Приложение A

Подготовьте систему к пробным экзаменам

Рэнди Расселл, директор по сертификации **Red Hat**, заявил в 2009 году в блоге, что экзамены **Red Hat** больше не требуют "установка на голое железо". Другими словами, когда вы сегодня сядете на экзамен **Red Hat**, вам будет предоставлена предустановленная система. В этом приложении вы создадите предустановленную систему, которая будет работать с образцами экзаменов, включенными в электронный формат на DVD в подкаталоге **"Exams/"**. Каждый экзамен описан на первой странице приложений с **B** по **E**, ответы на которые приводятся ниже.

Если вы только учитесь на **RHCSA**, прочитайте следующий раздел. Если вы также готовитесь к **RHCE**, прочитайте также и этот раздел.

Основные системные требования к образцам экзаменов.

Тестовая система для **RHEL** 7 требует большего. Для целей экзамена **RHCSA** или **RHCE** не требуется физическая «установка на голое железо». Однако для **RHCSA** вам необходимо «настроить физическую машину для размещения виртуальных гостей». Можно также ожидать «установки систем **Red Hat Enterprise Linux** в качестве виртуальных гостей».

Для виртуальной машины RHEL 7 по умолчанию (**KVM**) требуется процессор, поддерживающий аппаратную виртуализацию, как описано **в главе 1**. Возможно, вам потребуется включить поддержку аппаратной виртуализации в BIOS.

С учетом этих целей можно настроить тестовую систему на основе следующих критериев:

- Установка на физическое 64-битное оборудование
    - Конфигурация с двойной загрузкой с другой операционной системой является приемлемой.
    - Включите поддержку аппаратной виртуализации в BIOS.
- Достаточно места на жестком диске
    - Всего 60–70 ГБ должно быть достаточно (хотя было бы полезно больше).
    - Кроме того, 16 ГБ каждый для двух или трех систем виртуальных машин должно быть достаточно.

В некоторых случаях возможно установить виртуальную машину внутри виртуальной машины. Хотя мы не тестировали такую конфигурацию для этой книги, решения виртуальных машин, такие как рабочие станции **VMware**, могут, в свою очередь, содержать гостевой гипервизор, на котором запущены другие виртуальные машины. Если это слишком дорого или сложно, просто установите **RHEL 7** на физическую 64-битную систему.

Поскольку одной из целей является "настройка физической машины для размещения виртуальных гостевых машин ", вам нужно будет настроить физическую систему без установки программного обеспечения KVM. (Конечно, вы должны быть готовы к установке KVM во время экзамена.) Как обсуждалось в Главе 1, это идеально, если у вас есть подлинный релиз RHEL 7 для этой цели. Дистрибутивы, такие, как **Scientific Linux 7, CentOS 7** и даже **Oracle Linux 7**, должно работать одинаково хорошо, поскольку они основаны на общедоступном исходном коде **RHEL 7**.

Однако вы не должны использовать **Fedora Linux** для подготовки к экзаменам **Red Hat**. Хотя **RHEL 7** основан на **Fedora Linux, RHEL 7** выглядит по-другому. В некоторых случаях он отличается по функциональности от большинства похожих выпусков **Fedora, Fedora 19** и **Fedora 20**.

Имея в виду эти условия, вы должны подготовить 64-битную физическую тестовую систему в соответствии с требованиями, описанными в главе 1. Как предлагается в этой главе, вы должны настроить установку узла виртуализации, как показано на рисунке A-1.

Вы также можете настроить графический интерфейс, как также обсуждалось в Главе 1. Для этого вы должны выбрать сервер с базовой средой GUI во время процесса установки. Это включает в себя следующие необязательные группы пакетов:

- **Клиент виртуализации (Virtualization Client)** Включает клиентов для установки и управления экземплярами виртуализации.
- **Virtualization Hypervisor** Устанавливает минимально возможную установку хоста виртуализации.
- **Virtualization Tools** Включают инструменты для автономного управления виртуальными образами

Но чтобы соответствовать подразумеваемым требованиям тестовой системы для **RHCSA**, вам необходимо убедиться, что программное обеспечение виртуальной машины не установлено во время процесса установки, как показано на **рисунке А-2.**

