



Содержание

Введение	6
Условные обозначения	7
Схема класса и виртуальной сети	8
Модуль 1. Системное администрирование	10
1.1. Процесс загрузки ОС	10
1.1.1. Универсальный загрузчик GRU	11
1.1.2. Работа с командами загрузчика GRUB	14
1.2. Уровни выполнения	18
1.3. Определение характеристик оборудования и его совместимости ..	23
1.4. Установка ОС	25
1.4.1. Методы установки ОС Linux	25
1.4.2. Создание инсталляционного ресурса	26
1.4.3. Процесс установки	27
1.4.4. Автоматизированная установка kickstart.....	32
1.4.5. Установка с использованием технологии PXE	36
1.5. Управление пакетами программ.....	36
1.5.1. Менеджер пакетов RPM	37
1.5.2. Менеджер пакетов YUM	42
1.5.3. Создание пакетов RPM	44
1.6. Организация хранения данных	47
1.6.1. Создание и управление массивами RAID	48
1.6.2. Создание и управление логическими томами с помощью LVM ..	51
1.7. Резервное копирование и восстановление данных.....	52
1.7.1. Утилиты dump и restore	53
1.7.2. Утилита tar	54
1.7.3. Утилита rsync	55
1.8. Автоматизация выполнения задач	56
1.9. Журналирование системных событий	58
1.10. Мониторинг и оптимизация производительности.....	61
1.10.1. Процессор	61
1.10.2. Память.....	64
1.10.3. Подсистема дискового ввода-вывода	66
1.10.4. Комплексные средства мониторинга системных ресурсов	67
1.11. Установка программ из исходного кода.....	68

Модуль 2. Сетевое администрирование	76
2.1. Централизованное хранилище данных. Каталоги LDAP	76
2.1.1. Настройка конфигурационных файлов LDAP	78
2.1.2. Создание каталога LDAP	79
2.1.3. Подключение к серверу LDAP	80
2.2. Организация общего доступа к файлам (NFS, SMB)	82
2.2.1. Организация общего доступа на основе NFS	82
2.2.2. Организация общего доступа на основе Samba	86
2.3. Система разрешения имен (DNS). Автоматизация получения сетевых параметров (DHCP)	89
2.3.1. Сервис DNS	89
2.3.2. Сервис DHCP	95
2.4. Администрирование веб-сервера Apache	96
2.5. Администрирование прокси-сервера SQUID	101
2.6. Защищенное администрирование. Пакет OpenSSH	104
2.7. Система обмена почтовыми сообщениями. Хранилище почтовых данных	107
2.7.1. Конфигурирование Sendmail	107
2.7.2. Конфигурирование Dovecot	110
2.8. Администрирование общих сетевых сервисов (xinetd, FTP, NTP)	111
2.8.1. Сервис xinetd	111
2.8.2. Сервис FTP	112
2.8.3. Сервис NTP	114
2.9. Основы маршрутизации в сетях TCP/IP	115
 Модуль 3. Организация информационной безопасности	 118
3.1. Управление интеллектуальными списками доступа (SELinux)	118
3.1.1. Режим работы и политика механизма SELinux	119
3.1.2. Использование утилиты SELinux Troubleshooting Tool	120
3.1.3. Работа с контекстами безопасности	120
3.2. Организация межсетевого экрана (iptables)	121
3.3. Организация виртуальных частных сетей (VPN)	126
3.4. Аудит системных событий (auditd)	130
 Приложения	 135
Приложение 1. Конфигурационный файл загрузчика GURB2	135
Приложение 2. Описание основных категорий и групп пакетов ОС Linux	136
Приложение 3. Основные команды управления LVM	138
Приложение 4. Основные журнальные файлы ОС Linux	140

