

Глава 15

Файловый сервер Samba

ЦЕЛИ СЕРТИФИКАЦИИ

15.01 Самба Сервис

15.02 Samba как клиент

15.03 Устранение неполадок Samba

✓ Двухминутная тренировка

Q&A Самопроверка

Samba - это реализация **Linux** сетевых протоколов, используемых для подключения операционных систем **Microsoft**. В сети компьютеров **Microsoft Windows** общий доступ к файлам основан на Общей файловой системе Интернета (**Common Internet File System CIFS**), которая была разработана на основе протокола **Server Message Block (SMB)**. **Samba** был разработан как свободно доступный **SMB**-сервер для всех связанных с **Unix** операционных систем, включая **Linux**, и был обновлен для поддержки **CIFS**.

Samba взаимодействует с **CIFS** настолько прозрачно, что клиенты **Microsoft** не могут отличить ваш сервер **Linux** от подлинного сервера **Windows**. Поскольку **Samba** работает только на компьютерах с **Linux**, лицензии на доступ к серверу, клиенту или клиенту отсутствуют. Если вы можете научиться редактировать основной файл конфигурации **Samba** из интерфейса командной строки, вы можете быстро настроить **Samba**.

Научитесь тестировать сетевые сервисы, такие как **Samba**. Это сервисы, которые вы можете настроить и/или устранить неисправности на экзаменах **Red Hat**. Потратьте некоторое время, чтобы понять файлы конфигурации, связанные с каждой из этих служб, и попрактикуйтесь, чтобы они работали в разных системах **Linux**. В некоторых случаях две или более систем, работающих под управлением **Linux**, будут полезны для практического изучения того, что вы изучите в этой главе.

Внутри экзамена

В этой главе непосредственно рассматриваются две цели **RHCE**, связанные со службами файловой системы **Samba**. Когда вы закончите работу с этой главой, вы узнаете, как

- Предоставлять сетевые ресурсы для конкретных клиентов
- Предоставлять сетевые ресурсы, подходящие для совместной работы в группах.

С **Samba** связь с клиентами **Microsoft** проходит без проблем. Однако, поскольку у вас может не быть доступа к **Microsoft Windows** во время экзаменов **Red Hat**, вы увидите, как **Samba** беспрепятственно связывается с другими клиентами **Linux**. Общие ресурсы могут быть ограничены определенными клиентами с **Samba** и другими параметрами безопасности.

Samba также обеспечивает поддержку совместной работы групп, как это делает **Apache** в главе 14. Принципы те же, что и у групповых директорий, настроенных в **Linux** в главе 8.

Не забывайте стандартные требования для всех сетевых сервисов, которые обсуждались в главах 10 и 11. Для обзора вам необходимо установить сервис, настроить его работу с **SELinux**, убедиться, что он запускается при загрузке, настроить сервис для базовой работы и настроить безопасность пользователей и хостов.

ЦЕЛЬ СЕРТИФИКАЦИИ 15.01

Samba Services

CIFS от **Microsoft** был построен по протоколу **SMB**. **SMB** был разработан в 1980-х годах **IBM**, **Microsoft** и **Intel** для обмена файлами и принтерами по сети.

Поскольку **Microsoft** превратила **SMB** в **CIFS**, разработчики **Samba** соответственно обновили **Samba**. Службы **Samba** предоставляют стабильную, надежную, быструю и высоко совместимую службу обмена файлами и принтерами, которая позволяет вашему компьютеру выступать в роли клиента,

рядового сервера, основной контроллер домена (**PDC**) или член службы **Active Directory (AD)** в сетях на базе **Microsoft**.

!!!! On the job !!!!

С выпуском Samba версии 4.0 вы теперь можете настроить Samba для работы в качестве контроллера домена **AD (DC)** в сети на базе **Microsoft**. Хотя конфигурация контроллера домена выходит за рамки экзамена **RHCE**, это важный навык для многих системных администраторов. **!!!!!!**

Samba легко настроить для выполнения ряда задач в сети на базе **Microsoft**. Вот некоторые примеры:

- Участие в **рабочей группе Microsoft Windows** или домене в качестве клиента, рядового сервера или даже **PDC**.
- Укажите имя пользователя/пароль и предоставьте общий доступ к базам данных каталогов локально, либо с другого сервера **Samba**, либо с **Windows PDC**.
- Настройте локальные каталоги, как общие файловые системы **SMB**.

Самба может сделать больше, но вы поняли. Функции **Samba** настраиваются через один очень большой файл **smb.conf** в каталоге **/etc/samba**. Хотя этот файл может запугать некоторых пользователей, прочтите комментарии в нем. Вы можете быть удивлены тем, что вы можете сделать с **Samba**!

!!!! EXAM Watch !!!!

В **RHEL7 Red Hat** больше не включает инструменты с графическим интерфейсом для настройки **Samba**. Вам придется редактировать файл конфигурации **Samba** напрямую. К счастью, файл конфигурации **/etc/samba/smb.conf** по умолчанию содержит много полезных комментариев и предлагаемых директив. **!!!!**

Установите службы **Samba**

Процесс установки **Samba** отличается от других серверов. Пакеты **Samba** не организованы в одну группу пакетов. Хотя все, что вам нужно для настройки сервера **Samba** - это **RPM-пакет Samba** (и его зависимости), вы найдете и другие полезные пакеты **Samba**. Важные пакеты **Samba** описаны в Таблице 15-1.

ТАБЛИЦА 15-1 Пакеты Samba

RPM пакет	Описание
samba	Включает базовое программное обеспечение SMB-сервера для обмена файлами и принтерами.
samba-client	Предоставляет утилиты, необходимые для подключения к общим папкам и принтерам SMB/CIFS .
samba-common	Содержит общие файлы Samba , используемые как клиентом, так и сервером.
samba-dc	Включено в RHEL Server Дополнительный репозиторий; обеспечивает интеграцию с Active Directory .
samba-libs	Содержит библиотеки, необходимые для других пакетов программного обеспечения Samba .
samba-python	Содержит модули Python , необходимые для других пакетов программного обеспечения Samba .
samba-winbind	Предоставляет демон Winbind , который позволяет Samba быть рядовым сервером в доменах на основе Microsoft и поддерживает пользователей Windows на серверах Linux .
samba-winbind-krb5-locator	Включено в RHEL Server Дополнительный репозиторий; позволяет локальной библиотеке Kerberos использовать тот же KDC , что и Samba .
samba-winbind-modules	Обеспечивает клиентское соединение с демоном Winbind через PAM и сетевой сервисный коммутатор (NSS).

Некоторое прошлое Samba

Сервисы **Samba** обеспечивают взаимодействие между системами **Microsoft Windows** и **Linux/Unix**. Перед настройкой Samba вам необходимо понять, как работает сеть **Microsoft Windows** с **TCP/IP**.

Первоначальные сети **Microsoft Windows** были настроены с именами компьютеров, известными как имена **NetBIOS**, с ограничением в 15 символов. Эти уникальные имена хостов обеспечивали простую систему плоских имен компьютеров для компьютеров в локальной сети.

Все запросы на идентификацию компьютеров были сделаны через трансляции. Эта общая сетевая транспортная система была известна как расширенный пользовательский интерфейс **NetBIOS** (**NetBEUI**) и не была «маршрутизируемой». Другими словами, она не позволяла осуществлять связь между различными сетями. В результате администраторы могли настроить только 100–200 узлов в исходных сетях ПК на базе **Microsoft**.

Microsoft нужно было решение для маршрутизации информации между сетями. Они могли бы использовать стек протоколов **Novell IPX/SPX**, но этого было недостаточно. По мере роста Интернета **Microsoft** требовался стандарт, совместимый с **TCP/IP**. **Microsoft** адаптировала свою систему **NetBIOS** для **TCP/IP** с **SMB**. Так как **Microsoft** опубликовала **SMB** как общепромышленный стандарт, любой мог настроить свой собственный сервис для работы с ним. По мере продвижения **Microsoft** к **CIFS** разработчики **Samba** адаптировались к изменениям.

Одной из особенностей сетей **Windows** является служба браузера. Все компьютеры регистрируют свои имена **NetBIOS** с помощью одного «избранного» главного (**master**) браузера, хранителя базы данных сетевых служб. Фактически, база данных просмотра поддерживается некоторым избранным хостом для каждого протокола, работающего в сети на основе **Microsoft**. Например, если протоколы **NetBEUI** и **TCP/IP** были установлены на хосте, то потребовались две дублированные базы данных просмотра - по одной на протокол - потому что доступные сервисы могут отличаться для разных протоколов.

Порты, межсетевые экраны и Samba

Samba, как сервис и клиент требует доступа через несколько сетевых портов. Чтобы включить связь через локальный брандмауэр для сервера **Samba**, выполните следующие команды:

```
# firewall-cmd --permanent --add-service=samba
# firewall-cmd --reload
```

Для клиентов **Samba** вам необходимо включить следующую службу **firewalld**:

```
# firewall-cmd --permanent --add-service=samba-client
# firewall-cmd --reload
```

Конфигурация соответствующих служб **firewalld** определена в файлах **samba.xml** и **samba-client.xml**, расположенных в каталоге **/usr/lib/firewalld/services**. Как показано на рисунках 15-1 и 15-2, серверу **Samba** требуется четыре открытых порта, тогда как службе клиента Samba требуется только два открытых порта.

Вы заметите, что два открытых порта связаны с протоколом пользовательских дейтаграмм (**UDP**), который не основан на соединении. Поэтому для отслеживания локально исходящих запросов **NetBIOS** и разрешения пакетов, соответствующих соответствующему возвращаемому трафику, через брандмауэр, службы **Samba** и **Samba Client** используют вспомогательный модуль **firewalld** **ns_conntrack_netbios_ns**.

Порты **TCP** и **UDP**, необходимые для клиента **Samba**, показаны в таблице 15-2. В совокупности службы, которые прослушивают порты 137–139, связаны с обменом данными **NetBIOS** через **TCP/IP** (**NBT**).

