Samba как контроллер домена AD

Введение

Данная статья основывается на материалах из wiki.samba.org

Samba, начиная с версии 4.0, может работать как контроллер домена (domain controller, DC) Active Directory (AD).

> При применении Samba в качестве DC AD в условиях реальной эксплуатации
> рекомендуется использовать два или более DC для обеспечения отказоустойчивости.

Эта статья рассказывает, как настроить Samba как первый DC в домене, чтобы построить новый лес AD.
Дополнительно, эту статью можно использовать для миграции из домена Samba NT4 в домен Samba AD.

> Если требуется подключить Samba к уже существующему доменному лесу AD, как дополнительный DC
>
> - Для быстрого подключения с помощью графического инструмента fly-admin-ad-server см. Samba: инструменты Astra Linux для быстрой настройки
> - Подробные инструкции см. Присоединение Samba DC к существующему домену Active Directory.

Samba при использовании в роли AD DC поддерживает:

- Интегрированый сервер LDAP как база данных AD. Подробности см. Поддерживают ли Samba AD DC работу с OpenLDAP или другими службами LDAP?;
- Авторизацию через службу Kerberos Key Distribution Center (KDC). Поддерживаются варианты MIT KDC и Heimdal KDC.
  Поставляемая в составе ОС ОН Орёл 2.21 и ОС СН Смоленск 1.6 Samba использует MIT KDC, также поставляемый в составе этих ОС;
- Работу с встроенным сервером DNS
- Работу с внешним сервером DNS (в примерах ниже рассматривается работа с сервером DNS BIND9)

Быстрая установка и настройка контроллера и клиента домена

Подготовка к инсталляции

- Выберите имя хоста для вашего AD DC;
  Никогда не используйте в качестве имен хостов такие идентификаторы, как PDC или BDC, унаследованные от NT4 .
  Эти сущности отсутствуют в AD, и такие названия вызывают путаницу;

- Выберите DNS-имя для вашего доменного леса AD. Это имя также будет использовано как имя области (realm) Kerberos AD ;

  > Для создания домена AD используйте DNS-имя, которое не понадобится изменять.
  > Samba не поддерживает переименование зон DNS AD и областей Kerberos.

- Используйте для DC статический адрес. Дополнительную информацию см. Часто задаваемые вопросы по именованию доменов AD
- Отключите инструменты (например, resolvconf), которые автоматически обновляют файл настроек DNS /etc/resolv.conf.
  AD DC и члены домена обязаны использовать сервер DNS, способный разрешать зоны DNS AD .

- Убедитесь, что файл /etc/hosts на DC корректно разрешает полное доменное имя (fully-qualified domain name, FQDN) и короткое имя хоста DC во внешний сетевой IP-адрес DC.
  Например:

  > 127.0.0.1 localhost.localdomain localhost
  > 10.0.2.254 DC.samdom.example.com DC

  имя хоста не должно разрешаться в IP-адрес 127.0.0.1 или в любой другой IP-адрес, кроме используемого на внешнем сетевом интерфейсе DC

Детальная настройка

Подготовка к инсталляции

- Выберите имя хоста для вашего AD DC;
  Никогда не используйте в качестве имен хостов такие идентификаторы, как PDC или BDC, унаследованные от NT4 .
  Эти сущности отсутствуют в AD, и такие названия вызывают путаницу;

- Выберите DNS-имя для вашего доменного леса AD. Это имя также будет использовано как имя области (realm) Kerberos AD ;

  > Для создания домена AD используйте DNS-имя, которое не понадобится изменять.
  > Samba не поддерживает переименование зон DNS AD и областей Kerberos.

- Используйте для DC статический адрес. Дополнительную информацию см. Часто задаваемые вопросы по именованию доменов AD
- Отключите инструменты (например, resolvconf), которые автоматически обновляют файл настроек DNS /etc/resolv.conf.
  AD DC и члены домена обязаны использовать сервер DNS, способный разрешать зоны DNS AD .

