ДОКУМЕНТАЦИЯ ALT LINUX TEAM

Доменная инфраструктура на базе Samba

Руководство администратора

Редакция апрель, 2024

Аннотация

Samba может выступать в роли контроллера домена и сервиса Active Directory.

Данное руководство соответствует текущему состоянию сведений, но какие-либо окончательные правки могли не попасть в него. В случае обнаружения ошибок и неточностей в руководство вносятся изменения.

Глава 1. Введение

1.1. Основные сведения о логической модели AD

Домен

Группа компьютеров, пользователей, принтеров и других объектов, совместно использующих общую БД каталога.

Дерево доменов

Иерархическая система доменов, имеющая единый корень (корневой домен).

Лес доменов

Множество деревьев доменов, находящихся в различных формах доверительных отношений.

Сервер

Компьютер, выполняющий определённые роли в домене.

Контроллер домена

Сервер, хранящий каталог и обслуживающий запросы пользователей к каталогу. Помимо хранения данных контроллер домена может выступать в качестве одной из FSMO-ролей.

Организационное подразделение (OU)

Субконтейнер в домене, который может содержать различные объекты AD: другие контейнеры, группы, аккаунты пользователей и компьютеров. OU представляет собой единицу административного управления внутри домена, на который администратор может назначить объекты групповых политик и назначить разрешения другим пользователем.

Группа

Объекты, являющиеся участниками системы безопасности (security principals) и предназначенные для управления доступом к ресурсам. Каждой группе присваивается уникальный идентификатор безопасности (Security Identifier, SID), который сохраняется в течение всего срока службы.

Группы — это объекты, являющиеся участниками системы безопасности (security principals) и предназначенные для управления доступом к ресурсам. Каждой группе присваивается уникальный идентификатор безопасности (Security Identifier, SID), который сохраняется в течение всего срока службы.

1.2. Схема стенда

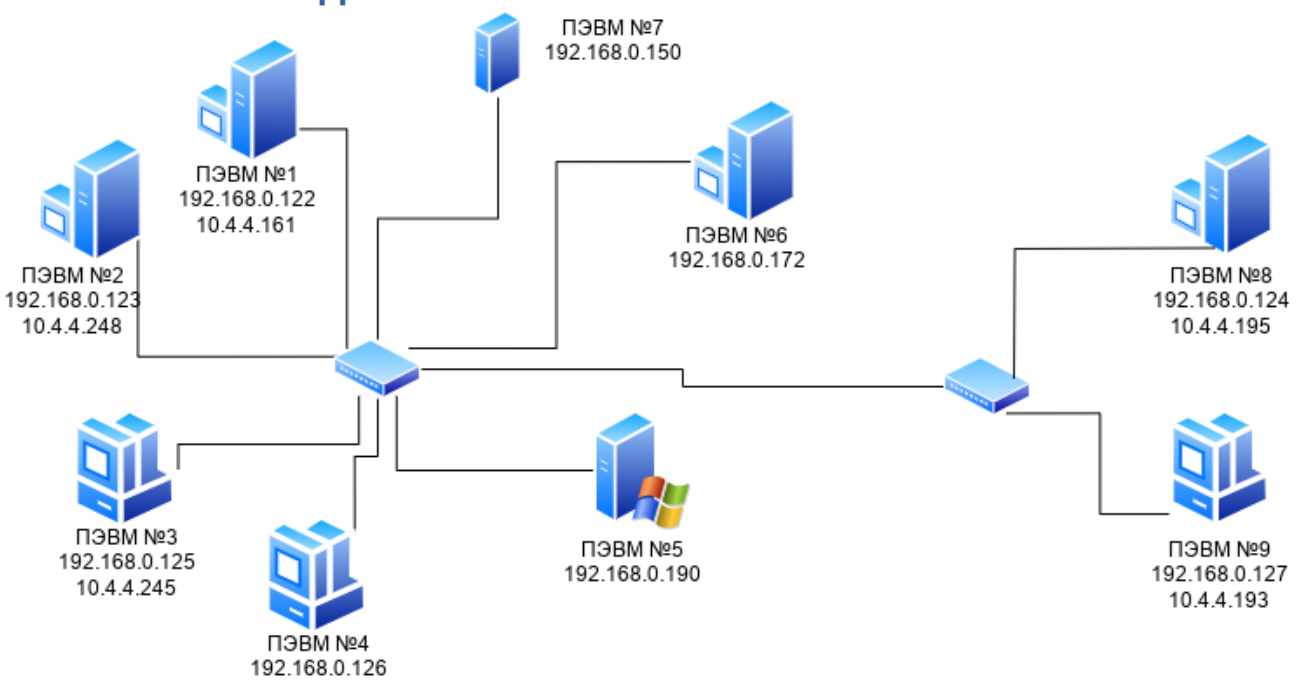


Таблица 1.1. Состав технических и программных средств стенда

№ ПЭВМ	Программная среда	Описание
1	ОС «Альт Сервер»	Контроллер домена test.alt
2	ОС «Альт Сервер»	Дополнительный контроллер домена test.alt
3	ОС Альт («Альт Рабочая станция», «Альт Рабочая станция К», «Альт Образование»)	Рабочая станция
4	ОС Альт («Альт Рабочая станция», «Альт Рабочая станция К», «Альт Образование»)	Рабочая станция
5	ОС Microsoft Windows Server 2012	Контроллер домена win.alt
6	ОС «Альт Сервер»	Контроллер домена example.alt
7	ОС «Альт Сервер»	Веб-сервер, прокси-сервер
8	ОС «Альт Сервер»	Контроллер домена test.alt только для чтения (RODC)
9	ОС Альт («Альт Рабочая станция», «Альт Рабочая станция К», «Альт Образование»)	Рабочая станция

Параметры домена:

- домен AD — test.alt;

- сервер AD (ОС ALT) — dc1.test.alt (192.168.0.122);
- дополнительный сервер AD (ОС ALT) — dc2.test.alt (192.168.0.123);
- RODC (ОС ALT) — rodc.test.alt (192.168.0.124);
- веб-сервер, прокси-сервер (ОС ALT) — web.test.alt (192.168.0.150);
- рабочая станция 1 (ОС ALT) — host-01.test.alt (192.168.0.125);
- рабочая станция 2 (ОС ALT) — host-02.test.alt (192.168.0.126);
- рабочая станция 3 (ОС ALT) — host-03.test.alt (192.168.0.127);
- имя пользователя-администратора — Administrator;
- пароль администратора — Pa$$word.

Дополнительные домены:

- win.alt: сервер AD (ОС Windows) — dc1.win.alt (192.168.0.190);
- example.alt: сервер AD (ОС ALT) — s1.example.alt (192.168.0.172).

Глава 2. Создание контроллера домена Active Directory на базе Samba

Использование Samba 4 в роли контроллера домена Active Directory позволяет вводить Windows 7/8 в домен без манипуляций с реестром.

Поддерживаются следующие базовые возможности Active Directory:

- аутентификация рабочих станций Windows и Linux и служб;
- авторизация и предоставление ресурсов;

- групповые политики (GPO);
- перемещаемые профили (Roaming Profiles);
- поддержка инструментов Microsoft для управления серверами (Remote Server Administration Tools) с компьютеров под управлением Windows;
- поддержка протоколов SMB2 и SMB3 (в том числе с поддержкой шифрования).

Предупреждение

Samba AD DC конфликтует с OpenLDAP и MIT Kerberos, поскольку эти приложения запускают одни и те же службы на одних тех же, по умолчанию, портах для протоколов LDAP и Kerberos.

Предупреждение

Samba AD DC функционирует на уровне контроллера доменов Windows 2008 R2 . Можно ввести его в домен Windows 2012 как клиента, но не как контроллер домена.

2.1. Подготовка системы к установке сервера Samba AD DC

В этом разделе перечислены требования для установки сервера Samba AD DC. Перед установкой необходимо убедиться, что система соответствует этим требованиям.

Примечание

Для установки сервера Samba AD DC нужны привилегии суперпользователя.

Примечание

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

2.1.1. Системные требования к серверу Samba AD DC

2.1.1.1. RAM

https://samba.tranquil.it/doc/en/samba_fundamentals/samba_server_dimensionning.html

Для демонстрационной/тестовой системы рекомендуется 2 ГБ.

Для производственной установки рекомендуется не менее 4 ГБ ОЗУ, а затем 2 ГБ на каждую дополнительную 1000 пользователей.

Примечание

Параметр, который оказывает наибольшее влияние на требования к памяти, — это количество одновременных открытий сеансов.

2.1.1.2. Размеры хранилища

10 ГБ достаточно для доменов с несколькими сотнями пользователей.

Также, при планировании размера хранилища, необходимо учесть:

- уровни журналов и политику хранения журналов;
- использование изображений/аватаров для идентификации пользователей;
- количество пользователей, машин и групп;
- место под резервные копии.

2.1.1.3. CPU

Для нескольких сотен пользователей достаточно 4 vCPUs.

Некоторые процессы Samba не являются многопоточными, поэтому увеличение числа процессоров не повысит производительность.

Чтобы сбалансировать нагрузку, необходимо создать второй контроллер домена в репликации с первым и применить политику балансировки нагрузки на уровне клиента.

Необходимое количество контроллеров домена зависит от нескольких параметров:

- количество сторонних приложений LDAP, подключенных к AD;
- качество кода сторонних LDAP-приложений, подключенных к AD;
- количество запросов к файловым серверам.

2.1.1.4. DNS

Не следует использовать существующий домен, если вы не являетесь владельцем домена. Рекомендуется использовать зарезервированный домен верхнего уровня RFC2606 (**`https://tools.ietf.org/html/rfc2606`**) для частных тестовых установок, например alt.test.

Имя домена для разворачиваемого DC должно состоять минимум из двух компонентов, разделённых точкой.

Важно

Необходимо избегать суффиксов .local. При указании домена, имеющего суффикс .local, потребуется на сервере и подключаемых компьютерах под управлением Linux отключить службу **`avahi-daemon`**.

Примечание

Имя контроллера домена Samba AD не должно превышать 15 символов (ограничение связано с ***sAMAccountName*** в Active Directory).

2.1.2. Синхронизация времени

2.1.3. Требования к портам

Служба samba, предоставляющая функции AD DC, требует, чтобы на контроллере домена были открыты следующие порты:

Таблица 2.1. Порты используемые Samba AD DC

Служба	Порт	Протокол	Примечание
DNS	53	TCP и UDP	Может быть предоставлен внутренним DNS-сервером Samba или DNS-сервером Bind9
Kerberos	88	TCP и UDP	
NTP	123	UDP (Опционально)	Если на контроллере домена настроен и работает NTP
End Point Mapper (DCE/RPC Locator Service)	135	TCP	
NetBIOS Name Service	137	UDP	
NetBIOS Datagram	138	UDP	
NetBIOS Session	139	TCP	
LDAP	389	TCP и UDP	
SMB over TCP	445	TCP	
Kerberos	464	TCP и UDP	Используется **kadmin** для установки и смены пароля
LDAPS	636	TCP	Если в файле **smb.conf** установлено **tls enabled = yes** (по умолчанию)
Global Catalog	3268	TCP	
Global Catalog SSL	3269	TCP	Если в файле **smb.conf** установлено **tls enabled = yes** (по умолчанию)
Dynamic RPC Ports	49152-65535	TCP	

Служба	Порт	Протокол	Примечание
			Диапазон соответствует диапазону портов, используемому в Windows Server 2008 и более поздних версиях. Чтобы вручную установить диапазон портов в Samba 4.7 и более поздних версиях, необходимо указать параметр **`rpc server port`** в файле **`smb.conf`**. Подробности смотрите в описании параметра на справочной странице **`man smb.conf`**.

2.2. Создание домена

Samba поддерживает следующие серверные части DNS:

- **`SAMBA_INTERNAL`** — встроенный сервер имен:
  - используется по умолчанию при подготовке нового домена, присоединении к существующему домену или переносе домена NT4 в AD;
  - прост в настройке и не требует дополнительного ПО или знаний о DNS;
  - следует использовать для простых настроек DNS;
- **`BIND9_DLZ`** — использует samba4 AD для хранения информации о зоне:
  - требуется BIND 9.8 или более поздняя версия, установленная и настроенная локально на контроллере домена (DC) Samba Active Directory (AD);
  - необходимы знания о DNS-сервере BIND и о том, как настроить службу;
  - следует использовать для сложных сценариев DNS, которые нельзя настроить во внутреннем DNS.

Примечание

Внутренний DNS-сервер Samba не управляет кешем, поэтому он будет отправлять запрос серверу пересылки для каждого DNS-запроса, который не соответствует его домену. Бэкенд Bind-DLZ использует кэш Bind для рекурсивных запросов. Запросы на сам домен каждый раз передаются модулю DLZ, кэша на этом уровне у него нет.

Важно

Бэкенд **DNS BIND9_FLATFILE** не поддерживается.

2.2.1. Параметры команды разворачивания домена

Команда **samba-tool domain provision** имеет множество опций, которые можно использовать для предоставления дополнительной информации при интерактивной установке сервера. Их также можно использовать в скриптах.

Ниже описаны некоторые опции. Для получения более подробной информации следует обратиться к man странице **samba-tool(8)**.

Таблица 2.2. Основные опции для samba-tool domain provision

Опция	Описание
-d DEBUGLEVEL, --debuglevel=DEBUGLEVEL	Включить отладку
--interactive	Запрашивать ввод данных у пользователя (интерактивное создание домена)
--domain=DOMAIN	Имя домена NetBIOS (имя рабочей группы)
--domain-guid=GUID	Установить domainguid (иначе используется случайное значение)
--domain-sid=SID	Установить domainsid (иначе используется случайное значение)
--ntds-guid=GUID	Установить GUID объекта NTDS (иначе используется случайное значение)
--host-name=HOSTNAME	Установить имя хоста
--host-ip=IPADDRESS	Установить IPv4 IP-адрес
--host-ip6=IP6ADDRESS	Установить IPv6 IP-адрес
--adminpass=PASSWORD	Пароль основного администратора домена (иначе используется случайное значение)
--krbtgtpass=PASSWORD	Пароль krbtgtpass (иначе используется случайное значение)
--dns-backend=NAMESERVER-BACKEND	Бэкенд DNS-сервера: SAMBA_INTERNAL — встроенный сервер имен (по умолчанию), BIND9_FLATFILE — использует текстовую базу данных bind9 для хранения информации о зоне, BIND9_DLZ — использует samba4 AD для хранения информации о зоне, NONE — полностью пропускает настройку DNS (не рекомендуется).
--dnspass=PASSWORD	Пароль dns (иначе используется случайное значение)
--server-role=ROLE	Позволяет указать тип серверной роли: domain controller, dc (по умолчанию), member server, member или standalone
--function-level=FOR-FUN-LEVEL	

Опция	Описание
	Позволяет указать уровень домена и леса: 2000, 2003, 2008, 2008_R2 (по умолчанию) или 2016
--base-schema=BASE-SCHEMA	Версия базовой схемы домена. По умолчанию 2019
--use-rfc2307	Позволяет поддерживать расширенные атрибуты типа UID и GID в схеме LDAP и ACL на файловой системе Linux
--machinepass=PASSWORD	Пароль для машины (иначе используется случайное значение)
--plaintext-secrets	Сохранять конфиденциальные данные в виде обычного текста на диске (по умолчанию конфиденциальные данные шифруются)
--realm=REALM	Задаёт область Kerberos (LDAP), и DNS имя домена
--option=OPTION	Позволяет установить параметры **`smb.conf`** из командной строки
-s FILE, --configfile=FILE	Файл конфигурации

2.2.2. Установка пакетов

Samba поддерживает серверные части Heimdal и MIT Kerberos.

Установить пакет *task-samba-dc* для Samba DC на базе Heimdal Kerberos:

```
# apt-get install task-samba-dc
```

или *task-samba-dc-mitkrb5* для Samba DC на базе MIT Kerberos:

```
# apt-get install task-samba-dc-mitkrb5
```

Примечание

Samba на базе Heimdal Kerberos использует KDC несовместимый с MIT Kerberos, поэтому на контроллере домена на базе Heimdal Kerberos из пакета *samba-dc*, для совместимости с клиентской библиотекой libkrb5, в **`krb5.conf`** (в блоке — libdefaults) необходимо отключить использование ядерного кеша ключей — ***`KEYRING:persistent:%{uid}`***:

```
# control krb5-conf-ccache default
```

Так как Samba в режиме контроллера домена (Domain Controller, DC) использует как свой LDAP, так и свой сервер Kerberos, несовместимый с MIT Kerberos, перед установкой необходимо остановить конфликтующие службы **`krb5kdc`** и **`slapd`**, а также **`bind`**:

```
# for service in smb nmb krb5kdc slapd bind; do systemctl disable $service;
systemctl stop $service; done
```

2.2.3. Внутренний DNS-сервер Samba (SAMBA_INTERNAL)

Контроллер домена (DC) Samba Active Directory (AD) предоставляет внутренний DNS-сервер, который поддерживает основные функции, необходимые для AD. Он прост в настройке и не требует дополнительного программного обеспечения или знаний о DNS. Создание домена с внутренним DNS-сервером рекомендуется для простых настроек DNS.

Внутренний DNS Samba имеет следующие недостатки:

- нельзя использовать как кэширующий сервер;
- не поддерживает рекурсивные запросы;
- не поддерживает подпись транзакции с общим ключом (TSIG) (shared-key transaction signature);
- нет зоны-заглушки (stub zones);
- не поддерживает zone transfers;
- не поддерживает балансировку нагрузки циклического перебора между контроллерами домена (Round Robin load balancing among DC's).

Внутренний DNS-сервер может разрешать только DNS-зоны Active Directory (AD). Чтобы включить рекурсивные запросы других зон, следует в параметре ***dns forwarder*** в файле **smb.conf** указать один или несколько IP-адресов DNS-серверов, поддерживающих рекурсивное разрешение. Например:

```
dns forwarder = 192.168.0.190
```

Примечание

Samba 4.5 и более поздние версии в параметре ***dns forwarder*** поддерживают несколько IP-адресов, разделенных пробелами. Старые версии поддерживают один IP-адрес. Обращение ко второму и последующим DNS-серверам произойдёт только в том случае, если первый не вернул никакого ответа.

Примечание

Внешний DNS-сервер можно указать при создании домена.

При создании домена с внутренним DNS-сервером нужно использовать параметр ***--dns-backend=SAMBA_INTERNAL*** или не указывать этот параметр вообще.

2.2.3.1. Выбор имени домена

Должно быть установлено правильное имя узла и домена для сервера. Для этого в файл **/etc/sysconfig/network** необходимо добавить строку:

```
HOSTNAME=dc1.test.alt
```

И выполнить команды:

```
# hostnamectl set-hostname dc1.test.alt
# domainname test.alt
```

Примечание

После изменения имени компьютера могут перестать запускаться приложения. Для решения этой проблемы необходимо перезагрузить систему.

2.2.3.2. Настройка файла /etc/resolvconf.conf

Для корректного распознавания всех локальных DNS-запросов в файле **/etc/resolvconf.conf** должна присутствовать строка:

```
name_servers=127.0.0.1
```

Если этой строки в файле **/etc/resolvconf.conf** нет, то в конец этого файла следует добавить строку:

```
name_servers=127.0.0.1
```

и перезапустить сервис resolvconf:

```
# resolvconf -u
```

2.2.3.3. Восстановление к начальному состоянию Samba

Необходимо очистить базы и конфигурацию Samba (домен, если он создавался до этого, будет удалён):

```
# rm -f /etc/samba/smb.conf
# rm -rf /var/lib/samba
# rm -rf /var/cache/samba
# mkdir -p /var/lib/samba/sysvol
```

Предупреждение

Перед созданием домена необходимо обязательно удалить **/etc/samba/smb.conf**: **rm -f /etc/samba/smb.conf**

2.2.3.4. Интерактивное создание домена

Для запуска интерактивной установки необходимо выполнить команду:

```
# samba-tool domain provision
```

В ответе на первые два вопроса нужно указать доменное имя и имя рабочей группы:

```
Realm [TEST.ALT]:
Domain [TEST]:
```

Примечание

Чтобы принять значение по умолчанию, необходимо нажать **Enter**.

Далее нужно указать тип серверной роли и бэкенд DNS-сервера:

```
Server Role (dc, member, standalone) [dc]:
DNS backend (SAMBA_INTERNAL, BIND9_FLATFILE, BIND9_DLZ, NONE) [SAMBA_INTERNAL]:
```

В *DNS forwarder IP address* нужно указать внешний DNS-сервер, чтобы DC мог разрешать внешние доменные имена:

```
DNS forwarder IP address (write 'none' to disable forwarding) [127.0.0.1]:
8.8.8.8
```

Задать пароль для администратора:

```
Administrator password:
Retype password:
```

Примечание

Пароль администратора должен быть не менее 7 символов и содержать символы как минимум трёх групп из четырёх возможных: латинских букв в верхнем и нижнем регистрах, чисел и других небуквенно-цифровых символов. Пароль не полностью соответствующий требованиям это одна из причин завершения развертывания домена ошибкой.

Начнется процесс конфигурации:

```
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=test,DC=alt
Adding configuration container
Setting up sam.ldb schema
Setting up sam.ldb configuration data
Setting up display specifiers
Modifying display specifiers and extended rights
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=test,DC=alt
Creating DomainDnsZones and ForestDnsZones partitions
Populating DomainDnsZones and ForestDnsZones partitions
Setting up sam.ldb rootDSE marking as synchronized
Fixing provision GUIDs
The Kerberos KDC configuration for Samba AD is located at /var/lib/samba/private/
kdc.conf
A Kerberos configuration suitable for Samba AD has been generated at /var/lib/
samba/private/krb5.conf
Merge the contents of this file with your system krb5.conf or replace it with
this one. Do not create a symlink!
Once the above files are installed, your Samba AD server will be ready to use
Server Role:           active directory domain controller
Hostname:              dc1
NetBIOS Domain:        TEST
DNS Domain:            test.alt
DOMAIN SID:            S-1-5-21-3617232745-2316959539-2936900449
```

2.2.3.5. В пакетном режиме

Пример команды создания контроллера домена test.alt в пакетном режиме:

```
# samba-tool domain provision --realm=test.alt --domain=test --adminpass='Pa$
$word' --dns-backend=SAMBA_INTERNAL --option="dns forwarder=8.8.8.8" --server-
role=dc --use-rfc2307
```

Для пакетной установки необходимо указать следующие параметры:

- **`--realm REALM_NAME`** — имя области Kerberos (LDAP), и DNS имя домена;
- **`--domain=DOMAIN`** — имя домена (имя рабочей группы);
- **`--adminpass=PASSWORD`** — пароль основного администратора домена;
- **`dns forwarder`** — внешний DNS-сервер, чтобы DC мог разрешать внешние доменные имена;
- **`--server-role=ROLE`** — тип серверной роли;
- **`--dns-backend=NAMESERVER-BACKEND`** — бэкенд DNS-сервера;
- **`--use-rfc2307`** — позволяет поддерживать расширенные атрибуты типа UID и GID в схеме LDAP и ACL на файловой системе Linux.

Примечание

Пароль администратора должен быть не менее 7 символов и содержать символы как минимум трёх групп из четырёх возможных: латинских букв в верхнем и нижнем регистрах, чисел и других небуквенно-цифровых символов. Пароль не полностью соответствующий требованиям это одна из причин завершения развертывания домена ошибкой.

Если уровень не указан, то домен разворачивается на уровне 2008_R2. Для разворачивания домена на другом уровне, уровень необходимо явно указать, например:

```
# samba-tool domain provision --realm=test.alt --domain=test --adminpass='Pa$
$word' --dns-backend=SAMBA_INTERNAL --option="dns forwarder=8.8.8.8" --option="ad
dc functional level = 2016" --server-role=dc --function-level=2016
```

Примечание

Если необходим уровень 2012_R2, то следует сначала развернуть домен на уровне 2008_R2, а затем повысить его до 2012_R2 (см. Повышение уровня схемы, функционального уровня домена).

Примечание

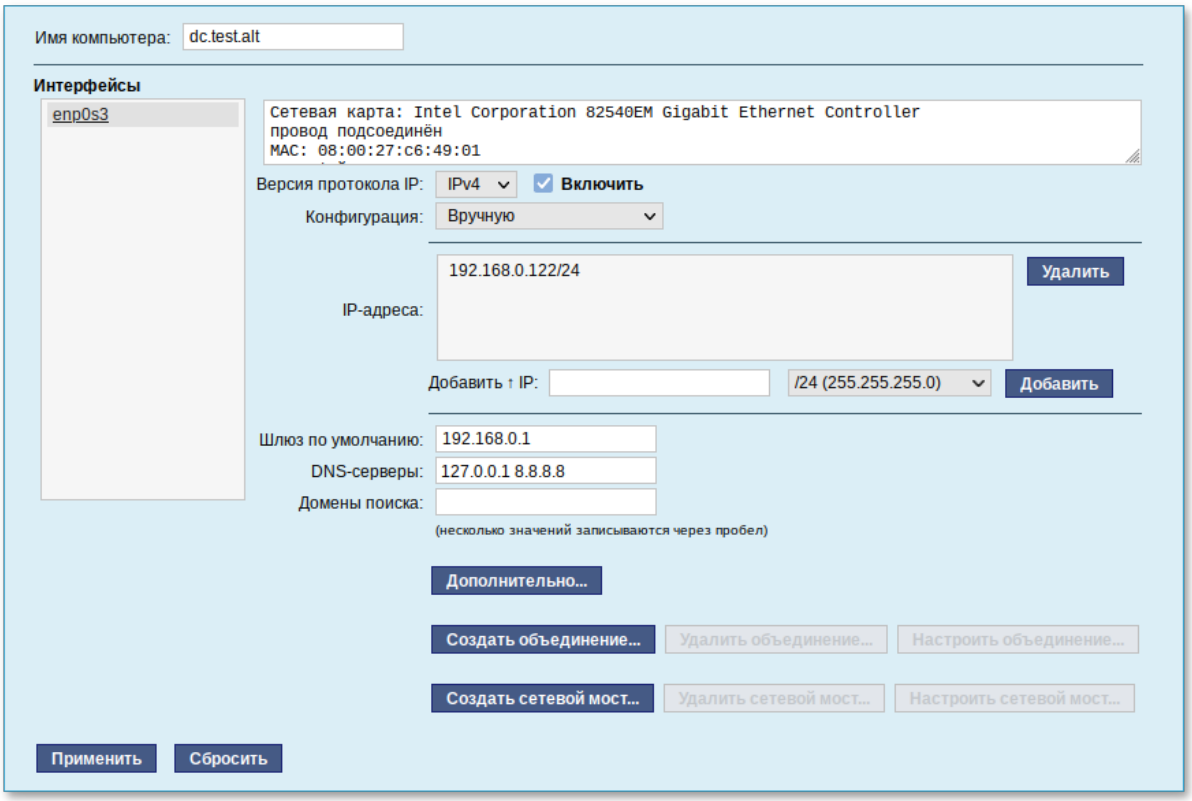
Полный список параметров можно увидеть, запустив команду:

```
# samba-tool domain provision --help
```

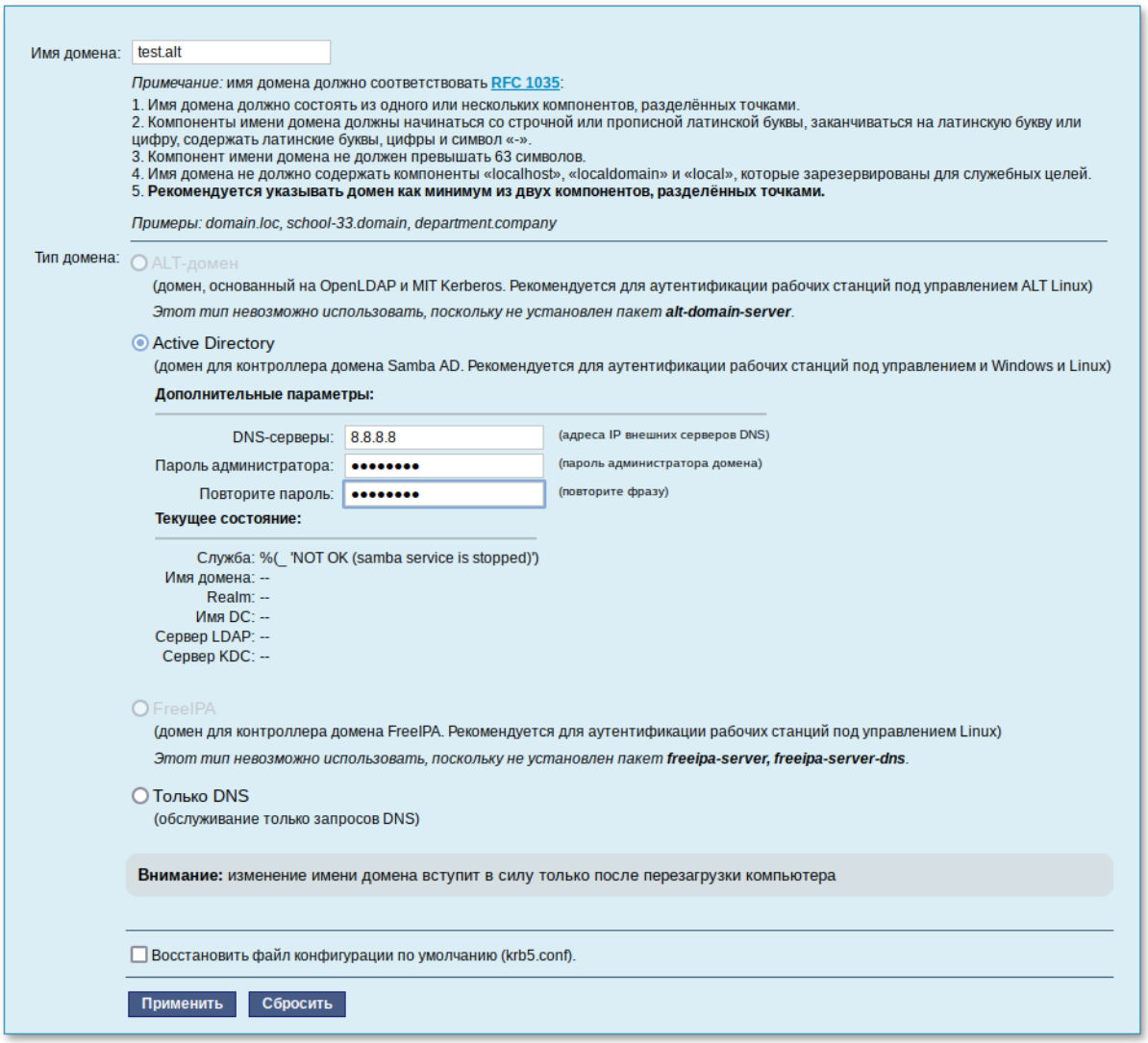
2.2.3.6. Создание домена в ЦУС

При инициализации домена в веб-интерфейсе ЦУС следует выполнить следующие действия:

1. В модуле **Ethernet-интерфейсы** указать имя компьютера и DNS 127.0.0.1:



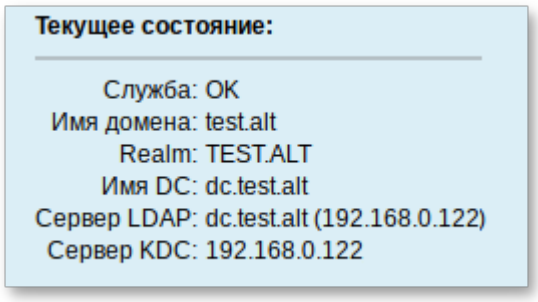
2. В модуле **Домен** указать имя домена, отметить пункт **`Active Directory`**, указать IP-адреса внешних DNS-серверов, задать пароль администратора домена и нажать кнопку **`Применить`**:



Примечание

Пароль администратора должен быть не менее 7 символов и содержать символы как минимум трёх групп из четырёх возможных: латинских букв в верхнем и нижнем регистрах, чисел и других небуквенно-цифровых символов. Пароль не полностью соответствующий требованиям это одна из причин завершения развертывания домена ошибкой.

3. После успешного создания домена, будет выведена информация о домене:



4. Перегрузить сервер.

2.2.3.7. Запуск службы

Установить службу по умолчанию и запустить её:

```
# systemctl enable --now samba
```

Примечание

Если служба после установки никаким способом не запускается, необходимо перезагрузить сервер.

Примечание

Пример файла **/etc/samba/smb.conf** после создания домена с SAMBA_INTERNAL:

```
 Global parameters
[global]
        dns forwarder = 8.8.8.8
        netbios name = DC1
        realm = TEST.ALT
        server role = active directory domain controller
        workgroup = TEST
        idmap_ldb:use rfc2307 = yes

[sysvol]
        path = /var/lib/samba/sysvol
        read only = No

[netlogon]
        path = /var/lib/samba/sysvol/test.alt/scripts
        read only = No
```

2.2.4. Домен с BIND9_DLZ

Работа с внешним сервером DNS осуществляется с помощью бэкенда BIND9_DLZ и используется в следующих случаях:

- сложная схема зон DNS;
- поддержка больше одного сервера форвардинга (параметр ***dns forwarder*** на бэкенде INTERNAL работает только с одним адресом).

Если планируется настроить контроллер домена (DC) Samba Active Directory (AD) с использованием серверной части BIND9_DLZ, необходимо сначала установить и настроить DNS-сервер BIND.

На сервере должны быть установлены пакеты *bind* и *bind-utils*:

```
# apt-get install bind bind-utils
```

Примечание

Во избежании появлении ошибки при запуске bind:

```
мая 03 14:25:13 dc1 named[3825]: samba_dlz: Failed to configure zone
'test.alt'
мая 03 14:25:13 dc1 named[3825]: loading configuration: already exists
мая 03 14:25:13 dc1 named[3825]: exiting (due to fatal error)
мая 03 14:39:44 dc1 named[4309]: Loading 'AD DNS Zone' using driver dlopen
```

не следует, при установке системы, задавать полное имя для DC (dc1.test.alt).

Примечание

Пакет *bind* содержит различные утилиты, связанные с DNS, например:

- **named-checkconf** — проверка синтаксиса файлов конфигурации;
- **named-checkzone** — проверка файлов зон DNS;
- **rndc** — инструмент управления службой DNS.

Пакет *bind-utils* содержит различные утилиты, связанные с DNS, например:

- **dig** — многофункциональный инструмент для опроса DNS-серверов;
- **host** — преобразовать имя хоста в IP-адрес;
- **nslookup** — получить информацию DNS об удаленном сервере;
- **nsupdate** — инструмент для динамического обновления записей DNS.

Основные файлы настройки DNS:

- **/etc/named.conf** — основной файл конфигурации, содержит в себе ссылки на остальные конфигурационные файлы;
- **/etc/bind/options.conf** — файл для глобальных настроек службы;
- **/etc/bind/rndc.conf** — получить информацию DNS об удаленном сервере;
- **/etc/bind/local.conf** — файл для настроек зоны DNS;
- **/var/lib/samba/bind-dns/named.conf** — инструмент для динамического обновления записей DNS.

Ниже описаны некоторые параметры конфигурационного файла **/etc/bind/options.conf**. Для получения более подробной информации следует обратиться к man странице **named.conf(5)**.

Таблица 2.3. Основные параметры конфигурационного файла /etc/bind/options.conf

Опция	Описание
directory	Указывает каталог расположения таблиц зон
listen-on	Позволяет указать сетевые интерфейсы, которые будет прослушивать служба

Опция	Описание
allow-query	IP-адреса и подсети от которых будут обрабатываться запросы
allow-transfer	Устанавливает возможность передачи зон для slave-серверов
allow-query-cache	
allow-recursion	IP-адреса и подсети от которых будут обрабатываться рекурсивные запросы
tkey-gssapi-keytab	
minimal-responses	
max-cache-ttl	
forward	Позволяет указать каким образом сервер обрабатывает запрос клиента. При значении *first* DNS-сервер будет пытаться разрешать имена с помощью DNS-серверов, указанных в параметре forwarders. Если разрешить имя с помощью данных серверов не удалось, то попытаться разрешить имя самостоятельно. Если указать значение *none*, сервер не будет пытаться разрешить имя самостоятельно
forwarders	DNS-сервер, на который будут перенаправляться запросы клиентов
type	Тип зоны

Настройка BIND9 для работы с Samba AD:

1. Отключить chroot:

```
# control bind-chroot disabled
```

2. Отключить KRB5RCACHETYPE:

```
#
grep -q KRB5RCACHETYPE /etc/sysconfig/bind || echo 'KRB5RCACHETYPE="none"'
>> /etc/sysconfig/bind
```

3. Подключить плагин BIND_DLZ:

```
# grep -q 'bind-dns' /etc/bind/named.conf || echo 'include "/var/lib/samba/
bind-dns/named.conf";' >> /etc/bind/named.conf
```

4. Отредактировать файл **/etc/bind/options.conf**:

   - в раздел *options* добавить строки:

   ```
   tkey-gssapi-keytab "/var/lib/samba/bind-dns/dns.keytab";
   minimal-responses yes;
   ```

   - в параметре **forwarders** указать сервера, куда будут перенаправляться запросы, на которые нет информации в локальной зоне (если этой информации нет в файле **/etc/bind/resolvconf-options.conf**):

```
forward first;
forwarders { 8.8.8.8; };
```

- в параметр **`listen-on`** добавить IP-адрес DNS-сервера, на котором он будет принимать запросы;
- раскомментировать параметр **`allow-query`** и указать в нём подсети из которых разрешено подавать запросы;
- раскомментировать параметр **`allow-recursion`** и указать в нём подсети из которых будут обрабатываться рекурсивные запросы;
- в раздел *logging* добавить строку:

```
category lame-servers {null;};
```

Пример файла **`/etc/bind/options.conf`**:

```
options {
        version "unknown";
        directory "/etc/bind/zone";
        dump-file "/var/run/named_dump.db";
        statistics-file "/var/run/named.stats";
        recursing-file "/var/run/recursing";


        // disables the use of a PID file
        pid-file none;
        tkey-gssapi-keytab "/var/lib/samba/bind-dns/dns.keytab";
        minimal-responses yes;

        listen-on { 127.0.0.1; 192.168.0.152; };
        listen-on-v6 { ::1; };

        include "/etc/bind/resolvconf-options.conf";

        allow-query { localnets; 192.168.0.0/24; };
        allow-recursion { localnets; 192.168.0.0/24; };

        //max-cache-ttl 86400;

};

logging {
        category lame-servers {null;};
};
```

5. В файле **`/etc/bind/resolvconf-options.conf`** в параметре **`forwarders`** должен быть указан DNS-сервер, на который будут перенаправляться запросы клиентов;
6. Выполнить остановку **`bind`**:

```
# systemctl stop bind
```

Если в роли DNS-сервера Samba используется Bind, то при создании домена нужно использовать параметр ***`--dns-backend=BIND9_DLZ`***.

2.2.4.1. Восстановление к начальному состоянию Samba

Необходимо очистить базы и конфигурацию Samba (домен, если он создавался до этого, будет удалён):

```
# rm -f /etc/samba/smb.conf
# rm -rf /var/lib/samba
# rm -rf /var/cache/samba
# mkdir -p /var/lib/samba/sysvol
```

Предупреждение

Перед созданием домена необходимо обязательно удалить **/etc/samba/smb.conf**: **rm -f /etc/samba/smb.conf**

2.2.4.2. Интерактивное создание домена

Для запуска интерактивной установки необходимо выполнить команду:

```
# samba-tool domain provision
```

В ответе на первые два вопроса нужно указать доменное имя и имя рабочей группы:

```
Realm [TEST.ALT]:
Domain [TEST]:
```

Примечание

Чтобы принять значение по умолчанию, необходимо нажать **Enter**.

Далее нужно указать тип серверной роли и бэкенд DNS-сервера:

```
Server Role (dc, member, standalone) [dc]:
DNS backend (SAMBA_INTERNAL, BIND9_FLATFILE, BIND9_DLZ, NONE) [SAMBA_INTERNAL]:
BIND9_DLZ
```

Задать пароль для администратора:

```
Administrator password:
Retype password:
```

Примечание

Пароль администратора должен быть не менее 7 символов и содержать символы как минимум трёх групп из четырёх возможных: латинских букв в верхнем и нижнем регистрах, чисел и других небуквенно-цифровых символов. Пароль не полностью соответствующий требованиям это одна из причин завершения развертывания домена ошибкой.

Начнется процесс конфигурации:

```
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=test,DC=alt
Adding configuration container
Setting up sam.ldb schema
Setting up sam.ldb configuration data
Setting up display specifiers
Modifying display specifiers and extended rights
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=test,DC=alt
Creating DomainDnsZones and ForestDnsZones partitions
Populating DomainDnsZones and ForestDnsZones partitions
See /var/lib/samba/bind-dns/named.conf for an example configuration include file
for BIND
and /var/lib/samba/bind-dns/named.txt for further documentation required for
secure DNS updates
Setting up sam.ldb rootDSE marking as synchronized
Fixing provision GUIDs
The Kerberos KDC configuration for Samba AD is located at /var/lib/samba/private/
kdc.conf
A Kerberos configuration suitable for Samba AD has been generated at /var/lib/
samba/private/krb5.conf
Merge the contents of this file with your system krb5.conf or replace it with
this one. Do not create a symlink!
Once the above files are installed, your Samba AD server will be ready to use
Server Role:           active directory domain controller
Hostname:              dc1
NetBIOS Domain:        TEST
DNS Domain:            test.alt
DOMAIN SID:            S-1-5-21-3684382553-2825304832-3399765044
```

2.2.4.3. В пакетном режиме

Пример команды создания контроллера домена test.alt в пакетном режиме:

```
# samba-tool domain provision --realm=test.alt --domain test --adminpass='Pa$
$word' --dns-backend=BIND9_DLZ --server-role=dc
```

Для пакетной установки необходимо указать следующие параметры:

- **`--realm REALM_NAME`** — имя области Kerberos (LDAP), и DNS имя домена;
- **`--domain=DOMAIN`** — имя домена (имя рабочей группы);
- **`--adminpass=PASSWORD`** — пароль основного администратора домена;
- **`--server-role=ROLE`** — тип серверной роли;
- **`--dns-backend=NAMESERVER-BACKEND`** — бэкенд DNS-сервера;
- **`--use-rfc2307`** — позволяет поддерживать расширенные атрибуты типа UID и GID в схеме LDAP и ACL на файловой системе Linux.

Примечание

Пароль администратора должен быть не менее 7 символов и содержать символы как минимум трёх групп из четырёх возможных: латинских букв в верхнем и нижнем регистрах, чисел и других небуквенно-цифровых символов. Пароль не полностью соответствующий требованиям это одна из причин завершения развертывания домена ошибкой.

Если уровень не указан, то домен разворачивается на уровне 2008_R2. Для разворачивания домена на другом уровне, уровень необходимо явно указать, например:

```
# samba-tool domain provision --realm=test.alt --domain=test --adminpass='Pa$
$word' --dns-backend=BIND9_DLZ --option="ad dc functional level = 2016" --server-
role=dc --function-level=2016
```

Примечание

Если необходим уровень 2012_R2, то следует сначала развернуть домен на уровне 2008_R2, а затем повысить его до 2012_R2 (см. Повышение уровня схемы, функционального уровня домена).

Примечание

Полный список параметров можно увидеть, запустив команду:

```
# samba-tool domain provision --help
```

2.2.4.4. Запуск службы

Установить службы **`samba`** и **`bind`** по умолчанию и запустить их:

```
# systemctl enable --now samba
# systemctl enable --now bind
```

Примечание

Если служба **samba** после установки никаким способом не запускается, необходимо перезагрузить сервер.

Примечание

Пример файла **/etc/samba/smb.conf** после создания домена с BIND9_DLZ:

```
# Global parameters
[global]
        netbios name = DC1
        realm = TEST.ALT
        server role = active directory domain controller
        server services = s3fs, rpc, nbt, wrepl, ldap, cldap, kdc, drepl,
winbindd, ntp_signd, kcc, dnsupdate
        workgroup = TEST

[sysvol]
        path = /var/lib/samba/sysvol
        read only = No

[netlogon]
        path = /var/lib/samba/sysvol/test.alt/scripts
        read only = No
```

2.2.4.5. Проверка зон

Следующие примеры запрашивают службу DNS о локальном хосте (127.0.0.1).

Проверка зоны перенаправления localhost:

```
# host -t A localhost 127.0.0.1
Using domain server:
Name: 127.0.0.1
Address: 127.0.0.1#53
Aliases:
localhost has address 127.0.0.1
```

Проверка реверсивной зоны 0.0.127.in-addr.arpa.:

```
# host -t PTR 127.0.0.1 127.0.0.1
Using domain server:
Name: 127.0.0.1
Address: 127.0.0.1#53
Aliases:
1.0.0.127.in-addr.arpa domain name pointer localhost.
```

2.3. Настройка Kerberos

Внести изменения в файл **/etc/krb5.conf**. Следует раскомментировать строку *default_realm* и содержимое разделов *realms* и *domain_realm* и указать название домена (обратите внимание на регистр символов), в строке *dns_lookup_realm* должно быть установлено значение false:

```
includedir /etc/krb5.conf.d/

[logging]
# default = FILE:/var/log/krb5libs.log
# kdc = FILE:/var/log/krb5kdc.log
# admin_server = FILE:/var/log/kadmind.log

[libdefaults]
dns_lookup_kdc = true
dns_lookup_realm = false
ticket_lifetime = 24h
renew_lifetime = 7d
forwardable = true
rdns = false
default_realm = TEST.ALT
# default_ccache_name = KEYRING:persistent:%{uid}

[realms]
TEST.ALT = {
default_domain = test.alt
}

[domain_realm]
dc = TEST.ALT
```

Примечание

В момент создания домена Samba конфигурирует шаблон файла **krb5.conf** для домена в каталоге **/var/lib/samba/private/**. Можно просто заменить этим файлом файл, находящийся в каталоге **/etc/**:

```
# cp /var/lib/samba/private/krb5.conf /etc/krb5.conf
```

2.4. Проверка работоспособности домена

Просмотр общей информации о домене:

```
# samba-tool domain info 127.0.0.1
Forest           : test.alt
Domain           : test.alt
Netbios domain   : TEST
DC name          : dc1.test.alt
DC netbios name  : DC1
Server site      : Default-First-Site-Name
Client site      : Default-First-Site-Name
```

Просмотр предоставляемых служб:

```
# smbclient -L localhost -Uadministrator
Password for [TEST\administrator]:

    Sharename       Type      Comment
    ---------       ----      -------
    sysvol          Disk
    netlogon        Disk
    IPC$            IPC       IPC Service (Samba 4.19.4)
SMB1 disabled -- no workgroup available
```

Создаваемые по умолчанию общие ресурсы netlogon и sysvol нужны для функционирования сервера AD и создаются в **`smb.conf`** в процессе развертывания/модернизации.

Проверка конфигурации DNS:

- Проверка наличия nameserver 127.0.0.1 в **`/etc/resolv.conf`**:

```
# cat /etc/resolv.conf
# Generated by resolvconf
# Do not edit manually, use
# /etc/net/ifaces/<interface>/resolv.conf instead.
search test.alt
nameserver 127.0.0.1

# host test.alt
test.alt has address 192.168.0.122
```

- Проверка имён хостов:
  - адрес **_kerberos._udp.***адрес домена с точкой:

```
# host -t SRV _kerberos._udp.test.alt.
_kerberos._udp.test.alt has SRV record 0 100 88 dc1.test.alt.
```

  - адрес **_ldap._tcp.***адрес домена с точкой:

```
# host -t SRV _ldap._tcp.test.alt.
_ldap._tcp.test.alt has SRV record 0 100 389 dc1.test.alt.
```

  - адрес **адрес хоста.***адрес домена с точкой:

```
# host -t A dc1.test.alt.
dc1.test.alt has address 192.168.0.122
```

  Если имена не находятся, следует проверить выключение службы **bind** (если не включен плагин BIND9_DLZ).

Проверка Kerberos (имя домена должно быть в **верхнем регистре**):

```
# kinit administrator@TEST.ALT
Password for administrator@TEST.ALT:
Warning: Your password will expire in 15 days on Пт 12 апр 2024 11:46:29
```

Просмотр полученного билета:

```
# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: administrator@TEST.ALT

Valid starting       Expires              Service principal
27.03.2024 14:14:36  28.03.2024 00:14:36  krbtgt/TEST.ALT@TEST.ALT
        renew until 28.03.2024 14:14:32
```

2.5. Редактирование существующего домена

2.5.1. Повышение уровня схемы, функционального уровня домена

Просмотреть текущий уровень домена и леса можно, выполнив команду:

```
# samba-tool domain level show
Domain and forest function level for domain 'DC=test,DC=alt'

Forest function level: (Windows) 2008 R2
Domain function level: (Windows) 2008 R2
Lowest function level of a DC: (Windows) 2008 R2
```

Для повышения уровня домена необходимо выполнить следующие действия:

1. Указать функциональный уровень AD, который будет поддерживаться контроллером домена в параметре ***ad dc functional level*** файла **/etc/samba/smb.conf**. Возможные значения:

   - 2008_R2 — аналог функционального уровня Windows 2008 R2 (по умолчанию);
   - 2012 — аналог функционального уровня Windows 2012;
   - 2012_R2 — аналог функционального уровня Windows 2012 R2;
   - 2016 — аналог функционального уровня Windows 2016.

2. Обновить схему домена, выполнив команду:

   ```
   # samba-tool domain schemaupgrade --schema=<SCHEMA>
   ```

   где SCHEMA — схема, до которой необходимо выполнить обновление (по умолчанию 2019).

3. Подготовить функциональный уровень домена, выполнив команду:

   ```
   # samba-tool domain functionalprep --function-level=<FUNCTION_LEVEL>
   ```

   где FUNCTION_LEVEL — функциональный уровень, к которому нужно подготовиться (по умолчанию 2016).

4. Указать функциональные уровни домена и леса, выполнив команду:

   ```
   # samba-tool domain level raise --domain-level=<DOMAIN_LEVEL> --forest-level=<FOREST_LEVEL>
   ```

где:

- FOREST_LEVEL — уровень работы леса. Возможные значения: 2003, 2008, 2008_R2, 2012, 2012_R2, 2016.
- DOMAIN_LEVEL — уровень работы домена. Возможные значения: 2003, 2008, 2008_R2, 2012, 2012_R2, 2016.

Примечание

При установке значения параметра ***ad dc functional level*** в файле **/etc/samba/smb.conf** вручную, защита от несовпадения функций между контроллерами домена снижается. Поэтому на всех контроллерах домена должна использоваться одна и та же версия Samba, чтобы гарантировать, что поведение, наблюдаемое клиентом, будет одинаковым независимо от того, к какому контроллеру домена осуществляется соединение.

Пример повышения уровня домена до 2016:

- в раздел [global] файла **/etc/samba/smb.conf** добавить строку:

```
ad dc functional level = 2016
```

- перезагрузить службу samba:

```
# systemctl restart samba.service
```

- обновить схему домена:

```
# samba-tool domain schemaupgrade --schema=2019
```

- подготовить функциональный уровень домена:

```
# samba-tool domain functionalprep --function-level=2016
```

- повысить функциональные уровни домена и леса до 2016:

```
# samba-tool domain level raise --domain-level=2016 --forest-level=2016
Domain function level changed!
Forest function level changed!
All changes applied successfully!
```

- убедиться, что уровни домена и леса повышены:

```
# samba-tool domain level show
Domain and forest function level for domain 'DC=test,DC=alt'

Forest function level: (Windows) 2016
Domain function level: (Windows) 2016
Lowest function level of a DC: (Windows) 2016
```

2.5.2. Включение RFC2307 после разворачивания домена

Примечание

До запуска этой процедуры следует убедиться, что она необходима.

Проверка того, что расширения NIS установлены в AD:

```
# ldbsearch -H /var/lib/samba/private/sam.ldb -s base -b
CN=ypservers,CN=ypServ30,CN=RpcServices,CN=System,DC=test,DC=alt cn

# record 1
dn: CN=ypservers,CN=ypServ30,CN=RpcServices,CN=System,DC=test,DC=alt
cn: ypservers

# returned 1 records
# 1 entries
# 0 referrals
```

Если команда **ldbsearch** возвращает одну запись (returned 1 records), расширения NIS установлены и больше ничего делать не нужно.

Предупреждение

Обновление схемы может привести к поломке AD. Прежде чем обновлять схему, необходимо убедиться в наличии рабочей резервной копии.

Для установки расширения NIS необходимо выполнить следующие действия:

1. Найти контроллер домена (DC) с ролью (FSMO) хозяина схемы:

   ```
   # samba-tool fsmo show | grep SchemaMasterRole
   SchemaMasterRole owner: CN=NTDS Settings,CN=DC1,CN=Servers,CN=Default-First-
   Site-Name,CN=Sites,CN=Configuration,DC=test,DC=alt
   ```

   В выводе команды показано имя DC, которому принадлежит эта роль. Все дальнейшие дествия следует выполнять на этом DC.

2. Остановить службу **samba**:

   ```
   # systemctl stop samba
   ```

3. Создать копию файла схемы **ypServ30.ldif**, например:

   ```
   # cp /usr/share/samba/setup/ypServ30.ldif /tmp/
   ```

4. Заменить переменные в скопированном файле LDIF именем домена (DN), именем NetBIOS и доменом NIS вашей установки, например:

```
#
sed -i -e 's/\${DOMAINDN}/DC=test,DC=alt/g' -e 's/\${NETBIOSNAME}/DC/g' -e
's/\${NISDOMAIN}/test/g' /tmp/ypServ30.ldif
```

5. Импортировать измененный файл LDIF в локальную базу данных Samba AD **/var/lib/samba/private/sam.ldb**:

```
# ldbmodify -H /var/lib/samba/private/sam.ldb /tmp/ypServ30.ldif --
option="dsdb:schema update allowed"=true
```

6. В файл **/etc/samba/smb.conf** в секцию **[global]** добавить параметр::

```
idmap_ldb:use rfc2307 = yes
```

7. Запустить службу **samba**:

```
# systemctl start samba
```

AD реплицирует обновленную схему на все контроллеры домена в лесу.

2.6. Заведение дополнительного DC

Системные требования к дополнительному DC такие же, как и для основного сервера Samba AD DC (см. Системные требования к серверу Samba AD DC).

Примечание

В терминологии контроллеров домена нет понятия PDC/BDC, т.е. все контроллеры равны, но один из них выступает владельцем ролей FSMO (см. Просмотр и передача ролей FSMO).

Присоединение дополнительного Samba DC к существующему AD отличается от инициализации первого DC в лесу AD.

Все действия выполняются на узле dc2.test.alt (192.168.0.123), если не указано иное.

1. Установить пакет *task-samba-dc*, который установит все необходимое:

```
# apt-get install task-samba-dc
```

2. Остановить конфликтующие службы **krb5kdc** и **slapd**, а также **bind**:

```
# for service in smb nmb krb5kdc slapd bind; do systemctl disable $service;
systemctl stop $service; done
```

3. Очистить базы и конфигурацию Samba (домен, если он создавался до этого, будет удалён):

```
# rm -f /etc/samba/smb.conf
# rm -rf /var/lib/samba
# rm -rf /var/cache/samba
# mkdir -p /var/lib/samba/sysvol
```

4. На существующем контроллере домена завести IP-адрес для дополнительного DC:

Предупреждение

Указание аутентифицирующей информации (имени пользователя и пароля) обязательно!

```
# samba-tool dns add 192.168.0.122 test.alt DC2 A 192.168.0.123 -
Uadministrator
Password for [TEST\administrator]:
Record added successfully
```

5. На дополнительном DC установить следующие параметры в файле конфигурации клиента Kerberos **/etc/krb5.conf**):

```
[libdefaults]
default_realm = TEST.ALT
dns_lookup_realm = false
dns_lookup_kdc = true
```

Примечание

На дополнительном DC в **/etc/resolv.conf** обязательно должен быть добавлен первый DC как nameserver:

```
# echo "name_servers=192.168.0.122" >> /etc/resolvconf.conf
# echo "search_domains=test.alt" >> /etc/resolvconf.conf
# resolvconf -u
# cat /etc/resolv.conf
search test.alt
nameserver 192.168.0.122
nameserver 8.8.8.8
```

6. Для проверки настройки запросить билет Kerberos для администратора домена:

```
# kinit administrator@TEST.ALT
Password for administrator@TEST.ALT:
```

Предупреждение

Имя домена должно быть указано в верхнем регистре.

7. Убедиться, что билет получен:

```
# klist
Ticket cache: KEYRING:persistent:0:0
Default principal: administrator@TEST.ALT

Valid starting       Expires              Service principal
27.03.2024 14:14:36  28.03.2024 00:14:36  krbtgt/TEST.ALT@TEST.ALT
        renew until 28.03.2024 14:14:32
```

8. Ввести дополнительный DC в домен test.alt в качестве контроллера домена (DC):

```
# samba-tool domain join test.alt DC -Uadministrator --realm=test.alt --
option="dns forwarder=8.8.8.8"
```

Если всё нормально, в конце будет выведена информация о присоединении к домену:

```
Joined domain TEST (SID S-1-5-21-80639820-2350372464-3293631772) as a DC
```

Примечание

При использовании dns internal, необходимо указать значение ***dns forwarder***, чтобы на новом сервере была настроена пересылка запросов. Форвардером может быть как вышестоящий DNS-сервер организации, так и публичные от google или yandex.

Если первый контроллер домена создавался с ключом **`--rfc2307`**, то и для текущего необходимо это учесть, указав параметр:

```
--option='idmap_ldb:use rfc2307 = yes'
```

9. Сделать службу **samba** запускаемой по умолчанию и запустить её:

```
# systemctl enable --now samba
```

Примечание

Для получения дополнительной информации о параметрах команды **`samba-tool domain join`** можно воспользоваться командой:

```
# samba-tool domain join --help
```

2.7. Контроллер домена на чтение (RODC)

Основная цель контроллера домена, доступного только на чтение (RODC — read-only domain controller), — возможность безопасной установки собственного контролера домена в удаленных филиалах, в которых сложно обеспечить физическую защиту сервера. Контроллер домена RODC содержит копию базы Active Directory, доступную только на чтение. Это означает, что никто, даже при получении физического доступа к такому контроллеру домена, не сможет изменить данные в AD (в том числе сбросить пароль администратора домена).