РИСУНОК 15-1 Файл конфигурации для службы Samba firewalld

```
[root@server1 ~]# cat /usr/lib/firewalld/services/samba.xml
<?xml version="1.0" encoding="utf-8"?>
<service>
  <short>Samba</short>
  <description>This option allows you to access and participate in Windows file
and printer sharing networks. You need the samba package installed for this opti
on to be useful.</description>
  <port protocol="udp" port="137"/>
  <port protocol="udp" port="138"/>
  <port protocol="tcp" port="139"/>
  <port protocol="tcp" port="445"/>
  <module name="nf_conntrack_netbios_ns"/>
</service>
[root@server1 ~]# █
```

РИСУНОК 15-2 Файл конфигурации для службы Samba Client firewalld

```
[root@server1 ~]# cat /usr/lib/firewalld/services/samba-client.xml
<?xml version="1.0" encoding="utf-8"?>
<service>
  <short>Samba Client</short>
  <description>This option allows you to access Windows file and printer sharing
networks. You need the samba-client package installed for this option to be use
ful.</description>
  <port protocol="udp" port="137"/>
  <port protocol="udp" port="138"/>
  <module name="nf_conntrack_netbios_ns"/>
</service>
[root@server1 ~]# █
```

ТАБЛИЦА 15-2 Коммуникационные услуги Samba

Порт/Протокол	Описание
137/UDP	Служба имен NetBIOS
138/UDP	Служба дейтаграмм NetBIOS
139/TCP	Служба сеансов NetBIOS
445/TCP	Samba по TCP/IP

Настройте логические выражения SELinux для Samba

Несколько директив связаны с работой сервера **Samba** с **SELinux** в targeted режиме, как описано в таблице 15-3. Возможно, вам придется активировать одно или несколько логических значений для поддержки различных функций **Samba**. Хотя это может показаться повторяющимся для некоторых читателей, **SELinux** не очень хорошо понимают даже многие эксперты по **Linux**.

Если вы хотите разрешить **Samba** обмениваться локальными домашними каталогами с другими пользователями в сети, выполните следующую команду:

```
# setsebool -P samba_enable_home_dirs 1
```

-P гарантирует, что изменение переживет перезагрузку.

Если вам необходимо настроить каталоги для совместного использования с другими службами, целесообразно включить логическое значение **samba_export_all_ro** или **samba_export_all_rw**. Например, файлы, к которым открыт общий доступ через веб-сервер **Apache**, должны быть помечены контекстом файла **httpd_sys_content_t**.

Однако для **Samba** требуется другой контекст **SELinux** для файлов и каталогов, **samba_share_t**. Чтобы разрешить **Samba** доступ к файлам, которые не имеют метки **samba_share_t**, необходимо включить логическое значение **samba_export_all_ro** или **samba_export_all_rw**.

Настроить контексты файлов SELinux для Samba

Обычно **Samba** может предоставлять общий доступ только к тем файлам и каталогам, которые помечены типом файла **samba_share_t**. Однако тип файла **samba_share_t** не требуется, если включены логические значения **samba_export_all_ro** или **samba_export_all_rw**. Это также не требуется, если файлы помечены как **public_content_rw_t** или **public_content_t**, а логическое значение **smbd_anon_write** включено.

Однако включение **samba_export_all_rw** может быть угрозой безопасности, поскольку это позволит **Samba** совместно использовать все каталоги независимо от их контекста **SELinux**. Таким образом, в большинстве случаев вы хотите пометить каталоги (и файлы в них) контекстом **SELinux samba_share_t**, выполнив следующую команду:

```
# chcon -R -t samba_share_t /share
```

Кроме того, чтобы изменения остались в силе с **SELinux**, вам нужно изменить политику контекста файла по умолчанию, определенную в файле **file_contexts.local** в каталоге **/etc/selinux/target/contexts/files**. Это может быть достигнуто с помощью такой команды:

```
# semanage fcontext -a -t samba_share_t '/share(/.*)?'
```

ТАБЛИЦА 15-3 Samba SELinux Booleans

Директивы для определения логических значений Samba	Описание
cdrecord_read_content	Позволяет команде cdrecord читать общие каталоги Samba (и других сетей)
ksmtuned_use_cifs	Позволяет KSM (сервис, который сокращает идентичные страницы памяти в одну страницу) доступ к файловым системам CIFS
samba_create_home_dirs	Поддерживает создание домашних каталогов, обычно через pam_mkhome.so PAM модуль
samba_domain_controller	Позволяет Samba выступать в качестве контроллера домена для управления аутентификацией
samba_enable_home_dirs	Включает общий доступ к домашним каталогам пользователей.
samba_export_all_ro	Настраивает доступ только для чтения к любому каталогу, даже без метки типа файла samba_share_t
samba_export_all_rw	Настраивает доступ на чтение/запись к любому каталогу, даже без метки типа файла samba_share_t
samba_portmapper	Позволяет Samba выступать в роли portmapper
samba_run_unconfined	Поддерживает выполнение неограниченных сценариев из каталога /var/lib/samba/scripts
samba_share_fusefs	Позволяет Samba совместно использовать файловые системы, смонтированные через fusefs , например, файловые системы GlusterFS
samba_share_nfs	Обеспечивает совместное использование файловых систем NFS из Samba
smbd_anon_write	Позволяет Samba изменять файлы в общедоступных каталогах, настроенных с помощью контекстов SELinux public_content_rw_t и public_content_r_t
sanlock_use_samba	Позволяет sanlock (диспетчер блокировки общего хранилища) получать доступ к файловым системам CIFS
use_samba_home_dirs	Поддерживает использование удаленного сервера Samba для локальных домашних каталогов
virt_sandbox_use_samba	Позволяет контейнерам песочницы получать доступ к файловым системам CIFS
virt_use_samba	Позволяет виртуальной машине получать доступ к файлам, смонтированным в файловой системе CIFS

Samba Демоны

Совместное использование каталогов и принтеров в сети в стиле **Microsoft** требует нескольких демонов и ряда связанных команд. Работая вместе, команды могут помочь настроить **Samba**, а демоны помогают ему обмениваться данными через различные коммуникационные порты, описанные ранее в этой главе.

Samba включает в себя команды, которые запускают службу, а также помощь в настройке. Наиболее важными из этих команд являются двоичные файлы в каталоге **/usr/sbin**, которые запускают различные службы **Samba**.

Для запуска **Samba** необходимы два демона: основная служба **Samba (smbd)** и служба имен **NetBIOS (nmbd)**. Кроме того, некоторые администраторы могут захотеть запустить службу **Winbind (winbindd)** для разрешения имен пользователей и хостов. Это обеспечивается **RPM-пакетом samba-winbind**. Все три демона настраиваются через файл конфигурации **/etc/samba/smb.conf**.

Если вы хотите быть уверенными, что службы будут запущены при следующей загрузке **Linux**, выполните следующую команду:

```
# systemctl enable smb nmb winbind
```

Вы можете запустить связанные демоны **smbd**, **nmbd** и **winbindd** с помощью следующей команды:

```
# systemctl start smb nmb winbind
```

Команда **systemctl** может помочь вам подтвердить, как работает демон. Например, команда, показанная на **рисунке 15-3**, подтверждает, что служба **Samba** работает с основным **PID 14691**.

РИСУНОК 15-3 Отображение информации о состоянии сервиса smb

```
[root@server1 rhel7]# systemctl status smb
smb.service - Samba SMB Daemon
  Loaded: loaded (/usr/lib/systemd/system/smb.service; disabled)
  Active: active (running) since Mon 2015-05-04 11:29:46 BST; 1min 20s ago
  Main PID: 14691 (smbd)
  Status: "smbd: ready to serve connections..."
  CGroup: /system.slice/smb.service
          └─14691 /usr/sbin/smbd
             └─14692 /usr/sbin/smbd

May 04 11:29:46 server1.example.net systemd[1]: Starting Samba SMB Daemon...
May 04 11:29:46 server1.example.net smbd[14691]: [2015/05/04 11:29:46.609245...]
May 04 11:29:46 server1.example.net systemd[1]: Started Samba SMB Daemon.
Hint: Some lines were ellipsized, use -l to show in full.
[root@server1 rhel7]# █
```

Глобальная конфигурация сервера Samba

Вы можете настроить сервер **Samba** через основной файл конфигурации **Samba**, **/etc/samba/smb.conf**. Этот файл длинный и содержит ряд директив, которые требуют некоторого понимания концепций, связанных с сетью **Microsoft Windows**. К счастью, версия этого файла по умолчанию также содержит полезную документацию с предложениями и полезными опциями.

Файл конфигурации **Samba** по умолчанию включает в себя ряд некомментируемых закомментированных директив. Значение по умолчанию для таких директив можно найти на странице руководства для файла **smb.conf**.

Прежде чем редактировать этот файл, изучите его содержимое. Как только вы поймете, как устроен файл, создайте его резервную копию и попробуйте изменить файл напрямую. Проверьте синтаксис **smb.conf** с помощью команды **testparm**. Проверьте результат ваших изменений, перезагрузив сервер **Samba** с помощью следующей команды:

```
# systemctl reload smb
```

Чтобы помочь вам в этом процессе, мы проанализируем версию этого файла по умолчанию для **RHEL 7**. Далее приведены выдержки из этого файла. В некоторых случаях мы заменяли комментарии в

файле нашими собственными объяснениями. Вы также можете просмотреть свой собственный файл `/etc/samba/smb.conf`.

Файл **smb.conf** содержит два типа строк комментариев. Символ хеша (#) используется в качестве общего текстового комментария. Обычно это словоблудие, которое описывает функцию. Вторым символом комментария является точка с запятой (;), используемая для комментирования директив **Samba** (которую вы можете позже раскомментировать, чтобы включить функцию). (Обратите внимание, что физические размеры этой книги ограничивают длину строк кода. В некоторых случаях мы немного изменили строки кода, чтобы соответствовать этому ограничению, не меняя намерения какой-либо команды в этом файле конфигурации.)

```
# This is the main Samba configuration file. For detailed information
# about the options listed here, refer to the smb.conf(5) manual page.
# Samba has a huge number of configurable options, most of which are
# not shown in this example.
# Note: Run the "testparm" command after modifying this file to check
# for basic syntax errors.
```

Хотя вам необходимо знать, что можно сделать с различными глобальными настройками, вам следует как можно меньше менять. Чем меньше вы меняете, тем меньше, что то может пойти не так. Идеальные файлы конфигурации не требуются. Необходимы Файлы конфигурации, соответствующие определенным требованиям экзамена или работы.

!!!! Exav watch !!!!

Как указано в руководстве по подготовке к экзамену Red Hat, RHCE должны иметь возможность настраивать различные службы, включая Samba, для базовой работы. Некоторые детали версии по умолчанию основной конфигурации Samba выходят за рамки базовой операции. !!!!!

Файл **smb.conf** можно разбить на разные разделы. После первого набора комментариев это еще один закомментированный блок с описанием из наиболее важных логических **SELinux** и файловые контексты, связанные с **Samba**. Из-за нехватки места мы показываем только первые строки этого раздела. Прочтите все комментарии файла **smb.conf**, потому что они являются очень полезным источником информации:

```
#Security-Enhanced Linux (SELinux) Notes:
#
# Turn the samba_enable_home_dirs Boolean on if you want to share home
# directories via Samba. Run the following command as the root user to turn
# this boolean on:
# setsebool -P samba_enable_home_dirs on
#
# If you create a new directory, such as a new top-level directory, label it
# with samba_share_t so that SELinux allows Samba to read and write to it. Do
# not label system directories, such as /etc/ and /home/, with samba_share_t,
# as such directories should already have an SELinux label.
```

Затем есть раздел глобальных настроек, который определяет общие атрибуты сервера. Этот раздел начинается со следующих двух строк:

```
#===== Global Settings=====
[global]
```

Теперь изучите глобальные настройки, которые следуют. Во-первых, если вы видите строку

```
##--authconfig--start-line--
```

это означает, что файл конфигурации был изменен с помощью **authconfig** или инструмента **system-config-authentication**.