- Убедитесь, что файл /etc/hosts на DC корректно разрешает полное доменное имя (fully-qualified domain name, FQDN) и короткое имя хоста DC во внешний сетевой IP-адрес DC.
  Например:

  > 127.0.0.1 localhost.localdomain localhost
  > 10.0.2.254 DC.samdom.example.com DC

  имя хоста не должно разрешаться в IP-адрес 127.0.0.1 или в любой другой IP-адрес, кроме используемого на внешнем сетевом интерфейсе DC
- Если Samba уже была установлена (настроена):

  - Убедитесь, что все процессы Samba остановлены:

```
ps ax | egrep "samba|smbd|nmbd|winbindd"
```

  - Если вывод команды показывает наличие любого из процессов samba, smbd, nmbd, или winbindd, то остановите эти процессы:

```
sudo systemctl stop samba
sudo systemctl stop smbd
sudo systemctl stop nmbd
sudo systemctl stop winbind
```

:

- `winbind 'd'`
- `winbindd 'dd'`
- `winbind 'd'`

- Удалите все существующие файлы конфигурации Samba smb.conf file. Чтобы получить список путей к этим файлам:

```
smbd -b | grep "CONFIGFILE"
CONFIGFILE: /usr/local/samba/etc/samba/smb.conf
```

- Удалите все файлы баз данных Samba (*.tdb и *.ldb). Чтобы получить список путей к этим файлам:

```
smbd -b | egrep "LOCKDIR|STATEDIR|CACHEDIR|PRIVATE_DIR"
LOCKDIR: /usr/local/samba/var/lock/
STATEDIR: /usr/local/samba/var/locks/
CACHEDIR: /usr/local/samba/var/cache/
PRIVATE_DIR: /usr/local/samba/private/
```

Только полная очистка настроек поможет предотвратить ошибки, и гарантирует, что никакие файлы из предыдущей настроки Samba не попадут в новые настройки DC.

- Если существует файл настроек Kerberos /etc/krb5.conf file, также удалите его:

```
sudo rm /etc/krb5.conf
```

Установка Samba

Пакет Samba входит в дистрибутивы ОСОН Орёл и ОССН Смоленск, и может быть установлен с помощью графического менеджера пакетов, или из командной строки командой

```
sudo apt install samba
```

После установки сервис smbd будет запущен автоматически с настройками "по умолчанию".

Для использования samba в качестве домена AD нужно установить дополнительные пакеты:

```
sudo apt install winbind libpam-winbind libnss-winbind libpam-krb5 krb5-config krb5-user krb5-kdc samba-dsdb-modules
```

Назначение Samba на роль AD DC

В английском языке для настройки Samba в роли AD DC используется термин "provisioning", в данном тексте в качестве перевода будет использоваться термин "назначение".

В процессе назначения Samba на роль AD DC создаются базы данных AD и в них добавляются базовые записи, такие как учетная запись администратора домена, и необходимые записи DNS.

При осуществлении миграции из домена Samba NT4 в домен AD, этот шаг следует пропустить, и выполнить стандартное обновление.
Детали см. Миграция домена Samba NT4 в домен Samba AD (стандартное обновление).

Выполнение настроек AD требует наличия привилегий суперпользователя для создания файлов и установки прав.

Назначение Samba на роль DC выполняется с помощью команды samba-tool domain provision.
Эта команда поддерживает параметры для выполнения настроек в интерактивном или автоматическом режимах. Подробности см.:

samba-tool domain provision --help

При создании нового домена AD рекомендуется сразу включить так называемые расширения NIS (NIS extensions), передав инструменту samba-tool domain provision параметр --use-rfc2307.
Это позволит хранить в AD специфические атрибуты Unix:

- Числовые идентификаторы пользователей (UID);
- Пути у домашним каталогам;
- Идентификаторы групп.

Включение расширений NIS при установке не влечёт за собой никаких отрицательных побочных эффектов, а их включение в существующем домене требует ручного расширения схемы AD.