РИСУНОК А-1 RHEL 7 Установка хоста виртуализации

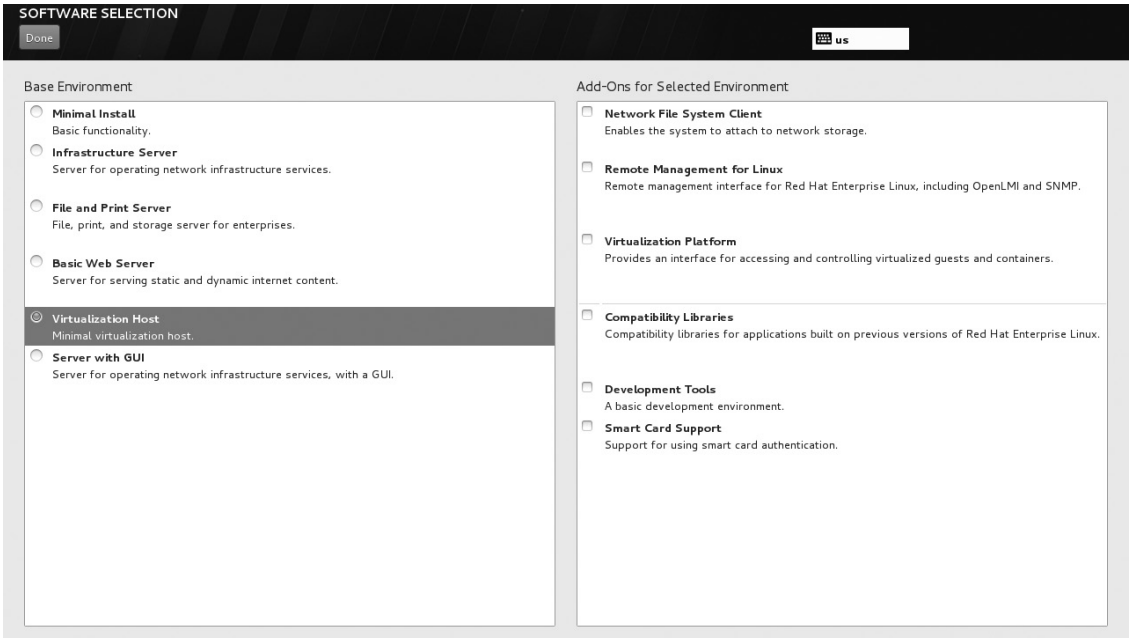
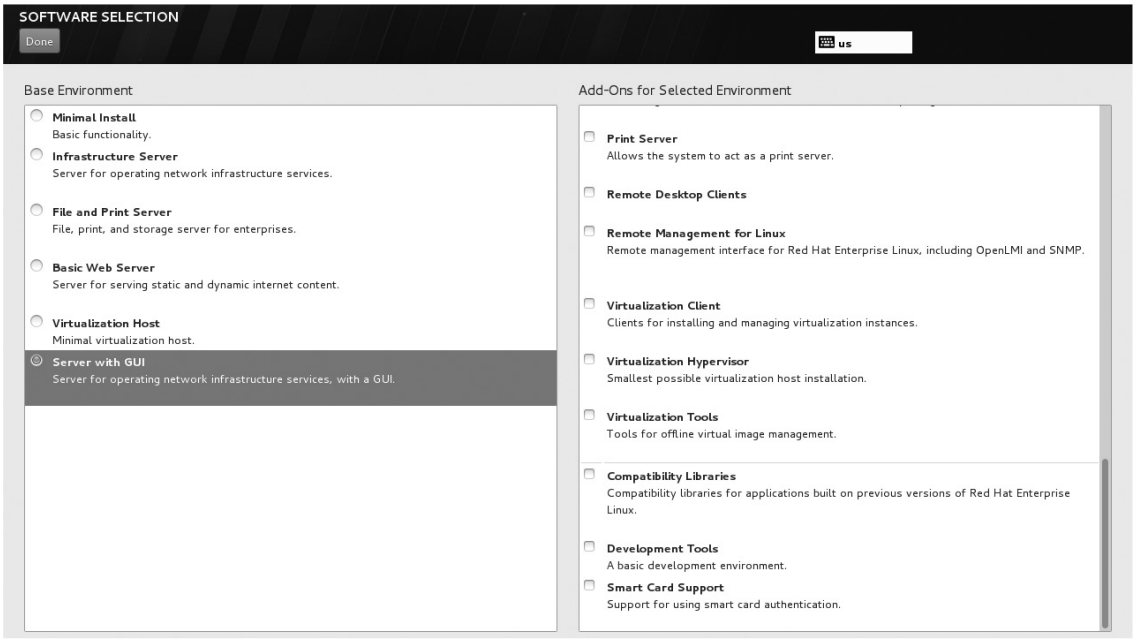


РИСУНОК А-2 RHEL 7 Сервер с установкой графического интерфейса, без программного обеспечения виртуальной машины



После завершения установки система будет готова к экзамену **RHCSA**. Но требуется еще один шаг. Вам необходимо настроить репозиторий установки для локальной сети. Это нормально делать на физической хост-системе. Один метод описан в **главе 1, лабораторная работа 2**.

Дополнительный образец экзаменационной системы

Требования к RHCE

Чтобы быть готовым к экзамену **RHCE**, вам необходимо сделать больше. В частности, вам понадобится как минимум две системы виртуальных машин в системе физического хоста. В главе 1 были настроены три системы виртуальных машин и одна запасная в двух разных сетях.

Если вы только учитесь на **RHCE**, вы можете включить программное обеспечение виртуальной машины в процесс установки для физической системы хоста. Вам следует настроить виртуальные системы в соответствии с требованиями, описанными в **главах 1 и 2**. Файлы **Kickstart ks.cfg, ks1.cfg** и **ks2.cfg** доступны на DVD-диске в подкаталоге **Exams/**, чтобы помочь в создании этих виртуальных систем.

Приложение Б

Образец экзамена 1: RHCSA

Следующие вопросы помогут оценить ваше понимание материалов, представленных в этой книге. Как уже говорилось во введении, вы должны быть готовы к сдаче экзамена **RHCSA** за 2,5 часа.

Экзамен **RHCSA** является «закрытой книгой». Однако вам разрешается использовать любую документацию, которую можно найти на компьютере **Red Hat Enterprise Linux**. Хотя средства тестирования позволяют вам делать заметки, вы не сможете получать эти заметки из комнаты тестирования.

RHCSA полностью отделена от **RHCE**. Хотя оба экзамена охватывают одни и те же услуги, цели этих служб различны.

В большинстве случаев не существует единого решения, единого метода решения проблемы или установки службы. В **Linux** существует почти бесконечное количество вариантов, поэтому мы не можем охватить все возможные сценарии.

Даже для следующих упражнений не используйте производственный компьютер. Небольшая ошибка в некоторых или во всех этих упражнениях может привести к невозможности загрузки **Linux**. Если вы не можете выполнить действия, описанные в этих упражнениях, вам может потребоваться переустановить **Red Hat Enterprise Linux**. Сохранение любых данных, которые вы имеете в локальной системе, может оказаться невозможным.

Red Hat представляет свои экзамены в электронном виде. По этой причине экзамены в этой книге доступны на сопутствующем DVD в подкаталоге **Exams/**. Этот экзамен находится в файле с именем **RHCSAsampleexam1** и доступен в форматах **.txt, .doc** и **.html**. Для получения подробной информации о том, как настроить RHEL 7 в качестве системы, подходящей для практического экзамена, см. **Приложение А**. Обязательно настройте репозиторий, настроенный в **главе 1, лабораторная работа 2**.

Не переворачивайте страницу, пока не закончите с пробным экзаменом!

RHCSA Образец экзамена 1

Начните с предварительно сконфигурированной системы **RHEL 7**, описанной в **Приложении А**. При необходимости убедитесь, что система в данный момент выключена. Как описано в **Приложении А**, текущий репозиторий установочного DVD-диска **доступен с FTP-сервера**, настроенного в локальной системе. У вас будет два с половиной часа для выполнения следующих задач:

1. Убедитесь, что **SELinux** установлен в принудительном режиме.
2. Установите программное обеспечение для виртуализации в локальной системе.
3. Используйте файл **ks.cfg** из подкаталога **Exams/** для создания виртуальной машины. При необходимости измените его, чтобы настроить систему с именем хоста **server2.example.com** по адресу **IPv4 192.168.122.51**.

4. Настройте виртуальную машину на автоматический запуск при следующей загрузке локальной физической системы.
5. Используйте **ssh** для доступа к **VM**, как если бы это была удаленная система. Установите новый пароль **root** в **RedHat4Ever!** (примечание: текущий пароль **root** не предоставляется).

   Дополнительные шаги в этом экзамене должны быть применены к системе **server2.example.com**.