Сетевые параметры

Прокрутите вниз до подраздела, озаглавленного

#----- Network Related Options -----

Изучите каждую из директив в этой части раздела «Глобальные настройки». Несмотря на имя, переменная рабочей группы может указывать имя рабочей группы или, чаще, домена. Однако, поскольку одноранговые рабочие группы были разработаны в первую очередь, рабочей группой **Samba** по умолчанию является **WORKGROUP**, которая в старых системах **Microsoft Windows** оказывается рабочей группой по умолчанию для одноранговой сети. На **RHEL 7** теперь установлено следующее значение:

workgroup = MYGROUP

Следующая строковая директива сервера становится комментарием, отображаемым с именем **NetBIOS** системы в видимом списке просмотра, где **Samba** заменяет номер версии на переменную **%v**:

server string = Samba Server Version %v

Рекомендуется добавить в этот файл имя **NetBIOS** для локальной системы. Ограниченный 15 символами, он может совпадать с именем хоста, используемым в системе. Это становится тем, что другие клиенты видят в списках просмотра по сети, например, те, которые отображаются с помощью команды **Microsoft net view** или команды **Linux smbclient**.

; netbios name = MYSERVER

Если локальная система подключена к нескольким сетям, вы можете указать интерфейсы, которые **Samba** должна слушать, с помощью директивы **interfaces**, как показано здесь. Конечно, устройства и сетевые адреса должны быть изменены соответствующим образом.

; interfaces = lo eth0 192.168.12.2/24 192.168.13.2/24

Если вы активируете директиву **hosts**, то это действие может разрешить доступ только к указанной сети. Следующее значение по умолчанию ограничит доступ к хостам в сетях 192.168.12.0/24 и 192.168.13.0/24, а также к локальному компьютеру (127.):

; hosts allow = 127. 192.168.12. 192.168.13.

Можно настроить директиву **deny hosts** аналогичным образом. С такими директивами вы можете настроить безопасность на основе хоста для **Samba**. В глобальном разделе такая защита будет применяться на всем сервере. Вы также можете использовать директивы **hosts allow** и **hosts deny** в определениях для отдельных общих каталогов, как описано далее в этой главе.

Затем директива **max protocol** указывает самый высокий уровень протокола, который будет поддерживать сервер **Samba**. По умолчанию это установлено на версию **Windows 7 SMB2**:

; max protocol = SMB2

Параметры ведения журнала

В следующем разделе настраиваются параметры ведения журнала, как указано в следующей строке:

#----- Logging Options -----

Директива файла журнала, как показано, устанавливает отдельные файлы журнала для каждого компьютера, который подключается к этому серверу **Samba**, на основе имени компьютера (**%m**). По умолчанию размер файла журнала ограничен **50 КБ**. Как следует из комментария, файлы журнала,

которые превышают заданный размер, перемещаются. Если журналы превышают этот размер, вы все равно увидите их в каталоге **/var/log/samba** с расширением **.old**.

```
# log files split per-machine
log file = /var/log/samba/log.%m
# maximum size of 50KB per log file, then rotate:
max log size = 50
```

Параметры автономного сервера

В следующем разделе настраиваются параметры безопасности на основе конфигурации в качестве автономного сервера:

```
#----- Standalone Server Options -----
```

Директива безопасности может быть немного запутанной. Стандартное значение директивы, как показано здесь, означает, что соединения проверяют локальную базу паролей. Это целесообразно при настройке этого компьютера в качестве контроллера домена (DC), в частности, основного контроллера домена (PDC).

```
security = user
```

Кроме того, вы можете настроить этот компьютер в качестве рядового сервера в домене для использования базы данных паролей от контроллера домена. В этом случае вы должны заменить следующую команду:

```
security = domain
```

!!!! On the job !!!!

Чтобы настроить систему Linux в качестве рабочей станции с общим каталогом в домене Microsoft, вам необходимо настроить компьютер в качестве рядового сервера в этом домене. !!!!

В качестве альтернативы, чтобы настроить систему в качестве члена домена в области служб Active Directory, введите следующую команду:

```
security = ads
```

Наконец, обратите внимание, что значения сервера и общего ресурса устарели. Подводя итог, можно выделить три основных варианта аутентификации: **user**, **domain**, и **ads**.

Теперь переориентируйте эту директиву на базу данных аутентификации. По умолчанию это **security = user**; не забудьте создать имена пользователей и пароли **Samba** для заполнения базы данных пользователей. Если база данных является локальной, это может быть одно из двух:

```
passdb backend = smbpasswd
```

или

```
passdb backend = tdbsam
```

База данных **smbpasswd** хранится в локальном каталоге **/etc/samba**. Параметр **tdbsam**, сокращенно от **Trivial Database Security Accounts Manager**, является рекомендуемым форматом базы данных и хранится в каталоге **/var/lib/samba/private**.

В качестве альтернативы для удаленной базы данных, такой как **LDAP**, вы можете активировать следующую директиву. Если сервер **LDAP** расположен в удаленной системе, этот адрес универсального идентификатора ресурса (**URI**) может быть включен сюда.

```
passdb backend = ldapsam
```

Если вы настроили **security=ads**, вы также захотите активировать следующую директиву, чтобы указать область **Active Directory (AD)**, заменив фактическую область **AD** на **MY_REALM**:

```
; realm = MY_REALM
```

Параметры контроллера домена

В следующем разделе поддерживается настройка системы в качестве контроллера домена, начиная со следующего комментария:

```
#----- Domain Controller Options -----
```

Дополнительная настройка требуется для сервера **Samba**, настроенного в качестве контроллера домена. Вкратце, эти параметры определяют роль системы как хозяина домена и как системы, которая получает запросы на вход в домен:

```
; domain master = yes
; domain logons = yes
```

Следующая директива устанавливает сценарии входа в систему из командной строки **Microsoft** для компьютеров и пользователей. После этого директива сохраняет профили пользователей **Microsoft** на локальном сервере **Samba**:

```
# the following login script name is determined by the machine name
# (%m):
; logon script = %m.bat
# the following login script name is determined by the UNIX user
# used:
; logon script = %u.bat
; logon path = \\%L\Profiles\%u
```

Остальные параметры конфигурации довольно понятны, как сценарии, которые добавляют и удаляют пользователей, группы и учетные записи компьютеров:

```
; add user script = /usr/sbin/useradd "%u" -n -g users
; add group script = /usr/sbin/groupadd "%g"
; add machine script = /usr/sbin/adduser -n -c □
"Workstation (%u)" -M -d /nohome -s /bin/false "%u"
; delete user script = /usr/sbin/userdel "%u"
; delete user from group script = /usr/sbin/userdel "%u" "%g"
; delete group script = /usr/sbin/groupdel "%g"
```

Параметры управления просмотром

В следующем разделе указывается, можно ли и как настроить систему в качестве мастера просмотра, который ведет список ресурсов в сети. Связанные директивы начинаются со следующего комментария:

```
#----- Browser Control Options -----
```

Если опция локального мастера (**local master**) включена, **Samba** участвует в выборах браузера, как и любой другой компьютер с **Microsoft Windows**, используя указанный приоритет **os level**:

```
; local master = no
; os level = 33
```

Вы можете принудительно выбрать локальный браузер при запуске **nmbd**, используя директиву **preferred master**:

; preferred master = yes

Разрешение имени

В следующем разделе вы можете настроить сервер **Samba** с базой данных имен и **IP-адресов** **NetBIOS**. Раздел начинается со следующего комментария:

#----- Name Resolution -----

Служба **Windows Internet Name Service (WINS)** функционально аналогична **DNS** в сетях на базе **Microsoft**. Если вы активируете следующую опцию конфигурации, демон **nmbd** включит сервер **WINS** на локальном компьютере:

; wins support = yes

Кроме того, вы можете указать локальный компьютер на удаленный сервер **WINS** в сети; Конечно, вам нужно заменить **IP-адрес** на **w.x.y.z**. Не активируйте обе команды поддержки **win** и **wins** на одной и той же системе, поскольку они являются взаимоисключающими.

; wins server = w.x.y.z

WINS может не поддерживаться на некоторых клиентах. В этом случае вы можете включить следующую директиву, чтобы **Samba** могла отвечать на запросы разрешения от имени этих клиентов:

; wins proxy = yes

Если **Samba** выступает в качестве сервера **WINS**, а имя **NetBIOS** не зарегистрировано, следующая директива разрешит поиск **DNS**-имени через локально настроенные **DNS**-серверы:

; dns proxy = yes

Параметры печати

Принтеры были включены в задачи экзамена **RHCT** для **RHEL 5**. Однако они не перечислены ни в целях **RHCSA**, ни в **RHCE** для **RHEL 6** и **RHEL 7**. Тем не менее, печать является частью конфигурации сервера **Samba** по умолчанию, поэтому вам следует как минимум просмотреть соответствующий раздел в файле конфигурации **Samba**, начиная со следующего комментария:

#----- Printing Options -----

Эти настройки принтера по умолчанию необходимы для общего доступа к принтерам с этого сервера **Samba**. Следующие три директивы загружают принтеры, как определено в **printcap name=/etc/printcap**. Директива **cups options=raw** означает, что **CUPS** отправляет данные на принтер в «**raw**»(необработанном) режиме, то есть без какой-либо дополнительной фильтрации. Этот параметр используется, когда драйвер клиента установлен на клиентах **Windows**, поэтому **CUPS** не требует дополнительной обработки данных:

load printers = yes

cups options = raw

printcap name = /etc/printcap

Кроме того, можно настроить другой сервер печати. Следующая опция получает информацию от принтеров, настроенных на хостах **System V**, которые полагаются на команду **lpstat** для вывода списка доступных принтеров:

printcap name = lpstat

Параметры файловой системы

В следующем разделе описывается, как хранятся атрибуты файловой системы **Microsoft Disk Operating System (DOS)**. Наилучшим вариантом для поддержки атрибутов **DOS** является хранение общих ресурсов **Samba** в файловой системе, которая поддерживает расширенные атрибуты, например **XFS**. В качестве альтернативы **Samba** может создавать мапы между **атрибутами DOS** и **битами разрешений Unix**. Следующие директивы определяют значения по умолчанию для всех общих каталогов:

#----- File System Options -----

Во-первых, директива **map archive** может контролировать, сопоставляется ли атрибут **DOS** файлового архива с битовым исполнением локального владельца файла, если поддерживается директивой **create mask**:

; map archive = no

Директива **map hidden** может контролировать, отображаются ли скрытые файлы **DOS** на локальный бит выполнения:

; map hidden = no

Директива **map read only**, также известная как **map readonly** в документации **Samba**, управляет отображением атрибута **DOS** только для чтения в **Linux**:

; map read only = no

Директива **map system**, если установлено в **yes**, поддерживает отображение системных файлов в стиле **DOS** бит выполнения у группы файлов:

; map system = no

Наконец, директива **store dos attribute**, если она активна, говорит **Samba** попытаться прочитать атрибуты **DOS** из атрибутов расширенных файловой системой, а не отображать атрибуты **DOS** в биты разрешений. Это значение по умолчанию:

; store dos attributes = yes

Общие каталоги Samba

Вторая часть основного файла конфигурации **Samba**, **/etc/samba/smb.conf**, используется для настройки общих каталогов и принтеров через **Samba**. Этот раздел включает анализ версии файла по умолчанию.