Основные отличия RODC от обычных контроллеров домена, доступных для записи (RWDC):

- RODC хранит копию базы AD, доступную только для чтения. Клиенты не могут вносить изменения в базу такого контролера домена;
- RODC не реплицирует данные AD на другие контроллеры домена (RWDC) (используется односторонняя репликация);
- контроллер RODC хранит полную копию базы AD, за исключением хэшей паролей объектов AD и других атрибутов, содержащих чувствительную информацию;
- при получении контроллером RODC запроса на аутентификацию от пользователя, он перенаправляет этот запрос на ближайший RWDC контроллер;
- контроллер RODC может кэшировать учетные данные некоторых пользователей (это ускоряет аутентификацию и позволяет пользователям авторизоваться на контроллере домена, даже при отсутствии связи с RWDC);
- DNS служба на RODC работает только на чтение.

Требования, которые должны быть выполнены для разворачивания RODC:

- на сервере должен быть назначен статический IP;
- уровень леса и домена должен соответствовать 2008R2. Это можно проверить, выполнив следующую команду на контролере домена:

```
# samba-tool domain level show
Domain and forest function level for domain 'DC=test,DC=alt'

Forest function level: (Windows) 2008 R2
Domain function level: (Windows) 2008 R2
Lowest function level of a DC: (Windows) 2008 R2
```

- в качестве DNS сервера должен быть указан ближайший RWDC контроллер.

2.7.1. Установка и настройка RODC

Все действия выполняются на узле rodc.test.alt (192.168.0.124), если не указано иное.

1. Установить пакет *task-samba-dc*, который установит все необходимое:

```
# apt-get install task-samba-dc
```

2. Остановить конфликтующие службы **krb5kdc** и **slapd**, а также **bind**:

```
# for service in smb nmb krb5kdc slapd bind; do systemctl disable $service;
systemctl stop $service; done
```

3. Очистить базы и конфигурацию Samba (домен, если он создавался до этого, будет удалён):

```
# rm -f /etc/samba/smb.conf
# rm -rf /var/lib/samba
# rm -rf /var/cache/samba
# mkdir -p /var/lib/samba/sysvol
```

4. На существующем контроллере домена завести IP-адрес для RODC:

Предупреждение

Указание аутентифицирующей информации (имени пользователя и пароля) обязательно!

```
# samba-tool dns add 192.168.0.122 test.alt DC2 A 192.168.0.124 -
Uadministrator
Password for [TEST\administrator]:
Record added successfully
```

5. На RODC установить следующие параметры в файле конфигурации клиента Kerberos **/etc/krb5.conf**):

```
[libdefaults]
default_realm = TEST.ALT
dns_lookup_realm = false
dns_lookup_kdc = true

[realms]
TEST.ALT = {
kdc = rodc.test.alt
kdc = dc1.test.alt
default_domain = TEST.ALT
}
```

Примечание

На RODC в **/etc/resolv.conf** должен быть добавлен первый DC как nameserver:

```
# echo "name_servers=192.168.0.122" >> /etc/resolvconf.conf
# echo "search_domains=test.alt" >> /etc/resolvconf.conf
# resolvconf -u
# cat /etc/resolv.conf
search test.alt
nameserver 192.168.0.122
nameserver 8.8.8.8
```

6. Для проверки настройки запросить билет Kerberos для администратора домена:

```
# kinit administrator@TEST.ALT
Password for administrator@TEST.ALT:
```

Предупреждение

Имя домена должно быть указано в верхнем регистре.

7. Убедиться, что билет получен:

```
# klist
Ticket cache: KEYRING:persistent:0:0
Default principal: administrator@TEST.ALT

Valid starting       Expires              Service principal
27.03.2024 14:14:36  28.03.2024 00:14:36  krbtgt/TEST.ALT@TEST.ALT
        renew until 28.03.2024 14:14:32
```

8. Ввести дополнительный DC в домен test.alt в качестве контроллера домена, доступного только для чтения (RODC):

```
# samba-tool domain join test.alt RODC -Uadministrator@TEST.ALT --
realm=test.alt --option="dns forwarder=8.8.8.8"
```

Если всё нормально, в конце будет выведена информация о присоединении к домену:

```
Joined domain TEST (SID S-1-5-21-578923263-1107570656-1287136478) as an RODC
```

Примечание

При использовании dns internal, необходимо указать значение ***dns forwarder***, чтобы на новом сервере была настроена пересылка запросов. Форвардером может быть как вышестоящий DNS-сервер организации, так и публичные от google или yandex.

Если первый контроллер домена создавался с ключом **--rfc2307**, то и для текущего необходимо это учесть, указав параметр:

```
--option='idmap_ldb:use rfc2307 = yes'
```

9. Сделать службу **samba** запускаемой по умолчанию и запустить её:

```
# systemctl enable --now samba
```

Тестирование репликации пароля пользователя на сервере RODC:

1. На DC1 создать пользователя и добавить его в группу *Allowed RODC Password Replication Group* (пароли пользователей/групп, входящих в группу *Allowed RODC Password Replication Group* разрешено реплицировать на RODC).

2. На RODC проверить возможность загрузки кэша пароля, выполнив команду:

```
# samba-tool rodc preload ivanov --server=dc1.test.alt
Replicating DN CN=Иван Иванов,CN=Users,DC=test,DC=alt
Exop on[CN=Иван Иванов,CN=Users,DC=test,DC=alt] objects[1] linked_values[0]
```

2.7.2. Политики репликации и кэширования паролей на RODC

На RODC можно задать список пользователей, чьи хэши паролей можно или нельзя реплицировать на данный контролер домена.

Примечание

Все пользователи в кэше RODC смогут аутентифицироваться на этом контроллере домена, даже если отсутствует связь с RWDC.

Пример получения билета при отсутствии связи с RWDC (пользователь ivanov есть в кэше RODC, а пользователь kim — нет):

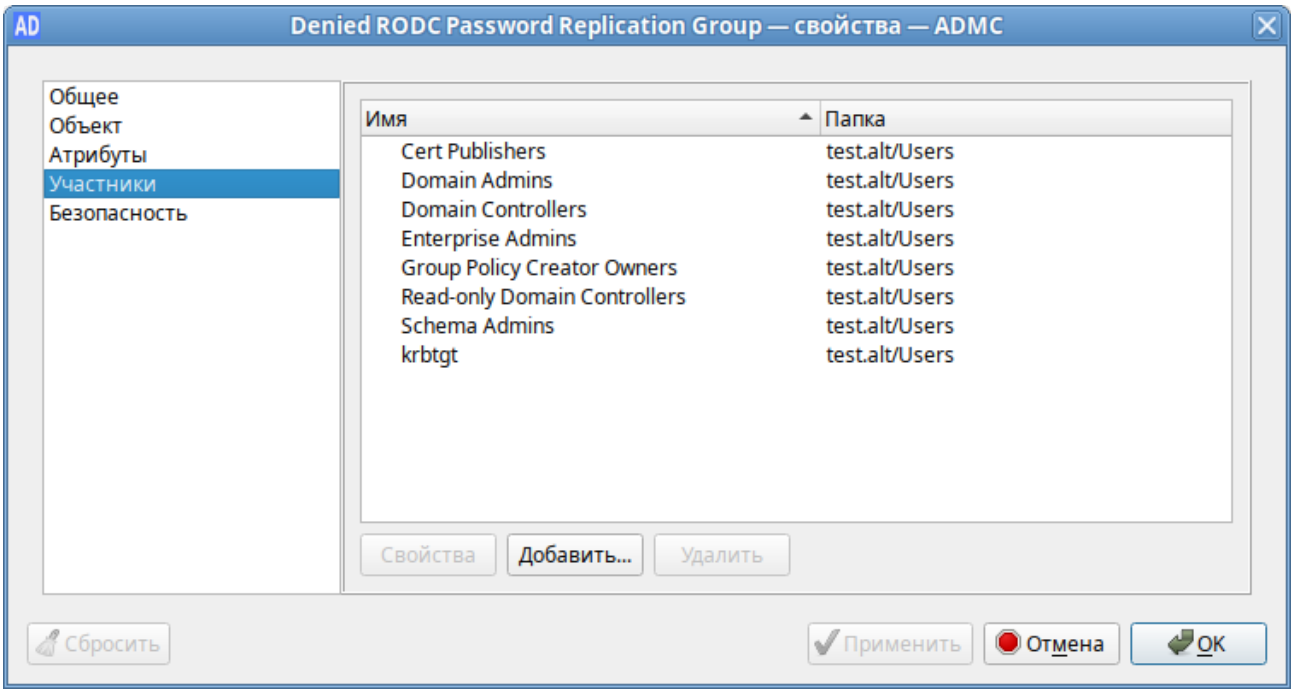
```
$ kinit ivanov
Password for ivanov@TEST.ALT:

$ kinit kim
kinit: A service is not available that is required to process the request
while getting initial credentials
```

По умолчанию в домене создаются две новые глобальные группы:

- Allowed RODC Password Replication Group
- Denied RODC Password Replication Group

Первая группа по умолчанию пуста, а во второй содержатся административные группы безопасности, пароли пользователей которых нельзя реплицировать и кэшировать на RODC. В группу *Denied RODC Password Replication Group* по умолчанию входят группы:

- Cert Publishers
- Domain Admins
- Domain Controllers
- Enterprise Admins
- Group Policy Creator Owners
- Read-only Domain Controllers
- Schema Admins
- учётная запись krbtgt



В группу *Allowed RODC Password Replication Group* обычно добавляются группы пользователей филиала, в котором находится RODC.

2.8. Изменение DNS бэкенда контроллера домена Active Directory

Samba позволяет переключаться между бэкендом INTERNAL_DNS и BIND9_DLZ на контроллере домена Active Directory без потери данных.

2.8.1. Миграция с Samba INTERNAL на BIND9_DLZ

Для переключения с Samba INTERNAL на BIND9_DLZ на контроллере домена необходимо выполнить следующие шаги:

1. Установить и настроить DNS-сервер BIND (см. Настройка BIND9 для работы с Samba AD);
2. Остановить службу **samba**:

```
# systemctl stop samba
```

3. Выполнить миграцию:

```
# samba_upgradedns --dns-backend=BIND9_DLZ
```

4. Отключить модуль SAMBA_INTERNAL в файле **/etc/samba/smb.conf**:
   - если в файле нет параметра ***server services***, добавить в секцию ***global*** строку:

```
server services = -dns
```

   - если в секции ***global*** есть параметр ***server services***, удалить опцию **dns**, например:

```
server services = s3fs, rpc, nbt, wrepl, ldap, cldap, kdc, drepl,
winbindd, ntp_signd, kcc, dnsupdate
```

5. Запустить службу **bind** и сделать её запускаемой по умолчанию:

```
# systemctl enable --now bind
```

6. Запустить службу **samba**:

```
# systemctl start samba
```

2.8.2. Миграция с BIND9_DLZ на Samba INTERNAL

Для переключения с BIND9_DLZ на Samba INTERNAL на контроллере домена необходимо выполнить следующие шаги:

1. Остановить службу **bind** и убрать её из автозагрузки:

```
# systemctl disable --now bind
```

2. Остановить службу **samba**:

```
# systemctl stop samba
```

3. Выполнить миграцию:

```
# samba_upgradedns --dns-backend=SAMBA_INTERNAL
```

4. Отключить модуль BIND9_DLZ в файле **/etc/samba/smb.conf**:

   - если в параметре ***server services*** есть только опция **-dns**, удалить этот параметр из файла (удалить всю строку):

     ```
     server services = -dns
     ```

   - если в секции ***global*** есть параметр ***server services***, добавить в него опцию **dns**, например:

     ```
     server services = s3fs, rpc, nbt, wrepl, ldap, cldap, kdc, drepl,
     winbindd, ntp_signd, kcc, dnsupdate, dns
     ```

5. Запустить службу **samba**:

```
# systemctl start samba
```

Примечание

Так как INTERNAL DNS — это одна из настроек по умолчанию для параметра ***server services***, удаление параметра ***server services*** включает все серверы по умолчанию, включая DNS-сервер.

2.9. Отладочная информация

2.9.1. Настройка уровня журналирования Samba

Дополнительные сведения см. в разделе Уровни журналирования.

2.9.2. Управление процессами

Для проверки выполнения процессов Samba можно использовать утилиту **ps**:

```
# ps axf | grep -E "samba|smbd|winbindd"
…
3078 ?        S      0:00 /usr/sbin/samba --no-process-group
   3091 ?        S      0:00  \_ /usr/sbin/samba --no-process-group
   3092 ?        S      0:00  |   \_ /usr/sbin/samba --no-process-group
   3096 ?        S      0:00  |       \_ /usr/sbin/samba --no-process-group
   3101 ?        Ss     0:00  |           \_ /usr/sbin/smbd -D --option=server
role check:inhibit=yes --foreground
   3138 ?        S      0:00  |               \_ /usr/sbin/smbd -D --
option=server role check:inhibit=yes --foreground
   3139 ?        S      0:00  |               \_ /usr/sbin/smbd -D --
option=server role check:inhibit=yes --foreground
   3149 ?        S      0:00  |               \_ /usr/sbin/smbd -D --
option=server role check:inhibit=yes --foreground
   3150 ?        S      0:00  |               \_ /usr/sbin/smbd -D --
option=server role check:inhibit=yes --foreground
…
   3127 ?        Ss     0:00  |           \_ /usr/sbin/winbindd -D --
option=server role check:inhibit=yes --foreground
   3140 ?        S      0:00  |               \_ /usr/sbin/winbindd -D --
option=server role check:inhibit=yes --foreground
…
```

Все процессы **samba**, **smbd** и **winbindd** должны быть дочерними процессами одного процесса **samba**.

Если структура процесса не отображается:

- следует проверить файлы журнала Samba. Для подробного вывода можно увеличить уровень журнала (см. раздел Уровни журналирования);
- можно запустить Samba в интерактивном режиме и посмотреть на результат:

```
# samba -i
```

2.9.3. DNS

2.9.3.1. Устранение неполадок, связанных с серверной частью DNS

2.9.3.1.1. Внутренний DNS-сервер Samba (SAMBA_INTERNAL)

Если клиенты не могут разрешать записи из зоны DNS AD, необходимо убедиться, что на клиенте указан IP-адрес DNS-сервера, способного разрешать зону AD DNS.

Если конфигурация клиента правильная, следует убедиться, что DNS-сервер Samba работает.

Если DNS-сервер Samba не запускается, необходимо убедиться, что ни один другой процесс не использует TCP- и UDP-порт 53:

- проверить файлы журнала Samba на наличие ошибок, связанных с DNS;
- убедиться, что никакой другой процесс не прослушивает TCP- и UDP-порт 53, например:

```
# ss -tulpn | grep ":53"
```

Если порт 53 занят другим процессом, необходимо:

- остановить службу, прослушивающую порт 53, и отключить её автоматический запуск во время загрузки;
- перезапустить Samba.

2.9.3.1.2. Samba с BIND9_DLZ

Каталог **`/var/lib/samba/bind-dns`** создается только в том случае, если произошло одно из следующих трёх событий:

- при создании контроллера домена использовался параметр ***`--dns-backend=BIND9_DLZ`***;
- при подключении к домену использовался параметр ***`--dns-backend=BIND9_DLZ`***;
- домен был обновлён до Bind9 с помощью команды **`samba_upgradedns`** и опции ***`--dns-backend=BIND9_DLZ`***.

2.10. Удаление контроллера домена

В некоторых ситуациях необходимо навсегда удалить контроллер домена из Active Directory. Если для обычного участника домена достаточно просто удалить соответствующую учётную запись, то чтобы удалить контроллер из домена требуется понизить его роль (demoting).

Если роль контроллера домена будет понижена неправильно, домен может стать нестабильным. Например:

- могут начаться сбои репликации;
- оставшиеся контроллеры домена могут замедлять свою работу из-за тайм-аутов и неудачных попыток репликации;
- вход в систему доменных пользователей может завершиться ошибкой или занять больше времени.

2.10.1. Понижение роли онлайн-контроллера домена

Если удаляемый контроллер домена всё ещё работает правильно, для понижения его роли необходимо выполнить следующие действия (в примере понижается роль DC3):

1. Авторизоваться на контроллере домена под локальным пользователем.
2. Убедиться, что контроллер не владеет никакими ролями FSMO:

```
# samba-tool fsmo show
SchemaMasterRole owner: CN=NTDS Settings,CN=DC1,CN=Servers,CN=Default-First-
Site-Name,CN=Sites,CN=Configuration,DC=test,DC=alt
InfrastructureMasterRole owner: CN=NTDS
Settings,CN=DC2,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=test,DC=alt
RidAllocationMasterRole owner: CN=NTDS
Settings,CN=DC1,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=test,DC=alt
PdcEmulationMasterRole owner: CN=NTDS Settings,CN=DC1,CN=Servers,CN=Default-
First-Site-Name,CN=Sites,CN=Configuration,DC=test,DC=alt
DomainNamingMasterRole owner: CN=NTDS Settings,CN=DC1,CN=Servers,CN=Default-
First-Site-Name,CN=Sites,CN=Configuration,DC=test,DC=alt
DomainDnsZonesMasterRole owner: CN=NTDS
Settings,CN=DC1,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=test,DC=alt
ForestDnsZonesMasterRole owner: CN=NTDS
Settings,CN=DC1,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=test,DC=alt
```

Если контроллеру домена принадлежит одна или несколько ролей FSMO, передать их другому контроллеру домена (см. Просмотр и передача ролей FSMO).

3. Вывести **`objectGUID`** контроллера домена:

```
#
ldbsearch -H /var/lib/samba/private/sam.ldb '(invocationId=*)' --cross-ncs
objectguid | grep -A1 DC3
dn: CN=NTDS Settings,CN=DC3,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=test,DC=alt
objectGUID: 512f03b4-7042-434d-93c0-61dd6a2ea895
```

Для того чтобы убедиться, что все записи DNS были удалены после понижения роли контроллера домена, необходимо знать имя хоста, IP-адрес и objectGUID контроллера домена.

4. Понизить DC:

```
# samba-tool domain demote -Uadministrator
Using dc1.test.alt as partner server for the demotion
Password for [TEST\administrator]:
Deactivating inbound replication
Asking partner server dc1.test.alt to synchronize from us
Changing userControl and container
Removing Sysvol reference: CN=DC3,CN=Enterprise,CN=Microsoft System
Volumes,CN=System,CN=Configuration,DC=test,DC=alt
Removing Sysvol reference: CN=DC3,CN=test.alt,CN=Microsoft System
Volumes,CN=System,CN=Configuration,DC=test,DC=alt
Removing Sysvol reference: CN=DC3,CN=Domain System Volumes (SYSVOL
share),CN=File Replication Service,CN=System,DC=test,DC=alt
Removing Sysvol reference: CN=DC3,CN=Topology,CN=Domain System
Volume,CN=DFSR-GlobalSettings,CN=System,DC=test,DC=alt
updating ForestDnsZones.test.alt keeping 2 values, removing 1 values
updating test.alt keeping 6 values, removing 1 values

…
Demote successful
```

5. Остановить службу **samba**:

```
# systemctl stop samba
```

6. Если этот контроллер работал, как доменный сервер DNS:

   - остановите службу DNS:

     ```
     # systemctl stop bind
     ```

   - убедиться, что члены домена и контроллеры домена больше не используют этот хост для разрешения зон AD DNS.

2.10.2. Понижение автономного контроллера домена

В определенных ситуациях, например при сбое оборудования, из домена необходимо удалить контроллер домена, который больше недоступен. В этом случае понизить уровень контроллера домена, можно на оставшемся работающий контроллер домена Samba.

Важно

Эта процедура должна выполняться только в том случае, если контроллер домена, который нужно понизить, больше не подключен к AD, и его нельзя понизить так, как описано в разделе Понижение роли онлайн-контроллера домена. Это гарантирует, что все изменения, такие как изменения пароля, будут реплицированы на другой контроллер домена. В противном случае такие изменения будут потеряны. Вы можете получить список изменений с помощью Samba-инструмента ldapcmp. При описанной ниже процедуре все изменения (например, изменения паролей) не будут реплицированы на работающий DC.

Важно

Нельзя понизить статус автономного удаленного контроллера домена с контроллера домена, на котором работает *Samba* 4.4 или более ранней версии.

Для понижения статуса неработающего контроллера домена необходимо выполнить следующие действия (в примере понижается статус DC3):

1. Авторизоваться на работающем контроллере домена.

2. Убедиться, что понижаемый контроллер не владеет никакими ролями FSMO:

   ```
   # samba-tool fsmo show
   SchemaMasterRole owner: CN=NTDS Settings,CN=DC1,CN=Servers,CN=Default-First-
   Site-Name,CN=Sites,CN=Configuration,DC=test,DC=alt
   InfrastructureMasterRole owner: CN=NTDS
   Settings,CN=DC2,CN=Servers,CN=Default-First-Site-
   Name,CN=Sites,CN=Configuration,DC=test,DC=alt
   RidAllocationMasterRole owner: CN=NTDS
   Settings,CN=DC1,CN=Servers,CN=Default-First-Site-
   Name,CN=Sites,CN=Configuration,DC=test,DC=alt
   PdcEmulationMasterRole owner: CN=NTDS Settings,CN=DC1,CN=Servers,CN=Default-
   First-Site-Name,CN=Sites,CN=Configuration,DC=test,DC=alt
   ```

```
DomainNamingMasterRole owner: CN=NTDS Settings,CN=DC1,CN=Servers,CN=Default-
First-Site-Name,CN=Sites,CN=Configuration,DC=test,DC=alt
DomainDnsZonesMasterRole owner: CN=NTDS
Settings,CN=DC1,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=test,DC=alt
ForestDnsZonesMasterRole owner: CN=NTDS
Settings,CN=DC1,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=test,DC=alt
```

Если понижаемому контроллеру домена принадлежит одна или несколько ролей FSMO, захватить их локальном контроллере домена (см. Захват роли FSMO).

3. Убедиться, что понижаемый контроллер домена отключён.

4. Вывести **`objectGUID`** контроллера домена:

```
#
ldbsearch -H /var/lib/samba/private/sam.ldb '(invocationId=*)' --cross-ncs
objectguid | grep -A1 DC3
dn: CN=NTDS Settings,CN=DC3,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=test,DC=alt
objectGUID: 512f03b4-7042-434d-93c0-61dd6a2ea895
```

Для того чтобы убедиться, что все записи DNS были удалены после понижения роли контроллера домена, необходимо знать имя хоста, IP-адрес и objectGUID контроллера домена.

5. Понизить статус удалённого контроллера домена:

```
# samba-tool domain demote --remove-other-dead-server=DC3
```

6. Если пониженный контроллер работал как доменный сервер DNS, убедиться, что члены домена и контроллеры домена больше не используют этот хост для разрешения зон AD DNS.

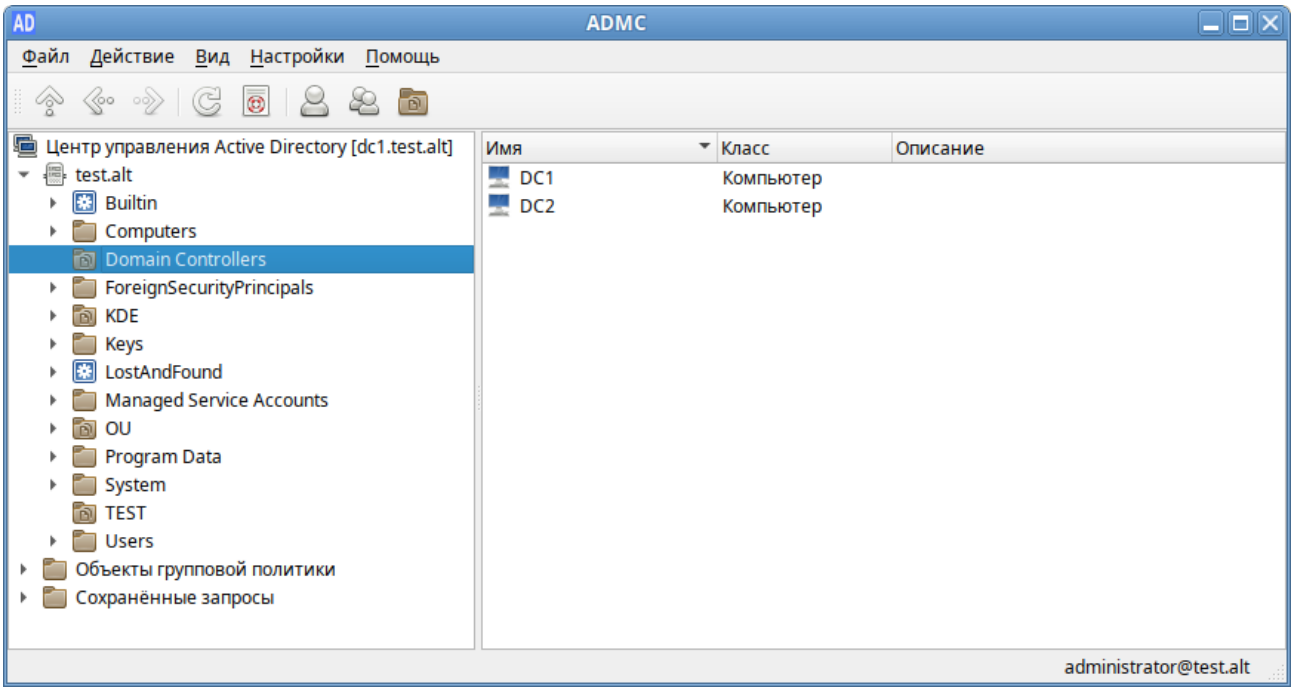
Важно

Не следует подключать к сети контроллер, выведенный по данной процедуре. Иначе ваш домен станет несогласованным.

2.10.3. Проверка

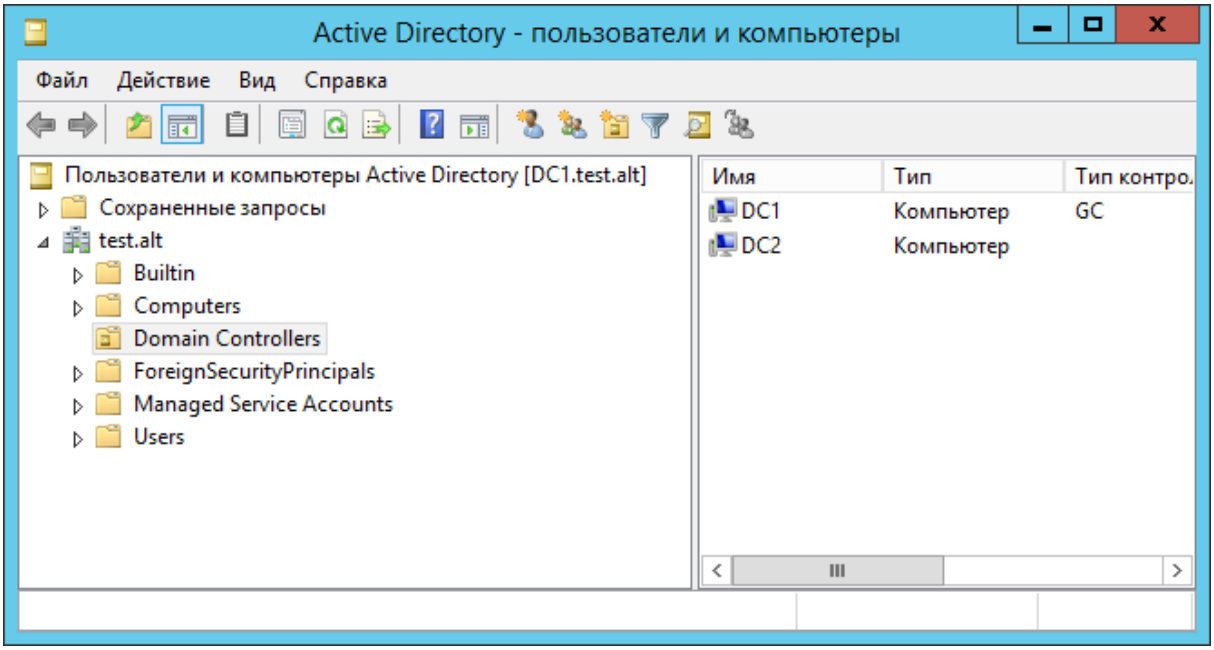
Действия, описанные в этом разделе, предназначены только для проверки и ручного удаления оставшихся записей, если процесс понижения контроллера не удался.

На машине введённой в домен запустить модуль удалённого управления базой данных конфигурации (ADMC) (подробнее см. Модуль удалённого управления базой данных конфигурации). Выбрать запись **`Domain Controllers`** и убедиться, что пониженный контроллер домена был удален:



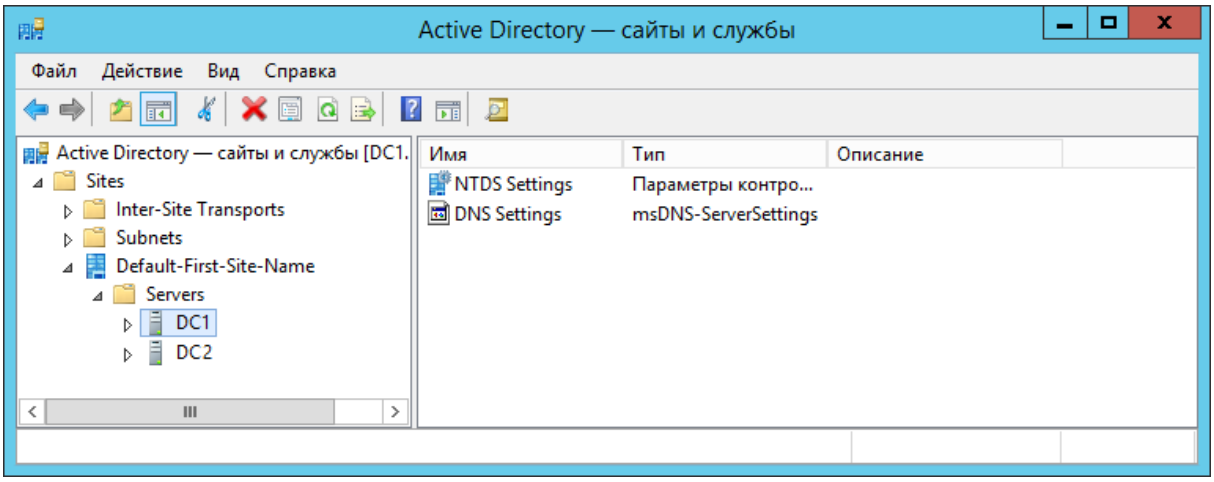
Проверить, что контроллер домена был понижен, можно также в RSAT (см. Установка RSAT). Для этого на машине Windows введённой в домен:

1. Открыть приложение **`Пользователи и компьютеры Active Directory`**, перейти к записи **`Контроллеры домена`** и убедиться, что пониженный контроллер домена был удален:



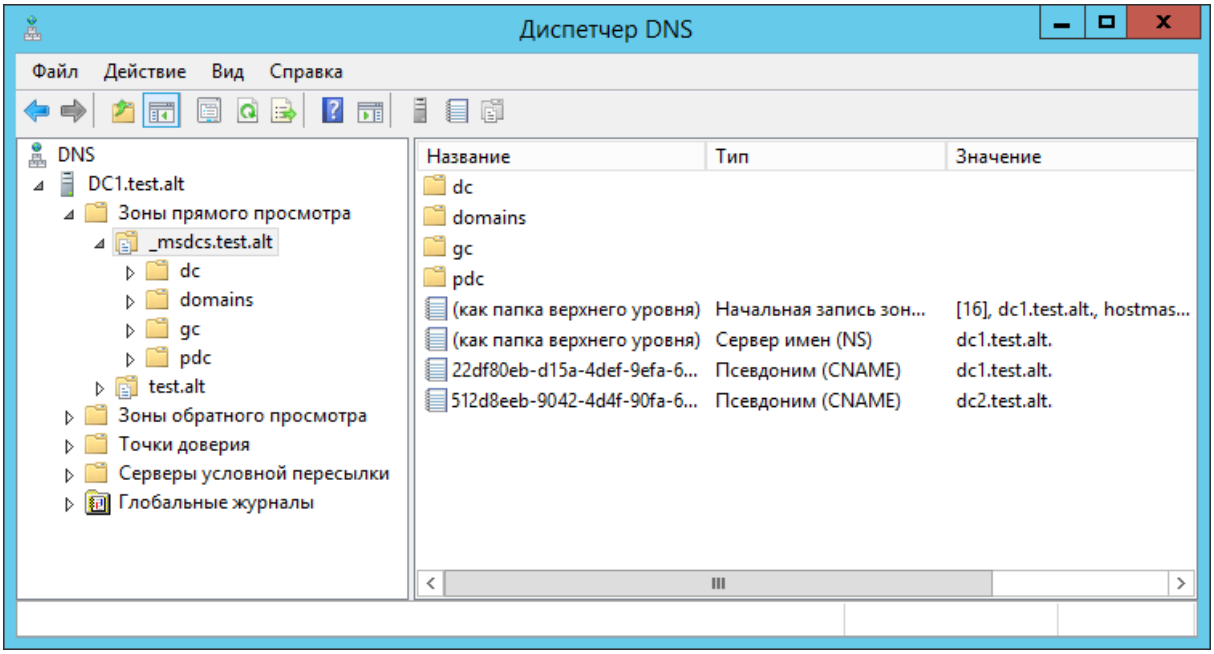
   Если запись всё ещё присутствует в списке, её можно удалить вручную, выбрав в контекстном меню записи пункт **Удалить**.

2. Открыть приложение **`Сайты и службы Active Directory`**, и убедиться, что контроллер домена с пониженным статусом больше не указан ни в одной записи сайта Active Directory:



Если запись всё ещё присутствует в списке, её можно удалить вручную, выбрав в контекстном меню записи пункт **Удалить**.

3. Открыть приложение **DNS**, и убедиться, что имя хоста, IP-адрес и objectGUID контроллера домена больше не используются ни в одной записи DNS в любой зоне AD DNS. Например:



Если записи всё ещё присутствуют в списке, ех можно удалить вручную, выбрав в контекстном меню записи пункт **Удалить**.

2.11. Управление политиками паролей домена

В AD настройки пароля управляют:

- минимальные требования к длине и сложности пароля;
- длина истории паролей: предотвращает повторное использование пользователем предыдущего пароля;
- минимальный и максимальный срок действия пароля: как часто пользователь может/должен менять свой пароль;

- блокировка учетной записи: пороговое значение неудачных попыток входа в систему перед блокировкой учетной записи пользователя и продолжительность блокировки.

Управление политиками паролей домена производится на контроллере домена.

2.11.1. Глобальные парольные политики

Просмотр текущих параметров политик паролей:

```
# samba-tool domain passwordsettings show
Password information for domain 'DC=test,DC=alt'

Password complexity: on
Store plaintext passwords: off
Password history length: 24
Minimum password length: 7
Minimum password age (days): 1
Maximum password age (days): 42
Account lockout duration (mins): 30
Account lockout threshold (attempts): 0
Reset account lockout after (mins): 30
```

Изменить параметр политик паролей:

```
# samba-tool domain passwordsettings set <параметр>
```

Возможные параметры:

- ***--complexity=on|off|default*** — должен ли пароль отвечать требованиям сложности (по умолчанию **on**);
- ***--store-plaintext=on|off|default*** — хранить пароли используя обратимое шифрование (по умолчанию **off**);
- ***--history-length=целое число|default*** — число хранимых предыдущих паролей пользователей (требование неповторяемости паролей) (по умолчанию **24**);
- ***--min-pwd-length=целое число|default*** — минимальное количество символов в пароле (по умолчанию **7**);
- ***--min-pwd-age=целое число|default*** — минимальный срок действия пароля (по умолчанию **1**);
- ***--max-pwd-age=целое число|default*** — максимальный срок действия пароля (по умолчанию **43**);
- ***--account-lockout-duration=целое число|default*** — интервал времени (в минутах), в течение которого возможность аутентификации для пользователя, превысившего количество попыток входа, будет заблокирована (по умолчанию **30**);
- ***--account-lockout-threshold=целое число|default*** — допустимое количество неудачных попыток ввода пароля перед блокировкой учетной записи (по умолчанию **0** — никогда не блокировать);
- ***--reset-account-lockout=целое число|default*** — интервал времени (в минутах), по истечении которого записанное количество попыток начинается заново (по умолчанию **30**).

Изменить минимальную длину пароля и количество неудачных попыток входа в систему:

```
# samba-tool domain passwordsettings set --min-pwd-length=7 --account-lockout-threshold=3
Minimum password length changed!
Account lockout threshold changed!
All changes applied successfully!
```

Примечание

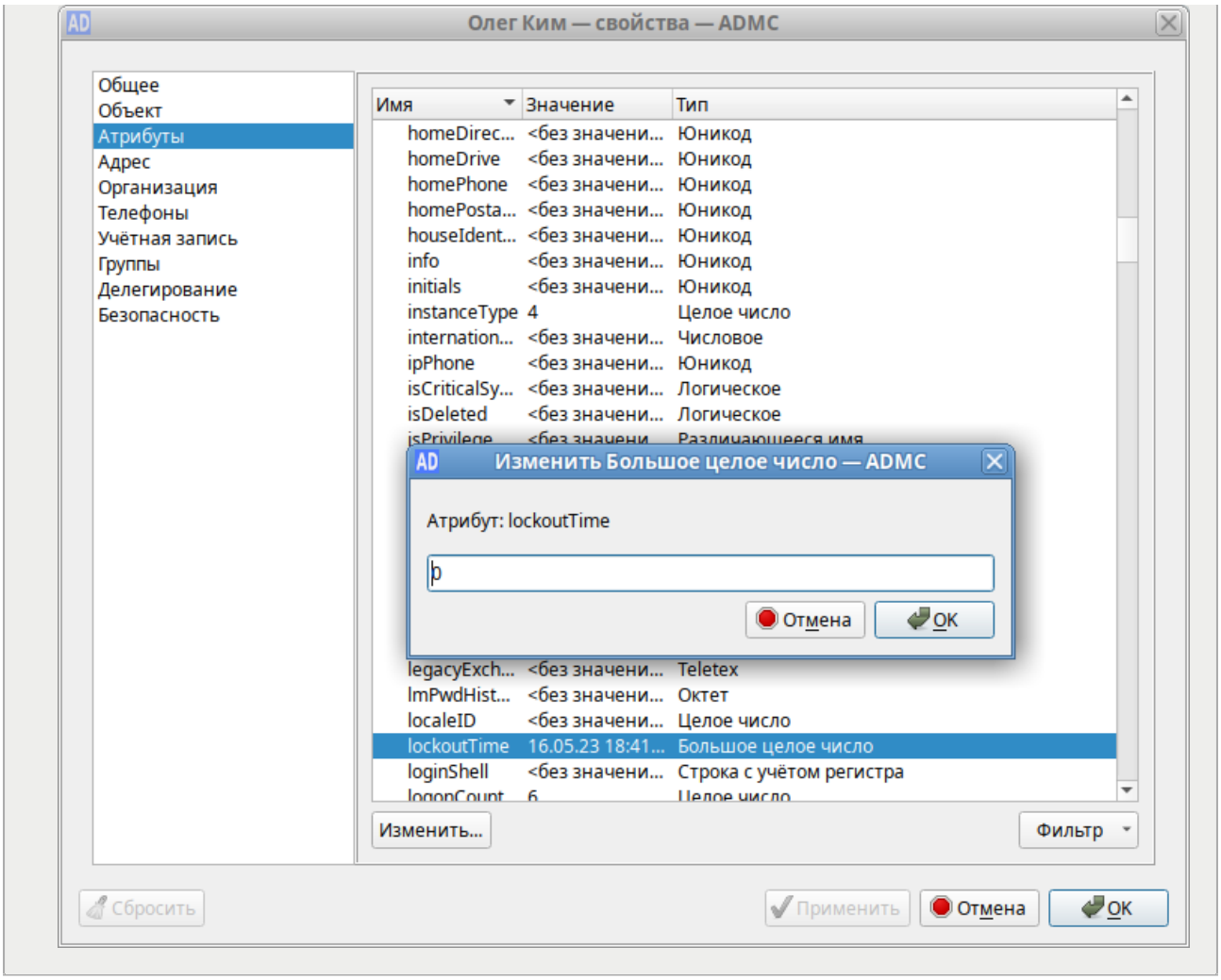
Определить, что учётная запись пользователя заблокирована после нескольких неудачных попыток входа в систему можно, если ***badPwdCount*** достиг своего порога и для пользователя существует параметр ***lockoutTime***:

```
# samba-tool user show ivanov
…
badPwdCount: 3
badPasswordTime: 133560395216186060
lockoutTime: 133560395216186060
…
```

Чтобы разблокировать пользователя, необходимо отредактировать объект учётной записи пользователя, установив для атрибута ***lockoutTime*** значение 0:

```
# samba-tool user edit ivanov
Modified User 'ivanov' successfully

# samba-tool user show ivanov
…
badPasswordTime: 133560395216186060
lockoutTime: 0
…
```

Разблокировать пользователя также можно в модуле удалённого управления базой данных конфигурации (ADMC) (подробнее см. Модуль удалённого управления базой данных конфигурации):



2.11.2. Объекты настроек паролей (PSO)

PSO позволяют администраторам AD переопределять параметры политики паролей домена и настраивать более точные параметры паролей для конкретных пользователей или групп пользователей. Например, для определённых пользователей можно установить требование минимальной длины пароля, ослабить ограничения сложности для других пользователей и т.д. PSO могут применяться к группам или к отдельным пользователям.

Изменить PSO:

```
# samba-tool domain passwordsettings pso <подкоманда>
```

Доступные подкоманды:

1. **`apply`** — применить политику паролей PSO к пользователю или группе;
2. **`create`** — создать новый объект настроек пароля (PSO);
3. **`delete`** — удалить объект настроек пароля (PSO);
4. **`list`** — вывести список всех объектов настроек пароля (PSO);
5. **`set`** — изменить объект настроек пароля (PSO);
6. **`show`** — показать детали объекта настроек пароля;

7. **show-user** — отобразить настройки пароля, которые применяются к пользователю;

8. **unapply** — обновить PSO, чтобы он больше не применялся к пользователю или группе.

Создание правила пароля для пользователя ivanov:

```
# samba-tool domain passwordsettings pso create PwPolicyUser 1 --min-pwd-
length=10
Not all password policy options have been specified.
For unspecified options, the current domain password settings will be used as the
default values.
PSO successfully created: CN=PwPolicyUser,CN=Password Settings
Container,CN=System,DC=test,DC=alt
Password information for PSO 'PwPolicyUser'

Precedence (lowest is best): 1
Password complexity: on
Store plaintext passwords: off
Password history length: 24
Minimum password length: 10
Minimum password age (days): 1
Maximum password age (days): 42
Account lockout duration (mins): 30
Account lockout threshold (attempts): 0
Reset account lockout after (mins): 30

# samba-tool domain passwordsettings pso apply PwPolicyUser ivanov
The following PSO settings apply to user 'ivanov'.

Password information for PSO 'PwPolicyUser'

Precedence (lowest is best): 1
Password complexity: on
Store plaintext passwords: off
Password history length: 24
Minimum password length: 10
Minimum password age (days): 1
Maximum password age (days): 42
Account lockout duration (mins): 30
Account lockout threshold (attempts): 0
Reset account lockout after (mins): 30

Note: PSO applies directly to user (any group PSOs are overridden)
```

К одному и тому же пользователю может применяться множество различных PSO (напрямую или через группы). Если несколько PSO применяются к одному и тому же пользователю, в основном вступает в силу PSO с наименьшим приоритетом. Однако PSO, которые применяются непосредственно к пользователю, всегда превосходят PSO, унаследованные через членство в группе. Чтобы увидеть, какой PSO действует для данного пользователя, используется команда настройки пароля домена **samba-tool pso show-user**:

```
# samba-tool domain passwordsettings pso show-user kim
No PSO applies to user 'kim'. The default domain settings apply.
Refer to 'samba-tool domain passwordsettings show'.
```

Если для пользователя не создано правила, будет применяться правило по умолчанию.

Примечание

Необходимо одновременно настраивать политику паролей для всех остальных пользователей, иначе есть риск снижения производительности при настройке PSO и применении их к пользователям. Например:

```
# samba-tool domain passwordsettings pso create PwPolicyAdmins 1 --min-pwd-length=16
# samba-tool domain passwordsettings pso apply PwPolicyAdmins "domain admins"
# samba-tool domain passwordsettings pso create PwPolicyUsers 3 --min-pwd-length=8
# samba-tool domain passwordsettings pso apply PwPolicyUsers "domain admins"
# samba-tool domain passwordsettings pso create PwPolicyService 2 --min-pwd-length=24
# samba-tool domain passwordsettings pso apply PwPolicyService "domain admins"
```

Если объектов PSO вообще нет, производительность не снижается.

Расчет PSO включает в себя расчет членства пользователя в группах, что является довольно дорогостоящим расчетом. Если PSO применяется непосредственно к пользователю (а не к группе), то дорогостоящие групповые вычисления пропускаются. Однако применение PSO непосредственно к пользователям делает управление PSO более сложным по сравнению с применением PSO к группам.

Глава 3. Репликация

Репликация Active Directory — метод, посредством которого изменения в базе службы каталогов на одном контроллере домена передаются другим контроллерам.

В Samba всё, что хранится внутри AD, реплицируется между контроллерами домена (пользователи, группы и записи DNS).

В настоящее время Samba не поддерживает протокол репликации распределенной файловой системы (DFS-R), используемый для репликации Sysvol. Методы решения этой проблемы см. в разделе Двунаправленная репликация SysVol.

3.1. Настройка репликации

Предупреждение

Без успешной двунаправленной репликации в течение 14 дней DC исключается из Active Directory.

Предупреждение

Указание аутентифицирующей информации (имени пользователя и пароля) обязательно!

Команда репликации:

```
# samba-tool drs replicate <destinationDC> <sourceDC> <NC> [options]
```

Процедура двусторонней репликации:

1. Репликация с первого контроллера домена на второй:

   ```
   # samba-tool drs replicate dc2.test.alt dc1.test.alt dc=test,dc=alt -
   Uadministrator
   Password for [TEST\administrator]:
   Replicate from dc1.test.alt to dc2.test.alt was successful.
   ```

   Сначала указывается приемник, затем источник, после этого реплицируемая ветка в LDAP.

2. Репликация на первый контроллер домена со второго:

   ```
   # samba-tool drs replicate dc1.test.alt dc2.test.alt dc=test,dc=alt -
   Uadministrator
   Password for [TEST\administrator]:
   Replicate from dc2.test.alt to dc1.test.alt was successful.
   ```

   Сначала указывается приемник, затем источник, после этого реплицируемая ветка в LDAP.

   Примечание

   Имя домена в именах серверов можно опустить (если они одинаковые).

3. Для просмотра статуса репликации можно запустить команду на DC (подробнее см. Проверка статуса репликации):

   ```
   # samba-tool drs showrepl
   ```

Примечание

Если репликация на Windows не работает, следует добавить в Active Directory Sites and Services новое соединение Active Directory, реплицировать на DC, подождать минут 5 и попробовать реплицировать с Samba на Windows.

3.2. Проверка статуса репликации

3.2.1. Отображение статуса репликации на контроллере домена Samba

Команда **`samba-tool drs showrepl`** отображает установленные связи с другими контроллерами домена в лесу AD. Соединения отображаются с точки зрения контроллера домена, на котором запускается команда. Пример:

```
# samba-tool drs showrepl
Default-First-Site-Name\DC2
DSA Options: 0x00000001
DSA object GUID: 899a8050-fd2f-44f6-9f19-53f7f63b0348
DSA invocationId: ac8f1710-0f0b-401a-aa8b-4bdf30517f6b

==== INBOUND NEIGHBORS ====

DC=DomainDnsZones,DC=test,DC=alt
    Default-First-Site-Name\DC1 via RPC
        DSA object GUID: 82c19d1f-a5d8-4ad9-a2e5-a38cf2e8a497
        Last attempt @ Wed Apr 19 11:09:03 2023 EET was successful
        0 consecutive failure(s).
        Last success @ Wed Apr 19 11:09:03 2023 EET

CN=Configuration,DC=test,DC=alt
    Default-First-Site-Name\DC1 via RPC
        DSA object GUID: 82c19d1f-a5d8-4ad9-a2e5-a38cf2e8a497
        Last attempt @ Wed Apr 19 11:09:03 2023 EET was successful
        0 consecutive failure(s).
        Last success @ Wed Apr 19 11:09:03 2023 EET

DC=ForestDnsZones,DC=test,DC=alt
    Default-First-Site-Name\DC1 via RPC
        DSA object GUID: 82c19d1f-a5d8-4ad9-a2e5-a38cf2e8a497
        Last attempt @ Wed Apr 19 11:09:03 2023 EET was successful
        0 consecutive failure(s).
        Last success @ Wed Apr 19 11:09:03 2023 EET

DC=test,DC=alt
    Default-First-Site-Name\DC1 via RPC
        DSA object GUID: 82c19d1f-a5d8-4ad9-a2e5-a38cf2e8a497
        Last attempt @ Wed Apr 19 11:09:04 2023 EET was successful
        0 consecutive failure(s).
        Last success @ Wed Apr 19 11:09:04 2023 EET

CN=Schema,CN=Configuration,DC=test,DC=alt
    Default-First-Site-Name\DC1 via RPC
        DSA object GUID: 82c19d1f-a5d8-4ad9-a2e5-a38cf2e8a497
        Last attempt @ Wed Apr 19 11:09:04 2023 EET was successful
        0 consecutive failure(s).
        Last success @ Wed Apr 19 11:09:04 2023 EET

==== OUTBOUND NEIGHBORS ====

DC=DomainDnsZones,DC=test,DC=alt
    Default-First-Site-Name\DC1 via RPC
        DSA object GUID: 82c19d1f-a5d8-4ad9-a2e5-a38cf2e8a497
        Last attempt @ NTTIME(0) was successful
        0 consecutive failure(s).
```

```
        Last success @ NTTIME(0)

CN=Configuration,DC=test,DC=alt
    Default-First-Site-Name\DC1 via RPC
        DSA object GUID: 82c19d1f-a5d8-4ad9-a2e5-a38cf2e8a497
        Last attempt @ NTTIME(0) was successful
        0 consecutive failure(s).
        Last success @ NTTIME(0)

DC=ForestDnsZones,DC=test,DC=alt
    Default-First-Site-Name\DC1 via RPC
        DSA object GUID: 82c19d1f-a5d8-4ad9-a2e5-a38cf2e8a497
        Last attempt @ NTTIME(0) was successful
        0 consecutive failure(s).
        Last success @ NTTIME(0)

DC=test,DC=alt
    Default-First-Site-Name\DC1 via RPC
        DSA object GUID: 82c19d1f-a5d8-4ad9-a2e5-a38cf2e8a497
        Last attempt @ NTTIME(0) was successful
        0 consecutive failure(s).
        Last success @ NTTIME(0)

CN=Schema,CN=Configuration,DC=test,DC=alt
    Default-First-Site-Name\DC1 via RPC
        DSA object GUID: 82c19d1f-a5d8-4ad9-a2e5-a38cf2e8a497
        Last attempt @ NTTIME(0) was successful
        0 consecutive failure(s).
        Last success @ NTTIME(0)

==== KCC CONNECTION OBJECTS ====

Connection --
    Connection name: a46c895e-658b-463e-9ab5-a1c237fca4b1
    Enabled        : TRUE
    Server DNS name : dc1.test.alt
    Server DN name  : CN=NTDS Settings,CN=DC1,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=test,DC=alt
        TransportType: RPC
        options: 0x00000001
Warning: No NC replicated for Connection!
```

Связи отображаются в разделах ***INBOUND NEIGHBORS*** и ***OUTBOUND NEIGHBORS***. В каждом разделе должно быть по 5 пунктов:

```
CN=Schema,CN=Configuration,DC=test,DC=alt
DC=ForestDnsZones,DC=test,DC=alt
DC=test,DC=alt
DC=DomainDnsZones,DC=test,DC=alt
CN=Configuration,DC=test,DC=alt
```

В разделе ***INBOUND NEIGHBORS*** в пункте ***Last attempt*** должны стоять актуальные дата и время, идентичные указанным в строке ***Last success*** (отображает время последней репликации). Должно быть ***0 consecutive failure(s)***.

Если в разделе ***INBOUND NEIGHBORS*** есть записи:

```
Last attempt @ NTTIME(0) was successful
…
Last success @ NTTIME(0)
```

необходимо подождать (соединение устанавливается).

В разделе ***KCC CONNECTION OBJECTS*** быть приведён список всех контроллеров домена чьи KCC установили соглашения о репликации с текущим контроллером домена. В случае когда контроллер домена только только был добавлен в домен и запущен, может пройти до 15 минут до того, как соглашения будут установлены.

Примечание

Предупреждение

```
No NC replicated for Connection!
```

можно игнорировать. Оно появляется из-за того, что при регистрации нового DC Samba неверно устанавливает некоторые флаги репликации.

Так же можно проверить репликацию LDAP:

```
# samba-tool ldapcmp ldap://dc1.test.alt ldap://dc2.test.alt -Uadministrator
Password for [TEST\administrator]:

* Comparing [DOMAIN] context...

* Objects to be compared: 274

* Result for [DOMAIN]: SUCCESS

* Comparing [CONFIGURATION] context...

* Objects to be compared: 1625

* Result for [CONFIGURATION]: SUCCESS

* Comparing [SCHEMA] context...

* Objects to be compared: 1739

* Result for [SCHEMA]: SUCCESS

* Comparing [DNSDOMAIN] context...

* Objects to be compared: 41

* Result for [DNSDOMAIN]: SUCCESS

* Comparing [DNSFOREST] context...

* Objects to be compared: 18

* Result for [DNSFOREST]: SUCCESS
```

Данная команда сравнит значения атрибутов объектов всего каталога на DC1 и DC2. В ряде случаев атрибуты объектов на разных контроллерах могут отличаться, и в выводе команды это будет видно. Но не во всех случаях это будет признаком проблемы с репликацией.

3.2.2. Отображение статусов репликации на контроллере домена Windows

Для отображения статуса входящей репликации на контроллере домена Windows можно использовать утилиту **repadmin**:

```
> repadmin /showrepl
```

Windows не поддерживает отображение статусов исходящих подключений репликации. Чтобы обойти эту проблему, можно отобразить статусы входящих подключений на контроллерах домена Samba, на которые реплицируется контроллер домена Windows:

1. Найти в AD всех партнеров репликации Windows DC. Например, чтобы отобразить партнеров по репликации контроллера домена с именем WindowsDC:

   ```
   # ldbsearch -H /var/lib/samba/private/sam.ldb '(fromServer=*CN=WindowsDC*)'
   --cross-ncs dn
   # record 1
   dn: CN=a46c895e-658b-463e-9ab5-a1c237fca4b1,CN=NTDS
   Settings,CN=DC2,CN=Servers,CN=Default-First-Site-
   Name,CN=Sites,CN=Configuration,DC=test,DC=alt

   # returned 1 records
   # 1 entries
   # 0 referrals
   ```

   В этом примере возвращается один партнер по репликации (имя хоста: DC2). Имя хоста партнера по репликации является частью возвращаемого отличительного имени (DN).

2. На каждом контроллере домена Samba, полученном на предыдущем шаге, выполнить команду **samba-tool drs showrepl** для отображения статуса репликации каталога.

   Необходимо убедиться, что каждый реплицируемый контейнер каталогов указан для контроллера домена Windows в разделе ***INBOUND NEIGHBORS*** на контроллере домена Samba, а статусы успешны.

3.3. Двунаправленная репликация SysVol

Каталог **Sysvol** присутствует на всех контроллерах домена AD и используется для хранения логон скриптов и объектов групповых политик. Отсутствие репликации этого каталога приведет к неправильной работе групповых политик и сценариев входа.

Samba в своем текущем состоянии не поддерживает репликацию SysVol через DFS-R (репликация распределенной файловой системы) или более старую FRS (службу репликации файлов), используемую в Windows Server 2000/2003 для репликации SysVol. В настоящее время для репликации SysVol можно использовать один из следующих обходных путей:

- двунаправленная репликация SysVol на основе Rsync/Unison (только Samba DC);
- двунаправленная репликация SysVol на основе Rsync/osync (только Samba DC);

Важно

Следует синхронизировать **idmap.ldb** из контроллера домена, имеющего роль FSMO PDC_Emulator, со всеми другими контроллерами домена. Это гарантирует, что все контроллеры домена будут использовать одни и те же идентификаторы. Если файл **idmap.ldb** не синхронизируется, на каждом контроллере домена будут разные идентификаторы.

Синхронизировать **idmap.ldb** (см. раздел Сопоставления встроенных идентификаторов пользователей и групп) необходимо при первом присоединении к новому контроллеру домена, а затем переодически (для того чтобы гарантировать постоянство идентификаторов не нужно синхронизировать **idmap.ldb** каждый раз при синхронизации SysVol, но это следует делать периодически).

3.3.1. Настройка двунаправленной репликации SysVol на базе Rsync/Unison

Исходные данные:

- все команды выполняются от пользователя root;
- первый контроллер домена — DC1;
- второй контроллер домена — DC2 (уже присоединён к домену);
- **sysvol** расположен в **/var/lib/samba/** как на DC1, так и на DC2;
- **rsync** расположен в **/usr/bin/rsync**;
- **unison** расположен в **/usr/bin/unison**;
- журнал sysvolsync пишется в файл **/var/log/sysvol-sync.log**.

