

Глава 8

Администрирование пользователей

ЦЕЛИ СЕРТИФИКАЦИИ

8.01 Управление учетной записью пользователя

8.02 Административный контроль

8.03 Конфигурация пользователя и оболочки

8.04 Пользователи и сетевая аутентификация

8.05 Специальные группы

✓ Двухминутная тренировка

Q & A Самопроверка

Основой администрирования Linux является управление пользователями и группами. В этой главе вы изучите различные способы управления различными пользователями и группами, доступными для Linux. Важные навыки в этой области варьируются от простого входа в систему до управления учетными записями пользователей, членства в группах, совместной работы в группах и сетевой аутентификации. Настройка административных привилегий для пользователей Linux может помочь главному администратору распределить обязанности.

Вы увидите, как управлять этими задачами из командной строки, с помощью файлов набора теневого паролей. Для настройки некоторых из этих задач вы также будете использовать такие инструменты, как Диспетчер пользователей и Инструмент настройки аутентификации. Как и следовало ожидать, инструменты Red Hat GUI не могут сделать все это, что подчеркивает важность понимания управления пользователями из командной строки.

ВНУТРИ экзамена

Внутри экзамена

В этой главе рассматриваются несколько целей RHCSA. Вкратце, эти цели включают следующее:

- Вход и переключение пользователей в многопользовательских целях

Вкратце, это означает, что вам нужно знать, как войти в систему с обычными учетными записями, когда RHEL 7 работает в многопользовательских или графических целях. Чтобы переключать пользователей, вам нужно знать, как выйти из системы и войти в нее с помощью второй учетной записи. Достаточно просто.

- Создание, удаление и изменение учетных записей локальных пользователей.
- Смена паролей и настройка устаревания паролей для локальных учетных записей пользователей.

- Создавать, удалять и изменять локальные группы и членство в группах

Вы можете использовать такие команды, как **useradd**, **usermod**, **groupadd**, **groupmod** и **chage**, а также **User Manager** для выполнения этих задач. Хотя в этой главе объясняется, как вы можете использовать оба типа инструментов, нет никакой гарантии, что Менеджер пользователя будет доступен во время экзамена.

- Создание и настройка каталогов set-GID для совместной работы

Когда был доступен экзамен RHCT, связанной задачей было «Настроить разрешения файловой системы для совместной работы». Другими словами, цель теперь более конкретна - вам рассказывают, как настроить один или несколько каталогов для совместной работы между группой пользователей.

- Сконфигурируйте систему для использования существующей службы аутентификации для информации о пользователях и группах

В предыдущей версии экзамена RHCSA для RHEL 6 эта цель была ограничена «Присоединить систему к централизованному серверу **LDAP**». Теперь область действия задачи шире и может включать в себя любую услугу, такую как **Kerberos**, **Microsoft Active Directory** или сервер идентификации, политики и аудита (**IPA**).

ЦЕЛЬ СЕРТИФИКАЦИИ 8.01

Управление учетной записью пользователя

Вам нужно знать, как создавать и настраивать пользователей. Это означает, что вы должны знать, как настраивать и изменять учетные записи, работать с паролями и организовывать пользователей в группы. Вам также необходимо знать, как настроить среду, связанную с каждой учетной записью пользователя: в файлах конфигурации и в пользовательских настройках.

Если вы установили RHEL 7 с помощью **Kickstart** или в текстовом режиме или иным образом избежали процесса **Firstboot**, описанного в главе 1, установка Red Hat по умолчанию включает в себя только одну учетную запись для входа в систему: **root**. Хотя другие учетные записи не требуются, важно настроить некоторые обычные учетные записи пользователей. Даже если вы собираетесь быть единственным пользователем в системе, создайте хотя бы одну неадминистративную учетную запись для повседневной работы. Тогда вы можете использовать учетную запись **root** только тогда, когда это необходимо для администрирования системы. Вы можете добавлять учетные записи в системы Red Hat Enterprise Linux, используя различные утилиты, включая прямое редактирование пароля. файлы конфигурации (ручной метод), команда **useradd** (метод командной строки) и утилита **User Manager** (графический метод).

Разные виды пользователей

Существует три основных типа учетных записей пользователей Linux: административные (**root**), обычные и служебные. Административная корневая учетная запись автоматически создается при установке Linux и имеет административные привилегии для всех служб в системе Linux. Хакер «черной шляпы», у которого есть шанс получить контроль над этой учетной записью, может получить полный контроль над этой системой.

Для случаев, когда вы входите в систему как администратор, RHEL внедряет меры безопасности для пользователей **root**. Войдите в систему как пользователь **root**, а затем выполните команду **alias**. Вы увидите следующие записи:

alias rm='rm -i'

Из-за этого конкретного псевдонима, когда пользователь **root** запускает команду **rm**, оболочка фактически выполняет команду **rm -i**, которая запрашивает подтверждение, прежде чем команда **rm** удалит файл. К сожалению, такая команда, как **rm -rf directoryname**, заменяет этот параметр безопасности.

Обычные пользователи имеют необходимые привилегии для выполнения стандартных задач на компьютере с Linux. Они могут получать доступ к таким программам, как текстовые процессоры, базы данных и веб-браузеры. Они могут хранить файлы в своих домашних каталогах. Поскольку обычные пользователи обычно не имеют прав администратора, они не могут случайно удалить важные файлы конфигурации операционной системы. Вы можете назначить обычную учетную запись большинству пользователей, будучи уверенными в том, что они не могут нарушить работу системы с привилегиями, которые они имеют для этой учетной записи.

Такие службы, как Apache, Squid, почта и печать, имеют свои собственные индивидуальные учетные записи. Эти учетные записи существуют, чтобы позволить каждому из этих сервисов взаимодействовать с системами Linux. Обычно вам не нужно менять какую-либо учетную запись службы, но если вы видите, что кто-то использует оболочку Bash через одну из этих учетных записей, будьте осторожны. Кто-то может ворваться в вашу систему.

!!!!

Чтобы просмотреть последние логины, запустите *last* / *less* команды. Если имя входа из удаленного местоположения, оно будет связано с определенным IP-адресом вне вашей сети.

!!!!

The Shadow Password Suite(Набор Теневых Паролей)

Когда Unix был впервые разработан в 1970-х годах, безопасность не была серьезной проблемой. Все необходимое для управления пользователями и группами содержится в файлах **/etc/passwd** и **/etc/group**. Как следует из названия, пароли изначально были в файле **/etc/passwd**. Проблема в том, что файл «доступен для чтения всем». Любой, у кого есть копия этого файла до набора теневых паролей, будет иметь копию пароля для каждого пользователя. Даже пароли, которые зашифрованы в этом файле, в конечном итоге могут быть расшифрованы. Именно это и послужило причиной разработки набора теневых паролей, в котором более конфиденциальная информация была перемещена в другие файлы, которые могут прочитать только пользователи с правами администратора.

Четырьмя файлами набора теневых паролей являются **/etc/passwd**, **/etc/group**, **/etc/shadow** и **/etc/gshadow**. Значения по умолчанию в этих файлах определяются файлом **/etc/login.defs**.

Файл **/etc/passwd**

Файл **/etc/passwd** содержит основную информацию о каждом пользователе. Откройте этот файл в текстовом редакторе и немного поищите. В верхней части файла находится основная информация для пользователя **root**. Другие пользователи в этом файле могут относиться к таким службам, как **mail**, **ftp** и **sshd**. Они могут быть конкретными пользователями, предназначенными для входа в систему.

В файле **/etc/passwd** есть семь столбцов информации, обозначенных двоеточиями. Каждый столбец в **/etc/passwd** содержит конкретную информацию, описанную в **таблице 8-1**.

Версия **/etc/passwd** для RHEL 7 включает более безопасные функции для учетных записей пользователей по сравнению с некоторыми другими дистрибутивами Linux. Единственные учетные записи с реальной оболочкой входа - это учетные записи пользователей. Если хакер «черной шляпы» каким-то образом взломает учетную запись службы, такую как почта или nobody, с помощью оболочки **ложный /sbin/nologin**, этот пользователь не получит автоматически доступ к командной строке.

ТАБЛИЦА 8-1 описание /etc/passwd

Поле	Пример	Назначение
Username	mj	Пользователь входит в систему с этим именем. Имена пользователей могут включать цифры, дефисы (-), точки (.) И подчеркивания (_). Однако они не должны начинаться с дефиса или быть длиннее 32 символов.
Password	x	Пароль. Вы должны увидеть либо x(икс) , либо звездочку (*) , либо случайную группу букв и цифр. X указывает на /etc/shadow для действительного пароля. Звездочка означает, что учетная запись отключена. Случайная группа букв и цифр представляет зашифрованный пароль.
User ID	1000	Уникальный числовой идентификатор пользователя (UID) для этого пользователя. По умолчанию Red Hat начинает идентификаторы пользователей с 1000.
Group ID	1000	Основной идентификатор группы (GID), связанный с этим пользователем. По умолчанию RHEL создает новую группу для каждого нового пользователя, и номер соответствует UID , если соответствующий GID доступен. Некоторые другие системы Linux и Unix назначают всех пользователей в группу пользователей по умолчанию.
User info	Michal Jang	Вы можете ввести любую информацию по вашему выбору в этом поле. Стандартные параметры включают полное имя пользователя, номер телефона, адрес электронной почты и физическое местоположение. Вы можете оставить это поле пустым.
Home Directory	/home/mj	По умолчанию RHEL помещает новые домашние каталоги в /home/username .
Login Shell	/bin/bash	По умолчанию RHEL назначает пользователей для оболочки bash . Вы можете изменить это на любую установленную вами легальную оболочку.

Файл /etc/group

Каждый пользователь Linux назначен в группу. По умолчанию в RHEL 7 каждый пользователь получает свою личную группу. Пользователь является единственным членом этой группы, как определено в файле конфигурации **/etc/group**. Откройте этот файл в текстовом редакторе. Просмотрите его. Первая строка в этом Файл определяет информацию для группы пользователей с правами администратора. Некоторые пользователи сервиса включают других пользователей в качестве членов этой группы. Например, пользователь **qemu** является членом группы **kvm**, которая предоставляет сервисы, связанные с привилегиями эмулятора **QEMU** с виртуальной машиной на основе ядра (**KVM**).

В файле **/etc/group** есть четыре столбца информации, обозначенных двоеточиями. Каждый столбец в **/etc/group** указывает информацию, описанную в **таблице 8-2**.

ТАБЛИЦА 8-2 Анатомия **/etc/group**

Поле	Пример	Назначение
Groupname	mj	Каждый пользователь получает свою собственную группу, имя которой совпадает с именем пользователя. Вы также можете создавать уникальные имена групп.
Password	x(Икс)	Пароль. Вы должны увидеть либо x , либо, казалось бы, случайную группу букв и цифр. Символ x указывает на /etc/gshadow для действительного пароля. Случайная группа букв и цифр представляет зашифрованный пароль.
Group ID	1000	Числовой идентификатор группы (GID), связанный с группой. По умолчанию RHEL создает новую группу для каждого нового пользователя. Если вы хотите создать специальную группу, такую как менеджеры, вам следует назначить номер GID вне стандартного диапазона; в противном случае GID и UID Red Hat , вероятно, вышли бы из последовательности.
Group members	Mj,vp,aj	Перечисляет имена пользователей, которые являются членами группы. Если есть имя пользователя, которое перечисляет GID группы в качестве своей основной группы в /etc/passwd , это имя пользователя также является членом группы.

Как показано в **Таблице 8-3**, **/etc/shadow** включает зашифрованный пароль во втором столбце, а остальная информация относится к способу управления паролями. Фактически, первые два символа второго столбца основаны на хэше шифрования для пароля. Если вы видите **\$1**, пароль хэшируется в алгоритме **Message Digest 5 (MD5)**, стандартном для RHEL 5. Если вы видите **\$6**, пароль защищен **512-битным алгоритмом безопасного хэширования (SHA-512)**, стандарт для RHEL 6 и 7.