6. Настройте новый раздел объемом **500 МБ** в доступном пустом пространстве диска. Создайте физический том (**physical volume**) в новом разделе и группу томов (**volume group**) с именем «**vg01**» с размером физического экстента (**extent**) **8 МБ**. Настройте логический том (**logical volume**) в новой группе томов (**volume group**) с именем «**lv_project**» размером **logical extents 32**.
7. Отформатируйте новый логический том в файловой системе **xfs** и смонтируйте его в каталоге **/project**. Убедитесь, что он автоматически монтируется при следующей загрузке системы. Используйте **UUID** нового тома.
8. Найдите все файлы в каталоге **/etc**, имя которых заканчивается расширением «***.conf**», и сохраните их полные имена файлов в файле **/root/configfiles.txt**.
9. Создайте сжатый **bzip** архив **tar** с именем **/tmp/etc.tar.bz2**, содержащий все файлы в каталоге **/etc**.
10. Настройте следующих пользователей для RHEL: **nancy, randy, donna,** и **mike.** Сделайте **nancy** и **randy** частью группы с именем **friends** с **GID 2000**. Создайте каталог **/home/friends** и разрешите им обмениваться файлами без необходимости изменять права доступа или владельца любого файла, который они помещают в этот каталог. Не давайте **donna** или **mike** права на чтение в этом каталоге.
11. Убедитесь, что срок действия учетной записи пользователя **mike** истекает через неделю.
12. Настройте задание на удаление всех обычных файлов в каталоге **/home/mike/tmp** во второй день каждого месяца в 3:50.
13. Установите файл **project.test** в домашнем каталоге пользователя **mike**. Настройте списки **ACL** для файла с именем **project.test**, чтобы позволить пользователю **donna** читать этот файл.
14. Настройте систему на использование сервера **LDAP 192.168.122.1** для получения информации о пользователе и для аутентификации. Установите для базового **LDAP search DN to dc=example,dc=com**. Включить **TLS**.
15. Отключите экзаменационную систему.

RHCSA Образец экзамена 1 Обсуждение

В этом обсуждении мы опишем один из способов проверки вашей работы на соответствие требованиям, перечисленным для экзамена RHCSA образца 1.

1. Один из способов проверить, установлен ли **SELinux** в принудительном режиме, - запустить команду **sestatus**.
2. Если программное обеспечение для виртуализации установлено в локальной системе, у вас будет доступ к диспетчеру виртуальных машин в графическом интерфейсе или, по крайней мере, к командам **virt-install** и **virsh** из командной строки.
3. В случае успеха вы сможете получить доступ к новой системе **server2.example.com** через **ssh** или через диспетчер виртуальных машин.
4. Один из способов настроить отмеченную систему на автоматический запуск при следующей загрузке хоста с помощью команды **virsh autostart server2.example.com**. Один из способов подтвердить это - вывод команды **virsh dominfo server2.example.com**.
5. Если вы не знаете, как восстановить пароль **root**, просмотрите **упражнение 5-2**.
6. Чтобы просмотреть текущие группы томов (**volume groups**), выполните команду **vgdisplay**. Проверьте размер **PE**. Чтобы вывести список всех логических томов (**logical volumes**), выполните команду **lvdisplay**. Размер нового тома должен составлять 32 логических экстента (**logical extents**), что эквивалентно **256 МБ**.
7. Чтобы убедиться, что том автоматически монтируется при следующей загрузке системы, он должен быть настроен в **/etc/fstab** на соответствующий формат с **UUID**, связанным с томом, как это предусмотрено командой **blkid**. Вот пример:

   UUID=d055418f-1ff6-46bf-8476-b391e82a6f51 /project xfs defaults 1 2 8.

8. Следующая команда показывает один метод для выполнения этой задачи:

   # find /etc -type f -name "*.conf" >/root/configfiles.txt 2>/dev/null 9.

9. Запустите команду **file /tmp/etc.tar.bz2**, чтобы убедиться, что созданный вами файл сжат **bzip**. Распакуйте архив, чтобы проверить его содержимое, или проверьте его с помощью следующей команды:

   # cat /tmp/etc.tar.bz2 | bunzip2 | tar -t

10. Каталог **/home/friends** должен принадлежать группе **friends**. Пока пользователи **donna** и **mike** не входят в эту группу, а другие пользователи не имеют разрешений (или **ACL**) для этого каталога, доступ должен быть ограничен членами группы **friends**. Каталог также должен иметь права **SGID**:

    # ls -ld /home/friends
    drwxrws---. 2 root friends 6 Nov 18 10:54 /home/friends
    # getent group friends
    friends:x:2000:nancy,randy

11. Если вы изменили учетную запись пользователя **mike**, чтобы срок действия его учетной записи истек через семь дней, правильная дата окончания срока действия должна появиться в выходных данных команды **chage -l mike**.
12. Есть несколько способов настроить работу **cron**; это можно настроить в каталоге **/etc/cron.monthly** или задание **cron** для пользователя **root** или **mike** с помощью команды **crontab -u mike -e**. В любом из этих случаев команда будет связана с соответствующей меткой времени, с такой строкой:

    50 3 2 * * /bin/find /home/mike/tmp -type f -exec /bin/rm {} \;

13. Запустите команду **getfacl /home/mike/project.test**. Если пользователь **donna** имеет разрешения на чтение в **ACL**, вы увидите это в выводе этой команды. Вы также должны установить **ACL** в каталоге **/home/mike** и предоставить пользователю **donna** разрешение на выполнение для доступа к файлам в каталоге.
14. Запустите команду **authconfig-gtk**, чтобы просмотреть текущие настройки. «**Use LDAP**» должно быть включено в настройках Информация о пользователе вместе с «**Use LDAP Authentication**». URL-адрес сервера должен быть установлен в **ldap://192.168.122.1**, с включенным (**enabled**) **TLS**.

Приложение C

Образец экзамена 2: RHCSA

Следующие вопросы помогут оценить ваше понимание материалов, представленных в этой книге. Как уже говорилось во введении, вы должны быть готовы к сдаче экзамена **RHCSA** за 2,5 часа.

Экзамен **RHCSA** является «закрытой книгой». Однако вам разрешается использовать любую документацию, которую можно найти на компьютере **Red Hat Enterprise Linux**. Хотя средства тестирования позволяют вам делать заметки, вы не сможете получать эти заметки из комнаты тестирования.

RHCSA полностью отделена от **RHCE**. Хотя оба экзамена охватывают одни и те же услуги, цели этих служб различны.

В большинстве случаев не существует единого решения, единого метода решения проблемы или установки службы. В **Linux** существует почти бесконечное количество вариантов, поэтому мы не можем охватить все возможные сценарии.