Примечание

Предварительно должно быть настроено беспарольное межсерверное взаимодействие (подробнее, см. Настройка беспарольного доступа по ssh)

На первом контроллере домена (DC1):

1. Установить пакеты *rsync* и *unison*:

```
# apt-get install rsync unison
```

2. При низких скоростях в сети, **unison** может некорректно работать, поэтому при повторной его работе будет использоваться ранее созданное подключение по ssh, для этого:

```
# mkdir ~/.ssh/ctl
# cat < < EOF > ~/.ssh/ctl/config
Host *
ControlMaster auto
ControlPath ~/.ssh/ctl/%h_%p_%r
ControlPersist 1
EOF
```

3. Создать каталог **/root/.unison/**:

```
# mkdir /root/.unison
```

4. Для определения политики синхронизации создать файл конфигурации unison **/root/.unison/default.prf** с следующим содержимым:

```
# Список каталогов, которые будут синхронизированы
root = /var/lib/samba
root = ssh://root@DC2.test.alt//var/lib/samba
# Список подкаталогов, которые нужно синхронизировать
path = sysvol

auto=true
batch=true
perms=0
rsync=true
maxthreads=1
retry=3
confirmbigdeletes=false
servercmd=/usr/bin/unison
# использовать rsync только для больших файлов??
copythreshold=1000
copyprog = /usr/bin/rsync -XAavz --rsh='ssh -p 22' --inplace --compress
copyprogrest = /usr/bin/rsync -XAavz --rsh='ssh -p 22' --partial --inplace
--compress
copyquoterem = true
copymax = 1

# Сохранять журнал с результатами работы в отдельном файле
logfile = /var/log/sysvol-sync.log
```

5. Создать файл для записи журнала репликации (необходимо настроить ротацию логов для этого файла, так как размер журнала не контролируется): # **touch /var/log/sysvol-sync.log**

На втором контроллере домена (DC2) установить пакеты *rsync* и *unison*:

```
# apt-get install rsync unison
```

Сделать резервную копию каталога **sysvol**, и запустить команду синхронизации:

```
# /usr/bin/rsync -XAavz --log-file /var/log/sysvol-sync.log --delete-after -f"+
*/" -f"- *" /var/lib/samba/sysvol root@dc2.test.alt:/var/lib/samba && /usr/bin/
unison
```

Утилита **rsync** создает структуры каталогов с расширенными атрибутами, а затем утилита **unison** копирует только эти расширенные атрибуты файлов.

На DC1 включить синхронизацию по расписанию:

```
# crontab -e
*/5 * * * * /usr/bin/unison -silent
```

Повторная синхронизация каталога:

- отключить синхронизацию по расписанию на DC1;
- **rsync** и **unison** не должны выполняться в данный момент (можно проверить командой **ps -aux**);
- удалить хеш-файлы на DC1 и DC2 в **/root/.unison**;
- проверить **sysvol** и повторить синхронизацию;
- убедиться, что синхронизация выполнена успешно;
- включить синхронизацию по расписанию на DC1.

Если контроллеров домена больше чем два, можно создать больше заданий для cron на DC1:

1. Скопировать файл **/root/.inison/default.prf** в другой файл, например: **/root/.inison/sync_dc2.prf**.
2. В файле **/root/.inison/dc2.prf** изменить значение параметра ***root***.
3. Повторить шаги 1 и 2 для всех контроллеров домена.
4. Изменить задание на синхронизацию по расписанию на DC1:

```
* * * * * /usr/bin/unison sync_dc2 -silent
* * * * * /usr/bin/unison sync_dc3 -silent
…
```

3.3.2. Настройка двунаправленной репликации SysVol на базе Rsync/osync

Исходные данные:

- все команды выполняются от пользователя root;
- первый контроллер домена — DC1;
- второй контроллер домена — DC2 (уже присоединён к домену);
- **sysvol** расположен в **/var/lib/samba/** как на DC1, так и на DC2;
- **rsync** расположен в **/usr/bin/rsync**;
- **osync** расположен в **/usr/bin/osync**;
- журнал sysvolsync пишется в файл **/var/log/osync_*.log**;
- настроено беспарольное взаимодействие между rootами всех контроллеров домена (см. Настройка беспарольного доступа по ssh).

Примечание

Предварительно должно быть настроено беспарольное межсерверное взаимодействие (например, см. Настройка беспарольного доступа по ssh)

На первом контроллере домена (DC1):

1. Установить пакеты *rsync* и *osync*:

```
# apt-get install rsync osync
```

2. Отредактировать файл **/etc/osync/sync.conf**:

```
#!/usr/bin/env bash
INSTANCE_ID="sync_sysvol"
 # Путь до SysVol на текущем сервере
INITIATOR_SYNC_DIR="/var/lib/samba/sysvol"
 # Путь до SysVol на удалённом сервере
TARGET_SYNC_DIR="ssh://root@DC2:22//var/lib/samba/sysvol"
 # ssh ключ root
SSH_RSA_PRIVATE_KEY="/root/.ssh/id_ed25519"
 # Удалённые хосты которые osync пингует перед стартом
REMOTE_3RD_PARTY_HOSTS=""
 # Сохранять xattr
PRESERVE_ACL=yes
 # Сохранять xattr
PRESERVE_XATTR=yes
 # Сохранять резервную копию удалённых файлов
SOFT_DELETE=yes
DESTINATION_MAILS="your@test.alt"
REMOTE_RUN_AFTER_CMD="/usr/bin/samba-tool ntacl sysvolreset"
```

На втором контроллере домена (DC2) установить пакет *rsync*:

```
# apt-get install rsync
```

Сделать резервную копию **sysvol** и запустить команду синхронизации:

```
# /usr/bin/osync.sh /etc/osync/sync.conf --dry --verbose
```

Если команда выполнилась без ошибок, можно удалить параметр **--dry** и запустить команду синхронизации снова:

```
# /usr/bin/osync.sh /etc/osync/sync.conf --verbose
```

В результате **sysvol** будет синхронизирован на обоих серверах.

Примечание

Если в файле **sysvol** параметры ***SOFT_DELETE*** (сохранять резервные копии удалённых файлов) и ***CONFLICT_BACKUP*** (сохранять резервные копии файлов на целевой реплике, если они обновлены из исходной реплики) установлены в значение *yes*, то на источнике и получателе репликации необходимо создать каталоги **.osync_workdir/deleted** и **.osync_workdir/backup**:

```
# mkdir /var/lib/samba/sysvol/.osync_workdir/deleted
# mkdir /var/lib/samba/sysvol/.osync_workdir/backup
```

На DC1 включить синхронизацию по расписанию:

```
# crontab -e
*/5 * * * * root  /usr/bin/osync.sh /etc/osync/sync.conf --silent
```

Если при попытке синхронизировать каталог возникают проблемы необходимо:

- отключить синхронизацию по расписанию на DC1;
- убедиться, что **rsync** и **osync** не выполняются в данный момент (можно проверить, выполнив команду **ps -aux| grep sync**);
- удалить хеш-файлы **.osync_workdir** на DC1 и DC2 в **/var/lib/samba/sysvol/**;
- проверить **sysvol** и повторить синхронизацию;
- убедиться, что синхронизация выполнена успешно;
- включить синхронизацию по расписанию на DC1.

Если контроллеров домена больше чем два, можно создать больше заданий для cron на DC1:

1. Скопировать файл **/etc/osync/sync.conf** в другой файл, например: **/etc/osync/sync_dc3.conf**.
2. В файле **/etc/osync/sync_dc3.conf** изменить значение параметра ***TARGET_SYNC_DIR***.
3. Повторить шаги 1 и 2 для всех контроллеров домена.
4. Изменить задание на синхронизацию по расписанию на DC1:

```
# crontab -e
*/5 * * * * root  /usr/bin/osync.sh /etc/osync/sync.conf --silent
*/5 * * * * root  /usr/bin/osync.sh /etc/osync/sync_dc3.conf --silent
…
```

3.3.3. Сопоставления встроенных идентификаторов пользователей и групп

Чтобы использовать обходной путь репликации Sysvol, все контроллеры домена должны использовать одни и те же сопоставления идентификаторов для встроенных пользователей и групп.

По умолчанию контроллер домена Samba сохраняет идентификаторы пользователей и групп в атрибутах ***xidNumber*** в **idmap.ldb**. Из-за особенностей работы **idmap.ldb** нельзя гарантировать, что каждый контроллер домена будет использовать один и тот же идентификатор для данного пользователя или группы. Для того чтобы убедиться, что используются одни и те же идентификаторы, необходимо:

1. Создать горячую резервную копию файла **/usr/local/samba/private/idmap.ldb** на существующем контроллере домена:

   ```
   # tdbbackup -s .bak /usr/local/samba/private/idmap.ldb
   ```

   Будет создан файл резервной копии **/usr/local/samba/private/idmap.ldb.bak**.

2. Переместить файл резервной копии в каталог **/usr/local/samba/private/** на новом присоединенном контроллере домена с удалением суффикса .bak, (заменить существующий файл).

3. Запустить очистку кэша на новом контроллере домена:

   ```
   # net cache flush
   ```

4. Синхронизировать Sysvol с новым контроллером домена.

5. Сбросить списки управления доступом к файловой системе (ACL) каталога Sysvol на новом контроллере домена:

   ```
   # samba-tool ntacl sysvolreset
   ```

Глава 4. Клиент сети Active Directory

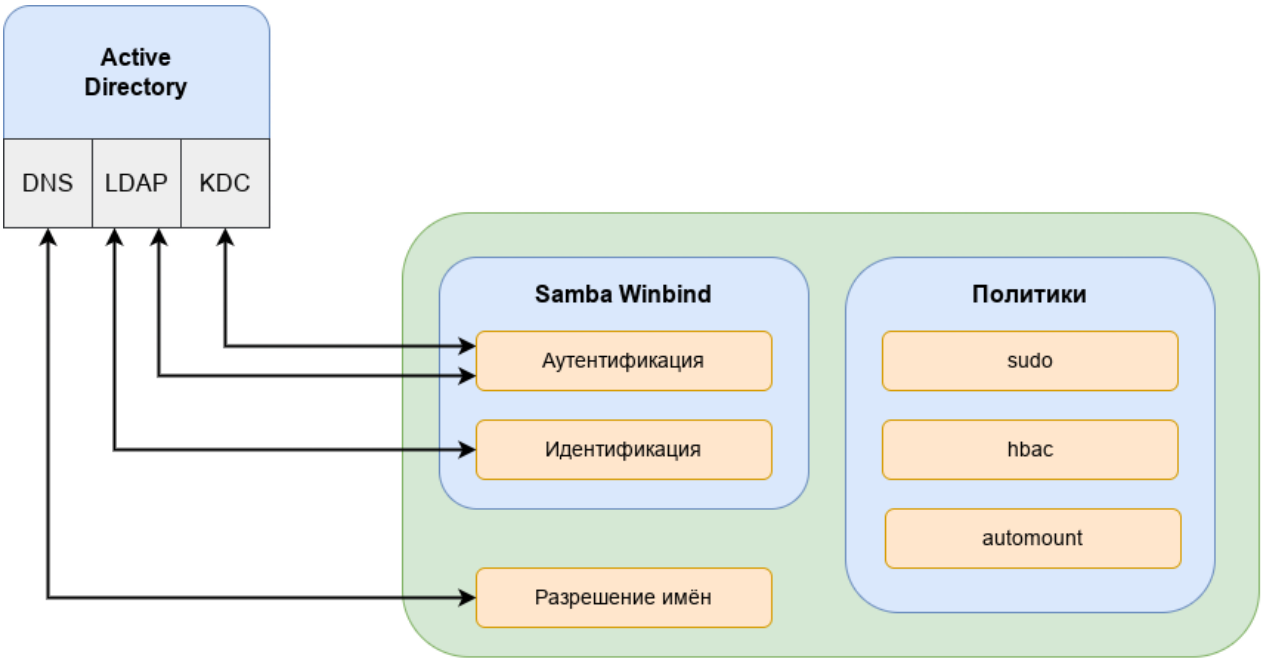
4.1. SSSD vs Winbind

Существует несколько способов прямого подключения системы Linux к AD. В этом разделе описаны функции и возможности двух вариантов интеграции: решение на основе Samba winbind и решение на базе SSSD.

Машины под управлением ОС Альт рекомендуется вводить в домен AD с помощью SSSD, но есть несколько исключений:

1. Если в сети уже развернуты системы Linux, которые уже используют Samba winbind для целей интеграции.
2. Если используется AD с включенным протоколом NTLM (так как SSSD не поддерживает протокол NTLM).
3. Если SSSD не поддерживает определенную функцию, которую поддерживает winbind (например, SSSD не поддерживает доверительные отношения AD между лесами при прямом подключении к AD).

Ниже рассмотрены преимущества и недостатки интеграции на основе Samba winbind и на базе SSSD.

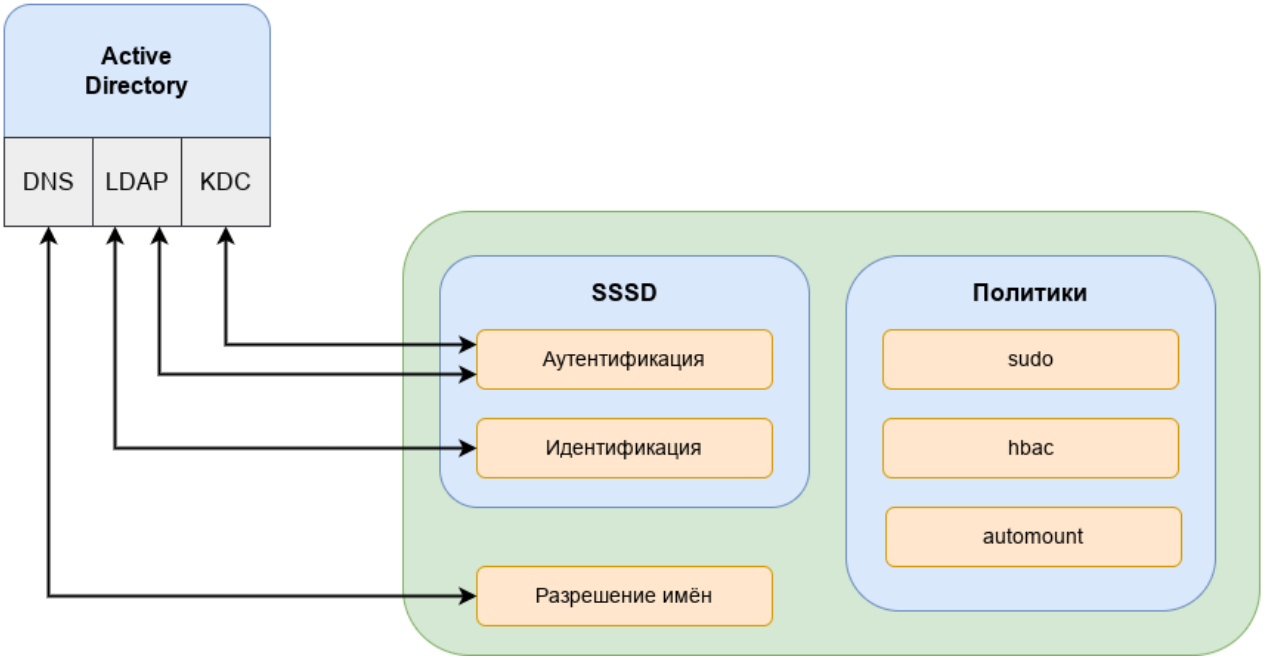


Преимущества варианта интеграции с использованием Samba Winbind:

- Samba Winbind эмулирует клиент Windows в системе Linux и использует преимущества собственных протоколов Windows и расширений протокола LDAP;
- Winbind понимает концепцию доменов и лесов, а также работает с доверием между доменами и лесами;
- Winbind может обнаруживать серверы, используя DNS;
- Winbind может переключиться на другой сервер, если контроллер домена AD становится недоступным;
- Winbind может динамически выполнять сопоставление идентификаторов на основе идентификаторов объектов AD (SID) или использовать атрибуты POSIX, хранящиеся в AD (если эти расширения были загружены).;
- Winbind хорошо интегрируется с клиентом Samba FS и CIF;
- безопасность соединения основана на идентификации клиентской системы и ключах Kerberos, выданных этой системе.

Ограничения Samba Winbind:

- политики не управляются централизованно и должны распространяться вне группы;
- может подключаться только к AD.



SSSD это группа служб, которые являются частью ядра операционной системы Linux и работают вместе для обеспечения аутентификации, поиска удостоверений и возможностей управления доступом для системы Linux. SSSD может взаимодействовать с AD, FreeIPA, Samba DC или любыми другими стандартными реализациями сервера LDAP и/или Kerberos.

Единственным серьезным ограничением для интеграции с использованием SSSD, является поддержка (старого) протокола NTLM. SSSD не реализует этот протокол, потому что по современным стандартам NTLM больше не является безопасным для развертывания. Наилучшей практикой является отказ от использования NTLM.

Преимущества SSSD:

- возможность загрузки и применения политик управления доступом на основе хоста с использованием объектов групповой политики, управляемых в AD;
- может взаимодействовать с разными источниками идентификации, а не только с AD;
- поддерживает очистку DNS (т.е. обнаруживает, были ли удалены или обновлены записи DNS для серверов);
- предоставляет расширенные интерфейсы идентификации на локальной шине сообщений (D-Bus). Этот интерфейс можно использовать для лучшей интеграции приложений, работающих в ОС Linux, с корпоративными источниками идентификации, такими как AD и FreeIPA.

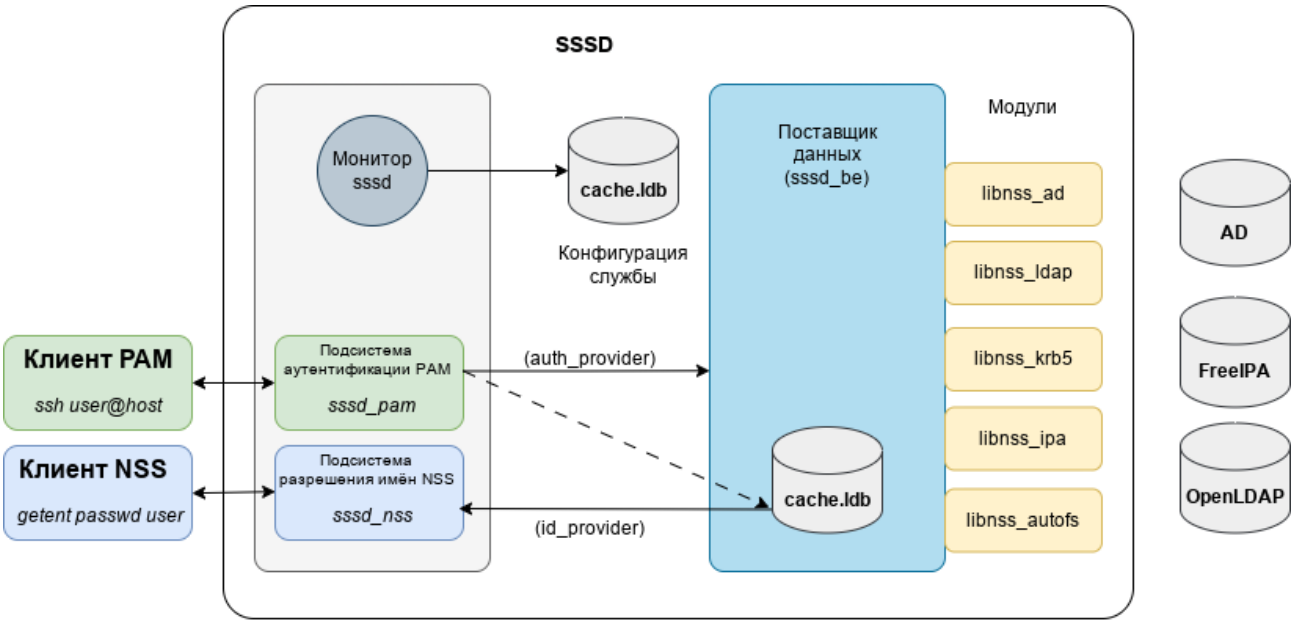


Таблица 4.1. Сравнение Winbind и SSSD

Категория	Описание	Winbind	SSSD
Аутентификация	Проверка подлинности с использованием Kerberos	Да	Да
	Проверка подлинности LDAP	Да	Да
	Поддержка нескольких доменов AD	Да	Да
	Поддержка лесов AD	Да	Да
	Поддержка гетерогенных сетей AD/FreeIPA	Нет	Да
Безопасность	Простота настройки безопасной конфигурации	Нет	Да
	Система имеет идентификатор и её ключ используется для защиты доступа к центральному серверу	Да	Да
	Поддержка NTLM	Да	Нет
Поиск и сопоставление идентификаторов	Динамическое сопоставление идентификаторов AD SID	Да	Да
		Да	Да

Категория	Описание	Winbind	SSSD
	Использование преимуществ конкретных расширений и протоколов AD		
DNS	Обновление и очистка DNS AD	Нет	Да
	Поддержка сайтов AD DNS	Да	Да
Обмен файлами	Интеграция с Samba FS	Да	Да
	Интеграция с клиентом CIFS	Да	Да
Служба печати	Сервер печати CUPS с использованием Kerberos	Да	Да
Политики	Централизованное управление контролем доступа на основе хоста через GPO	Нет	Да
Интеграция с другими сервисами и приложениями	Интеграция с основными утилитами, такими как SSH, sudo, automount	Нет	Да
	Расширенные интерфейсы идентификации по локальной шине сообщений D-Bus	Нет	Да
	Специальные функции для приложений (Docker, Cockpit, GSS Proxy и др.)	Нет	Да

4.2. Подготовка системы к вводу в домен

4.2.1. Установка пакетов

Установить пакет *task-auth-ad-sssd*:

```
# apt-get install task-auth-ad-sssd
```

4.2.2. Синхронизация времени

Синхронизация времени с контроллером домена производится автоматически.

4.2.3. Настройка DNS

AD использует DNS для обнаружения других контроллеров домена и служб, таких как Kerberos. Поэтому, члены и серверы домена AD должны иметь возможность разрешать зоны AD DNS.

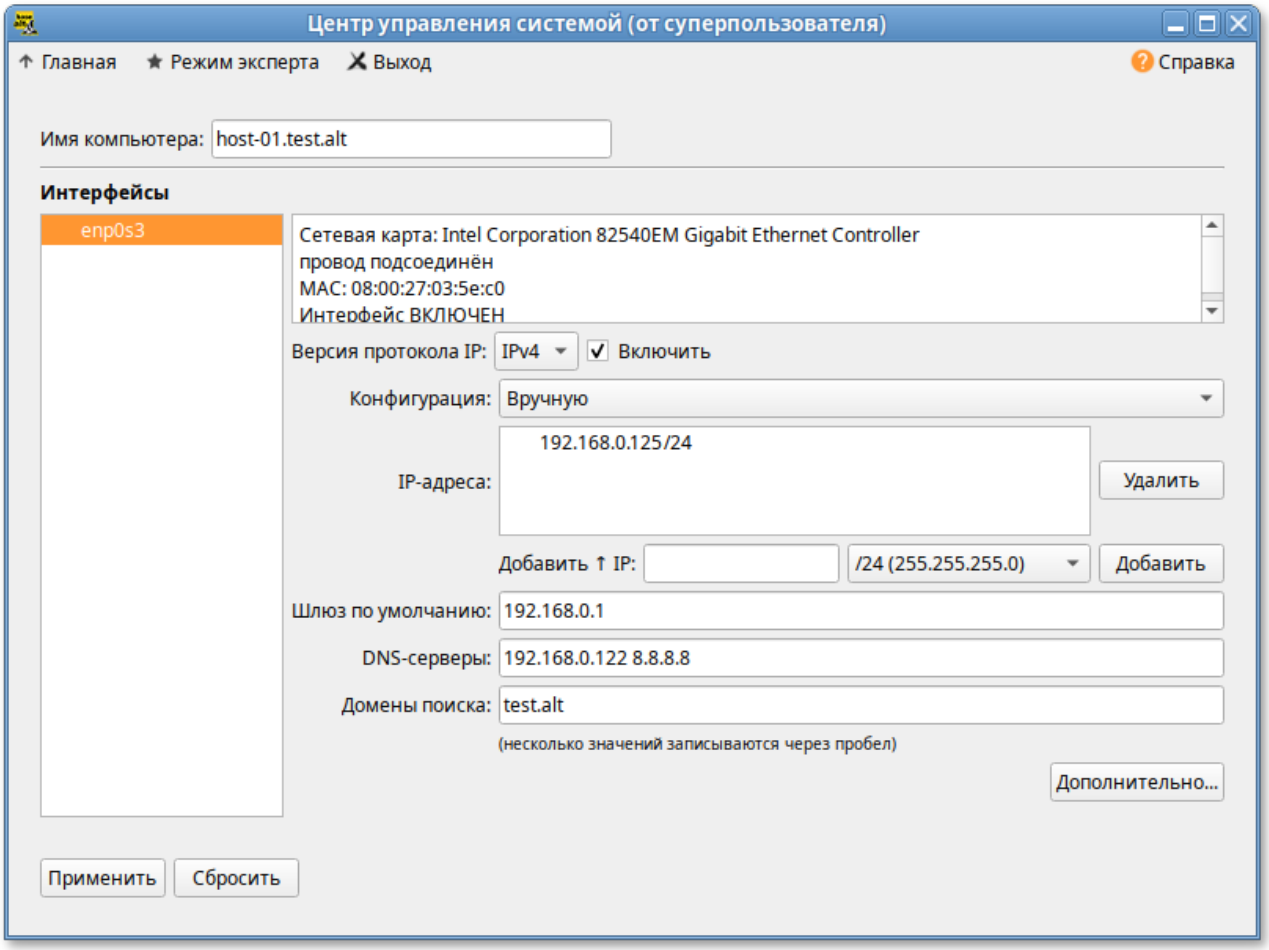
Для ввода компьютера в домен, на нём должен быть доступен сервер DNS, имеющий записи про контроллер домена Active Directory. При получении IP-адреса по DHCP данные о сервере DNS также должны быть получены от DHCP-сервера.

Ниже приведен пример настройки сетевого интерфейса со статическим IP-адресом.

4.2.3.1. Настройка клиентов для использования DNS-серверов вручную

Настройку сети можно выполнить как в графическом интерфейсе, так и в консоли.

В Центре управления системой **Сеть** → **Ethernet интерфейсы** задать имя компьютера, указать в поле **DNS-серверы** DNS-сервер домена и в поле **Домены поиска** — домен для поиска:



Примечание

После изменения имени компьютера могут перестать запускаться приложения. Для решения этой проблемы необходимо перезагрузить систему.

В консоли:

- задать имя компьютера:

```
# hostnamectl set-hostname host-01.test.alt
```

- в качестве первичного DNS должен быть указан DNS-сервер домена. Для этого необходимо создать файл **/etc/net/ifaces/enp0s3/resolv.conf** со следующим содержимым:

```
nameserver 192.168.0.122
```

где 192.168.0.122 — IP-адрес DNS-сервера домена.

- указать службе resolvconf использовать DNS контроллера домена и домен для поиска. Для этого в файле **/etc/resolvconf.conf** добавить/отредактировать следующие параметры:

```
interface_order='lo lo[0-9]* lo.* enp0s3'
search_domains=test.alt
```

где enp0s3 — интерфейс на котором доступен контроллер домена, test.alt — домен.

- обновить DNS адреса:

```
# resolvconf -u
```

Примечание

После изменения имени компьютера могут перестать запускаться приложения. Для решения этой проблемы необходимо перезагрузить систему.

В результате выполненных действий в файле **/etc/resolv.conf** должны появиться строки:

```
search test.alt
nameserver 192.168.0.122
```

4.2.3.2. Проверка разрешения DNS

Для проверки того, что настройки DNS верны и машины могут разрешать IP-адреса и имена, можно использовать команды **nslookup** и **host**.

Прямой поиск:

```
# nslookup dc1.test.alt
Server:         192.168.0.122
Address:192.168.0.1222#53

Name:   dc1.test.alt
Address: 192.168.0.122

# host dc1.test.alt
dc1.test.alt has address 192.168.0.122
```

Обратный поиск:

```
# nslookup 192.168.0.122
122.0.168.192.in-addr.arpa      name = dc1.alt.test.

# host 192.168.0.122
122.0.168.192.in-addr.arpa domain name pointer dc1.alt.test.
```

Обратите внимание, что в Samba AD обратная зона не настраивается автоматически. Чтобы настроить обратную зону, см. Администрирование DNS.

AD использует записи SRV для поиска служб, таких как Kerberos и LDAP. Проверка разрешения SRV-записей:

```
$ nslookup
> set type=SRV
> _ldap._tcp.test.alt
Server:         192.168.0.122
Address:192.168.0.122#53

_ldap._tcp.test.alt     service = 0 100 389 dc2.test.alt.
_ldap._tcp.test.alt     service = 0 100 389 dc1.test.alt.
> exit
```

или:

```
$ host -t SRV _ldap._tcp.test.alt
_ldap._tcp.test.alt has SRV record 0 100 389 dc1.test.alt.
_ldap._tcp.test.alt has SRV record 0 100 389 dc2.test.alt.
```

4.3. Ввод клиентских машин в Active Directory

4.3.1. Параметры команды system-auth

Для ввода клиентских машин в домен Active Directory, в дистрибутивах Альт используется команда **system-auth**:

```
# system-auth <Действие> <Опции>
```

В таблице Опции команды system-auth приведено описание опций этой команды.

Таблица 4.2. Опции команды system-auth

Параметр	Описание
Действие	
status	Показать текущую схему аутентификацию
list	Вывести список доступных схем аутентификации
write	Установить заданные параметры аутентификации
Опция	
-d	Включить отладку
--winbind	

Параметр	Описание
	Использовать Samba Winbind для подключения системы к AD (если этот параметр не указан, будет использован SSSD)
--gpo	Включить групповые политики на машине
--createcomputer=OU/SubOU	Субконтейнер в AD (организационная единица/подразделение), куда будет помещена машина при вводе в домен
--windows2003	Ввести станцию в домен windows 2003
--version	Вывести версию программы

Примеры использования:

- Вывести текущую схему аутентификации:

```
# system-auth status
ad TEST.ALT HOST-01 TEST
```

- Использовать локальную аутентификацию:

```
# system-auth write local
```

- Использовать аутентификацию AD (по умолчанию используется билет Kerberos):

```
# system-auth write ad <Домен> <Имя компьютера> <Рабочая группа> <Имя
пользователя> [<Пароль>] [--windows2003] [--createcomputer="COMPUTEROU/
SubCOMPUTEROU/SubSubCOMPUTEROU"] [--winbind] [--gpo]
```

4.3.2. Подключение к AD с помощью SSSD

В этом разделе описывается использование демона служб безопасности системы (SSSD) для подключения системы к Active Directory (AD).

SSSD используется для доступа к пользовательскому каталогу для аутентификации и авторизации через общую структуру с кэшированием пользователей, чтобы разрешить автономный вход в систему. SSSD легко настраивается; он обеспечивает интеграцию подключаемых модулей аутентификации (PAM) и службы переключения имен (NSS), базу данных для хранения локальных пользователей, а также расширенных пользовательских данных, полученных с центрального сервера.

Дополнительные ресурсы:

- **man realm**
- **man sssd-ad**
- **man sssd**

4.3.2.1. Ввод в домен в командной строке

Для ввода компьютера в домен необходимо выполнить команду:

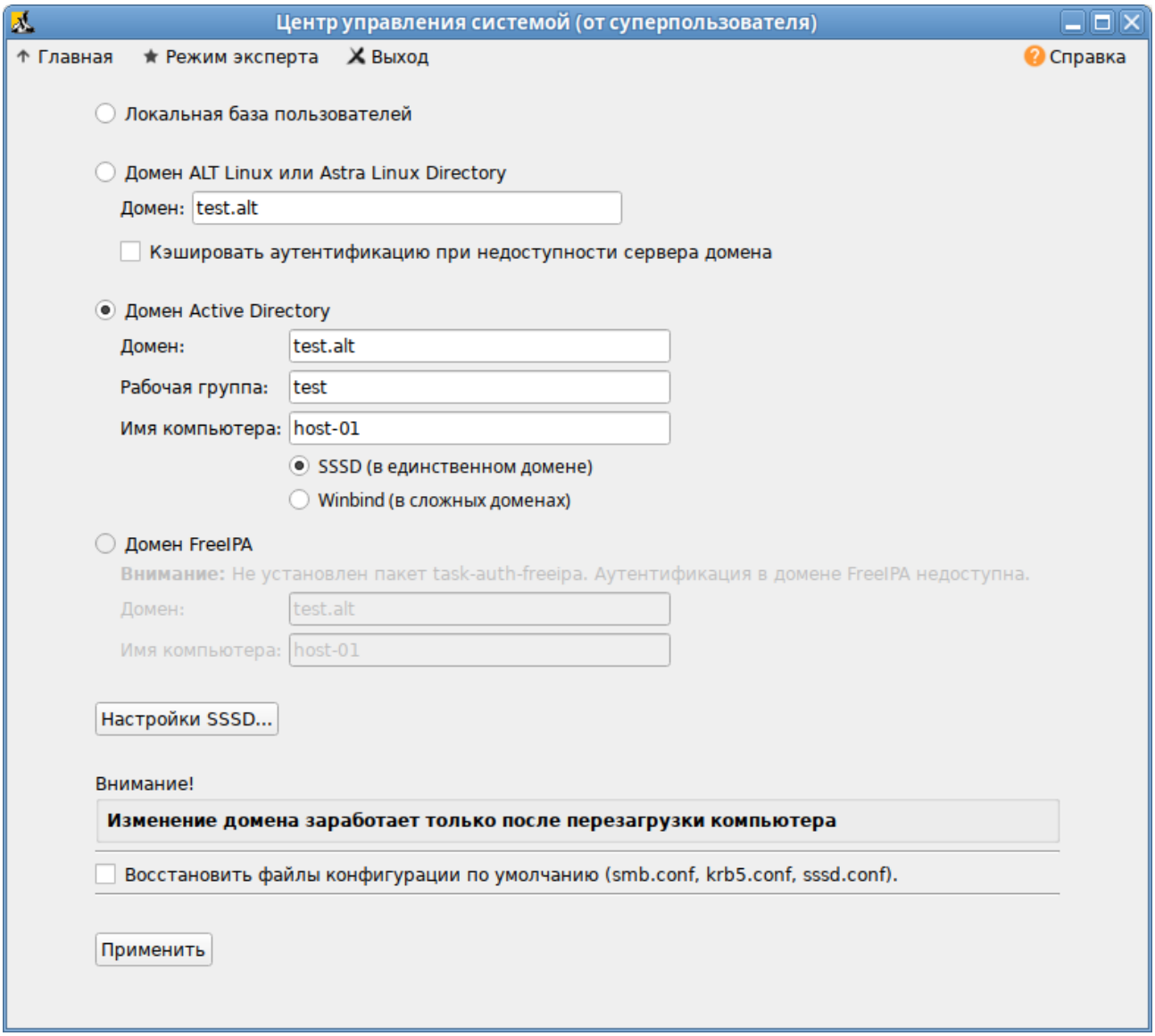
```
# system-auth write ad test.alt host-01 test 'administrator' 'Pa$$word'
Joined 'HOST-01' to dns domain 'test.alt'
```

Перезагрузить рабочую станцию.

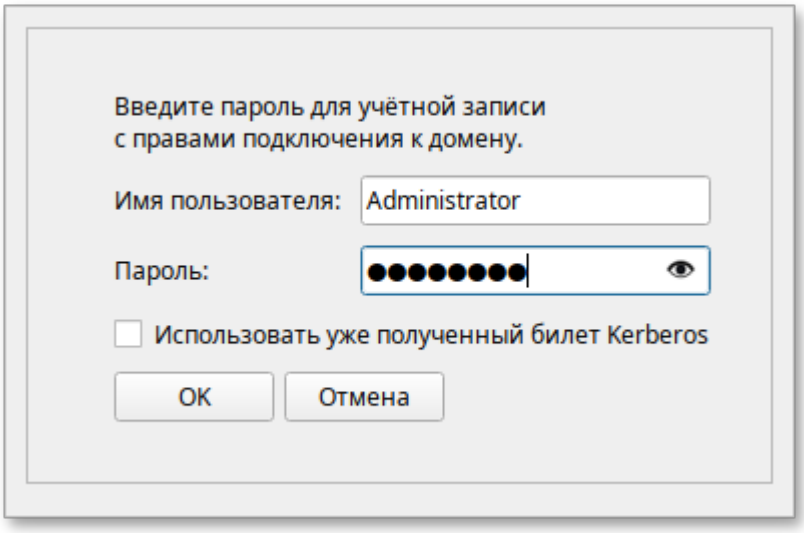
4.3.2.2. Ввод в домен в Центре управления системой

Для ввода компьютера в домен в Центре управления системой необходимо выбрать пункт **Пользователи** → **Аутентификация**.

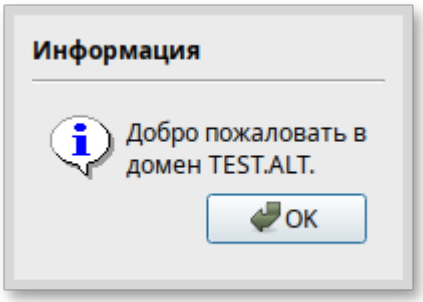
В окне модуля **Аутентификация** следует выбрать пункт **`Домен Active Directory`**, заполнить поля (**`Домен`**, **`Рабочая группа`**, **`Имя компьютера`**), выбрать пункт **`SSSD (в единственном домене)`** и нажать кнопку **`Применить`**:



В открывшемся окне необходимо ввести имя пользователя, имеющего право вводить машины в домен, и его пароль и нажать кнопку **`OK`**:



При успешном подключении к домену, отобразится соответствующая информация:



Перезагрузить рабочую станцию.

4.3.2.3. Проверка клиента

Отображение сведений о пользователе AD (ivanov — пользователь в домене):

```
# getent passwd ivanov
ivanov:*:1187401105:1187400513:Иван Иванов:/home/TEST.ALT/ivanov:/bin/bash

# net ads info
LDAP server: 192.168.0.122
LDAP server name: dc1.test.alt
Realm: TEST.ALT
Bind Path: dc=TEST,dc=ALT
LDAP port: 389
Server time: Ср, 27 мар 2024 10:36:51 EET
KDC server: 192.168.0.122
Server time offset: 2
Last machine account password change: Ср, 20 мар 2024 11:13:27 EET

# net ads testjoin
Join is OK
```

Примечание

Список пользователей можно посмотреть на сервере командой:

```
# samba-tool user list
```

Примечание

О настройке SSSD см. Настройка SSSD и Настройки SSSD в ЦУС.

4.3.3. Подключение к AD с помощью Samba Winbind

В этом разделе описывается использование Samba Winbind для подключения системы к Active Directory (AD).

Samba Winbind эмулирует клиент Windows в системе Linux и взаимодействует с серверами AD.

Дополнительные ресурсы:

- **man realm**
- **man winbindd**

4.3.3.1. Ввод в домен в командной строке

Для ввода компьютера в домен необходимо выполнить команду:

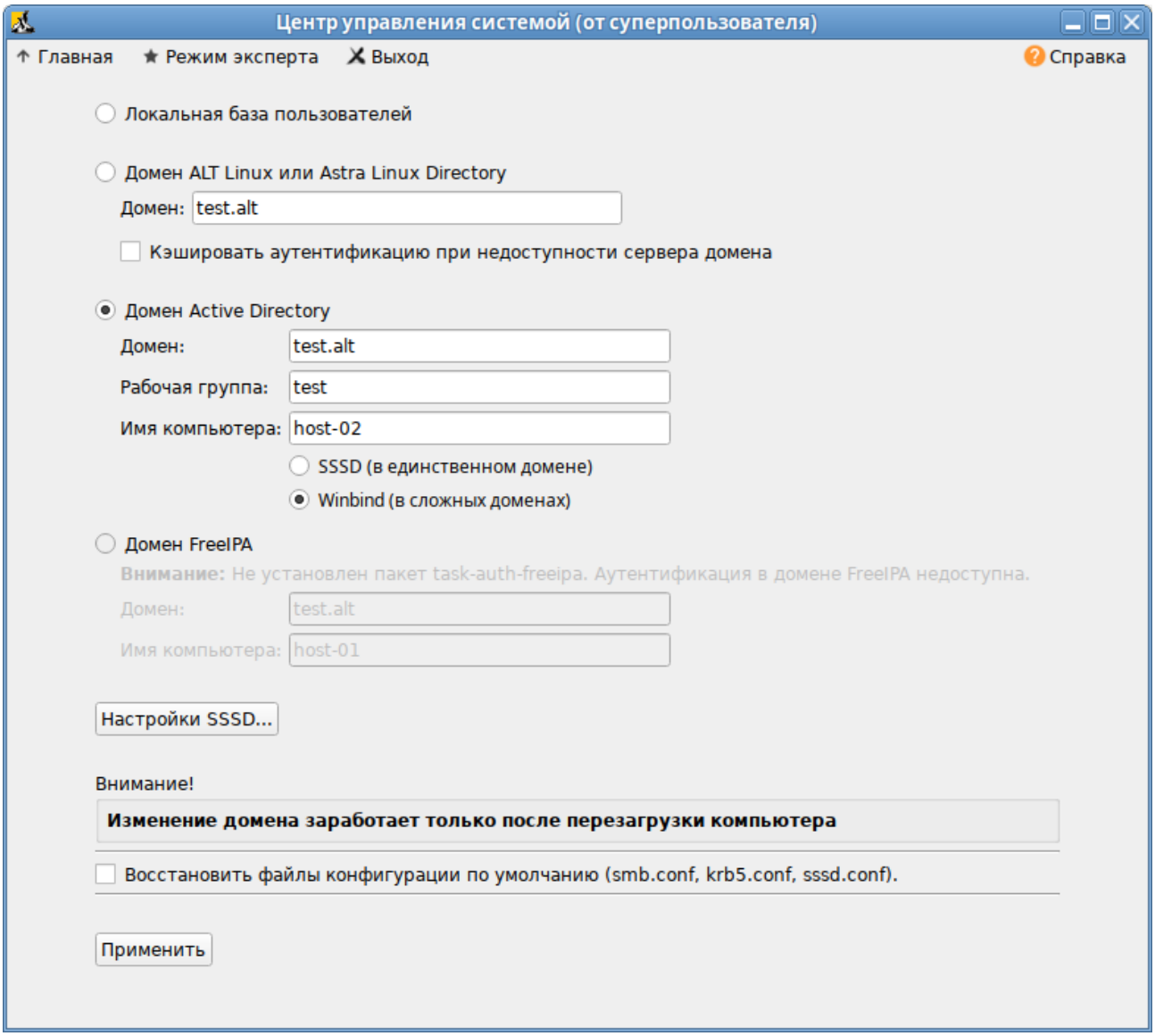
```
# system-auth write ad test.alt host-02 test 'administrator' 'Pa$$word' --winbind
Joined 'HOST-02' to dns domain 'test.alt'
```

Перезагрузить рабочую станцию.

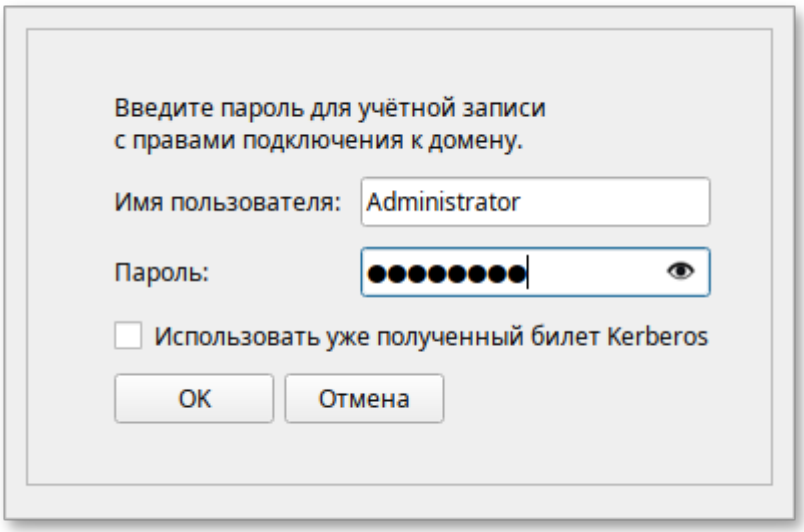
4.3.3.2. Ввод в домен в Центре управления системой

Для ввода компьютера в домен в **Центре управления системой** необходимо выбрать пункт **Пользователи** → **Аутентификация**.

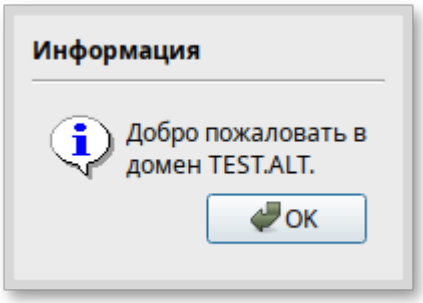
В окне модуля **Аутентификация** следует выбрать пункт **Домен Active Directory**, заполнить поля (**Домен**, **Рабочая группа**, **Имя компьютера**), выбрать пункт **Winbind (в сложных доменах)** и нажать кнопку **Применить**:



В открывшемся окне необходимо ввести имя пользователя, имеющего право вводить машины в домен, и его пароль и нажать кнопку **OK**:



При успешном подключении к домену, отобразится соответствующая информация:



Перезагрузить рабочую станцию.

4.3.3.3. Проверка клиента

Отображение сведений о пользователе AD (ivanov — пользователь в домене):

```
# getent passwd ivanov
ivanov:*:10000:10001::/home/TEST.ALT/ivanov:/bin/bash

# net ads info
LDAP server: 192.168.0.122
LDAP server name: dc1.test.alt
Realm: TEST.ALT
Bind Path: dc=TEST,dc=ALT
LDAP port: 389
Server time: Ср, 27 мар 2024 13:20:46 EET
KDC server: 192.168.0.122
Server time offset: 2
Last machine account password change: Ср, 20 мар 2024 12:36:35 EET

# net ads testjoin
Join is OK
```

Примечание

Список пользователей можно посмотреть на сервере командой:

```
# samba-tool user list
```

4.4. Отладочная информация

4.4.1. Настройка уровня журналирования Samba

Дополнительные сведения см. в разделе Уровни журналирования.

4.4.2. Ошибка при подключении к IP-адресу 127.0.0.1

Используя настройки по умолчанию, команда **net** подключается к IP-адресу 127.0.0.1. Если Samba не прослушивает петлевой интерфейс, соединение не устанавливается. Например:

```
# net rpc rights list -U administrator
Could not connect to server 127.0.0.1
Connection failed: NT_STATUS_CONNECTION_REFUSED
```

Чтобы решить эту проблему, необходимо настроить Samba для дополнительного прослушивания интерфейса loopback. Дополнительные сведения см. в разделе Настройка Samba для привязки к определённым интерфейсам.

Примечание

Чтобы временно обойти проблему, можно передать параметр ***-I <IP-адрес>*** или ***-S <Имя хоста>*** в команду **net**:

```
# net rpc rights list -U administrator -I 192.168.0.122
Password for [TEST\administrator]:
     SeMachineAccountPrivilege  Add machines to domain
      SeTakeOwnershipPrivilege  Take ownership of files or other objects
      …
```

4.4.3. getent не показывает доменных пользователей и группы

Используя команду **getent passwd** и **getent group** нельзя увидеть доменных пользователей и группы. Этот функционал отключен по умолчанию, для того чтобы сократить нагрузку на серверы. Поэтому для проверки необходимо указать точное имя пользователя:

```
# getent passwd <имя_пользователя>
```

Примечание

Список пользователей можно посмотреть на сервере командой:

```
# samba-tool user list
```

Если команда **getent passwd <имя_пользователя>** ничего не возвращает, следует попробовать выполнить команду:

```
# getent passwd <рабочая_группа>\<имя_пользователя>
```

Например:

```
# getent passwd "TEST\ivanov"
```

Если эта команда работает, а первая нет, то необходимо добавить следующую строку в файл **smb.conf**:

```
winbind use default domain = yes
```

4.4.4. Ошибки при присоединении к домену

4.5. Повторная регистрация клиента

В этом разделе рассмотрена процедура повторной регистрации клиента в AD с тем же именем хоста. Повторная регистрация может потребоваться, если клиентский компьютер был уничтожен и потерял связь с серверами AD, например, из-за аппаратного сбоя клиента.

4.6. Удаление клиента AD

Чтобы вывести систему из домена, можно воспользоваться командой **`realm leave`**. Эта команда удалит конфигурацию домена из SSSD и локальной системы:

```
# realm leave test.alt
```

По умолчанию удаление выполняется от имени администратора (для AD — administrator). Если для присоединения к домену использовалась учётная запись другого пользователя, может потребоваться выполнить удаление от имени этого пользователя. Чтобы указать пользователя следует использовать параметр **`-U`**:

```
# realm leave test.alt -U <пользователь>
```

Сначала команда пытается подключиться без использования учетных данных, но при необходимости запрашивает пароль.

Следует обратить внимание, что когда клиент удаляется из домена, учётная запись компьютера не удаляется из каталога; удаляется только конфигурация локального клиента. Если необходимо удалить учётную запись компьютера, следует запустить команду с параметром **`--remove`**:

```
# realm leave --remove test.alt
```

Для получения дополнительной информации см. справочную страницу **`man realm`** (8).

Примечание

После вывода из домена, схема аутентификации пользователей в системе должна переключиться на локальную базу:

```
# control system-auth
local
```

Примечание

Для того чтобы в окне входа отображался список доступных пользователей, необходимо в файле **`/etc/lightdm/lightdm.conf`** закомментировать строку в группе ***`[SeatDefaults]`***:

```
#greeter-hide-users=true
```

4.7. Настройка аутентификации доменных пользователей на DC

Важно

На текущий момент (*samba 4.19.4*, *gpupdate 0.9.13.8*) данный метод не позволяет применять групповые политики на контроллере домена.

Важно

На текущий момент (*samba 4.19.4*, *sssd 2.9.4*) для каталога **`/var/lib/samba/sysvol`** SID'ы домена не корректно транслируются в UNIX user id и group id.

Контроллер домена в рамках доменной инфраструктуры является, в том числе, ещё одной машиной и имеет соответствующий машинный аккаунт. После применения настроек, описанных в этом разделе, машина с контроллером домена сможет выполнять, в том числе, и функции обычного члена домена, такие как:

- аутентификация доменными пользователями (в том числе по ssh);
- применение групповых политик;
- всё, что поддерживает обычная клиентская машина (в качестве клиента SSSD или Winbind).

Важно

В качестве клиента на контроллере домена рекомендуется использовать Winbind. Использование SSSD не желательно.

4.7.1. Winbind

4.7.1.1. Установка пакетов

На контроллере домена необходимо установить пакеты *task-auth-ad-winbind* и *gpupdate*:

```
# apt-get install task-auth-ad-winbind gpupdate
```

4.7.1.2. Изменение файлов конфигурации

4.7.1.2.1. Настройка Kerberos (krb5.conf)

В файле **`/etc/krb5.conf`** должны быть заданы следующие параметры:

- dns_lookup_realm = false

- default_realm = TEST.ALT

Пример файла **/etc/krb5.conf**:

```
[logging]

[libdefaults]
 dns_lookup_kdc = true
 dns_lookup_realm = false
 ticket_lifetime = 24h
 renew_lifetime = 7d
 forwardable = true
 rdns = false
 default_realm = TEST.ALT

[realms]

[domain_realm]
```

4.7.1.2.2. Настройка Samba (smb.conf)

В файле **/etc/samba/smb.conf** должны быть заданы следующие параметры:

- kerberos method = dedicated keytab
- dedicated keytab file = /etc/krb5.keytab

Значения остальных параметров в файле должно соответствовать аналогичному файлу на обычных клиентах домена.

Пример файла **/etc/samba/smb.conf**:

```
[global]
        dns forwarder = 8.8.8.8
        netbios name = DC1
        kerberos method = dedicated keytab
        dedicated keytab file = /etc/krb5.keytab
        realm = TEST.ALT
        server role = active directory domain controller
        workgroup = TEST
        idmap_ldb:use rfc2307 = yes

        template shell = /bin/bash
        template homedir = /home/TEST.ALT/%U

        wins support = no
        winbind use default domain = yes
        winbind enum users = no
        winbind enum groups = no
        winbind refresh tickets = yes
        winbind offline logon = yes

[sysvol]
        path = /var/lib/samba/sysvol
        read only = No
```

```
[netlogon]
        path = /var/lib/samba/sysvol/test.alt/scripts
        read only = No
```

4.7.1.2.3. Настройка NSS (nsswitch.conf)

В файле **`/etc/nsswitch.conf`** должны быть заданы следующие параметры:

- passwd: files winbind systemd
- shadow: tcb files winbind
- group: files [SUCCESS=merge] winbind role systemd

Пример файла **`/etc/nsswitch.conf`**:

```
passwd:     files winbind systemd
shadow:     tcb files winbind
group:      files [SUCCESS=merge] winbind role systemd
gshadow:    files

hosts:      files myhostname dns

ethers:     files
netmasks:   files
networks:   files
protocols:  files
rpc:        files
services:   files

automount:  files
aliases:    files
```

4.7.1.3. Настройка аутентификации

Необходимо переключить PAM-стек на использование для аутентификации winbind-модуля:

```
# control system-auth winbind
```

4.7.2. SSSD

4.7.2.1. Установка пакетов

На контроллере домена должны быть установлены пакеты *task-auth-ad-sssd* и *gpupdate*:

```
# apt-get install task-auth-ad-sssd gpupdate
```

4.7.2.2. Изменение файлов конфигурации

4.7.2.2.1. Настройка Kerberos (krb5.conf)

В файле **`/etc/krb5.conf`** должны быть заданы следующие параметры:

- includedir /etc/krb5.conf.d/

- dns_lookup_realm = false
- default_realm = TEST.ALT

Пример файла **/etc/krb5.conf**:

```
includedir /etc/krb5.conf.d/
[logging]

[libdefaults]
 dns_lookup_kdc = true
 dns_lookup_realm = false
 ticket_lifetime = 24h
 renew_lifetime = 7d
 forwardable = true
 rdns = false
 default_realm = TEST.ALT

[realms]

[domain_realm]
```

4.7.2.2.2. Настройка SSSD (sssd.conf)

В файле **/etc/sssd/sssd.conf** должны быть заданы следующие параметры:

- user = root
- ad_maximum_machine_account_password_age = 0

Значения остальных параметров в файле должно соответствовать аналогичному файлу на обычных клиентах домена.

Пример файла **/etc/sssd/sssd.conf**:

```
[sssd]
config_file_version = 2
services = nss, pam

# Managed by system facility command:
## control sssd-drop-privileges unprivileged|privileged|default
user = root

# SSSD will not start if you do not configure any domains.
domains = TEST.ALT
[nss]

[pam]
[domain/TEST.ALT]
id_provider = ad
auth_provider = ad
chpass_provider = ad
access_provider = ad
default_shell = /bin/bash
fallback_homedir = /home/%d/%u
debug_level = 0
; cache_credentials = false
```

```
ad_gpo_ignore_unreadable = true
ad_gpo_access_control = permissive
ad_update_samba_machine_account_password = true
ad_maximum_machine_account_password_age = 0
```

4.7.2.2.3. Настройка Samba (smb.conf)

В файле **`/etc/samba/smb.conf`** должны быть заданы следующие параметры:

- idmap config * : range = 200000-2000200000
- idmap config * : backend = sss

Значения остальных параметров в файле должно соответствовать аналогичному файлу на обычных клиентах домена.

Пример файла **`/etc/samba/smb.conf`**:

```
[global]
        dns forwarder = 8.8.8.8
        netbios name = DC1
        realm = TEST.ALT
        server role = active directory domain controller
        workgroup = TEST
        idmap_ldb:use rfc2307 = yes

        template shell = /bin/bash
        template homedir = /home/TEST.ALT/%U

        kerberos method = system keytab
        wins support = no
        winbind use default domain = yes
        winbind enum users = no
        winbind enum groups = no
        winbind refresh tickets = yes
        winbind offline logon = yes

        idmap config * : range = 200000-2000200000
        idmap config * : backend = sss

[sysvol]
        path = /var/lib/samba/sysvol
        read only = No

[netlogon]
        path = /var/lib/samba/sysvol/test.alt/scripts
        read only = No
```

4.7.2.2.4. Настройка NSS (nsswitch.conf)

В файле **`/etc/nsswitch.conf`** должны быть заданы следующие параметры:

- passwd: files sss systemd
- shadow: tcb files sss
- group: files [SUCCESS=merge] sss role systemd

Пример файла **/etc/nsswitch.conf**:

```
passwd:     files sss systemd
shadow:     tcb files sss
group:      files [SUCCESS=merge] sss role systemd
gshadow:    files

hosts:      files myhostname dns

ethers:     files
netmasks:   files
networks:   files
protocols:  files
rpc:        files
services:   files

automount:  files
aliases:    files
```

4.7.2.3. Настройка аутентификации

Необходимо переключить PAM-стек на использование для аутентификации sss-модулей:

```
# control system-auth sss
```

4.7.3. Генерация keytab-файла

Необходимо сгенерировать системный keytab-файл для машинного аккаунта контроллера домена. Для этого следует выполнить следующую команду:

```
# net ads keytab create
```

4.7.4. Службы

Необходимо отключить сервис **nscd**:

```
# systemctl disable --now nscd
```

Если используется схема с SSSD клиентом, необходимо запустить и включить автоматический запуск для службы **sssd**:

```
# systemctl enable --now sssd
```

4.7.5. Настройка ролей

Необходимо указать, какие локальные роли каким группам домена соответствуют:

- обычные пользователи домена (Domain Users) соответствуют локальной роли *users*:

  ```
  # roleadd 'domain users' users
  ```

- администраторы домена (Domain Admins) соответствуют локальной роли *localadmins*:

```
# roleadd 'domain admins' localadmins
```

Важно

В русскоязычных версиях MS Windows Server встроенные группы *Domain Users* и *Domain Admins* имеют русифицированные названия *Пользователи домена* и *Администраторы домена*.

4.7.6. Групповые политики

Для включения поддержки групповых политик необходимо выполнить:

```
# gpupdate-setup enable --local-policy ad-domain-controller
```

Важно

Работа групповых политик на контроллере домена с SSSD клиентом может быть не стабильной.

4.7.7. Настройка SSH

Разрешить удалённый доступ по ssh только *Администраторам домена*:

```
# control sshd-allow-groups enabled
# control sshd-allow-groups-list remote
```

При необходимости можно разрешить аутентификацию по Kerberos билетам:

```
# control sshd-gssapi-auth enabled
```

Для применения настроек необходимо перезапустить сервис **sshd**:

```
# systemctl restart sshd
```

Примечание

Данные настройки можно применить с помощью механизма групповых политик control. Подробнее см. Групповые политики control.