Таблица 8-3 Анатомия **/etc/shadow**

Колонка	Поле	Описание
1	Username	имя пользователя
2	Password	Зашифрованный пароль; требует x во втором столбце /etc/passwd
3	Password history	Дата последней смены пароля в количестве дней после 1 января 1970 г.
4	mindays	Минимальное количество дней, в течение которых пользователь должен хранить пароль
5	maxdays	Максимальное количество дней, после которых пароль должен быть изменен
6	warndays	Количество дней до истечения срока действия пароля при получении предупреждения
7	inactive	Количество дней после истечения срока действия пароля, в течение которого пароль все еще принимается, но пользователю предлагается изменить свой пароль
8	disabled	Количество дней с 1 января 1970 года, после которого учетная запись отключена

Файл /etc/gshadow

Файл **/etc/gshadow** является файлом конфигурации группы в наборе теневых паролей. Он включает в себя администраторов группы, которые могут добавлять других членов группы с помощью команды **gpasswd**. При желании вы можете даже настроить хешированный пароль. После установки пароля другие пользователи могут стать членами группы с помощью команды **newgrp** и ввода необходимого пароля. **Таблица 8-4** описывает столбцы в **/etc/gshadow** слева направо.

Таблица 8-4 Анатомия **/etc/shadow**

Поле	Пример	Назначение
Groupname	mj	Название группы.
Password	!	У большинства групп есть ! , что означает отсутствие пароля; некоторые группы могут иметь хешированный пароль, аналогичный показанному в файле /etc/shadow .
Administrators	mj	Разделенный запятыми список пользователей, которые входят в группу и могут изменить участников или пароль группы с помощью команды gpasswd .
Group members	vp, ao	Список имен пользователей, являющихся членами группы, через запятую

Файл /etc/login.defs

Файл **/etc/login.defs** предоставляет базовую линию для ряда параметров в наборе теневых паролей. В этом разделе представлен краткий анализ каждой активной директивы в версии этого файла по умолчанию. Как вы увидите, директивы выходят за рамки аутентификации. Первый параметр конфигурации указывает каталог с локальной доставкой электронной почты, перечисленный по имени пользователя:

MAIL_DIR /var/spool/mail

Следующие четыре директивы относятся к информации об устаревании пароля по умолчанию. Директивы объяснены в комментарии к файлу и в **таблице 8-5**.

ТАБЛИЦА 8-5 /etc/login.defs Параметры конфигурации устаревания пароля

Параметр конфигурации	Назначение
PASS_MAX_DAYS	По истечении этого количества дней пароль должен быть изменен.
PASS_MIN_DAYS	Пароли должны храниться не менее этого количества дней.
PASS_MIN_LEN	Длина пароля должна быть не менее этого количества символов.
PASS_WARN_AGE	Пользователи предупреждаются об этом количестве дней до PASS_MAX_DAYS .

Как было предложено ранее, номера идентификаторов пользователей (**UID**) и идентификаторов групп (**GID**) для обычных пользователей и групп начинаются с 1000. Поскольку Linux поддерживает номера **UID** и **GID**, превышающие 4 миллиарда (фактически до 232–1), максимальный **UID** и **GID** числа **60000**, определенные в файле **/etc/login.defs**, могут показаться странными. Тем не менее, он оставляет более высокие номера доступными для других баз данных аутентификации, например, связанных с **LDAP** и **Microsoft Windows** (через

Winbind). Как указано в директивах, **UID_MIN** определяет минимальный **UID**, **UID_MAX** указывает максимальный **UID** и так далее:

UID_MIN 1000
UID_MAX 60000
GID_MIN 1000
GID_MAX 60000

Аналогично, команды **useradd** и **groupadd** с ключом **-r** создают системного пользователя или системную группу соответственно, чей идентификатор выбирается в следующем диапазоне:

SYS_UID_MIN 201
SYS_UID_MAX 999
SYS_GID_MIN 201
SYS_GID_MAX 999

Обычно, когда команда **useradd** запускается для создания нового пользователя, она также автоматически создает домашние каталоги, что подтверждается следующей директивой:

CREATE_HOME yes

Следующая директива имеет решающее значение в реализации схемы «Частная группа пользователей», где новые пользователи также становятся членами своей собственной частной группы, обычно с такими же номерами **UID** и **GID**. Это означает, что когда новые пользователи создаются (или удаляются), соответствующая группа также добавляется (или удаляется):

USERGROUPS_ENAB yes

Наконец, следующая директива определяет алгоритм, используемый для шифрования паролей, обычно **SHA 512** для **RHEL 7**:

ENCRYPT_METHOD SHA512

Различные методы шифрования могут быть установлены с помощью инструмента настройки аутентификации, описанного далее в этой главе.

Инструменты командной строки

Существует два основных способа добавления пользователей через интерфейс командной строки. Вы можете добавлять пользователей напрямую, отредактировав файл **/etc/passwd** в текстовом редакторе, таком как **vi**. С этой целью как **vipw**, так и **vigr** были описаны в главе 3. Кроме того, вы можете использовать текстовые команды, настроенные для этой цели.

Добавить пользователей напрямую

Откройте файл **/etc/passwd** в любом текстовом редакторе. Как описано в главе 3, вы можете сделать это с помощью команды **vipw**. Однако если вы добавляете пользователей путем непосредственного редактирования файлов набора теневого паролей, вам придется сделать еще две вещи:

Добавьте домашний каталог пользователя. Например, для пользователя Донна, вам нужно добавить Домашний каталог **/home/donna**, убедившись, что пользователь **donna** и группа **donna** оба владеют этим каталогом.

Заполните домашний каталог пользователя. Опция по умолчанию - копировать файлы из Каталог **/etc/skel**, обсуждаемый далее в этой главе. Вы также должны убедиться, что пользователь **donna** и группа **donna** являются владельцами этих файлов, скопированными в каталог **/home/donna**.

Добавить пользователей в группу напрямую

Каждый пользователь Linux назначается в группу, по крайней мере, в свою личную группу. Как подразумевается в главе 3, номер **GID**, указанный в файле **/etc/group**, обычно должен совпадать с номером, указанным для этого пользователя в файле **/etc/passwd**.

Пользователь является единственным членом этой группы.

Конечно, пользователи могут быть членами других групп. Например, чтобы создать группу с именем **project**, вы можете добавить записи в файлы **/etc/group** и **/etc/gshadow**. Один из способов сделать это в текстовом редакторе - использовать команду **vigr**. Например, следующая запись может быть подходящей для группы с именем **project**:

project:x:60001:

Используется число 60001, так как оно выходит за пределы директивы **GID_MAX** от Файл **/etc/login.defs**, описанный ранее. Но это просто произвольно. Нет запрета на меньшее число, если оно не мешает существующим **GID**. Однако это удобно, когда номера **UID** и **GID** обычных пользователей совпадают.

Конечно, чтобы группа была полезной, вам нужно добавить пользователей, уже настроенных в файл **/etc/passwd** в конце строки. В следующем примере предполагается, что эти пользователи уже существуют:

project:x:60001:michael,elizabeth,stephanie,tim

Вам также необходимо добавить эту группу в файл **/etc/gshadow**. Вы можете сделать это напрямую с помощью команды **vigr -s**. В качестве альтернативы, чтобы настроить администратора группы с помощью пароля, вы можете запустить команду **gpasswd**. Например, команда проекта **gpasswd** установит пароль для администрирования группы, связанный с командами **newgrp** и **sg**, описанными далее в этой главе. Он автоматически добавит зашифрованный пароль с указанным именем группы в файл **/etc/gshadow**.

Добавить пользователей в командной строке

Кроме того, вы можете автоматизировать этот процесс с помощью команды **useradd**. Команда **useradd pm** добавит пользователя **pm** в файл **/etc/passwd**. Кроме того, команда **useradd** создает домашний каталог **/home/pm**, добавляет стандартные файлы из каталога **/etc/skel** и назначает оболочку по умолчанию **/bin/bash**. Но **useradd** универсален. Он включает в себя ряд параметров команды, как показано в таблице 8-6.

Назначить пароль

После создания нового пользователя вы можете использовать команду **passwd username** для назначения пароля этому пользователю. Например, команда **passwd pm** предлагает вам назначить новый пароль пользователю **pm**. **RHEL** настроен, чтобы избежать паролей, которые основаны на слове, короче восьми символов, слишком простые, основанные на палиндромах, и другие, подобные критерии по соображениям безопасности. Тем не менее,

такие пароли являются законными и принимаются, если команда **passwd** запускается пользователем **root**.

ТАБЛИЦА 8-6 Параметры команды **useradd**

Вариант	Назначение
-u UID	Переопределяет назначенный по умолчанию UID . По умолчанию в RHEL это начинается с 1000 и может продолжаться последовательно до максимального числа пользователей, поддерживаемых ядром 2.6, которое составляет 232–1, что составляет более четырех миллиардов пользователей.
-g GID	Переопределяет назначенный по умолчанию GID . Если доступно, RHEL использует одинаковые номера GID и UID для каждого пользователя. Если вы назначаете GID , он должен быть либо 100 (пользователи), либо уже существовать.
-c info	Введите комментарий по вашему выбору о пользователе, например, его имя.
-d dir	Переопределяет домашний каталог по умолчанию для пользователя, /home/username .
-e ГГГГ-ММ-ДД	Устанавливает срок действия учетной записи пользователя.
-f num	Указывает количество дней после истечения срока действия пароля, когда учетная запись отключена.
-G group1, group	Делает пользователя членом group1 и group2 , основываясь на их текущих именах, определенных в файле /etc/group . Пробел между group1 и group2 может привести к ошибке.
-s shell	Переопределяет оболочку по умолчанию для пользователя, /bin/bash .

Добавить или удалить группу в командной строке

Когда уместно добавить специальную группу в набор теневого пароля, вы можете использовать команду **groupadd**. Как правило, вы хотите использовать его с ключом **-g**. Например, следующая команда создаст специальную группу проектов с **GID 60001**:

```
# groupadd -g 60001 project
```

Если вы не используете ключ **-g**, команда **groupadd** получает следующий доступный номер **GID**. Например, если в системе настроены два постоянных пользователя, каждый из них имеет номера **UID** и **GID 1000** и **1001** соответственно. Если вы запустили команду проекта **groupadd** без указания номера **GID**, группе проекта будет присвоен **GID 1002**. Следующий созданный обычный пользователь получит **UID 1002** и **GID 1003**, что может привести к путанице.

К счастью, команда для удаления группы проще. Если группа проекта завершила свою работу, вы можете удалить эту группу из базы данных набора теневого пароля с помощью следующей команды:

```
# groupdel project
```

Удалить пользователя

Удаление учетной записи пользователя является простым процессом. Самый простой способ удалить учетную запись пользователя с помощью команды **userdel**. По умолчанию эта

команда не удаляет домашний каталог этого пользователя, поэтому администраторы могут передавать файлы от этого пользователя, возможно, сотруднику, который принял на себя задачи удаленного пользователя. Кроме того, команда **userdel -r username** удаляет домашний каталог этого пользователя вместе со всеми файлами, хранящимися в этом домашнем каталоге.

Это намного быстрее, чем метод **GUI**, для которого вы открываете **Red Hat User Manager**, выбираете пользователя и затем нажимаете **Delete**. Хотя менее опытному пользователю, вероятно, легче запомнить метод **GUI**, текстовые команды работают быстрее.

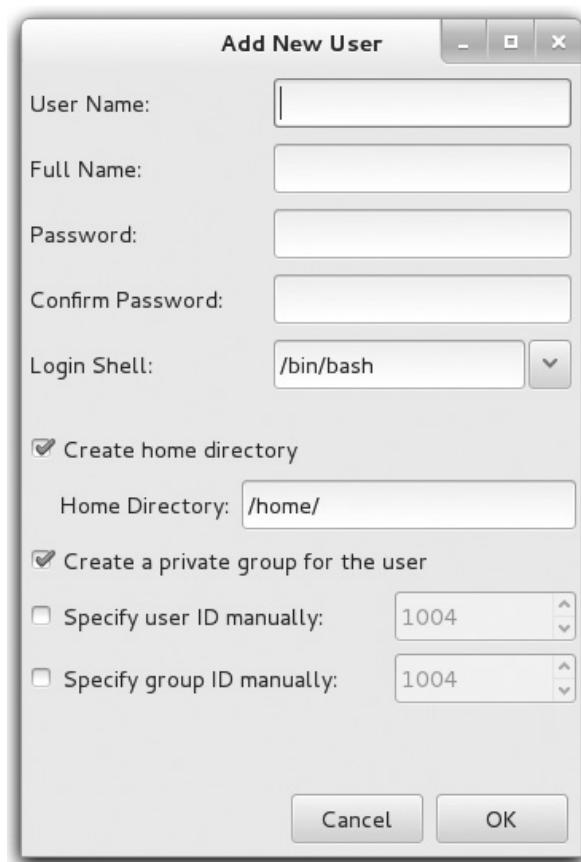
УПРАЖНЕНИЕ 8-1

Добавить пользователя с помощью Red Hat User Manager

Если доступен графический интерфейс, одной из альтернатив команд управления пользователями, таких как **useradd** и **usermod**, является **Red Hat User Manager**. Если возможно, попробуйте открыть его удаленно через соединение **ssh -X**, как описано в главе 2. Например, если вы настроили **server1.example.com**, как описано в предыдущих главах, подключитесь к этой системе из удаленный графический интерфейс с помощью команды **ssh -X root@192.168.122.50**. После входа в систему введите Команду **system-config-users**.

