ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ
И ЭКСПОРТНОМУ КОНТРОЛЮ

Рекомендации по безопасной настройке программного обеспечения «Samba»

2026

Настройка программного обеспечения «Samba» в роли файлового сервера осуществляется путем редактирования файла конфигурации:

/etc/samba/smb.conf.

Для безопасной настройки программного обеспечения «Samba» необходимо выполнить следующие действия.

1. Настройка общего доступа.

1.1 Создать директорию общего доступа следующей командой в терминале:

sudo mkdir -p /srv/samba/share

sudo chmod -R 0777 /srv/samba/share.

1.2 Добавить следующий раздел в файл конфигурации:

[share]

comment = Общий доступ

path = /srv/samba/share

browseable = yes

read only = no

guest ok = yes

1.3 Для применения настроек перезапустить службу *smdb* программного обеспечения «Samba» следующей командой в терминале:

sudo systemctl restart smbd.

2. Произвести расширенные настройки.

2.1 Ограничить доступ внутри выделенной директории путем редактирования файла конфигурации в разделе *[public]*:

path = /srv/samba/public

guest ok = no

Кроме того, из раздела *[global]* необходимо удалить строку:

map to guest = Bad User

2.2 Необходимо указать только те подсети, доступ с которых необходим для работы, а также заблокировать входящий трафик в разделе *[global]*:

hosts allow = 192.168.0.0/24

hosts deny = 0.0.0.0/0

Номера указанных подсетей приведены в качестве примера.

2.3 Разграничить доступ к создаваемым файлам в общем разделе *[shared]*:

path = /srv/samba/shared

create mask = 0640

directory mask = 0750

2.4 Отключить NetBIOS (по возможности), а также использовать для SMB только порт 445/tcp в разделе *[global]*:

disable netbios = yes

smb ports = 445

Обеспечить защиту хоста с развернутым и настроенным Samba-сервером имеющимися средствами контроля сетевого трафика (например, iptables).

2.5 Отключить использование устаревшего протокола SMBv1 в разделе *[global]*:

server min protocol = SMB2

server max protocol = SMB3

Для применения расширенных настроек необходимо перезапустить службу smdb программного обеспечения «Samba» командой, указанной в пункте 1.3 настоящих рекомендаций.

3. Настройка аудита программного обеспечения «Samba».

3.1 Для настройки аудита в файле конфигурации в раздел *[global]* необходимо добавить следующие строки, например:

log level = 1 vfs:3

vfs objects = full_audit

full_audit:prefix = %u|%I|%S

full_audit:success = connect, open, mkdir, rmdir, unlink, write, rename, lock, pwrite, renameat, unlinkat

full_audit:failure = connect, open, mkdir, rmdir, unlink, write, rename

full_audit:facility = local5

full_audit:priority = notice

где:

log level = 1 vfs:3 – команда для осуществления журналирования базовых событий всех подсистем и расширенных событий подсистемы *vfs*. В данном

примере цифра «1» означает сбор событий по 1 уровню всех подсистем, параметр «*vfs:3*» означает сбор событий по 3 уровню для подсистемы *vfs*. Перечень подсистем и уровней журналирования прилагаются.

vfs objects = full_audit – команда для включения модуля журналирования для подсистемы v*fs*.

full_audit:prefix = %u|%I|%S – команда для осуществления записи действий пользователей по выбранным значениям. Перечень значений для команды *full_audit:prefix* прилагается.

full_audit:success = connect, open, mkdir, rmdir, unlink, write, rename, lock, pwrite, renameat, unlinkat – команда для осуществления записи успешных действий пользователей по выбранным значениям.

full_audit:failure = connect, open, mkdir, rmdir, unlink, write, rename – команда для осуществления записи неуспешных действий пользователей по выбранным значениям.

Перечень событий, фиксируемых командами *full_audit: success* и *full_audit:failure* прилагается.

full_audit:facility = local5 – команда, определяющая, что события аудита *syslog* будут направлены в категорию LOCAL5. (Необходимо предварительно определить для системы на уровне syslog категорию LOCAL5).

full_audit:priority = notice – команда, задающая уровень приоритета сообщений аудита. Перечень типов приоритета прилагается.

При осуществлении индивидуальной настройки каждой подсистемы необходимо руководствоваться перечнями подсистем, уровней журналирования, значений для команды *full_audit:prefix*, событий, фиксируемых командами *full_audit:success* и *full_audit:failure* и типов приоритета, указанными в приложении к настоящим рекоменедациям.

4. В целях проверки недостатков конфигурации программного обеспечения «Samba» необходимо выполнить следующие мероприятия.

4.1 Проверить шифрование при LDAP Bind.