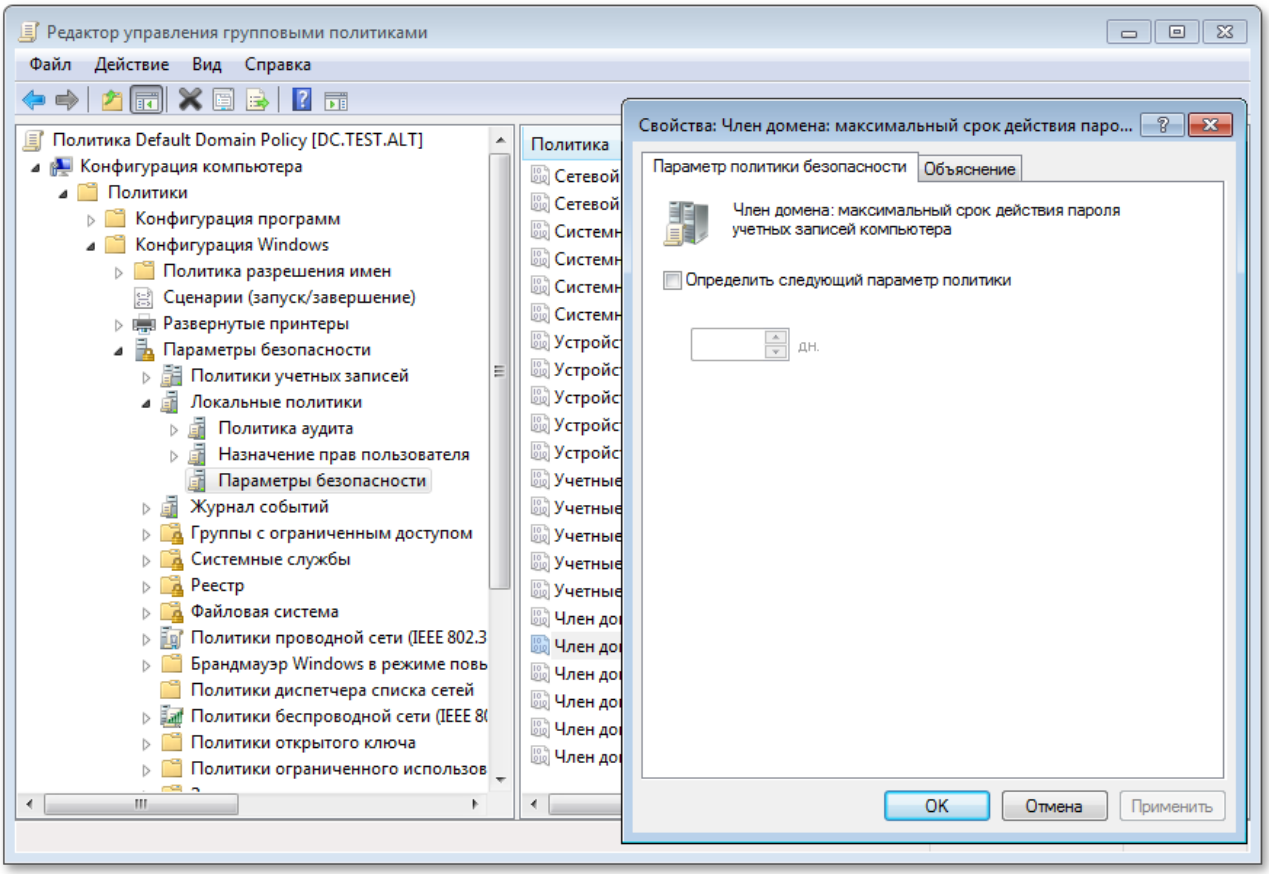
4.8. Настройка обновления паролей аккаунтов машин

После завершения процедуры ввода в домен каждая машина получает специальный аккаунт вида MACHINE01$. Такой аккаунт, ассоциированный с машиной, а не с конкретным пользователем, позволяет машине выполнять в домене действия от своего имени. Например, запрашивать информацию о пользователях, получать машинные групповые политики и т. д.

Как и у любого другого пользователя, у машинного пользователя есть свой пароль, генерируемый автоматически в процессе ввода машины в домен. В отличии от обычных пользователей, у машинных аккаунтов нет ограничения на время жизни пароля, но машина имеет возможность поменять его самостоятельно. По умолчанию машины с MS Windows 2000 и старше меняют пароль раз в 30 дней. Информация о последней смене пароля хранится в атрибуте машинного аккаунта **`pwdlastset`**.

4.8.1. Локальная политика смены пароля

Сменой пароля пароля учётной записи компьютера можно управлять с помощью групповых политик. Для этого нужно отредактировать параметр политики домена по умолчанию (**`Default domain policy`**) **`Член домена: максимальный срок действия пароля учётной записи компьютера`**, который располагается в подразделе **Конфигурация компьютера** → **Политики** → **Конфигурация Windows** → **Параметры безопасности** → **Локальные политики** → **Параметры безопасности** (**Computer Configuration** → **Policies** → **Windows Settings** → **Security Settings** → **Local Policies** → **Security Options**).



Примечание

На данный момент в ADMC (*admc 0.11.2*), нет возможности настроить данные параметры групповой политики. Необходимо использовать оснастку RSAT «Управление групповыми политиками» (см. Установка RSAT).

Этот параметр безопасности определяет, как часто член домена будет пытаться изменить пароль учётной записи компьютера. Значение по умолчанию: 30 дней.

С помощью параметра **`Член домена: отключить изменение пароля учётных записей компьютера`** можно отключить обновления пароля машинного аккаунта совсем, но делать этого не рекомендуется.

Важно

Выше указанные параметры корректно работают на машинах с ОС MS Windows 2000 и старше.

Важно

На машинах с ОС Альт (*sssd 2.8.1*) данные параметры игнорируются.

4.8.2. Включение обновления пароля

4.8.2.1. ОС Windows

Для включения периодического обновления пароля учётной записи компьютера на машинах под управлением ОС Windows 2000 и старше дополнительных действий не требуется. Периодичность обновления настраивается с помощью соответствующей групповой политики.

4.8.2.2. ОС Альт

За обновление пароля машинного аккаунта на машинах под управлением ОС Альт отвечают сервисы **`sssd`** и **`winbind`**.

4.8.2.2.1. Winbind

Winbind, на текущий момент (*samba-winbind 4.19.4*), не умеет после смены пароля учётной записи компьютера обновлять системный keytab-файл (**`/etc/krb5.keytab`**). Поэтому, во избежание конфликтов с sssd, следует отключить этот функционал.

Для отключения периодического обновления пароля учётной записи компьютера необходимо в файл **`/etc/samba/smb.conf`** в секцию ***`[global]`*** добавить параметр ***`machine password timeout = 0`***:

```
[global]
machine password timeout = 0
```

4.8.2.2.2. SSSD

`sssd` для обновления пароля учётной записи компьютера использует утилиту **`adcli`**. Необходимо убедиться, что пакет *adcli* установлен в системе:

```
# apt-get install adcli
```

Периодичностью обновления пароля учётной записи компьютера можно управлять с помощью параметра ***`ad_maximum_machine_account_password_age`*** (секция ***`[domain/<Домен>]`***) в **`/etc/sssd/sssd.conf`**. Значение по умолчанию: 30 дней.

Для корректного функционирования обновления пароля учётной записи компьютера **sssd** необходим доступ на запись в файл **/etc/krb5.keytab**. Для этого не достаточно привилегий пользователя _sssd, от которого обычно и запускается **sssd**. Необходимо запускать **sssd** с правами суперпользователя. Для этого следует в файле **/etc/sssd/sssd.conf** в секции ***[sssd]*** изменить значение параметра ***user*** на root:

```
[sssd]
user = root

[domain/<Домен>]
ad_update_samba_machine_account_password = true
```

Важно

При вводе компьютера в домен с помощью ЦУС следующие параметры прописываются в конфигурационные файлы по умолчанию:

- **/etc/samba/smb.conf**:

  ```
  machine password timeout = 0
  ```

- **/etc/sssd/sssd.conf**:

  ```
  ad_update_samba_machine_account_password = true
  ```

4.8.3. Отключение обновления пароля

4.8.3.1. ОС Windows

Для отключения периодического обновления пароля учётной записи компьютера на машинах под управлением ОС Windows 2000 и старше достаточно включить параметр групповой политики **Default domain policy Член домена: отключить изменение пароля учётных записей компьютера**.

4.8.3.2. ОС Альт

Для отключения периодического обновления пароля учётной записи компьютера на машинах под управлением ОС Альт необходимо:

- в файле **/etc/sssd/sssd.conf** (секция ***[domain/<Домен>]***) значение параметра ***ad_maximum_machine_account_password_age*** установить равным 0:

  ```
  [domain/<Домен>]
  ad_maximum_machine_account_password_age = 0
  ```

- в файле **/etc/samba/smb.conf** (секция ***[global]***) значение параметра ***machine password timeout*** установить равным 0:

  ```
  [global]
  machine password timeout = 0
  ```

4.8.4. Диагностика

4.8.4.1. Дата последней смены пароля

Дата последней смены пароля учётной записи компьютера хранится в базе данных AD. Запросить её можно одним из следующих способов:

- на введённой в домен машине выполнить команду:

```
# net ads info
…
Last machine account password change: Ср, 20 мар 2024 12:36:35 EET
```

- если машина уже потеряла доверие в домене, то выполнить эту же команду от доменного пользователя:

```
# net ads info -U <user>
```

Дата последней смены пароля учётной записи компьютера будет показана в параметре ***Last machine account password change***.

4.8.4.2. Потеря доверия между машиной и доменом

Для проверки того, имеет ли машина возможность аутентифицироваться в домене можно выполнить следующие действия:

- убедиться, что файл keytab (**/etc/krb5.keytab**) содержит корректную информацию:

```
# klist -ke
Keytab name: FILE:/etc/krb5.keytab
KVNO Principal
----
---------------------------------------------------------------------------
   1 host/work.test.alt@TEST.ALT (aes256-cts-hmac-sha1-96)
   1 host/WORK@TEST.ALT (aes256-cts-hmac-sha1-96)
   1 host/work.test.alt@TEST.ALT (aes128-cts-hmac-sha1-96)
   1 host/WORK@TEST.ALT (aes128-cts-hmac-sha1-96)
   1 host/work.test.alt@TEST.ALT (DEPRECATED:arcfour-hmac)
   1 host/WORK@TEST.ALT (DEPRECATED:arcfour-hmac)
   1 restrictedkrbhost/work.test.alt@TEST.ALT (aes256-cts-hmac-sha1-96)
   1 restrictedkrbhost/WORK@TEST.ALT (aes256-cts-hmac-sha1-96)
   1 restrictedkrbhost/work.test.alt@TEST.ALT (aes128-cts-hmac-sha1-96)
   1 restrictedkrbhost/WORK@TEST.ALT (aes128-cts-hmac-sha1-96)
   1 restrictedkrbhost/work.test.alt@TEST.ALT (DEPRECATED:arcfour-hmac)
   1 restrictedkrbhost/WORK@TEST.ALT (DEPRECATED:arcfour-hmac)
   1 WORK$@TEST.ALT (aes256-cts-hmac-sha1-96)
   1 WORK$@TEST.ALT (aes128-cts-hmac-sha1-96)
   1 WORK$@TEST.ALT (DEPRECATED:arcfour-hmac)
```

- попытаться получить билет Kerberos для учётной записи компьютера (в примере WORK$), используя файл keytab **/etc/krb5.keytab**:

```
# kinit -k WORK\$@TEST.ALT
```

- убедиться, что билет успешно получен и удалить его:

```
# klist
Ticket cache: KEYRING:persistent:0:0
Default principal: WORK$@TEST.ALT

Valid starting       Expires              Service principal
21.04.2023 12:25:37  21.04.2023 22:25:37  krbtgt/TEST.ALT@TEST.ALT
    renew until 28.04.2023 12:25:37

# kdestroy -p WORK\$@TEST.ALT
```

Важно

Следует убедиться, что имя машины в keytab-файле (**/etc/krb5.keytab**) соответствует реальному имени машины (см. вывод команды **hostnamectl**).

4.8.5. Восстановление работоспособности

Если диагностика показала, что машина потеряла доверие с доменом, то, для восстановления работоспособности, необходимо выполнить следующие действия:

- обновить систему:

```
# apt-get update && apt-get dist-upgrade
```

- удалить файл **/etc/krb5.keytab**;
- повторно ввести машину в домен используя ЦУС;
- убедиться, что конфигурационные файлы соответствуют одному из сценариев: Включение обновления пароля или Отключение обновления пароля;
- перезагрузить машину.

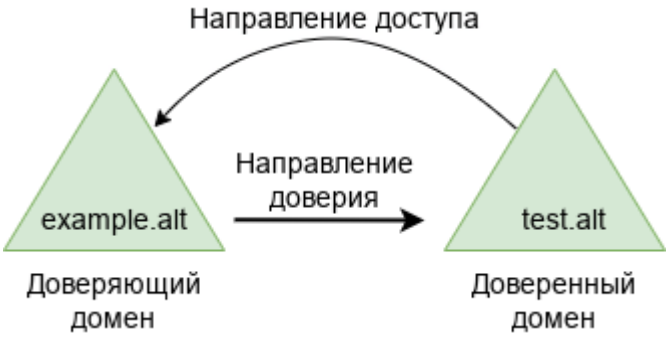
Глава 5. Доверительные отношения (Трасты)

Доверительные отношения (trusts) позволяют аутентифицироваться под пользователями не только текущего домена, но и доверенных.

5.1. Настройка доверия

5.1.1. Общие сведения

Доверительные отношения реализуются в рамках механизма аутентификации. Суть доверительных отношений между двумя доменами сводится к тому, что доверяющий домен (trusting domain) доверяет процесс аутентификации доверенному домену (trusted domain). Пользователь, аутентифицированный доверенным доменом, может получить доступ к ресурсам в доверяющем домене.



Отношения доверия обеспечивают доступ к ресурсам в одном или двух направлениях:

- одностороннее доверие — позволяет пользователям и группам из домена А получать доступ к ресурсам в домене Б, но не наоборот. Домен А доверяет домену Б, но домен Б не доверяет домену А. При создании такого доверия нужно указать направление (входящее или исходящее);
- двустороннее доверие — позволяет пользователям и группам из домена А получать доступ к ресурсам в домене Б и наоборот. Запросы проверки подлинности могут передаваться между двумя доменами в обоих направлениях. Домен А доверяет домену Б, а домен Б доверяет домену А.

Транзитивность определяет, можно ли расширить доверие за пределы двух доменов, для которых оно сформировано:

- транзитивное доверие можно использовать для расширения отношений доверия на другие домены;
- нетранзитивное доверие можно использовать для запрета отношений доверия с другими доменами.

Типы доверия:

- доверие леса (Forest) — связывает леса и все их домены (это двухсторонние или односторонние отношения доверия между разными лесами, всегда являющиеся транзитивными);
- внешнее доверие (External) — устанавливается между двумя доменами напрямую вне леса (для установки двухстороннего доверия нужно использовать два разнонаправленных доверия, которыми надо связать все требуемые пары доменов).

5.1.2. Особенности доверительных отношений в Samba

Поддерживается:

- доверие леса (это доверие может быть установленным между двумя Samba-доменами или Samba-доменом и Windows-доменом);
- внешние доверительные отношения между доменом AD и доменом в стиле NT;
- добавление пользователей и групп доверенного домена в группы доверяющего домена (при этом необходимо использовать SID пользователей и групп, имя пользователя или имя группы использовать невозможно);
- в RSAT можно увидеть ***foreignSecurityPrincipal*** для всех добавленных пользователей и групп из доверенного домена.

Особенности и ограничения:

- не применяются правила фильтрации SID;
- нельзя добавить пользователей и группы доверенного домена в доменные группы доверяющего домена по имени;
- для входа в доверенный домен через SSSD надо использовать тип связи **External**, а не **Forest**;
- обе стороны траста должны полностью доверять друг другу (администратор из домена А может управлять всеми объектами в домене Б и наоборот);
- не поддерживается выборочная аутентификация;
- нельзя создать доверительные отношения между доменами в одном дереве с одним и тем же пространством имён верхнего уровня. NetBIOS имена доменов должны отличаться (домен MYDOMAIN.WIN и MYDOMAIN.NEW будут иметь одинаковое короткое имя — MYDOMAIN, это приведет к невозможности установки доверительных отношений).

Для управления доверием можно использовать инструмент командной строки **samba-tool**.

Таблица 5.1. Команды управления доверием

Команда	Описание	Примечание
domain trust create <домен>	Создать доверие домена или леса	Можно использовать следующие опции: - ***--type=TYPE*** — тип доверия (**external**, **forest**; - ***--direction=DIRECTION*** — направление доверия (**incoming**, **outgoing**, **both**);

Команда	Описание	Примечание
		--create-location=LOCATION — где создать объект доверенного домена (**local**, **both**; ***--quarantined=yes|no*** — применять к доверию специальные правила фильтрации SID (если ***--type=external*** по умолчанию **yes**, если ***--type=forest*** по умолчанию **no**); ***-U USERNAME*** — имя пользователя.
domain trust modify <домен>	Изменить доверие домена или леса	
domain trust delete <домен>	Удалить доверие домена или леса	Можно использовать следующие опции: ***--delete-location=LOCATION*** — где удалить объект доверенного домена (**local**, **both**; ***-U USERNAME*** — имя пользователя.
domain trust list	Вывести список доверительных отношений домена	
domain trust show <домен>	Показать сведения о доверенном домене	
domain trust validate <домен>	Проверить доверие к домену	Можно использовать следующие опции: ***--validate-location=LOCATION*** — где проверить объект доверенного домена (**local**, **both**; ***-U USERNAME*** — имя пользователя.

5.2. Настройка DNS

Перед настройкой доверия необходимо убедиться, что серверы видят друг друга и правильно разрешают доменные имена.

5.2.1. Два домена Samba

Таблица 5.2. Исходные данные

Имя домена	Контроллер домена	IP-адрес	ОС контроллера домена	Версия Samba
TEST.ALT	dc1.test.alt	**192.168.0.122**	ALT Server 10.2	4.19.4
EXAMPLE.ALT	s1.example.alt	**192.168.0.172**	ALT Server 10.2	4.19.4

5.2.1.1. Настройка переадресации DNS на DC с BIND9_DLZ

Если используется dns_backend BIND9_DLZ, добавить информацию о зоне в конец файла **/etc/bind/options.conf**.

- на контроллере домена dc1.test.alt добавить строки:

```
zone "example.alt" {
      type forward;
      forwarders { 192.168.0.172; };
};
```

- на контроллере домена s1.example.alt:

```
zone "test.alt" {
      type forward;
      forwarders { 192.168.0.122; };
};
```

Перезапустить службу DNS:

```
# systemctl restart bind.service
```

Примечание

Если удалённый DNS-сервер не использует DNSSEC и включить проверку DNSSEC на удаленном DNS-сервере нельзя, можно отключить проверку DNSSEC на сервере AD. Для этого необходимо в файл **/etc/bind/options.conf** в секцию ***options*** добавить параметр:

```
dnssec-validation no;
```

И перезапустить службу DNS:

```
# systemctl restart bind.service
```

5.2.1.2. Настройка переадресации DNS на DC с SAMBA_INTERNAL

Если используется DC с dns_backend SAMBA_INTERNAL, самый простой способ заставить работать разрешение имен — настроить DNS-прокси между двумя доменами. DNS-прокси будет перенаправлять запрос между доменами и внешним DNS-серверами. В примере, в качестве DNS-прокси используется отдельный сервер (IP-адрес 192.168.0.150) с настроенным bind9.

На каждом контроллере домена:

1. Указать DNS-прокси, как сервер пересылки в файле **`/etc/samba/smb.conf`** (в параметре ***`dns forwarder`***). Например:

   ```
   dns forwarder = 192.168.0.150 8.8.8.8
   ```

2. Перезапустить службу samba:

   ```
   # systemctl restart samba
   ```

На сервере bind9 отредактировать файл **`/etc/bind/options.conf`**:

- отключить проверку DNSSEC, для этого в секцию ***`options`*** добавить параметр:

  ```
  dnssec-validation no;
  ```

- в конец файла добавить информацию о зонах:

  ```
  zone "example.alt" {
        type forward;
        forwarders { 192.168.0.172; };
  };

  zone "test.alt" {
        type forward;
        forwarders { 192.168.0.122; };
  };
  ```

И перезапустить службу DNS:

```
# systemctl restart bind.service
```

5.2.1.3. Проверка конфигурации DNS

Для проверки настройки следует убедиться, что на обоих контроллерах домена разрешаются SRV-записи:

- на контроллере домена dc1.test.alt:

  ```
  # host -t srv _kerberos._tcp.example.alt
  _kerberos._tcp.example.alt has SRV record 0 100 88 s1.example.alt.
  # host -t srv _kerberos._tcp.test.alt
  _kerberos._tcp.test.alt has SRV record 0 100 88 dc1.test.alt.
  ```

- на контроллере домена s1.example.alt:

```
# host -t srv _kerberos._tcp.example.alt
_kerberos._tcp.example.alt has SRV record 0 100 88 s1.example.alt.
# host -t srv _kerberos._tcp.test.alt
_kerberos._tcp.test.alt has SRV record 0 100 88 dc1.test.alt.
```

Проверить возможность получения билета Kerberos:

- на контроллере домена dc1.test.alt:

```
# kinit administrator@EXAMPLE.ALT
Password for administrator@EXAMPLE.ALT:
# klist
Ticket cache: KEYRING:persistent:0:krb_ccache_eFyZ8Tr
Default principal: administrator@EXAMPLE.ALT

Valid starting       Expires              Service principal
27.03.2024 14:14:36  28.03.2024 00:14:36  krbtgt/TEST.ALT@TEST.ALT
        renew until 28.03.2024 14:14:32
```

- на контроллере домена s1.example.alt:

```
# kinit administrator@TEST.ALT
Password for administrator@TEST.ALT:
# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: administrator@TEST.ALT

Valid starting       Expires              Service principal
27.03.2024 15:17:50  28.03.2024 01:17:50  krbtgt/TEST.ALT@TEST.ALT
        renew until 28.03.2024 15:17:46
```

Важно

realm должен быть записан заглавными буквами.

5.2.2. Samba DC и Windows Server с AD

Таблица 5.3. Исходные данные

Имя домена	Контроллер домена	IP-адрес	ОС	Версия Samba
TEST.ALT	dc1.test.alt	**192.168.0.122**	ALT Server 10.2	4.19.4
WIN.ALT	DC1.win.alt	**192.168.0.190**	Windows Server 2012	

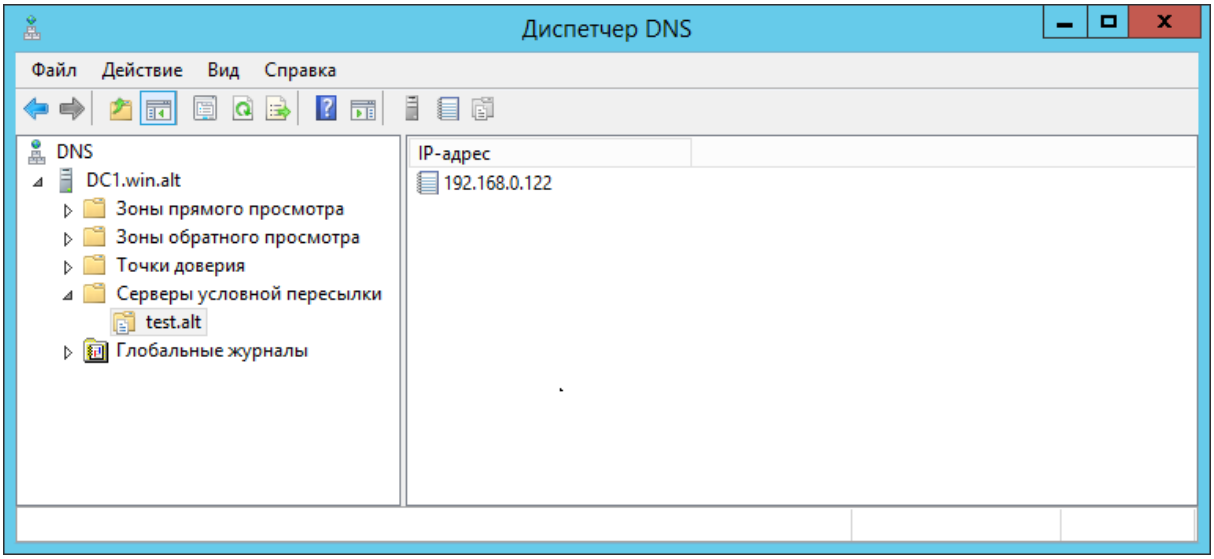
5.2.2.1. Windows Server с AD

На AD сервере создать сервер условной пересылки для зоны Samba домена.

В графическом интерфейсе:

1. Открыть **Диспетчер DNS** (**DNS Manager**).

2. В разделе **Серверы условной пересылки** (**Conditional Forwarders**) добавить новый сервер пересылки, указав FQDN или IP-адрес сервера Samba:



3. Сохранить настройки.

В командной строке:

```
C:\> dnscmd 127.0.0.1 /ZoneAdd test.alt /Forwarder 192.168.0.122
DNS Server 127.0.0.1 created zone test.alt:

Command completed successfully
```

Или выполнить следующую команду в сеансе PowerShell для настройки пересылки DNS:

```
PS C:\Windows\system32> Add-DnsServerConditionalForwarderZone -Name test.alt -
MasterServers 192.168.0.122 -ReplicationScope Forest
```

5.2.2.2. Samba DC с BIND9_DLZ

Если используется dns_backend BIND9_DLZ, добавить в конец файла **/etc/bind/options.conf** (или **/etc/bind/ddns.conf**) строки:

```
zone "win.alt" {
      type forward;
      forwarders { 192.168.0.190; };
};
```

И перезапустить службу DNS:

```
# systemctl restart bind.service
```

Примечание

Если удалённый DNS-сервер не использует DNSSEC и включить проверку DNSSEC на удаленном DNS-сервере нельзя, можно отключить проверку DNSSEC на сервере AD. Для этого необходимо в файл **/etc/bind/options.conf** в секцию ***options*** добавить параметр:

```
dnssec-validation no;
```

И перезапустить службу DNS:

```
# systemctl restart bind.service
```

5.2.2.3. Samba DC с SAMBA_INTERNAL

Если используется DC с dns_backend SAMBA_INTERNAL, самый простой способ заставить работать разрешение имен — настроить DNS-прокси между двумя доменами. DNS-прокси будет перенаправлять запрос между доменами и внешним DNS-серверами. В примере, в качестве DNS-прокси используется отдельный сервер (IP-адрес 192.168.0.150) с настроенным bind9.

На контроллере домена:

1. Указать DNS-прокси, как сервер пересылки в файле **`/etc/samba/smb.conf`** (в параметре ***`dns forwarder`***). Например:

   ```
   dns forwarder = 192.168.0.150 8.8.8.8
   ```

2. Перезапустить службу samba:

   ```
   # systemctl restart samba
   ```

На сервере bind9 отредактировать файл **`/etc/bind/options.conf`**:

- отключить проверку DNSSEC, для этого в секцию ***`options`*** добавить параметр:

  ```
  dnssec-validation no;
  ```

- в конец файла добавить информацию о зонах:

  ```
  zone "win.alt" {
        type forward;
        forwarders { 192.168.0.190; };
  };
  ```

И перезапустить службу DNS:

```
# systemctl restart bind.service
```

5.2.2.4. Проверка конфигурации DNS

Перед настройкой доверия необходимо убедиться, что серверы могут разрешать себя и друг друга.

На Samba DC:

1. Запись отвечающая за работу сервисов Kerberos через UDP и LDAP через TCP:

```
# dig +short -t SRV _kerberos._udp.test.alt
0 100 88 dc1.test.alt.
# dig +short -t SRV _ldap._tcp.test.alt
0 100 389 dc1.test.alt.
```

В выводе команд должен быть отображен список всех серверов.

2. Наличие записей для работы сервисов AD на DNS-сервере Samba:

```
# dig +short -t SRV _kerberos._tcp.dc._msdcs.win.alt
0 100 88 dc1.win.alt.
# dig +short -t SRV _ldap._tcp.dc._msdcs.win.alt
0 100 389 dc1.win.alt.
```

3. Проверить возможность получения билета Kerberos:

```
# kinit administrator@WIN.ALT
Password for administrator@WIN.ALT:
# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: administrator@WIN.ALT

Valid starting       Expires              Service principal
27.04.2023 17:42:28  28.04.2023 03:42:28  krbtgt/WIN.ALT@WIN.ALT
    renew until 28.04.2023 17:42:25
```

Проверить наличие записей DNS-сервере AD:

1. Запустить утилиту nslookup.exe для поиска служебных записей:

```
C:\> nslookup.exe
> set type=SRV
```

Ввести доменное имя для служебных записей Kerberos через UDP и LDAP через TCP:

```
> _kerberos._udp.test.alt
_kerberos._udp.test.alt       SRV service location:
    priority                = 0
    weight                  = 100
    port                    = 88
    svr hostname            = dc1.test.alt
…
test.alt
    primary name server = dc1.test.alt
    responsible mail addr = hostmaster.test.alt
    serial = 7
    refresh = 900 (15 mins)
    retry = 600 (10 mins)
    expire = 86400 (1 days)
    default TTL = 3600 (1 hours)
> _ldap._tcp.test.alt
_ldap._tcp.test.alt       SRV service location:
    priority                = 0
    weight                  = 100
    port                    = 389
    svr hostname            = dc1.test.alt
…
```

5.3. Создание двухстороннего транзитивного подключения

5.3.1. Два домена Samba

На контроллере домена dc1.test.alt:

```
# samba-tool domain trust create EXAMPLE.ALT --type=forest --direction=both --
create-location=both -U administrator@EXAMPLE.ALT
LocalDomain Netbios[TEST] DNS[test.alt]
SID[S-1-5-21-1455776928-3410124986-2843404052]
RemoteDC Netbios[S1] DNS[s1.example.alt]
ServerType[PDC,GC,LDAP,DS,KDC,TIMESERV,CLOSEST,WRITABLE,GOOD_TIMESERV,FULL_SECRET
_DOMAIN_6]
Password for [administrator@EXAMPLE.ALT]:
RemoteDomain Netbios[EXAMPLE] DNS[example.alt]
SID[S-1-5-21-3274802069-598906262-3677769431]
Creating remote TDO.
Remote TDO created.
Setting supported encryption types on remote TDO.
Creating local TDO.
Local TDO created
Setting supported encryption types on local TDO.
Setup local forest trust information...
Namespaces[2] TDO[example.alt]:
TLN: Status[Enabled]                  DNS[*.example.alt]
DOM: Status[Enabled]                  DNS[example.alt] Netbios[EXAMPLE]
SID[S-1-5-21-3274802069-598906262-3677769431]
Setup remote forest trust information...
Namespaces[2] TDO[test.alt]:
TLN: Status[Enabled]                  DNS[*.test.alt]
DOM: Status[Enabled]                  DNS[test.alt] Netbios[TEST]
SID[S-1-5-21-1455776928-3410124986-2843404052]
Validating outgoing trust...
OK: LocalValidation: DC[\\s1.example.alt] CONNECTION[WERR_OK] TRUST[WERR_OK]
VERIFY_STATUS_RETURNED
Validating incoming trust...
OK: RemoteValidation: DC[\\dc1.test.alt] CONNECTION[WERR_OK] TRUST[WERR_OK]
VERIFY_STATUS_RETURNED
Success
```

Важно

Для входа в доверенный домен через SSSD надо использовать тип связи **`external`**, а не **`forest`**.

Проверка доверия:

- Просмотр доверия с dc1.test.alt:

```
[root@dc1 ~]# samba-tool domain trust show EXAMPLE.ALT
LocalDomain Netbios[TEST] DNS[test.alt]
SID[S-1-5-21-1455776928-3410124986-2843404052]
TrustedDomain:

NetbiosName:    EXAMPLE
```

```
DnsName:        example.alt
SID:            S-1-5-21-3274802069-598906262-3677769431
Type:           0x2 (UPLEVEL)
Direction:      0x3 (BOTH)
Attributes:     0x8 (FOREST_TRANSITIVE)
PosixOffset:    0x00000000 (0)
kerb_EncTypes:  0x18 (AES128_CTS_HMAC_SHA1_96,AES256_CTS_HMAC_SHA1_96)
Namespaces[2] TDO[example.alt]:
TLN: Status[Enabled]                  DNS[*.example.alt]
DOM: Status[Enabled]                  DNS[example.alt] Netbios[EXAMPLE]
SID[S-1-5-21-3274802069-598906262-3677769431]
```

- Просмотр доверия с s1.example.alt:

```
[root@s1 ~]# samba-tool domain trust show TEST.ALT
LocalDomain Netbios[EXAMPLE] DNS[example.alt]
SID[S-1-5-21-3274802069-598906262-3677769431]
TrustedDomain:

NetbiosName:    TEST
DnsName:        test.alt
SID:            S-1-5-21-1455776928-3410124986-2843404052
Type:           0x2 (UPLEVEL)
Direction:      0x3 (BOTH)
Attributes:     0x8 (FOREST_TRANSITIVE)
PosixOffset:    0x00000000 (0)
kerb_EncTypes:  0x18 (AES128_CTS_HMAC_SHA1_96,AES256_CTS_HMAC_SHA1_96)
Namespaces[2] TDO[test.alt]:
TLN: Status[Enabled]                  DNS[*.test.alt]
DOM: Status[Enabled]                  DNS[test.alt] Netbios[TEST]
SID[S-1-5-21-1455776928-3410124986-2843404052]
```

- Список трастов:

```
[root@dc1 ~]# samba-tool domain trust list
Type[Forest]   Transitive[Yes] Direction[BOTH]     Name[example.alt]
```

В разных доменах могут быть разные результаты. Результат зависит от типа траста который установлен с этим доменом.

Если после настройки доверия возникли проблемы с доступом пользователей из трастового домен в свой домен, тогда следует проверить, действительно ли установлен траст:

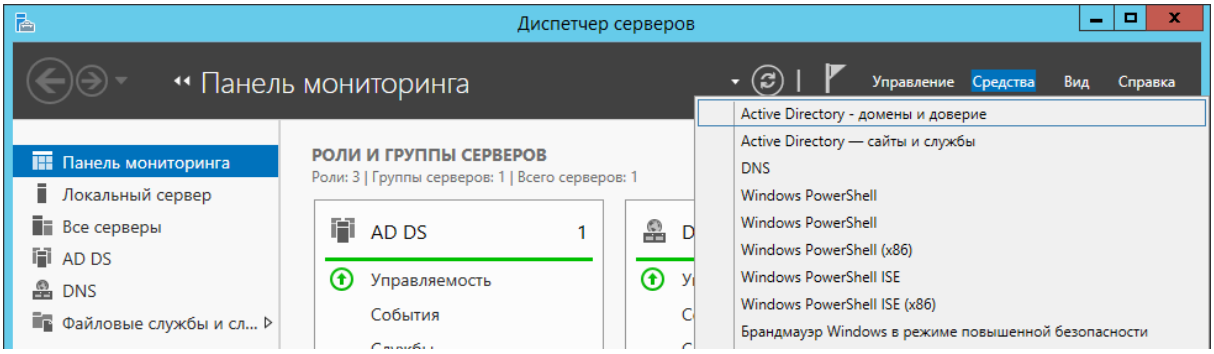
```
[root@dc1 ~]# samba-tool domain trust validate EXAMPLE.ALT -
Uadministrator@EXAMPLE.ALT
LocalDomain Netbios[TEST] DNS[test.alt]
SID[S-1-5-21-1455776928-3410124986-2843404052]
LocalTDO Netbios[EXAMPLE] DNS[example.alt]
SID[S-1-5-21-3274802069-598906262-3677769431]
OK: LocalValidation: DC[\\s1.example.alt] CONNECTION[WERR_OK] TRUST[WERR_OK]
VERIFY_STATUS_RETURNED
OK: LocalRediscover: DC[\\s1.example.alt] CONNECTION[WERR_OK]
RemoteDC Netbios[S1] DNS[s1.example.alt]
ServerType[PDC,GC,LDAP,DS,KDC,TIMESERV,CLOSEST,WRITABLE,GOOD_TIMESERV,FULL_SECRET
_DOMAIN_6]
```

```
Password for [administrator@EXAMPLE.ALT]:
OK: RemoteValidation: DC[\\dc1.test.alt] CONNECTION[WERR_OK] TRUST[WERR_OK]
VERIFY_STATUS_RETURNED
OK: RemoteRediscover: DC[\\dc1.test.alt] CONNECTION[WERR_OK]
```

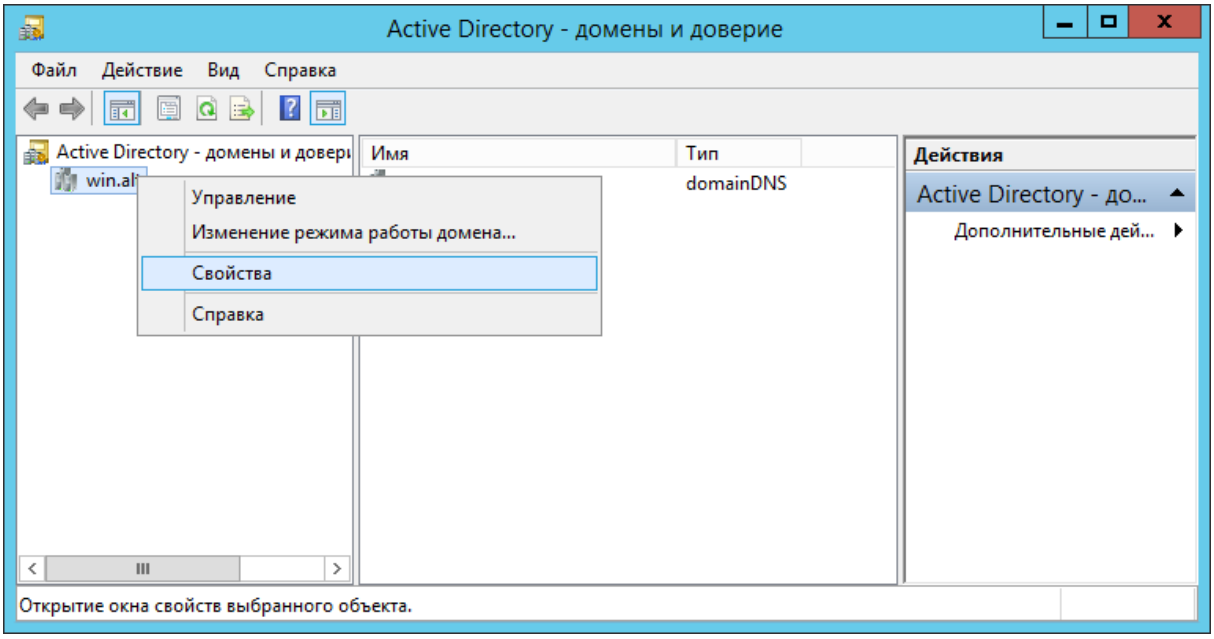
5.3.2. Samba DC и Windows Server с AD

Настройка на стороне Windows:

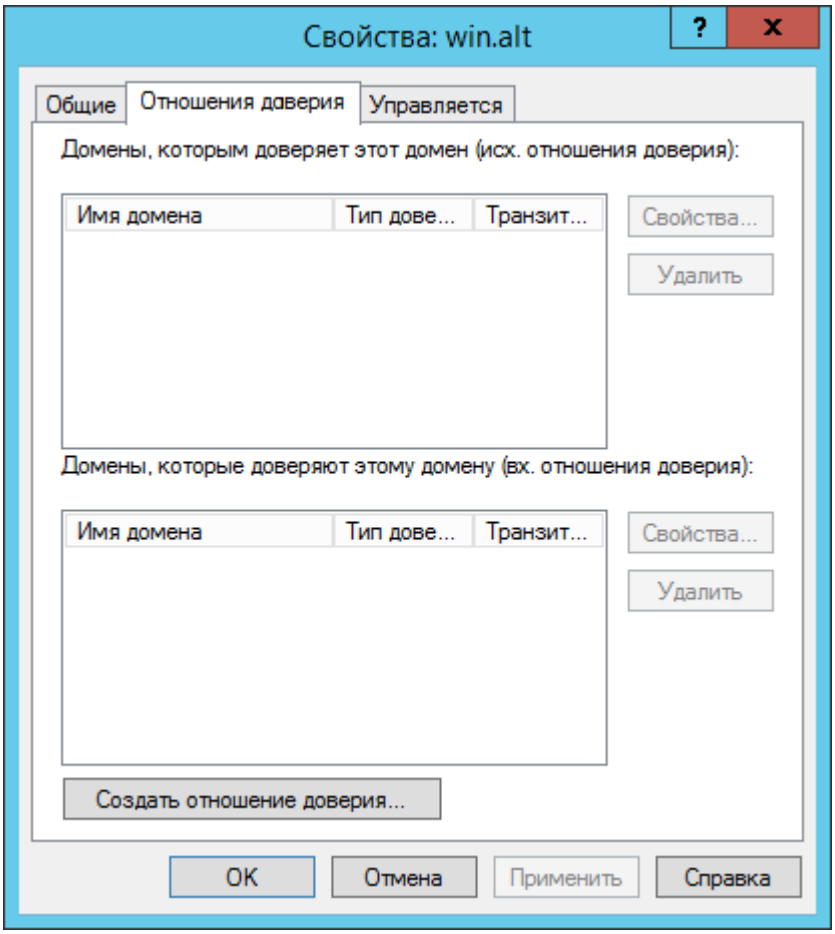
1. Открыть **`Диспетчер серверов`**, выбрать **Средства** → **Active Directory — Домены и Доверие**:



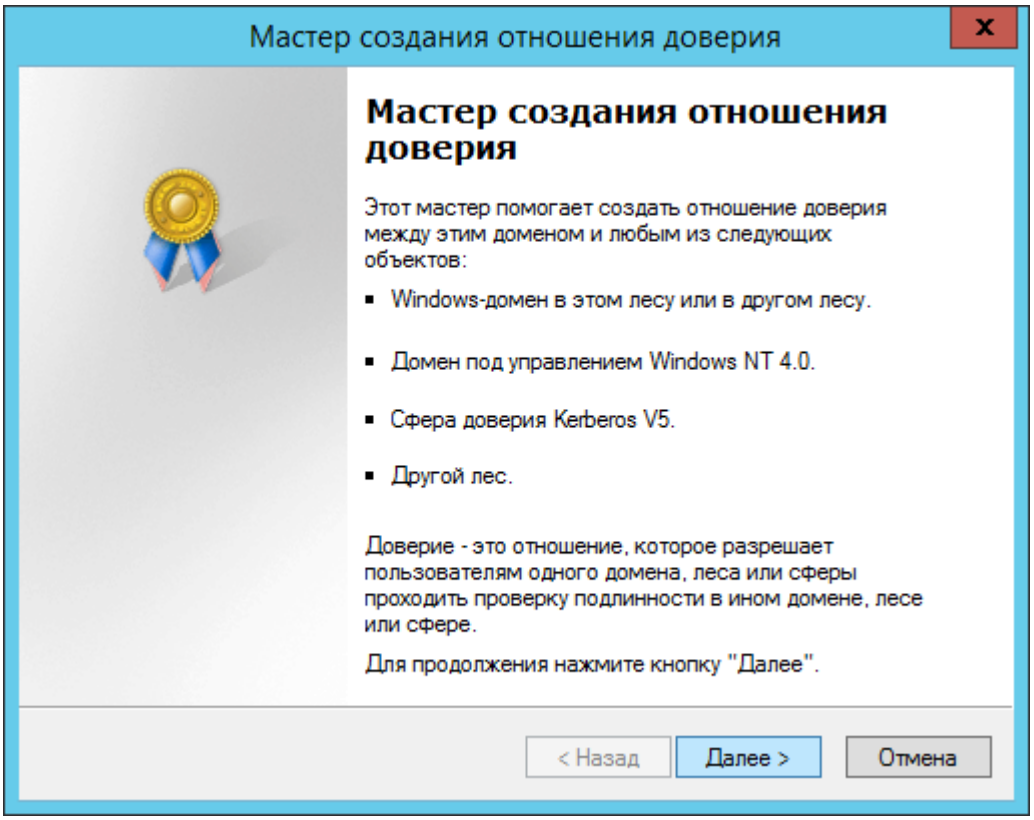
2. В открывшемся окне в контекстном меню домена выбрать пункт **Свойства**:



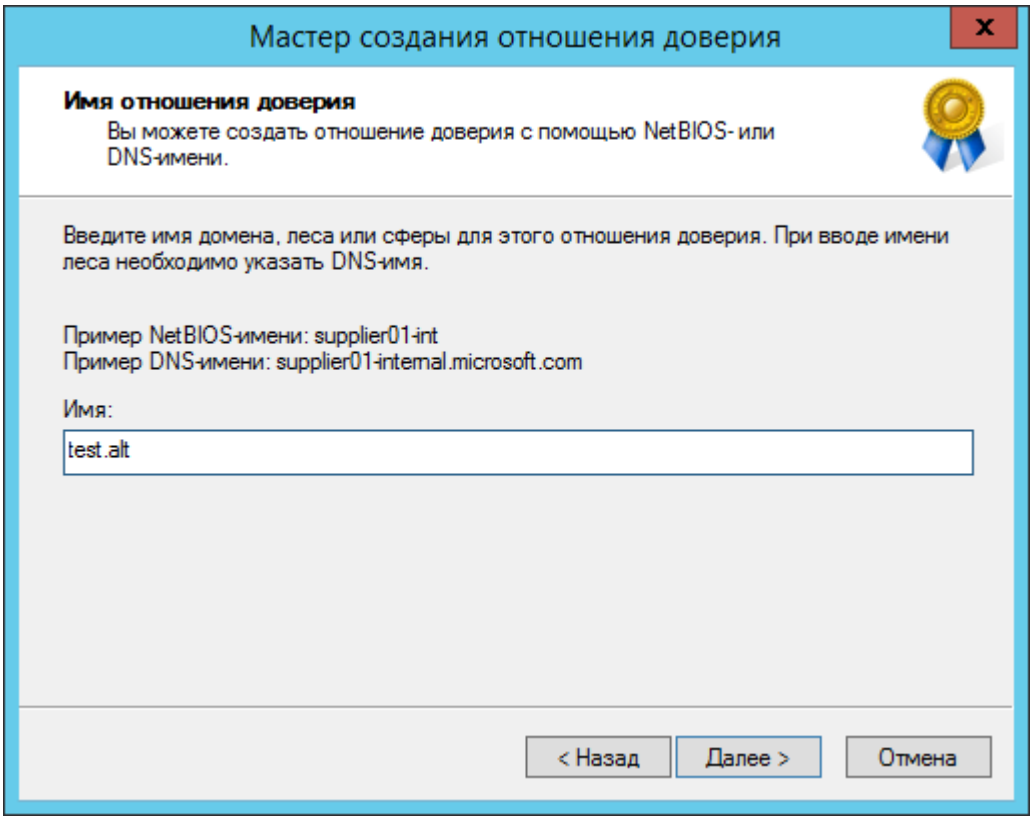
Откроется окно свойств домена. Необходимо перейти во вкладку **`Отношения доверия`** и нажать кнопку **`Создать отношение доверия…`**:



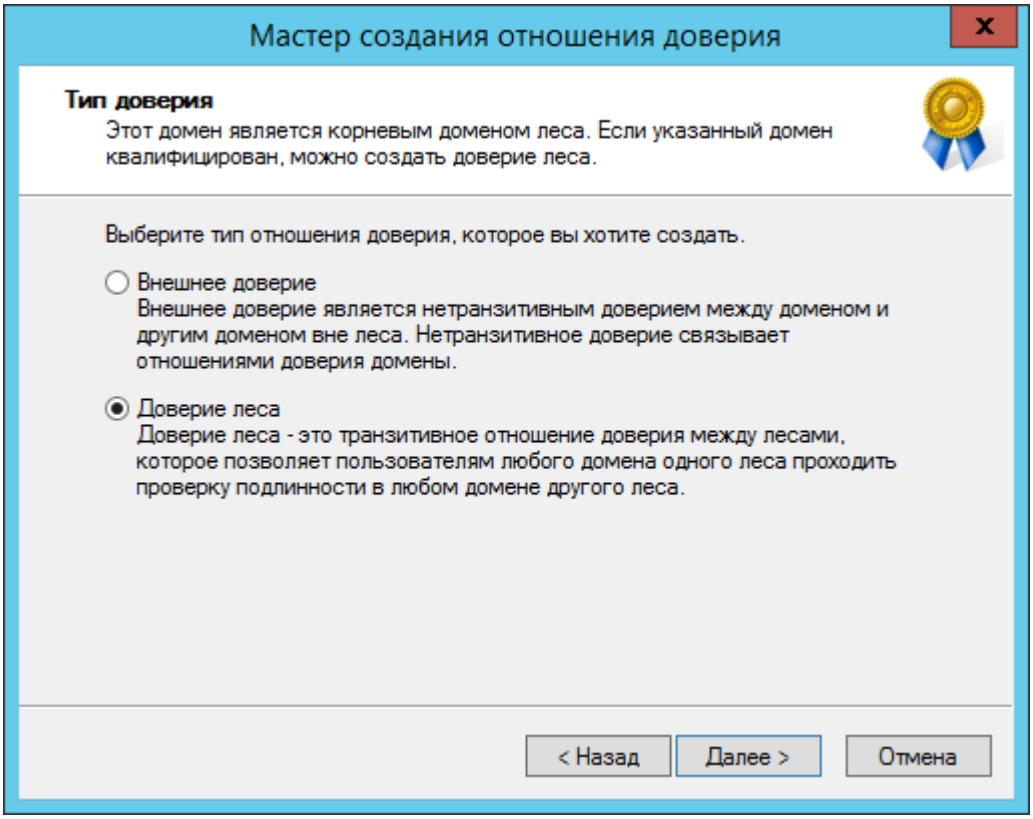
3. Будет запущен **`Мастер создания отношения доверия`**:



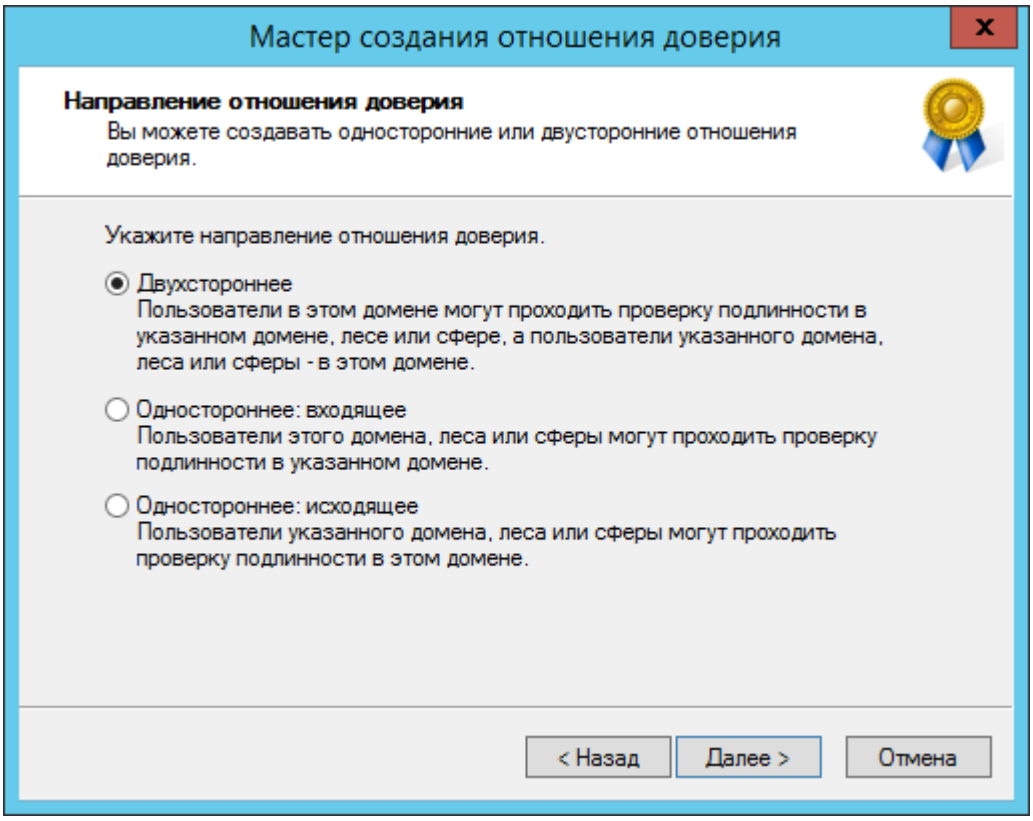
На втором шаге создания отношения доверия необходимо ввести имя домена Samba DC (в примере TEST.ALT):



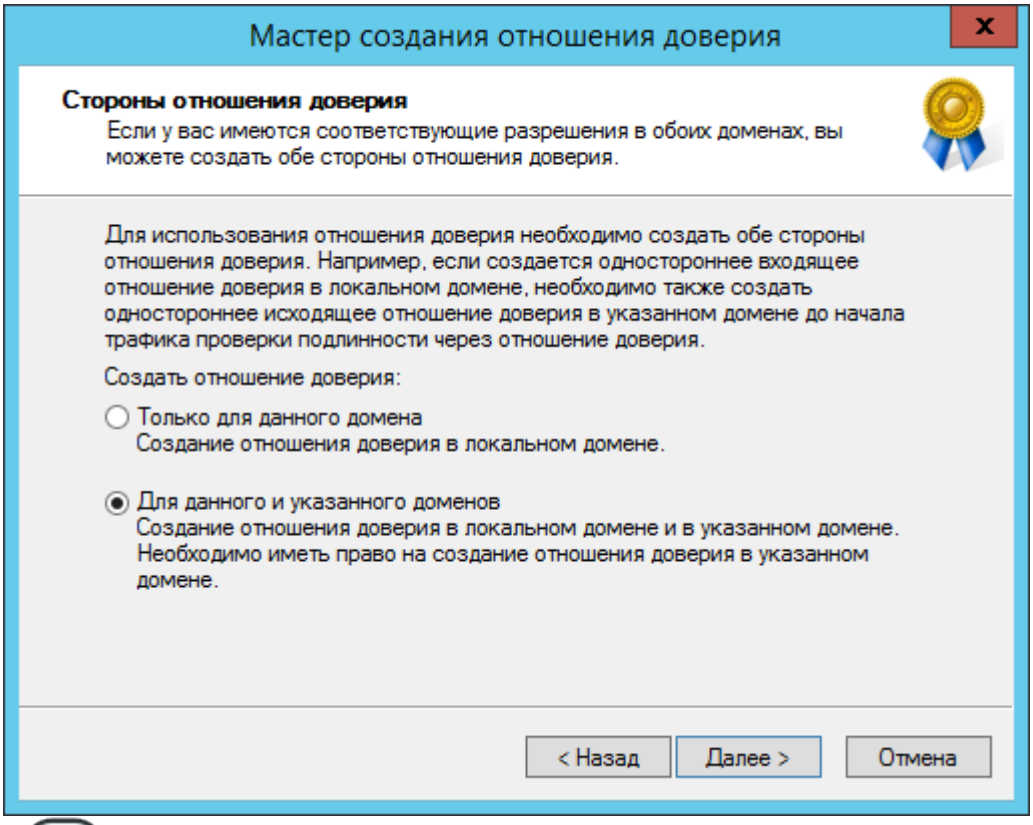
На следующем шаге следует выбрать тип доверия:



Далее выбирается направление доверия:

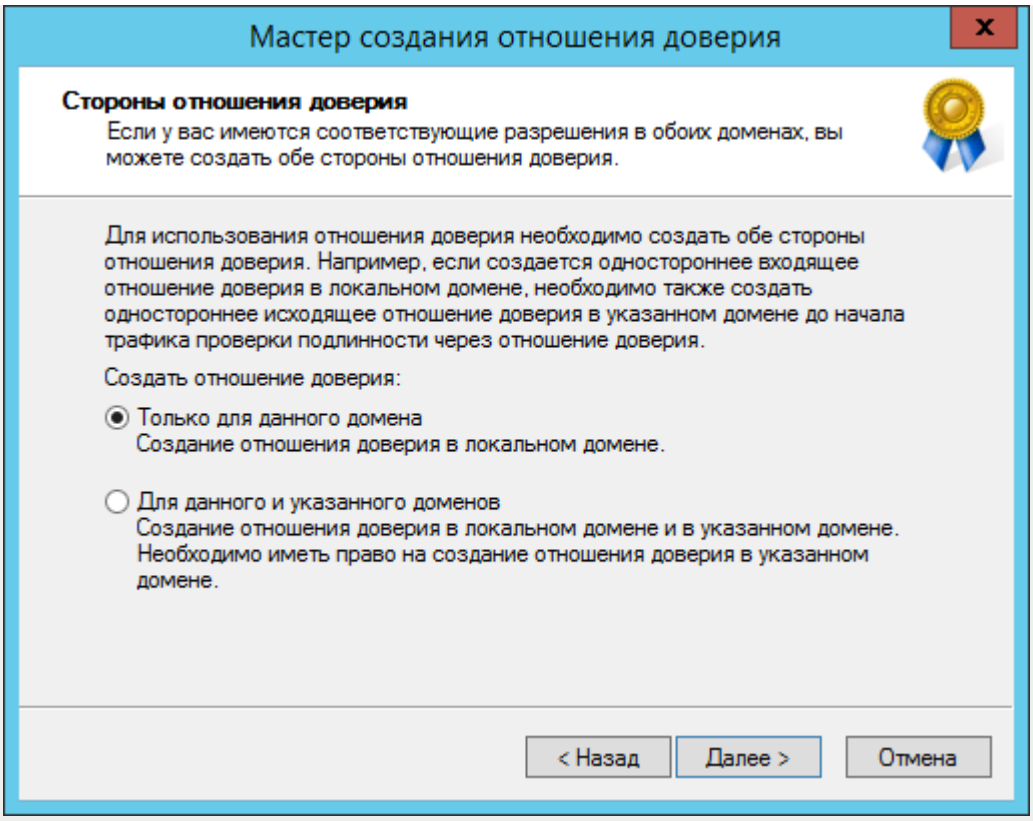


В открывшемся окне **Стороны отношения доверия** нужно выбрать, на каком из доменов применяется настройка. Если есть права администратора для обоих доменов, можно выбрать пункт **Для данного и указанного домена**:

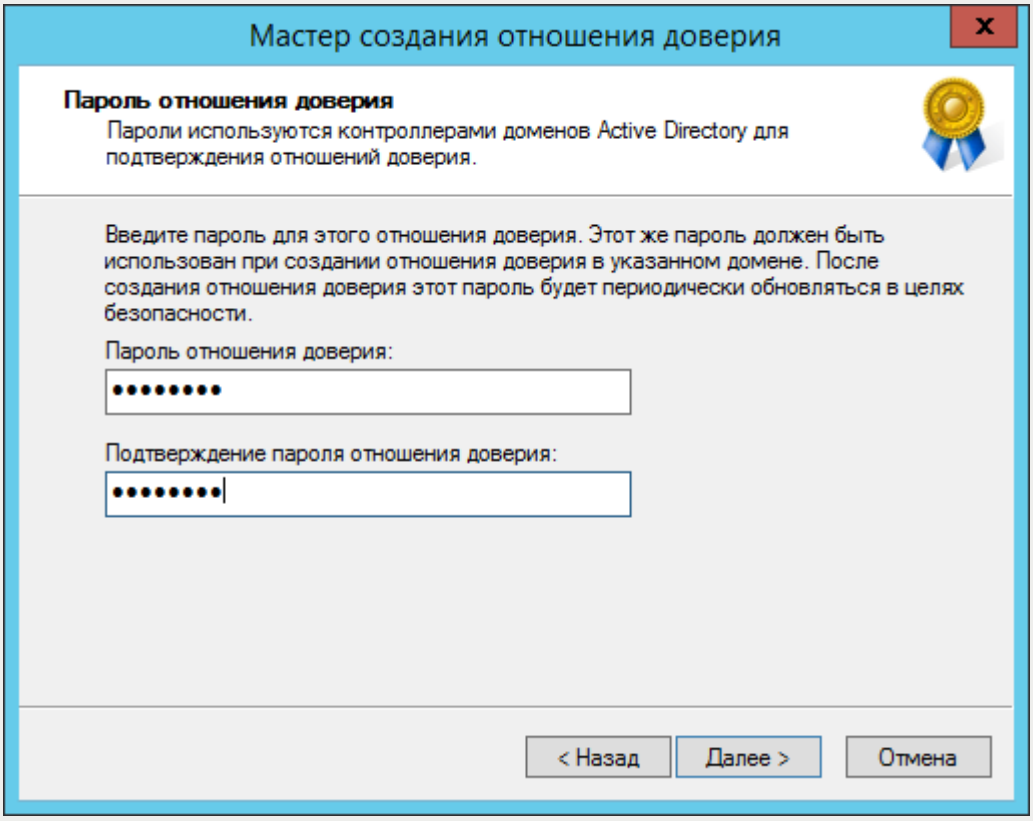


Примечание

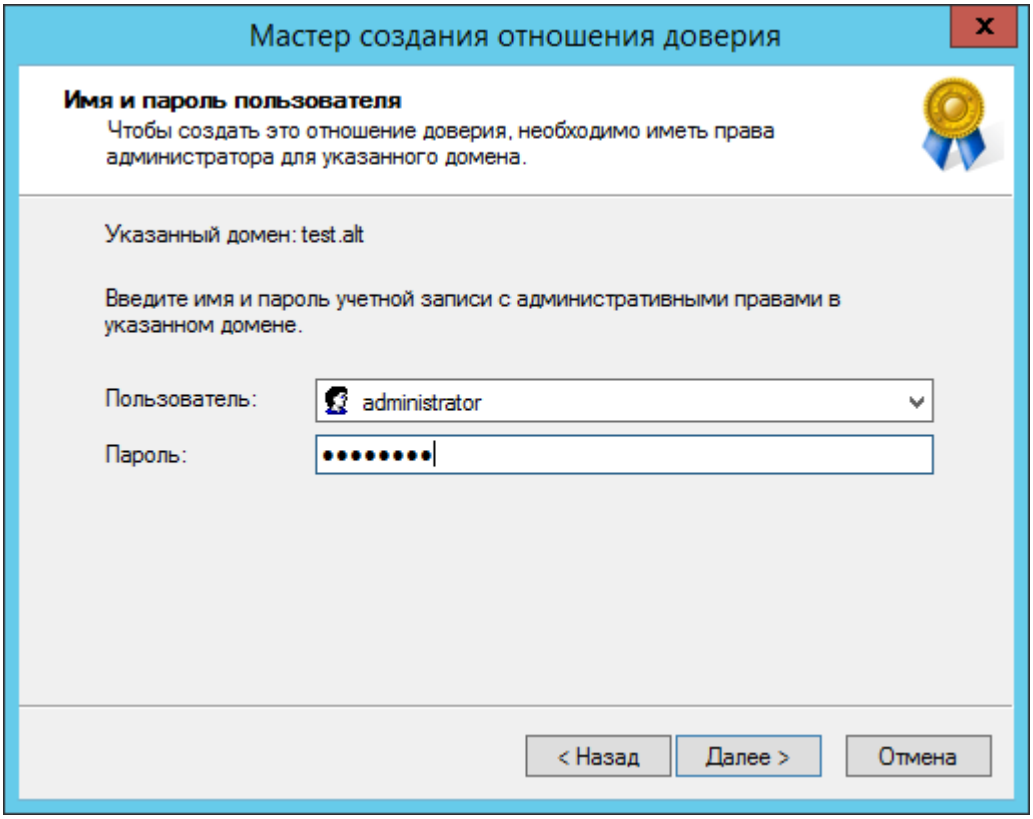
Если выбрать параметр **Только для данного домена**:



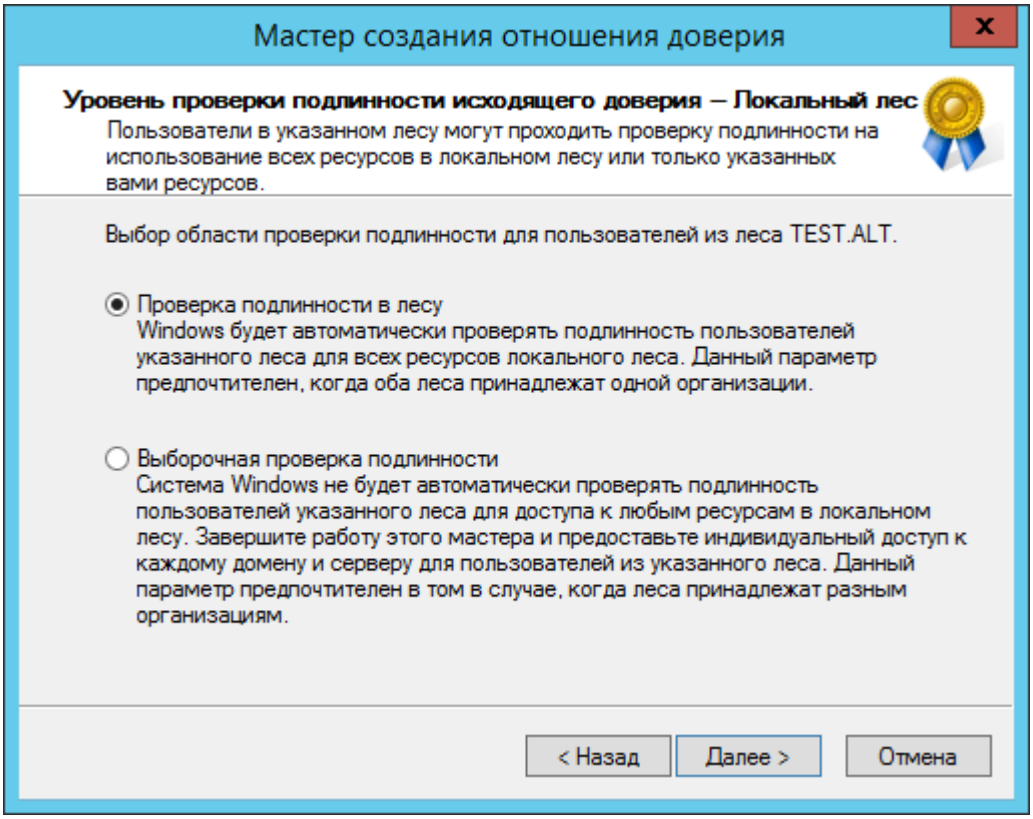
Необходимо задать **`Пароль отношения доверия`** (**`Trust Secret Key`**), который в дальнейшем будет использоваться при создании доверительного отношения на стороне Samba DC:



На следующем этапе мастер свяжется с удалённым доменом (если он доступен), и запросит имя и пароль пользователя с правами установки доверительных отношений в домене:

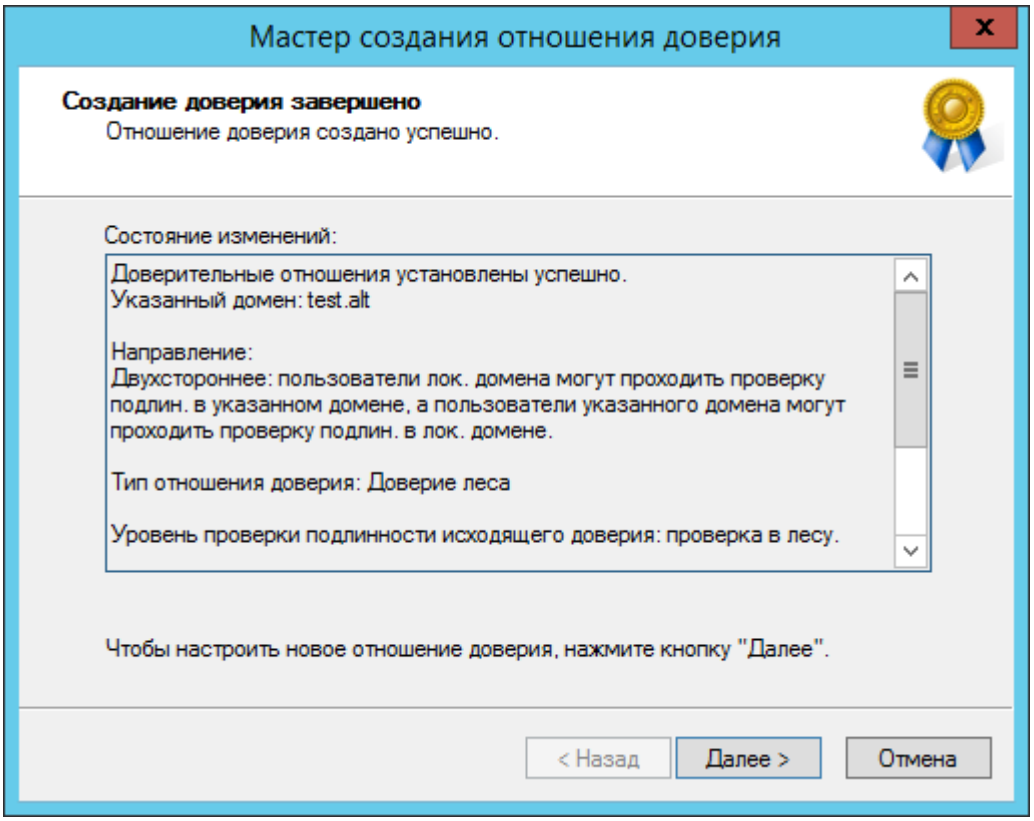


Далее на шаге **Уровень проверки подлинности исходящего доверия – Локальный лес** следует выбрать **Проверка подлинности в лесу**:

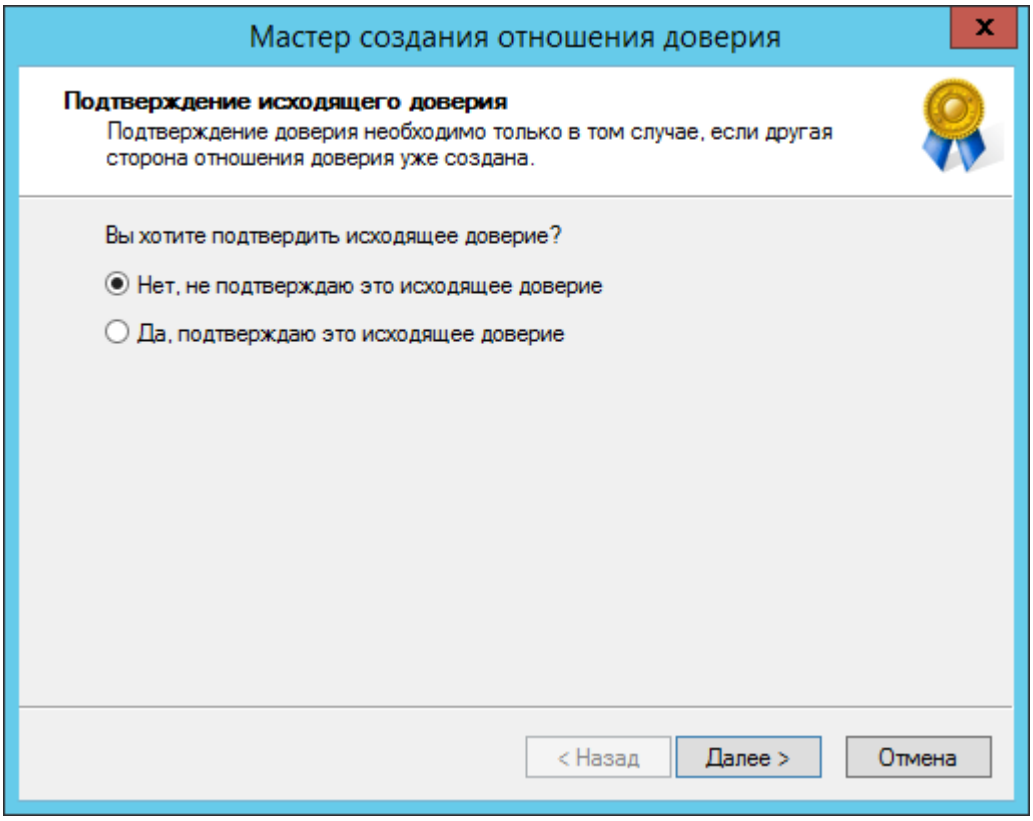


на шаге **Уровень проверки подлинности исходящего доверия — Указанный лес** также следует выбрать пункт **Проверка подлинности в лесу**.

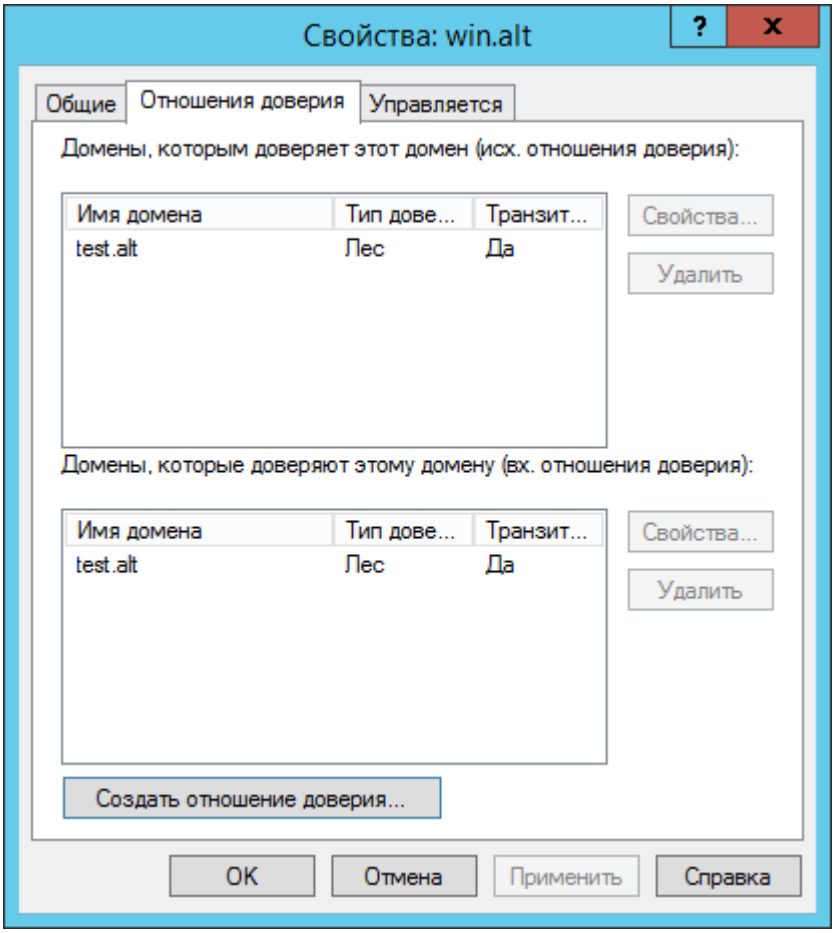
В окне **Выбор доверия завершен** мастер выдаст уведомление о том, что готов создать новое отношение доверия, и покажет краткую сводку с выбранными параметрами. Если согласиться с параметрами, то должно появиться уведомление о том, что создание доверия завершено:



После нажатия кнопки **Далее** появится окно **Подтверждение исходящего доверия**, а после него **Подтверждение входящего доверия**. Здесь можно оставить выбранным пункт **Нет, не подтверждаю это исходящее/входящее отношение доверие**, так как на стороне Samba DC доверие ещё не создавалось:



В результате будут получены двухсторонние доверительные отношения между доменами:



На стороне Samba DC для создания доверия необходимо выполнить команду:

```
# samba-tool domain trust create win.alt --type=forest --direction=both --create-location=both -Uadministrator@WIN
```

Важно

Для входа в доверенный домен через SSSD надо использовать тип связи **`external`**, а не **`forest`**.

При появлении запроса введите пароль администратора. сли все настроено верно, будет установлено доверие к домену AD.

```
LocalDomain Netbios[TEST] DNS[test.alt]
SID[S-1-5-21-3848605173-1839566900-710408900]
RemoteDC Netbios[DC1] DNS[DC1.win.alt]
ServerType[PDC,GC,LDAP,DS,KDC,TIMESERV,CLOSEST,WRITABLE,GOOD_TIMESERV,FULL_SECRET
_DOMAIN_6,ADS_WEB_SERVICE,DS_8,__unknown_00008000__]
Password for [administrator@WIN]:
RemoteDomain Netbios[WIN] DNS[win.alt]
SID[S-1-5-21-212759798-1661061060-862600140]
Creating local TDO.
Local TDO created
Setting supported encryption types on local TDO.
Setup local forest trust information...
Namespaces[2] TDO[win.alt]:
TLN: Status[Enabled]                  DNS[*.win.alt]
DOM: Status[Enabled]                  DNS[win.alt] Netbios[WIN]
SID[S-1-5-21-212759798-1661061060-862600140]
Validating outgoing trust...
OK: LocalValidation: DC[\\DC1.win.alt] CONNECTION[WERR_OK] TRUST[WERR_OK]
VERIFY_STATUS_RETURNED
Validating incoming trust…
OK: RemoteValidation: DC[\\dc1.test.alt] CONNECTION[WERR_OK] TRUST[WEER_OK]
VERIFY_STATUS_RETURNED
Success.
```

В случае использования Trust Secret Key в параметре ***`--create-location`*** нужно заменить опцию **`both`** на **`local`**, Samba DC прежде чем создать доверительные отношения сначала запросит Trust Key (??Incoming Trust Password/Outgoing Trust Password), созданный ранее при настройке в Windows.

```
# samba-tool domain trust create win.alt --type=forest --direction=both --create-location=local -Uadministrator@WIN
New Incoming Trust Password:
Retype Incoming Trust Password:
New Outgoing Trust Password:
Retype Outgoing Trust Password:
LocalDomain Netbios[TEST] DNS[test.alt]
SID[S-1-5-21-3848605173-1839566900-710408900]
RemoteDC Netbios[DC1] DNS[DC1.win.alt] ServerType[PDC,GC,LDAP,DS,KDC,TIMESERV,…]
Password for [administrator@WIN]:
…
```

Проверка доверия с dc1.test.alt:

- Просмотр доверия:

```
# samba-tool domain trust show WIN.ALT
LocalDomain Netbios[TEST] DNS[test.alt]
SID[S-1-5-21-3848605173-1839566900-710408900]
TrustedDomain:

NetbiosName:    WIN
DnsName:        win.alt
SID:            S-1-5-21-212759798-1661061060-862600140
Type:           0x2 (UPLEVEL)
Direction:      0x3 (BOTH)
Attributes:     0x8 (FOREST_TRANSITIVE)
PosixOffset:    0x00000000 (0)
kerb_EncTypes:  0x18 (AES128_CTS_HMAC_SHA1_96,AES256_CTS_HMAC_SHA1_96)
Namespaces[2] TDO[win.alt]:
TLN: Status[Enabled]                  DNS[*.win.alt]
DOM: Status[Enabled]                  DNS[win.alt] Netbios[WIN]
SID[S-1-5-21-212759798-1661061060-862600140]
```

- Список трастов:

```
# samba-tool domain trust list
Type[Forest]   Transitive[Yes] Direction[BOTH]     Name[win.alt]
```

В разных доменах могут быть разные результаты. Результат зависит от типа траста который установлен с этим доменом.

Если после настройки доверия возникли проблемы с доступом пользователей из трастового домен в свой домен, тогда следует проверить, действительно ли установлен траст:

```
# samba-tool domain trust validate win.alt -Uadministrator@WIN
LocalDomain Netbios[TEST] DNS[test.alt]
SID[S-1-5-21-3848605173-1839566900-710408900]
LocalTDO Netbios[WIN] DNS[win.alt] SID[S-1-5-21-212759798-1661061060-862600140]
OK: LocalValidation: DC[\\DC1.win.alt] CONNECTION[WERR_OK] TRUST[WERR_OK]
VERIFY_STATUS_RETURNED
OK: LocalRediscover: DC[\\DC1.win.alt] CONNECTION[WERR_OK]
RemoteDC Netbios[DC1] DNS[DC1.win.alt]
ServerType[PDC,GC,LDAP,DS,KDC,TIMESERV,CLOSEST,WRITABLE,GOOD_TIMESERV,FULL_SECRET
_DOMAIN_6,ADS_WEB_SERVICE,DS_8,__unknown_00008000__]
Password for [administrator@WIN]:
OK: RemoteValidation: DC[\\dc2.test.alt] CONNECTION[WERR_OK] TRUST[WERR_OK]
VERIFY_STATUS_RETURNED
OK: RemoteRediscover: DC[\\dc2.test.alt] CONNECTION[WERR_OK]
```

5.4. Управление пользователями и группами

Теперь можно назначать пользователей и группы из доверяющего домена в группу доверенного домена. Так как настроено двустороннее доверие, можно назначать пользователей и группы в обоих направлениях.

Примечание

Предварительно необходимо создать несколько пользователей и групп в обоих доменах (см. Управление пользователями и группами).

5.4.1. Список пользователей и групп

С помощью команды **wbinfo** нельзя получить список пользователей и групп из доверяющего домена, можно получить список пользователей и групп только из своего домена. Пример:

- команды выполняются на контроллере домена dc1.test.alt:

```
# wbinfo -u --domain=EXAMPLE.ALT
# wbinfo -u --domain=TEST.ALT
TEST\administrator
TEST\guest
TEST\krbtgt
TEST\dns-dc1
TEST\ivanov
```

- команды выполняются на контроллере домена s1.example.alt:

```
# wbinfo -u --domain=EXAMPLE.ALT
EXAMPLE\administrator
EXAMPLE\guest
EXAMPLE\krbtgt
EXAMPLE\dns-s1
EXAMPLE\kim
# wbinfo -u --domain=TEST.ALT
```

Для получения списка всех пользователей можно выполнить LDAP-запрос с помощью команды **samba-tool**. Пример получения списка пользователей из обоих доменов на контроллере домена dc1.test.alt:

```
# samba-tool user list -H ldap://s1 -Uadministrator@EXAMPLE.ALT
Password for [administrator@EXAMPLE.ALT]:
dns-s1
krbtgt
Administrator
Guest
kim
# samba-tool user list -H ldap://dc1 -Uadministrator@TEST.ALT
Password for [administrator@TEST.ALT]:
dns-dc1
krbtgt
Guest
Administrator
ivanov
```

Получение дополнительной информации о доменах (в примере команды выполняются на контроллере домена dc1.test.alt):

```
# wbinfo --all-domains
BUILTIN
TEST
EXAMPLE

# wbinfo --own-domain
TEST

# wbinfo --trusted-domains
BUILTIN
TEST
EXAMPLE

# wbinfo --online-status
BUILTIN : active connection
TEST : active connection
EXAMPLE : active connection
```

Получение SID пользователей и групп (в примере команды выполняются на контроллере домена dc1.test.alt):

```
# wbinfo -n TEST\\ivanov
S-1-5-21-1455776928-3410124986-2843404052-1105 SID_USER (1)

# wbinfo -n EXAMPLE\\kim
S-1-5-21-3274802069-598906262-3677769431-1104 SID_USER (1)

# wbinfo -n TEST\\office
S-1-5-21-1455776928-3410124986-2843404052-1107 SID_DOM_GROUP (2)

# wbinfo -n EXAMPLE\\office2
S-1-5-21-3274802069-598906262-3677769431-1107 SID_DOM_GROUP (2)

# wbinfo -i TEST\\ivanov
TEST.ALT\ivanov:*:3000022:100::/home/TEST.ALT/ivanov:/bin/false

# wbinfo -i EXAMPLE\\kim
EXAMPLE\kim:*:3000020:3000021::/home/EXAMPLE/kim:/bin/false
```

5.4.2. Тестирование аутентификации

С помощью команды **`wbinfo`** можно протестировать процесс аутентификации разных пользователей из обоих доменов.

`wbinfo` попытается авторизовать пользователя. Первой проверкой будет аутентификация по паролю с открытым текстом. Этот тип аутентификации применяется, когда пользователь входит в систему локально (plaintext не означает, что пароль будет отправлен без шифрования, это просто название процесса входа в систему). Вторая проверка — аутентификация по паролю запрос/ответ. Этот тип аутентификации использует NTLM или Kerberos.

Проверка методов аутентификации (в примере команды выполняются на контроллере домена dc1.test.alt):

```
# wbinfo -a TEST\\ivanov
Enter TEST\ivanov's password:
plaintext password authentication succeeded
Enter TEST\ivanov's password:
```

```
challenge/response password authentication succeeded


# wbinfo -a EXAMPLE\\kim
Enter EXAMPLE\kim's password:
plaintext password authentication succeeded
Enter EXAMPLE\kim's password:
challenge/response password authentication succeeded
```

Посмотреть какие контроллеры домена отвечают за аутентификацию:

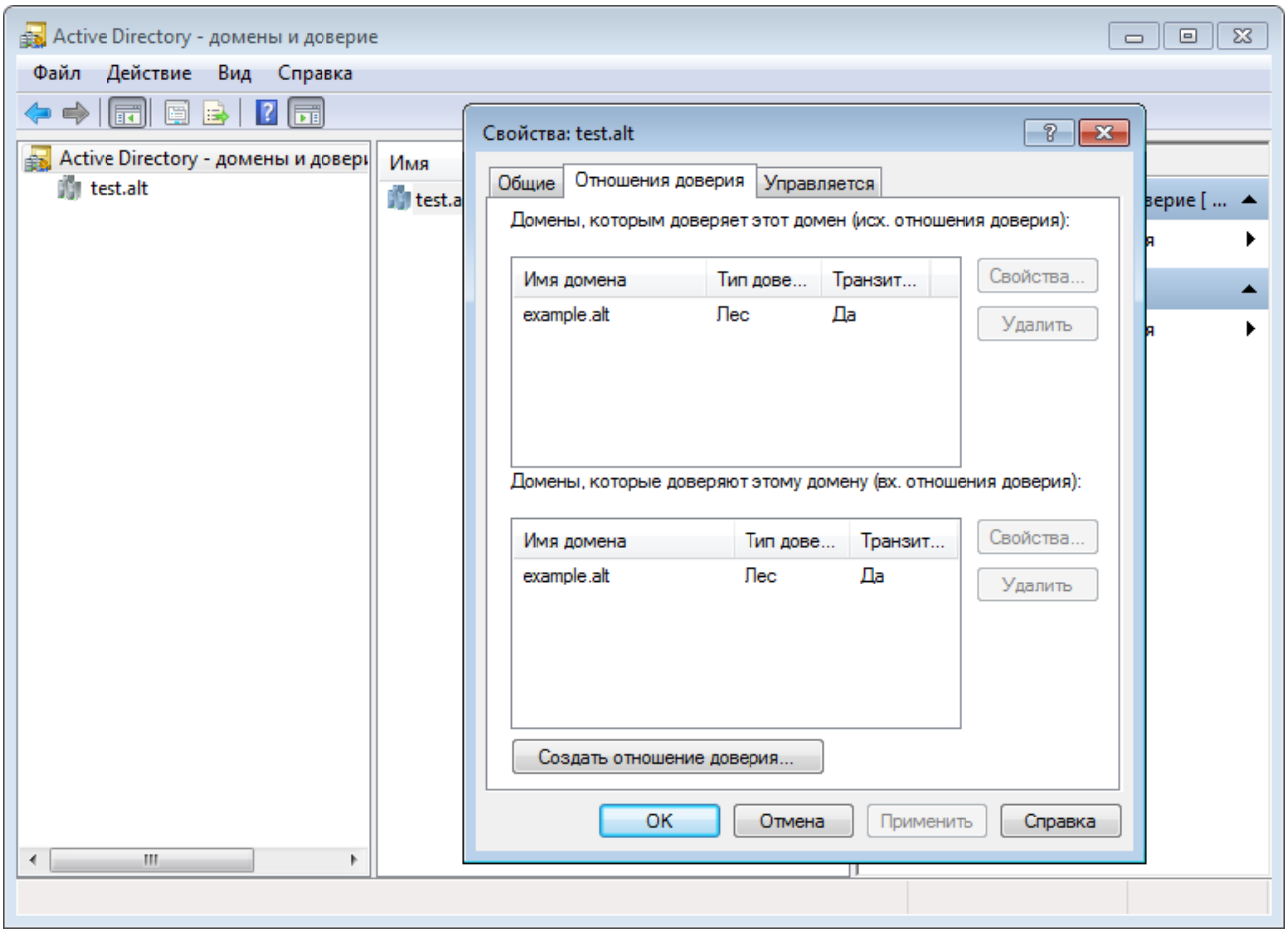
```
# wbinfo --ping-dc
checking the NETLOGON for domain[TEST] dc connection to "dc1.test.alt" succeeded

# wbinfo --ping-dc --domain=EXAMPLE.ALT
checking the NETLOGON for domain[EXAMPLE.ALT] dc connection to "s1.example.alt"
succeeded
```

Назначение пользователей и групп из доверенных доменов в группу доверяющего домена:

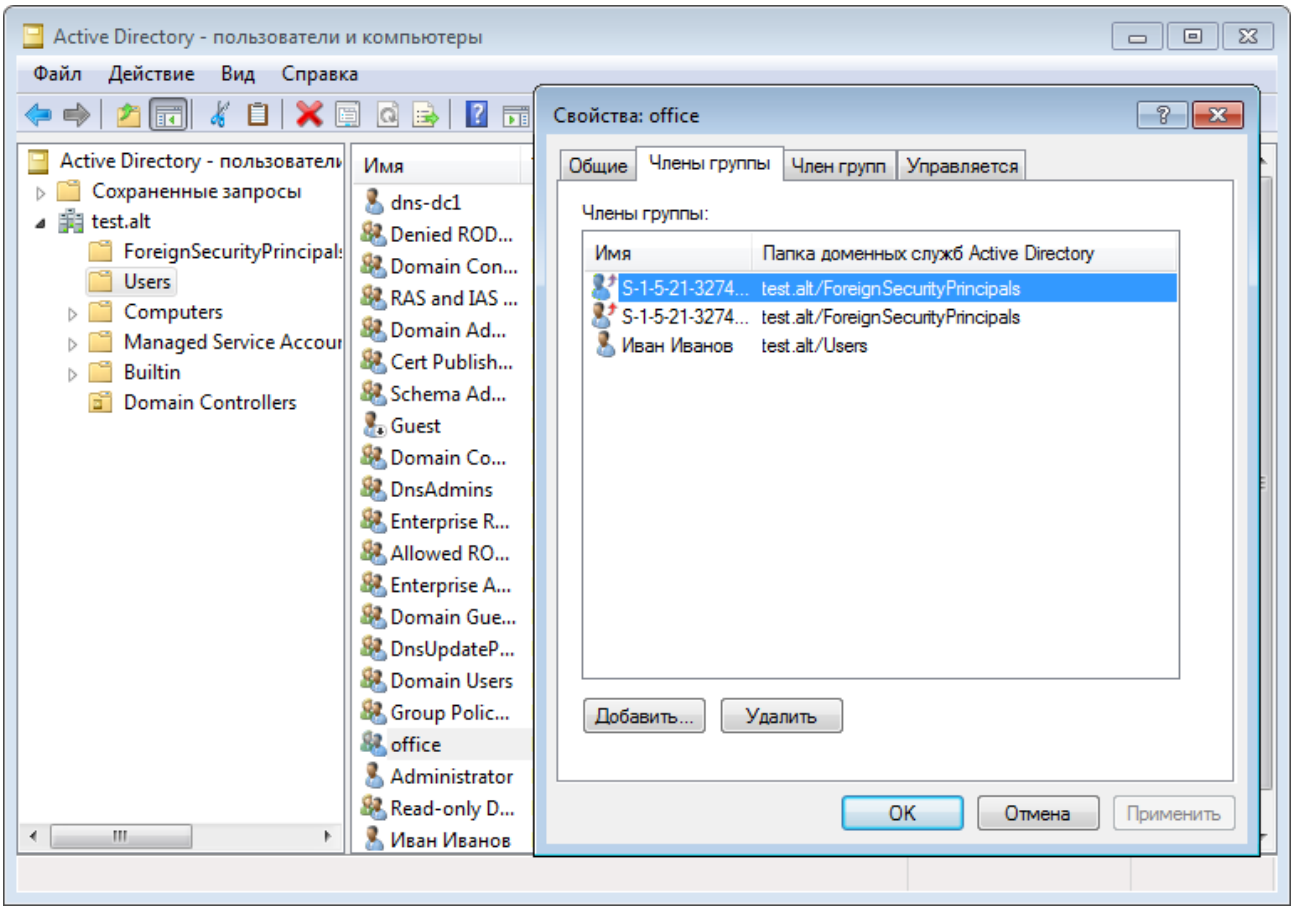
```
# wbinfo -n EXAMPLE\\kim
S-1-5-21-3274802069-598906262-3677769431-1104 SID_USER (1)

# samba-tool group addmembers office
S-1-5-21-3274802069-598906262-3677769431-1104
Added members to group office

# wbinfo -n EXAMPLE\\office2
S-1-5-21-3274802069-598906262-3677769431-1107 SID_DOM_GROUP (2)

# samba-tool group addmembers office
S-1-5-21-3274802069-598906262-3677769431-1107
Added members to group office

# samba-tool group listmembers office
S-1-5-21-3274802069-598906262-3677769431-1104
ivanov
S-1-5-21-3274802069-598906262-3677769431-1107
```

5.4.3. Просмотр доверия в Windows

Модуль RSAT (см. Установка RSAT) «Active Directory — домены и доверие» («Active Directory — Domain and Trusts») позволяет проверить состояние отношений доверия между доменами:



В модуле RSAT Active Directory — пользователи и компьютеры (Active Directory — Users and Computers) можно просмотреть список пользователей группы:



5.5. Использование трастов на LINUX-клиентах

Если необходимо использовать пользователей из обоих доменов (установлены двухсторонние доверительные отношения с типом связи **Лес**), то рабочую станцию с ОС Альт следует вводить в домен через winbind (см. Подключение к AD с помощью Samba Winbind).

5.5.1. Настройка winbind

На машине, введённой в домен, необходимо в файле **`smb.conf`** установить ID-маппинг для обоих доменов (backend = rid/tdb ??). Пример файла **`smb.conf`** на машине введённой в домен example.alt:

```
[global]
        security = ads
        realm = EXAMPLE.ALT
        workgroup = EXAMPLE
        netbios name = WORK1
        template shell = /bin/bash
        kerberos method = system keytab
        wins support = no
        winbind use default domain = yes
        winbind enum users = no
        winbind enum groups = no
        template homedir = /home/EXAMPLE.ALT/%U
        winbind refresh tickets = yes
        winbind offline logon = yes
        idmap config * : range = 10000-20000000
        idmap config * : backend = tdb
```

```
        idmap config EXAMPLE : backend = rid
        idmap config EXAMPLE : range = 10000-20000000
        idmap config TEST : backend = rid
        idmap config TEST : range = 10000-20000000
```

После перезапуска **smbd**, **nmbd**, **winbind** можно проверить, есть ли возможность просматривать пользователей из обоих доменов:

```
# net rpc trustdom list -Uadministrator
Password for [EXAMPLE\administrator]:
Trusted domains list:

TEST                S-1-5-21-1455776928-3410124986-2843404052

Trusting domains list:

TEST                S-1-5-21-1455776928-3410124986-2843404052


# wbinfo -n TEST\\ivanov
S-1-5-21-1455776928-3410124986-2843404052-1105 SID_USER (1)

# wbinfo -n EXAMPLE\\kim
S-1-5-21-3274802069-598906262-3677769431-1104 SID_USER (1)
```

Проверка с помощью **getent**:

```
# getent group TEST\\office
TEST\office:*:11107:

# getent group EXAMPLE\\office2
office2:*:11107:

# getent passwd TEST\\ivanov
TEST\ivanov:*:11105:10513::/home/EXAMPLE.ALT/ivanov:/bin/bash

# getent passwd EXAMPLE\\kim
kim:*:10000:10001:Олег Ким:/home/EXAMPLE.ALT/kim:/bin/bash
```

Проверка входа по SSH пользователями из обоих доменов:

```
$ ssh TEST\\ivanov@192.168.0.126
TEST\ivanov@192.168.0.126's password:
[TEST\ivanov@work1 ~]$ exit
выход
Connection to 192.168.0.126 closed.

$ ssh EXAMPLE\\kim@192.168.0.126
EXAMPLE\kim@192.168.0.126's password:
[kim@work1 ~]$ exit
выход
Connection to 192.168.0.126 closed.
```

5.5.2. Настройка SSSD

На машине введённой в домен необходимо в файл **/etc/sssd/sssd.conf** добавить доверенный домен:

```
[domain/EXAMPLE.ALT/TEST.ALT]
use_fully_qualified_names = false
```

После перезапуска **sssd** можно проверить, есть ли возможность просматривать пользователей из обоих доменов:

```
# getent passwd ivanov
ivanov:*:1855401105:1855400513:Иван Иванов:/home/TEST.ALT/ivanov:/bin/bash

# getent passwd kim
```

5.6. Удаление доверия

5.6.1. На стороне Samba

Пример удаления доверия на контроллере домена dc1.test.alt:

```
# samba-tool domain trust delete EXAMPLE.ALT -U administrator@EXAMPLE.ALT
LocalDomain Netbios[TEST] DNS[test.alt]
SID[S-1-5-21-1455776928-3410124986-2843404052]
RemoteDC Netbios[S1] DNS[s1.example.alt]
ServerType[PDC,GC,LDAP,DS,KDC,TIMESERV,CLOSEST,WRITABLE,GOOD_TIMESERV,FULL_SECRET
_DOMAIN_6]
Password for [administrator@EXAMPLE.ALT]:
RemoteDomain Netbios[EXAMPLE] DNS[example.alt]
SID[S-1-5-21-3274802069-598906262-3677769431]
RemoteTDO deleted.
```

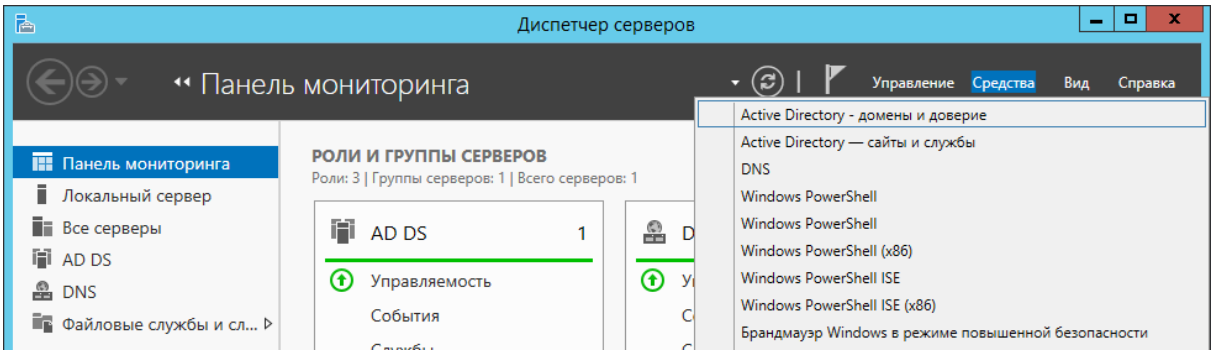
Проверка:

```
# samba-tool domain trust list
```

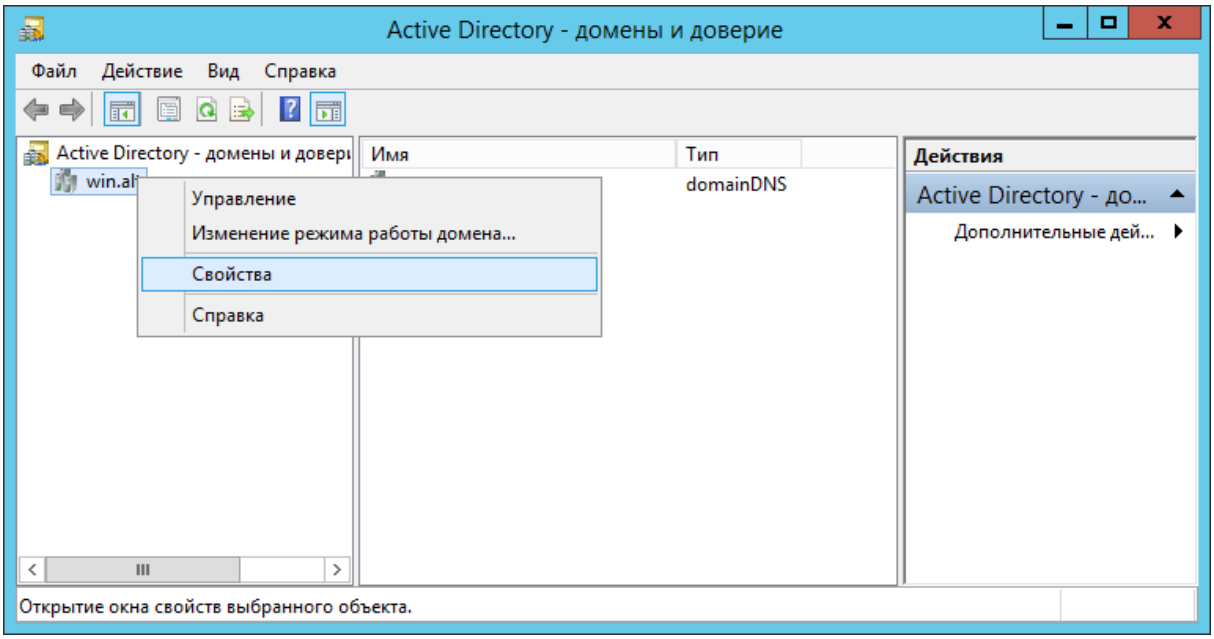
5.6.2. На стороне Windows Server с AD

Удаление доверия:

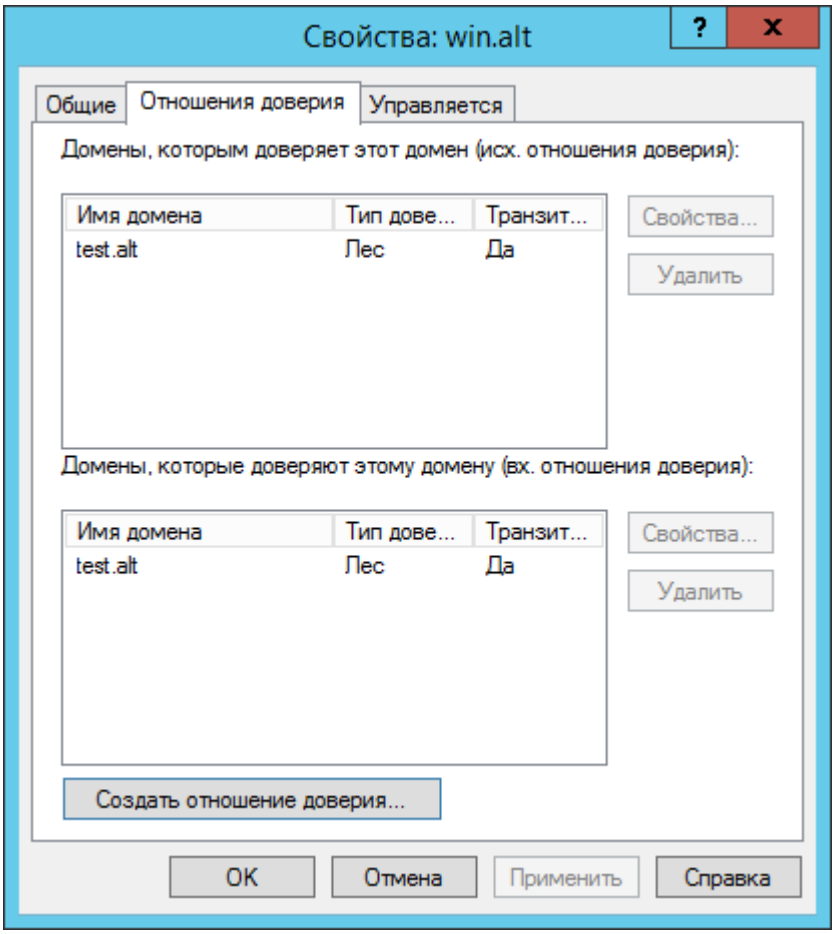
1. Открыть **Диспетчер серверов**, выбрать **Средства** → **Active Directory — Домены и Доверие**:



2. В открывшемся окне в контекстном меню домена выбрать пункт **Свойства**:

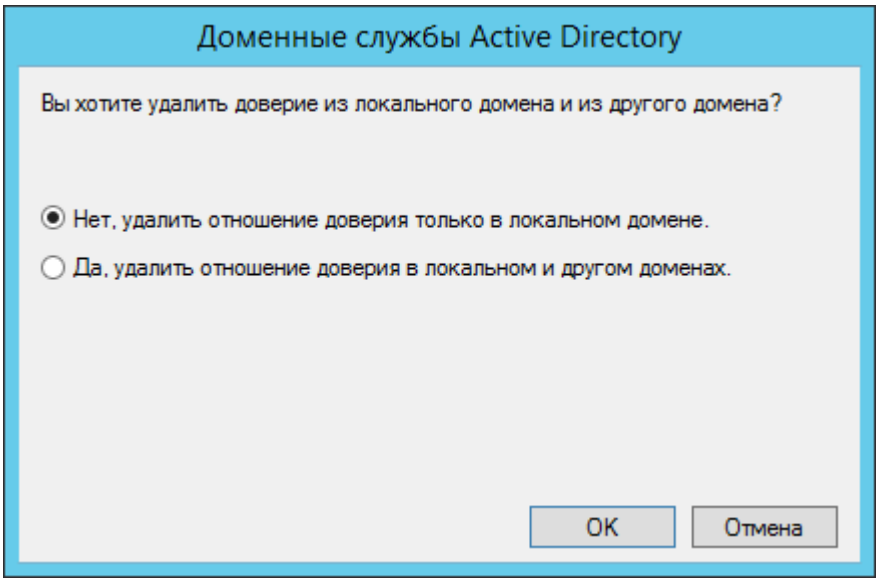


Откроется окно свойств домена. Необходимо перейти во вкладку **Отношения доверия** и нажать кнопку **Создать отношение доверия…**:



3. В группе **Домены, которым доверяет этот домен (исх. отношения доверия)** или группе **Домены, которые доверяют этому домену (вх. отношения доверия)** выбрать доверие, которое требуется удалить, а затем нажать кнопку **Удалить**.

4. В открывшемся окне выбрать где нужно удалить доверие и нажать кнопку **OK**.



Если выбран параметр **Нет, удалить отношение доверия только в локальном домене**, рекомендуется повторить эту процедуру для домена второй стороны. Если выбран параметр **Да, удалить отношение доверия в локальном и другом доменах**, необходимо ввести учетную запись и пароль администратора для домена второй стороны.

Глава 6. Конфигурирование Samba

6.1. Журналирование в Samba

Файлы журналов службы Samba находятся в каталоге **/var/log/samba/**.

6.1.1. Уровни журналирования

6.1.1.1. Установка уровня журналирования в файле smb.conf

Установить уровень журналирования для Samba можно, используя параметр ***log level*** в файле **/etc/samba/smb.conf**. Для разных классов отладки можно указывать разные уровни журналирования и отдельные файлы журналов.

Чтобы настроить ведение журналов для определенных классов так, чтобы они входили в другой файл, а не в файл журнала, вы можете добавить @PATH к классу.

Примеры:

- установить уровень журнала для всех классов отладки на 3:

```
log level = 3
```

- установить общий уровень журнала на 3 и для классов passdb и auth на 5:

```
log level = 3 passdb:5 auth:5
```

- установить уровень журнала для класса winbind на 1 и писать логи в файл **/var/log/winbind.log**:

```
log level = 3 winbind:1@/var/log/winbind.log
```

Получить дополнительную информацию и список классов отладки можно на справочной странице smb.conf(5) (**man smb.conf**).

6.1.1.2. Установка уровня журналирования при выполнении команд

Команды Samba используют уровень журналирования, установленный в параметре ***log level*** в файле **/etc/samba/smb.conf**. Это значение можно переопределить, используя опцию **-d** для всех команд Samba. Например:

```
$ net usershare add Share2 /tmp/share2 -d 5
```

6.1.2. Настройка ведения журнала аудита

Samba поддерживает ведение журнала событий аутентификации и авторизации, а также ведение журнала изменений базы данных AD DC. Это позволяет регистрировать, например, неудачные запросы аутентификации или сбросы пароля.

Ведение журнала аудита является локальной настройкой, эту функцию необходимо включить на каждом сервере Samba. События регистрируются на сервере Samba, на котором произошло событие. Чтобы хранить все журналы на централизованном сервере, следует настроить централизованный сервер системных журналов, настроить Samba для регистрации в syslog и настроить syslog для отправки журналов на централизованный сервер.

Описание параметров ***logging***, ***syslog*** и ***syslog only*** можно посмотреть на справочной странице smb.conf(5) (**man smb.conf**).

Примечание

Samba генерирует некоторые журналы на узле в конфигурации файлового сервера и члена домена, но полная поддержка доступна только в AD DC.

Samba поддерживает протоколирование успешных событий авторизации, но не неуспешных событий авторизации. Samba может регистрировать как успешные, так и неуспешные события аутентификации.

Примечание

Аутентификация

Аутентификация происходит, когда Samba проверяет комбинацию имени пользователя и пароля.

Авторизация

Авторизация происходит при запуске сеанса.

Журнал аудита Samba поддерживает стандартный формат и формат JSON. Можно включить каждый формат по отдельности или оба вместе, используя разные классы отладки журнала.

В зависимости от уровня журналирования Samba регистрирует разные события. Чтобы ограничить количество записей в журнале, можно увеличить уровень журналирования только для классов отладки, связанных с аудитом. Для управления уровнем журнала аудита можно использовать следующие классы отладки:

- **auth_audit** — стандартный формат журнала;
- **auth_json_audit** — формат JSON.

Пример включения ведения журнала аудита аутентификации (установить уровень журнала по умолчанию — 1, включить регистрацию неудачных и успешных запросов аутентификации — 3):

1. Установить в секции ***[global]*** файла **/etc/samba/smb.conf**:

```
log level = 1 auth_audit:3 auth_json_audit:3
```

2. Перезапустить службу Samba.

Пример записей о неуспешной и успешной попытках аутентификации пользователя на контроллере домена Samba с использованием стандартного формата журнала:

```
[2023/04/13 11:51:20.341735,  2] ../../auth/auth_log.c:
647(log_authentication_event_human_readable)
  Auth: [Kerberos KDC,ENC-TS Pre-authentication] user [(null)]\[petrov\
\@TEST.ALT@TEST.ALT] at [Thu, 13 Apr 2023 11:51:20.341726 EET] with [aes256-cts-
hmac-sha1-96] status [NT_STATUS_WRONG_PASSWORD] workstation [(null)] remote host
[ipv4:192.168.0.125:49382] mapped to [TEST]\[petrov]. local host [NULL]

[2023/04/13 11:51:32.859080,  3] ../../auth/auth_log.c:
647(log_authentication_event_human_readable)
  Auth: [Kerberos KDC,ENC-TS Pre-authentication] user [(null)]\[petrov\
\@TEST.ALT@TEST.ALT] at [Thu, 13 Apr 2023 11:51:32.859051 EET] with [aes256-cts-
hmac-sha1-96] status [NT_STATUS_OK] workstation [(null)] remote host
[ipv4:192.168.0.125:52630] became [TEST]\[petrov]
[S-1-5-21-1723588197-2340999690-1379671080-1106]. local host [NULL]
```

Пример записей о неуспешной и успешной попытках аутентификации пользователя на контроллере домена Samba с использованием формата JSON:

```
[2023/04/13 11:46:08.614095,  2] ../../auth/auth_log.c:
647(log_authentication_event_human_readable)
  Auth: [Kerberos KDC,ENC-TS Pre-authentication] user [(null)]\[petrov\
\@TEST.ALT@TEST.ALT] at [Thu, 13 Apr 2023 11:46:08.614055 EET] with [aes256-cts-
hmac-sha1-96] status [NT_STATUS_WRONG_PASSWORD] workstation [(null)] remote host
[ipv4:192.168.0.125:42738] mapped to [TEST]\[petrov]. local host [NULL]
  {"timestamp": "2023-04-13T11:46:08.614338+0200", "type": "Authentication",
"Authentication": {"version": {"major": 1, "minor": 2}, "eventId": 4625,
"logonId": "10c3af2c9c39fef4", "logonType": 3, "status":
"NT_STATUS_WRONG_PASSWORD", "localAddress": null, "remoteAddress":
"ipv4:192.168.0.125:42738", "serviceDescription": "Kerberos KDC",
"authDescription": "ENC-TS Pre-authentication", "clientDomain": null,
"clientAccount": "petrov\\@TEST.ALT@TEST.ALT", "workstation": null,
"becameAccount": "petrov", "becameDomain": "TEST", "becameSid":
"S-1-5-21-1723588197-2340999690-1379671080-1106", "mappedAccount": "petrov",
"mappedDomain": "TEST", "netlogonComputer": null, "netlogonTrustAccount": null,
"netlogonNegotiateFlags": "0x00000000", "netlogonSecureChannelType": 0,
"netlogonTrustAccountSid": null, "passwordType": "aes256-cts-hmac-sha1-96",
"duration": 6096}}

[2023/04/13 11:48:45.902778,  3] ../../auth/auth_log.c:
647(log_authentication_event_human_readable)
  Auth: [Kerberos KDC,ENC-TS Pre-authentication] user [(null)]\[petrov\
\@TEST.ALT@TEST.ALT] at [Thu, 13 Apr 2023 11:48:45.902759 EET] with [aes256-cts-
hmac-sha1-96] status [NT_STATUS_OK] workstation [(null)] remote host
[ipv4:192.168.0.125:52840] became [TEST]\[petrov]
[S-1-5-21-1723588197-2340999690-1379671080-1106]. local host [NULL]
  {"timestamp": "2023-04-13T11:48:45.902942+0200", "type": "Authentication",
"Authentication": {"version": {"major": 1, "minor": 2}, "eventId": 4624,
"logonId": "71c99af1de51eaf6", "logonType": 3, "status": "NT_STATUS_OK",
"localAddress": null, "remoteAddress": "ipv4:192.168.0.125:52840",
"serviceDescription": "Kerberos KDC", "authDescription": "ENC-TS Pre-
authentication", "clientDomain": null, "clientAccount": "petrov\
\@TEST.ALT@TEST.ALT", "workstation": null, "becameAccount": "petrov",
"becameDomain": "TEST", "becameSid":
"S-1-5-21-1723588197-2340999690-1379671080-1106", "mappedAccount": "petrov",
"mappedDomain": "TEST", "netlogonComputer": null, "netlogonTrustAccount": null,
"netlogonNegotiateFlags": "0x00000000", "netlogonSecureChannelType": 0,
"netlogonTrustAccountSid": null, "passwordType": "aes256-cts-hmac-sha1-96",
"duration": 9023}}
```

Пример включения ведения журнала аудита базы данных DC AD (установить уровень журнала по умолчанию — 1, включить ведение журнала изменений базы данных в формате JSON):

1. Установить в секции ***[global]*** файла **/etc/samba/smb.conf**:

```
log level = 1 dsdb_json_audit:5 dsdb_password_json_audit:5
dsdb_group_json_audit:5 dsdb_transaction_json_audit:5
```

2. Перезапустить службу Samba.

6.1.3. Интерпретация журналов аудита JSON

Если включено ведение журнала аудита в формате JSON, сведения о различных событиях регистрируются в формате JSON. Каждое событие имеет множество атрибутов. Внешний слой атрибутов состоит из трёх элементов: метки времени, типа события и объекта данных:

```
{
  "timestamp": 2023-04-13T11:48:45.902942+0200,
  "type": одно из значений "Authentication", "Authorization", "dsdbChange",
          "dsdbTransaction", "passwordChange", "replicatedUpdate",
          "groupChange",
  type: { data }
}
```

Примечание

Некоторые атрибуты по-прежнему будут присутствовать в журнале, даже если они неприменимы. Например, если NETLOGON не используется (согласно ***serviceDescription***), для параметра ***netlogonComputer*** будет установлено значение «null», для параметра ***netlogonNegotiateFlags*** будет установлено значение «0x00000000», а другие поля сетевого входа будут иметь аналогичные пустые значения.