Подробности см. в:

- Настройка RFC2307 в AD
- idmap config = ad

Описание применяемых параметров

При назначении будут применяться следующие параметры:

Интерактивный режим	Автоматический режим	Комментарий
--use-rfc2307	--use-rfc2307	Включает расширения NIS
Realm	--realm	Область Kerberos. Также, используется как домен DNS AD . Например: samdom.example.com.
Domain	--domain	Имя домена для NetBIOS. Рекомендуется использовать первую часть имени домена DNS AD. Например, для домена samdom.example.com это будет имя samdom.
Server Role	--server-role	Устанавливает роль контроллера DC.
DNS backend	--dns-backend	Выбирает службу DNS. Первый DC в домене AD обязательно должен быть настроен на использование какой-либо службы DNS. Отметим, что вариант службы BIND9_FLATFILE более не поддерживается.
DNS forwarder IP address	недоступно	Эта настройка доступна только при выборе службы DNS SAMBA_INTERNAL DNS. Подробности см. Настройка перенаправления DNS.
Administrator password	--adminpass	Устанавливает пароль администратора домена. Если заданный пароль не будет соответствовать требованиям по сложности пароля, назначение не будет выполнено. Подробности см. Microsoft TechNet: Сложность паролей должна соответствовать требованиям.

Другие параметры, часто используемые в команде samba-tool domain provision:

--option="interfaces=lo eth0" --option="bind interfaces only=yes": Если сервер имеет несколько сетевых интерфейсов, используйте эти параметры для привязки Samba к нужным интерфейсам. Это позволить команде samba-tool зарегистрировать корректный сетевой адрес при настройке.

- Не используйте NONE как службу DNS, эта возможность больше не поддерживается;
- При использовании в качестве службы DNS службы BiIND, не используйте вариант BIND9_FLATFILE, эта возможность больше не поддерживается;
- После назначения первого DC в домене AD не настраивайте больше таким способом никакие другие DC в этом домене, используйте процедуру присоединение (Join) для настройки остальных DC.

Назначение Samba в интерактивном режиме

Для назначения Samba в интерактивном режиме выполните команду:

```
samba-tool domain provision --use-rfc2307 --interactive
```

После этого должен произойти примерно такой диалог:

```
# Запрашивается имя области Kerberos
Realm [SAMDOM.EXAMPLE.COM]: SAMDOM.EXAMPLE.COM

# Запрашивается имя домена
Domain [SAMDOM]: SAMDOM

# Запрашивается роль сервера
Server Role (dc, member, standalone) [dc]: dc

# Выбирается служба DNS
DNS backend (SAMBA_INTERNAL, BIND9_FLATFILE, BIND9_DLZ, NONE) [SAMBA_INTERNAL]: BIND9_DLZ

# Выбирается IP-адрес для перенаправления запросов DNS
DNS forwarder IP address (write 'none' to disable forwarding) [10.0.2.254]: 8.8.8.8

# Ввод и подтверждение пароля администратора
Administrator password: Passw0rd
Retype password: Passw0rd
```

Looking up IPv4 addresses
Looking up IPv6 addresses
No IPv6 address will be assigned
Setting up share.ldb
Setting up secrets.ldb
Setting up the registry
Setting up the privileges database
Setting up idmap db
Setting up SAM db
Setting up sam.ldb partitions and settings
Setting up sam.ldb rootDSE
Pre-loading the Samba 4 and AD schema
Adding DomainDN: DC=samdom,DC=example,DC=com
Adding configuration container
Setting up sam.ldb schema
Setting up sam.ldb configuration data
Setting up display specifiers
Modifying display specifiers
Adding users container
Modifying users container
Adding computers container
Modifying computers container
Setting up sam.ldb data
Setting up well known security principals
Setting up sam.ldb users and groups
Setting up self join
Adding DNS accounts
Creating CN=MicrosoftDNS,CN=System,DC=samdom,DC=example,DC=com
Creating DomainDnsZones and ForestDnsZones partitions
Populating DomainDnsZones and ForestDnsZones partitions
Setting up sam.ldb rootDSE marking as synchronized
Fixing provision GUIDs
A Kerberos configuration suitable for Samba 4 has been generated at /usr/local/samba/private/krb5.conf
Setting up fake yp server settings
Once the above files are installed, your Samba4 server will be ready to use
Server Role: active directory domain controller
Hostname: DC
NetBIOS Domain: SAMDOM
DNS Domain: samdom.example.com
DOMAIN SID: S-1-5-21-2614513918-2685075268-614796884