4.1.1 Добавить запись (при ее отсутствии) в раздел *[global]* файла конфигурации:

[global]

ldap server require strong auth = yes

4.2 Осуществить настройку шифров Kerberos.

4.2.1 Добавить (изменить) запись (при ее отсутствии) в раздел *[libdefaults]* файла */etc/krb5.conf*:

[libdefaults]

permitted_enctypes = aes256-cts-hmac-sha1-96 aes128-cts-hmac-sha1-96

default_tgs_enctypes = aes256-cts-hmac-sha1-96

default_tkt_enctypes = aes256-cts-hmac-sha1-96

4.3 Ограничить доступ к каталогу SYSVOL следующими командами в терминале:

sudo chmod -R 775 /var/lib/samba/sysvol/

ls -ld /var/lib/samba/sysvol/

getfacl /var/lib/samba/sysvol/

4.4 Обеспечить ручное резервное копирование базы данных Active Directory раз в 90 дней.

4.4.1 При выключенном состоянии программного обеспечения «Samba» осуществить резервное копирование в выделенный каталог и внешний носитель информации следующей командой в терминале, например:

samba-tool domain backup offline –target-dir=/srv/ad-backup/

Указанная команда создает копию файлов базы данных Active Directory в директории */srv/ad-backup/*.

4.4.2 Ограничить права доступа к директории резервной копии.

4.5 Обеспечить регулярную ручную проверку состава группы Domain Admins следующей командой в терминале:

samba-tool group listmembers "Domain Admins"

Указанная команда выводит в терминал перечень всех учетных записей, входящих в группу Domain Admins, позволяющий выявлять нелегитимные записи, а также корректировать состав группы.

4.6 Обеспечить регулярную ручную проверку групповых политик базы данных Active Directory с использованием команды терминала:

samba-tool gpo listall

Указанная команда выводит в терминал перечень всех политик, зарегистрированных в каталоге SYSVOL и в базе Active Directory, позволяющий выявлять лишние записи, а также корректировать состав политик.

4.7 Осуществить настройку парольной политики (длина пароля должна быть не менее 15 символов, пароль должен содержать буквы верхнего и нижнего регистра (А-Я, A-Z, а-я, a-z), специальные символы (!, », №, %, *, /), в пароле не должно быть персонифицированной информации (имен, адресов, даты рождения, телефонов)).

samba-tool domain passwordsettings set --min-pwd-length=15

samba-tool domain passwordsettings set --complexity=on

samba-tool domain passwordsettings set --history-length=10

samba-tool domain passwordsettings set --max-pwd-age=90

где:

--min-pwd-length=15 — команда задает минимальную дину пароля 15 символов;

--complexity=on — команда включает необходимость использовать в пароле цифры, буквы и специальные символы;

--history-length=10 — команда запрещает после изменения использовать одинаковые пароли;

--max-pwd-age=90 — команда задает необходимость смены пароля через 90 дней после создания предыдущего.

Приложение 1

Таблица 1. Перечень подсистем

Подсистема	Описание
all	Включает все сообщения отладки и подходит для общего мониторинга системы
tdb	Отвечает за отладку работы с TDB (Trivial Database). TDB — это простая встраиваемая база данных, используемая программным обеспечением «Samba» для хранения различных данных, таких как сессии, аутентификационные данные, метаданные файлов и другие внутренние структуры
printdrivers	Используется для отладки драйверов печати. Этот класс полезен для отладки и анализа работы с принтерами, включая загрузку, установку и настройку драйверов
lanman	Предназначена для отладки протоколов LAN Manager, что может быть полезно при работе с устаревшими системами или приложениями
smb	Предназначена для регистрации вызовов по протоколу SMB
rpc_parse	Включает информацию об обработке RPC-сообщений. Может использоваться при анализе репликации
rpc_srv	Включает информацию о регистрации конечных точек RPC
rpc_cli	Предназначена для регистрации информации, связанной с работой RPC-клиента (Remote Procedure Call). Используется для отладки взаимодействия между клиентом и сервером в контексте RPC-вызовов, которые используются для выполнения различных операций в программном обеспечении «Samba», таких как управление доменными службами, доступ к общим ресурсам и другие действия, связанные с протоколами SMB/CIFS
passdb	Предназначена для регистрации доступа к хранилищу данных паролей
sam	Предназначена для регистрации событий, связанных с управлением учетными записями пользователей и групп в AD (SAM — Security Accounts Manager)
auth	Предназначена для регистрации событий аутентификации пользователей. Включает процессы проверки учетных данных (логин/пароль), использование Kerberos, NTLM и других механизмов аутентификации