Практические работы	142
Описание виртуальных машин	142
Практическая работа 1. Системное администрирование ОС Linux	143
Упражнение 1.1. Изменение параметров загрузки ядра ОС Linux.....	143
Упражнение 1.2. Управление системными сервисами	144
Упражнение 1.3. Сетевая инсталляция ОС Linux с использованием сервиса NFS	145
Упражнение 1.4. Установка ядра ОС Linux	148
Упражнение 1.5. Создание отказоустойчивого и масштабируемого хранилища.....	149
Упражнение 1.6. Синхронизация данных.....	152
Упражнение 1.7. Централизованное хранилище журнальных файлов..	156
Упражнение 1.8. Мониторинг системных ресурсов	157
Самостоятельные упражнения и дополнительные вопросы	159
Практическая работа 2. Сетевое администрирование ОС Linux	160
Упражнение 2.1. Сетевая аутентификация пользователей LDAP	160
Упражнение 2.2. Настройка монтирования домашнего каталога пользователя по требованию.....	163
Упражнение 2.3. Настройка динамического обновления записей DNS.....	165
Упражнение 2.4. Организация централизованного веб-доступа к документации ОС Linux.	169
Упражнение 2.5. Настройка аутентификации SSH по публичному ключу.	172
Упражнение 2.6. Создание защищенного почтового сервиса на основе MTA Sendmail и Dovecot.	174
Упражнение 2.7. Организация файлообменного сервиса FTP.....	178
Упражнение 2.8. Синхронизации времени.	181
Самостоятельные упражнения и дополнительные вопросы	183
Практическая работа 3. Организация информационной безопасности ОС Linux	184
Упражнение 3.1. Анализ работы механизма SELinux.....	184
Упражнение 3.2. Настройка ограничений на подключение к Telnet	185
Упражнение 3.3. Организация межсетевого экрана	186
Самостоятельные упражнения и дополнительные вопросы	188
Упражнение 3.4. Организация контроля целостности файлов.....	189
Упражнение 3.5. Организация VPN тунеля	190



Введение

Данное пособие – второе в серии книг по Linux, издаваемых совместно ДМК-пресс (www.dmk-press.ru) и Softline Academy Alliance (www.it-academy.ru). Данный курс предполагает наличие у слушателей знаний в объеме курса RH-033 «Основы работы с ОС Red Hat Enterprise Linux» и является следующей ступенью в освоении ОС Linux. Курс позволяет получить знания и навыки, необходимые для успешного администрирования ОС Linux. В качестве основного рассматриваемого в данном курсе дистрибутива используется Red Hat Enterprise Linux 5 (RHEL)¹, являющийся коммерческим решением компании Red Hat.

Курс предназначен для системных администраторов и инженеров начального² уровня знаний, стремящихся освоить системное и сетевое администрирование ОС Linux, а также использовать данную ОС для решения задач информационной безопасности. После прохождения данного курса, при желании, слушатели могут успешно сертифицироваться на звания Red Hat Certified Technician (RHCT) и Red Hat Certified Engineer (RHCE)³.

Предлагаемый вашему вниманию конспект лекций и практические работы – это основной учебный материал для проведения лекционных и практических занятий по курсу «Администрирование ОС Red Hat Enterprise Linux 5» в учебных центрах Softline Academy (www.it-academy.ru). Эти учебные центры создаются в рамках инициативы Softline Academy Alliance, цель которой объединить учебные заведения и организации, заинтересованные в качественной и эффективной подготовке студентов и молодых специалистов для работы в области IT.

Курс разработан преподавателями Учебного центра ВМК МГУ & Softline Academy (www.it-university.ru), который является первым в России авторизованным учебным центром программы Microsoft IT Academy и первой Академией Softline. Курс рассчитан на 40 академических часов и может быть освоен как самостоятельно, так и под руководством опытного преподавателя в любой из двадцати пяти Академий Softline, находящихся в восемнадцати регионах России.

Данный курс состоит из трех частей, изучение каждой из которых предполагает хорошее усвоение предыдущего материала.

Первая часть курса полностью посвящена системному администрированию и

¹ Здесь и далее по тексту под «ОС Linux» будет пониматься дистрибутив Red Hat Enterprise Linux 5. Начальная подготовка предполагают уверенное знание.

² Начальная подготовка предполагают уверенное знание основ ОС Linux и командного интерпретатора bash, полученных в ходе изучения курса RH-033.

³ Основная информация по программе сертификации Red Hat представлена на сайте <https://www.redhat.com/certification/>

содержит материал, необходимый для успешной сдачи экзамена RHCT (RH202). Данная часть курса содержит в себе вопросы инсталляции ОС Linux, управления пакетами программ, обеспечения резервного копирования, организации хранилища данных, а также другие важные вопросы, связанные с системным администрированием.