В **Samba** параметры общих каталогов объединены в разделы, представляющие собой группы команд, связанных с именем общего ресурса. (**Stanza** не кажется техническим термином, но некоторые считают, что правильно составленный код конфигурации - это как хорошая поэзия.)

Общие домашние каталоги

Первые четыре строки в этом разделе определяют общий ресурс **[homes]**, который автоматически разделяет домашние каталоги пользователей. Команда **browseable = no** запрещает показ общего ресурса, когда клиент ищет на серверах доступные общие ресурсы.

Раздел «**homes**» является особым, так как нет каталога по умолчанию **/homes**. Это просто ярлык. Вам не нужно указывать домашний каталог, потому что **Samba** прочитает запись учетной записи пользователя в **/etc/passwd**, чтобы определить каталог для общего доступа. По умолчанию это не разрешает доступ неизвестным пользователям (**guest ok = no**). Кроме того, вы можете ограничить системы, которые могут использовать этот общий ресурс, директивами, такими как **hosts allow** и **hosts deny**, как описано ранее. Эффекты директив **hosts allow** и **hosts deny** ограничены разделом общего доступа, где они используются.

```
#===== Share Definitions =====
```

```
[homes]
```

```
comment = Home Directories
```

```
browseable = no
```

```
writable = yes
```

!!!! On the job !!!!!

В smb.conf есть ряд директив, которые пишутся неправильно, например, browseable. В некоторых случаях правильное написание (просматриваемое) также работает. Даже если они написаны с ошибками, они по-прежнему считаются переменными Samba. Если есть сомнения, проверьте правописание на справочной странице smb.conf.

!!!!!!

Общие принтеры

Раздел [printers] обычно работает как есть, чтобы разрешить доступ всем пользователям с учетными записями на компьютере или в домене. Хотя каталог пула (/var/spool/samba) не доступен для просмотра, связанные принтеры доступны для просмотра по их именам NetBIOS. Несмотря на то, что изменения просты, стандартные опции означают, что гостевым пользователям не разрешается печатать, связанные пулы печати недоступны для записи, и **printable = yes** является обязательным условием для загрузки связанных файлов конфигурации, например, для CUPS.

NOTE: If you have a BSD-style print system there is no need to

specifically define each individual printer

```
[printers]
```

```
comment = All Printers
```

```
path = /var/spool/samba
```

```
browseable = no
```

```
# Set guest ok = yes to allow users to connect without a password
```

```
guest ok = no
```

```
writable = no
```

```
printable = yes
```

Вход в домен

Команды в следующем разделе поддерживают настройку общего ресурса [netlogon] для рабочих станций Microsoft Windows. Поскольку нет общих ресурсов [netlogon], даже для рабочих станций Linux с поддержкой Samba, в этом разделе для проверки работоспособности требуется компьютер под управлением Microsoft Windows. Если вы считаете, что у вас будет доступ к компьютеру под управлением Microsoft Windows во время экзаменов Red Hat, внимательно изучите этот раздел.

Un-comment the following and create the netlogon directory for

Domain Logons

```
; [netlogon]
```

```
; comment = Network Logon Service
```

```
; path = /var/lib/samba/netlogon
```

```
; guest ok = yes
```

```
; writable = no
```

```
; share modes = no
```

Профили рабочих станций

В следующем разделе настраивается конкретный общий ресурс перемещаемого профиля для рабочих станций Microsoft Windows. Поскольку эти профили используются рабочими станциями Windows, вы вряд ли настроите этот раздел в сети компьютеров, работающих только на Linux. Примите решение о том, может ли этот раздел применяться во время экзамена RHCE.

Un-comment the following to provide a specific roving profile

share. The default is to use the user's home directory:

```
:[Profiles]
; path = /var/lib/samba/profiles
; browseable = no
; guest ok = yes
```

Директории групп

В следующем разделе, как предлагается в комментарии, настраивается каталог **/home/samba**, который будет использоваться группой с именем **staff**. Вы можете настроить эту общую группу пользователей для совместного использования этого каталога. Чтобы настроить специальное владение и разрешения для **/home/samba**, вам также необходимо настроить соответствующие разрешения. Оба процесса описаны в **главе 8**.

```
# A publicly accessible directory that is read only, except for
# users in the "staff" group (which have write permissions):
:[public]
; comment = Public Stuff
; path = /home/samba
; public = yes
; writable = yes
; printable = no
; write list = +staff
The staff group can be labeled +staff or @staff. To set up appropriate permissions on the shared
directory, you might also want to include the following directives for creating files and directories:
create mask = 0770
directory mask = 2770
```

Затем создайте уникальное имя группы, предпочтительно с большим номером **GID**, с помощью команды **groupadd**. Убедитесь, что соответствующие пользователи являются членами этой группы **Linux**, и что эти пользователи также присутствуют в базе данных пользователей **Samba**, как описано ниже. Кроме того, каталог **/home/samba** вместе с любыми файлами, содержащимися в этом каталоге, обычно должен иметь надлежащий контекст файла **SELinux**, что возможно с помощью следующей команды:

```
# chcon -R -t samba_share_t /home/samba
```

Конечно, вы захотите убедиться, что такое изменение сохраняется в **SELinux relabel**, и это можно настроить для отмеченного каталога с помощью следующей команды:

```
# semanage fcontext -a -t samba_share_t '/home/samba(/.*)?'
```

Другие образцы строк(Stanzas)

Чтобы узнать больше о **Samba**, может быть полезно изучить другие разделы для общих каталогов. Следующие примеры были включены в более ранние выпуски **Red Hat** от **Samba**. Хотя они не включены в комментарии для **Samba**, они все же могут быть включены в файл конфигурации **smb.conf** и, следовательно, по-прежнему полезны, по крайней мере, в учебных целях.

Например, следующая общая папка **/tmp** может предоставить общую папку, в которой пользователи обмениваются загруженными файлами. Если он активирован, все пользователи (**public = yes**) получают доступ на запись (**read only = no**) к этой общей папке.

```
# This one is useful for people to share files
:[tmp]
; comment = Temporary file space
; path = /tmp
; read only = no
; public = yes
This stanza configures a directory for Fred's exclusive use. It allows that user exclusive access to his home
directory via Samba. A better location for the path would be within the /home directory.
```

```
# A private directory, usable only by fred. Note that fred
# requires write access to the directory.
;[fredsdir]
; comment = Fred's Service
; path = /usr/somewhere/private
; valid users = fred
; public = no
; writable = yes
; printable = no
```

!!!! Examen watch !!!!!

Цели RHCE определяют требование «предоставить общие сетевые ресурсы, подходящие для совместной работы группы».

!!!!

!!!! On the job !!!!!

Некоторые параметры в `smb.conf` являются инвертированными синонимами, такими как *writable* = *yes* и *read only* = *no*. Вы можете указать либо одну форму, либо другую, потому что они имеют одинаковый эффект.

Следующая строка немного отличается от общей папки `[tmp]`. Единственный пользователь, которому разрешено подключаться, - это гость без аутентификации. Если вы не настроили гостевой пользователь в **Samba**, это значение по умолчанию для пользователя с именем **nobody**.

```
# A publicly accessible directory, read/write to all users. Note
# that all files created in the directory by users will be owned
# by the default guest user, so any user with access can delete
# other user's files. Obviously this directory must be writable
# by the default user. Another user could of course be specified,
# in which case all files would be owned by that user instead.
;[public]
; path = /usr/somewhere/else/public
; public = yes
; only guest = yes
; writable = yes
; printable = no
```

Наконец, это еще один вариант схемы группы пользователей, которая создает каталог группы. В отличие от `[public]` строфы, эта доступная папка является частной.

```
# The following two entries demonstrate how to share a directory so
# that two users can place files there that will be owned by the
# specific users. In this setup, the directory should be writable
# by both users and should have the sticky bit set on it to prevent
# abuse. Obviously this could be extended to as many users as required.
;[myshare]
; comment = Mary's and Fred's stuff
; path = /usr/somewhere/shared
; valid users = mary fred
; public = no
; writable = yes
; printable = no
; create mask = 0765
```

Позвольте Samba присоединиться к домену

Если вы настроили сервер **Samba**, а он не является DC для сети, вам может потребоваться настроить его в качестве члена домена. Для этого вы можете настроить **учетную запись на DC** для

сети. Пока в этой сети есть один домен, вы можете присоединиться к домену с помощью следующей команды:

```
# net rpc join -U Administrator
```

Если доступно более одного домена, замените имя контроллера на DC в команде **net rpc join -S DC -U root**. Это предполагает, что пользователь с именем **Administrator** является административным пользователем на контроллере домена. Если команда выполнена успешно, она запрашивает пароль этого пользователя на удаленном контроллере домена. Результат добавляет учетную запись для локального компьютера в пользовательскую базу данных DC.

База данных пользователей Samba

Вы можете установить идентичные имена пользователей и пароли для компьютеров под управлением **Microsoft Windows** и **Samba с Linux** в сети. Однако это не всегда возможно, особенно когда уже существуют базы данных. В этом случае вы можете настроить базу данных пользователей и паролей **Samba**, которые соответствуют текущим именам пользователей и паролям **Microsoft** в вашей сети.

Самый быстрый способ настроить пользователей **Samba** - это команда **smbpasswd**, предоставляемая **RPM**-пакетом **samba-client**. Помните, что вы можете создать нового пользователя **Samba** только из действительных учетных записей на компьютере с **Linux**.

Тем не менее, вы можете настроить такую учетную запись без прав входа в систему **Linux**. Например, следующая команда добавляет указанного пользователя без действительной оболочки входа в систему:

```
# useradd winuser1 -s /sbin/nologin
```

Затем вы можете настроить этого пользователя с помощью пароля **Samba** с помощью команды **smbpasswd -a winuser1**. Команда **smbpasswd** является мощной; он включает в себя ряд полезных переключателей, как описано в таблице 15-4.