winbind	Предназначена для регистрации сообщений при присоединении клиентов к программному обеспечению «Samba» для проведения различных операций. Позволяет анализировать работу сервиса Winbind
vfs	Предназначена для журналирования проблем с правами доступа и некорректным поведением бэкенда, абстрагируемого VFS
idmap	Предназначена для регистрации событий установки соответствия между SID и группами в Linux (Identity Mapping)
quota	Предназначена для регистрации информации, связанной с управлением квотами (quotas) на файловых системах. Квоты используются для ограничения объема дискового пространства, которое может использовать пользователь или группа
acls	Предназначена для регистрации событий проверки и изменения прав доступа на основе списков управления доступом (Access Control Lists)
locking	Предназначена для регистрации событий блокировок файлов базы данных каталога и конкретных записей при одновременном доступе к ним разных клиентов
msdfs	Предназначена для регистрации событий, связанных с поддержкой DFS (Distributed File System) в программном обеспечении «Samba». DFS позволяет объединять несколько общих ресурсов в одну виртуальную иерархию
dmapi	Предназначена для регистрации событий, связанных с использованием DMAPI (Data Management API) в программном обеспечении «Samba»
registry	Предназначена для регистрации взаимодействия с данными реестра Windows, которые используются в службе каталогов
scavenger	Предназначена для регистрации событий «сборки мусора» (garbage collection) в программном обеспечении «Samba». Этот процесс используется для очистки устаревших или неиспользуемых данных, таких как открытые файлы, сессии, аутентификации и другие ресурсы, которые больше не нужны
dns	Предназначена для регистрации запросов на поиск и изменение записей DNS
ldb	Предназначен для регистрации подключений к базе данных LDAP

tevent	Предназначен для регистрации сообщений библиотеки управления памятью talloc
auth_audit, auth_json_audit	Предназначены для регистрации событий аутентификации и авторизации учетных записей (успешных и неуспешных попытках входа в систему, изменениях паролей и изменениях статусов учетных записей). Могут использоваться, например, для отслеживания попыток несанкционированного входа
kerberos	Предназначен для регистрации событий взаимодействия по протоколу Kerberos
drs_repl	Предназначен для регистрации событий входящей и исходящей репликации на контроллере домена
smb2	Предназначен для регистрации вызовов по протоколу SMB (SMB2 и SMB3)
smb2_credits	Предназначен для регистрации запросов передачи данных по протоколу SMB. Записи содержат информацию о количестве переданных запросов и количестве запросов, которые осталось выполнить для завершения передачи файлов
dsdb_audit, dsdb_json_audit	Предназначены для регистрации изменений в базе данных контроллера домена программного обеспечения «Samba» (sam.ldb) (изменения пользователей, групп, разрешений, структуры каталога и т. д.)
dsdb_password_audit, dsdb_password_json_audit	Предназначены для регистрации событий изменения и сброса паролей
dsdb_transaction_audit, dsdb_transaction_json_audit	Предназначены для регистрации транзакций (фиксация, откат) в базе данных каталога. Могут использоваться для контроля целостности данных
dsdb_group_audit, dsdb_group_json_audit	Предназначены для регистрации изменений в составе групп

Таблица 2. Перечень уровней журналирования

Уровень	Назначение	Что записывается
0	**Только критические ошибки**	Это уровень по умолчанию для минимального ведения журнала, при котором регистрируются только сообщения о критических ошибках.
1	**Основные ошибки и важные события**	Стандартный рабочий уровень. Ошибки доступа, падения демонов, системные проблемы.
2	**Предупреждения и ошибки**	Регистрирует как предупреждения, так и ошибки, предоставляя более подробную информацию о проблемах, которые могут быть не критичными, но всё же требуют внимания.
3	**Базовая отладка**	Начинает включаться информация о доступе к файлам, базовые действия клиента.
4	**Подробная отладка клиента**	Углубленная информация о действиях клиента (например, открытие/закрытие файлов, чтение).
5	**Расширенная отладка**	Записываются внутренние вызовы функций, состояние соединений, авторизация.
6	**Больше внутренних данных**	Детали протоколов SMB, расширенная информация об операции.
7	**Очень подробная отладка**	Для разработчиков и глубокого аудита.
8	**Отладка сетевого уровня и внутренностей**	Всё о передаче данных, буферах, параметрах соединений и т.п.
9	**Максимальная отладка**	Все функции, все параметры, каждый шаг внутренней логики.
10	**Диагностика на уровне разработки**	Включает в себя всё: от высокоуровневых операций до низкоуровневой отладочной информации о внутренней работе программного обеспечения «Samba», включая время, сведения о подключении и даже детали на уровне пакетов.

Перечень значений для команды *full_audit:prefix*

%S - Имя текущей службы.