Если команда не выполняется, необходимо до установить пакет управления пользователями и группами, используя **yum**, или графический интерфейс Приложение | Системные | Программы | Управление системой | Графические средства управления | **system-config-users-.....**

1. В диспетчере пользователей Red Hat нажмите кнопку «Добавить пользователя» или выберите «Файл | Добавить пользователя. Откроется окно «Добавить нового пользователя», как показано здесь:



The screenshot shows a window titled "Add New User" with the following fields and options:

- User Name: [text input]
- Full Name: [text input]
- Password: [password input]
- Confirm Password: [password input]
- Login Shell: [dropdown menu showing /bin/bash]
- ☒ Create home directory
- Home Directory: [text input showing /home/]
- ☒ Create a private group for the user
- ☐ Specify user ID manually: [spin box showing 1004]
- ☐ Specify group ID manually: [spin box showing 1004]
- Buttons: Cancel, OK

2. Заполните форму. Все записи обязательны, кроме ФИО. Записи довольно понятны (см. Предыдущие обсуждения каждой области). Пароль должен состоять как минимум из

восьми символов и в идеале должен содержать сочетание прописных и строчных букв, цифр и знаков препинания, чтобы сделать его более защищенным от стандартных программ взлома паролей.

3. Введите идентичный пароль в поле Подтверждение пароля.
4. Запишите номер, связанный с опциями «Указать идентификатор пользователя вручную» и «Указать идентификатор группы вручную»; это номера **UID** и **GID**, которые будут назначены новому пользователю. Нажмите **ОК**, когда вы закончите.
5. Повторите процесс по желанию для любых дополнительных новых пользователей, которые могут потребоваться. Обязательно создайте хотя бы одного нового пользователя перед выполнением упражнения 8-2.

УПРАЖНЕНИЕ 8-2

Реальные и поддельные оболочки (shell)

Не выполняйте это упражнение, если в локальной системе уже не создан обычный пользователь. При желании сначала запустите упражнение 8-1, так как это позволит вам создать нового обычного пользователя в целевой системе.

1. Откройте файл **/etc/passwd**. Найдите текущего обычного пользователя с **UID 1000** или выше.
2. Определите оболочку по умолчанию. Это указано в последнем столбце, обычно **/bin/bash** для обычных пользователей.
3. Измените оболочку по умолчанию на **/sbin/nologin** и сохраните изменения в Файл **/etc/passwd**.
4. Откройте другую виртуальную консоль. Нажмите клавиши **ctrl-alt-f2**, чтобы открыть другую консоль. (Если вы уже во второй виртуальной консоли, замените **f3**, **f4**, **f5** или **f6** на **f2**. Если вы используете виртуальную машину на основе **KVM** в графическом интерфейсе, вы можете перейти на вторую виртуальную консоль, нажав Отправить ключ | **Ctrl-Alt-F2**.)
5. Попробуйте войти в систему как измененный пользователь. Что происходит?
6. Вернитесь к оригинальной консоли. Если это **GUI**, он должен быть доступен с помощью комбинации клавиш **ctrl-alt-f1**. Если это невозможно (например, когда **GUI** не установлен), вы все равно сможете войти в систему как пользователь **root**.
7. Снова откройте файл **/etc/passwd**. Восстановите оболочку **/bin/bash** для обычного целевого пользователя.

Изменить аккаунт

Как администратор **Linux**, вы можете добавить некоторые ограничения к учетным записям пользователей. Самый простой способ проиллюстрировать некоторые изменения - это инструмент **User Manager GUI**. Запустите Диспетчер пользователей, выберите настроенного пользователя и нажмите «Свойства», чтобы открыть диалоговое окно «Свойства пользователя».

Нажмите на вкладку **Account Information** для информации об истечении срока действия учетной записи, показанной на **рисунке 8-1**. Как показано на рисунке, вы можете ограничить срок действия учетной записи, чтобы срок ее действия истек в определенную дату, или вы можете отключить учетную запись, заблокировав ее.

Нажмите вкладку Информация о пароле. Как показано на **рисунке 8-2**, вы можете установить несколько характеристик, связанных с паролем отдельного пользователя. Даже когда установлены хорошие пароли, часто Смена пароля может помочь обеспечить дополнительную безопасность. Категории, показанные на рисунке, говорят сами за себя.

Нажмите вкладку **Группы**. Пользователи могут принадлежать к нескольким группам в **Linux**. На вкладке Группы, показанной на **рис. 8-3**, вы можете назначить целевого пользователя другим группам. Например, чтобы обмениваться файлами и облегчить совместную работу в команде управления, вы можете назначить соответствующих пользователей группе с именем «менеджеры». Вы можете назначить членов команды в соответствующую группу на вкладке «Группы».

РИСУНОК 8-1 Управление сроком действия учетной записи пользователя.



РИСУНОК 8-2 Настройте информацию о пароле.



РИСУНОК 8-3 Назначить группу.



Дополнительные команды управления пользователями и группами

Хотя утилита **Red Hat User Manager GUI** удобна, часто быстрее выполнять связанные административные функции через интерфейс командной строки. Мы описали некоторые из этих команд, такие как **useradd**, **userdel**, **groupadd** и **groupdel**. Три другие ключевые команды администрирования пользователей - **usermod**, **groupmod** и **chage**.

usermod

Команда **usermod** изменяет различные настройки в **/etc/passwd**. Кроме того, это позволяет вам установить срок действия для учетной записи или дополнительной группы. Например, следующая команда устанавливает срок действия учетной записи, связанной с пользователем **test1**, **8 июня 2016 года**:

```
# usermod -e 2016-06-08 test1
```

ТАБЛИЦА 8-7 Параметры команды usermod

Вариант	Назначение
-a -G group1	Присоединяется к существующим группам; Можно указать несколько групп, разделенных запятой, без пробелов.
-l newlogin	Меняет имя пользователя на newlogin , не меняя домашний каталог.
-L	Блокирует пароль пользователя.
-U	Разблокирует пароль пользователя.

Следующая команда делает пользователя **test1** членом специальной группы:

```
# usermod -G special test1
```

Команда **usermod** тесно связана с командой **useradd**; на самом деле команда **usermod** может использовать все переключатели команды **useradd**, перечисленные ранее в таблице 8-6.

Команда **usermod** включает в себя несколько дополнительных ключей, перечисленных в таблице 8-7.

groupmod

Команда **groupmod** относительно проста. Он имеет два практических применения. Следующая команда изменяет номер **GID** группы с именем **project** (в данном случае, на **60002**):

```
# groupmod -g 60002 project
```

Напротив, следующая команда изменяет имя группы с именем **project** на **secret**:

```
# groupmod -n secret project
```

Chage

Команда **chage** в основном используется для управления устаревшей информацией для пароля, которая хранится в файле **/etc/shadow**. Хотя некоторые из параметров также могут быть установлены с помощью команд **useradd** и **usermod**, большинство из опций другие, как описано в таблице 8-8.

!!!!

Команда **chage** является отличным способом решения задачи RHCE «настроить устаревание пароля для локальных учетных записей пользователей».

!!!!

ТАБЛИЦА 8-8 Параметры команды chage

Вариант	Назначение
-Д ГГГГ-ММ-ДД	Устанавливает дату последнего изменения пароля; выходные данные отображаются в /etc/shadow как количество дней после 1 января 1970 года.
-Е ГГГГ-ММ-ДД	Назначает дату истечения срока действия для учетной записи; выходные данные отображаются в /etc/shadow как количество дней после 1 января 1970 года.
-I num	Блокирует учетную запись через несколько дней после истечения срока действия пароля; можно установить -1 , чтобы сделать учетную запись постоянной.
-l	Перечисляет всю устаревшую информацию.
-m num	Устанавливает минимальное количество дней, в течение которых пользователь должен хранить пароль.
-M num	Устанавливает максимальное количество дней, в течение которых пользователю разрешено хранить пароль; может быть установлен в -1 , чтобы удалить этот предел.
-W num	Указывает, когда пользователю предлагается сменить пароль, в количестве дней до истечения срока действия пароля.

ЦЕЛЬ СЕРТИФИКАЦИИ 8.02

Административный контроль

Для администраторов важно выполнять большинство действий как обычные пользователи, потому что администратор **root** имеет полные привилегии в системе.

Ограничения для обычных пользователей могут помочь защитить системы Linux от несчастных случаев. Обычные пользователи, имеющие пароль администратора **root**, могут временно получить права **root** с помощью команды **su**. Команда **su** может выполнять больше действий с другими учетными записями. Напротив, команда **sg** связана с привилегиями в специальных группах.

Хотя команда **su** подходит для небольших сетей, ни один администратор не должен работать в одиночку. С помощью команды **sudo**, настроенной в файле **/etc/sudoers**, можно настроить выделенных администраторов с частичными или полными привилегиями администратора **root** или выполнить команду от имени другого пользователя.

Возможность войти в систему как root

Можно запретить пользователям входить в систему напрямую от имени пользователя **root**. Локальный доступ регулируется в файле **/etc/security**. По умолчанию он содержит директивы доступа для 11 виртуальных консолей. Хотя в файле **/etc/systemd/logind.conf** включены только шесть виртуальных консолей. Как обсуждалось в главе 5, можно настроить 12 (в зависимости от количества функциональных клавиш на клавиатуре).

Виртуальные консоли, перечисленные в **/etc/security**, определяют консоли, на которых пользователю с правами администратора разрешено входить в систему. Если директивы в этом файле были закомментированы, администраторы не смогут напрямую войти в учетную запись **root**. Им придется войти в обычную учетную запись и использовать для администрирования команду **su** или **sudo**.

Хотя по-прежнему возможно удаленно войти в систему как пользователь **root** с помощью команды **ssh**, эту возможность также можно регулировать. Таким образом, конфигурация сервера **SSH** является навыком RHCE, описанным в главе 11.

УПРАЖНЕНИЕ 8-3

Ограничить root-логины

В этом упражнении вы изучите эффект удаления консолей в файле **/etc/security**. Но сначала вы подтвердите, что пользователь с правами администратора может войти в стандартные консоли на виртуальных терминалах с 1 по 6. В этом упражнении предполагается, что в локальной системе доступна обычная учетная запись.

1. Перейдите ко второй виртуальной консоли. Нажмите **Ctrl-Alt-F2**; в качестве альтернативы, в виртуальной машине **KVM** щелкните **Отправить ключ | Ctrl-Alt-f2**. При появлении приглашения **login**: войдите в систему как пользователь **root**.
2. Повторите процесс с первой, третьей, четвертой, пятой и шестой виртуальными консолями. Если **/etc/security** ещё не был изменен, вы должны иметь возможность войти в систему как пользователь **root** во всех этих консолях.
3. Сделайте резервную копию текущего файла **/etc/security**.
4. Откройте файл **/etc/security** в текстовом редакторе. Закомментируйте все директивы и сохраните файл.
5. Выйдите из консоли. Попробуйте снова войти в систему как пользователь **root**. Что происходит? Повторите процесс в других виртуальных консолях. Что происходит?
6. Войдите в консоль как обычный пользователь. Это работает? Запустите команду **su -**, чтобы получить права **root**. Восстановите исходный файл **/etc/security**.
7. Если в системе не существует учетной записи обычного пользователя, вам придется перезагрузить систему в целевом средстве восстановления, как описано в главе 5. После этого вы сможете восстановить Файл **/etc/security** из появившейся подсказки.

Возможность авторизации

За файлом **/etc/securetty** находится **/etc/security/access.conf**, который регулирует доступ для всех пользователей. Хотя версия этого файла по умолчанию полностью закомментирована, комментарии содержат полезные примеры. Первый пример запретил бы (с -) вход в первую виртуальную консоль (**tty1**) всем пользователям, кроме **root**:

-:ALL EXCEPT root:tty1

Перейдите к следующей строке в файле. Следующая строка представляет собой несколько более сложный пример, который запрещает доступ всем пользователям, кроме пользователей, которые являются членами группы **wheel**, а также пользователям **shutdown** и **sync** при локальных (не сетевых) входах в систему:

-:ALL EXCEPT (wheel) shutdown sync:LOCAL

Прокрутите вниз в файле. Следующие строки (с +) позволяют пользователю **root** получать доступ к системе с трех определенных удаленных IP-адресов вместе с адресом **localhost**:

+: root: 192.168.200.1 192.168.200.4 192.168.200.9
+: root: 127.0.0.1

Если вы защищаете систему от внешних сетей, этот тип ограничения на прямой доступ с правами администратора имеет смысл. Пока команда **su** или **sudo** позволяет это, пользователи, которые входят удаленно, как обычные пользователи, могут соответствующим образом повышать свои привилегии.