Таблица 6.1. Аутентификация

Атрибут	Значение
authDescription	Тип аутентификации, в том числе: ▸«simple bind/TLS», «simple bind»: простая привязка LDAP с каналом TLS или без него ▸«guest»: анонимный запрос SMB1 ▸«bare-NTLM»: SMB, использующий протокол NT1 ▸«plaintext»: обычный текст SMB1 ▸«interactive»: as if physically at a workstation ▸«network»: проверка подлинности запроса/ответа по сети ▸«Unknown Auth Description», «Unknown Pre-authentication»: события KDC ▸«ServerAuthenticate»: запрос/ответ компьютера при входе в систему с использованием NETLOGON

Атрибут	Значение
	▸«LDAP Modify»: смена пароля (не событие аутентификации, но регистрируется здесь, чтобы администратор не пропустил его).
becameAccount	Имя учетной записи, под которой выполнен вход (может отличаться от учетной записи, предоставленной клиентом)
becameDomain	Имя домена, в который произведён вход
becameSid	SID аутентифицированной учетной записи
clientAccount	Сообщаемое клиентом имя учётной записи
clientDomain	Имя домена, о котором сообщает клиент
duration	Сколько времени заняла аутентификация в микросекундах
eventId	Идентификатор события Windows, указывающий в общих чертах, что произошло
localAddress	Адрес сервера и используемый порт
logonId	Случайный 64-битный идентификатор, помогающий отслеживать события входа в систему на разных этапах
logonType	Тип входа в Windows, для Samba один из ▸2: интерактивный, то есть на этом компьютере ▸3: по сети ▸8: NetworkCleartext с использованием нехешированных паролей
mappedAccount	Имя учетной записи клиента, преобразованное в имя учетной записи AD
mappedDomain	Клиентский домен преобразованный в доменное имя AD
netlogonComputer	Заявленное имя компьютера в аутентификации NETLOGON RPC
netlogonNegotiateFlags	Флаги параметров согласования NETLOGON
netlogonSecureChannelType	Тип используемого канала NETLOGON
netlogonTrustAccount	Учетная запись, используемая для аутентификации NETLOGON
netlogonTrustAccountSid	SID, принадлежащий доверенной учетной записи NETLOGON
passwordType	Алгоритм/протокол пароля (например, «HMAC-SHA256», «NTLMv2», «arcfour-hmac-md5»).
remoteAddress	Заявленный адрес (и порт) удаленного клиента
serviceDescription	Тип службы, например "LDAP", "SMB2", "NETLOGON", "Kerberos KDC"

Атрибут	Значение
status	Сообщение NT STATUS. Для успешной аутентификации это будет "NT_STATUS_OK". Неудачная аутентификация может иметь здесь «NT_STATUS_OK», если аутентификация не удалась после регистрации этого сообщения, но обычно имеет код ошибки. Некоторые типы сообщений ▸NT_STATUS_ACCESS_DENIED: доступ запрещен по неустановленным причинам, но, вероятно, из-за неправильных учетных данных ▸NT_STATUS_WRONG_PASSWORD: неверный пароль ▸NT_STATUS_NO_SUCH_USER: неверный пользователь ▸NT_STATUS_NO_SUCH_DOMAIN: неверный домен ▸NT_STATUS_ACCOUNT_RESTRICTION: учетная запись защищена или иным образом ограничена ▸NT_STATUS_INVALID_SYSTEM_SERVICE: выбранная служба аутентификации недоступна ▸NT_STATUS_NO_MEMORY: сервер не может завершить аутентификацию и заявляет о нехватке памяти
workstation	Заявленное имя клиентской рабочей станции

Таблица 6.2. Успешные события авторизации

Атрибут	Значение
account	Имя авторизуемой учетной записи
accountFlags	Битовое поле атрибутов учетной записи
authType	Строка, описывающая тип авторизации (например, «krb5», «NTLMSSP», «simple bind»)
domain	Домен
localAddress	Адрес сервера и используемый порт
logonServer	Сервер, на котором выполнена аутентификация
remoteAddress	Видимый адрес клиента
serviceDescription	Тип службы, например "LDAP", "SMB2", "DCE/RPC"
sessionId	GUID, идентифицирующий сеанс
sid	SID авторизованной учетной записи

Атрибут	Значение
transportProtection	Тип защиты канала (например, «SMB», «TLS», «SEAL», «NONE»)

Остальные таблицы: dsdbChange? (https://wiki.samba.org/index.php/Interpreting_JSON_Audit_Logs)

6.2. Создание keytab-файла

SPN (Service Principal Name) — уникальный идентификатор экземпляра сервиса. SPN используется аутентификацией Kerberos для сопоставления экземпляра сервиса с учетной записью сервиса (service logon account). Это позволяет клиентским приложением аутентифицироваться в роли сервиса даже не зная имени пользователя.

До того как аутентификация Kerberos сможет использовать SPN для аутентификации сервиса, SPN должен быть привязан к учётной записи, которая будет использоваться для входа. К учётной записи может быть привязано несколько SPN. SPN может быть привязан только к одной учетной записи. Если учетная запись, привязанная к SPN, изменяется, то необходимо заново выполнить привязку.

Можно иметь столько SPN, сколько необходимо. Когда клиент хочет воспользоваться сервисом, он находит экземпляр сервиса и составляет SPN для этого экземпляра, далее использует этот SPN для аутентификации. Если клиент не может найти правильный SPN, он не сможет запросить билет службы.

Примечание

Если клиент не может найти правильный SPN, он не сможет запросить билет службы. Поэтому формирование SPN было глобально нормализовано:

- для файлового сервера могут использоваться следующие SPN (их можно добавить столько, сколько нужно):
  - HOST/fileserver.test.alt
  - HOST/fileserver
  - HOST/fileserver@TEST.ALT
  - CIFS/fileserver.test.alt
- для веб-сервера (подробнее см. Настройка аутентификации для веб-сервера):
  - HTTP/web.test.alt
- для прокси-сервера:
  - HTTP/proxy.test.alt
- на практике можно сопоставить SPN с IP-адресом, но это не рекомендуется:
  - HOST/192168.0.129@TEST.ALT

Keytab-файл — это файл содержащий пары Kerberos принципалов и их ключей (полученных с использованием Kerberos пароля). Эти файлы используются для аутентификации в системах, использующих Kerberos, без ввода пароля. Если пароль принципала изменится, то keytab-файл необходимо будет сгенерировать заново.

Важно

Каждый кто имеет разрешения на чтения keytab-файла может воспользоваться любыми ключами в нем. Чтобы предотвратить нежелательное использование, необходимо ограничивать права доступа при создании keytab-файла.

6.2.1. Создание SPN и генерация keytab с помощью samba-tool

Добавить имена SPN для пользователя можно с помощью команды **samba-tool**:

```
samba-tool spn add host/fdqn@KerberosRealm <sAMAccount name>
```

После добавления SPN можно сгенерировать keytab, выполнив команду:

```
samba-tool domain exportkeytab <имя>.keytab --principal=[<sAMAccount name> |
<SPN>]
```

В результате выполнения этой команды будет создан keytab-файл **<имя>.keytab**, содержащий UPN или SPN, в зависимости от того, что было указано в параметре ***--principal***.

Получить дополнительную информацию можно на справочной странице samba-tool (8) (**man samba-tool**).

Примечание

В команде нужно использовать или <sAMAccount name> или <SPN>, но не оба параметра сразу,

Пример:

- привязать к пользователю SPN:

```
# samba-tool spn add HTTP/test.alt webauth
```

- создать keytab:

```
# samba-tool domain exportkeytab /tmp/web.keytab --principal=HTTP/test.alt
Export one principal to /tmp/keytab
```

- проверка:

```
# klist -ke /tmp/web.keytab
Keytab name: FILE:/tmp/web.keytab
KVNO Principal
----
---------------------------------------------------------------------------
   2 HTTP/test.alt@TEST.ALT (DEPRECATED:arcfour-hmac)
```

Также можно проверить авторизацию в домене по имени SPN с помощью keytab-файла. Для этого на контроллере домена получить билет Kerberos:

```
kinit administrator@TEST.ALT
Password for administrator@TEST.ALT:
```

И выполнить команду:

```
kinit -5 -V -k -t /tmp/web.keytab HTTP/test.alt
Using default cache: /tmp/krb5cc_0
Using principal: HTTP/test.alt@TEST.ALT
Using keytab: /tmp/web.keytab
Authenticated to Kerberos v5
```

Примечание

Если при проверке авторизации возникает ошибка:

```
kinit: Client not found in Kerberos database while getting initial
credentials
```

Необходимо в ADMC изменить для пользователя webauth значение параметра ***userPrincipalName*** на значение **servicePrincipalName + REALM** (в данном примере нужно поменять webauth на HTTP/test.alt@TEST.ALT).

Глава 7. Администрирование Samba

7.1. Управление пользователями и группами

7.1.1. В ADMC

Для управления пользователями и группами в AD можно использовать модуль удалённого управления базой данных конфигурации (ADMC). Подробнее см. Модуль удалённого управления базой данных конфигурации.

7.1.2. С помощью samba-tool

Для управления пользователями и группами в AD можно использовать инструмент командной строки **samba-tool**.

Таблица 7.1. Команды управления пользователями

Команда	Описание	Примечание
user add <имя пользователя> [<пароль>]	Создать нового пользователя в AD	
user create <имя пользователя> [<пароль>]	Создать нового пользователя в AD	Команда доступна только в целях совместимости. Рекомендуется вместо этой команды использовать команду **samba-tool user add**
user delete <имя пользователя> [<опции>]	Удалить существующего пользователя	
user disable <имя пользователя>	Отключить пользовательский аккаунт	
user edit <имя пользователя>	Редактировать объект пользовательского аккаунта AD	В опции **--editor=<редактор>** можно указать редактор (по умолчанию *vi*)
user enable <имя пользователя>	Включить пользовательский аккаунт	
user list	Вывести список пользователей	По умолчанию выводятся sAMAccountNames пользователей. Можно использовать следующие опции: - **--full-dn** — показать различающиеся имена пользователей (CN) вместо sAMAccountNames; - **-b BASE_DN|--base-dn=BASE_DN** — вывести пользователей с указанным базовым DN;

Команда	Описание	Примечание
		- **`--hide-expired`** — не выводить просроченные учётные записи пользователей; - **`--hide-disabled`** — не выводить отключенные учётные записи пользователей.
user setprimarygroup <имя пользователя> <имя группы>	Установить основную группу для учётной записи пользователя	
user getgroups <имя пользователя>	Вывести список групп, в которые входит учётная запись пользователя напрямую	
user show <имя пользователя>	Вывести пользовательский объект AD	В опции **`--attributes=USER_ATTRS`** можно указать, разделённый запятыми, список атрибутов
user move <имя пользователя> <контейнер>	Переместить учётную запись пользователя в указанную организационную единицу или контейнер	Имя пользователя указывается в команде в формате sAMAccountName. Имя организационной единицы или контейнера можно указать как полное DN или без компонента domainDN.
user password	Изменить пароль,указанной при аутентификации, учётной записи пользователя	
user rename <имя пользователя>	Переименовать пользователя и изменить его атрибуты	По умолчанию выводятся sAMAccountNames пользователей. Для удаления атрибута следует использовать пустое значение атрибута. Имя пользователя указывается в команде в формате sAMAccountName. Можно использовать следующие опции: - **`--surname=SURNAME`** — новая фамилия;

Команда	Описание	Примечание
		- **--given-name=GIVEN_NAME** — новое имя; - **--initials=INITIALS** — новые инициалы; - **--force-new-cn=NEW_CN** — новый CN (вместо использования комбинации имени, инициалов и фамилии); - **--reset-cn** — установить CN на комбинацию имени, инициалов и фамилии по умолчанию; - **--display-name=DISPLAY_NAME** — новое отображаемое имя; - **--mail-address=MAIL_ADDRESS** — новая электронная почта; - **--samaccountname=SAMACCOUNTNAME** — новое имя для входа (sAMAccountName); - **--upn=UPN** — новое основное имя пользователя.
user setexpiry <имя пользователя>	Установить срок действия для учётной записи пользователя	
user setpassword <имя пользователя>	Установить или сбросить пароль учетной записи пользователя	
user unlock <имя пользователя>	Разблокировать учётную запись пользователя в домене AD	
user getpassword <имя пользователя>	Получить атрибуты пароля учётной записи пользователя	
user syncpasswords --cache-ldb-initialize	Синхронизировать пароли всех учётных записей пользователей с помощью дополнительного сценария	Эта команда должна выполняться только на одном контроллере домена (обычно на PDC)

Примеры:

- Создать пользователя ivanov:

```
# samba-tool user create ivanov --given-name='Иван Иванов' --mail-
address='ivanov@test.alt'
New Password:
Retype Password:
User 'ivanov' added successfully
```

- Разблокировать пользователя ivanov:

```
# samba-tool user setexpiry ivanov --noexpiry
Expiry for user 'ivanov' disabled.
```

- Просмотреть доступных пользователей:

```
# samba-tool user list
Guest
ivanov
Administrator
krbtgt
```

- Отключить пользователя:

```
# samba-tool user disable ivanov
```

- Изменить пароль пользователя:

```
# samba-tool user setpassword ivanov
```

Предупреждение

Не следует допускать одинаковых имён для пользователя и компьютера, это может привести к коллизиям (например, такого пользователя нельзя добавить в группу). Если компьютер с таким именем заведён, удалить его можно командой: **`pdbedit -x -m имя`**

Таблица 7.2. Команды управления группами

Команда	Описание	Примечание
group add <имя группы> [<опции>]	Создать новую группу	
group create <имя группы> [<опции>]	Создать новую группу	Доступна только в целях совместимости. Рекомендуется вместо этой команды использовать команду **`samba-tool group add`**
group addmembers <имя группы> <участник> [<опции>]	Добавить участников в группу	
group delete <имя группы> [<опции>]	Удалить группу AD	
group edit <имя группы>	Редактировать объект группы AD	

Команда	Описание	Примечание
		В опции **`--editor=<редактор>`** можно указать редактор (по умолчанию *vi*)
group list	Вывести список групп	
group listmembers <имя группы> [<опции>]	Вывести список участников данной группы	По умолчанию выводятся sAMAccountNames участников. Если sAMAccountName недоступен, будет использоваться CN. Можно использовать следующие опции: - **`--full-dn`** — показать различающиеся имена участников (CN) вместо sAMAccountNames; - **`--hide-expired`** — не выводить членов группы с истекшим сроком действия; - **`--hide-disabled`** — не выводить отключённых членов группы.
group move <имя группы> <контейнер> [<опции>]	Переместить группу в указанную организационную единицу или контейнер	Имя группы указывается в команде в формате sAMAccountName. Имя организационной единицы или контейнера можно указать как полное DN или без компонента domainDN.
group removemembers <имя группы> <участник> [<опции>]	Удалить участника из группы	
group show <имя группы> [<опции>]	Вывести группу и её атрибуты	В опции **`--attributes=USER_ATTRS`** можно указать, разделённый запятыми, список атрибутов
group stats [<опции>]	Показать статистику для общих групп и членства в группах	
group rename <имя группы> [<опции>]	Переименовать группу и изменить её атрибуты	По умолчанию выводятся sAMAccountNames групп. Для удаления атрибута следует использовать пустое значение атрибута.

Команда	Описание	Примечание
		Имя группы указывается в команде в формате sAMAccountName. Можно использовать следующие опции: - **`--force-new-cn=NEW_CN`** — новый CN (вместо использования sAMAccountName); - **`--reset-cn`** — установить CN равным sAMAccountName; - **`--mail-address=MAIL_ADDRESS`** — новая электронная почта; - **`--samaccountname=SAMACCOUNTNAME`** — новое имя для входа (sAMAccountName);

Примеры:

- Добавить группу:

```
# samba-tool group add office
```

- Добавить UNIX-группу:

```
# samba-tool group add groupname --nis-domain=samdom --gid-number=<next
available GID>
```

- Удалить группу:

```
# samba-tool group delete office
```

- Добавить пользователя в группу:

```
# samba-tool group addmembers "Domain Users" user
# samba-tool group addmembers "Domain Users" user,user1,user2
```

- Удалить пользователя из группы:

```
# samba-tool group removemembers "Domain Users" user
```

- Вывести пользователей группы:

```
# samba-tool group listmembers "Domain Users" | grep ivanov
```

7.2. Резервное копирование и восстановление Samba AD DC

7.2.1. Восстановление произвольного контроллера домена после фатального сбоя

Если, в результате каких либо технических проблем, контроллер домена пришел в неработоспособное состояние, алгоритм его восстановления под тем же именем следующий:

1. Вывести контроллер домена из эксплуатации, путём удаления всей информации о нём. Для этого на любом работающем контроллере домена выполнить команду:

   ```
   # samba-tool domain demote --remove-other-dead-server=dc2 -UAdministrator
   ```

   где dc2 — имя (hostname) не функционирующего контроллера домена.

2. На узле, который будет заменой вышедшего из строя контроллера домена, выполнить следующие действия:

   - в файле **/etc/krb5.conf** указать опции **default_realm = TEST.ALT** и **dns_lookup_realm = false**;
   - остановить все зависимые службы:

     ```
     # for service in samba smb nmb krb5kdc slapd bind; do systemctl disable
     $service; systemctl stop $service; done
     ```

   - очистить всю конфигурацию Samba:

     ```
     # rm -f /etc/samba/smb.conf
     # rm -rf /var/lib/samba
     # rm -rf /var/cache/samba
     # mkdir -p /var/lib/samba/sysvol
     ```

   - ввести узел в домен как дополнительный контроллер домена:

     ```
     # samba-tool domain join test.alt DC --dns-backend=SAMBA_INTERNAL -
     Uadministrator --realm=test.alt
     ```

   - запустить samba и обновить dns:

     ```
     # systemctl enable --now samba
     # samba_dnsupdate --use-samba-tool --verbose
     ```

Важно

На других контроллерах домена в выводе команды **samba-tool drs showrepl** некоторое время будет присутствовать сообщение WERR_GEN_FAILURE в секции неисправного КД:

```
…
DC=DomainDnsZones,DC=test,DC=alt
  Default-First-Site-Name\DC2 via RPC
    DSA object GUID: b78f2c9d-5c62-4497-a5e1-4fc85aedf1cb
```

```
    Last attempt @ Wed Apr 24 07:51:24 2024 MSK failed, result 31
(WERR_GEN_FAILURE)
    28 consecutive failure(s).
    Last success @ NTTIME(0)

DC=ForestDnsZones,DC=test,DC=alt
  Default-First-Site-Name\DC2 via RPC
    DSA object GUID: b78f2c9d-5c62-4497-a5e1-4fc85aedf1cb
    Last attempt @ Wed Apr 24 07:51:24 2024 MSK failed, result 31
(WERR_GEN_FAILURE)
    28 consecutive failure(s).
    Last success @ NTTIME(0)
…
```

Это нормально, и через некоторое время после полной репликации оно исчезнет. Репликация может занять до нескольких часов.

7.2.2. Резервное копирование и восстановление из резервной копии

Резервные копии Samba позволяют восстановить домен Samba AD в случае сбоя работы. Резервное копирование отдельных контроллеров домена не выполняется.

Если контроллер домена используется и в качестве файлового сервера (что не рекомендуется), потребуется также создать отдельные резервные копии этих данных.

Есть несколько разновидностей резервного копирования:

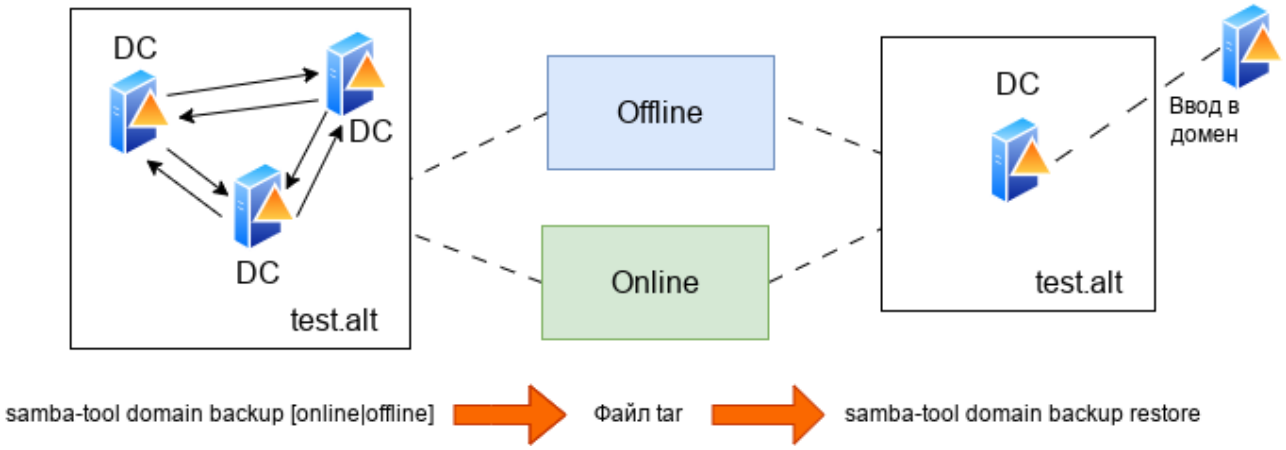
- *Online* — выполняется клонирование работающей базы данных DC. По функциональности это похоже на присоединение нового контроллера домена к сети;
- *Offline* (локальный) — резервные копии Samba создаются в том виде, в котором они появляются на диске. Сюда входят метаданные репликации, которые являются локальными для этого конкретного контроллера домена и которые не включаются в online резервные копии. Резервную копию также можно создать, когда контроллер домена находится в автономном режиме (т.е. процесс samba фактически не запущен).
- *Rename* (локальный) — создаётся файл резервной копии с переименованным доменом (предназначен только для временной замены).

Резервные копии можно создать, используя команду **`samba-tool domain backup`**. При этом будет создан файл резервной копии **`.tar.bz2`**, который будет содержать полную резервную копию домена (на основе данного контроллера домена). Этот файл резервной копии можно использовать для восстановления домена с помощью команды **`samba-tool domain backup restore`**.

Примечание

Следует иметь ввиду, что файл резервной копии — это резервная копия домена, а не контроллера домена. Восстановление файла резервной копии создаст новый DC с информацией о домене. Чтобы восстановить последующие контроллеры домена, необходимо присоединить новые контроллеры домена к восстановленному контроллеру домена.

7.2.2.1. Создание резервной копии в режиме онлайн/оффлайн режимах



7.2.2.1.1. Онлайн режим

Для создания резервной копии в режиме онлайн (*online*), следует выполнить команду:

```
# samba-tool domain backup online --targetdir=<output-dir> --server=<DC-server> -
UAdministrator
```

Эту команду можно запустить как локально на контроллере домена, так и удалённо на другом компьютере. При удалённом запуске можно указать параметр **`--configfile`**, чтобы в резервную копию были включены правильные настройки **`smb.conf`** (т.к. локальный файл **`smb.conf`** может не существовать или его настройки могут отличаться от настроек контроллера домена.

Пример создания резервной копии в режиме онлайн на контроллере домена:

```
# mkdir /var/samba-backup-online
# samba-tool domain backup online --targetdir=/var/samba-backup-online --
server=dc1 -UAdministrator
Password for [TEST\Administrator]:
workgroup is TEST
realm is test.alt
Looking up IPv4 addresses
Looking up IPv6 addresses
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
A Kerberos configuration suitable for Samba AD has been generated at /var/samba-
backup-online/tmpxqc6dwts/private/krb5.conf
Merge the contents of this file with your system krb5.conf or replace it with
this one. Do not create a symlink!
…
Creating backup file /var/samba-backup-online/samba-backup-
test.alt-2023-04-17T20-09-56.883910.tar.bz2..
```

7.2.2.1.2. Создание резервной копии в автономном режиме

Для создания автономной (*offline*) резервной копии, следует на контроллере домена выполнить команду:

```
# samba-tool domain backup offline --targetdir=<output-dir>
```

Примечание

Несмотря на название этого резервного копирования, контроллеру домена не нужно быть в автономном режиме при выполнении этой команды. Инструмент просто выполняет резервное копирование локальных файлов и имеет достаточную блокировку, чтобы гарантировать безопасное создание резервной копии.

Пример создания автономной резервной копии на контроллере домена:

```
# mkdir /var/samba-backup-offline
# samba-tool domain backup offline --targetdir=/var/samba-backup-offline
running backup on dirs: /var/lib/samba/private /var/lib/samba /etc/samba
Starting transaction on /var/lib/samba/private/secrets
Starting transaction on /var/lib/samba/private/sam.ldb
   backing up /var/lib/samba/private/sam.ldb

…
   adding misc file etc/lmhosts
   adding misc file etc/smb.conf
Backup succeeded.
```

7.2.2.1.3. Восстановление домена

Для восстановления домена из резервной копии необходимо выполнить следующие шаги:

1. Остановить **samba** на всех старых контроллерах домена. Этот шаг можно пропустить если используется не *Rename* резервная копия.
2. Запустить команду **samba-tool domain backup restore**, чтобы восстановить базу данных домена на одном новом контроллере домена.
3. Запустить **samba** на новом DC.
4. Повторно добавить старые контроллеры домена в сеть, присоединив их к восстановленному DC, например, командой

   ```
   samba-tool domain join <dns-realm> DC --server=<restored-dc>
   ```

5. Если используется *rename* резервная копия, также потребуется перенастроить сетевые устройства, так чтобы трафик перенаправлялся в восстановленный домен, а не в неисправный/исходный домен.

Примечание

> Из файла резервной копии восстанавливается весь домен, а не конкретный контроллера домена. Шаг с командой **samba-tool domain backup restore** выполняется только один раз, при этом домен воссоздается на одном контроллере домена. Затем все старые контроллеры домена должны быть повторно присоединены к восстановленному контроллеру домена.

7.2.2.1.3.1. Восстановление из файла резервной копии

Этап восстановления из файла резервной копии аналогичен разворачиванию домена, который выполнялся при первой настройке сети Samba, за исключением того, что резервная копия содержит в себе все объекты базы данных, которые были добавлены с момента создания домена. Как и при создании нового домена, при запуске команды восстановления домена потребуется указать новый контроллер домена. Этот контроллер домена не должен был существовать ранее в сети Samba.

Команда восстановления:

```
# samba-tool domain backup restore --backup-file=<tar-file> --newservername=<DC-name> --targetdir=<new-samba-dir>
```

Следует обратить внимание, что указанный целевой каталог должен быть пустым (или не должен существовать). Т.е. нецелесообразно восстанавливать базу данных домена в место установки по умолчанию (например, **/var/lib/samba**). Вместо этого рекомендуется восстановить базу данных домена в другой целевой каталог, а затем, при запуске samba, использовать параметр **-s** (или **--configfile**), например:

```
# samba -s <targetdir>/etc/smb.conf
```

Указание восстановленного **smb.conf** гарантирует, что Samba будет использовать файлы базы данных в правильном месте.

Восстановленный DC будет добавлен на сайт 'Default-First-Site-Name'. Этот сайт будет создан в восстановленной БД, если он еще не существует. Можно указать альтернативный сайт для добавления восстановленного контроллера домена с помощью параметра **--site**.

Перед запуском samba на восстановленном контроллере домена следует еще раз проверить правильность восстановленных настроек **smb.conf**.

Пример восстановления данных из резервной копии:

```
# mkdir /var/lib/samba/new
# samba-tool domain backup restore
--backup-file=/home/user/samba-backup-test.alt-2023-04-17T20-09-56.883910.tar.bz2
--newservername=newdc  --targetdir=/var/lib/samba/new
Adding new DC to site 'Default-First-Site-Name'
Updating basic smb.conf settings...
…
Backup file successfully restored to /var/lib/samba/new
Please check the smb.conf settings are correct before starting samba.
```

7.2.2.1.4. Рекомендуемая стратегия

Восстановление файла резервной копии имеет несколько неудобств:

- необходимость использовать другой каталог для установки по умолчанию;
- необходимо указать имя сервера DC, отличное от того, что было ранее в сети.

Свести эти неудобства к минимуму можно, используя временный сервер (или виртуальную машину) для восстановления контроллера домена:

- выполнить восстановление из файла резервной копии на временный контроллер домена и запустить Samba;
- повторно по одному присоединить исходные контроллеры домена к временному контроллеру домена (во время присоединения можно повторно использовать одно и то же имя сервера и место установки по умолчанию);
- после присоединения всех исходных контроллеров домена к восстановленному домену, можно удалить временный контроллер домена (например, с помощью команды **samba-tool domain demote**). В этом случае сеть контроллеров домена будет точно такой же, как и раньше.

Примечание

Пример разворачивания домена (SAMBA_INTERNAL) из резервной копии на ВМ:

1. Подготовить узел:
   - установить пакет *task-samba-dc* (или *task-samba-dc-mitkrb5*):

     ```
     # apt-get install task-samba-dc
     ```

   - остановить конфликтующие службы:

     ```
     # for service in smb nmb krb5kdc slapd bind; do systemctl disable
     $service; systemctl stop $service; done
     ```

   - очистить базы и конфигурацию Samba:

     ```
     # rm -f /etc/samba/smb.conf
     # rm -rf /var/lib/samba/*
     # rm -rf /var/cache/samba
     ```

2. Скопировать файл резервной копии на ВМ и выполнить восстановление домена из файла резервной копии:

   ```
   # samba-tool domain backup restore --backup-file=/home/user/samba-
   backup-test.alt-2023-04-17T20-09-56.883910.tar.bz2 --
   newservername=newdc --targetdir=/var/lib/samba
   Adding new DC to site 'Default-First-Site-Name'
   Updating basic smb.conf settings...
   …
   Backup file successfully restored to /var/lib/samba
   Please check the smb.conf settings are correct before starting samba.
   ```

3. Скопировать файл **smb.conf** из каталога **/var/lib/samba/etc/** в **/etc/samba/**:

```
# cp /var/lib/samba/etc/smb.conf /etc/samba/
```

4. Запустить Samba:

```
# systemctl enable --now samba
```

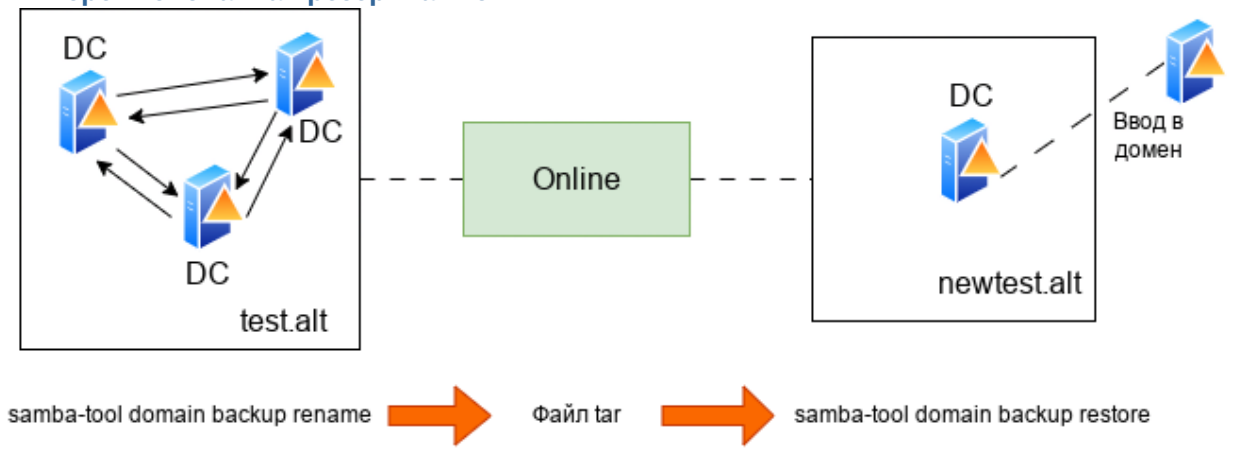
5. Заменить файл **/etc/krb5.conf** файлом из каталога **/var/lib/samba/private/**:

```
# cp /var/lib/samba/private/krb5.conf /etc/krb5.conf
```

6. Проверить работоспособность домена (см. Проверка работоспособности домена):

```
# samba-tool domain info 127.0.0.1
Forest           : test.alt
Domain           : test.alt
Netbios domain   : TEST
DC name          : newdc.test.alt
DC netbios name  : NEWDC
Server site      : Default-First-Site-Name
Client site      : Default-First-Site-Name

# smbclient -L localhost -Uadministrator
Password for [TEST\administrator]:

    Sharename       Type      Comment
    ---------       ----      -------
    sysvol          Disk
    netlogon        Disk
    share           Disk      Commonplace
    Free            Disk
    IPC$            IPC       IPC Service (Samba 4.19.4)
SMB1 disabled -- no workgroup available

# host -t SRV _kerberos._udp.test.alt.
_kerberos._udp.test.alt has SRV record 0 100 88 newdc.test.alt.
```

7.2.2.2. Переименованная резервная копия



Создание резервной копии в режиме переименования может применяться для:

- запуска временного альтернативного домена на случай катастрофического отказа основного домена. На альтернативный/переименованный домен можно переключиться с минимальными усилиями. Затем можно запустить два домена одновременно, не мешая друг другу (переименованный/альтернативный домен будет предоставлять основные сетевые службы Samba, в это же время на исходных контроллерах домена можно устранять неполадки);
- создания реалистичного лабораторного домена: домен переименовывается и удаляются конфиденциальные данные (на данный момент только самые важные), чтобы создать предпроизводственную среду для тестирования.

Переименование домена выполняется в два этапа:

- создание переименованной резервной копии домена: **samba-tool** делает клон работающей базы данных DC, в процессе клонирования переименовывает домен и создаёт файл резервной копии;
- восстановление резервной копии домена: **samba-tool** берет файл резервной копии и заполняет файлы, необходимые для запуска нового контроллера домена Samba.

7.2.2.2.1. Создание переименованной резервной копии

Команда для создания переименованной (*rename*) резервной копии:

```
# samba-tool domain backup rename <new-domain-netbios> <newdomain-dns-realm>
--server=<dc-to-backup> --targetdir=<output-dir> --no-secrets -UAdministrator
```

где

- new-domain-netbios — новое имя NETBIOS;
- newdomain-dns-realm — новая область DNS;
- output-dir — каталог, куда будет записан сгенерированный файл резервной копии.

Пример:

```
# mkdir /var/samba-backup-rename
# samba-tool domain backup rename NEWTEST newtest.alt --server=dc1 --targetdir=/
var/samba-backup-rename --no-secrets -UAdministrator
New realm for backed up domain: newtest.alt
New base DN for backed up domain: DC=newtest,DC=alt
New domain NetBIOS name: NEWTEST
Password for [TEST\Administrator]:
Provisioning the new (renamed) domain...
…
INFO 2023-04-17 20:19:06,012 pid:4195 /usr/lib64/samba-dc/python3.9/samba/netcmd/
domain_backup.py #815: Deleting old DNS zone
DC=test.alt,CN=MicrosoftDNS,DC=DomainDnsZones,DC=newtest,DC=alt
ERROR(ldb): uncaught exception - No Deleted Objects container for DN
DC=_msdcs,DC=test.alt,CN=MicrosoftDNS,DC=DomainDnsZones,DC=newtest,DC=alt
  File "/usr/lib64/samba-dc/python3.9/samba/netcmd/__init__.py", line 186, in
_run
    return self.run(*args, **kwargs)
  File "/usr/lib64/samba-dc/python3.9/samba/netcmd/domain_backup.py", line 925,
in run
```

```
    self.delete_old_dns_zones(logger, samdb, old_realm)
  File "/usr/lib64/samba-dc/python3.9/samba/netcmd/domain_backup.py", line 816,
in delete_old_dns_zones
    samdb.delete(dn, ["tree_delete:1"])
```

Предупреждение

Параметр **`--no-secrets`** исключает из резервной копии конфиденциальную информацию о паролях (например, такие атрибуты, как ***`unicodePwd`***, ***`lmPwdHistory`*** и т. д.) для всех пользователей в домене. При этом, файл резервной копии по-прежнему содержит конфиденциальную информацию, такую как имена учётных записей пользователей.

В случае, если команда создания резервной копии запускается на узле, который будет использоваться в качестве нового контроллера домена (он должен быть подключён к рабочему домену), рекомендуется иметь файл **`smb.conf`**, максимально соответствующий производственному контроллеру домена, и передать его команде резервного копирования (с помощью параметра **`--configfile=smb.conf`**). Это гарантирует, что резервная копия будет содержать **`smb.conf`**, точно соответствующий домену.

Если команда создания резервной копии запускается на другом узле, (например, на рабочем контроллере домена), необходимо скопировать сгенерированный файл резервной копии на узел, который будет использоваться в качестве нового контроллера домена.

7.2.2.2.2. Восстановление данных из резервной копии

Команда восстановления из резервной копии:

```
# mkdir /var/lib/samba/newtest
# samba-tool domain backup restore --targetdir=/var/lib/samba/newtest --
newservername=NEWDC1 --backup-file=/home/user/samba-backup-
test.alt-2023-04-17T20-09-56.883910.tar.bz2
```

Примечание

Целевой каталог должен быть пустым (или не должен существовать). Поэтому нецелесообразно восстанавливать базу данных домена в место установки по умолчанию (например, **`/var/lib/samba/`**). Однако можно указать подкаталог (например, **`/var/lib/samba/newtest/`**).

Примечание

Новый контроллер домена не может использовать то же имя сервера, что и контроллер домена в исходной сети.

7.2.2.2.3. Сброс пароля

Во время резервного копирования/восстановления пароль для учётной записи администратора сбрасывается на случайно сгенерированный пароль. Для его изменения можно просто обновить базу данных на локальном диске, выполнив команду:

```
# samba-tool user setpassword Administrator
--newpassword=<пароль>-H /var/lib/samba/newtest/private/sam.ldb
```

Для тестирования аутентификации пользователей можно либо добавить дополнительные «тестовые» учётные записи пользователей/машин, либо «командовать» некоторыми учётными записями, скопированными из рабочего домена. Для учётных записей, скопированных из рабочего домена, не будут установлены пароли, поэтому на этом этапе также можно сбросить пароли для выбранных учётных записей. Или можно сделать это позже, когда Samba действительно запустится на новом контроллере домена.

7.2.2.2.4. Запуск Samba

Перед запуском **samba** на новом контроллере домена, необходимо проверить правильность настроек **smb.conf** (например, **/var/lib/samba/newtest/etc/smb.conf**) и **/etc/krb5.conf**.

При запуске **samba** необходимо указать восстановленный **smb.conf** (это гарантирует, что Samba загрузит правильные файлы базы данных для нового домена). Например:

```
# samba -s /var/lib/samba/newtest/etc/smb.conf
```

При первом запуске **samba** могут быть зарегистрированы ошибки DNS. Это связано с тем, что **samba_dnsupdate** запускается автоматически и добавляет записи DNS для нового домена.

После запуска **samba** можно проверить правильность работы нового контроллера домена, например:

```
# ldbsearch -H ldap://NEWDC1 -UAdministrator
```

7.2.2.2.5. Обновление подсетей сайта

Новый домен будет содержать все сайты AD рабочего домена, но ни один из рабочих контроллеров домена. Однако подсети, которые используют эти сайты, скорее всего, больше не будут иметь смысла для экспериментального домена.

7.2.2.3. Отладочная информация

Если команда резервного копирования или восстановления завершится с ошибкой, то они могут оставить после себя временный каталог (указанный в параметре **--targetdir**). Это может помочь понять, почему произошел сбой. Необходимо удалить этот каталог перед повторным запуском команды восстановления.

Создание резервной копии:

- резервное копирование следует запускать от имени пользователя root. Онлайн-резервное копирование может быть успешным для пользователя без полномочий root, но при попытке восстановить данные из такой резервной копии могут возникнуть проблемы;
- для резервных копий выполненных в режиме «онлайн» или «переименования» следует проверите правильность используемых учётных данных и сведений о сервере. Например:

  ```
  # ldbsearch -H ldap://<server> -UAdministrator
  ```

- чтобы узнать больше информации о причине сбоя можно увеличить уровень журналирования. Например, добавить в команду параметр **`--debug=3`**;

- работа команд для выполнения резервного копирования в режиме «онлайн» или «переименование» очень похожа на присоединение к контроллеру домена. Если известно, что присоединение к контроллеру домена в вашей сети не удается, то эти команды также вряд ли будут работать. Сообщения «Committing SAM database» и «Cloned domain <domain>», говорят о том, что часть резервного копирования, подобная присоединению, скорее всего, выполнена успешно;

- инструменты резервного копирования не работают напрямую с контроллером домена Windows (в основном простое резервное копирование файлов sysvol не удается из-за блокировки службы DFSR). Если у вас смешанный домен контроллера домена, следует создать резервную копию контроллера домена Samba, а не контроллера домена Windows. Если у вас домен Windows, можно на время резервного копирования на контроллере домена остановить службу DFSR «Репликация DFS».

Восстановление из резервной копии:

- команду восстановления необходимо запускать от имени пользователя root;

- имя, указанное в параметре **`--newservername`**, не должно существовать в исходном домене. В противном ошибке вы получите ошибку вида:

```
Adding CN=NEWDC,OU=Domain Controllers,DC=test,DC=alt
ERROR(ldb): uncaught exception - Entry CN=NEWDC,OU=Domain
Controllers,DC=test,DC=alt already exists
  File "/usr/lib64/samba-dc/python3.9/samba/netcmd/__init__.py", line 186, in
_run
    return self.run(*args, **kwargs)
  File "/usr/lib64/samba-dc/python3.9/samba/netcmd/domain_backup.py", line
562, in run
    ctx.join_add_objects(specified_sid=dom_sid(str(sid)))
  File "/usr/lib64/samba-dc/python3.9/samba/join.py", line 674, in
join_add_objects
    ctx.samdb.add(rec, controls=controls)
```

- если команда резервного копирования выполнялась локально на контроллере домена, то файл резервной копии должен содержать файл **`smb.conf`** контроллера домена. Однако **`smb.conf`** в файле резервной копии может содержать конфигурацию «интерфейсов», которая не соответствует IP-адресам на DC, на котором разворачиваются данные из резервной копии. Избежать этой проблемы можно, указав аргумент **`--host-ip`** во время восстановления (это имеет значение только на переименованных резервных копий).

7.3. Роли FSMO

FSMO, или Flexible single-master operations (операции с одним исполнителем) — это операции, выполняемые контроллерами домена AD, которые требуют обязательной уникальности сервера для каждой операции. В зависимости от типа операции уникальность FSMO подразумевается в пределах одного домена или леса доменов. Различные типы FSMO могут выполняться как на одном, так и на нескольких контроллерах домена. Выполнение FSMO сервером называют ролью сервера, а сами сервера — хозяевами операций.

Active Directory — это центральный репозиторий, в котором хранятся все объекты и соответствующие им атрибуты. Это иерархическая база данных с поддержкой нескольких источников. Большинство операций в AD можно выполнять на любом контроллере домена. Служба репликации AD скопирует изменения на остальные контролеры домена, обеспечив идентичность базы AD на всех контролерах одного домена. Один из способов разрешения конфликтов заключается в том, что сохраняются изменения, внесенные последними. Изменения, внесенные остальными контроллерами домена, игнорируются.

Однако существует несколько операций (например, изменение схемы AD), при которых конфликты недопустимы. В AD некоторые обновления выполняются на одном специальном контроллере домена, а затем реплицируются на все остальные. AD использует роли, назначенные контроллерам домена, для этих специальных задач. Так как роль не привязана к одному контроллеру домена, она называется ролью FSMO.

В настоящее время существует семь ролей FSMO с разными областями действия:

- *Эмулятор PDC/PDC Emulator* (один на домен);
- *Хозяин RID/RID Master* (один на домен);
- *Хозяин схемы/Schema Master* (один на лес);
- *Хозяин именования доменов/Domain Naming Master* (один на лес);
- *Хозяин инфраструктуры/Infrastructure Master* (один на домен);
- *Хозяин зоны DNS домена/Domain DNS Zone Master role* (один на домен) ;
- *Хозяин зоны DNS леса/Forest DNS Zone Master role* (один на лес).

7.3.1. Семь ролей FSMO

Ниже описаны роли FSMO, их функции и требования к доступности. Эти сведения позволяют определить последствия, когда контроллер домена, владеющий этой ролью, находится в автономном режиме.

7.3.1.1. Эмулятор PDC

Владелец роли эмулятора PDC отвечает за следующие задачи в домене:

- является сервером точного времени для клиентов в домене. Для аутентификации Kerberos необходима точная синхронизация времени. Эмулятор PDC корневого домена в лесу является по умолчанию сервером точного времени для эмуляторов PDC в дочерних доменах;
- изменения паролей, внесенные другими контроллерами домена в домене, реплицируются преимущественно в эмулятор PDC. В случае недоступности эмулятора PDC информация об изменении пароля всё равно распространится по домену, просто произойдет это несколько медленнее;
- выполняет все функции, предоставляемые PDC в стиле NT4;
- обрабатывает блокировки учетных записей. Сбои аутентификации на любом контроллере домена в домене, вызванные неправильным паролем, перенаправляются в эмулятор PDC до того, как сообщение о сбое из-за неправильного пароля будет передано пользователю. При успешной аутентификации учётной записи сразу после неудачной попытки, о ней уведомляется эмулятор PDC и сбрасывает счетчик неудачных попыток в ноль;

- консоль управления групповыми политиками по умолчанию соединяется с эмулятором PDC, и изменения политик происходят на нем же. Если эмулятор PDC недоступен, то будет нужно указать редактору, к какому контроллеру домена подключиться;
- в больших средах контроллер домена, которому принадлежит роль эмулятора PDC, может иметь высокую загрузку ЦП из-за сквозной аутентификации, смены пароля и синхронизации времени.

На каждый домен приходится один эмулятор PDC.

Этот контроллер домена должен, по возможности, быть доступен всегда, потому что для Kerberos требуется точное время на всех машинах в домене. Если клиенты настроены на использование другого источника времени и в сети нет клиентов до Windows 2000, временное отсутствие может быть менее критичным.

Для поиска эмулятора PDC можно использовать команду **`host`**:

```
# host -t SRV _ldap._tcp.pdc._msdcs.<домен>
```

Например:

```
# host -t SRV _ldap._tcp.pdc._msdcs.test.alt
_ldap._tcp.pdc._msdcs.test.alt has SRV record 0 100 389 dc1.test.alt.
```

7.3.1.2. Хозяин RID

Владелец роли FSMO хозяина RID отвечает за обработку запросов пула RID от всех DC в домене. Он также отвечает за перемещение объектов в другой домен и удаление их из домена.

Все объекты безопасности, например, учётные записи и группы пользователей/компьютеров имеют уникальный идентификатор безопасности (SID). SID объектов содержит идентификатор безопасности (SID) домена, одинаковый для всех объектов в домене, и относительный идентификатор (RID), уникальный для каждого идентификатора безопасности субъекта безопасности, созданного в домене.

Каждому контроллеру домена в домене выделяется пул относительных идентификаторов RID, которые разрешено назначать созданным субъектам безопасности. По умолчанию это диапазон из 500 уникальных RID для всего домена, назначаемых хозяином RID каждому контроллеру домена. Если объект безопасности создается на контроллере домена, то RID берется из этого пула, что гарантирует его уникальность в домене. Если выделенный пул RID контроллера домена оказывается ниже порогового значения (ниже 50 %), контроллер домена выполняет запрос дополнительных идентификаторов RID к хозяину RID в домене. Хозяин RID в домене отвечает на запрос, извлекая идентификаторы RID из невыделенного пула RID домена и назначая их пулу запрашивающего контроллера домена.

На каждый домен приходится один хозяин RID.

Этот контроллер домена должен быть активен, при создании нового контроллера домена в домене, чтобы назначить ему пул RID. Также хозяин RID должен быть доступен, когда существующие контроллеры домена обновляют свой резервный пул RID.

С другой стороны, если хозяин RID находится в автономном режиме, то на каждом контроллере домена можно создавать новые объекты безопасности, пока локальный пул RID не станет пустым. Если пулы RID на всех контроллерах домена опустеют, создание дополнительных объектов станет невозможно. Также пока хозяин RID домена находится в автономном режиме невозможно присоединиться к дополнительным контроллерам домена,

7.3.1.3. Хозяин схемы

Контроллер домена, обладающий ролью хозяина схемы, является единственным в лесу AD, кому разрешено обновлять схему каталога. После завершения обновления изменения реплицируются на все другие контроллеры домена в лесу.

Схема каталога (контекст именования схемы) или LDAP://cn=schema,cn=configuration,dc=<домен> существует на всех контроллерах домена. Обновления выполняются только на хозяине схемы. После завершения обновления схема реплицируется из хозяина схемы во все остальные контроллеры домена каталога.

В каждом лесу есть один хозяин схемы.

Этот контроллер домена должен быть подключен к сети при выполнении обновлений схемы.

7.3.1.4. Хозяин именования доменов

Хозяин именования доменов отвечает за внесение изменений в пространство доменных имен в масштабах леса. Только этот контроллер домена может добавлять или удалять домены, доверительные отношения с внешними каталогами и разделами приложений в/из леса.

Информация об именах доменов хранится в разделе «Контекст именования конфигурации» в CN=Partitions,CN=Configuration,DC=<домен>. Этот раздел существует на всех контроллерах домена, но обновляется только на хозяине именования доменов.

На каждый лес приходится один хозяин именования доменов.

Этот контроллер домена должен быть подключен к сети, когда устанавливаются доверительные отношения с внешними каталогами и доменами, а разделы приложений добавляются или удаляются из леса.

7.3.1.5. Хозяин инфраструктуры

Контроллер домена, которому принадлежит роль хозяина инфраструктуры, отвечающий за обновление идентификатора безопасности (SID) и различающегося имени объекта в ссылке на междоменный объект. Это используется, например, если пользователь из одного домена добавляется в группу безопасности другого домена.

На каждый домен приходится один хозяин инфраструктуры.

Если этот контроллер домена временно отключен, междоменные изменения невозможны.

7.3.1.6. Хозяин зоны DNS домена

Контроллер домена, которому принадлежит роль хозяина зоны DNS домена, отвечает за координацию добавления или удаления любых зон DNS, интегрированных в AD, на контроллерах домена с DNS-серверами, на которых размещен домен.

На каждый домен приходится один хозяин зоны DNS домена.

7.3.1.7. Хозяин зоны DNS леса

Контроллер домена, которому принадлежит роль хозяина зоны DNS леса, отвечает за координацию добавления или удаления записей всего леса на DNS-серверах, на которых размещена зона DNS верхнего уровня. Эти записи содержат имена серверов глобального каталога (GC).

На каждый домен приходится один хозяин зоны DNS леса.

7.3.2. Просмотр и передача ролей FSMO

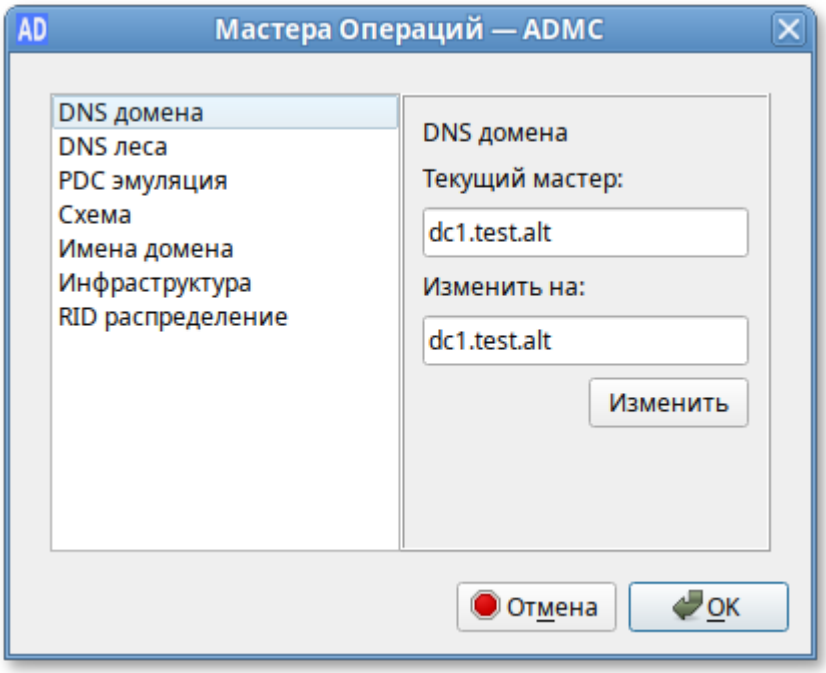
По возможности следует передавать роли FSMO штатным образом и не использовать принудительную передачу (захват роли). Для штатной передачи роли требуется, чтобы контроллер домена, которому в данный момент принадлежит роль, работал и был подключен к сети. В этом случае при передаче роли старый контроллер домена узнает, что он больше не владеет ролью.

Если контроллер домена сломан (например, из-за аппаратного дефекта) и больше никогда не будет возвращён в сеть, можно использовать принудительную передачу (захватить роль на оставшемся контроллере домена). Если старый контроллер домена будет снова подключён к сети, это вызовет конфликты и приведет к неконсистентному AD (т.к. старый контроллер домена не заметит изменения и по-прежнему будет считать себя владельцем роли).

Роли FSMO можно передавать с помощью инструмента командной строки **`samba-tool`** или в модуле удалённого управления базой данных конфигурации (ADMC) (подробнее см. Модуль удалённого управления базой данных конфигурации).

7.3.2.1. ADMC

Для просмотра текущего владельца роли необходимо выбрать пункт меню **Файл** → **Мастера Операций**. В открывшемся окне в списке слева выбрать роль и в поле **`Текущий мастер`** будет показан владелец роли:

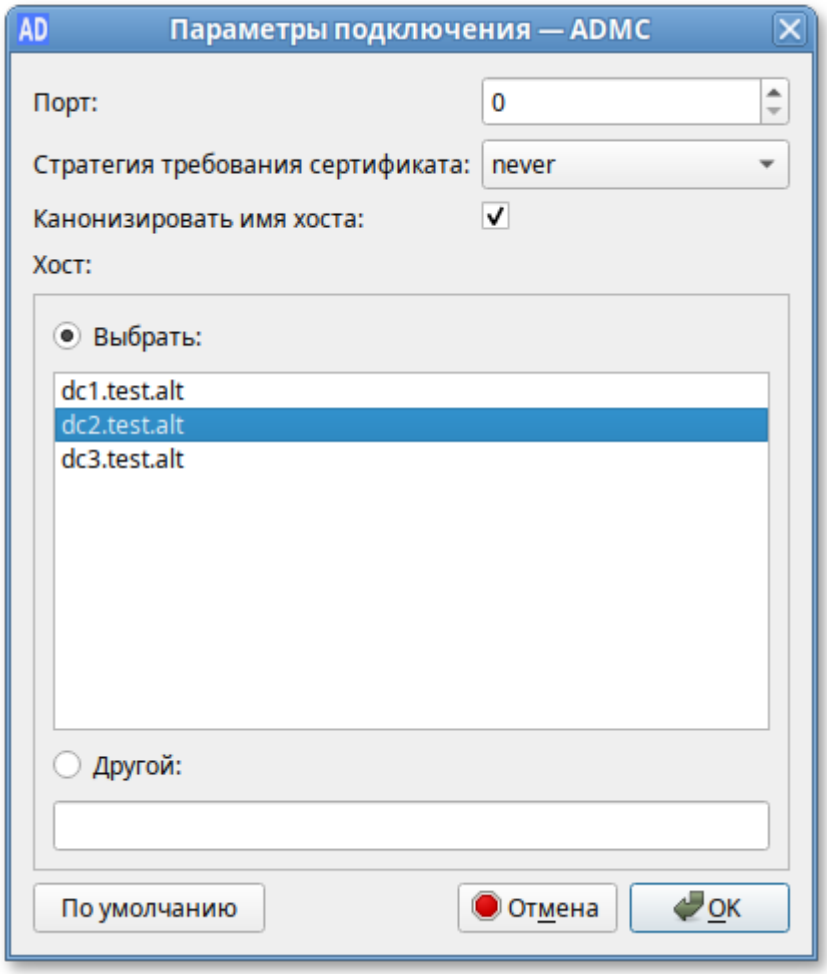


Список возможных ролей:

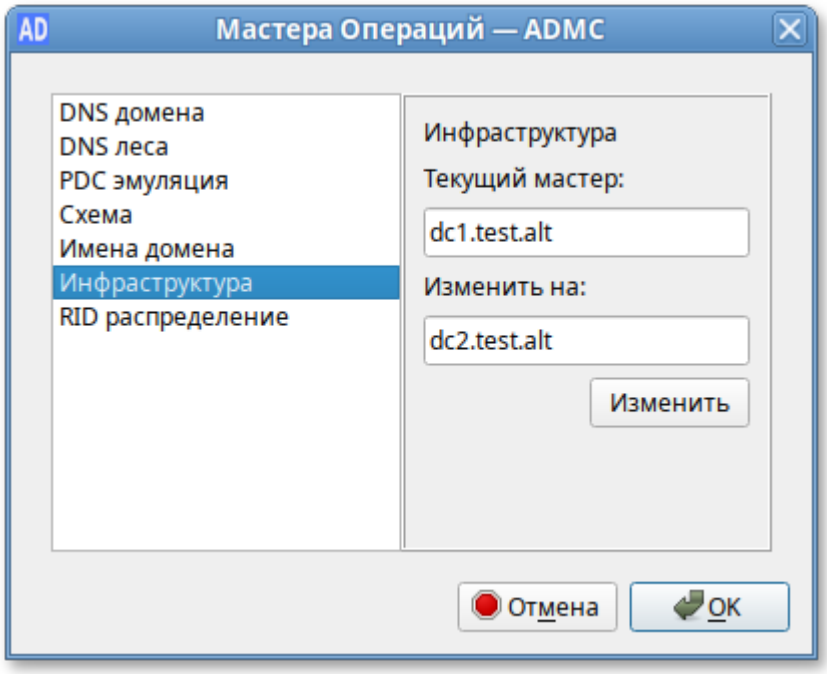
1. **DNS домена** — хозяин зоны DNS домена;
2. **DNS леса** — хозяин зоны DNS леса;
3. **PDC эмуляция** — эмулятор PDC;
4. **Схема** — хозяин схемы;
5. **Имена домена** — хозяин именования доменов;
6. **Инфраструктура** — хозяин инфраструктуры;
7. **RID распределение** — хозяин RID.