%P - Корневой каталог текущей службы.

%u - Пользователь текущей службы.

%g - Основная группа %u.

%U - Имя пользователя для сеанса.

%G - Основная группа %U.

%H - Домашний каталог пользователя.

%v - Версия программного обеспечения «Samba».

%h - Имя хоста, на котором работает программное обеспечение «Samba».

%m - NetBIOS имя компьютера клиента.

%L - NetBIOS имя сервера. Эта переменная может оказаться полезной в том случае, если вы на одном Samba-сервере запускаете несколько NetBIOS серверов.

%M - Имя хоста для компьютера клиента.

%N - Имя NIS (Network Information System) сервера домашних каталогов. Значение определяется при помощи настройки системы NIS auto.map.

%p - Путь к домашнему каталогу службы. Значение определяется при помощи файла настройки системы NIS auto.map. Запись в этом файле представляется как %N:%p.

%R - Выбранный после установления соединения уровень протокола.

%d - Номер текущего серверного процесса.

%a - Операционная система клиента.

%I - IP адрес клиентской машины.

%T - Текущие дата и время.

Таблица 3. Перечень событий, фиксируемых командами *full_audit: success* и *full_audit:failure*

Событие	**Описание**
chdir	Смена текущего каталога
chflags	Изменение флагов файла
chmod	Изменение прав доступа к файлу/каталогу
chmod_acl	Изменение прав доступа через ACL
chown	Смена владельца файла/каталога
close	Закрытие файла
closedir	Закрытие каталога (после opendir)
connect	Установка сетевого соединения
disconnect	Разрыв сетевого соединения
disk_free	Получение информации о свободном месте на диске
fchmod	Изменение прав файла по дескриптору
fchmod_acl	Изменение ACL по дескриптору
fchown	Смена владельца файла по дескриптору
fget_nt_acl	Получение ACL в формате NT по дескриптору
fgetxattr	Получение расширенного атрибута по дескриптору
flistxattr	Список расширенных атрибутов по дескриптору
fremovexattr	Удаление расширенного атрибута по дескриптору
fset_nt_acl	Установка NT ACL по дескриптору
fsetxattr	Установка расширенного атрибута по дескриптору
fstat	Получение информации о файле по дескриптору
fsync	Синхронизация данных файла с диском
ftruncate	Обрезка файла до заданного размера
get_nt_acl	Получение ACL в формате NT
get_quota	Получение квоты пользователя
get_shadow_copy_data	Получение информации о теневой копии
getlock	Получение состояния блокировки файла
getwd	Получение текущего рабочего каталога
getxattr	Получение расширенного атрибута файла
kernel_flock	Блокировка файла средствами ядра
link	Создание жесткой ссылки
linux_setlease	Установка lease на файл (особенность Linux)
listxattr	Список расширенных атрибутов файла
lock	Блокировка части файла
lseek	Изменение положения курсора в файле
lstat	Получение информации о символической ссылке
mkdir	Создание каталога
mknod	Создание специального файла (например, устройства)
open	Открытие файла
opendir	Открытие каталога
pread	Чтение из файла с указанного смещения
pwrite	Запись в файл с указанного смещения
read	Чтение данных из файла
readdir	Чтение содержимого каталога
readlink	Чтение содержимого символической ссылки
realpath	Получение абсолютного пути
removexattr	Удаление расширенного атрибута
rename	Переименование файла/каталога
rewinddir	Возврат к началу каталога (после readdir)

rmdir	Удаление каталога
seekdir	Установка позиции чтения каталога
sendfile	Копирование данных напрямую между файловыми дескрипторами
set_nt_acl	Установка NT ACL
set_quota	Установка квот
setxattr	Установка расширенного атрибута
stat	Получение информации о файле/каталоге
statvfs	Получение информации о файловой системе
symlink	Создание символической ссылки
sys_acl_delete_def_file	Удаление дефолтного ACL у файла
sys_acl_get_fd	Получение ACL по файловому дескриптору
sys_acl_get_file	Получение ACL по имени файла
sys_acl_set_fd	Установка ACL по файловому дескриптору
sys_acl_set_file	Установка ACL по имени файла
telldir	Получение текущей позиции в каталоге
unlink	Удаление файла
utime	Изменение времени последнего доступа/модификации
write	Запись данных в файл

Таблица 4. Перечень типов приоритета

Уровень	**Назначение**
emerg	Авария: система неработоспособна
alert	Требуется немедленное вмешательство
crit	Критические ошибки
err	Ошибки (ошибка уровня приложения)
warning	Предупреждения
notice	Нормальные, но важные события
info	Информационные сообщения
debug	Отладочная информация