Вторая часть курса ориентирована на администрирование сетевых служб и содержит материал, необходимый для успешной сдачи экзамена RHCE (RH302). В данной части курса рассматриваются вопросы организации каталогов LDAP, проектирования и развертывания веб-серверов на базе Apache, управления системами кеширования и фильтрации контента, администрирования общих сетевых служб, а также использования ОС Linux для решения задач маршрутизации данных в сетях TCP/IP.

В третьей части курса рассматриваются вопросы информационной безопасности, которые должны знать специалисты, сертифицирующиеся на звание RHCE и желающие продолжить дальнейшее обучение в области защиты данных.

После завершения обучения данному курсу вы будете обладать необходимыми знаниями, и уметь:

- устанавливать, настраивать и обновлять ОС Linux;
- устанавливать и настраивать дополнительные пакеты программ;
- устанавливать программы из исходного кода;
- определять характеристики серверного оборудования и выбирать оптимальную конфигурацию ОС Linux с учетом системных требований;
- эффективно управлять системными процессами и сервисами;
- администрировать учетные записи пользователей и групп;
- обеспечивать надежное хранение и резервирование данных;
- администрировать основные сетевые службы, поддерживаемые ОС Linux;
- настраивать маршрутизацию трафика в сетях TCP/IP, используя ОС Linux и соответствующие программы;
- организовывать безопасное функционирование системных и сетевых служб, используя механизм SELINUX;
- настраивать межсетевой экран;
- настраивать аудит системных и сетевых событий;
- обеспечивать ведение централизованного журнала событий;
- определять «узкие» места в производительности ОС Linux и приложений;
- восстанавливать ОС Linux в случае программных или аппаратных сбоев.

Условные обозначения

В данном пособии применяются следующие условные обозначения.

Имена файлов и папок начинаются со строчных букв (при работе в командной строке или графической оболочке регистр букв всегда имеет значение).

Аббревиатуры напечатаны ПРОПИСНЫМИ БУКВАМИ.

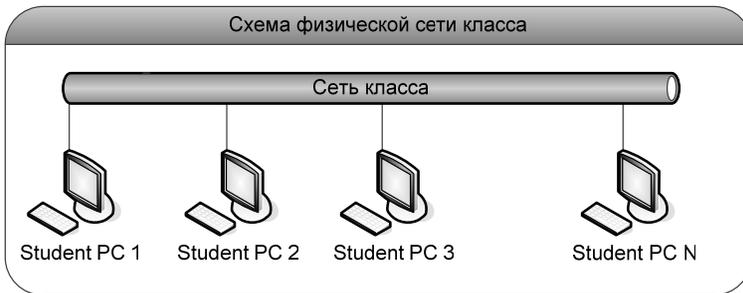
Листинги кода, примеры команд, а также текста, выводимого на экран, выделены данным шрифтом, причем ввод команды выделен **жирным шрифтом**.

Необязательные аргументы команд заключены в квадратные скобки (например: данный [аргумент] является необязательным).

Обязательные аргументы команд записываются без квадратных скобок.

Ключевые термины выделены *полужирным курсивом*.

Схема класса и виртуальные машины



Класс, в котором выполняются практические работы, состоит из физических компьютеров, объединенных в локальную сеть с адресом 192.168.1.0/24 и имеющих динамическую IP-адресацию (DHCP). Все практические работы по данному курсу выполняются на виртуальных машинах, работающих под управлением ПО VMware Player.

Учетные данные для регистрации на физическом компьютере слушателя (Host PC):

Имя пользователя: _____

Пароль: _____

Домен (если есть): _____

В качестве операционной системы *хостовой машины* (физической рабочей станции слушателя, на которой работает ПО VMware Player) используется ОС Microsoft Windows XP. В качестве операционной системы *гостевых машин*, в которых непосредственно выполняются все практические работы, используется ОС Red Hat Enterprise Linux 5 (RHEL5).

У каждого слушателя имеется одна виртуальная машина `rhel5.linux.lab`. Данная виртуальная машина имеет один сетевой интерфейс (`eth0`), используемый для связи между виртуальными машинами и выхода в физическую сеть класса. Все практические работы выполняются на виртуальной машине `rhel5.linux.lab`.