Для штатной передачи роли необходимо выполнить следующие действия:

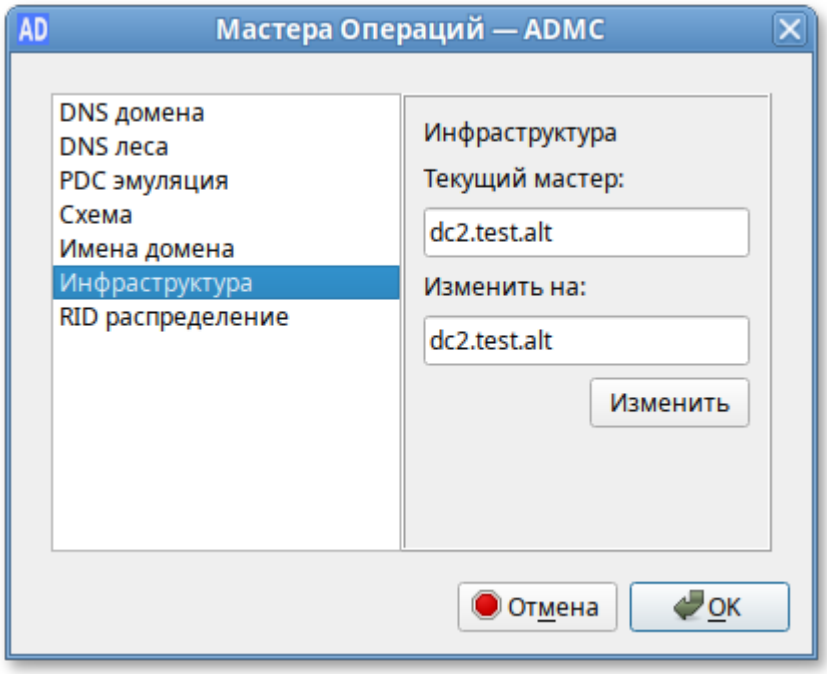
1. В окне **Параметры подключения — ADMC** (**Файл** → **Параметры подключения**) выбрать контроллер домена, который должен стать новым владельцем роли и нажать кнопку **OK**:



2. В окне **Мастера Операций — ADMC** (**Файл** → **Мастера Операций**) выбрать роль (при этом в поле **Текущий мастер** будет показан текущий владелец роли, а в поле **Изменить на** — контроллер домена, который должен стать новым владельцем роли) и нажать кнопку **Изменить**:



Владелец роли будет изменён:



7.3.2.2. Инструмент samba-tool

Просмотр текущего состояния (команда выполняется на контроллере домена):

```
# samba-tool fsmo show
SchemaMasterRole owner: CN=NTDS Settings,CN=DC1,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=test,DC=alt
InfrastructureMasterRole owner: CN=NTDS Settings,CN=DC1,CN=Servers,CN=Default-
First-Site-Name,CN=Sites,CN=Configuration,DC=test,DC=alt
RidAllocationMasterRole owner: CN=NTDS Settings,CN=DC1,CN=Servers,CN=Default-
First-Site-Name,CN=Sites,CN=Configuration,DC=test,DC=alt
PdcEmulationMasterRole owner: CN=NTDS Settings,CN=DC1,CN=Servers,CN=Default-
```

```
First-Site-Name,CN=Sites,CN=Configuration,DC=test,DC=alt
DomainNamingMasterRole owner: CN=NTDS Settings,CN=DC1,CN=Servers,CN=Default-
First-Site-Name,CN=Sites,CN=Configuration,DC=test,DC=alt
DomainDnsZonesMasterRole owner: CN=NTDS Settings,CN=DC1,CN=Servers,CN=Default-
First-Site-Name,CN=Sites,CN=Configuration,DC=test,DC=alt
ForestDnsZonesMasterRole owner: CN=NTDS Settings,CN=DC1,CN=Servers,CN=Default-
First-Site-Name,CN=Sites,CN=Configuration,DC=test,DC=alt
```

Для штатной передачи роли необходимо на контроллере домена, который должен стать новым владельцем роли выполнить команду:

```
# samba-tool fsmo transfer --role=<роль>
```

Список возможных ролей:

- rid — хозяин RID (RidAllocationMasterRole);
- pdc — эмулятор PDC (PdcEmulationMasterRole);
- infrastructure — хозяин инфраструктуры (InfrastructureMasterRole);
- schema — хозяин схемы (SchemaMasterRole);
- naming — хозяин именования доменов (DomainNamingMasterRole);
- domaindns — хозяин зоны DNS домена (DomainDnsZonesMasterRole);
- forestdns — хозяин зоны DNS домена (ForestDnsZonesMasterRole);
- all — все роли.

Пример штатной передачи роли (команда выполняется на DC2):

```
# samba-tool fsmo transfer --role=infrastructure
FSMO transfer of 'infrastructure' role successful
```

Проверка:

```
# samba-tool fsmo show
SchemaMasterRole owner: CN=NTDS Settings,CN=DC1,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=test,DC=alt
InfrastructureMasterRole owner: CN=NTDS Settings,CN=DC2,CN=Servers,CN=Default-
First-Site-Name,CN=Sites,CN=Configuration,DC=test,DC=alt
RidAllocationMasterRole owner: CN=NTDS Settings,CN=DC1,CN=Servers,CN=Default-
First-Site-Name,CN=Sites,CN=Configuration,DC=test,DC=alt
PdcEmulationMasterRole owner: CN=NTDS Settings,CN=DC1,CN=Servers,CN=Default-
First-Site-Name,CN=Sites,CN=Configuration,DC=test,DC=alt
DomainNamingMasterRole owner: CN=NTDS Settings,CN=DC1,CN=Servers,CN=Default-
First-Site-Name,CN=Sites,CN=Configuration,DC=test,DC=alt
DomainDnsZonesMasterRole owner: CN=NTDS Settings,CN=DC1,CN=Servers,CN=Default-
First-Site-Name,CN=Sites,CN=Configuration,DC=test,DC=alt
ForestDnsZonesMasterRole owner: CN=NTDS Settings,CN=DC1,CN=Servers,CN=Default-
First-Site-Name,CN=Sites,CN=Configuration,DC=test,DC=alt
```

Для принудительной передачи роли (если контроллер домена вышел из строя) необходимо на контроллере домена, который должен стать новым владельцем роли выполнить команду:

```
# samba-tool fsmo seize --role=<роль>
```

Важно

Если роль была передана принудительно, старый контроллер домена больше никогда не должен подключаться к сети!

Примечание

При передаче ролей *domaindns* и *forestdns* необходимо предоставить аутентификацию.

Примечание

В ранних версиях **samba-tool** была ошибка, не позволявшая захватить роль *naming*:

```
# samba-tool fsmo seize --role=naming
ERROR (ldb): uncaught exception – Failed FSMO transfer: WERR_BADFILE
```

В этом случае необходимо использовать «ещё более принудительную передачу»:

```
# samba-tool fsmo seize --force --role=naming
```

7.4. Настройка Samba для привязки к определённым интерфейсам

Если на сервере настроено несколько сетевых интерфейсов, можно настроить Samba для привязки только к определенным интерфейсам.

Например, для того чтобы привязать все службы Samba к устройству enp0s3 и loopback (lo) необходимо добавить следующие параметры в раздел ***[global]*** файла **smb.conf**:

```
bind interfaces only = yes
interfaces = lo enp0s3
```

и перезапустить службу Samba:

```
# systemctl restart samba.service
```

В параметре **interfaces** вместо имён интерфейсов можно указывать IP-адреса.

Примечание

Некоторые утилиты подключаются к петлевому IP-адресу, если имя хоста не указано. Поэтому всегда нужно указывать Samba прослушивать петлевые (lo) устройства.

7.5. Аутентификация других сервисов в Samba AD

7.5.1. Настройка аутентификации Kerberos для веб-сервера Apache

В этом разделе показано, как обеспечить прозрачную авторизацию пользователей домена на веб-сайте, размещенном на веб-сервере Apache2.

В качестве веб-сервера используется отдельный сервер (web.test.alt, IP-адрес 192.168.0.150), введенный в домен.

Примечание

Веб-сервер может быть присоединен или не присоединен к домену, это не имеет значения.

Добавить зону обратного просмотра для подсети 192.168.0.0/24, в которой располагается веб-сервер:

```
# samba-tool dns zonecreate dc1 0.168.192.in-addr.arpa -Uadministrator
Password for [TEST\administrator]:
Zone 0.168.192.in-addr.arpa created successfully
```

где dc1 — имя контроллера домена.

Если требуется более одной обратной зоны (при использовании нескольких подсетей), следует запустить приведенную выше команду еще раз, но с данными для другой подсети.

Обратная зона работает напрямую без перезапуска Samba или BIND.

Добавить зону обратного просмотра для веб-сервера:

```
# samba-tool dns add dc1 0.168.192.in-addr.arpa 150 PTR web.test.alt
```

7.5.1.1. Создание keytab-файла

Нужно настроить SPN (имена участников-служб) для имени сервера, на которое разрешается любой веб-сайт (подробнее см. Создание keytab-файла). Если виртуальный хостинг не используется, веб-адрес и имя машины будут одинаковыми. Для создания SPN на контроллере домена выполнить команды:

```
# samba-tool user create --random-password webauth
# samba-tool user setexpiry webauth
# samba-tool spn add HTTP/web.test.alt webauth
```

Создать Kerberos keytab файл для Apache2:

```
# samba-tool domain exportkeytab /tmp/httpd.keytab --principal=HTTP/
web.test.alt@TEST.ALT
Export one principal to /tmp/httpd.keytab
```

Перенести полученный файл keytab на веб-сервер в **/etc/httpd2/conf/**, установить права на него, так чтобы apache мог читать, но не изменять keytab-файл:

```
# chown root:apache /etc/httpd2/conf/httpd.keytab
# chmod 640 /etc/httpd2/conf/httpd.keytab
```

7.5.1.2. Настройка Apache2

На веб-сервере установить пакет *apache2-mod_auth_gssapi* и включить необходимые модули:

```
# apt-get install apache2-mod_auth_gssapi
# a2enmod auth_gssapi
# a2enmod authn_core
# a2enmod authz_user
# service httpd2 condreload
```

Добавить в конфигурацию Apache строки:

```
<Location "/login.html">
        AuthType GSSAPI
        AuthName "GSSAPI Login"
        #GssapiBasicAuth On
        GssapiCredStore keytab:/etc/httpd2/conf/httpd.keytab
        GssapiAllowedMech krb5
        Require valid-user
</Location>
```

Перезапустить Apache:

```
# systemctl restart httpd2
```

7.5.1.3. Проверка аутентификации

Тестовый сайт должен быть доступен по адресу http://<полное_доменное_имя_веб-сервера>.

На рабочей станции, введённой в домен, получить билет Kerberos:

```
$ kinit ivanov
Password for ivanov@TEST.ALT:
$ klist
Ticket cache: KEYRING:persistent:500:krb_ccache_5VitJSL
Default principal: ivanov@TEST.ALT

Valid starting       Expires              Service principal
28.04.2023 15:54:41  29.04.2023 01:54:41  krbtgt/TEST.ALT@TEST.ALT
    renew until 05.05.2023 15:54:38
```

Попытаться прочитать содержимое сайта, используя аутентификацию Kerberos:

```
$ curl --negotiate -u : http://web.test.alt/login.html
<html><body><h1>It works!</h1></body></html>
```

Получено содержимое страницы.

Удалить билеты Kerberos:

```
$ kdestroy
$ klist
```

Попытаться прочитать содержимое сайта, используя аутентификацию Kerberos:

```
$ curl --negotiate -u : http://web.test.alt/login.html
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
  "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" lang="en" xml:lang="en">
<head>
<title>Authentication required!</title>
</head>

<body>
<h1>Authentication required!</h1>
…
<h2>Error 401</h2>
<address>
  <a href="/">web.test.alt</a><br />
  <span>Apache/2.4.57 (Unix) mod_auth_gssapi/1.6.3 OpenSSL/1.1.1u</span>
</address>
</body>
</html>
```

Содержимое страницы не доступно.

7.5.2. Настройка аутентификации Kerberos для веб-сервера Nginx

В этом разделе показано, как обеспечить прозрачную авторизацию пользователей домена на веб-сайте, размещенном на веб-сервере Nginx.

В качестве веб-сервера используется отдельный сервер (web.test.alt, IP-адрес 192.168.0.150), введенный в домен.

Примечание

Веб-сервер может быть присоединен или не присоединен к домену, это не имеет значения.

Добавить зону обратного просмотра для подсети 192.168.0.0/24, в которой располагается веб-сервер:

```
# samba-tool dns zonecreate dc1 0.168.192.in-addr.arpa -Uadministrator
Password for [TEST\administrator]:
Zone 0.168.192.in-addr.arpa created successfully
```

где dc1 — имя контроллера домена.

Если требуется более одной обратной зоны (при использовании нескольких подсетей), следует запустить приведенную выше команду еще раз, но с данными для другой подсети.

Обратная зона работает напрямую без перезапуска Samba или BIND.

Добавить зону обратного просмотра для веб-сервера:

```
# samba-tool dns add dc1 0.168.192.in-addr.arpa 150 PTR web.test.alt
```

7.5.2.1. Создание keytab-файла

Подробнее см. Создание keytab-файла.

Нужно настроить SPN (имена участников-служб) для имени сервера, на которое разрешается любой веб-сайт (таким образом, фактическое имя сервера, на которое указывает CNAME, является полным). Если виртуальный хостинг не используется, веб-адрес и имя машины будут одинаковыми. Для этого на контроллере домена:

```
# samba-tool user create --random-password nginxauth
# samba-tool user setexpiry nginxauth
# samba-tool spn add HTTP/web.test.alt nginxauth
```

Создать Kerberos keytab файл для Nginx:

```
# samba-tool domain exportkeytab /tmp/nginx.keytab --principal=HTTP/
web.test.alt@TEST.ALT
Export one principal to /tmp/nginx.keytab
```

7.5.2.2. Настройка Nginx

Для работы прозрачной доменной аутентификации (SSO) в nginx необходимо установить пакеты *nginx* и *nginx-spnego*:

```
# apt-get install nginx nginx-spnego
```

Модуль SPNEGO для Nginx — это программный компонент для возможности прохождения аутентификации (Single Sign-On или SSO) через сервер LDAP.

Включить модуль http_auth_spnego:

```
# ln -s /etc/nginx/modules-available.d/http_auth_spnego.conf /etc/nginx/modules-
enabled.d/
```

Перенести полученный на контроллере домене файл keytab на веб-сервер в **`/etc/nginx`**. Установить права на файл keytab:

```
# chmod 644 /etc/nginx/nginx.keytab
```

Nginx должен иметь права на чтение keytab-файла, но не на его изменение.

Настроить аутентификацию в секции server файла конфигурации сайта:

```
server {
    …
    location /
    {
        root /var/www/html;
        auth_gss on;
        auth_gss_realm TEST.ALT; #имя kerberos области
        auth_gss_keytab /etc/nginx/nginx.keytab; #путь к keytab-файлу
        auth_gss_service_name HTTP/web.test.alt; #имя используемого SPN
        auth_gss_allow_basic_fallback off;
    }
}
```

Описание опций:

- ***auth_gss*** — включение/отключение аутентификации;
- ***auth_gss_keytab*** — абсолютный путь к файлу keytab, содержащему учётные данные службы;
- ***auth_gss_realm*** — имя области Kerberos;
- ***auth_gss_service_name*** — имя субъекта-службы, используемое при получении учетных данных;
- ***auth_gss_allow_basic_fallback*** — включить/отключить базовую аутентификацию. При включённой базовой аутентификации (по умолчанию), если SSO не проходит (машина не в домене) разрешает обычный ввод логина и пароля. Если используется SPNEGO без SSL, рекомендуется отключить базовую аутентификацию, так как в этом случае пароль будет отправлен в виде открытого текста.

Перезапустить nginx:

```
# systemctl restart nginx
```

Если нужно авторизовать только определенный набор пользователей, можно использовать параметре ***auth_gss_authorized_principal***. Можно указывать несколько записей, по одной на строку:

```
auth_gss_authorized_principal <username>@<realm>
auth_gss_authorized_principal <username2>@<realm>
```

Список пользователей также можно указать с помощью шаблона регулярного выражения в параметре ***auth_gss_authorized_principal_regex***. Этот параметр можно использовать вместе с параметром ***auth_gss_authorized_principal***:

```
auth_gss_authorized_principal <username>@<realm>
auth_gss_authorized_principal_regex ^(<username>)/(<group>)@<realm>$
```

7.5.2.3. Проверка аутентификации

Тестовый сайт должен быть доступен по адресу http://<полное_доменное_имя_веб-сервера>.

На рабочей станции, введённой в домен, получить билет Kerberos:

```
$ kinit ivanov
Password for ivanov@TEST.ALT:
$ klist
Ticket cache: KEYRING:persistent:500:krb_ccache_5VitJSL
Default principal: ivanov@TEST.ALT

Valid starting       Expires              Service principal
28.04.2023 15:54:41  29.04.2023 01:54:41  krbtgt/TEST.ALT@TEST.ALT
    renew until 05.05.2023 15:54:38
```

Попытаться прочитать содержимое сайта, используя аутентификацию Kerberos:

```
$ curl --negotiate -u : http://web.test.alt
<html><body><h1>It works!</h1></body></html>
```

Получено содержимое страницы.

Удалить билеты Kerberos:

```
$ kdestroy
$ klist
```

Попытаться прочитать содержимое сайта, используя аутентификацию Kerberos:

```
$ curl --negotiate -u : http://web.test.alt
<html>
<head><title>401 Authorization Required</title></head>
<body>
<center><h1>401 Authorization Required</h1></center>
<hr><center>nginx/1.22.1</center>
</body>
</html>
```

Содержимое страницы не доступно.

7.5.3. Настройка браузеров для SSO

Предварительно необходимо ввести компьютер в домен (см. Подключение к AD) и убедиться, что доменный пользователь получает билет Kerberos.

Для работы SSO в браузерах необходимо произвести некоторые настройки.

7.5.3.1. Настройка Mozilla Firefox

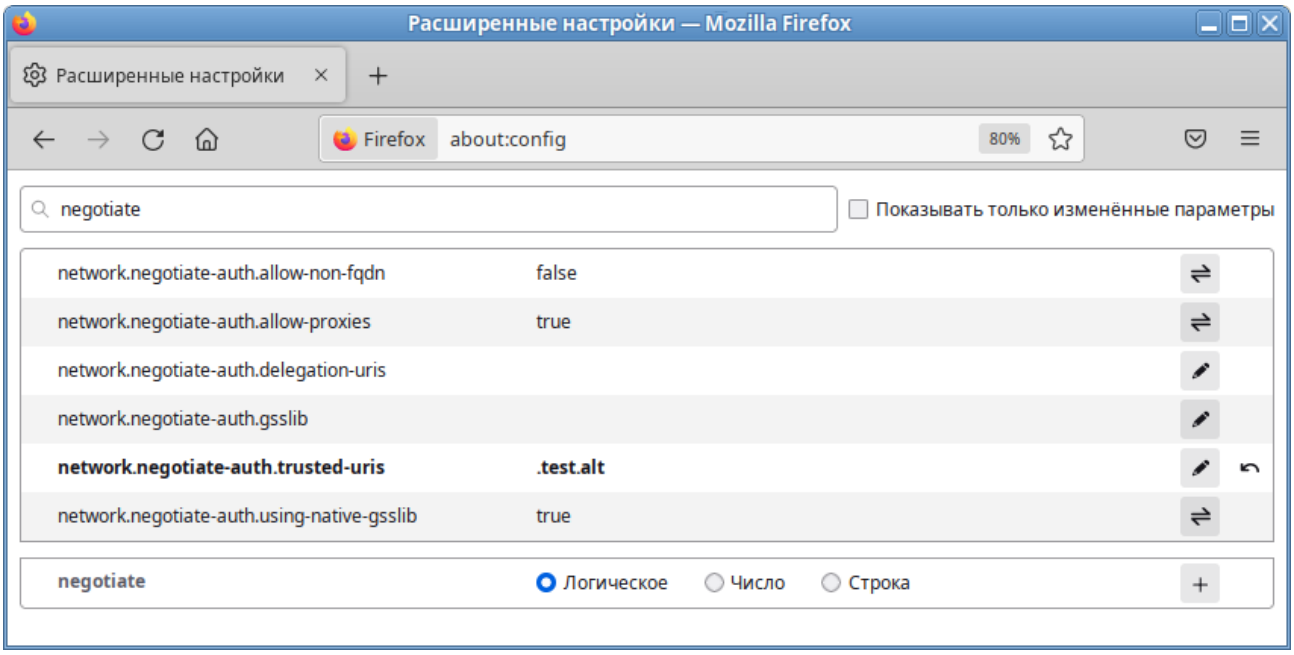
Порядок действий:

1. В адресной строке ввести **about:config**, чтобы отобразить список текущих параметров конфигурации (необходимо будет нажать кнопку **`Принять риск и продолжить`**).

2. В поле **`Фильтр`** ввести **negotiate**, чтобы ограничить список параметров.

3. Выбрать параметр ***`network.negotiate-auth.trusted-uris`***.

4. Указать в этом параметре имя kerberos области (realm), включая предшествующую точку (.). Если нужно добавить несколько доменов, их необходимо указать через запятую.



В ряде случаев может потребоваться отредактировать еще несколько параметров:

- параметр ***network.automatic-ntlm-auth.trusted-uris*** выставить в kerberos realm: **.test.alt**;
- параметр ***network.negotiate-auth.delegation-uris*** выставить в kerberos realm: **.test.alt**;
- параметр ***network.automatic-ntlm-auth.allow-non-fqdn*** выставить в: **true**;
- параметр ***network.negotiate-auth.allow-non-fqdn*** выставить в: **true**;

Вместо выставления этих параметров можно создать файл **`/usr/lib64/firefox/browser/defaults/preferences/prefs.js`** со следующим содержимым:

```
pref("network.negotiate-auth.trusted-uris",".test.alt");
pref("network.automatic-ntlm-auth.trusted-uris",".test.alt");
pref("network.automatic-ntlm-auth.allow-non-fqdn","true");
pref("network.negotiate-auth.allow-non-fqdn","true");
pref("network.negotiate-auth.delegation-uris",".test.alt");
```

Эти параметры могут быть распространены через групповые политики для Firefox:

- параметр ***network.negotiate-auth.trusted-uris*** — политика **SPNEGO**;
- параметр ***network.automatic-ntlm-auth.trusted-uris*** — политика **NTLM**;
- параметр ***network.negotiate-auth.delegation-uris*** — политика **Делегированная авторизация**;
- параметр ***network.automatic-ntlm-auth.allow-non-fqdn*** — политика **Разрешить неполное доменное имя (Non FQDN)**;
- параметр ***network.negotiate-auth.allow-non-fqdn*** — политика **Разрешить неполное доменное имя (Non FQDN)**;

Подробнее см. Групповые политики для Firefox

7.5.3.2. Настройка Chromium

В файл **/etc/chromium/policies/managed/policies.json** добавить строку:

```
{
    "AuthServerAllowlist": "*.test.alt"
}
```

Где .test.alt — имя kerberos области (realm).

Для применения настроек необходимо перезапустить браузер. Результат применения параметров политики для Chromium можно проверить, указав в адресной строке URL: "chrome://policy".

Этот параметр может быть распространён через групповые политики для Chromium: политика **Список разрешенных серверов для аутентификации**. Подробнее см. Групповые политики для Chromium

Примечание

Для проверки работы аутентификации без изменения настроек браузера можно запустить браузер из командной строки, выполнив команду:

```
$ chromium-browser --auth-server-whitelist="*.test.alt"
```

7.5.3.3. Настройка «Яндекс.Браузера»

В файл **/etc/opt/yandex/browser/policies/managed/policies.json** добавить строку:

```
{
    "AuthServerAllowlist": "*.test.alt"
}
```

Где .test.alt — имя kerberos области (realm).

Для применения настроек необходимо перезапустить браузер. Результат применения параметров политики для «Яндекс.Браузера» можно проверить, указав в адресной строке URL: "browser://policy".

Этот параметр может быть распространён через групповые политики для «Яндекс.Браузера»: политика **Список разрешенных серверов для аутентификации**. Подробнее см. Групповые политики для «Яндекс.Браузера».

7.6. Distributed File System

Распределенная файловая система (Distributed File System, DFS) — серверная технология Microsoft, предназначенная для упрощения доступа к общим файловым ресурсам, распределенным по сети. С помощью DFS можно объединять в единую логическую структуру файловые ресурсы, физически находящиеся на различных серверах, а также производить между ними репликацию. Функционал DFS образуют две составляющих: пространство DFS-имен — DFS-N (DFS-Namespace) и механизм репликации — DFS-R (DFS-Replication).

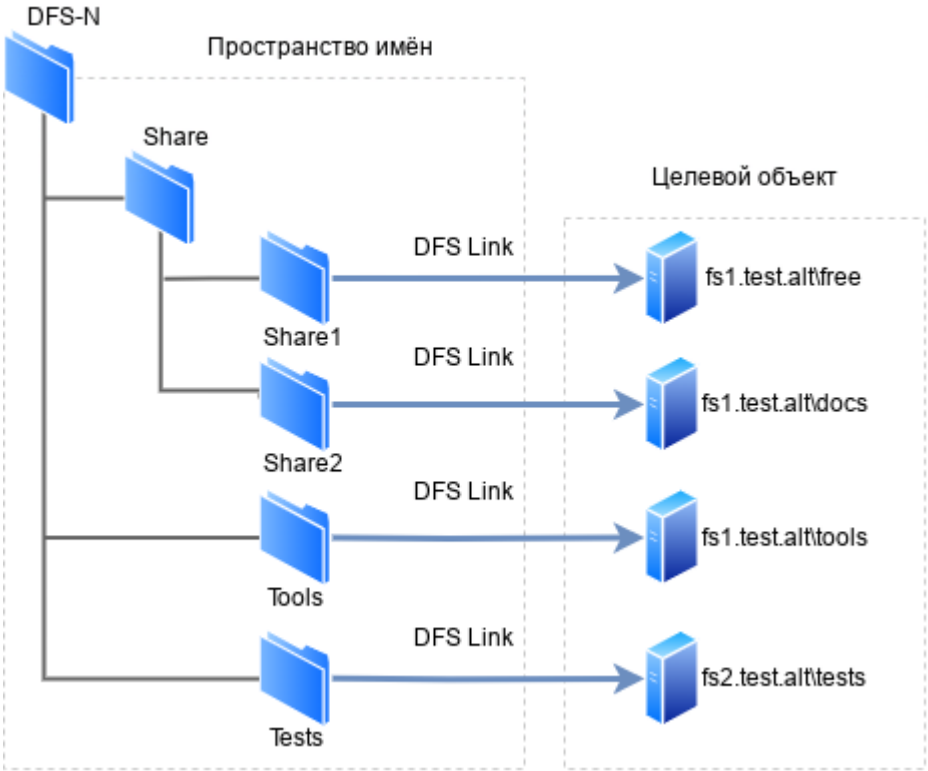
Samba поддерживает DFS-N, но пока не поддерживает DFS-R.

7.6.1. Пространство DFS-имен

Пространство DFS-имен — это единый виртуальный каталог, содержащий ссылки на общие каталоги, расположенные на разных файловых серверах. Пространство имен состоит из корня (root), ссылок (folders) и целевых объектов (folder targets). Пространство имен DFS может быть двух типов: автономное (Stand-alone) и доменное (Domain-based).

Автономный вариант работает на одном сервере и приводит к тому, что имена DFS содержат имя этого сервера, они выглядят как общие ресурсы, предоставляемые этим сервером (можно создать распределенную файловую систему не используя доменные службы AD).

При доменном варианте имена DFS содержат только имя домена, а не имя какого-либо конкретного сервера (имя сервера пространства имен скрыто от пользователей, проще замена сервера пространства имен или перенос пространства имен на другой сервер).



Корень пространства имен (Namespace root) — это базовая точка, от которой начинается отсчёт пространства имён. В зависимости от типа корень доступен по адресу \\ServerName\RootName (Stand-alone) или \\DomainName\RootName (Domain-based).

Сервер пространства имен (Namespace server) — физический сервер, на котором содержится пространство имён DFS.

Каталог — ссылка в пространстве имен DFS, указывающая на целевой объект. Каталог без конечных объектов (например, каталог Share) образуют структуру и иерархию в пространстве имен, а каталоги с целевыми объектами (например, каталог Share1) предоставляют пользователям доступ к фактическому содержимому.

Целевой объект (Folder targets) — ссылка на общий файловый ресурс, находящийся на определенном файловом сервере. Одна ссылка может указывать как на один, так и на несколько целевых объектов.

7.6.2. Настройка DFS на сервере Samba

Прежде, чем перейти к добавлению пространства имен, необходимо создать хотя бы один сетевой каталог на любом из серверов, добавленных в домен.

Сервер Samba можно сделать сервером DFS, задав логический параметр ***host msdfs*** в файле **/etc/samba/smb.conf**. Корень DFS назначается с помощью логического параметра ***root msdfs***. Если для этого параметра установлено значение **yes**, Samba будет воспринимать открытый для общего доступа ресурс как корневой DFS. Ссылки DFS, указываемые в открытом для доступа каталоге, имеют вид: **msdfs:serverA\shareA,serverB\shareB** и т.д. Корневой каталог DFS в Samba содержит ссылки DFS в виде символических ссылок,

Для создания нового пространства имён необходимо выполнить следующие действия:

- Создать каталог, в котором будут настроены ссылки DFS на другие серверы в сети (в примере **/media/dfsroot**):

```
# mkdir /media/dfsroot
```

- В файле **/etc/samba/smb.conf** в секцию **[global]** добавить параметр:

```
host msdfs = yes
```

  и добавить секцию **[dfs]**, с указанием корня:

```
[dfs]
        path = /media/dfsroot
        msdfs root = yes
```

- В каталоге **/media/dfsroot** настроить ссылки DFS на общие ресурсы в сети:

```
# cd /media/dfsroot
# ln -s msdfs:dc1.test.alt\\free linka
# ln -s msdfs:web.test.alt\\tests linkb
```

- Перезапустить samba:

```
# systemctl restart samba
```

- Дерево DFS теперь доступно по адресу //test.alt/dfs/. При доступе к ссылкам linka или linkb (которые отображаются для клиента как каталоги) пользователи напрямую переходят к соответствующим общим ресурсам в сети. Проверка:

```
$  smbclient //test.alt/dfs/linka -U 'ivanov'
Password for [TEST\ivanov]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Mon May 22 10:13:28 2023
  ..                                  D        0  Mon May 22 10:13:06 2023
  dc.txt                              N        5  Mon May 22 15:57:14 2023

        48254668 blocks of size 1024. 40859796 blocks available
smb: \> exit
```

Примечание

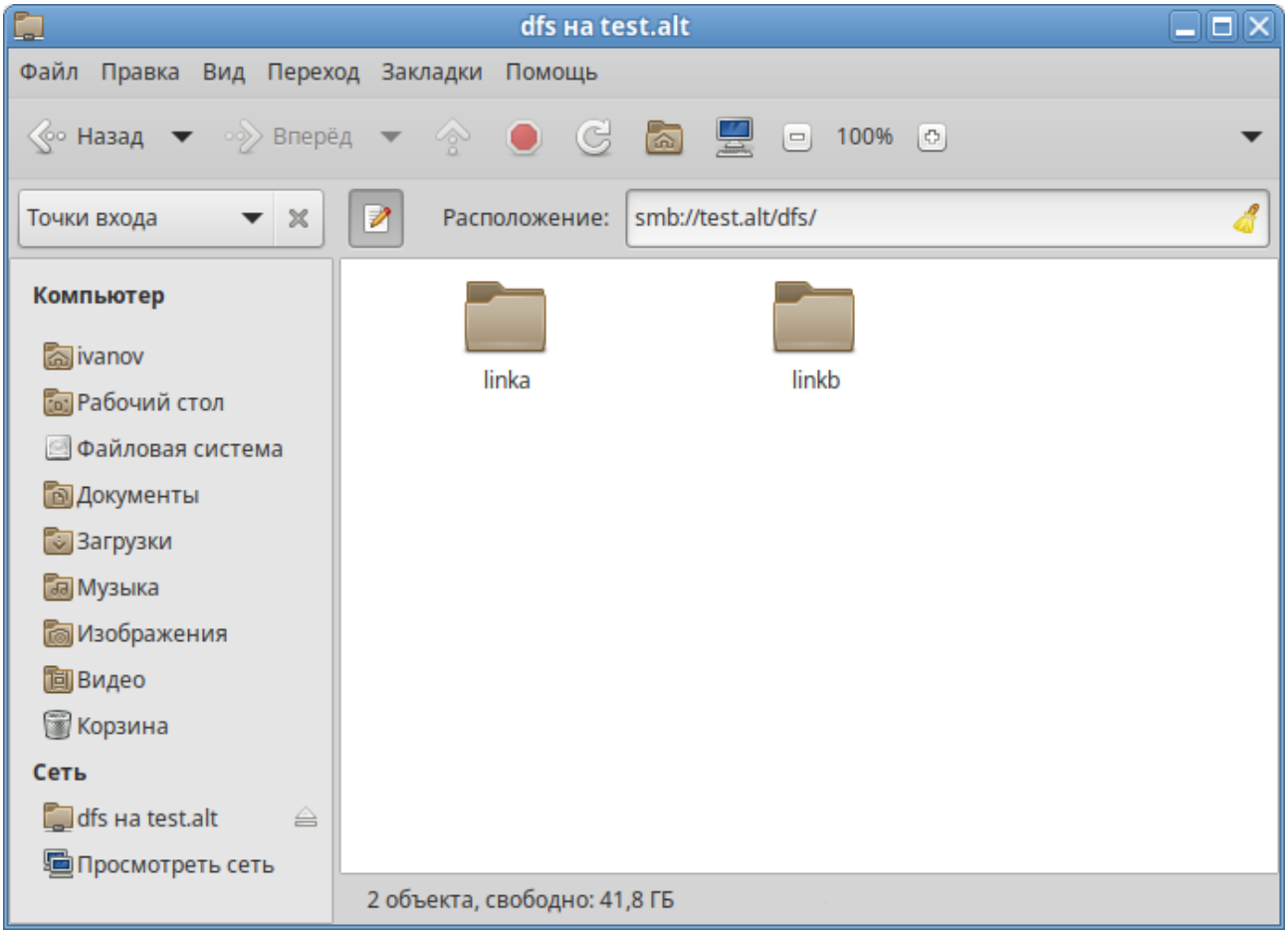
Для доступа к ресурсам DFS по имени домена с использованием аутентификации Kerberos необходимо добавить к имени сервера псевдоним — имя домена. Это можно сделать, выполнив на контроллере домена команду:

```
# samba-tool spn add cifs/cifs/<имя_домена> <имя_сервера>$
```

Например:

```
# samba-tool spn add cifs/test.alt dc1$
```

Подключиться к данному пространству можно, набрав в адресной строке следующий адрес: smb://<имя_домена>/<имя_пространства_имен>:



7.7. Настройка SSSD

7.7.1. Журналирование SSSD

7.7.1.1. Файлы журналов SSSD

Каждая служба SSSD записывает логи в свой собственный файл журнала в каталоге **/var/log/sssd/**. Например, для машины в домене AD test.alt, файлы журналов SSSD могут выглядеть следующим образом:

```
 # ls -l /var/log/sssd/
итого 1660
-rw------- 1 _sssd _sssd       0 мая 18 12:55 gpo_child.log
-rw------- 1 _sssd _sssd       0 мая 18 12:55 krb5_child.log
-rw------- 1 _sssd _sssd       0 мая 18 12:54 ldap_child.log
-rw------- 1 root  root      261 июн 19 10:10 sssd_ifp.log
-rw------- 1 root  root     3955 июн 19 09:34 sssd.log
-rw------- 1 _sssd _sssd 1677605 июн 19 11:18 sssd_nss.log
-rw------- 1 _sssd _sssd    1134 июн 19 09:34 sssd_pac.log
-rw------- 1 _sssd _sssd    3067 июн 19 09:34 sssd_pam.log
-rw------- 1 _sssd _sssd       0 мая 18 12:54 sssd_TEST.ALT.log
```

krb5_child.log

Файл журнала для недолговечного вспомогательного процесса, участвующего в аутентификации Kerberos.

ldap_child.log

Файл журнала для недолговечного вспомогательного процесса, участвующего в получении билета Kerberos для связи с сервером LDAP.

sssd_<domain.name>.log

Для каждого раздела [domain] в файле **sssd.conf** служба SSSD записывает информацию о взаимодействии с LDAP-сервером в отдельный файл журнала.

sssd.log

Файл журнала для мониторинга SSSD и связи его с ответчиком и внутренними процессами.

sssd_ifp.log

Файл журнала для ответчика InfoPipe, который предоставляет общедоступный интерфейс D-Bus, доступный через системную шину.

sssd_nss.log

Файл журнала для ответчика Name Services Switch (NSS), который извлекает информацию о пользователях и группах.

sssd_pac.log

Файл журнала для ответчика Microsoft Privilege Attribute Certificate (PAC), который собирает PAC из билетов AD Kerberos и извлекает информацию о пользователях AD из PAC, что позволяет избежать её запроса непосредственно из AD.

`sssd_pam.log`

Файл журнала для ответчика Pluggable Authentication Module (PAM).

`sssd_ssh.log`

Файл журнала для процесса ответчика SSH.

7.7.1.2. Уровни журналирования SSSD

Таблица 7.3. Уровни журналирования SSSD

Уровень	Описание
0, 0x0010	**Фатальные ошибки**. Ошибки, которые не позволяют запустить службу SSSD или вызывает завершение работы сервиса.
1, 0x0020	**Критические ошибки**. Ошибки, которые не завершают работу службы SSSD, но означает, что как минимум одна из основных функций не работает должным образом.
2, 0x0040	**Серьёзные ошибки**. Ошибки, сообщающие о том, что определенный запрос или операция завершились неудачно. *Это уровень журналирования по умолчанию*.
3, 0x0080	**Незначительные ошибки**. Ошибки, которые могут стать причиной ошибок 2-го уровня (ошибок при выполнении действий).
4, 0x0100	**Настройки конфигурации**.
5, 0x0200	**Данные функций**.
6, 0x0400	Сообщения трассировки для функций **действ ий**.
7, 0x1000	Сообщения трассировки для функций **внутре ннего управления**.
8, 0x2000	Содержимое переменных **внутренних функций**.
9, 0x4000	Информация **трассировки крайне низкого уровня**.
9, 0x20000	**Быстродействие и статистические данные**. Из-за способа обработки запросов на внутреннем уровне, записанное в журнал время выполнения запроса может быть больше, чем оно было на самом деле.
10, 0x10000	Информация **трассировки libldb** ещё более низкого уровня. Практически никогда не требуется.

Установка уровня журнала также включает все уровни ниже него. Например, установка уровня журнала на 6 также включает уровни с 0 по 5.

Чтобы вести журнал для необходимых уровней журналирования, указанных в представлении битовых масок, следует просто сложить их номера. Например, чтобы вести журнал для фатальных, критических, серьёзных ошибок и для данных функций, следует использовать значение **`0x0270`**.

7.7.1.3. Настройка уровня журналирования для SSSD в файле `sssd.conf`

Чтобы включить подробное журналирование, сохраняющееся при перезапуске службы SSSD, следует добавить опцию ***`debug_level=<целое_число>`*** в каждую секцию файла **`/etc/sssd/sssd.conf`**. Где значение *<целое_число>* — число от 0 до 10. Уровни до 3 регистрируют крупные сбои, а уровни начиная с 8 и выше предоставляют большое количество подробных сообщений журнала. Уровень *6* является хорошей отправной точкой для отладки проблем.

Пример настройки уровня журналирования в файле **`/etc/sssd/sssd.conf`**:

```
[sssd]
debug_level = 6
config_file_version = 2
services = nss, pam

[domain/TEST.ALT]
debug_level = 6
id_provider = ad
…

[nss]
debug_level = 6

[pam]
debug_level = 6
```

Чтобы загрузить новые параметры конфигурации необходимо перезапустить службу SSSD:

```
# systemctl restart sssd
```

7.7.1.4. Настройка уровня журналирования для SSSD с помощью команды sssctl

Изменить уровень журналирования службы SSSD можно с помощью команды **`sssctl debug-level <целое_число>`**. Где значение *<целое_число>* — число от 0 до 10. Уровни до 3 регистрируют крупные сбои, а уровни начиная с 8 и выше предоставляют большое количество подробных сообщений журнала. Уровень *6* является хорошей отправной точкой для отладки проблем.

Просмотр текущего уровня журналирования:

```
# sssctl debug-level
sssd                      0x0070
nss                       0x0070
pam                       0x0070
pac                       0x0070
domain/TEST.ALT           0x0070
```

Установка нового уровня журналирования:

```
# sssctl debug-level 6
# sssctl debug-level
sssd                        0x07f0
nss                         0x07f0
pam                         0x07f0
pac                         0x07f0
domain/TEST.ALT             0x07f0
```

Примечание

Уровень журналирования, заданный с помощью команды **`sssctl debug-level`** будет действовать до перезапуска службы sssd.

7.7.2. Настройки SSSD в ЦУС

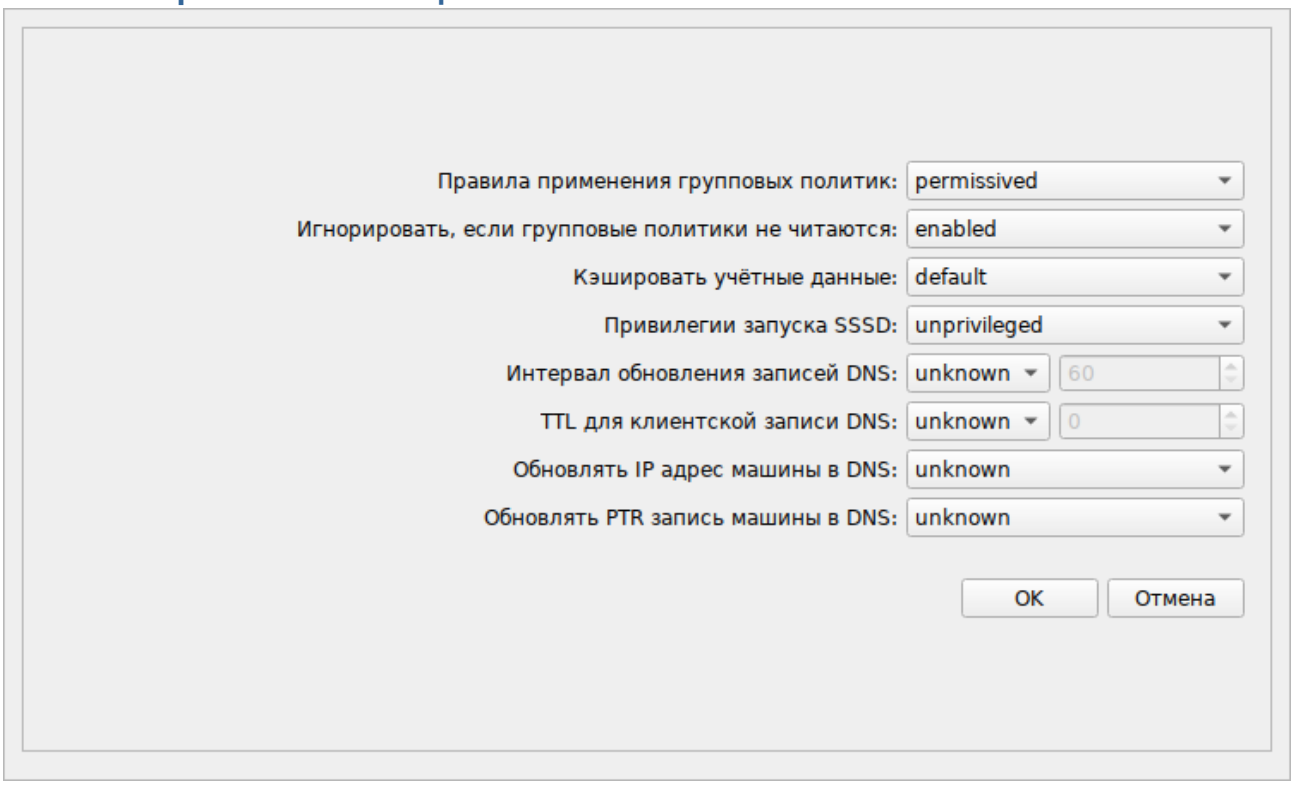


Таблица 7.4. Настройки SSSD в Alterator

Настройка	Опция в файле `/etc/sssd/sssd.conf`	Описание	Режимы
Правила применения групповых политик	**`ad_gpo_access_control`**	Определяет в каком режиме будет осуществляться контроль доступа в SSSD основанный на групповых политиках Active Directory (GPO)	**`enforced`** (принудительный режим) — правила управления доступом в SSSD основанные на

Настройка	Опция в файле /etc/sssd/sssd.conf	Описание	Режимы
			GPO выполняются, ведётся логирование **permissived** (разрешающий режим) — правила управления доступом в SSSD основанные на GPO не выполняются, ведётся только логирование. Такой режим необходим администратору, чтобы оценить, как срабатывают новые правила **disabled** (отключить) — правила управления доступом в SSSD основанные на GPO не логируются и не выполняются **default** (по умолчанию) — настройка контроля доступом в SSSD основанное на GPO сброшена на значение по умолчанию в пакете
Игнорировать, если групповые политики не читаются	**ad_gpo_ignore_unreadable**	Определяет будут ли проигнорированы правила управления доступом в SSSD основанные на групповых политиках, если недоступен	**enabled** (включить) — игнорировать правила управления доступом через групповые

Настройка	Опция в файле /etc/sssd/sssd.conf	Описание	Режимы
		какой-либо шаблон (GPT) объекта групповой политики (GPO)	политики, если шаблоны групповых политик не доступны для SSSD **disabled** (отключить) — запретить доступ пользователям SSSD AD, которым назначены групповые политики, если шаблоны групповых политик не доступны **default** (по умолчанию) — настройка игнорирования политик, при недоступности шаблонов групповых политик сброшена на значение по умолчанию в пакете
Кэшировать учётные данные	**cache-credentials**	Определяет, будут ли учётные данные удалённых пользователей сохраняться в локальном кэше SSSD	**enabled** (включить) — сохранение в локальном кэше SSSD учётных данных пользователей включено **disabled** (отключить) — сохранение в локальном кэше SSSD учётных данных пользователей отключено

Настройка	Опция в файле /etc/sssd/sssd.conf	Описание	Режимы
			default (по умолчанию) — настройка сохранения в локальном кэше SSSD учётных данных пользователей сброшена на значение по умолчанию в пакете
Привилегии запуска SSSD	**control sssd-drop-privileges**	Позволяет сбросить права службы SSSD, чтобы избежать работы от имени суперпользователя (root)	**privileged** (привилегированный) — служба SSSD запущена от имени привилегированного суперпользователя (root) **unprivileged** (непривилегированный) — служба SSSD запущена от имени непривилегированного пользователя (_sssd) **default** (по умолчанию) — режим привилегий службы SSSD задан по умолчанию в пакете
Интервал обновления записей DNS	**dyndns_refresh_interval**	Определяет как часто серверная часть должна выполнять периодическое обновление DNS в дополнение к автоматическому обновлению,	**enabled** (включить) — задать интервал

Настройка	Опция в файле /etc/sssd/sssd.conf	Описание	Режимы
		выполняемому при подключении серверной части к сети. Этот параметр применим только в том случае, если для **dyndns_update** установлено значение **true**.	▸**disabled** (отключить) — установить значение по умолчанию (86400) ▸**unknown**
TTL для клиентской записи DNS	**dyndns_ttl**	Срок жизни, применяемый к DNS-записи клиента при ее обновлении. Если **dyndns_update** имеет значение **false**, это не имеет никакого эффекта	▸**enabled** (включить) — задать TTL ▸**disabled** (отключить) — установить значение по умолчанию (3600) ▸**unknown**
Обновлять IP-адрес машины в DNS	**dyndns_update**	Позволяет включить или отключить автоматическое обновление DNS-записей (защищенных с помощью GSS-TSIG) с IP-адресом клиента через SSSD	▸**enabled** (включить) — автоматическое обновление DNS-записи клиента через SSSD включено ▸**disabled** (отключить) — автоматическое обновление DNS-записи клиента через SSSD отключено ▸**default** (по умолчанию) — настройка автоматического обновления DNS-записи клиента через SSSD задана по умолчанию в пакете ▸**unknown**

Настройка	Опция в файле /etc/sssd/sssd.conf	Описание	Режимы
Обновлять PTR-запись машины в DNS-записей	**dyndns_update_ptr**	Определяет будет ли обновляться клиентская PTR-запись (защищенная с помощью GSS-TSIG) при обновлении DNS-записей клиента. Применимо, только если **dyndns_update** имеет значение **true**.	▹**enabled** (включить) — автоматическое обновление DNS-записи обратной зоны через SSSD включено ▹**disabled** (отключить) — автоматическое обновление DNS-записи обратной зоны через SSSD отключено ▹**default** (по умолчанию) — настройка автоматического обновления DNS-записи обратной зоны задана по умолчанию в пакете ▹**unknown**

7.7.3. Включение автономной аутентификации

По умолчанию SSSD не кэширует учетные данные пользователей. При обработке запросов на аутентификацию SSSD всегда обращается к поставщику идентификационных данных. Если провайдер недоступен, аутентификация пользователя не проходит.

Чтобы пользователи могли пройти аутентификацию, даже когда провайдер идентификации недоступен, можно включить кэширование учетных данных, установив параметр ***cache_credentials*** в значение **true** в файле **/etc/sssd/sssd.conf**.

Чтобы пользователи могли пройти аутентификацию, даже когда провайдер идентификации недоступен, можно включить кэширование учетных данных, установив параметр ***cache_credentials*** в значение **true** в разделе домена.

Дополнительно можно использовать параметр ***offline_credentials_expiration*** в разделе [pam], чтобы установить ограничение по времени (в днях), в течении которого пользователи смогут аутентифицироваться в автономном режиме с момента последнего успешного входа.

Пример настройки возможности автономной аутентификации пользователей в течение 5 дней с момента последнего успешного входа:

```
[pam]
offline_credentials_expiration = 5
[domain/TEST.ALT]
cache_credentials = true
```

7.8. Файловый сервер

Samba можно настроить как файловый сервер. Samba также можно настроить как сервер печати для совместного доступа к принтеру.

7.9. Монтирование общих ресурсов samba

Рассматриваемые ниже способы позволяют подключать файловые ресурсы (file shares) для доменного пользователя без повторного ввода пароля (SSO, Single Sign-On).

7.9.1. Подключение с использованием gio

Примечание

Способ актуален для дистрибутивов, использующих gio (например, Simply Linux, Альт Рабочая станция).

Недостаток этого способа — необходимо открыть ресурс в файловом менеджере (**Caja**, **Pcmanfm**). Однако можно открывать любые ресурсы на любых серверах, входящие в домен **Active Directory**.

- Установить необходимые пакеты:

```
# apt-get install fuse-gvfs gvfs-backend-smb libgio
```

- Включить пользователя в группу fuse:

```
# gpasswd -a <пользователь> fuse
```

- Разрешить для всех доступ к fuse под root:

```
# control fusermount public
```

- Войти под доменным пользователем.
- Открыть ресурс в файловом менеджере (например, по адресу smb://server/sysvol). Ресурс смонтирован по пути **/var/run/<uid_пользователя>/gvfs** или **/var/run/user/<uid_пользователя>/gvfs/smb-share:server=сервер,share=ресурс**.
- Другой вариант (полезно для скриптов в автозапуске):

```
gio mount smb://server/sysvol/
```

Примечание

Если необходимо открывать что-то с ресурса в WINE, в winecfg слледует добавить диск с путём **/var/run/uid_пользователя/gvfs**

7.9.2. Подключение с использованием pam_mount

При этом способе сетевой ресурс подключается с заданного сервера автоматически при каждом входе доменным пользователем.

- Установить пакеты *pam_mount* и *cifs-utils*:

```
# apt-get install pam_mount cifs-utils
```

Важно

Для того чтобы файловые ресурсы, подключенные с помощью pam_mount, корректно отключались при завершении сеанса, следует установить пакет *systemd-settings-enable-kill-user-processes* и перезагрузить систему:

```
# apt-get install systemd-settings-enable-kill-user-processes
```

- Прописать pam_mount в схему аутентификации по умолчанию. Для этого в конец файла **/etc/pam.d/system-auth** добавить строки:

```
session         [success=1 default=ignore] pam_succeed_if.so  service =
systemd-user quiet
session         optional        pam_mount.so disable_interactive
```

- Установить правило монтирования ресурса в файле **/etc/security/pam_mount.conf.xml** (перед тегом <cifsmount>):

```
<volume uid="10000-2000200000" fstype="cifs" server="dc1.test.alt"
path="sysvol" mountpoint="~/share"
options="sec=krb5i,cruid=%(USERUID),nounix,uid=%(USERUID),gid=%
(USERGID),file_mode=0664,dir_mode=0775" />
```

где

- uid="10000-2000200000" — диапазон присваиваемых для доменных пользователей UID (подходит для Winbind и для SSSD);
- server="dc1.test.alt" — имя сервера с ресурсом;
- path="sysvol" — имя файлового ресурса;
- mountpoint="**~/share**" — путь монтирования в домашней папке пользователя.

Опционально можно добавить:

- sgrp="group_name" — имя группы, при членстве пользователя в которой, папка будет примонтирована.

Параметр ***sec=krb5i*** более безопасный, но требует больше вычислительных ресурсов. Вместо него можно указать ***sec=krb5***.

Предупреждение

В параметре ***server*** необходимо указывать настоящее имя сервера, а не имя домена.

Предупреждение

По умолчанию для монтирования используется smb версии 1.0, если он отключен, то необходимо указать в параметрах версию 2 или 3:

```
<volume uid="10000-2000200000" fstype="cifs" server="dc1.test.alt"
path="sysvol" mountpoint="~/share"
options="sec=krb5i,vers=2.0,cruid=%(USERUID),nounix,uid=%(USERUID),gid=%
(USERGID),file_mode=0664,dir_mode=0775" />
```

Для проверки можно попробовать смонтировать ресурс в сессии:

```
mount.cifs //dc1.test.alt/sysvol /mnt/  -o vers=2.0,user=ivanov
```

Также можно проверить доступность ресурса с помощью **smbclient**, например:

```
smbclient -L dc1.test.alt -U ivanov -m SMB2
```

7.9.3. Подключение с использованием Autofs

При этом способе заданный ресурс подключается автоматически при каждом обращении пользователя и отключается после определенного времени бездействия (определяется конфигурацией Autofs).

Принцип работы:

- задаётся каталог, в котором будет происходить подключение, например, **/mnt/auto/**;
- при необходимости обратиться к сетевой файловой системе, следует обратиться к каталогу с именем этой ФС в этом каталоге. Например, **/mnt/auto/server/share/**;
- при обращении будет произведена попытка смонтировать соответствующий сетевой ресурс;
- при отсутствии обращения, после заданного таймаута, сетевой ресурс будет отмонтирован;

AutoFS использует для конфигурирования шаблоны **/etc/auto***. Основной шаблон называется **auto.master**, он может указывать на один или несколько других шаблонов для конкретных типов носителей. Пример содержимого файла **/etc/auto.master**:

```
# Format of this file:
# mountpoint map options
# For details of the format look at autofs(8).
/mnt/auto       /etc/auto.tab   -t 5
/mnt/net        /etc/auto.avahi -t 120
```

Первое значение в каждой строке определяет базовый каталог, в который носители будут монтироваться, второе значение — файл конфигурации или скрипт, который будет использован.

Примечание

Параметр ***-t*** (***--timeout***) устанавливает количество секунд, после истечения которых каталоги будут размонтированы. Значение 0 отключает таймаут. Значения параметра по умолчанию задаются в файле **/etc/autofs.conf**.

Базовый каталог будет создан, если он не существует. Он станет точкой монтирования, отображающей в себе динамически подключаемые носители, что означает, что существующее содержимое базового каталога будет недоступно пока autofs работает.

Пример настройки автоматического подключения сетевых файловых ресурсов Windows (Samba) при входе пользователя:

1. Добавить в **/etc/auto.master** строку:

   ```
   /mnt/samba /etc/auto.smb -t 120
   ```

   Здесь **/mnt/samba** — каталог в котором будут подключаться сетевые файловые системы, **/etc/auto.smb** — стандартный скрипт, входящий в состав пакета autofs, 120 — таймаут подключения при отсутствии обращения.