Интерактивный режим настройки поддерживает различные параметры команды samba-tool domain provision, что позволяет задавать настройки, не содержащиеся в интерактивном диалоге.

Назначение Samba в автоматическом режиме

Для примера назначения Samba в автоматическом режиме используем следующие параметры:

- Роль сервера: dc
- Расширения NIS: включены
- Служба DNS: внутренний DNS BIND9_DLZ
- Область Kerberos и зона DNS AD: samdom.example.com
- Имя домена для NetBIOS: SAMDOM
- Пароль администратора: Passw0rd
- Используется сеть 10.0.2.0/24
- Адрес хоста Samba 10.0.2.254

Для указанных параметров команда назначения будет выглядеть так:

```
samba-tool domain provision --server-role=dc --use-rfc2307 --dns-backend=BIND9_DLZ --realm=SAMDOM.EXAMPLE.COM --domain=SAMDOM --adminpass=Passw0rd
```

Настройка запуска служб после назначения

После выполнения назначения следует включить автоматический запуск служб AD DC:

```
systemctl unmask samba-ad-dc
systemctl enable samba-ad-dc
```

Настройка Kerberos

Общий сервер Kerberos-Samba

Остановить службу Kerberos:

```
sudo systemctl stop krb5-kdc
```

Запретить автоматический запуск службы Kerberos:

```
sudo systemctl disable krb5-kdc
```

Скопировать автоматически созданные при назначении Samba файлы /var/lib/samba/private/kdc.conf /var/lib/samba/private/krb5.conf и в рабочую конфигурацию Kerberos KDC и клиента Kerberos:

```
sudo cp -b /var/lib/samba/private/kdc.conf /etc/krb5kdc/kdc.conf
sudo cp -b /var/lib/samba/private/krb5.conf /etc/krb5.conf
```

После выполнения вышеуказанных операций служба Kerberos krb5-kdc будет автоматически запускаться вместе с остальными доменными службами Samba.

Отдельный сервер Kerberos

В разработке.

Запуск Samba AD DC

После выполнения назначения и завершения настроек службу следует запустить командой samba:

```
samba
```

Настройка службы DNS AD

Пропустите этот шаг, если используется служба DNS SAMBA_INTERNAL.

Настройте и запустите сервер DNS BIND9 и модуль BIND9_DLZ. Подробности см. Настройка сервера DNS BIND

Проверить правильность работы сервиса для использованного в примере домена samdom.example.com можно с помощью команды dig:

```
dig samdom.example.com
```

Ответ должен выглядеть примерно так:

```
; <<>> DiG 9.10.3-P4-Debian <<>> samdom.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17101
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;samdom.example.com. IN A

;; ANSWER SECTION:
samdom.example.com. 900 IN A 10.0.2.254

;; AUTHORITY SECTION:
samdom.example.com. 900 IN NS dhcp.samdom.example.com.

;; ADDITIONAL SECTION:
dhcp.samdom.example.com. 900 IN A 10.0.2.254
```

;; Query time: 0 msec
;; SERVER: 10.0.2.254#53(10.0.2.254)
;; WHEN: Mon Sep 17 11:24:12 MSK 2018
;; MSG SIZE rcvd: 98

Настройка DNS участников домена

Участники домена AD используют DNS для поиска сервисов, например, таких, как LDAP и Kerberos. Для этого они должны использовать сервер DNS, способный разрешать зоны DNS AD.