Помните, что директивы в этом файле рассматриваются по порядку. Таким образом, если директивы, которые разрешают доступ (с +), идут первыми, то следующая директива запрещает доступ всем другим пользователям из всех других локальных и удаленных имен входа:

- : ALL : ALL

Правильное использование команды **su**

В некоторых случаях, таких как экзамены **Red Hat**, целесообразно войти в систему как пользователь **root**. Но в реальных производственных системах лучше всего войти в систему как обычный пользователь. Как обычный пользователь вы можете временно открыть оболочку с правами администратора **root** с помощью команды **su**. Обычно эта команда запрашивает пароль пользователя с правами администратора. После того, как вы выполнили административные задачи, лучше всего выйти из корневой учетной записи администратора; команда выхода вернется к обычной учетной записи этого пользователя.

Команда **su** - немного отличается, потому что она открывает оболочку входа для учетной записи администратора **root**. Если пароль принят, он переходит в домашний каталог пользователя **root /root** и устанавливает среду, как если бы пользователь **root** вошел в систему напрямую.

Если у вас есть пароль второго пользователя, вы можете использовать команду **su - username** для входа непосредственно в эту учетную запись. Например, если вы хотите войти в учетную запись пользователя **dickens**, вы бы запустили команду **su - dickens**. Когда вы успешно введете ее пароль, команда приведет вас в каталог **/home/dickens**.

Наконец, команда **su -c** может использоваться для получения прав администратора для одной команды. Например, следующая команда может использоваться для изменения первого виртуального диска в системе (при условии, что в ответ на приглашение был успешно введен пароль администратора **root**):


```
$ su -c '/sbin/fdisk /dev/vda'
```

Ограничить доступ к su

Как обсуждалось ранее, возможность входа в систему непосредственно от имени пользователя **root** может регулироваться. Возможны дополнительные ограничения административного доступа. Например, вы можете ограничить пользователей, которым разрешено запускать команду **su**. Это требует двух основных шагов.

Во-первых, вам нужно перечислить пользователей, которые должны иметь доступ к команде **su**. Сделайте их частью группы **wheel**. По умолчанию, вот как выглядит эта строка в **/etc/group**:

```
wheel: x: 10:
```

Вы можете добавить выбранных пользователей в конец этой строки непосредственно с помощью команды **usermod -G wheel username** или с помощью диспетчера пользователей.

Во-вторых, это требует изменения конфигурации сменных модулей аутентификации (PAM). Хотя PAM, как описано в Главе 10, является целью RHCE, в файле **/etc/pam.d/su** есть готовая закомментированная директива:

```
# auth required pam_wheel.so use_uid
```

Если эта строка активирована, только пользователи, которые являются членами группы **wheel**, могут использовать команду **su**.

Правильное использование команды sg

С помощью команды **sg** вы можете выполнить другую команду с правами, связанными со специальной группой. Это предполагает, что вы являетесь участником группы или вы установили групповой пароль для группы проектов с помощью команды проекта **gpasswd**. Затем команда **sg project -c** Правильное использование команды sg

С помощью команды **sg** вы можете выполнить другую команду с правами, связанными со специальной группой. Это предполагает, что вы являетесь участником группы или вы установили групповой пароль для группы проектов с помощью команды проекта **gpasswd**. Затем команда **sg project -c command** позволяет вам получить доступ к файлам и каталогам, принадлежащим группе с именем **project**. Например, если каталог **/home/secret** принадлежит группе проекта, следующая команда копирует файл **important.doc** в указанный каталог:

```
$ sg project -c 'cp important.doc /home /project'
```

позволяет вам получить доступ к файлам и каталогам, принадлежащим группе с именем **project**. Например, если каталог **/home/secret** принадлежит группе проекта, следующая команда копирует файл **important.doc** в указанный каталог:

```
$ sg project -c 'cp important.doc /home/project'
```

Пользовательские администраторы с командой sudo

Вы можете ограничить доступ к команде **sudo**. Обычные пользователи, авторизованные в **/etc/sudoers**, могут получить доступ к административным командам со своим паролем. Вам не нужно выдавать административный пароль всем, кто считает, что знает столько же, сколько сертифицированный специалист Red Hat.

Чтобы получить доступ к **/etc/sudoers** с помощью редактора, указанного в файле **/etc/environment**, выполните команду **visudo**. Команда **visudo** блокирует файл **/etc/sudoers** от

одновременного редактирования и проверяет синтаксис файла перед выходом. Следующая директива активна в версии файла по умолчанию. Это дает пользователю **root** полный доступ к административным командам:

root ALL = (ALL) ALL

Другим пользователям может быть предоставлен административный доступ. Например, если вы хотите разрешить пользователю **boris** полный административный доступ, добавьте следующую директиву в **/etc/sudoers**:

boris ALL=(ALL) ALL

В этом случае все, что нужно **boris** для запуска административной команды, - это ввести ее с командой **sudo**. Например, если **boris** запускает следующую команду, он запрашивает собственный пароль обычного пользователя перед запуском указанной службы:

\$ sudo systemctl start vsftpd

Password:

Кроме того, вы можете разрешить специальным пользователям административный доступ без пароля. Как следует из комментариев, следующая директива в **/etc/sudoers** позволит всем пользователям, которые являются членами группы **wheel**, запускать административные команды без пароля:

% wheel ALL = (ALL) NOPASSWD: ALL

Но вам не нужно разрешать полный административный доступ. Например, если вы хотите разрешить пользователям, являющимся членами группы **% users**, завершать работу локальной системы, активируйте следующую директиву:

% users localhost = /sbin/shutdown -h now

Во многих файлах конфигурации **Linux** знак **%** перед директивой указывает группу. Несмотря на то, что **GID** группы пользователей равен **100**, в нее могут входить обычные пользователи. Например, другая директива, показанная в комментариях, задает группу команд, которые могут запускаться пользователями, которые являются членами группы **% sys**:

%sys ALL = NETWORKING, SOFTWARE, SERVICES, STORAGE, DELEGATING, \ PROCESSES, LOCATE, DRIVERS

Каждая из директив может быть связана с набором команд. Например, пользователи в группе **sys**, которым разрешено запускать директивы **PROCESSES**, могут запускать команды, связанные со следующей строкой конфигурации:

Cmnd_Alias PROCESSES = /bin/nice, /bin/kill, /usr/bin/kill, /usr/bin/killall

Аналогичным образом вы можете настроить группу администраторов, которым разрешено запускать эти команды, с помощью следующей директивы:

%admin ALL = PROCESSES

Это предполагает, что такие группы, как **admin**, существуют в файлах **/etc/group** и **/etc/gshadow**.

Другие административные пользователи

Различные сервисы могут быть настроены с их собственными группами административных пользователей. Например, проверьте следующую директиву из файла **/etc/cups/cups-files.conf**:

SystemGroup sys root

Члены групп, перечисленных в **SystemGroup**, получают административные привилегии на сервере печати RHEL 7.

!!!!

CUPS больше не является аббревиатурой, чтобы избежать проблем со словом «UNIX» в качестве товарного знака. Однако **CUPS** по-прежнему является именем сервера печати Linux по умолчанию.

!!!!

ЦЕЛЬ СЕРТИФИКАЦИИ 8.03

Конфигурация пользователя и оболочки

Каждый пользователь в любой системе Red Hat Enterprise Linux имеет среду окружения при входе в систему. Среда определяет каталоги, в которых Linux ищет программы для запуска, внешний вид приглашения входа в систему, тип терминала и многое другое. В этом разделе объясняется, как вы можете настроить среду по умолчанию для локальных пользователей. Все общесистемные файлы конфигурации оболочки хранятся в каталоге **/etc**. Это файлы **bashrc**, **profile** и скрипты в каталоге **/etc/profile.d**. Эти файлы и сценарии дополняются скрытыми файлами в домашнем каталоге каждого пользователя, как только что описано. Давайте посмотрим на эти файлы.

Домашние каталоги и /etc/skel

Когда новый пользователь создается с помощью стандартных команд, таких как **useradd**, или таких утилит, как **User Manager**, набор файлов конфигурации по умолчанию копируется в домашний каталог пользователя из каталога **/etc/skel**.

Домашний каталог

Домашний каталог - это то место, откуда пользователь начинает входить в систему **RHEL**. Домашним каталогом для большинства пользователей является **/home/username**, где **username** - это имя пользователя для входа. Каждый пользователь обычно должен иметь разрешение на запись в своем собственном домашнем каталоге, чтобы каждый пользователь мог свободно читать и записывать свои собственные файлы.

/etc/skel

Каталог **/etc/skel** содержит файлы среды по умолчанию для новых учетных записей. Команда **useradd** и **Red Hat User Manager** копируют эти файлы в домашний каталог для новых пользователей. Содержимое **/etc/skel** может отличаться. Хотя стандартные файлы в этом каталоге скрыты, администраторы могут добавлять новые файлы для новых пользователей. Стандартные файлы из одной копии **/etc/skel** описаны в **таблице 8-9**.

!!!!

Linux содержит много скрытых файлов, которые начинаются с точки (.). Чтобы получить список этих файлов, выполните команду **ls -a**. Например, если вы хотите получить список всех файлов в каталоге **/etc/skel**, введите команду **ls -a /etc/skel**.

ТАБЛИЦА 8-9 Стандартные файлы в каталоге /etc/skel

Файл	Назначение
.bashrc	Этот базовый файл конфигурации bash может содержать ссылку на общий файл конфигурации /etc/bashrc . Он может включать команды, запускаемые при запуске оболочки bash . Одним из примеров является псевдоним, такой как rm = 'rm -i' .
.bash_logout	Этот файл выполняется при выходе из оболочки bash и может включать в себя команды, подходящие для этой цели, такие как команды для очистки экрана.
.bash_profile	Этот файл создается только при вызове оболочки входа в bash и настраивает среду запуска bash . Это подходящее место для добавления переменных среды или изменения каталогов в вашей учетной записи PATH .
.kde /	Определяет настройки для K Desktop Environment . Он не добавляется в /etc/skel и не копируется в домашние каталоги пользователей, если KDE не установлен.
.mozilla /	Включает опции, связанные с веб-браузером Firefox , разработанным проектом Mozilla .

Если вы установили в **RHEL** более стандартного набора программных пакетов, дополнительные файлы конфигурации и подкаталоги могут появиться в каталоге **/etc/skel**. Например, установка некоторых пакетов может включать файлы конфигурации, связанные с **emacs** и оболочкой **Z (zsh)** в этом каталоге.

Как системный администратор, вы можете редактировать эти файлы или помещать пользовательские файлы в **/etc/skel**. Когда создаются новые пользователи, эти файлы распространяются в домашние каталоги новых пользователей.

/etc/bashrc

Файл **/etc/bashrc** используется для псевдонимов и функций в масштабе всей системы. Откройте этот файл в текстовом редакторе по вашему выбору. Прочитайте каждую строку в этом файле. Даже если вы не понимаете команд программирования, вы можете видеть, что этот файл устанавливает следующие параметры оболочки **bash** для каждого пользователя:

- Он присваивает значение **umask**, которое создает разрешения по умолчанию для вновь создаваемых файлов. Он поддерживает один набор разрешений для пользователей **root** и системы (с идентификаторами пользователей ниже **200**), а другой - для обычных пользователей. (Официально **RHEL** резервирует все идентификаторы пользователей выше **1000** для обычных пользователей, однако это не отражено в **/etc/bashrc**.)
- Он назначает и определяет приглашение, которое вы видите перед курсором в командной строке.
- Он содержит настройки из файлов ***.sh** в каталоге **/etc/profile.d/**.

Настройки здесь дополняются файлом **.bashrc** в домашнем каталоге каждого пользователя и, для оболочек входа в систему, файлами **/etc/profile**, **.bash_profile** и **.bash_logout**.

/etc/profile и /etc/profile.d

Файл **/etc/profile** используется для общесистемных сред и файлов запуска и исходит из того, что **bash** вызывается как оболочка входа в систему.