Расположение базы данных аутентификации зависит от значения директивы **passdb backend**. Если установлен старый формат **smbpasswd**, вы найдете его в файле **/etc/samba/smbpasswd**. Если для него установлено значение **tdbsam**, вы найдете его в файле **passwd.tdb** в каталоге **/var/lib/samba/private**. Чтобы прочитать список текущих пользователей, выполните следующую команду:

```
# pdbedit -L
```

ТАБЛИЦА 15-4 Различные параметры команды **smbpasswd**

Опции smbpasswd	Описание
-a username	Добавляет указанное имя пользователя в базу данных.
-d username	Отключает указанное имя пользователя, тем самым предотвращая аутентификацию этой учетной записи с помощью SMB .
-e username	Включает указанное имя пользователя; противоположность -d .
-r computername	Позволяет изменять пароль Windows или Samba на удаленном компьютере. Обычно идет с -U .
-U username	Обычно изменяет имя пользователя на удаленном компьютере, если указано с ключом -r .
-x username	Удаляет указанное имя пользователя из базы данных.

Создать публичный ресурс

С этой информацией, вы будите знать, как создать общий ресурс общего доступа для использования со всей сетью. Для примера создайте каталог **/publicshare**. В следующем примере раздела в файле конфигурации **/etc/samba/smb.conf** отображается каталог, доступный для всех пользователей:

[PublicShare]

```
comment = Shared Public Directory
path = /publicshare
writeable = yes
browseable = yes
guest ok = yes
```

Но безопасность может не соответствовать необходимому уровню. Например, предположим, что желательны следующие пределы:

- Доступ к [PublicShare] должен быть ограничен пользователями с обычной локальной учетной записью **Linux** (или пользователем, который может локально войти в систему на основе базы данных удаленной аутентификации, такой как **LDAP**).
- Запрещен доступ для гостевых пользователей и других.
- Доступ ко всем пользователям в локальном домене **example.com**.
- Запрещен доступ всем пользователям с подозрительного компьютера, такого как **evil.example.com**.

Чтобы это произошло, измените последнюю директиву в этом разделе. Поскольку **guest ok = no** является значением по умолчанию, вы можете просто стереть директиву **guest ok = yes**. Чтобы предоставить доступ всем пользователям в данном домене, добавьте следующую команду:

```
hosts allow = .example.com
```

Затем, чтобы запретить доступ к одному конкретному компьютеру в этой сети, вы можете добавить **EXCEPT**; например, следующая строка специально исключает отмеченную систему **evil.example.com** из списка:

```
hosts allow = .example.com EXCEPT evil.example.com
```

В качестве альтернативы, если этот домен находится в сети 192.168.122.0, любая из следующих директив поддерживает доступ ко всем системам в этой сети:

```
hosts allow = 192.168.122.
hosts allow = 192.168.122.0/255.255.255.0
```

Вы могли бы специально запретить доступ к компьютерам с помощью команды, такой как следующее:

```
hosts deny = evil.example.com
```

В качестве альтернативы вы можете заменить **IP-адреса** на **evil.example.com**.

УПРАЖНЕНИЕ 15-1

Настройте домашний каталог Samba

В этом упражнении вы узнаете об общей папке общего каталога. Вам понадобится как минимум два компьютера, один из которых должен быть сервером **Samba**. Другой может быть клиентом **Linux** или **Microsoft Windows**. Вы подключитесь к серверу **Samba** с клиента и получите доступ к файлам в своем домашнем каталоге на сервере **Samba**. Эти шаги предполагают, что учетной записью пользователя является **майкл**; при необходимости замените имя своего обычного пользователя.

1. Установите и настройте **Samba** для запуска при загрузке, используя методы, описанные ранее в этой главе.
2. Откройте файл конфигурации **/etc/samba/smb.conf**. Найдите текущее значение для **workgroup**.
3. Убедитесь, что компьютеры в локальной сети имеют одинаковое значение для рабочей группы. Если локальная сеть является доменом в стиле **Windows**, задайте для рабочей группы имя домена.
4. Запустите команду **testparm**.

5. Прочитайте и устраните все проблемы, которые появляются в выходных данных команды **testparm**. Исправьте любые проблемы с синтаксисом **smb.conf**, определенные в выходных данных.
6. Активируйте логическое значение **samba_enable_home_dirs** на сервере **Samba** с помощью следующей команды:

```
# setsebool -P samba_enable_home_dirs on
```

7. Настройте учетную запись пользователя на сервере **Samba** в базе данных аутентификации с помощью следующей команды. Обратите внимание, что соответствующая учетная запись уже должна существовать в **/etc/passwd**; в противном случае команда не будет выполнена (введите соответствующий пароль при появлении запроса):

```
# smbpasswd -a michael
```

8. Запустите службы **Samba** с помощью следующей команды:

```
# systemctl start smb nmb
```

В качестве альтернативы, если **Samba** уже запущена, перезагрузите конфигурацию в файле **smb.conf** с помощью следующей команды:

```
# systemctl reload smb nmb
```

9. Откройте соответствующие порты в брандмауэре для сервера **Samba**:

```
# firewall-cmd --permanent --add-service=samba  
# firewall-cmd --reload
```

На клиентах следующие команды открывают необходимые порты в **firewalld**:

```
# firewall-cmd --permanent --add-service=samba-client  
# firewall-cmd --reload
```

10. Перейдите на удаленную рабочую станцию **Linux** или **Microsoft Windows** в том же домене или рабочей группе. На компьютере с **Linux** убедитесь, что установлен **RPM-пакет samba-client**.
11. Если вы можете просмотреть список компьютеров с сервера **Samba** с помощью следующей команды, просмотр работает. Замените имя настроенного хоста сервера **Samba** на **sambaserver**.

```
# smbclient -L sambaserver -U michael
```

12. Войдите в систему как пользователь **root** на удаленном клиенте **RHEL 7**. Убедитесь, что **RPM-пакет cifs-utils** установлен.
13. С этого удаленного клиента **RHEL 7** используйте команду **mount.cifs**, чтобы настроить удаленный общий каталог **[homes]** в пустом локальном каталоге. Например, как пользователь **root**, вы можете подключиться к каталогу **local /share** (при необходимости создайте его) с помощью следующей команды:

```
# mount //sambaserver/michael /share -o username=michael
```

14. Проверьте результат. Можете ли вы просмотреть домашний каталог на удаленном компьютере?
15. Бонус: отключите логическое значение **samba_enable_home_dirs** и попробуйте снова. Что происходит?

ЦЕЛЬ СЕРТИФИКАЦИИ 15.02

Самба как клиент

Вы можете настроить два типа клиентов через **Samba**. Одним из них является **FTP-подобный клиент**, который может просматривать и получать доступ к каталогам и принтерам, совместно используемым с серверов **Microsoft Windows** или серверов **Samba в Linux/Unix**. Второй добавляет поддержку команды **mount** для протоколов **SMB** и **CIFS**. Клиентские команды **Samba** доступны из **RPM-пакетов samba-client и cifs-utils Linux/Unix** компьютер на базе **Samba**. Предполагая, что это разрешено через брандмауэр, вы можете использовать **smbclient** для проверки общих каталогов и принтеров из других систем, по крайней мере, в локальной сети. Например, следующая команда **smbclient** проверяет общие каталоги и принтеры:

```
# smbclient -L server1.example.com -U donna
```

Мы указали два аргумента с помощью команды **smbclient**: аргумент **-L** сообщает имя сервера **Samba**, а аргумент **-U** указывает имя пользователя на удаленном компьютере. Когда команда достигает сервера **Samba**, вам предлагается ввести соответствующий пароль.

Появится список доступных ресурсов; например, следующий вывод показывает общие ресурсы с именами **public** и **donna**, а также принтер с именем **OfficePrinter** в удаленной системе с именем **Maui**:

Domain=[MYGROUP] OS=[Unix] Server=[Samba 4.1.1]		
Sharename	Type	Comment
-----	----	-----
public	Disk	Public Stuff
IPC\$	IPC	IPC Service (Samba Server Version 4.1.1)
OfficePrinter	Printer	Printer in the office
donna	Disk	Home Directories

Из отображаемого вывода есть доступный ресурс с именем **public**. Вы также можете использовать команду **smbclient** для просмотра и копирования файлов аналогично **FTP-клиенту**. Необходимая команда для установления соединения показана ниже:

```
$ smbclient //server1.example.com/public -U michael
```

Конечно, большинство администраторов предпочли бы смонтировать этот общий ресурс в локальном каталоге. Вот где полезны опции команды **mount**.

Варианты монтирования

Общие ресурсы могут быть смонтированы пользователем с правами администратора. Стандарт применяется к команде **mount.cifs**, функционально эквивалентной команде **mount -t cifs**. Например, следующая команда монтирует общий ресурс с именем **public** в локальный каталог **/home/shared**:

```
# mount.cifs //server1.example.com/public /home/shared -o username=donna
```

Эта команда запрашивает пароль пользователя **donna** на удаленном сервере. Этот пароль должен быть частью базы данных аутентификации пользователя **Samba** в системе **server1.example.com**, обычно отличной от стандартной базы данных аутентификации **Linux**.

Хотя для общих каталогов **Samba** больше нет команды **umount.cifs**, вы можете использовать команду **umount** для размонтирования таких каталогов.

Автоматическое монтирование Samba

Поскольку для настройки общего каталога требуется несколько дополнительных шагов, вы можете автоматизировать процесс. Один из способов автоматизации монтирования - через файл конфигурации **/etc/fstab**, рассмотренный в главе 6. Чтобы просмотреть основные элементы этой главы, вы можете настроить публичный общий ресурс в **/etc/fstab**, добавив следующую строку (которую можно упаковать в этот файл):

```
//server1.example.com/public /home/shared cifs username=donna,password=pass, 0 0
```

Однако это может быть опасно, поскольку файл **/etc/fstab** доступен для чтения всем. Для этого вы можете настроить выделенный файл учетных данных с именем пользователя и паролем следующим образом:

```
//server1.example.com/public /home/share cifs credentials=/etc/smbdonna 0 0
```

Как предложено в **главе 6**, вы можете настроить имя пользователя и пароль в файле с именем, например, **/etc/smbdonna**:

```
username=donna
password=donnaspassword
```

Хотя содержимое этого файла все еще должно существовать в виде открытого текста, вы можете настроить файл **/etc/smbdonna** доступный для чтения только пользователю с правами администратора. Также возможно настроить авто монтирование с аналогичной информацией. Однако, поскольку автомонтирование является навыком **RHCSA**, вам придется обратиться к **Главе 6** за этой информацией.