Если в системе используется сервер DHCP, то в его настройках можно указать имя домена, которое будет передаваться всем хостам при запросе адреса
Подробнее см. DHCP

Помимо использования DHCP, настройку на нужный сервер можно выполнить непосредствнно на хостах - участниках домена в файле /etc/resolv.conf.
Для этого укажите в файле:

- имя домена DNS AD как имя домена для поиска (search),
- IP-адрес вашего DC как значение параметра nameservere.

Например:

```
search samdom.example.com
nameserver 10.0.2.254
```

Создание реверсивной зоны

С помощью команды samba-tool dns zonecreate можно добавить необязательную зону реверсивного поиска:

```
samba-tool dns zonecreate -U Administrator samdom.example.com 2.0.10.in-addr.arpa

Password for [administrator@SAMDOM.EXAMPLE.COM]:
Zone 2.0.10.in-addr.arpa created successfully
```

Если требуется использовать несколько реверсивных зон, просто выполните команду несколько раз с указанием параметров соответствующих подсетей.
Изменение реверсивных зон не требует перезапуска сервисов Samba или BIND.

Участники домена

При работе в домене AD, Kerberos используется для аутентификации пользователей, хостов, и сервисов.

Процедуры установки и настройки клиентов Kerberos см. Kerberos

Во время процедуры назначения Samba создает конфигурационный файл /vat/lib/samba/private/krb5.conf для клиентов Kerberos, настроенный на создаваемый DC.
Это файл должен быть скопирован в рабочую конфигурацию Kerberos на хостах, входящих в домен. Например:

```
cp -b /var/lib/samba/private/krb5.conf /etc/krb5.conf
```

Так как автоматически создаваемый файл конфигурации Kerberos настраивает клиентов Kerberos на использование сервисных записей DNS (SRV) для поиска контроллера Kerberos (KDC),
в домене должна быть правильно настроена и работать служба DNS.

Тестирование Samba AD DC

Для ручного запуска сервиса samba в режиме AD DC используйте команду:

```
samba
```

Samba не поддерживает инициализационные сценарии System V, systemd, upstart, или иные файлы конфигурации сервисов.

Если Samba была установлена с использованием системы пакетов, то для запуска Samba следует использовать сценарии или файлы конфигурации, включенные в пакет.
Если вы собирали Samba самостоятельно, см. Управление сервисом Samba AD DC.

Тестирование файлового сервера

Во время назначения автоматически создаются разделяемые ресурсы netlogon и sysvol, и они обязательно должны существовать в DC.
Чтобы увидеть все разделяемые файловые ресурсы, предоставляемые DC:

```
smbclient -L localhost -U%
```

```
Domain=[SAMDOM] OS=[Unix] Server=[Samba x.y.z]

Sharename Type Comment
--------- ---- -------
netlogon Disk
sysvol Disk
IPC$ IPC IPC Service (Samba x.y.z)
Domain=[SAMDOM] OS=[Unix] Server=[Samba x.y.z]

Server Comment
--------- -------

Workgroup Master
--------- -------
```

Для проверки работы аутентификации, подключитесь к ресурсу netlogon с использованием учётной записи администратора домена:

```
smbclient //localhost/netlogon -UAdministrator -c 'ls'
```

```
Enter Administrator's password:
Domain=[SAMDOM] OS=[Unix] Server=[Samba x.y.z]
. D 0 Tue Nov 1 08:40:00 2016
.. D 0 Tue Nov 1 08:40:00 2016

49386 blocks of size 524288. 42093 blocks available
```

Если тесты не выполняются, см. Поиск и устранение проблем

Тестирование DNS

Чтобы убедиться, что AD DNS работает корректно, запросим некоторые записи DNS:

- SRV-запись доменного сервиса _ldap по протоколу TCP:

```
host -t SRV _ldap._tcp.samdom.example.com.
_ldap._tcp.samdom.example.com has SRV record 0 100 389 dc.samdom.example.com.
```

- SRV-запись доменного сервиса _kerberos по протоколу UDP:

```
host -t SRV _kerberos._udp.samdom.example.com.
_kerberos._udp.samdom.example.com has SRV record 0 100 88 dc.samdom.example.com.
```

- A-запись контроллера домена:

```
host -t A dc.samdom.example.com.
dc.samdom.example.com has address 10.99.0.1
```

Если тесты не выполняются, см. Поиск и устранение проблем

Проверка Kerberos

Получение билета Kerberos для учетной записи администратора домена:

```
kinit administrator
Password for administrator@SAMDOM.EXAMPLE.COM:
```

Если имя принципала не задано в в виде user@REALM, то название области Kerberos добавится автоматически.

Имена областей Kerberos всегда пишутся заглавными буквами.

Список кешированных билетов Kerberos:

```
klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: administrator@SAMDOM.EXAMPLE.COM

Valid starting Expires Service principal
01.11.2016 08:45:00 12.11.2016 18:45:00 krbtgt/SAMDOM.EXAMPLE.COM@SAMDOM.EXAMPLE.COM
renew until 02.11.2016 08:44:59
```

Если тесты не выполняются, см. Поиск и устранение проблем

Настройка синхронизации времени

Kerberos требует синхронизации времени от всех участников домена. Подробности см. в Настройка NTP или в Синхронизация времени.

Управление Samba AD DC из командной строки

Инструмент samba-tool

Для управления Samba AD DC в состав пакета Samba входит инструмент командной строки samba-tool.

Основные команды иструмента:

Команда	Описание
dbcheck	Проверка локальной базы данных AD на наличие ошибок
delegation	Управление делегированием
dns	Управление параметрами доменной службы DNS
domain	Управление параметрами домена
drs	Управление службой репликации каталогов (Directory Replication Services, DRS)
dsacl	Управление списками контроля доступа DS
fsmo	Управление ролями (Flexible Single Master Operations, FSMO)
gpo	Управление групповыми политиками
group	Управление группами
ldapcmp	Сравнение двух баз данных ldap
ntacl	Управление списками контроля доступа ACL
processes	Вывод списвка процессов (для упрощения отладки без использования setproctitle).
rodc	Управление контроллером домена (Read-Only Domain Controller, RODC)
sites	Управление сайтами
spn	Управление службой принципалов (Service Principal Name, SPN)
testparm	Проверка конфигурационного файла на корректность синтаксиса
time	Получение показаний текущего времени сервера

user	Управление пользователями
visualize	Графическое представление состояния сети Samba

Подробная информация об инструменте доступна в справочнике man:

```
man samba-tool
```

Краткую справку по работе инструмента можно получить командой

```
samba-tool -h
```

Инструмент wbinfo

При установке пакета samba автоматически устанавливается служба winbindd.

Для работы с этой службой используется инструмент командной строки wbinfo,
позволящий получать информацию о пользователях и группах AD.

Примеры команд:

Команда	**Описание**
wbinfo -u	Вывести список пользователей
wbinfo -g	Вывести список групп
wbinfo -i имя_пользователя	Вывести подробную информацию о пользователе
wbinfo -? wbinfo --help	Вывести справку по командам

Настройка хостов - участников домена для входа доменных пользователей

По умолчанию, пользователи домена AD не могут выполнять вход в Linux-системы.
Для обеспечения входа в Linux-системы с учетными записями Active Directory необходимо внести следующие изменения в настройки Samba AD DC в настройки пользовательских компьютеров.