Первая часть файла устанавливает **PATH** для поиска команд. Дополнительные каталоги добавляются в **PATH** с помощью команды **pathmunge**. (Если вы не используете оболочку **Korn**, игнорируйте раздел «**ksh workaround**».) Затем он экспортирует переменные **PATH**, **USER**, **LOGNAME**, **MAIL**, **HOSTNAME**, **HISTSIZE** и **HISTCONTROL** и, наконец, устанавливает **umask** и запускает сценарии в каталоге **/etc/profile.d**. Вы можете проверить текущее значение любой из этих переменных с помощью команды **echo \$variable**.

/etc/profile.d

Каталог **/etc/profile.d** предназначен для хранения сценариев, которые должны выполняться в логине или интерактивной оболочке (то есть не в сценарии или команде, выполняемой как команда **bash -c**). Если вы выполнили установку «Сервер с графическим интерфейсом», ниже приведен частичный список файлов; те с расширениями **.sh** применяются к оболочке **bash** по умолчанию:

256term.csh	colorls.csh	PackageKit.sh
256term.sh	colorls.sh	vim.csh
abrt-cosole-notifiction.sh	lang.csh	vim.sh
bash_completion.sh	lang.sh	vte.sh
colorgrep.csh	less.csh	which2.csh
colorgrep.sh	less.sh	which2.sh

УПРАЖНЕНИЕ 8-4

Еще один способ обезопасить систему

Еще один способ защитить систему - изменить разрешения по умолчанию для новых файлов и каталогов. В этом упражнении вы перенастроите систему, чтобы удалить права доступа к файлам по умолчанию у других пользователей или групп.

1. Сделайте резервную копию текущей версии файлов **/etc/bashrc** и **/etc/profile**.
2. Откройте файл **/etc/bashrc** в текстовом редакторе. Две строки в файле задают маску. Выбирается одна из двух строк в зависимости от оператора **if** над ними. Посмотрите, сможете ли вы определить, какое значение **umask** назначено обычному (не **root**) пользователю.
3. Оператор **if** проверяет, совпадают ли имя пользователя и имя группы, и что **UID** больше **199**. Другими словами, значение **umask 002** присваивается обычным пользователям. Значение **umask 022** предоставляется пользователям системы.
4. Измените первый оператор **umask**, чтобы исключить все разрешения для групп и других. Другими словами, замените **umask 002** на **umask 077**.
5. Сохраните и выйдите из файла.
6. Повторите шаги с 2 по 5 для **/etc/profile**.
7. Войдите в систему как обычный непривилегированный пользователь. Используйте команду **touch**, чтобы создать новый пустой файл. Используйте **ls -l** для проверки прав доступа к этому файлу.
8. Войдите в систему как **root**. Опять же, используйте команду **touch**, чтобы создать новый пустой файл, и используйте **ls -l**, чтобы проверить разрешения для этого нового файла. Вы только что изменили **umask** по умолчанию для всех обычных пользователей. Хотя это отличный вариант для обеспечения безопасности, он может повлиять на шаги, используемые в других главах. Поэтому последний шаг важен.
9. Восстановите исходные версии **/etc/bashrc** и **/etc/profile** из резервной копии, созданной на шаге 1.

Файлы конфигурации оболочки в домашних каталогах пользователей

Как описано ранее, каждый пользователь получает копию всех файлов из каталога `/etc/skel`, обычно при создании учетной записи. Большинство из них скрыты и отображаются только такими командами, как **ls -a**. Когда пользователи начинают работать со своими учетными записями, в их домашние каталоги могут добавляться дополнительные файлы конфигурации. Некоторые пользователи могут работать в основном с оболочкой **bash** по умолчанию, в то время как другие будут иметь дополнительные файлы конфигурации, связанные с их средами рабочего стола с графическим интерфейсом, такими как GNOME. Оболочка **Linux** по умолчанию - **bash**, и до недавнего времени она была специально включена в качестве единственной оболочки, описанной в соответствующих задачах экзамена **Red Hat**. Хотя **bash** больше не включен в задачи, он используется по умолчанию для **RHEL 7**.

Вход в систему, выход из системы и переключение пользователей

Хотя это может показаться чем-то вроде «простой задачи» для пользователей Linux с опытом работы в течение всего нескольких дней, одна из тем RHCSA - «Вход в систему и переключение пользователей в многопользовательских целях». Она включает в себя концепции из разных глав. Как обсуждалось в Главе 5, многопользовательскими целями являются `multi-user.target` и `graphical.target`. Виртуальные терминалы доступны во всех этих целях. Для первого выпуска RHEL 7 текстовое приглашение для входа выглядит следующим образом:

```
Red Hat Enterprise Linux Server 7.0 (Maipo)
Kernel 3.10.0-123.el7.x86_64 on an x86_64
server1 login:
```

Имя хоста, а также версии RHEL 7 и ядра будут различаться. Но это не имеет отношения к реальным входам в систему; все, что вам нужно сделать, это ввести имя пользователя, нажать клавишу ввода и ввести пароль при появлении запроса. Выход из командной строки еще проще; все команды **exit**, **logout** и **ctrl-d** выполняют выход из командной строки. Конечно, как только вы выйдете из системы, появится только что появившееся приглашение.

Как обсуждалось ранее в этой главе, существует другой способ переключения учетных записей пользователей. Например, чтобы переключиться с текущей учетной записи на учетную запись пользователя **donna**, выполните следующую команду:

```
$ su - donna
```

Те же команды **exit**, **logout** и **ctrl-d** можно использовать для выхода из учетной записи пользователя **donna**.

Конечно, пользователи могут входить и выходить из **GUI**. Хотя шаги в зависимости от среды рабочего стола несколько различаются, они так же просты, как и шаги, необходимые для входа и выхода из любой другой операционной системы.

ЦЕЛЬ СЕРТИФИКАЦИИ 8.04

Пользователи и сетевая аутентификация

По умолчанию для доступа к компьютеру Linux требуются действительные имя пользователя и пароль. Одна проблема с большой сетью систем Linux состоит в том, что без какой-либо центральной базы данных каждому пользователю потребуется учетная запись на каждом компьютере Linux.

!!!!

В целях экзамена RHCSA для RHEL 6 единственным требованием сетевой аутентификации была возможность подключения клиента к серверу LDAP. Соответствующая цель для RHEL 7 является более общей и требует, чтобы вы «сконфигурировали систему для использования существующей службы аутентификации для информации о пользователях и группах». Это может включать не только LDAP, но и другие службы, такие как Kerberos, Active Directory и IPA. Инструмент authconfig поддерживает все из них и позволяет вам настроить клиента за несколько простых шагов. !!!!!

Доступно несколько сервисов, которые можно использовать как центральную базу данных аутентификации. Одним из устаревших вариантов для систем Linux является Служба сетевой информации (**Network Information Service NIS**). В отличие от этого, облегченный протокол доступа к каталогам (**Lightweight Directory Access Protocol LDAP**) обеспечивает большую безопасность и в настоящее время является стандартом де-факто. Доступны и другие службы, такие как **Winbind**, которые можно настроить для поддержки доступа систем и пользователей **Linux** к сетям, управляемым **Microsoft Active Directory**. Другим вариантом является **IPA** (и его бесплатная версия **FreeIPA**), который является сервером идентификации, политики и аудита, который включает в себя центр сертификации, а также LDAP и Kerberos Сервисы. В любом из этих случаев для сети существует одна база паролей и имен пользователей.

ТАБЛИЦА 8-10 Общие службы сетевой аутентификации

Сервисы	Информация о пользователе и группе	Аутентификация
Local files	Получено из /etc/passwd и /etc/group	Хэшированные пароли в /etc/shadow
Сервер сетевой информационной системы (NIS)	Централизованный /etc/passwd и /etc/group	Централизованный /etc/shadow
Сервер сетевой информационной системы (NIS) с MIT Kerberos KDC	Централизованный /etc/passwd и /etc/group	Kerberos
OpenLDAP, сервер каталогов 389	Протокол LDAP/LDAPS	Протокол LDAP/LDAPS
Сервер каталогов OpenLDAP или 389 Directory с MIT Kerberos KDC	Протокол LDAP/LDAPS	Kerberos
IPA, FreeIPA	LDAP/LDAPS против 389 Сервер каталогов	Kerberos
Microsoft Active Directory	Протокол LDAP/LDAPS	Kerberos

Таблица 8-10 иллюстрирует некоторые общие параметры, доступные для централизованной аутентификации, а также протоколы и ресурсы, на которые опирается каждое решение для получения информации о пользователе и выполнения аутентификации.

Как видно из таблицы 8-10, для получения информации об учетной записи пользователя и аутентификации могут использоваться разные решения. Например, вы можете использовать сервер **LDAP** в качестве базы данных для информации о пользователях и группах, в то время как аутентификация может быть предоставлена Центром распространения ключей **Kerberos** (KDC).

Основное внимание в следующем разделе уделяется **LDAP** как клиенту. Вы настроите систему RHEL 7 в качестве клиента **LDAP**, настроите аутентификацию в файле переключателя

службы имен и повторите процедуру с помощью инструментов сетевой аутентификации **Red Hat**. Сначала мы покажем вам, как можно настроить клиенты **LDAP** с помощью интерфейса командной строки, а затем использовать инструмент настройки аутентификации **Red Hat**, чтобы повторить процесс. Таким образом, вы узнаете два способа настройки клиентов **LDAP**.

В отличие от **NIS**, службы **LDAP** могут быть настроены на различных платформах. Конечно, серверы **LDAP** могут быть настроены на **RHEL 7**, но они не являются частью текущих целей экзаменов **RHCSA** или **RHCE**. **LDAP** также используется службами **IPA** и **Active Directory (AD)** на базе **Microsoft**.

!!!!

Службы каталогов **LDAP** и аутентификация были одним из основных направлений курса **RH423**, вышедшего на пенсию, тогда как новый курс **RH413** охватывает управление идентификацией с помощью **IPA**. Если вы хотите настроить централизованный сервер аутентификации **LDAP**, изучите сервер каталогов **389** по адресу <http://directory.fedoraproject.org>.

!!!!

Конфигурация клиента **LDAP**

Чтобы настроить компьютер **RHEL** в качестве клиента **LDAP**, вам понадобятся **RPM**-пакеты **openldap-clients**, **openldap** и **nss-pam-ldapd**. **RPM**-пакеты **openldap-clients** и **nss-pam-ldapd** являются необязательными частями группы пакетов клиента каталога. Пакет **openldap** должен быть установлен по умолчанию в системах **RHEL 7**, в которых при установке была выбрана группа среды «Сервер с графическим интерфейсом», как предлагалось в предыдущей лабораторной работе в этой книге.

Чтобы настроить клиент **LDAP**, вам необходимо настроить различные файлы конфигурации **LDAP**, а именно **/etc/nslcd.conf** и **/etc/openldap/ldap.conf**. Хотя файлы могут показаться сложными, вам не нужно много переконфигурировать, просто чтобы настроить клиент **LDAP**.

/etc/nslcd.conf

Версия файла **/etc/nslcd.conf** по умолчанию включает в себя ряд различных команд и комментариев. Стандартные изменения, необходимые для настройки базового клиента **LDAP**, основаны на нескольких директивах, показанных в таблице 8-11. Директивы, связанные с шифрованием в этом файле, могут быть связаны как с **Secure Sockets Layer (SSL)**, так и с его преемником **Transport Layer Security (TLS)**.

Файл **nslcd.conf** применяет подключаемые модули аутентификации к аутентификации **LDAP**. Он практически идентичен файлу **/etc/pam_ldap.conf** из **RHEL 6**; различия не влияют на успешную настройку клиента **LDAP**.