УПРАЖНЕНИЕ 15-2

Настройка общего ресурса Samba для групповой совместной работы

Настройка общего ресурса Samba для групповой совместной работы

В этом упражнении вы настроите **Samba** для совместного использования каталога для совместной работы, чтобы только пользователи из группы «**editors**» имели доступ для записи в общий ресурс.

1. Создайте пользователей только для Samba **michael** и **alex** и добавьте их в группу «**editors**»:

```
# groupadd editors
# useradd -s /sbin/nologin -G editors michael
# useradd -s /sbin/nologin -G editors alex
# smbpasswd -a michael
# smbpasswd -a alex
```

2. Создайте каталог **/editors** и назначьте подходящего владельца и разрешения для совместной работы (**2770**):

```
# mkdir /editors
# chgrp editors /editors
# chmod 2770 /editors
```

3. Обязательно установите соответствующий контекст **SELinux** для каталога с помощью следующей команды:

```
# chcon -R -t samba_share_t /editors
```

Кроме того, чтобы изменения остались в силе с **SELinux**, вам нужно обновить политику **SELinux** с помощью следующей команды:

```
# semanage fcontext -a -t samba_share_t '/editors(/.*)?'
```

4. Откройте файл **/etc/samba/smb.conf** в текстовом редакторе.
5. Настройте **Samba** для предоставления доступа к каталогу **/editors** пользователям, которые принадлежат к группе «**editors**». В разделе «Определения общего доступа» вы можете добавить следующие команды:

```
[Editors]
```

```
comment = shared directory for McGraw-Hill editors
path = /editors
valid users = @editors
writable = yes
```

6. Запишите и сохраните изменения в файле **smb.conf**.
7. Убедитесь, что брандмауэр предоставляет доступ к службе **Samba**. Если вы не помните, как разрешить этот трафик через брандмауэр, просмотрите **упражнение 15-1**.

```
# firewall-cmd --list-all
```

8. Вы можете увидеть, работает ли **Samba** с помощью команды **systemctl status smb nmb**. Если он остановлен, вы можете запустить его с помощью команды **systemctl start smb nmb**. Если он запущен, вы можете заставить **Samba** перечитать ваш файл конфигурации с помощью следующей команды:

```
# systemctl reload smb nmb
```

Эта опция позволяет вам изменить конфигурацию **Samba**, не отключая пользователей от сервера **Samba**.

9. На другом компьютере просмотрите общий ресурс, используя учетные данные **smbclient** и **michael**:

```
# smbclient //server1.example.com/Editors -U Michael
```

10. Смонтируйте общий ресурс в каталог, используя учетные данные **alex**, и убедитесь, что вы можете создать файл:

```
# mkdir /mnt/alex
# mount -t cifs -o username=alex //server1/Editors /mnt/alex
# touch /mnt/alex/testfile
```

11. В качестве бонуса создайте другого пользователя **Samba** с именем «**evil**». Попробуйте перемонтировать общий ресурс как «**evil evil**». Что происходит?

Многопользовательские монтирование Samba

При монтировании общего ресурса **Samba** с помощью команды **mount.cifs** от имени пользователя **root** необходимо указать учетные данные действительной учетной записи **Samba**, у которой есть права доступа к общему ресурсу. Эти учетные данные необходимы для проверки монтирования, а также прав доступа к файлам и каталогам. В многопользовательской среде это решение не идеально. Это происходит потому, что всякий раз, когда файл создается на общем ресурсе **Samba**, этот файл принадлежит пользователю, указанному в команде **mount**.

Для решения этой проблемы команда **mount.cifs** включает многопользовательскую опцию. В качестве примера вы можете изменить команду монтирования из **упражнения 15-2**, как показано ниже:

```
# mount.cifs -o multiuser,username=alex //server1/Editors /mnt/editors
```

Вы можете увидеть, как это работает, пройдя лабораторную **работу 6** в конце главы. Если в **Samba** не настроена аутентификация **Kerberos** (что выходит за рамки экзамена **RHCE**), пользователи должны ввести свои учетные данные **SMB** для доступа к смонтированному общему ресурсу. Средство **cifscreds**, включенное в **RPM-пакет cifs-utils**, служит для этой цели. Команда добавляет учетные данные пользователя в связку ключей ядра, как показано здесь:

```
$ cifscreds add server1.example.com
```

Учетные данные хранятся только для сеанса текущего пользователя. Когда новый сеанс установлен, он должен быть повторно введен путем повторного выполнения предыдущей команды.

ЦЕЛЬ СЕРТИФИКАЦИИ 15.03

Samba Устранение неполадок

Samba сложна. При сложном обслуживании простые ошибки могут быть трудно диагностируемыми. К счастью, в **Samba** есть отличные инструменты для устранения неполадок. Основная команда **testparm** проверяет синтаксис, но файлы журналов могут рассказать вам больше. Конечно, если в локальные брандмауэры не будут внесены соответствующие изменения, **Samba** может быть недоступен даже из удаленных систем.

Samba проблема идентификации

Samba - это всепрощающий сервис. Включает синонимы для ряда параметров. Но помимо этих параметров, команда **testparm**, о которой мы уже говорили, может помочь выявить проблемы. Например, **рисунки 15-5** иллюстрирует ряд проблем. Нераспознанные параметры подсвечиваются сообщением «неизвестный параметр (**unknown parameter**)».

Некоторые параметры не работают друг с другом. Например, следующее сообщение в выводе **testparm** выделяет две несовместимые директивы:

ERROR: both 'wins support = true' and 'wins server = <server list>' cannot be set in the smb.conf file. nmbd will abort with this setting.

РИСУНОК 15-5 Некоторые проблемы с синтаксисом, определенные testparm

```
[root@server1 ~]# testparm
Load smb config files from /etc/samba/smb.conf
rlimit_max: increasing rlimit_max (1024) to minimum Windows limit (16384)
Unknown parameter encountered: "ecurity"
Ignoring unknown parameter "ecurity"
Unknown parameter encountered: "assdb backend"
Ignoring unknown parameter "assdb backend"
Processing section "[homes]"
Processing section "[printers]"
Processing section "[public]"
Unknown parameter encountered: "rite list"
Ignoring unknown parameter "rite list"
Loaded services file OK.
ERROR: both 'wins support = true' and 'wins server = <server list>' cannot be se
t in the smb.conf file. nmbd will abort with this setting.
Server role: ROLE_STANDALONE
Press enter to see a dump of your service definitions
█
```

Иногда команды устранения неполадок поступают в выходной файл для других команд. Например, часто выводимое сообщение является простым, например, следующий вывод определенной команды **mount.cifs**, связанной с неверным именем общего ресурса. Это также предполагает, что случай с именами общих ресурсов менее важен в сетях, связанных с операционными системами **Microsoft**.

Retrying with upper case share name

Иногда сообщения могут показаться более простыми, такими как

mount error(13): Permission denied

Но это сообщение может относиться к неверному паролю или к пользователю, который не был настроен в базе данных **Samba**.

Иногда проблемы могут показаться более раздражающими. Например, если вы монтируете удаленный домашний каталог, и в этом каталоге не отображаются файлы, это может означать, что логическое значение **SELinux samba_enable_home_dirs** не включено. Если вы смонтируете удаленный каталог, отличный от домашнего каталога пользователя, это может означать, что каталог и связанные файлы неправильно помечены с типом контекста файла **samba_share_t**.

Проверка локального файла журнала

Проблемы, связанные с **Samba**, могут появляться в файле **/var/log/messages** или в разных файлах в каталоге **/var/log/samba**. Во-первых, синтаксические ошибки, обнаруженные в выходных данных команды **testparm**, также могут появляться в файле **/var/log/messages**. Когда службы **Samba** запускаются, ошибки в файле конфигурации - это проблемы, о которых стоит сообщить в стандартном файле системного журнала.

Кроме того, если попытка монтирования общего каталога **Samba** не удалась, соответствующие сообщения также появляются в файле **/var/log/messages**. Иногда сообщения просты, например, «**cifs_mount failed**» или **NT_STATUS_LOGON_FAILURE**.

Журнал **systemd** является очень полезным ресурсом для поиска и просмотра записей журнала **Samba**. Все сообщения, относящиеся к системному модулю **smb** и **nmb**, могут быть отображены с помощью следующей команды:

```
# journalctl -u smb -u nmb
```

Файлы журнала сервера **Samba** хранятся в каталоге **/var/log/samba**. Файлы журнала классифицируются по хосту или IP-адресу клиента, который подключается к серверу. По умолчанию **Samba** не очень многословна. Возможно, вы захотите установить запись уровня журнала в 1 или 2 в **/etc/samba/smb.conf** и посмотреть, как изменились подробности сообщений журнала. Например, подключение к локальной системе, полезной для устранения неполадок, может включать следующее сообщение в файле журнала **log.127.0.0.1**:

```
127.0.0.1 (ipv4:127.0.0.1:44218) connect to service michael initially as user michael (uid=1001, gid=1001) \ (pid 23800)
```

Подключенный пользователь идентифицируется номерами **UID, GID и PID**. Если подключается неавторизованный пользователь, эти номера могут помочь идентифицировать проблемного пользователя и/или скомпрометированную учетную запись вместе с соответствующим идентификационным номером процесса.

Большинство других файлов в этом каталоге относятся к различным службам с именами; например, файлы **log.smbd**, **log.nmbd** и **log.winbindd** собирают сообщения, связанные с демонами, указанными в каждом соответствующем файле журнала.

СЦЕНАРИЙ И РЕШЕНИЕ.	
Вам необходимо настроить общий доступ к сети с компьютерами Microsoft .	Установите Samba и настройте общие каталоги в /etc/samba/smb.conf . Убедитесь, что общие каталоги (кроме домашних каталогов пользователей) имеют соответствующий тип контекста SELinux samba_share_t .
Вы хотите настроить общий доступ к домашним каталогам пользователей через Samba .	Активируйте раздел [homes] , настройте соответствующих пользователей в базе данных аутентификации Samba и включите логическое значение samba_enable_home_dirs .
Вы хотите настроить безопасность на основе хоста для Samba .	Установите соответствующие разрешения hosts и запретите указывать хосты в smb.conf или настройте firewalld для ограничения доступа.
Вы хотите настроить безопасность Samba на основе пользователя.	Установите соответствующие допустимые пользователи и/или недопустимые директивы пользователей в файле smb.conf .
Вам необходимо настроить общий ресурс для совместной работы группы.	Установите раздел общего доступа с допустимыми пользователями, настроенными для определенной группы, наряду с writable=yes и соответствующими разрешениями для групповая совместная работа в общем каталоге. Убедитесь, что общий каталог и его содержимое имеют тип контекста SELinux samba_share_t .

