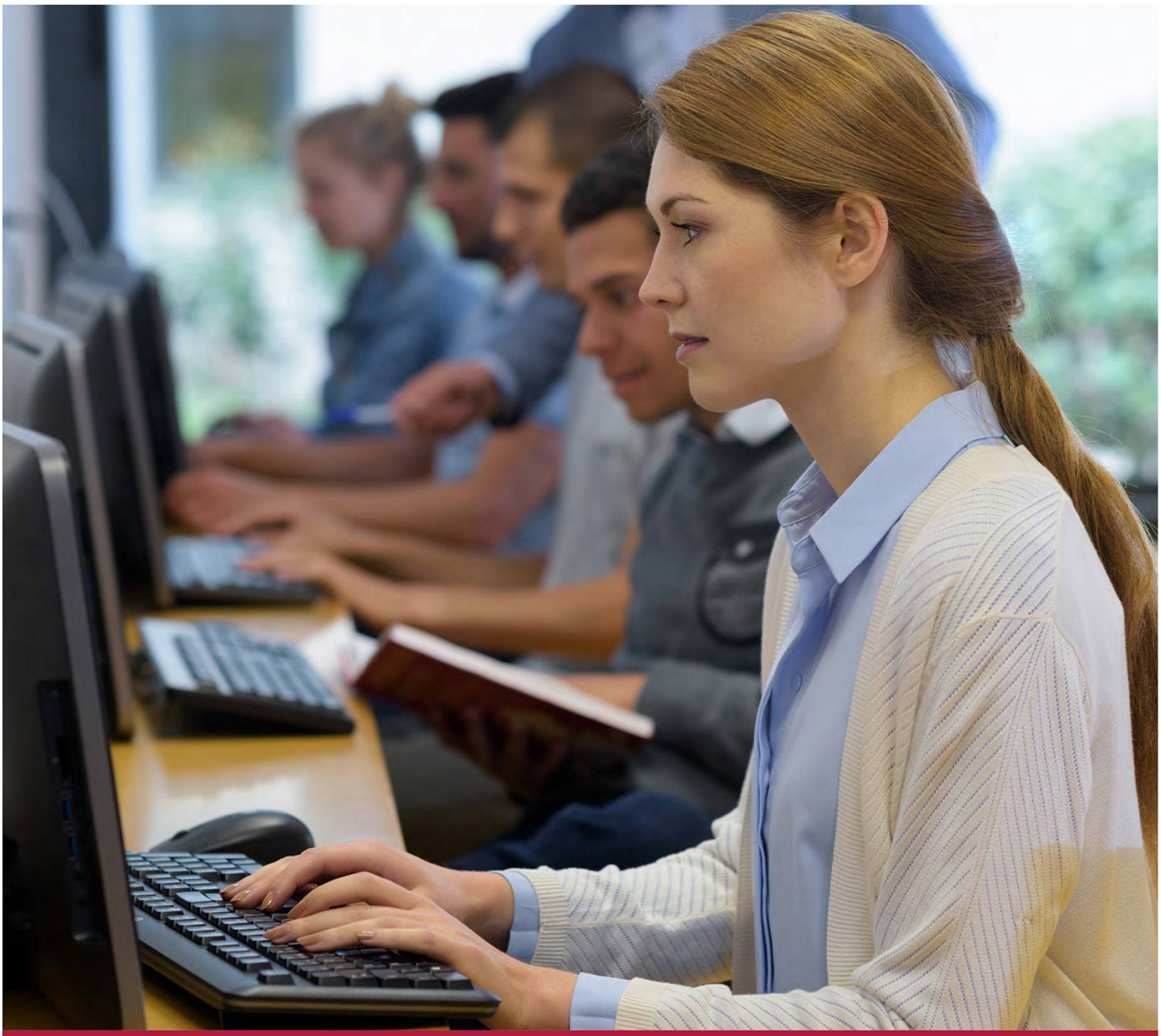
Академия АйТи
a Softline Company



Сетевое администрирование Linux

Код курса: LL-103

+7 (495) 150 96 00 | academy@academyit.ru | academyit.ru

Сетевое администрирование Linux

Код курса: LL-103

Длительность	32 ак. часа
Формат	
Разработчик курса	Академия АйТи
Тип	Учебный курс
Способ обучения	Под руководством тренера

О курсе

Если вы уже имеете уверенные навыки работы с операционной системой Linux на уровне пользователя и знакомы с работой в командной строке, тогда вам непременно будет интересен разработанный специалистами Учебного центра "Академия АйТи" четырёхдневный курс LL-103 Сетевое администрирование ОС Linux, который позволит вам получить теоретические основы о сетевых сервисах ОС Linux и их конфигурировании, а также базовые знания в области информационной безопасности. Курс состоит из десяти модулей и проводится сертифицированными тренерами Учебного центра "Академия АйТи" с учётом профессиональных навыков, знаний, опыта слушателей. Обучение проходит очно в оборудованных классах Учебного центра "Академия АйТи" в 11 городах России (Москве, Санкт-Петербурге, Екатеринбурге, Казани, Красноярске, Нижнем Новгороде, Новосибирске, Омске, Ростове-на-Дону и Хабаровске) или в онлайн формате. По итогам обучения выдаётся сертификат Учебного центра "Академия АйТи".