Связанные директивы включены в конец файла; они могут включать следующее. Во-первых, универсальный идентификатор ресурса, как указано в **URI**, должен перенаправить клиента на фактический **IP-адрес сервера LDAP**:

uri ldap://127.0.0.1/

Если вы хотите включить безопасную связь через **LDAP** через **SSL**, вы можете изменить **ldap** на **ldaps**; при настройке сервера **LDAP** эти протоколы по умолчанию используют порты **TCP/IP 389** и **636** соответственно. Сервер **LDAP** не будет работать, если брандмауэр блокирует эти порты. Если используется **LDAP** поверх **SSL**, вы должны либо указать **URI**, используя схему **ldaps://**, либо изменить следующее на **ssl yes**:

ssl no

ТАБЛИЦА 8-11 Параметры конфигурации клиента в /etc/nslcd.conf

Директива	Описание
uri	Настраивает URI для сервера LDAP в формате ldap://имя_хоста . Схема URI ldap:// определяет использование протокола LDAP в виде открытого текста (по протоколу TCP-к порту 389), тогда как ldaps:// предназначена для LDAP через SSL (на TCP-порту 636).
base dc=example,dc=com	Устанавливает базовое отличительное имя по умолчанию, которое будет использоваться для поиска LDAP для извлечения объектов пользователя и группы (в этом случае dc = example, dc = com).
ssl start_tls	Требуется, если StartTLS используется для согласования зашифрованной связи через TCP-порт 389 . В качестве альтернативы, зашифрованная связь также может быть обеспечена путем отключения StartTLS (ssl off) и использования LDAP через SSL через схему ldaps:// URI .
tls_cacertdir /etc/openldap/cacerts	Указывает каталог, в котором хранится сертификат центра сертификации (ЦС). Это требуется при использовании SSL или TLS для шифрования.
nss_initgroups_ignoreusers root	Запрещает групповой поиск для указанных пользователей на сервере LDAP .

Альтернативный способ получения зашифрованных соединений с сервером **LDAP** - использование **StartTLS**, который согласовывает безопасные соединения через **TCP-порт 389**. В этом случае вы должны установить **ssl start_tls** и ввести **URI**, используя схему **ldap://**.

Конечно, для включения безопасных соединений **LDAP** необходим доступ к соответствующим сертификатам. Хотя **TLS** является преемником **SSL**, он обычно используется в сочетании с директивами **SSL**. Следующая директива указывает каталог с этими сертификатами:

tls_cacertdir /etc/openldap/cacerts

Наконец, служба **nslcd** должна быть запущена и включена при загрузке:

```
systemctl enable nslcd
systemctl start nslcd
```

/etc/openldap/ldap.conf

В этом файле вам нужно будет указать переменные **URI**, **BASE** и **TLS_CACERTDIR**, как это было сделано в файле конфигурации **/etc/nslcd.conf**. Учитывая параметры в предыдущем разделе, вы можете даже увидеть четыре директивы в этом файле:

```
URI ldap://127.0.0.1
SASL_NOCANON on
BASE dc=example,dc=com
TLS_CACERTDIR /etc/openldap/cacerts
```

Если сервер **LDAP** не находится в локальной системе и базовое различающееся имя не является **dc=example,dc = com**, замените соответственно. Отдельные пользователи могут заменить этот файл в скрытом файле **.ldaprc** в своих домашних каталогах.

Файл переключателя службы имен

Файл переключателя службы имен (**Name Service Switch NSS**), **/etc/nsswitch.conf**, определяет, как компьютер ищет ключевые файлы, такие как базы паролей. Его можно настроить для просмотра **LDAP** и других баз данных сервера. Например, когда клиент ищет имя хоста компьютера, он может начинаться со следующей записи из **/etc/nsswitch.conf**:

hosts: files ldap dns

Эта строка указывает вашему компьютеру выполнять поиск в базе данных имен в следующем порядке:

1. Начните с базы данных имен хостов и IP-адресов в локальном файле **/etc/hosts**.
2. Найдите имя хоста, запросив сервер **LDAP**.
3. Если ни одна из этих баз данных не содержит нужного имени хоста, обратитесь к **DNS-серверу**.

Вы можете настроить файл конфигурации **/etc/nsswitch.conf** для просмотра сервера **LDAP** для желаемых баз данных. Например, чтобы настроить централизованную базу данных имен пользователей и паролей для вашей сети, вам необходимо настроить как минимум следующие команды **/etc/nsswitch.conf**:

passwd: files ldap
shadow: files ldap
group: files ldap

Другие базы данных аутентификации могут быть настроены; **NIS** связан с директивой **nis**; Аутентификация **Microsoft** может быть настроена либо через службы **AD** на основе **LDAP**, либо путем присоединения хоста Linux к домену AD с помощью **winbind**. Другой важный клиентский сервис аутентификации - это **sssd**, который является темой следующего раздела.

Демон службы безопасности системы

Демон системных служб безопасности (**System Security Services Daemon SSSD**) предоставляет службы кэширования и автономной проверки подлинности, чтобы пользователи могли проходить проверку подлинности, даже когда удаленный сервер **LDAP** недоступен. **SSSD** может использоваться в качестве замены для демона **nss-pam-ldapd**. Он поставляется с несколькими связанными пакетами **RPM**, такими как **sssd-ad**, который **SSSD** может использовать для получения идентификационных данных с сервера **Active Directory**. Вы можете установить эти пакеты с зависимостями, установив **RPM-пакет meta sssd**:

yum -y install sssd

Аналогично **nss-pam-ldapd**, **SSSD** предоставляет интерфейс для **NSS** и **PAM**. Однако **SSSD** намного мощнее и может также аутентифицировать пользователей с помощью **Kerberos**, **Active Directory** и **IPA**.

Вы можете найти файл конфигурации **SSSD** в **/etc/sss/sss.conf**. Если файл отсутствует в вашей системе, **authconfig** (инструмент настройки аутентификации Red Hat, описанный в следующем разделе) может сгенерировать файл для вас. Пример конфигурации для клиента **LDAP** показан здесь:

id_provider = ldap
auth_provider = ldap
chpass_provider = ldap

```
ldap_uri = ldap://127.0.0.1
ldap_id_use_start_tls = True
ldap_tls_cacertdir = /etc/openldap/cacerts
[sssd]
services = nss, pam
config_file_version = 1
domains = default
```

Первые три строки указывают **SSSD** использовать **LDAP** для операций с информацией о пользователе, аутентификации и смены пароля. Затем указывается **URI LDAP**, аналогично директиве **uri** в **/etc/nslcd.conf**. Следующие два параметра конфигурации позволяют использовать **TLS** для шифрования и каталог, в котором хранится сертификат **CA**. Затем **SSSD** поручается работать вместе с **NSS** и **PAM**. Наконец, по крайней мере должен быть настроен домен **SSSD** по умолчанию. Доменное имя используется для идентификации различной информации в базе данных пользователей в тех случаях, когда в сети доступно больше, чем метод аутентификации.

Когда **SSSD** используется для извлечения информации об удаленном пользователе и аутентификации, записи в **/etc/nsswitch.conf** должны выглядеть примерно так, как показано здесь:

```
passwd: files sss
shadow: files sss
group: files sss
```

В то время как директива **ldap** в **/etc/nsswitch.conf** указывает системе использовать демон **nslcd** для поиска информации о пользователях, ключевое слово **sss** вместо этого использует **SSSD**. Конечно, демон **SSSD** должен быть запущен и включен при загрузке:

```
# systemctl enable sssd
# systemctl start sssd
```

Инструменты сетевой аутентификации Red Hat

Как вы видели в предыдущих разделах, конфигурация клиента **LDAP** требует, чтобы вы отредактировали несколько файлов. Таким образом, процесс настройки может быть очень подвержен ошибкам, если вы не очень хорошо знакомы со всеми параметрами конфигурации. Конечно, проще настроить клиент с помощью инструмента настройки аутентификации **Red Hat**. В **RHEL 7** его можно открыть в графическом интерфейсе с помощью команды **system-config-authentication** или **authconfig-gtk**. Существует также консольная версия, которую можно запустить с помощью команды **authconfig-tui** или инструмента **CLI authconfig**. Инструменты **GUI** и **TUI** предоставляются пакетом **RPM authconfig-gtk**. Версия **GUI** показана на рисунке 8-4.

Клиент LDAP

Инструмент настройки аутентификации изменился. По умолчанию он настроен на просмотр только локальной базы данных аутентификации, но если щелкнуть раскрывающееся текстовое поле, в нем представлены пять других вариантов. **LDAP** является одним из наиболее распространенных протоколов для служб аутентификации и информации о пользователях, но вы также должны ознакомиться с настройками других параметров. Когда выбран **LDAP**, окно меняется, как показано на рисунке 8-5. По умолчанию используется метод аутентификации по паролю **Kerberos**.

РИСУНОК 8-4 Параметры конфигурации аутентификации

The screenshot shows the 'Authentication Configuration' dialog box with the 'Identity & Authentication' tab selected. The 'User Account Configuration' section has 'User Account Database' set to 'Local accounts only'. The 'Authentication Configuration' section has 'Authentication Method' set to 'Password'. At the bottom are 'Revert', 'Cancel', and 'Apply' buttons.

Authentication Configuration

Identity & Authentication | Advanced Options | Password Options

User Account Configuration

User Account Database: Local accounts only

Authentication Configuration

Authentication Method: Password

Revert Cancel Apply

РИСУНОК 8-5 Параметры конфигурации аутентификации LDAP

The screenshot shows the 'Authentication Configuration' dialog box with the 'Identity & Authentication' tab selected. A warning message at the top states: 'The /lib64/security/pam_krb5.so file was not found, but it is required for Kerberos password support to work properly. Install the pam_krb5 package, which provides this file.' with an 'Install' button. The 'User Account Configuration' section has 'User Account Database' set to 'LDAP', 'LDAP Search Base DN' set to 'dc=example,dc=com', and 'LDAP Server' set to 'ldap://127.0.0.1'. There is a checkbox for 'Use TLS to encrypt connections' and a 'Download CA Certificate...' button. The 'Authentication Configuration' section has 'Authentication Method' set to 'Kerberos password', 'Realm' set to '#', and empty fields for 'KDCs' and 'Admin Servers'. There are checkboxes for 'Use DNS to resolve hosts to realms' and 'Use DNS to locate KDCs for realms'. At the bottom are 'Revert', 'Cancel', and 'Apply' buttons.

Authentication Configuration

Identity & Authentication | Advanced Options | Password Options

The /lib64/security/pam_krb5.so file was not found, but it is required for Kerberos password support to work properly. Install the pam_krb5 package, which provides this file. Install

User Account Configuration

User Account Database: LDAP

LDAP Search Base DN: dc=example,dc=com

LDAP Server: ldap://127.0.0.1

☐ Use TLS to encrypt connections

Download CA Certificate...

Authentication Configuration

Authentication Method: Kerberos password

Realm: #

KDCs:

Admin Servers:

☐ Use DNS to resolve hosts to realms

☒ Use DNS to locate KDCs for realms

Revert Cancel Apply

Обратите внимание на предупреждение на **рисунке 8-5**. Это говорит нам о том, что для использования **Kerberos** в качестве метода аутентификации по паролю нам необходимо установить пакет **LDAP pam_krb5**. Если сервер **Kerberos** недоступен для аутентификации, щелкните текстовое поле «Метод аутентификации» и выберите «**Пароль LDAP**». Окно снова изменится и должно отобразить следующее предупреждение:

You must provide ldaps:// server address or use TLS for LDAP authentication.

РИСУНОК 8-6

Аутентификация LDAP с шифрованием TLS



Если вы используете **LDAPS** или **StartTLS** для шифрования трафика, предупреждение исчезнет. В этом случае то, что вы видите, должно напоминать **рисунк 8-6**.

Остальные варианты могут отличаться:

1. Текстовое поле «**LDAP Search Base DN**» обычно включает имя домена для сервера **LDAP** и одну или несколько организационных единиц (**ou**). Например, если локальный системный домен - **example.com**, а пользователи находятся в разделе **ou = People**, текстовое поле может содержать следующее:

ou=People,dc=example,dc=com

2. Текстовое поле сервера **LDAP** должно содержать **URI** этого сервера. Если ваш сервер **LDAP** находится на локальном компьютере, вы можете использовать **IP-адрес 127.0.0.1**. Но это маловероятно в производственных ситуациях, что означает, что это также маловероятно во время экзамена. Для стандартных соединений **LDAP**, предварите **URI** с помощью **ldap://**. Для связи **LDAP** на основе **SSL** предварите **URI** с помощью **ldaps://**. В

- качестве альтернативы, если вы используете **StartTLS**, предварите **URI** с помощью **ldap://** и установите флажок **Использовать TLS** для шифрования соединений.
3. Если вы настраиваете защищенный **LDAP**, вам необходимо включить сертификат центра сертификации (**CA**). Нажмите **Загрузить сертификат CA** откроется окно, в котором вы можете указать **URL** с сертификатом **CA**.
 4. Теперь выберите вкладку **Advanced Options**, показанную на **рисунке 8-7**. Это не связано с настройкой клиента **LDAP**. В некоторых конфигурациях вы можете выбрать «Создание домашних каталогов при первом входе в систему». Эта опция позволяет РМ-модулю **pam_mkhome** автоматически создавать домашний каталог пользователя при первом входе в систему, если он еще не существует.