Вы смонтировали общий ресурс CIFS в /etc/fstab и хотите, чтобы пользователи обращались к содержимому, используя свои собственные учетные данные Samba , а не те, которые указаны командой mount .	Самба поделится с многопользовательской опцией. Попросите пользователей выполнить команду cifscreds и предоставить свои учетные данные SMB перед доступом к содержимому общего ресурса.
---	--

РЕЗЮМЕ СЕРТИФИКАЦИИ

Samba позволяет компьютеру **Linux** появляться, как любой другой компьютер **Microsoft** в сети на базе **Windows**. **Samba** основана на протоколе **Server Message Block**, который позволяет компьютерам **Microsoft** взаимодействовать в сети **TCP/IP**. Это развивалось как **Microsoft** адаптировала **SMB** к общей файловой системе Интернета. Сетевое общение **Samba** работает через **UDP-порты 137 и 138**, а также **TCP-порты 139 и 445**.

Логический ключ **SELinux** – для **samba samba_enable_home_dirs**. На общие каталоги должны быть установлены на Тип контекста файла **samba_share_t**.

Основной файл конфигурации **Samba**, **/etc/samba/smb.conf**, содержит отдельные разделы для глобальных настроек и общих определений. Команду **smbpasswd** можно использовать для настройки существующих пользователей **Linux** в локальной базе данных аутентификации **Samba**. Возможность **multiuser** монтирования и команда **cifscreds** аутентифицируется с соответствующими учетными данными пользователя, даёт доступ к общему каталогу.

Что касается устранения неполадок, изменения в **smb.conf** могут быть легко протестированы с помощью утилиты **testparm**. **Samba** включает в себя ряд синонимов для директив; некоторые равильные директивы на основе орфографических ошибок. Хотя основные сообщения журнала службы **Samba** можно найти в файле **/var/log/messages**, большая часть информации журнала **Samba** находится в **/var/log/samba** каталоге. Многие из файлов в этом каталоге содержат имя клиента или IP-адрес.

Две минуты проверки.

Вот некоторые из ключевых моментов целей сертификации в главе 15.

Samba Services

- **Samba** позволяет компьютерам под управлением **Microsoft Windows** обмениваться файлами и принтерами между сетью, используя протокол **Server Message Block (SMB)** и **NetBIOS** через стек протоколов **TCP/IP**.
- **Samba** включает в себя клиента и сервер. Вариации команд **mount -t cifs** и **mount.cifs** поддерживают монтирование общей папки **Samba** даже при присоединении к **Microsoft** домен.
- Основной файл конфигурации **Samba** - это **/etc/samba/smb.conf**.
- **Samba** поддерживает настройку компьютера **Linux** в качестве сервера **Microsoft Windows**. Это также может предоставлять службы просмотра **Microsoft, WINS и Domain Controller**, даже на сеть **Active Directory**.

Самба как клиент

- Команда **smbclient** может отображать общие каталоги и принтеры из указанных удаленных серверов **Samba** и **Microsoft** с использованием **FTP-подобного интерфейса**.
- Команда **mount.cifs** может монтировать каталоги, общие для **Samba** или **Microsoft** серверов.
- Общие ресурсы **Samba** могут быть смонтированы в процессе загрузки с помощью конфигурационного файла **/etc/fstab**.
- Опции **multiuser** монтирования и команда **cifscreds** регулируют доступ и разрешения для общего ресурса с использованием учетных данных каждого пользователя, а не указанных по команде монтирования.

Samba Устранение неполадок

- Команда **testparm** выполняет синтаксическую проверку основного файла конфигурации **Samba** **/etc/samba/smb.conf**.
- Логирующие демоны **Samba** могут быть записаны в файл **/var/log/messages**.

- Большинство файлов журнала **Samba** можно найти в каталоге **/var/log/samba**. Различные файлы журнала могут быть найдены для клиентов и демона.

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 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.

Samba Services

1. ИТ-отдел, работающий с серверами **Microsoft**, настроил **Windows Server** для обработки файлов и услуги обмена печатью. Этот сервер правильно ссылается на сервер **WINS** на **192.168.55.3** для имени разрешения и настраивает все пользовательские логины через **DC** на **192.168.55.8**. Если вы настраиваете локальная система **Linux** как **DC**, какую директиву, как минимум, нужно настроить в локальном файле конфигурации **Samba**?

2. Вы недавно изменили файл конфигурации **Samba** и не хотите отключать текущий пользователи. Какая команда вынуждает службы **Samba** и **NetBIOS** перечитывать файл конфигурации без необходимости отключения пользователей **Microsoft** или перезапуска службы?

3. Какие порты должны быть открыты для работы сервера **Samba** с удаленными системами?

4. Какие настройки **SELinux** подходят для общего доступа к домашним каталогам через **Samba**?

5. Какой тип контекста файла **SELinux** подходит для общих каталогов на **Samba**?

6. Какая директива **Samba** ограничивает доступ к системам в сети **example.org**?

7. Какая директива **Samba** ограничивает доступ пользователей **Тим** и **Стефани**?

8. Какая директива **Samba** ограничивает доступ в разделяемом разделе к настроенной группе **ilovelinux**?

9. Какая директива **Samba** поддерживает доступ ко всем пользователям в общем каталоге?

10. Какая команда добавляет пользователя **elizabeth** в базу данных аутентификации **Samba** **tdbsam**?

Самба как клиент

11. Какую команду можно использовать для монтирования удаленно общих каталогов **Microsoft**?

Самба Устранение неполадок

12. Вы сделали несколько быстрых изменений в файле конфигурации **Samba**, и вам нужно быстро его проверить на синтаксические ошибки. Какая команда проверяет **smb.conf** на наличие синтаксических ошибок?
-

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 15**. Большинство лабораторных работ для этой главы просты и требуют очень небольшого количества команд или изменений в одном или двух файлах конфигурации.

Лабораторная работа 1

В этой лабораторной работе вы будете устанавливать и настраивать **Samba** только для основных операций. Если возможно, используйте систему, в которой **Samba** еще не установлена.

1. Убедитесь, что соответствующие пакеты **Samba** установлены правильно. Какие **RPM** вы установили и как вы их установили?
2. Убедитесь, что пакеты **samba-client**, **samba-winbind** и **cifs-utils** также установлены.
3. Убедитесь, что любой локальный брандмауэр поддерживает доступ к локальному серверу **Samba**. Убедитесь, что брандмауэр на всех клиентах поддерживает использование клиентского программного обеспечения **Samba**.
4. Убедитесь, что службы **Samba** и **NetBIOS** настроены для правильного запуска при загрузке **Linux**.
5. Запустите службы **Samba** и **NetBIOS** прямо сейчас. Какие опции команды **systemctl** вы использовали?
6. Убедитесь, что службы **Samba** работают. Как ты это сделал?

Лабораторная работа 2

Во время экзамена или, возможно, поездки на удаленный сайт, где доступ в Интернет невозможен, вам может потребоваться документация **Samba**, доступная с установленными пакетами.

1. Откройте страницу руководства для файла конфигурации **Samba**, **smb.conf**.
2. Убедитесь, что вы знаете, как искать ключевые директивы, например, разрешить хосты и недопустимых пользователей.
3. Запустите **rpm -qd samba samba-client cifs-utils**, чтобы вывести список всех файлов документации **Samba**, установленных в вашей системе.
4. Изучите содержимое следующих справочных страниц: **testparm**, **smbpasswd**, **samba_selinux**, **mount.cifs** и **cifscreds**.

Лабораторная работа 3

Перед началом этой лабораторной работы важно сделать резервную копию файла **/etc/samba/smb.conf**. Если вы этого не сделаете, может быть трудно перейти к дополнительным лабораторным занятиям в этой главе.

1. Настройте глобальные параметры **Samba** для предоставления услуг рабочей группе локальным пользователям. Задайте для имени рабочей группы что-то подходящее для локальной организации.
2. Можно ли ограничить доступ к корпоративному доменному имени (например, **example.com**) с помощью этого инструмента? Что ты должен делать?
3. С помощью этого инструмента вы можете запретить доступ к одному конкретному хосту или **IP-адресу**? Сделайте это для одного хоста в локальной сети.
4. Сохраните ваши изменения. Что нужно сделать, чтобы **Samba** перечитала файл конфигурации?
5. Протестируйте результат сначала с запрещенного хоста, указанного в **шаге 3**, а затем со второго хоста в локальной сети.

6. Бонусная лаборатория: выполните шаги, необходимые для переустановки **Samba** и соответствующей исходной версии файла конфигурации **smb.conf**.

Лабораторная работа 4

В этой лабораторной работе вы настроите общий ресурс **[homes]** по умолчанию для конкретных требований безопасности пользователя. Вам потребуется один общий пользователь как на локальном сервере **Samba**, так и на удаленном клиенте **Samba**.

1. Откройте основной файл конфигурации **Samba**.
2. Перейдите к предопределенному общему ресурсу **[homes]**.
3. Убедитесь, что общий ресурс **[homes]** доступен только хостам в локальной сети **example.com**. Кроме того, вы можете разрешить доступ ко всем системам в локальной сети, за исключением одного **IP-адреса**.
4. Убедитесь, что общий ресурс доступен для записи одному аутентифицированному пользователю.
5. Настройте этого пользователя в базе паролей **Samba**.
6. Проверьте результат из удаленной системы. Если возможно, проверьте результаты в системах как в сети **example.com**, так и за ее пределами. В качестве альтернативы, выполните тесты из систем, которые должны быть разрешены и запрещены в соответствии с настройкой шага 3.

Лабораторная работа 5

В этой лабораторной работе вы пойдете дальше и создадите общедоступный общий ресурс, доступный для всех пользователей.

1. Создайте новую папку с именем **[public]**.
2. Измените путь к общедоступному общему ресурсу на **/home/public**.
3. Настройте общедоступный общий ресурс, чтобы любой пользователь в локальном домене **example.com** мог получить доступ к общему ресурсу.
4. При необходимости создайте каталог **/home/public**. Измените разрешения для этого каталога на **1777**.
5. В чем преимущество **1777** разрешений?
6. Передайте ваши изменения.
7. Проверьте результат из удаленной системы. Что произойдет, если вы запишите файл в этот общий каталог?

Лабораторная работа 6

В этой лабораторной работе вы пойдете еще дальше и создадите общий каталог, доступ к которому будет ограничен группой из двух пользователей. Основные этапы такие же, как в лабораторной работе 5; однако вам необходимо создать каталог с разрешениями **SGID**, а также полные разрешения для владельца группы этого каталога. Основные шаги по созданию этого общего каталога те же, что и в **главе 8**.

Затем создайте учетную запись пользователя с минимальными разрешениями, которая будет использоваться для аутентификации с помощью команды **mount.cifs**. Протестируйте результат из удаленной системы и постоянно монтируйте общий ресурс **Samba** в **/etc/fstab** с опцией **multiuser**. Как обычный пользователь, запустите команду **cifscreds**, чтобы сохранить учетные данные доступа в связке ключей пользователя перед доступом к общему ресурсу.