Даже для следующих упражнений не используйте производственный компьютер. Небольшая ошибка в некоторых или во всех этих упражнениях может привести к невозможности загрузки **Linux**. Если вы не можете выполнить действия, описанные в этих упражнениях, вам может потребоваться переустановить **Red Hat Enterprise Linux**. Сохранение любых данных, которые вы имеете в локальной системе, может оказаться невозможным.

Red Hat представляет свои экзамены в электронном виде. По этой причине экзамены в этой книге доступны на сопутствующем DVD в подкаталоге **Exams/**. Этот экзамен находится в файле с именем **RHCSAsampleexam1** и доступен в форматах **.txt, .doc** и **.html**. Для получения подробной информации о том, как настроить RHEL 7 в качестве системы, подходящей для практического экзамена, см. **Приложение A**. Обязательно настройте репозиторий, настроенный в **главе 1, лабораторная работа 2**.

Не переворачивайте страницу, пока не закончите с пробным экзаменом!

RHCSA Образец экзамена 2

Начните с предварительно сконфигурированной системы **RHEL 7**, описанной в **Приложении A**. При необходимости убедитесь, что система в данный момент выключена. Как описано в **Приложении A**, текущий репозиторий установочного DVD-диска **доступен с FTP-сервера**, настроенного в локальной системе. У вас будет два с половиной часа для выполнения следующих задач:

1. Установите программное обеспечение для виртуализации в локальной системе.
2. Используйте файл **ks2.cfg** из подкаталога **Exams/** для создания виртуальной машины. При необходимости измените его, чтобы настроить систему с именем хоста **outsider2.example.org** на **IPv4-адресе 192.168.100.101**. (Если существует конфликт IP-адресов с другим хостом в сети, выберите другой адрес, например **192.168.100.102**.)
3. Используйте **ssh** для доступа к **VM**, как если бы это была удаленная система. Установите новый пароль для **root changeme**! (примечание: текущий пароль **root** не предоставляется).

   Дополнительные шаги в этом экзамене должны быть применены к системе **outsider2.example.org**.

4. Сконфигурируйте новый раздел объемом **500 МБ** в свободном месте на диске, отформатированном с помощью файловой системы **xfs.**
5. Смонтируйте эту файловую систему в новый каталог с именем **/cooks**. Убедитесь, что файловая система автоматически монтируется при следующей загрузке системы. Используйте **UUID** нового тома.
6. Установите дополнительное пространство подкачки в оставшееся свободное место на диске.
7. Убедитесь, что новое пространство подкачки автоматически монтируется при следующей загрузке системы. Используйте **UUID** нового тома.
8. Найдите все файлы в каталоге **/etc**, содержащие слово «**redhat**», и сохраните их полные имена в файле с именем **/root/etc-redhat.txt**.
9. Настройте следующих пользователей: **linus**, **richard**, **mark**, **bill**. Используя **ACL**, запретите пользователям выставлять счета и Ричарду доступ к каталогу **/cooks**. Разрешить доступ всем остальным пользователям.
10. Настройте автомонтирование и настройте его для чтения DVD в каталоге **/misc/dvd**.
11. Загрузите другое ядро из подкаталога **Chapter7/DVD**-диска книги. Установите это ядро. Убедитесь, что загрузчик по умолчанию указывает на исходное ядро.
12. Настройте систему для загрузки **boot** по умолчанию **multi-user target.**
13. Настройте локальный **NTP-сервер** в одной системе виртуальных машин. Установите этот **NTP-сервер**, чтобы он указывал на физический хост.
14. Убедитесь, что **SELinux** установлен в разрешающий режим (**permissive mode**). (Вы по-прежнему несете ответственность за любые проблемы, связанные с **SELinux**.)
15. Отключите экзаменационную систему.

RHCSA Пример экзамена 2 Обсуждение

В этом обсуждении мы опишем один из способов проверки вашей работы на соответствие требованиям, перечисленным для экзамена **RHCSA образца 2**.

1. Если программное обеспечение для виртуализации установлено в локальной системе, у вас будет доступ к диспетчеру виртуальных машин в графическом интерфейсе или, по крайней мере, к командам **virt-install** и **virsh** из командной строки.
2. Если новая установка **Kickstarted** прошла успешно, вы сможете получить доступ к новой системе **outsider2.example.org** либо через **ssh**, либо через диспетчер виртуальных машин.
3. Любой, у кого есть доступ к учетной записи администратора на виртуальной машине, может просматривать имена входа на основе **ssh** в файле **/var/log/secure**. Это простой способ убедиться, что вы использовали команду **ssh** для подключения к новой системе. Если вы не знаете, как восстановить пароль **root**, просмотрите **упражнение 5-2**.
4. Все разделы (новый раздел **500 МБ**, дополнительное пространство подкачки) должны быть показаны в выводе команды **fdisk -l**.
5. При правильной настройке новая файловая система должна отображаться в выходных данных команды **mount**, помеченных как «**type xfs**».
6. Когда создается дополнительное пространство подкачки, оно должно отображаться в содержимом файл **/proc/swaps**. В качестве альтернативы, общий объем пространства подкачки должен быть показан в выходных данных команды **free**.
7. Запустите команду **blkid**, чтобы получить **UUID** новых томов, которые нужно установить в **/etc/fstab**. Тип файловой системы должен быть указан как **swap** в файле **/etc/fstab**. Вот пример:

   UUID=a110ef54-caed-42b2-a5bb-e3086792d168 swap swap defaults 0 0

8. Следующая команда показывает один метод для выполнения этой задачи:

   # grep -rl redhat /etc/* >/root/etc-redhat.txt 2>/dev/null

   Другой метод указан ниже:

   # find /etc -type f -exec grep -l redhat {} \; >/root/etc-redhat.txt 2>/dev/null

9. Новые локальные пользователи должны быть перечислены в **/etc/passwd** и **/etc/shadow**. Чтобы специально запретить обычным пользователям доступ к каталогу, проще всего использовать **ACL**. Вы должны быть в состоянии подтвердить, что пользователи Билл и Ричард не имеют доступа к каталогу **/cooks** с помощью команды **getfacl /cooks**. Попробуйте создать файл как пользовательский счет или ричард с помощью сенсорной команды.