РИСУНОК 8-7 Вкладка "Дополнительные параметры"



IPA Client

IPA (и его бесплатная версия **FreeIPA**) - это пакет управления идентификацией, который включает в себя сервер каталогов **LDAP 389**, **MIT Kerberos KDC**, центр сертификации **Dogtag**, службу **NTP** и дополнительную службу **DNS**. Хотя настройка **IPA**-сервера выходит за рамки этой книги и экзамена **RHCSA**, настроить **IPA**-клиента относительно легко.

Сначала установите **RPM-пакет ipa-client**. Это также установит необходимые зависимые пакеты, такие как **krb5-workstation** и **sssd**:

```
# yum install ipa-client
```

Затем запустите **authconfig-gtk**, как показано на рисунке 8-8.

Параметры конфигурации просты:

- Домен является доменом **DNS**. Как клиент **IPA**, он должен соответствовать домену для служб управления идентификацией **IPA**. Например, если клиент **server1.example.com**, соответствующий домен будет **example.com**.
- Область является областью **Kerberos** и обычно указывается как домен заглавными буквами, например **EXAMPLE.COM**.
- Текстовое поле сервера должно содержать IP-адрес или полное доменное имя сервера.

После того, как все настройки введены, нажмите «Присоединиться к домену». Вам будет предложено ввести имя пользователя и пароль учетной записи IPA-сервера с правами для добавления новых клиентов в систему.

РИСУНОК 8-8 Параметры конфигурации аутентификации IPA

!!!!

Если вы хотите настроить IPA-сервер, обратитесь к проекту FreeIPA по адресу www.freeipa.org.

!!!!

ЦЕЛЬ СЕРТИФИКАЦИИ 8.05

Специальные группы

В прошлом группы постоянных пользователей Linux позволяли своим участникам обмениваться файлами. Red Hat помогла изменить это путем назначения уникальных номеров **UID** и **GID** каждому пользователю. Когда все обычные пользователи входят в одну и ту же основную группу, это также означает, что все в этой группе имеют доступ к домашним

каталогам всех остальных членов группы, а это часто нежелательно. Пользователи могут не захотеть делиться файлами в своих домашних каталогах с другими.

С другой стороны, **RHEL** дает каждому пользователю уникальный идентификатор пользователя и идентификатор группы в **/etc/passwd**. Это известно как схема частной группы пользователя. Пользователи получают эксклюзивный доступ к своим основным группам и не должны беспокоиться о том, что другие пользователи читают файлы в своих домашних каталогах.

Стандартные и Red Hat группы

В **RHEL** каждый пользователь по умолчанию получает свою собственную частную группу. Как отмечалось ранее, идентификаторы **UID** и **GID** обычно начинаются с **1000**, им присваиваются совпадающие номера и выполняются в порядке возрастания. Кроме того, вы можете создать специальные группы выделенных пользователей, в идеале с более высоким **GID**. Например, администратор может настроить **accgrp** для бухгалтерии, возможно, с **GID 70000**.

Общие каталоги

Большинство людей работают в группах, и они могут захотеть поделиться файлами. Однако у людей в этих группах могут быть веские причины скрывать свою информацию от других. Для поддержки таких групп вы можете создать общий каталог с ограниченным доступом к членам группы.

Предположим, вы хотите создать общий каталог **/home/accshared** для группы бухгалтеров. Для этого вы можете настроить общий каталог с помощью следующих основных шагов:

1. Создайте общий каталог:

```
# mkdir /home/accshared
```

2. Создать группу для бухгалтеров. Назовите это **accgrp**. Дайте ему идентификатор группы, который не мешает существующим идентификаторам группы или пользователя. Один из способов сделать это - добавить строку, такую как следующая, в файл **/etc/group** или с помощью диспетчера пользователей. Подставьте желаемые имена пользователей.

```
accgrp:x:70000:robertc,alanm,victorb,roberta,alano,charliew
```

3. Установите соответствующее владение для нового общего каталога. Следующие команды не позволяют любому конкретному пользователю получить контроль над каталогом и назначают владение группой для **accgrp**:

```
# chown nobody.accgrp /home/accshared  
# chmod 2770 /home/accshared
```

Любой пользователь, который является членом группы **accgrp**, теперь может создавать файлы и копировать файлы в каталог **/home/accshared**. Любые файлы, созданные в этом каталоге или скопированные в него, будут принадлежать группе **accgrp**.

Это стало возможным благодаря разрешениям **2770**, назначенным каталогу **/home/accshared**. Давайте разбить это на его составные части. Первая цифра (**2**) - это бит установленного идентификатора группы, также известный как бит **SGID**. Когда в каталоге установлен бит **SGID**, для всех файлов, созданных в этом каталоге, автоматически устанавливается принадлежность группы к владельцу группы в каталоге. Кроме того, групповое владение файлами, скопированными из других каталогов, переназначается (в данном случае, группе с именем **accgrp**). Есть второй способ установить бит **SGID** для каталога **/home/accshared**:

chmod g+s /home/acccshared

Остальные цифры являются базовыми знаниями для любого опытного пользователя **Linux** или **Unix**. **770** устанавливает права на **чтение, запись и выполнение** для пользователя и группы, которым принадлежит каталог. Другие пользователи не получают разрешений на этот каталог. Однако, поскольку владельцем пользователя каталога является непривилегированный пользователь с именем **nobody**, владелец группы каталога является наиболее важным. В этом случае члены группы **accgrp** имеют права на чтение, запись и выполнение для файлов, созданных в этом каталоге.

УПРАЖНЕНИЕ 8-5

Владение группой управления с помощью бита SGID

В этом упражнении вы создадите новые файлы в каталоге, предназначенном для совместного использования группой пользователей. Вы также увидите разницу в том, что происходит до и после установки бита **SGID**.

1. Добавьте пользователей с именами **test1**, **test2** и **test3**. Укажите пароли при появлении запроса. Проверьте файлы **/etc/passwd** и **/etc/group**, чтобы убедиться, что личная группа каждого пользователя была создана:

```
# useradd test1; echo changeme | passwd --stdin test1
# useradd test2; echo changeme | passwd --stdin test2
# useradd test3; echo changeme | passwd --stdin test3
```

2. Отредактируйте файл **/etc/group** и добавьте группу с именем **tg1**. Сделайте учетные записи **test1** и **test2** членами этой группы. Вы можете добавить следующую строку в **/etc/group** напрямую или использовать Red Hat User Manager:

```
tg1:x:99999:test1,test2
```

Прежде чем продолжить, убедитесь, что идентификатор группы, назначенный группе **tg1** (в данном случае **99999**), еще не используется. Убедитесь, что добавили следующую строку в **/etc/gshadow**. Групповой пароль не требуется.

```
tg1:!::test1,test2
```

3. Создайте каталог, предназначенный для использования группой **tg1**:

```
# mkdir /home/testshared
```

4. Измените пользователя и группу владельцев общего каталога:

```
# chown nobody.tg1 /home/testshared
```

5. Войдите как пользователь **test1**. Убедитесь, что логин переходит в каталог **/home/test1**. Запустите команду **umask**, чтобы убедиться, что файлы, созданные из этой учетной записи, будут иметь соответствующие разрешения. (Вывод команды **umask** для обычных пользователей, таких как **test1**, должен быть **0002**.) Если есть проблема с домашним каталогом или выводом **umask**, возможно, вы ранее допустили ошибку в этой главе с настройками пользователя. Если это так, повторите шаги 1–5 на другой виртуальной машине.

6. Запустите команду **cd /home/testshared**. Теперь попробуйте создать файл с помощью следующих команд. Что происходит?

```
$ date >> test.txt  
$ touch abcd
```

7. Теперь, как пользователь **root**, установите права на запись группы в каталоге **testshared**:

```
# chmod 770 /home/testshared
```

8. Снова войдите в систему как пользователь **test1**, вернитесь в каталог **/home/testshared** и попробуйте создать файл в новом каталоге. Все идет нормально.

7.

Теперь, как пользователь **root**, установите права на запись группы в каталоге **testshared**:

```
# chmod 770 /home/testshared
```

8.

Снова войдите в систему как пользователь **test1**, вернитесь в каталог **/home/testshared** и попробуйте создать файл в новом каталоге. Все идет нормально.

```
$ cd /home/testshared  
$ date >> test.txt  
$ ls -l test.txt
```

9. Удалите все разрешения для других пользователей для новых файлов в каталоге **/home/testshared**:

```
# chmod o-rwx /home/testshared/*
```

10. Теперь с помощью следующей команды проверьте владение новым файлом. Как вы думаете, другие пользователи в группе **tg1** могут получить доступ к этому файлу? Если сомневаетесь, войдите как пользователь **test2** и убедитесь сами.

```
$ ls -l
```

11. Из корневой учетной записи (**root**) установите бит **SGID** в каталоге:

```
# chmod g + s /home/testshared
```

(Да, если вы настроены на эффективность, вы можете знать, что команда **chmod 2770 /home/testshared** сочетает в себе эффект этой и предыдущих команд **chmod**.)

12. Вернитесь к учетной записи **test1**, вернитесь в каталог **/home/testshared** и создайте другой файл. Удалите разрешения для других пользователей во вновь созданном файле. Проверьте владение вновь созданным файлом. Вы думаете, что пользователь **test2** теперь может получить доступ к этому файлу? (Чтобы убедиться в этом, попробуйте это из учетной записи **test2**.)

```
$ date >> testb.txt  
$ chmod o-rwx /home/testshared/testb.txt  
$ ls -l
```

13. Теперь войдите в систему под учетной записью **test2**. Перейдите в каталог **/home/testshared**. Попробуйте получить доступ к файлу **testb.txt**. Создайте другой файл и затем используйте **ls -l**, чтобы снова проверить права доступа и владельца. (Чтобы

убедиться, что это работает, попробуйте получить доступ к этому файлу из учетной записи **test1**.)

14. Переключитесь на учетную запись **test3** и проверьте, может ли этот пользователь создавать файлы в этом каталоге и может ли этот пользователь просматривать файлы в этом каталоге.

РЕЗЮМЕ СЕРТИФИКАЦИИ

Вы можете управлять пользователями и группами с помощью файлов набора теневого паролей. Эти файлы могут быть изменены напрямую с помощью таких команд, как **useradd** и **groupadd** или инструмент **User Manager**. Способ настройки пользователей основан на файле **/etc/login.defs**. Любые переменные или общесистемные настройки определены в **/etc/bashrc** или **/etc/profile**. Они могут быть изменены файлами в домашних каталогах пользователей.

Есть несколько способов ограничить использование административных привилегий. Возможность входа в систему можно регулировать в таких файлах, как **/etc/securetty** и **/etc/security/access.conf**. Доступ к команде **su** может быть ограничен с помощью **PAM**. Частичные и полные административные привилегии можно настроить для команды **sudo** в файле **/etc/sudoers**.

Вы можете использовать централизованное управление учетными записями сети со службой **LDAP**. Системы **RHEL 7** можно настроить как клиент **LDAP** с помощью **/etc/nslcd.conf**, файлы **/etc/openldap/ldap.conf** и **/etc/nsswitch.conf**.

По умолчанию **Red Hat Enterprise Linux** назначает каждому новому пользователю уникальные идентификационные номера пользователей и групп. Это известно как схема частной группы пользователя. Эта схема поддерживает настройку специальных групп для определенного набора пользователей. Пользователи в группе могут быть настроены с привилегиями чтения и записи в выделенном каталоге, благодаря биту **SGID**.

Пару минут тренировки

Вот некоторые из ключевых моментов целей сертификации в главе 8.

Управление учетной записью пользователя

- После установки система может иметь только одну учетную запись для входа: **root**. На ежедневные операции, лучше всего создать одну или несколько обычных учетных записей.
- Набор теневого паролей настраивается в **/etc/passwd**, **/etc/shadow**, Файлы **/etc/group** и **/etc/gshadow**.
- Администраторы могут добавлять учетные записи пользователей и групп, напрямую редактируя файлы и теневые пароли или такие команды, как **useradd** и **groupadd**. Путь добавленные учетные записи определяются файлом **/etc/login.defs**.
- Учетные записи могут быть добавлены с помощью инструмента **Red Hat User Manager**. Вы также можете использовать этот инструмент или связанные команды, такие как **chage** и **usermod**, чтобы изменить параметры другой учетной записи.