Лабораторная работа 7

Для сервера важно, чтобы любые сделанные изменения были постоянными. Это означает, что изменения должны быть активны при перезагрузке **Linux**. Выполните упорядоченную перезагрузку локального сервера сейчас и убедитесь, что **Samba** запускается при загрузке **Linux**.

1. Как вы сделали ваши изменения постоянными?
2. Какую команду вы использовали для упорядоченного завершения работы?
3. Какие изменения в настройках **SELinux** вы должны проверить?

ОТВЕТЫ НА САМОПРОВЕРКУ

Samba Services

1. Как минимум, чтобы настроить систему **Linux** как **DC**, вам нужно изменить директиву **security=user**. Если это в системе **Active Directory**, вы должны использовать директиву **security=ads**.
2. Команда, которая заставляет службы **Samba** и **NetBIOS** перечитать файл конфигурации без отключения пользователей **Microsoft** или перезапуска службы - это **systemctl reload smb nmb**.
3. Открытые порты, связанные с обменом данными с сервером **Samba**, являются портами **UDP 137** и **138** так же, как **TCP 139** и **445**.
4. Логическое значение **SELinux**, связанное с общим доступом к домашним каталогам на **Samba**, **samba_enable_home_dirs**.
5. Тип контекста файла **SELinux**, подходящий для общих каталогов **Samba**, - это **samba_share_t**.
6. Директива **Samba**, ограничивающая доступ к системам в сети **example.org**

host allow = .example.org

Следующая директива также является приемлемым ответом:

allow hosts = .example.org

7. Одна директива **Samba**, которая ограничивает доступ для отмеченных пользователей,
valid users = tim stephanie
8. Одна директива **Samba**, ограничивающая доступ к указанной группе:
valid users = @ilovelinux
+ ilovelinux group также будет приемлемой.
9. Одна директива **Samba**, которая поддерживает доступ ко всем пользователям в общем каталоге,
guest ok = yes
10. Команда, которая добавляет пользователя **elizabeth** в базу данных аутентификации **Samba**
tdbsam
smbpasswd -a elizabeth

Samba как клиент

11. Командой, которая может использоваться для монтирования удаленно совместно используемых каталогов **Microsoft**, является **mount.cifs**. Команда **mount -t cifs** также является приемлемым ответом.

Самба Устранение неполадок

12. Команда, которая может проверить файл конфигурации **Samba** на наличие ошибок, называется **testparm**.

ОТВЕТЫ ЛАБОРАТОРНОЙ РАБОТЫ

Лабораторная работа 1

Лабораторные работы по главам **Samba** разработана так, чтобы им было легко следовать. Однако вам понадобится знания **Linux**, чтобы выполнить несколько шагов.

1. Вы установили группу «**File and Print Server**» или, в качестве альтернативы, группу «**File and Storage Server**», которая включает один **RPM**, связанный с **Samba**, **samba**. Зависимые пакеты, такие как **samba-common** и **samba-libs**, будут также установлены.
2. Один из способов найти все связанные пакеты **Samba** - воспользоваться командой **yum search samba**. Вы можете затем установить указанные пакеты с помощью команды **yum install packagename**.
3. Для поддержки связи с локальным сервером **Samba** выполните следующее:

```
# firewall-cmd --permanent --add-service=samba
# firewall-cmd --reload
```

На клиентах выполните следующие команды:

```
# firewall-cmd --permanent --add-service=samba-client
# firewall-cmd --reload
```

4. Вы можете использовать команду **systemctl enable smb nmb**, чтобы убедиться, что **Samba** и **NetBIOS** выполнится при следующей загрузке **Linux**.
5. Используйте команду **systemctl start smb nmb** для запуска служб **Samba** и **NetBIOS**.
6. Один из способов проверить, работает ли **Samba**, - это проверить наличие процессов **smbd** и **nmbd** в таблице процессов. Используйте **ps aux | grep mbd**, чтобы увидеть, присутствуют ли эти процессы. Другой способ – воспользоваться командой **systemd**, такой как команда **systemctl status smb nmb**.

Лабораторная работа 2

Эта **Лабораторная работа** должна познакомить вас с доступной документацией для файлового сервера **Samba**. Когда вы выполните команду **man smb.conf**, она откроет руководство для основного файла конфигурации **Samba**. Вы должны иметь возможность искать файл с помощью команд в стиле **vi**. Например, для поиска директивы **hosts allow**, перейдите в файл, и напечатайте следующие:

/hosts allow

и нажмите **N**, чтобы увидеть следующий экземпляр этой директивы. Либо для поиска в обратном направлении введите

?hosts allow

и нажмите **N**, чтобы увидеть предыдущий экземпляр этой директивы на странице руководства.

Из командной строки просмотрите другие справочные страницы **Samba**. Узнайте, что вам нужно в качестве справки для работы или для экзамена.

Лабораторная работа 3

В этой лабораторной работе предполагается, что вы создали резервную копию файла **smb.conf** из каталога **/etc/samba**.

1. Некоторые администраторы придерживаются стандартного имени рабочей группы **Microsoft Windows workgroup**. Вы можете найти его в выводе команды **smbclient -L //clientname**.
2. Чтобы ограничить доступ к серверу **Samba**, вы можете сделать это в глобальном разделе, директивой **hosts allow**.
3. Чтобы ограничить доступ с определенного компьютера, вы можете сделать это в глобальном разделе директивой **hosts deny**.
4. Вы можете заставить **Samba** прочитать изменения с помощью команды **systemctl reload smb**. До фиксируя изменения, вы можете проверить их с помощью команды **testparm**.
5. При тестировании соединения из другой системы используйте команду **smbclient**. Вам нужно для этой цели разрешить доступ через **UDP-порты 137 и 138**, что возможно разрешением доступа в настройках брандмауэра для службы **samba-client**.

6. Если вам нужна свежая версия файла **smb.conf**, удалите или переместите существующую версию файла из каталога **/etc/samba** и выполните команду **yum reinstall samba-common**.

Лабораторная работа 4

В случае успеха только один удаленный пользователь получит доступ к своему домашнему каталогу через **Samba**, что вы можете проверить с помощью соответствующих команд **smbclient** и **mount.cifs**. Один из способов реализации требования этой лабораторной работы заключается в следующих шагах.

1. Откройте основной файл конфигурации **Samba**, **/etc/samba/smb.conf**, в текстовом редакторе.
2. Перейдите к общей папке **[homes]** в последней части этого файла.
3. Если в разделе **[global]** этого файла уже нет соответствующих ограничений, вы можете ограничить в секции **[homes]** доступ директивой **hosts allow = .example.com**.
4. Добавьте директиву **users = username** с именем нужного пользователя в разделе **[homes]**.
5. Добавьте нужного пользователя в базу данных аутентификации **Samba** с помощью команды **smbpasswd -a username**.
6. Перезапустите или перезагрузите службу **Samba** с помощью соответствующей команды **systemctl**.
7. Сохраните внесенные изменения.
8. Проверьте результат из удаленной системы с помощью команды **smbclient**. Вы также должны быть в состоянии использовать команду **mount.cifs** из учетной записи **root** с **-o username=username** опции, чтобы смонтировать домашний каталог для общего пользователя.

Лабораторная работа 5

Эта лаборатория может быть продолжением **Лабораторной работы 4**. Вы просто добавляете еще одну строфу в основную **Samba** конфигурационный файл.

1. В конце файла раздел начинается **[public]**. Добавьте соответствующий комментарий к строфе.
2. Установите **path = /home/public**.
3. Обязательно установите **hosts allow = .example.com**. Сохраните ваши изменения в файле **smb.conf**.
4. Установите разрешения для общего ресурса с помощью следующих команд:

```
# mkdir /home/public
# chmod 1777 /home/public
```

Параметр **777** для разрешений предоставляет разрешения на чтение, запись и выполнение / поиск всем пользователям. (**root, root's group, и все остальные**). **1** в начале значения разрешения устанавливает липкий бит. Этот бит, установленный для каталогов, удерживает пользователей от удаления или переименования файлов, которые они не владеют.

5. Зафиксируйте изменения в работающей в данный момент службе **Samba** с помощью команды **systemctl reload smb**.
6. При тестировании результата с удаленной системы любое имя пользователя в локальной базе данных **Samba** должно сработать.

Лабораторная работа 6

Эта лабораторная работа может потребовать значительного объема работ. Вам нужно настроить группу пользователей, с группой владение выделенным каталогом. Потому что это обсуждение в **главе 8** было основано на RHCSA требование, возможно, вам придется повторить этот процесс в этой лабораторной работе.

Настройте учетную запись пользователя для монтирования общего ресурса **Samba**:

```
# useradd -M -s /sbin/nologin sambashare
# smbpasswd -a sambashare
```

Добавьте учетные данные этой учетной записи пользователя в файл (например, **/etc/smbashare**). Содержание файла должно включать следующие директивы:

```
username=smbashare
password=smbasharepassword
```

Затем добавьте строку, подобную следующей, в **/etc/fstab**:

```
//server1.example.com/public /home/share cifs multiuser, credentials=/etc/smbashare 0 0
```

Обратите внимание, что параметры монтирования включают директиву **multiuser**. После монтирования файловой системы пользователям необходимо выполнить следующую команду, чтобы сохранить свои учетные данные в системном наборе ключей и получить доступ к содержимому шары:

```
$ cifscreds add server1.example.com
```

Лабораторная работа 7

Важно убедиться, что настроенная служба действительно запускается после перезагрузки. На самом деле, это лучше чтобы убедиться, что настроенная служба работает после пере маркировки **SELinux**, но этот процесс может занять несколько минут или больше. Кроме того, вполне возможно, что у вас не будет такого времени на экзамене.

1. Чтобы выполнить множество изменений конфигурации **Linux**, вы должны убедиться, что служба
1. запускаться автоматически при перезагрузке компьютера. В общем, ключевой командой является **systemctl**. В этом случае команда **systemctl enable smb nmb** устанавливает демоны **smbd** и **nmbd** в активными, когда вы загрузите **Linux** с **target** по умолчанию.
2. Вы можете использовать различные команды для выполнения упорядоченного выключения, такие как **shutdown**, **halt** и многое другое.
3. После перезагрузки вы должны проверить хотя бы одно соответствующее изменение настройки в **Samba SELinux** с помощью следующей команды:

```
# getsebool samba_enable_home_dirs
```

4. Кроме того, вы должны подтвердить, что соответствующие каталоги настроены с типом контекста файла **samba_share_t**, не только с помощью команды **ls -Z** в указанных каталогах, но и в файле **file_contexts.local** в каталоге **/etc/selinux/target/contexts/files**.