Подробная информация

Профиль аудитории:

- Специалистам в области IT, желающим получить знания, необходимые для успешного администрирования систем на базе операционной системы Linux.

Предварительные требования:

- Уверенные навыки работы с операционной системой Linux на уровне пользователя.
- Опыт работы с использованием командной строки.

По окончании курса слушатели смогут:

- Создавать и настраивать сетевые подключения.
- Управлять сетевыми службами.
- Устанавливать и настраивать DNS-сервер BIND, веб-серверы, FTP-серверы, почтовые и SAMBA-серверы.
- Контролировать область информационной безопасности.

Программа курса

Модуль 1. Обсуждение целей курса. Сетевое взаимодействие. В этой части вы узнаете о принципах сетевого взаимодействия и о сетевой модели ОС Linux.

- Причины и задачи сетевого администрирования;
- Базовые принципы;
- Работа протокола IP:
- Сетевая модель OSI
- Протокол tcp;
- Протокол udp;
- Протокол icmp.
- Конфигурирование сети в ОС Linux.
- Управление сетевыми сервисами.
- Лабораторная работа.

Модуль 2. Основные сетевые сервисы, DNS и сервер BIND. В этой части вы узнаете о принципах работы сети Internet.

- Разрешение имён, как основа глобального взаимодействия.
- Иерархия DNS;
- Служба доменных имён и её основные задачи;
- Зоны и типы записей;
- Конфигурирование сервера BIND;
- Утилиты для работы с сервером имён;
- Лабораторная работа.

Модуль 3. Электронная почта. В этой части вы узнаете о принципах работы почтовых агентов.

- Принципы работы электронной почты;
- Почтовые службы: sendmail и postfix;
- Конфигурирование почтовых серверов;
- Зоны и типы записей;
- Борьба с нежелательной корреспонденцией и вредоносными программами;
- Лабораторная работа.

Модуль 4. HTTP. В этой части вы узнаете о построении web-сервера на базе apache.

- Принципы работы we-сервисов;
- Функционал web-сервера apache;
- Конфигурирование web-сервера apache;
- Проксирующий сервер Squid b его конфигурирование.

Модуль 5. Доступ к файловой системе. Вы познакомитесь с различными сетевыми сервисами, предназначенными для организации доступа к файловой системе сервере.

- Виды сетевого доступа к файловым ресурсам;
- Конфигурирование FTP-сервера;
- Конфигурирование NFS-сервера;
- Конфигурирование Samba-сервера;

- Работа с FTP, NFS, SAMBA-серверами;
- Лабораторная работа.

Модуль 6. Авторизация и аутентификация. В данном разделе вы узнаете о различных способах авторизации и аутентификации, основанных на сетевых хранилищах учётных записей.

- Основа AA – система PAM, принцип работы;
- Модули PAM;
- Конфигурирование системы PAM;
- Реализация парольной политики;
- Реализация ограничения доступа;
- Принцип работы NIS;
- Конфигурирование NIS;
- Организация доступа к NIS;
- Принцип работы LDAP;
- Конфигурирование OpenLDAP;
- Организация доступа к LDAP;
- Лабораторная работа.

Модуль 7. Основы безопасности. Этот раздел познакомит вас с основными проблемами безопасности и вариантами их решения.

- Принципы построения безопасной системы;
- Политика безопасности;
- Сетевые атаки и средства борьбы с ними;
- Методы диагностирования защищённости системы;
- Резервное копирование.

Модуль 8. Диагностика и защита сети. В данном разделе вы узнаете о процессе диагностирования сетевых соединений, обеспечении безопасности.

- Средства диагностики;
- Сканеры безопасности и интерпретация их отчётов;
- Обеспечение пакетной фильтрации средствами iptables;
- Принципы построения DMZ.

Модуль 9. Целостность данных. Этот раздел расскажет о том, как автоматизировать процесс мониторинга жизнедеятельности сервера, об обеспечении целостности данных.

- Автоматизация процесса мониторинга;
- Анализ журнальных файлов;
- Обеспечение целостности данных;
- Средства аудита;
- Определение производительности системы;
- Расширенные средства управления полномочиями, SELinux и расширенные атрибуты файловых систем ext2/ext3;
- Openssl и потребность в шифровании;
- Основы и типы шифрования.

Модуль 10. Защищённость сетевых сервисов. Вы узнаете о средствах защиты сетевых сервисов.

- Автономные средства разграничения прав доступа;
- Определение доступа с помощью tcp_wrappers;
- Разграничение полномочий средствами xinetd;
- Инструментальные средства обеспечения сетевой безопасности.

Посмотреть расписание курса и записаться на обучение

Обращайтесь по любым вопросам
к менеджерам Академии АйТи

+7 (495) 150 96 00 | academy@academyit.ru