Административный контроль

- Вход в систему от имени пользователя **root** может регулироваться файлом **/etc/securetty**.
- Как правило, вход в систему можно регулировать с помощью файла **/etc/security/access.conf**.
- Доступ к команде **su** можно регулировать с помощью файла **/etc/pam.d/su**.
- Настраиваемые права администратора можно настроить в файле **/etc/sudoers**.

Конфигурация пользователя и оболочки

- Домашний каталог для новых учетных записей для входа в систему заполняется из каталога **/etc/skel**.
- Каждый пользователь имеет среду при входе в систему, основанную на **/etc/bashrc**, **/etc/profile** и скрипты в **/etc/profile.d/**.
- Все пользователи имеют скрытые файлы конфигурации оболочки в своих домашних каталогах.

Пользователи и сетевая аутентификация

- **LDAP** позволяет вам настроить одно централизованно управляемое имя пользователя и пароль база данных с другими системами **Linux** и **Unix** в локальной сети.
- Клиенты **LDAP** настраиваются в **/etc/openldap/ldap.conf** и в **/etc/nslcd.conf**. (для демона **nslcd**) или **/etc/sss/sss.conf** (для **SSSD**).
- Необходимо внести изменения в **/etc/nsswitch.conf**, чтобы система выглядела удаленно база данных аутентификации, такая как **LDAP**.
- **Red Hat** включает в себя **authconfig-gtk** и **authconfig-tui**, два инструмента с графическим интерфейсом и консолью это может помочь вам настроить систему в качестве клиента **LDAP** или **IPA**.

Специальные группы

- Схема закрытой группы пользователей **Red Hat** настраивает пользователей на своих собственных уникальных пользователей и идентификационные номера группы.
- При наличии соответствующих разрешений **SGID** вы можете настроить общий каталог для конкретной группы пользователей.
- Установка бита **SGID** проста; используйте **chown**, чтобы никого не указывать в качестве владельца пользователя и название группы как владельца группы. Затем выполните команду **chmod 2770** на общий каталог.

САМОПРОВЕРКА

Следующие вопросы помогут оценить ваше понимание материалов, представленных в этой главе. Поскольку на экзаменах Red Hat не появляется вопросов с несколькими вариантами ответов, вопросы с несколькими вариантами ответов не отображаются в этой книге. Эти вопросы исключительно проверяют ваше понимание главы. Это нормально, если у вас есть другой способ выполнения задачи. Получение результатов, а не запоминание пустяков - вот на что рассчитывает Red Hat Экзамены. На многие из этих вопросов может быть более одного ответа.

Управление учетной записью пользователя

1. Какой стандартный минимальный идентификационный номер пользователя для обычных пользователей в дистрибутивах **Red Hat**?

2. Какая команда в текстовой консоли на основе графического интерфейса запускает **Red Hat User Manager**?

Административный контроль

3. Какой файл регулирует локальные консоли, где пользователь **root** может войти в систему?

4. Какой файл управляет командами, которые пользователь может запускать с правами **root** или другой пользователь?

5. Когда обычный пользователь использует команду **sudo** для запуска административной команды, какой пароль необходим?

Конфигурация пользователя и оболочки

6. Если вы хотите добавить файлы в каждую новую учетную запись пользователя, какой каталог вы должны использовать?

7. Какие системные файлы конфигурации связаны с **оболочкой bash**?

Пользователи и сетевая аутентификация

8. Если пользовательские объекты находятся в подразделении с именем «**People**», в другом организационная единица с именем «**Global**», которая является частью домена **LDAP** **dc=example, dc=org**, что такое **DN** базы поиска **LDAP**?

9. Какой полный путь к файлу, который ссылается на базу данных **LDAP** для аутентификации?

Специальные группы

10. Какая команда установит бит **SGID** в каталоге **/home/developer**?

11. Какая команда настроит владельца группы разработчиков на **/home/developer** каталог?

12. Какая команда добавит пользователя альфа в группу разработчиков? (Этот вопрос предполагает Альфа-пользователь и группа разработчиков уже существуют, и эта альфа не принадлежит ни одной группе, кроме его собственного.)

Лабораторная работа

Во время экзаменов **Red Hat** задания будут представлены в электронном виде. Таким образом, эта книга также представляет большинство лабораторий в электронном виде. Для получения дополнительной информации см. Раздел «Лабораторные вопросы» в конце главы 8. Большинство лабораторных работ для этой главы просты и требуют очень небольшого количества команд или изменений в одном или двух файлах конфигурации.

Лаборатория 1

Для этой лабораторной работы создайте нового пользователя с именем **newguy**. Убедитесь, что пользователь является членом группы пользователей. Создайте второго пользователя с именем **intern**. Создайте специальную группу с именем **peons** и сделайте обоих новых пользователей членами этой группы. Присвойте **GID 123456** этой группе.

Лаборатория 2

В этой лабораторной работе корневому администратору будет немного сложнее войти в любую консоль. Внесите все необходимые изменения, чтобы ограничить локальный доступ от пользователя **root** к шестой виртуальной консоли.

Лаборатория 3

Создайте нового пользователя с именем **senioradm**. Настройте этого пользователя с полными привилегиями **sudo**. Тем не менее, пользователю **senioradm** все равно необходимо ввести пароль своей обычной учетной записи, прежде чем ему разрешат выполнить административную команду.

Лаборатория 4

Создайте нового пользователя с именем **junioradm**. Настройте этого пользователя с правами на запуск команды **fdisk** с помощью **sudo**. В этом случае пользователю **junioradm** по-прежнему необходимо ввести пароль своей обычной учетной записи, прежде чем он сможет запустить команду **fdisk**.

Лаборатория 5

Убедитесь, что все новые пользователи получают копию подкаталога **info-** * каталога **/usr/share/doc**, включая все находящиеся в нем файлы, в своем домашнем каталоге. Проверьте результат, создав нового пользователя с именем **infouser** с помощью команды **useradd** и диспетчера пользователей.

Лаборатория 6

В этой лаборатории вы создадите частный каталог для группы инженеров, проектирующих некоторые камбузы. Вы хотите создать группу под названием «**galleys**» для

инженеров по имени Майк, Рик, Терри и Мариам(**mike, rick, terri, and maryam.**). Они захотят поделиться файлами в каталоге **/home/galley**. Что нужно сделать?

ТЕСТОВЫЕ ОТВЕТЫ

Управление учетной записью пользователя

1. Минимальный идентификационный номер пользователя для обычных пользователей в дистрибутивах Red Hat составляет **1000**.
2. Команда в текстовой консоли на основе графического интерфейса, которая запускает Red Hat User Manager:
authconfig-gtk или **system-config-users**.

Административный контроль

3. Файл, который регулирует локальные консоли, где пользователь **root** может войти в систему, находится в **/etc/securetty**.
4. Файл, управляющий тем, какие команды пользователь может запускать с правами **root** или другого пользователя. **/etc/sudoers**.
5. Когда обычный пользователь использует команду **sudo** для запуска административной команды, требуется пароль этого пользователя, если только директива **NOPASSWD** не была указана в **/etc/sudoers**.

Конфигурация пользователя и оболочки

6. Чтобы автоматически добавлять файлы в каждую новую учетную запись пользователя, вы должны использовать каталог **/etc/skel**.
7. Общесистемными файлами конфигурации, связанными с оболочкой **bash**, являются **/etc/bashrc**, **/etc/profile**, и сценарии в **/etc/profile.d/**.

Пользователи и сетевая аутентификация

8. DN базы поиска **LDAP**: **ou=People,ou=Global,dc=example,dc=org**.
9. Полный путь к файлу, который указывает на базу данных для аутентификации, - **/etc/nsswitch.conf**.

Специальные группы

10. Команда, которая установит бит **SGID** в каталоге **/home/developer**, имеет вид **chmod g+s /home/developer**. Числовые параметры, такие как **chmod 2770 /home/developer**, неверны, так как они выходят за рамки простой установки бита **SGID**.
11. Команда, которая устанавливает владельца группы разработчиков в каталоге **/home/developer**, имеет вид **chgrp** разработчик **/home/developer**.
12. Команда, которая добавляет пользователя **альфа** в группу разработчиков, является **usermod -aG developer alpha**.

ЛАБ ОТВЕТЫ

Лаборатория 1

Существует несколько методов создания новых пользователей и групп, но все они должны тот же результат.

1. Вывод команды **ls -l /home** должен включать следующий вывод, заменяя сегодняшняя дата:

```
drwx-----. 4 newguy newguy 4096 Jan 19 12:13 newguy
drwx-----. 4 intern intern 4096 Jan 19 12:13 intern
```

2. Запустите команду **ls -la /etc/skel**. Вывод должен включать в себя ряд скрытых файлов, принадлежащих пользователем **root** и группой **root**.

3. Запустите команды **ls -la /home/newguy** и **ls -la /home/intern**. Вывод должен включать те же скрытые файлы, что и в **/etc/skel**, но принадлежат пользователям, связанным с каждым **home** каталогом.

4. Конец файлов **/etc/passwd** и **/etc/shadow** должен содержать записи для обоих пользователей. Если вы установить пароль для этих пользователей, он должен быть в зашифрованном виде во втором столбце **/etc/shadow**.

5. Следующая запись должна существовать где-то в середине файла **/etc/group**. Это приемлемо если другие пользователи включены в конце строки. **users:x:100:newguy**

6. Следующая строка должна быть рядом или в конце файла **/etc/group**; порядок пользователей в четвертый столбец не имеет значения.

```
peons:x:123456:newguy,intern
```

Лаборатория 2

Самый простой способ ограничить вход в систему **root** шестой виртуальной консолью - в файле **/etc/securetty**. Единственные активные директивы в этом файле должны быть

```
vc/6
tty6
```

Конечно, в Linux есть и другие способы сделать что угодно. Чтобы попробовать это, нажмите **Ctrl-Alt-F1** и попробуйте войти в систему как пользователь **root**. Нажмите **ctrl-alt-f2** и повторите процесс через **виртуальный терминал 6**.

Лаборатория 3

Используйте ответ на первую часть лабораторной работы 1 в качестве руководства для проверки прав собственности и разрешений Каталог **/home/senioradm** вместе с файлами в нем. Что касается привилегий **sudo**, вы должны добавить следующую строку в файле **/etc/sudoers** используя **visudo**:

```
senioradm ALL = (ALL) ALL
```

Чтобы проверить результат, войдите в систему как пользователь **senioradm** и выполните административную команду, перед которой стоит **sudo**. Например, попробуйте следующую команду:

```
# sudo firewall-config
```

Если вы не запустили команду **sudo** в последние несколько минут, это действие запросит пароль. Введите пароль, созданный для пользователя **senioradm**. Он должен открыть инструмент настройки брандмауэра.

Лаборатория 4

Используйте ответ для лабораторной работы 1 в качестве руководства для проверки владения и разрешений для **/home/junioradm** каталог, вместе с файлами в нем. Что касается

привилегий **sudo**, вы должны добавить следующую строку в файле **/etc/sudoers** используя команду **visudo**:

junioradm ALL=/usr/sbin/fdisk : :

Далее попробуйте выполнить команду **fdisk**:

\$ sudo /usr/sbin/fdisk -l

Вам будет предложено ввести пароль. Введите пароль, созданный для пользователя **junioradm**. Если только пароли идентичны, пароль **root** не будет работать. В случае успеха, вы должны увидеть список разделов для подключенных дисков на выходе.

Лаборатория 5

Используйте ответ для лабораторной работы 1 в качестве руководства для проверки прав собственности и прав доступа к **/home/infouser** каталог, вместе с файлами в нем. Если вы добились успеха, этот каталог будет содержать **info-*/**подкаталог. Кроме того, каталог **/etc/skel** должен содержать подкаталог **info-*/**. Тот Подкаталог должен иметь те же файлы, что и в каталоге **/usr/share/doc/info-***. Конечно, это работает, только если вы копируете содержимое подкаталога **info-*** / из **/usr/share/doc** каталога в **/etc/skel**.

Лаборатория 6

Это простой процесс, использующий следующие основные шаги:

1. При необходимости создайте учетные записи для **mike, rick, terri, and maryam**. Вы можете использовать **useradd** введите команду, отредактируйте файл **/etc/passwd** напрямую или используйте Менеджер пользователей.
2. Настройте группу для этих пользователей. Настройте идентификатор группы вне диапазона обычных пользователей в **/etc/group** с такой строкой:

galley:x:88888:mike,rick,terri,maryam

3. Создайте каталог **/home/galley**. Дайте ему надлежащее право собственности и разрешения следующими командами:

```
# mkdir /home/galley
# chown nobody.galley
# chmod 2770 /home/galley
```