   # getfacl /cooks
   getfacl: removing leading '/' from absolute path names
   # file: cooks
   # owner: root
   # group: root
   user::rwx
   user:bill:---
   user:richard:---
   group::r-x
   mask::rwx
   other::rwx

10. Для подтверждения вы сможете вставить DVD-диск в соответствующий привод. (В качестве альтернативы вы можете настроить файл ISO на виртуальной машине.) Затем, когда вы запустите команду **ls /misc/dvd**, автомонтировщик смонтирует DVD и предоставит информацию о файле на этом диске. Это должна быть простая конфигурация, основанная на небольшом изменении файла по умолчанию **/etc/auto.misc**. Если вы не уверены, ознакомьтесь с **главой 6**, Цель **сертификации 6.06**. Конечно, вам нужно убедиться, что служба **autofs** запускается после перезагрузки, что может быть подтверждено командой **systemctl is-enabled autofs**.

11. Когда устанавливаются новые ядра, они должны включать новый раздел в файл конфигурации загрузчика, **/boot/grub2/grub.conf**. Раздел по умолчанию основан на директиве **save_entry** в файле **/boot/grub2/grubenv**; просто помни, **save_entry=0** указывает на первый раздел, **save_entry=1** указывает на второй раздел, и так далее. Используйте команду **grub2-set-default** для загрузки другого ядра по умолчанию.
12. Цели по умолчанию настраиваются с помощью команды **systemctl set-default**.
13. Отредактируйте файл **/etc/ntp.conf**. Директива сервера в этом файле должна указывать на желаемую систему (в данном случае, на физический хост). Конечно, проверка в этой системе с помощью команды **ntpq -p** не будет работать, если физический хост не настроен как **NTP-сервер**. В реальной конфигурации этот второй хост будет настоящим **NTP-сервером**. Еще раз, вам нужно убедиться, что служба **ntpd** запускается после перезагрузки, что можно подтвердить командой **systemctl is-enabled ntpd**.
14. Чтобы убедиться, что **SELinux** установлен в разрешающий режим, выполните команду **sestatus**.

Приложение D
Образец экзамена 3:
Образец экзамена RHCE 1

Следующие вопросы помогут оценить ваше понимание материалов, представленных в этой книге. Как уже говорилось во введении, вы должны быть готовы к сдаче экзамена RHCE за 3,5 часа.

Как и RHCSA, экзамен RHCE является «закрытой книгой». Однако вам разрешается использовать любую документацию, которую можно найти на компьютере Red Hat Enterprise Linux. Хотя средства тестирования позволяют вам делать заметки, вы не сможете получать эти заметки из комнаты тестирования.

Хотя экзамен RHCE полностью отделен от экзамена RHCSA, вам необходимо сдать оба экзамена для получения сертификата RHCE. Тем не менее, вы можете сначала сдать экзамен RHCE. Хотя оба экзамена охватывают одни и те же услуги, цели этих служб различны.

В большинстве случаев не существует единого решения, единого метода решения проблемы или установки службы. В Linux существует почти бесконечное количество вариантов, поэтому мы не можем охватить все возможные сценарии.

Даже для этих упражнений не используйте производственный компьютер. Небольшая ошибка в некоторых или во всех этих упражнениях может привести к невозможности загрузки Linux. Если вы не можете выполнить действия, описанные в этих упражнениях, вам может потребоваться переустановить Red Hat Enterprise Linux. Сохранение любых данных, которые вы имеете в локальной системе, может оказаться невозможным.

Red Hat представляет свои экзамены в электронном виде. По этой причине экзамены в этой книге доступны на сопутствующем DVD в подкаталоге **Exams/**. Этот экзамен находится в файле с именем RHCEsampleexam1 и доступен в форматах .txt, .doc и .html. Для получения подробной информации о том, как настроить RHEL 7 в качестве системы, подходящей для практического экзамена, см. Приложение A. Обязательно настройте репозиторий, настроенный в главе 1, лабораторная работа 2.

Не переворачивайте страницу, пока не закончите с пробным экзаменом!

RHCE Образец Экзамен 1

Начните с предварительно сконфигурированной системы **RHEL 7,** описанной в **Приложении A**. Убедитесь, что система в данный момент выключена. Как описано в **Приложении A**, текущий репозиторий установочного DVD-диска доступен с **FTP-сервера**, настроенного в локальной системе. **SELinux** должен быть установлен в режим **enforcing**. У вас будет три с половиной часа для выполнения следующих задач:

1. Настройте **SSH-сервер** на **server1.example.com** с ограниченным доступом к хостам в сети **192.168.122.0/24**. Создайте локальных пользователей с именем **katie** и **dickens**. Ограничьте доступ по **SSH** на сервере только пользователю **katie**.
2. Настройте сервер **Samba**. Поделитесь каталогом с именем **/food** с пользователем **dickens**. Общий доступ ко второму каталогу с именем **/book** разрешен только пользователям **tim** и **stephanie**.

3. Настройте локальный **NTP-сервер**, доступный для локальной сети.
4. Настройте **NFS-сервер на server1.example.com** для совместного использования каталога **/home** в режиме чтения-записи с физической хост-системой.
5. Настройте **Apache** на **server1.example.com** с двумя защищенными виртуальными хостами. Позвоните этим виртуальным хостам **shost1.example.com** и **shost2.example.com**. Создайте и настройте соответствующий **самозаверяющий сертификат SSL** для этих сайтов. Установите две веб-страницы по умолчанию с содержимым **shost1** и **shost2** соответственно.
6. Заблокируйте доступ к **веб-серверу Apache**, работающему на сервере **server1**, с сайта **outsider1.example.net**. Все остальные хосты должны иметь возможность подключаться к веб-серверу.
7. Создайте сценарий с именем **/usr/local/bin/backup.sh**, который принимает каталог в качестве аргумента и создает резервные копии всех файлов в этом каталоге в архиве **tar -gzip** в текущем каталоге. Если аргумент не указан, сценарий должен отобразить следующее сообщение об ошибке:

   Usage: backup.sh <DIRECTORY>

   Сконфигурируйте сценарий для **автоматического запуска в 2:00 каждый день**, чтобы создать резервную копию каталога **/home** в файловой системе **/tmp**.
8. Настройте пересылку **IPv4** и **IPv6 на server1.example.com**.
9. Настройте IPv6-адрес **2001:db8:1::1/64** на интерфейсе **eth0 server1.example.com** и **2001:db8:1::2/64** на интерфейсе **eth0 tester1.example.com**. Убедитесь, что две системы могут «пинговать» друг друга.
10. Настройте цель (**target**) **iSCSI** на **server1.example.com**. Создайте логический том объемом **500 МБ**, который будет использоваться в качестве резервного хранилища для нового **LUN** с **IQN iqn.2015-01.com.example:server1-lun1**. Установите **ACL** для предоставления доступа только к **tester1.example.com**.
11. Настройте **tester1.example.com** в качестве инициатора **iSCSI** с **IQN iqn.2015-01.com.example:tester1**. Найдите и смонтируйте **LUN** на **сервере server1.example.com** и создайте раздел с файловой системой **XFS**. Убедитесь, что том смонтирован при загрузке в каталоге **/mnt/iscsi**.
12. Настройте отчеты о работе системы, чтобы запускать соответствующий инструмент учета каждую минуту.
13. Настройте базу данных **MariaDB** под названием «**exam**» в **MariaDB**. Создайте таблицу с именем «**marks**», в которой в качестве первичного ключа используется столбец с целочисленным идентификатором, а в столбцах «**name**», «**date**» и «**mark**». Используйте соответствующее значение типа для каждого столбца. Вставьте следующие записи в таблицу:

    tim, 2015-03-21, 70
    alex, 2015-07-05, 60
    mike, 2015-04-25, 85

14. Добавьте пользователя **MariaDB** с именем **examuser** с паролем **pass123**. Пользователь **examuser** должен иметь полный доступ к базе данных **exam**. Установите пароль пользователя **root MariaDB pass456**. Убедитесь, что **MariaDB** принимает соединения только с локального хоста.

Образец экзамена RHCE 1 Обсуждение

В этом обсуждении мы опишем один из способов проверки вашей работы на соответствие требованиям, перечисленным для экзамена **RHCE образца 1**. Поскольку нет единого способа настроить конфигурацию **Red Hat Enterprise Linux**, нет единого правильного ответа на перечисленные требования. Тем не менее, есть некоторые общие вещи, которые нужно помнить. Вы должны убедиться, что ваши изменения работают после перезагрузки. Для **RHCE** вам необходимо убедиться, что настроенные вами сервисы настроены на автоматический запуск при загрузке.

1. Первое задание должно быть простым. Пользователи **Кэти** и **Диккенс** должны иметь учетные записи на **сервере SSH**. Хотя можно ограничить доступ пользователей к **SSH** через **TCP Wrappers**, самый простой способ сделать это - следующая директива в основном файле конфигурации сервера **SSH**:

AllowUsers katie

Конечно, «попробовать пудинг на вкус» является возможность для пользователя **katie** войти в систему из удаленной системы в локальной сети и для пользователя **dickens**, которому будет отказано в таком доступе. Кроме того, ограниченный доступ к локальной сети требует соответствующего ограничения с помощью правила межсетевого экрана на основе зоны или соответствующей строки в файлах конфигурации **TCP Wrappers, /etc/hosts.allow** и **/etc/hosts.deny.**

2. Сервер **Samba** будет настроен с двумя разными общими каталогами. Систему можно настроить с помощью логического значения **SELinux samba_export_all_rw** или, в качестве альтернативы, каталоги должны быть установлены с меткой типа **samba_share_t**. Кроме того, самый простой способ ограничить доступ для данных пользователей - с помощью директивы **allow users** в файле конфигурации **smb.conf** в соответствующих разделах. Данные пользователи должны существовать в отдельной базе паролей **Samba**. Конечно, успех основан на способности пользователей Диккенса, Тима и Стефани получать доступ к указанным каталогам из удаленной системы.
3. **NTP-серверы** ограничены локальной системой по умолчанию. Расширение доступа к локальной сети требует изменения файла **/etc/ntp.conf** в директиве **restrict**, а также соответствующих открытых портов в брандмауэре. Вы можете проверить соединение удаленно с помощью команды **ntpdate *ntpserver***. (Конечно, вы можете заменить IP-адрес именем хоста NTP-сервера.) Помните, что **NTP** связывается через **UDP-порт 123**.
4. Хотя доступны и другие методы, вы можете ограничить доступ в основном файле конфигурации NFS (**/etc/exports**) для одного хоста с помощью следующей директивы:

   /home maui.example.com(rw)

   Вам следует заменить имя хоста или IP-адрес вашей экзаменационной системы. Кроме того, вы можете столкнуться с различными требованиями, такими как доступ только для чтения (**ro**), отсутствие корневого доступа (**root_squash**) и другие. Доступ должен быть подтвержден из физической хост-системы путем монтирования общего каталога **NFS**.
5. Самый простой способ настройки защищенного виртуального веб-сайта - с помощью стандартной конфигурации, определенной в файле **ssl.conf** в каталоге **/etc/httpd/conf.d**. В случае успеха вы сможете получить доступ к защищенным веб-сайтам **https:// shost1.example.com** и **https://shost2.example.com**. Поскольку эти сертификаты выданы не официальным органом, вас не должно беспокоить сообщение «**неверный сертификат безопасности**», которое появляется в браузере, при условии, что в сообщении указаны имена ключей **SSL**.
6. Добавьте службу https в зону по умолчанию на локальном межсетевом экране сервера **.example.com**. Чтобы ограничить **HTTP-доступ от outstider1.example.net**, вы можете установить расширенное правило (**rich rule**). Также можно добавить **IP-адрес outsider1** в зону **drop** на брандмауэре. Перед тестированием убедитесь, что разрешение **DNS** для имен хостов **shost1.example.com** и **shost2.example.com** работают, добавляя IP и записи хоста в файлы **/etc/hosts** каждой машины.
7. Типичным местом для ежедневной работы **cron** является каталог **/etc/cron.d**. Сценарий **backup.sh** должен запускаться из локального каталога, в котором необходимо сохранить файлы резервных копий. Следовательно, вы должны перейти в каталог **/tmp** перед запуском скрипта. Строка **cron** должна выглядеть так:

   0 2 * * * root (cd /tmp; /usr/local/bin/backup.sh /home)

8. Чтобы настроить **переадресацию IP** для **адресации IPv4 и IPv6**, вам необходимо добавить следующие директивы в **/etc/sysctl.conf**:

   net.ipv4.ip_forward=1
   net.ipv6.conf.all.forwarding=1

9. Успешное выполнение этой задачи можно проверить, выполнив команду «**ping**» двух IPv6-адресов от двух хостов с помощью команд **ping6 2001:db8:1::1/64** и **ping6 2001:db8:1::2/64**.
10. Используйте оболочку **targetcli** для настройки **target iSCSI**. По завершению, команда **targetcli ls**

должна отображать все необходимые параметры конфигурации. Просмотрите Главу 13, цель сертификации 13.06, для получения дополнительной информации о том, как использовать оболочку **targetcli**.