Настрока Samba AD DC

В конфигурационном файле Samba /etc/samba/smb.conf необходимо добавить настройки службы winbind и разрешение авторизоваться через эту службу (добавленные строки выделены жирным шрифтом):

```
[global]
    netbios name = DHCP
    realm = SAMDOM.EXAMPLE.COM
    server role = active directory domain controller
    server services = s3fs, rpc, nbt, wrepl, ldap, cldap, kdc, drepl, winbindd, ntp_signd, kcc, dnsupdate
    workgroup = SAMDOM
    idmap_ldb:use rfc2307 = yes

    template shell = /bin/bash
    winbind use default domain = true
    winbind offline logon = false
    winbind nss info = rfc2307

    winbind enum users = yes
    winbind enum groups = yes
```

После внесения изменений проверить правильность конфигурации командой

```
testparm
```

И перезапустить службы samba.

Настройка пользовательских компьютеров

На пользовательском компьютере использовать команду

```
pam-auth-update
```

И убедиться, что включены все профили PAM.
При необходимости - включить аутентификацию winbind, используя клавишу "пробел".
По окончании нажать клавишу "Tab", перейти на "OK", и записать изменения.

В файле /etc/nsswitch.conf добавить слово winbind параметры password и group:

```
# /etc/nsswitch.conf
#
# Example configuration of GNU Name Service Switch functionality.
# If you have the `glibc-doc-reference' and `info' packages installed, try:
# `info libc "Name Service Switch"' for information about this file.

passwd: compat winbind
group: compat winbind
shadow: compat

hosts: files dns
networks: files

protocols: db files
services: db files
ethers: db files
rpc: db files

netgroup: nis
```

Чтобы пользователи AD после аутентификации могли менять свой пароль из командной строки в файле /etc/pam.d/common-password из строки `password [success=1 default=ignore] pam_winbind.so use_authtok try_first_passfile` убрать слово `use_authtok statement:`

password [success=1 default=ignore] pam_winbind.so ~~use_authtok~~ try_first_pass

Предупреждение: Использование контроллера домена как файлового сервера

Несмотря на то, что Samba в режиме AD DC может предоставлять услуги разделения файлов так же, как и в любом другом режиме применения, разработчкики Samba не рекомендуют использовать DC как файловый север по следующим причинам:

- Для всех организаций, за исключением самых маленьких, наличие более, чем одного DC, является реально хорошим способом резервирования, повышающим безопасность обновлений;
- Отсутсвие сложных данных и влияния на другие сервисы позволяет обновлять DC совместно с ОС хоста каждые год или два;
- Обновления могут выполняться путем установки новых версий, или внесения изменений, которые лучше проверены в Samba, что позволяет получить новые возможности, избежав множества рисков, связанных с повреждением данных;
- Необходимость модернизации DC и файлового сервера наступает в разные моменты. Потребность в новых возможностях DC и файлового сервера возникает в разные моментв времени. В то время, как AD DC стремительно развивается, приобретая новые возможности, файловый сервер, после более 20 лет, гораздо более консервативен;
- mandatory smb signing is enforced on the DC.

Если вы изучаете возможность использовать Samba DC как файловый сервер, рассмотрите вместо этого возможность использовать на DC виртуальную машину VM, содержащую отдельного участника домена.

Если вы вынуждены использовать Samba DC как файловый сервер, помните, что виртуальная файловая система (virtual file system, VFS) позволяет настраивать разделяемые ресурсы только со списками управления доступом access (control lists, ACL) Windows.
Разделяемые ресурсы с ACL POSIX на Samba DC не поддерживаются, и не работают.

Для предоставления сетевх разделяемых ресурсов с полными возможностями Samba, используйте отдельного участника домена Samba.

Подробности см.:

- Настройка Samba как участника домена
- Файловый сервис Samba

Если у вас маленький домен (маленький офис, домашняя сеть), нет желания следовать рекомендациям разработчиков Samba, и DC используется как файловый серверr, настройте Winbindd до начала настройки раздеяемых ресурсов.
Подробности см.: Configuring Winbindd on a Samba AD DC.

Поиск и устранение проблем

Продробности см.: Поиск и устранение проблем в Samba AD DC

Материалы для дальнейшего изучения

См. Пользовательская документация