11. На клиенте выполните команду **iscsiadm** в режиме базы данных обнаружения, чтобы увидеть удаленную цель. Если цели не отображаются, просмотрите конфигурацию, включая список доступа **iSCSI**, имена **IQN** и правила брандмауэра. Убедитесь, что службы **iscsi** и **target** работают на клиентском компьютере и сервере хранения соответственно. Если фаза обнаружения прошла успешно, войдите в систему и создайте файловую систему. Вам потребуется запись в **/etc/fstab** для автоматического монтирования тома при загрузке.
12. Период времени по умолчанию, когда запускается инструмент системного учета, составляет 10 минут, как показано в файле **/etc/cron.d/sysstat** по умолчанию. Это легко изменить на одну минуту в указанном файле.
13. Подключитесь с помощью команды **mysql -u root** к базе данных и введите следующие команды:

    USE exam;
    SELECT * from mark;

    Запрос **SELECT** должен вернуть три записи, перечисленные в упражнении.

14. В случае успеха вы сможете войти в базу данных **MariaDB**, выполнив **mysql -u examuser -p** и введите **pass123**. Пользователь должен иметь полный доступ к базе данных экзамена, которую можно подтвердить с помощью команды **SHOW GRANTS**. Пользователь **root** не должен иметь доступ к **MariaDB** без пароля. Вы можете подтвердить, что это так с командой **root mysql -u**.

Приложение E
Образец экзамена 4:
RHCE Образец экзамена 2

Следующие вопросы помогут оценить ваше понимание материалов, представленных в этой книге. Как уже говорилось во введении, вы должны быть готовы к сдаче экзамена RHCE за 3,5 часа.

Как и RHCSA, экзамен RHCE является «закрытой книгой». Однако вам разрешается использовать любую документацию, которую можно найти на компьютере Red Hat Enterprise Linux. Хотя средства тестирования позволяют вам делать заметки, вы не сможете получать эти заметки из комнаты тестирования.

Хотя экзамен RHCE полностью отделен от экзамена RHCSA, вам необходимо сдать оба экзамена для получения сертификата RHCE. Тем не менее, вы можете сначала сдать экзамен RHCE. Хотя оба экзамена охватывают одни и те же услуги, цели этих служб различны.

В большинстве случаев не существует единого решения, единого метода решения проблемы или установки службы. В Linux существует почти бесконечное количество вариантов, поэтому мы не можем охватить все возможные сценарии.

Даже для этих упражнений не используйте производственный компьютер. Небольшая ошибка в некоторых или во всех этих упражнениях может привести к невозможности загрузки Linux. Если вы не можете выполнить действия, описанные в этих упражнениях, вам может потребоваться переустановить Red Hat Enterprise Linux. Сохранение любых данных, которые вы имеете в локальной системе, может оказаться невозможным.

Red Hat представляет свои экзамены в электронном виде. По этой причине экзамены в этой книге доступны на сопутствующем DVD в подкаталоге Exams/. Этот экзамен находится в файле с именем RHCEsampleexam1 и доступен в форматах .txt, .doc и .html. Для получения подробной информации о том, как настроить RHEL 7 в качестве системы, подходящей для практического экзамена, см. Приложение A. Обязательно настройте репозиторий, настроенный в главе 1, лабораторная работа 2.

Не переворачивайте страницу, пока не закончите с пробным экзаменом!

RHCE Образец экзамена 2

Начните с предварительно сконфигурированной системы **RHEL 7**, описанной в **Приложении A**. Убедитесь, что система в данный момент выключена. Как описано в **Приложении A**, текущий репозиторий установочного DVD-диска доступен с **FTP-сервера**, настроенного в локальной системе. **SELinux** должен быть установлен в **режим enforcing**. У вас будет три с половиной часа для выполнения следующих задач:

1. [В качестве предварительного условия выполните **упражнение 12-5** на своей физической системе.] Настройте систему **server1.example.com** для аутентификации на **Kerberos KDC**, работающем на физической хост-системе. Область (**realm**) должна быть установлена в **EXAMPLE.COM**.
2. Настройте сервер **NFS** для совместного использования каталога **/nfsshare** для чтения и записи с **tester1.example.com**. Безопасно экспортируйте том с помощью аутентификации **Kerberos**, целостности связи и шифрования.
3. Настройте клиент **tester1.example.com** для автоматического монтирования тома **server1.example.com:/nfsshare** в точке монтирования **/mnt/nfs**.
4. Настройте **веб-сервер Apache** с двумя обычными виртуальными хостами. Установите его по **URL-адресам test1.example.com** и **test2.example.com**. Для этого создайте и используйте подкаталог **/web**. Включите соответствующие файлы **index.html** с содержимым для каждого **URL**.
5. Настройте общий подкаталог с именем **cubs** на **веб-сервере Apache test1.example.com**, доступный для пользователей **elizabeth** и **fred** с базовой аутентификацией **HTTP**. Ограничить доступ к локальной сети **192.168.122.0/24**.
6. Настройте скрипт **CGI**, доступный в системе **test1.example.com**. Для этой цели вы можете использовать следующий код в соответствующем скрипте **CGI**. Назовите это файлом **good.pl**.

   ```
   #!/usr/bin/perl
   print "Content-type: text/html\n\n";
   print "Good Job!\n";
   ```

7. Настройте **DNS-сервер** только для кэширования, который перенаправляет запросы в физическую хост-систему.
8. Настройте локальный **SMTP-сервер** в качестве **null** клиента, который перенаправляет все электронные письма на физическую хост-систему.
9. Настройте **SSH-сервер** для пользователя **mike** в системе **server1.example.com**. Сконфигурируйте аутентификацию на основе ключей из удаленной системы - либо **tester1.example.com**, либо с физического хоста. Используйте следующую кодовую фразу:

   Linux rocks, Windows does not

10. Настройте маскарадинг (**masquerading**) в физической системе хоста из сети **192.168.122.0/24** в сети **192.168.100.0/24**.
11. Выключите виртуальную машину и добавьте сетевой адаптер. Выберите модель устройства **virtio**. Настройте агрегирование каналов (используя драйвер **teaming** или **bonding**) в режиме циклического перебора.
12. Настройте сервер **Samba** для совместного использования домашних каталогов пользователей.
13. Настройте два **NTP-сервера**, настроенных как одноранговые.
14. Настройте систему **server1**, чтобы она не отвечала на команду **ping**.

RHCE Образец экзамена 2 Обсуждение

В этом обсуждении мы опишем один из способов проверки вашей работы на соответствие требованиям, указанным для образца 2 экзамена RHCE. Поскольку нет единого способа настроить конфигурацию Red Hat Enterprise Linux, нет единого правильного ответа на перечисленные требования. Тем не менее, есть некоторые общие вещи, которые нужно помнить. Вы должны убедиться, что ваши изменения работают после перезагрузки. Для RHCE вам необходимо убедиться, что настроенные вами сервисы настроены на автоматический запуск при загрузке.

1. Эта задача по существу идентична упражнениям **12-5** и **12-6**. Чтобы проверить конфигурацию, убедитесь, что субъекты **Kerberos** существуют на **KDC** для каждого пользователя. После того,

как вы откроете сеанс **SSH** на сервере **server1**, команда **klist** должна подтвердить, что **TGT** предоставлен. В случае возникновения проблем просмотрите конфигурацию. Исходя из этого, клиент должен включить следующие директивы в **/etc/krb5.conf**:

default_realm = EXAMPLE.COM

Кроме того, в директивах **ketc** и **admin_server** в файле **/etc/krb5.con** должно быть указано полное доменное имя физической системы хоста.

2. Первая часть этой задачи требует следующей строки конфигурации в **/etc/exports**:

/nfsshare tester1.example.com(rw)

Настройка общего ресурса **NFS**, защищенного с помощью **Kerberos**, описана в упражнениях **16-2** и **16-3**. Убедитесь, что вы создали и установили **Kerberos** хост и принципалы обслуживания для всех ваших машин. На сервере должны быть запущены службы **nfs-server** и **nfs-secure-server**. Общий ресурс **NFS** должен быть экспортирован с параметром **sec=krb5p**.

3. Это упражнение является продолжением предыдущего задания. Если клиент может автоматически смонтировать общий ресурс **NFS** при загрузке с параметром **sec=krb5p**, вы успешно выполнили эту задачу. Если у вас возникнут какие-либо проблемы, убедитесь, что на клиенте включена служба **nfs-secure**, и просмотрите правила брандмауэра. Запустите команду **mount** в подробном режиме **(-v)** и проанализируйте выходные данные и журналы на наличие сообщений об ошибках.
4. В случае успеха вы должны увидеть содержимое отмеченных файлов **index.html** для каждого **веб-сайта**. Вам также следует изменить контекст **SELinux** по умолчанию для каталога **/web**, чтобы он соответствовал контексту **/var/www/html**. Просмотрите **Главу 14**, **Цель сертификации 14.04**, для получения дополнительной информации о безопасных виртуальных хостах.
5. Если вы добьетесь успеха, пользователи **elizabeth** и **fred**, и никто другой, будут иметь доступ к подкаталогу **cubs** главного каталога. Оба пользователя будут иметь доступ только из систем локальной сети. Если ваша конфигурация не работает должным образом, проверьте настройки. У вас должен быть блочный контейнер **<Directory>** для подкаталога **cubs** в файлах конфигурации **Apache**, с **AuthType Basic** и требуемыми пользовательскиим директивами. Вам также понадобится строка **AuthUserFile,** указывающая на файл пароля. Вы можете ограничить доступ к локальной сети с помощью директивы **Allow from.**
6. Приложение CGI должно быть доступно по следующему URL:

http://test1.example.com/cgi-bin/good.pl

Когда вы переходите по этому URL, браузер должен напечатать строку **«Good Job!»**

7. Если вы используете **BIND**, файл конфигурации **named.conf** по умолчанию сам по себе достаточно для кэширующего **DNS-сервера**. К этому файлу вам нужно добавить директиву **forwarders** с **IP-адресом** физической хост-системы, которая предположительно имеет **DNS-сервер.**
8. Сконфигурируйте **Postfix** и просмотрите свою конфигурацию с помощью команды **postconf -n**. Как минимум, вам необходимо настроить директивы **myorigin, mydestination, local_transport** и **relayhost**. Протестируйте конфигурацию с помощью почтового клиента, такого как **Mutt**. Сервер должен принимать электронные письма только из локальной системы и доставлять их на ваш физический хост. Проверьте в **/var/log/maillog**, что это так.
9. Когда пользователь **mike** пытается подключиться с данного клиента, система должна запросить и принять парольную фразу, определенную в вопросе об экзамене: **Linux rocks, Windows does not**. (Обратите внимание, что парольная фраза включает запятую и точку.) Аутентификация на основе ключей **SSH** является обязательным требованием для экзаменов **RHCSA** и **RHCE** и была рассмотрена в **главе 4, Цель сертификации 4.04.**
10. Когда маскарадинг (**masquerading**) настроен, подключения от внутренних систем в сети **192.168.122.0/24**, таких как **server1.example.com** к **outsider1.example.net**, выглядят так, как если бы они исходили от физической хост-системы. Это может быть подтверждено попыткой соединения **SSH** и просмотром сообщений журнала в **/var/log/secure**.
11. Если конфигурация работает, у вас все равно должна быть возможность подключения по IP после отключения одного из интерфейсов с помощью команды **ifdown**. Убедитесь, что режим

циклического перебора (**round-robin**) используя команду **cat /proc/net/bonding/bond0** (если вы настроили **bonding**) или командой **teamdctl team state** (если вы настроили **teaming**). Для получения дополнительной информации о взаимодействии и связывании интерфейса см. **Главу 12, Цель сертификации 12.06.**

12. Пользователи с учетной записью на сервере **Samba** должны иметь возможность подключаться к своим домашним каталогам на этом сервере. Однако файлы в этом каталоге не будут доступны, если не активирован логический (**boolean**) параметр **samba_enable_home_dirs**.
13. Одноранговые узлы на **NTP-сервере** можно включить в файле **/etc/ntp.conf** вместо директивы сервера. Просто помните, что **NTP** связывается через **UDP-порт 123**. Один из способов проверить, открыт ли **UDP-порт 123**, с помощью следующей команды: **nmap -sU server1 -p 123**.
14. Чтобы избежать ответа на команду **ping**, которая работает через **IPv4**, опция **icmp_echo_ignore_all** должна быть активной. Вы можете установить это навсегда в **/etc/sysctl.conf** файл директивой **net.ipv4.icmp_echo_ignore_all = 1**.

Приложение F
О DVD

DVD-ROM, включенный в эту книгу, поставляется с файлами лабораторных работ, как описано в каждой главе, а также включает в себя цифровую копию книги. Чтобы получить доступ к лабораторным файлам и электронной книге, вставьте **DVD**. Если вы не используете графический интерфейс, в котором включена функция автоматического монтирования, вам нужно будет смонтировать **DVD** с помощью следующей команды:

 # mount /dev/cdrom/media

Системные Требования

Электронная книга требует либо **Adobe Reader**, либо эквивалентного **Linux PDF reader**, такого как **Evince**. Как обсуждалось в **главе 1, экзамен RHCSA** включает **KVM**, который **Red Hat поддерживает только в 64-битных системах.**