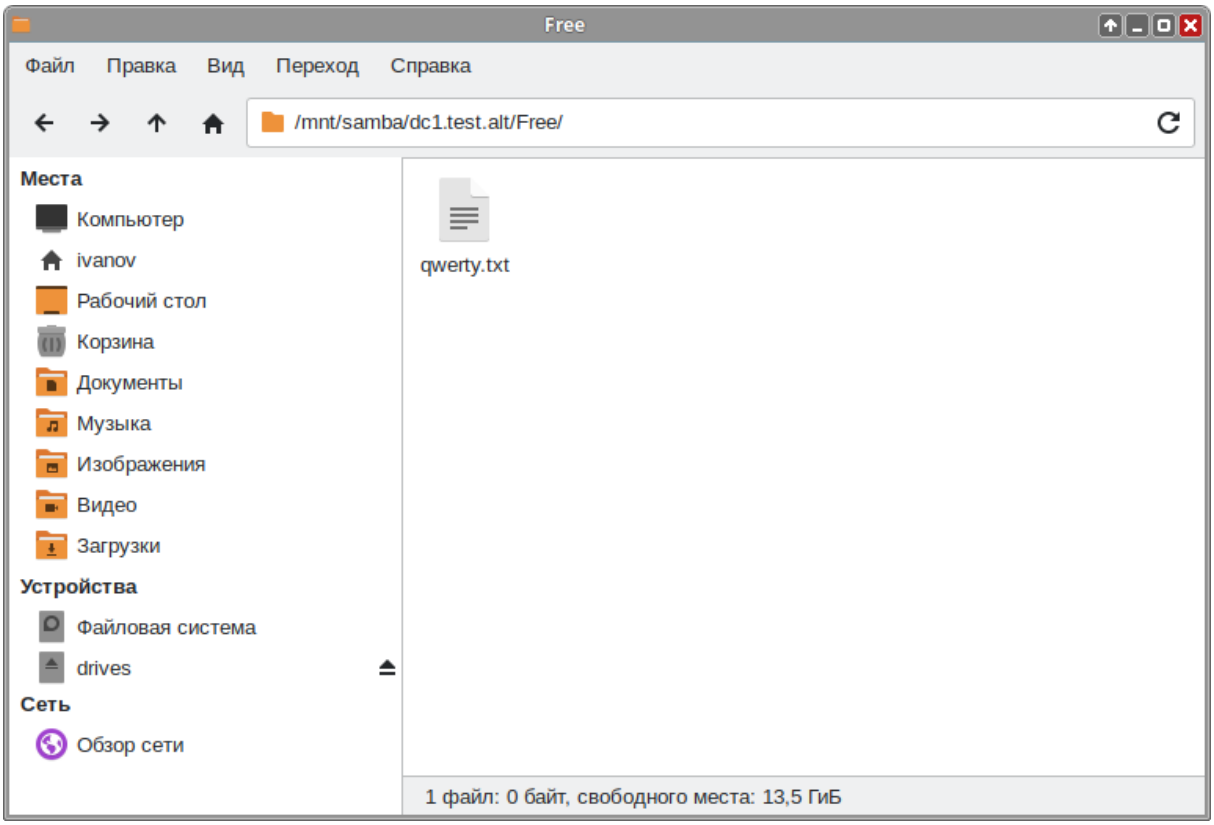
2. Включить и запустить сервис **autofs**:

   ```
   # systemctl enable --now autofs
   ```

3. Для автоматического подключения ресурсов достаточно обратиться к ресурсу по имени хоста, например:

   ```
   $ ls /mnt/samba/<имя_хоста>
   ```

   или в диспетчере файлов:



Пример настройки автоматического подключения сетевых файловых ресурсов Windows (Samba) при входе пользователя в систему для дистрибутивов с KDE (Альт Рабочая станция К, Альт Образование):

1. Установить пакет *kde5-autofs-shares*:

```
# apt-get install kde5-autofs-shares
```

2. Добавить в **`/etc/auto.master`** строку:

```
/mnt/samba /etc/auto.smb -t 120
```

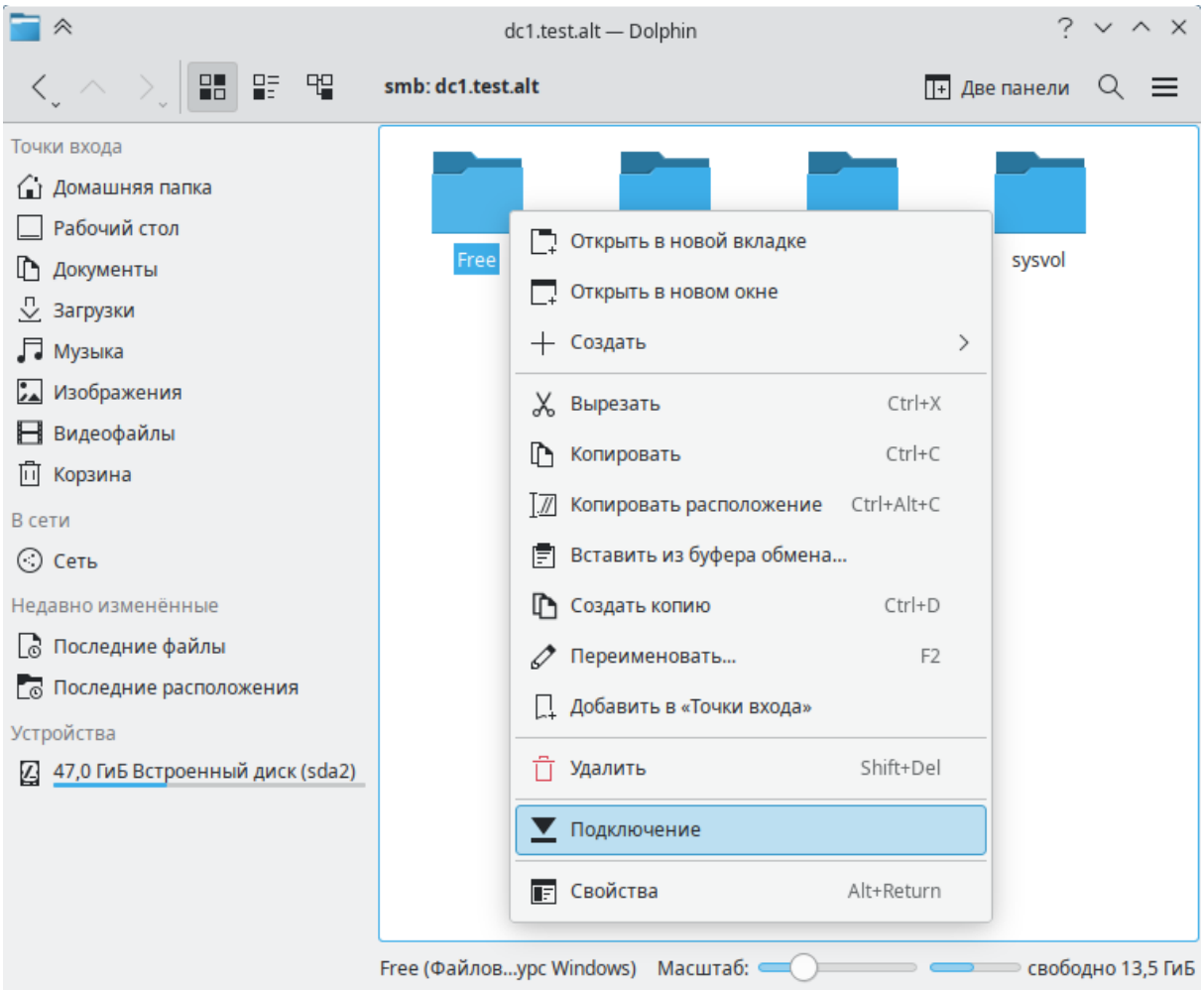
   Здесь **`/mnt/samba`** — каталог в котором будут подключаться сетевые файловые системы, **`/etc/auto.smb`** — скрипт, входящий в состав пакета *autofs*, 120 — таймаут подключения при отсутствии обращения.

3. Включить и запустить сервис **autofs**:

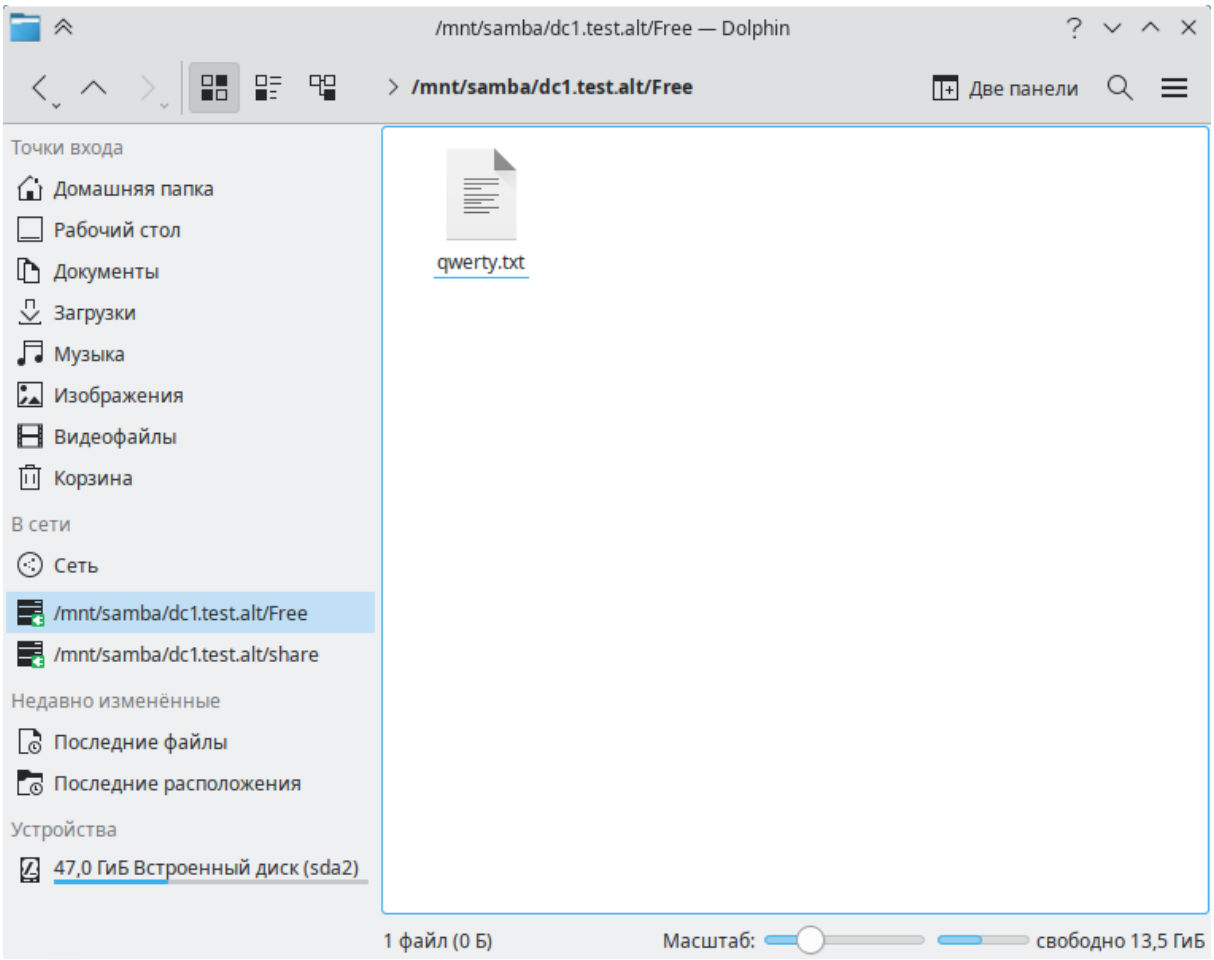
```
# systemctl enable --now autofs
```

4. В диспетчере файлов **Dolphin** по адресу smb://test.alt (**Сеть** → **Общие папки Samba**) найти нужный ресурс Windows (Samba).

5. В контекстном меню подключаемого ресурса выбрать пункт **Подключение**:



Данный ресурс будет подключаться автоматически при входе в систему:



Примечание

Список ресурсов для подключения хранится в файле **`~/.autofs.shares`**.

Важно

Данный способ работает только для ресурсов с гостевым доступом или ресурсов с авторизацией Kerberos.

7.10. Установка RSAT

Для администрирования Active Directory из Windows можно использовать средства удаленного администрирования сервера Microsoft (RSAT).

7.10.1. Windows Server

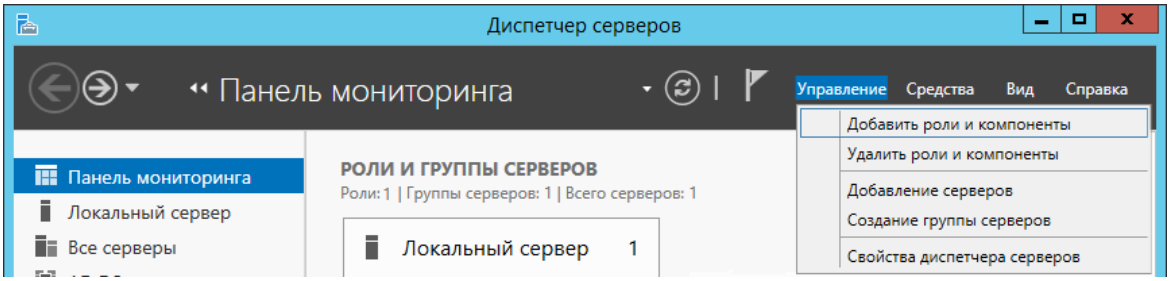
В ОС Windows Server средства удаленного администрирования сервера Microsoft (RSAT) включены по умолчанию.

Установка:

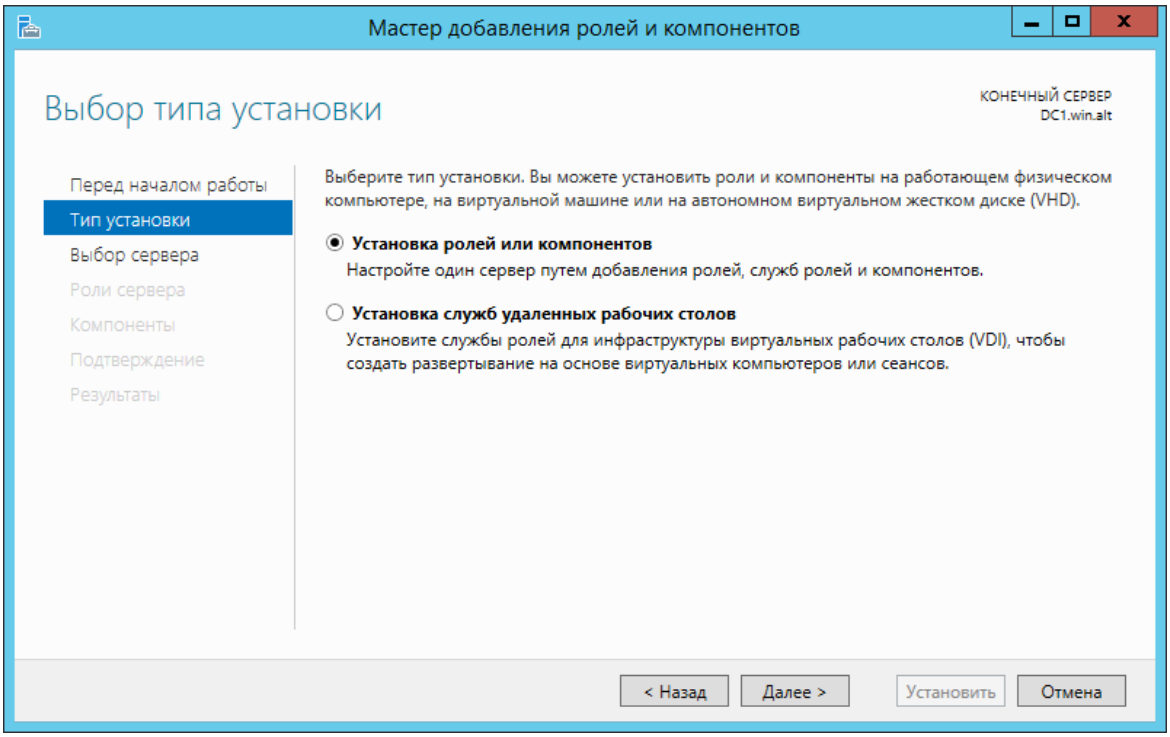
1. Запустить **`Диспетчер серверов`**.

2. На Windows Server 2012, 2012 R2, и 2016:

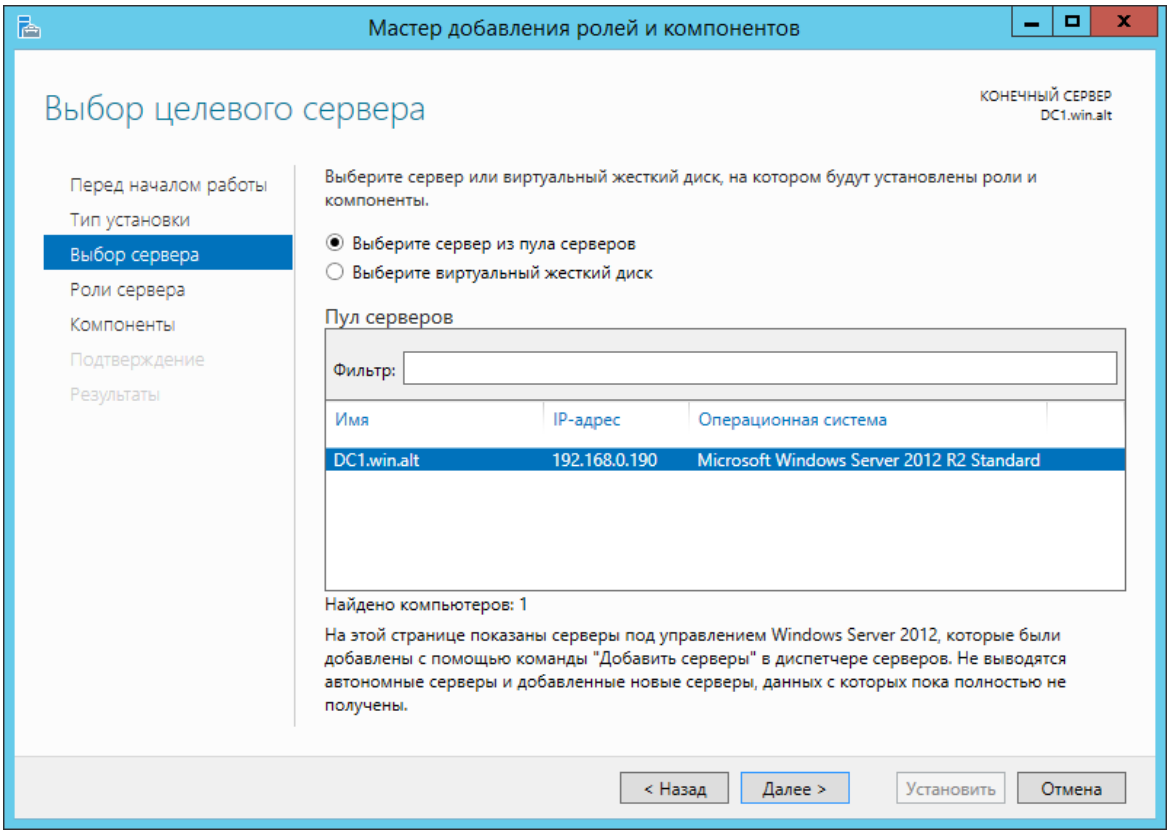
- выбрать **Управление** → **Добавить роли и компоненты**:



- В открывшемся окне **Мастер добавления ролей и компонентов** выбрать пункт **Установка ролей или компонентов**:



- Выбрать хост, на котором будут установлены компоненты:



- На шаге нажать кнопку **Далее**.

3. На Windows Server 2008 и 2008 R2 в дереве навигации выбрать **Компоненты** и нажать **Добавить компоненты**.

4. Выбрать компоненты для установки (см. Рекомендуемые компоненты для администрирования Samba AD):

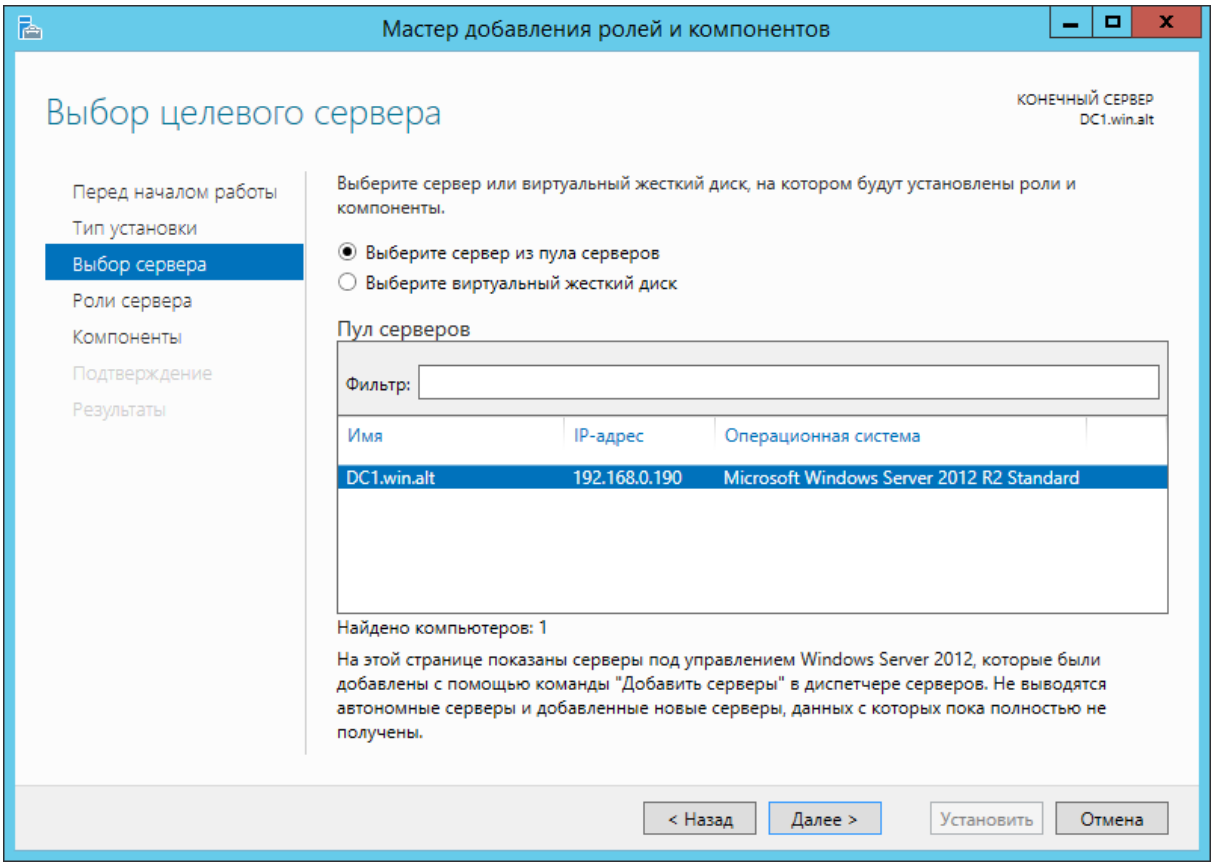


Таблица 7.5. Рекомендуемые компоненты для администрирования Samba AD

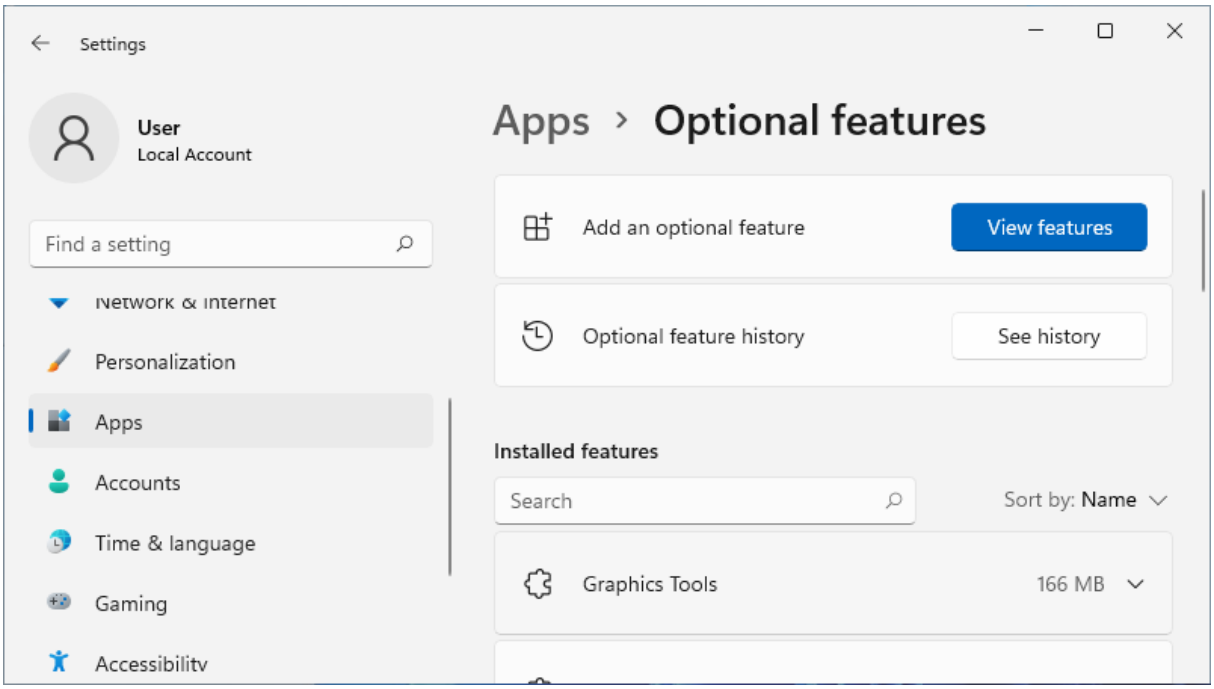
Компонент	Описание
Group Policy Management	Предоставляет оснастки для групповой политики: средство управления (GPMC), редактор управления (gpedit) и начальный редактор GPO
AD DS Snap-Ins and Command-Line Tools	Предоставляет оснастку «Пользователи и компьютеры Active Directory» (ADUC) и «Сайты и службы Active Directory» (ADSS)
Server for NIS	Добавляет вкладку **`Атрибуты UNIX`** в свойства объектов ADUC. Позволяет настраивать атрибуты RFC2307. Эта функция не поддерживается в Windows Server 2016
Active Directory Module for Windows PowerShell	Включает командлеты Active Directory (AD) PowerShell
DNS Server tools	Оснастка MMC DNS для удаленного управления DNS

7.10.2. Windows 10 (1809 и более поздних версиях)

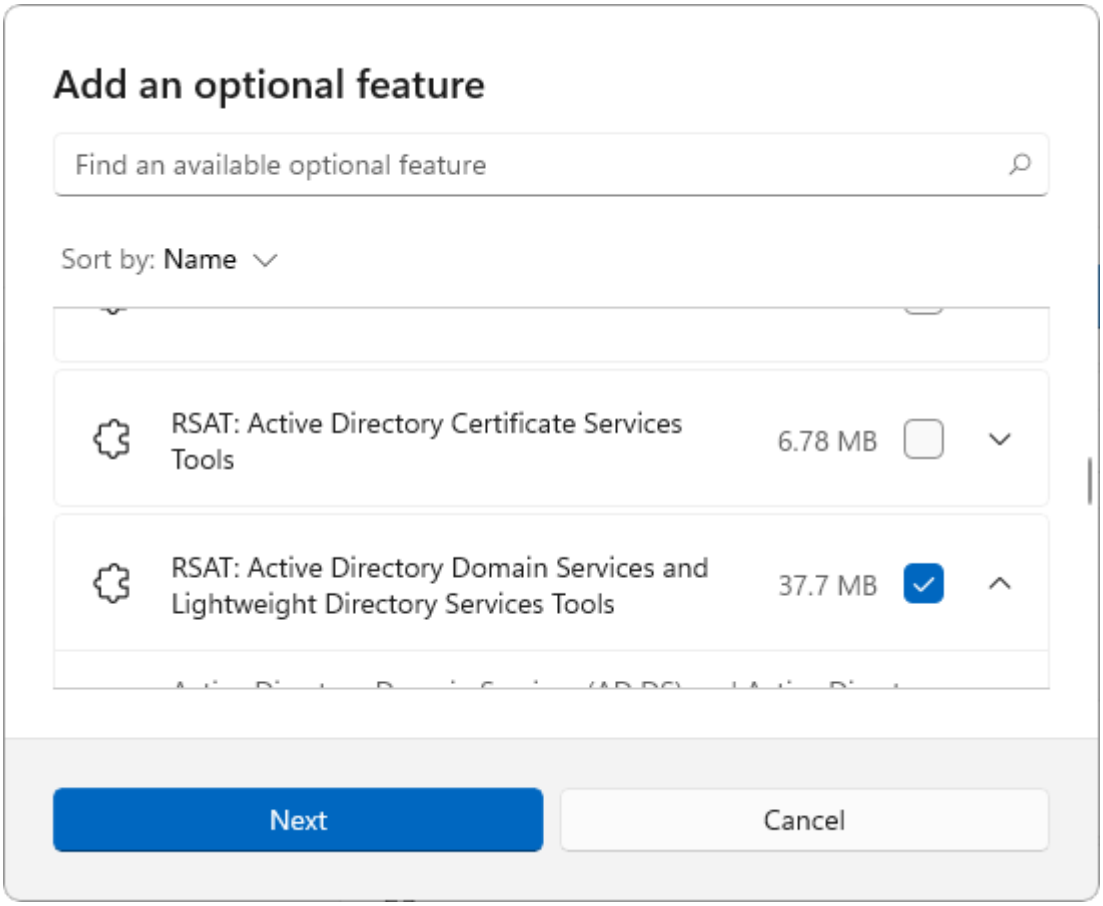
В Windows 10 1809 и более поздних версиях RSAT устанавливается в качестве дополнительной функции. Для установки компьютер должен иметь доступ в Интернет.

Установка:

1. Перейти в раздел **Settings** → **Apps** → **Optional Features** → **View features** (**Параметры Windows** → **Приложения** → **Дополнительные возможности** → **Добавить компонент**):



2. Выбрать нужные компоненты RSAT (см. Рекомендуемые компоненты для администрирования Samba AD) и нажать **`Next`**:



3. Нажать кнопку **`Install`**.

Таблица 7.6. Рекомендуемые компоненты для администрирования Samba AD

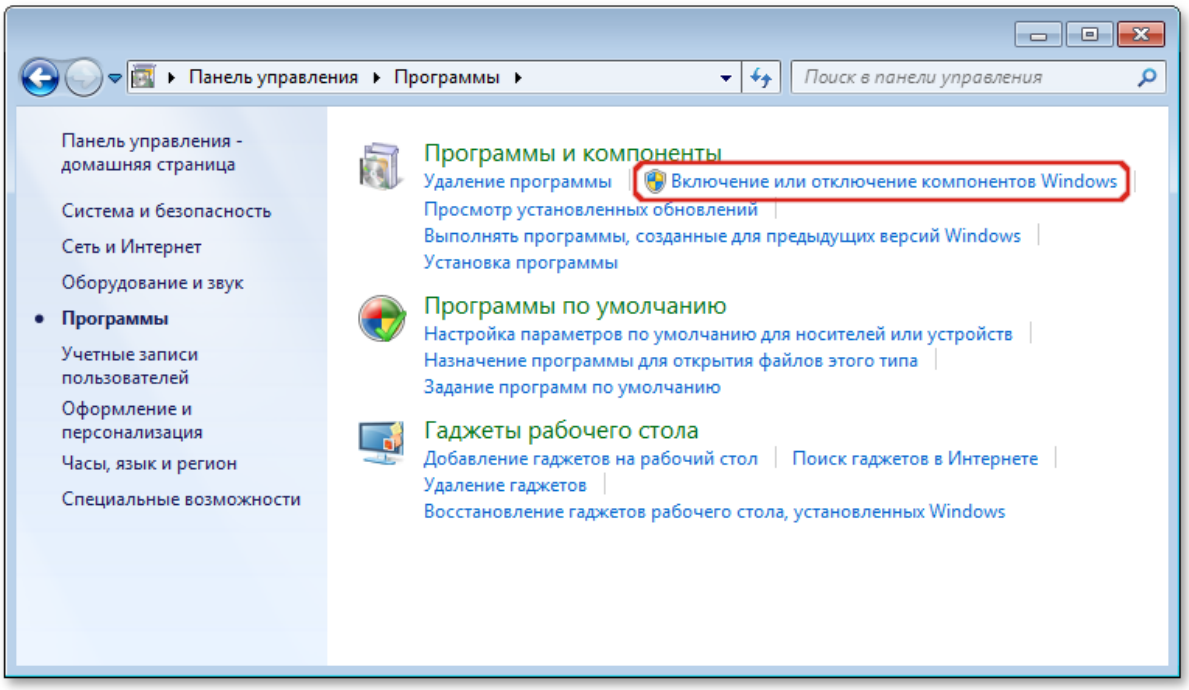
Компонент	Описание
RSAT: Group Policy Management Tools	Включают консоль управления групповыми политиками (gpmc.msc), редактор управления групповыми политиками (gpme.msc) и редактор GPO инициализирующей программы групповой политики (gpedit.msc)
RSAT: Active Directory Domain Services and Lightweight Directory Services Tools	Предоставляет оснастку «Пользователи и компьютеры Active Directory» (ADUC) и «Сайты и службы Active Directory» (ADSS)
RSAT: DNS Server Tools	Включает оснастку «Диспетчер DNS» для удаленного управления DNS и программу командной строки **`dnscmd.exe`**
RSAT: Remote Desktop Services Tool	Добавляет вкладку **`Профиль служб удаленных рабочих столов`** в свойства объекта пользователя ADUC и устанавливает оснастку MMC «Удаленные рабочие столы» для администрирования RDP-сервера (tsmmc.msc).

7.10.3. Windows Vista и 7

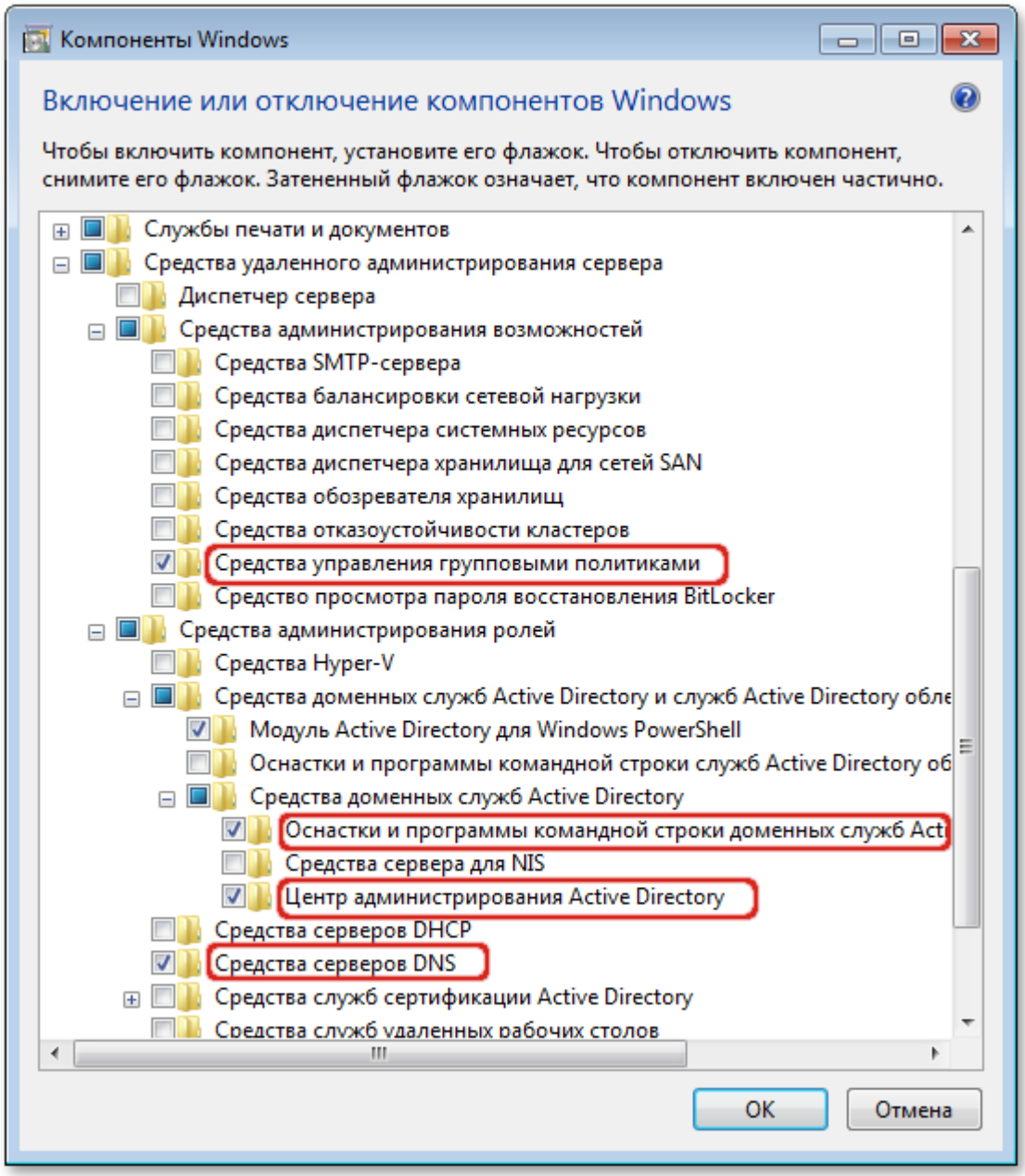
До версии Windows 10 1809 пакет удаленного администрирования серверов RSAT устанавливается в виде MSU обновления, которое нужно скачать с серверов Microsoft.

Установка:

1. Перейти в **Панель управления** → **Программы** → **Включение или отключение компонентов Windows**:



2. Включить компоненты (см. Рекомендуемые компоненты для администрирования Samba AD):



3. Нажать кнопку **OK**.

Таблица 7.7. Рекомендуемые компоненты для администрирования Samba AD

Компонент	Описание
Group Policy Management Tools (Средства управления групповыми политиками)	Включают консоль управления групповыми политиками (gpmc.msc), редактор управления групповыми политиками (gpme.msc) и редактор GPO инициализирующей программы групповой политики (gpedit.msc)
AD DS Tools (Оснастки и программы командной строки доменных служб Active Directory)	Предоставляет оснастку «Пользователи и компьютеры Active Directory» (ADUC) и «Сайты и службы Active Directory» (ADSS)
Server for NIS Tools (Средства сервера для NIS)	

Компонент	Описание
	Средства сервера для сетевых информационных служб добавляет вкладку **Атрибуты UNIX** (**UNIX Attributes**) в свойства объектов ADUC. Позволяет настраивать атрибуты RFC2307. Включает программу командной строки **ypclear.exe**
Active Directory Module for Windows PowerShell (Модуль Active Directory для Windows PowerShell)	Обеспечивает централизованную среду для управления службами каталогов
DNS Server tools (Средства серверов DNS)	Включает оснастку «Диспетчер DNS» для удаленного управления DNS и программу командной строки **dnscmd.exe**
Remote Desktop Services Tool (Средства служб удалённых рабочих столов)	Добавляет вкладку **Профиль служб удаленных рабочих столов** в свойства объекта пользователя ADUC и устанавливает оснастку MMC «Удаленные рабочие столы» для администрирования RDP-сервера (tsmmc.msc).

7.11. Инструменты командной строки

Таблица 7.8. Основные инструменты командной строки

Утилита	Описание
samba-tool	Основная утилита управления Samba
wbinfo	Позволяет получить информацию от демона winbindd
net	Инструмент администрирования Samba и удаленных серверов CIFS
adcli	Инструмент для выполнения действий в домене Active Directory
ldapsearch	Утилита для поиска информации в LDAP
testparm	Проверка корректности содержимого основного файла конфигурации Samba — **/etc/samba/smb.conf**

7.11.1. samba-tool

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

Таблица 7.9. Основные команды samba-tool

Команда	Описание
computer	Управление учетными записями компьютеров
contact	Управление контактами
dbcheck	

Команда	Описание
	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
forest	Управление конфигурацией леса
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 списка процессов
ou	Управление организационными подразделениями (OU)
rodc	Управление контроллером домена (Read-Only Domain Controller, RODC)
schema	Управление и запрос схемы
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

Получить дополнительную информацию можно на справочной странице samba-tool(8) (**`man samba-tool`**).

Пример получения дополнительной информации о подкоманде:

```
$ samba-tool fsmo --help
```

Примеры:

- вывести список групповых политик:

```
# samba-tool gpo listall
GPO          : {31B2F340-016D-11D2-945F-00C04FB984F9}
display name : Default Domain Policy
path         : \
```

```
\test.alt\sysvol\test.alt\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}
dn           :
CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=test,DC=alt
version      : 0
flags        : NONE

GPO          : {FE6268E4-FDEB-4DCA-94E8-BB1170C66F45}
display name : scripts
path         : \\test.alt\sysvol\test.alt\Policies\{FE6268E4-FDEB-4DCA-94E8-
BB1170C66F45}
dn           : CN={FE6268E4-FDEB-4DCA-94E8-
BB1170C66F45},CN=Policies,CN=System,DC=test,DC=alt
version      : 65536
flags        : NONE

GPO          : {6AC1786C-016F-11D2-945F-00C04FB984F9}
display name : Default Domain Controllers Policy
path         : \
\test.alt\sysvol\test.alt\Policies\{6AC1786C-016F-11D2-945F-00C04FB984F9}
dn           :
CN={6AC1786C-016F-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=test,DC=alt
version      : 0
flags        : NONE

GPO          : {44F1A3E9-BD0D-44D7-AC1D-CEEF2817C573}
display name : Общие каталоги
path         : \\test.alt\sysvol\test.alt\Policies\{44F1A3E9-BD0D-44D7-AC1D-
CEEF2817C573}
dn           : CN={44F1A3E9-BD0D-44D7-AC1D-
CEEF2817C573},CN=Policies,CN=System,DC=test,DC=alt
version      : 0
flags        : NONE
```

- вывести все связанные контейнеры для объекта групповой политики:

```
# samba-tool gpo listcontainers {44F1A3E9-BD0D-44D7-AC1D-CEEF2817C573}
Container(s) using GPO {44F1A3E9-BD0D-44D7-AC1D-CEEF2817C573}
    DN: OU=OU,DC=test,DC=alt
    DN: OU=KDE,DC=test,DC=alt
```

- вывести список групповых политик, связанных с контейнером:

```
# samba-tool gpo getlink OU=OU,DC=test,DC=alt
GPO(s) linked to DN OU=OU,DC=test,DC=alt
    GPO     : {96D5897A-CEFB-4A1B-90AF-5D83707130C4}
    Name    : Файлы
    Options : NONE

    GPO     : {A12547D7-2FFA-4E37-9382-D6767489E3DF}
    Name    : kde
    Options : NONE

    GPO     : {75E65DF7-56A7-48E1-A393-F5FFAA1010FD}
    Name    : Control_ping
    Options : NONE

    GPO     : {FE6268E4-FDEB-4DCA-94E8-BB1170C66F45}
    Name    : scripts
```

```
    Options : NONE

    GPO     : {44F1A3E9-BD0D-44D7-AC1D-CEEF2817C573}
    Name    : Общие каталоги
    Options : NONE

    GPO     : {0CCFA74C-57F5-42B5-98E2-007D4A59C4C4}
    Name    : firefox
    Options : NONE

    GPO     : {2CF4EB19-343E-448A-BBBC-A9EC2F7C22E9}
    Name    : Установка пакетов
    Options : NONE
```

7.11.2. wbinfo

Команда **wbinfo** создает запросы и возвращает информацию к (от) демона winbindd(8).

Таблица 7.10. Параметры команды wbinfo

Параметр	Описание	Пример

-a|--authenticate username%password	Попытаться аутентифицировать пользователя через winbindd(8).
	
	Проверяет два метода аутентификации: plaintext password (применяется при входе пользователя в систему локально), challenge/response password (использует NTLM или Kerberos).
		`$ wbinfo -a TEST\\ivanov`
		`Enter TEST\ivanov's password:`
		`plaintext password authentication succeeded`
		`Enter TEST\ivanov's password:`
		`challenge/response password authentication succeeded`

--allocate-gid	Получить новый GID из idmap	
--allocate-uid	Получить новый UID из idmap	

--all-domains	Вывести список всех доменов (доверенных и собственный)	`$ wbinfo --all-domains`
		`BUILTIN`
		`TEST`
		`EXAMPLE`

-c|--change-secret		

Параметр	Описание	Пример
	Изменить пароль доверительной учетной записи. Может использоваться вместе с доменом для изменения паролей учетных записей междоменного доверия.	
--ccache-save <имя_пользователя>%<пароль>	Сохранить имя пользователя и пароль для ccache	
--change-user-password <имя_пользователя>	Изменить пароль пользователя (будет запрошен старый и новый пароль)	(??)
--dc-info <домен>	Вывести текущий контроллер домена для домена	`$ wbinfo --dc-info TEST` `dc1.test.alt (192.168.0.122)`
--domain <домен>	Определяет домен, в котором будут выполняться любые указанные операции	

-D|--domain-info <домен>	Показать информацию об указанном домене	`$ wbinfo -D TEST`
		`Name : TEST`
		`Alt_Name : test.alt`
		`SID : S-1-5-21-578923263-1107570656-1287136478`
		`Active Directory : Yes`
		`Native : Yes`
		`Primary : Yes`

--dsgetdcname <домен>	Найти DC для домена	`$ wbinfo --dsgetdcname TEST`
		`\\dc1.test.alt`
		`\\192.168.0.122`
		`1`
		`d75c7b83-9472-4646-adb2-52b3d6968eb6`
		`test.alt`

Параметр	Описание	Пример

		`test.alt`
		`0xe00013fd`
		`Default-First-Site-Name`
		`Default-First-Site-Name`

--gid-info <gid>	Получить информацию о группе по gid	`$ wbinfo --gid-info 10000` `domain admins:*:10000:`
--group-info <группа>	Получить информацию о группе по имени группы	`$ wbinfo --group-info "TEST\\domain admins"` `domain admins:*:10000:`

-g|--domain-groups	Вывести список доменных групп	`$ wbinfo -g`
		`…`
		`TEST\domain admins`
		`TEST\domain users`
		`TEST\domain guests`
		`TEST\domain computers`
		`…`

--get-auth-user	Эта функция была перенесена в утилиту **net** (см. **net help getauthuser**)	
--getdcname <домен>	Вывести имя контроллера домена для указанного домена	`$ wbinfo --getdcname TEST` `DC1`
-G|--gid-to-sid <gid>		`$ wbinfo -G 10000` `S-1-5-21-578923263-1107570656-1287136478-512`

Параметр	Описание	Пример
	Преобразовать идентификатор группы UNIX в SID Windows NT. Если указанный gid не относится к диапазону gid idmap, операция завершится ошибкой.	
-i|--user-info <имя_пользователя>	Вывести информацию о пользователе	`$ wbinfo -i TEST\\ivanov` `ivanov:*:10000:10001:Иван Иванов:/home/TEST.ALT/ivanov:/bin/bash`
-I|--WINS-by-ip ip	Вывести NetBIOS-имя, связанное с IP-адресом	`$ wbinfo -I 192.168.0.135` `192.168.0.135 WORK135`

-K|--krb5auth <имя_пользователя>%<пароль>	Попытаться аутентифицировать пользователя через Kerberos	`$ wbinfo -K TEST\\ivanov`
		`Enter TEST\ivanov's password:`
		`plaintext kerberos password authentication for [TEST\ivanov] succeeded (requesting cctype: FILE)`

--krb5ccname KRB5CCNAME	Запросить определенный тип кэша учетных данных Kerberos, используемый для аутентификации	
--lanman	Использовать криптографию Lanman для аутентификации пользователей	
--logoff	Выйти из системы	
--logoff-uid UID		

Параметр	Описание	Пример
	Определяет идентификатор пользователя, используемый во время запроса на выход из системы	
--logoff-user <имя_пользователя>	Определяет имя пользователя, используемое во время запроса на выход из системы	
--lookup-sids SID1,SID2...	Поиск SID	`$ wbinfo --lookup-sids S-1-5-21-578923263-1107570656-1287136478-512` `S-1-5-21-578923263-1107570656-1287136478-512 -> <none>\Domain Admins 2`

-m|--trusted-domains	Вывести список доверенных доменов	`$ wbinfo --trusted-domains`
		`BUILTIN`
		`TEST`
		`EXAMPLE`

-n|--name-to-sid <имя>	Вывести SID, связанный с указанным именем. Если домен не указан, используется домен, указанный в параметре ***workgroup*** **smb.conf**	`$ wbinfo -n TEST\\ivanov` `S-1-5-21-578923263-1107570656-1287136478-1103 SID_USER (1)`
-N|--WINS-by-name <name>	Вывести IP-адрес, связанный с именем NetBIOS, указанным в параметре name	`$ wbinfo -N WORK135` `192.168.0.135 WORK135`
--ntlmv1	Использовать криптографию NTLMv1 для аутентификации пользователей	
--ntlmv2		

Параметр	Описание	Пример
	Использовать криптографию NTLMv2 для аутентификации пользователей	

--online-status <домен>	Показать, поддерживает ли winbind в настоящее время активное соединение или нет. Если домен не указан, будет выведен статус текущего домена	`$ wbinfo --online-status`
		`BUILTIN : active connection`
		`TEST : active connection`

--own-domain	Вывести собственный домен	`$ wbinfo --own-domain` `TEST`

--pam-logon <имя_пользователя>%<пароль>	Попытаться аутентифицировать пользователя так же, как это сделал бы pam_winbind	`$ wbinfo --pam-logon ivanov`
		`Enter ivanov's password:`
		`plaintext password authentication succeeded`

-p|--ping	Проверяет запущен ли winbindd(8)	`$ wbinfo -p` `Ping to winbindd succeeded`
-P|--ping-dc	Проверить безопасное соединение с контроллером домена	`$ wbinfo -P` `checking the NETLOGON for domain[TEST] dc connection to "dc1.test.alt" succeeded`

Параметр	Описание	Пример

-r|--user-groups <имя_пользователя>	Получить список идентификаторов групп, к которым принадлежит пользователь. Доступно только при наличии пользователя на контроллере домена	`$ wbinfo -r ivanov`
		`10001`
		`10003`

-R|--lookup-rids rid1, rid2, rid3..	Преобразовать RID в имена	
--remove-gid-mapping GID,SID	Удалить существующее сопоставление GID и SID из базы данных	
--remove-uid-mapping UID,SID	Удалить существующее сопоставление UID и SID из базы данных	
-s|--sid-to-name sid	Преобразовать SID в имя	`$ wbinfo -s S-1-5-21-578923263-1107570656-1287136478-1103` `TEST\ivanov 1`
--separator	Вывести активный разделитель winbind	`$ wbinfo --separator` `\`
--sequence	Команда устарела, вместо неё следует использовать параметр ***--online-status***	
--set-auth-user <имя_пользователя>%<пароль>	Эта функция была перенесена в утилиту **net** (см. **net help setauthuser**)	
--set-gid-mapping GID,SID	Создать сопоставление GID и SID в базе данных	
--set-uid-mapping UID,SID	Создать сопоставление UID и SID в базе данных	
-S|--sid-to-uid sid	Преобразовать SID в идентификатор пользователя	`$ wbinfo -S S-1-5-21-578923263-1107570656-1287136478-1103` `10000`

Параметр	Описание	Пример
--sid-aliases sid	Получить псевдонимы SID для заданного SID	
--sid-to-fullname sid	Преобразовать SID в полное имя пользователя (ДОМЕН\имя пользователя)	`$ wbinfo --sid-to-fullname S-1-5-21-578923263-1107570656-1287136478-1103` `TEST\Иван Иванов 1`
--sids-to-unix-ids sid1,sid2,sid3...	Преобразовать SID в Unix ID	`$ wbinfo --sids-to-unix-ids S-1-5-21-578923263-1107570656-1287136478-1103` `S-1-5-21-578923263-1107570656-1287136478-1103 -> uid 10000`
-t|--check-secret	Проверить, что доверительная учетная запись рабочей станции, созданная при добавлении сервера Samba в домен Windows NT, работает. Может использоваться вместе с доменом для проверки учетных записей междоменного доверия	

-u|--domain-users	Вывести список доменных пользователей	`$ wbinfo -u`
		`administrator`
		`krbtgt`
		`ivanov`
		`guest`

--uid-info uid	Получить информацию о пользователе по идентификатору	`$ wbinfo --uid-info 10000` `ivanov:*:10000:10001:Иван Иванов:/home/TEST.ALT/ivanov:/bin/bash`

Параметр	Описание	Пример
--usage	Вывести краткую справку о программе	

--user-domgroups sid	Вывести группы пользователей домена	`$ wbinfo --user-domgroups S-1-5-21-578923263-1107570656-1287136478-1103`
		`S-1-5-21-578923263-1107570656-1287136478-1103`
		`S-1-5-21-578923263-1107570656-1287136478-513`

--user-sidinfo sid	Получить информацию о пользователе по sid	`$ wbinfo --user-sidinfo S-1-5-21-578923263-1107570656-1287136478-1103` `ivanov:*:10000:10001:Иван Иванов:/home/TEST.ALT/ivanov:/bin/bash`

--user-sids sid	Получить SID групп пользователя	`$ wbinfo --user-sids S-1-5-21-578923263-1107570656-1287136478-1103`
		`S-1-5-21-578923263-1107570656-1287136478-1103`
		`S-1-5-21-578923263-1107570656-1287136478-513`
		`S-1-5-32-545`

-U|--uid-to-sid uid	Преобразовать идентификатор пользователя UNIX в SID	`$ wbinfo -U 10000` `S-1-5-21-578923263-1107570656-1287136478-1103`
-Y|--sid-to-gid sid	Преобразовать SID в идентификатор группы UNIX	

Параметр	Описание	Пример
		`$ wbinfo -Y S-1-5-21-578923263-1107570656-1287136478-513 10001`

7.11.3. net

net — инструмент администрирования Samba и удаленных серверов CIFS. Синтаксис:

```
net <протокол> <функция> <дополнительные_параметры> <параметры_цели>
```

где <протокол> — протокол, используемый при выполнении команды. Возможные значения: ads (Active Directory),rap (Win9x/NT3) или rpc (WindowsNT4/2000/2003/2008/2012). Если протокол не указан, **net** пытается определить его автоматически.

Таблица 7.11. Основные команды net ads

Команда	Описание
info	Вывод информации о домене
join	Присоединение машины к домену
testjoin	Проверка, действителен ли пароль учетной записи компьютера
leave	Удалить локальную машину из домена AD
status	Вывод информации об учетной записи компьютера
user	Список/изменение пользователей
group	Список/изменение групп
dns	Выполнить динамическое обновление DNS
password	Изменить пароль пользователей
changetrustpw	Изменить пароль доверительной учетной записи
printer	Список/изменение записей принтера
search	Выполнить поиск LDAP с использованием фильтра
dn	Выполнить поиск LDAP по DN
sid	Выполнить поиск LDAP по SID
workgroup	Показать имя рабочей группы
lookup	Найти контроллер домена AD с помощью поиска CLDAP
keytab	Управление локальным файлом keytab
spnset	Управление именами участников-служб (SPN)
gpo	Управление объектами групповой политики
kerberos	Управление keytab Kerberos

Команда	Описание
enctypes	Список/изменение enctypes

Получить дополнительную информацию можно на справочной странице net(8) (**`man net`**).

Пример получения дополнительной информации о подкоманде:

```
# net time --help
```

Получение информации о домене:

```
# net ads info
LDAP server: 192.168.0.122
LDAP server name: dc1.test.alt
Realm: TEST.ALT
Bind Path: dc=TEST,dc=ALT
LDAP port: 389
Server time: Ср, 27 мар 2024 10:36:51 EET
KDC server: 192.168.0.122
Server time offset: 2
Last machine account password change: Ср, 20 мар 2024 11:13:27 EET
```

Получение информации об учетной записи компьютера:

```
# net ads status -U administrator
```

7.11.4. adcli

`adcli` — инструмент для выполнения действий в домене Active Directory.

Таблица 7.12. Основные команды adcli

Команда	Описание
info домен	Вывести информацию о домене
join домен	Присоединить данную машину к домену (создает учетную запись компьютера в домене и настраивает keytab для этой машины. Не настраивает службу аутентификации, например, sssd)
update	Обновляет пароль учетной записи компьютера на контроллере домена для локальной машины, записывает новые ключи в keytab и удаляет старые ключи
testjoin	Проверить, действителен ли пароль учетной записи компьютера
create-user [--domain=домен] пользователь	Создать учетную запись пользователя
delete-user [--domain=домен] пользователь	Удалить учетную запись пользователя
passwd-user [--domain=домен] пользователь	Установить (повторно) пароль пользователя
create-group [--domain=домен] группа	Создать группу
delete-group [--domain=домен] группа	Удалить группу
	Добавить пользователей в группу

Команда	Описание
add-member [--domain=домен] группа пользователь или компьютер…	
remove-member [--domain=домен] группа пользователь…	Удалить пользователей из группы
preset-computer [--domain=домен] компьютер…	Предустановить учетные записи компьютеров (предварительно создает одну или несколько учетных записей компьютеров в домене, чтобы позже компьютеры могли использовать их при присоединении к домену. При этом, машины могут присоединяться с помощью одноразового пароля или автоматически без пароля)
reset-computer [--domain=домен] компьютер	Сбросить учетную запись компьютера (если соответствующая машина присоединена к домену, её членство будет нарушено)
delete-computer [--domain=домен] компьютер	Удалить учетную запись компьютера
show-computer [--domain=домен] компьютер	Показать атрибуты учетной записи компьютера, хранящиеся в AD
create-msa [--domain=домен]	Создать управляемую учетную запись службы (MSA) в заданном домене AD (это бывает нужно, если компьютер не должен присоединяться к домену Active Directory, но к нему необходим LDAP доступ)

Получить дополнительную информацию можно на справочной странице adcli(8) (**`man adcli`**).

Пример получения дополнительной информации о подкоманде:

```
# adcli testjoin --help
```

Получение информации о домене:

```
# adcli info test.alt
[domain]
domain-name = test.alt
domain-short = TEST
domain-forest = test.alt
domain-controller = dc1.test.alt
domain-controller-site = Default-First-Site-Name
domain-controller-flags = pdc gc ldap ds kdc timeserv closest writable good-
timeserv full-secret
domain-controller-usable = yes
domain-controllers = dc1.test.alt dc2.test.alt
[computer]
computer-site = Default-First-Site-Name
```

Показать атрибуты учетной записи компьютера:

```
# adcli show-computer -D test.alt win2012
Password for Administrator@TEST.ALT:
sAMAccountName:
 WIN2012$
```

```
userPrincipalName:
 - not set -
msDS-KeyVersionNumber:
 1
msDS-supportedEncryptionTypes:
 28
dNSHostName:
 win2012.test.alt
servicePrincipalName:
 HOST/win2012.test.alt
 RestrictedKrbHost/win2012.test.alt
 HOST/WIN2012
 RestrictedKrbHost/WIN2012
 Dfsr-12F9A27C-BF97-4787-9364-D31B6C55EB04/win2012.test.alt
operatingSystem:
 Windows Server 2012 R2 Standard
operatingSystemVersion:
 6.3 (9600)
operatingSystemServicePack:
 - not set -
pwdLastSet:
 133294743593838200
userAccountControl:
 4096
description:
 - not set -
```

Создать группу testldap в подразделении OU:

```
# adcli create-group -D test.alt -O OU=OU,dc=test,dc=alt testldap
Password for Administrator@TEST.ALT:
```

7.11.5. ldapsearch

`ldapsearch` — утилита для поиска информации в LDAP. Синтаксис:

```
ldapsearch <параметры> <фильтр> <атрибуты>
```

`ldapsearch` открывает соединение с сервером LDAP, подключается к нему и выполняет поиск с помощью фильтра.

Если утилита **`ldapsearch`** найдет одну или несколько записей, то значения указанных атрибутов этих записей будут переданы в стандартный поток вывода. Если в этом списке указан знак *, возвращаются все пользовательские атрибуты. Если в этом списке указан знак +, возвращаются все операционные атрибуты. Если атрибуты не указаны, то возвращаются все пользовательские атрибуты.

Если утилита **`ldapsearch`** найдет одну или несколько записей, то значения указанных атрибутов этих записей будут переданы в стандартный поток вывода. Если атрибуты не указаны, то возвращаются все атрибуты.

Результаты поиска отображаются в виде расширенной версии LDIF. Формат вывода контролируется с помощью параметра ***-L***.

Таблица 7.13. Параметры команды ldapsearch

Параметр	Описание
Параметры поиска	
-a {never|always|search|find}	Задает способ преобразования псевдонимов. Может принимать значения: never (по умолчанию), always, search или find, указывающие, соответственно, что псевдонимы не преобразуются, преобразуются всегда, преобразуются при поиске, либо преобразуются только при определении базового объекта для поиска
-A	Получить только атрибуты (без значений)
-b basedn	Позволяет переопределить заданную по умолчанию начальную точку поиска
-c	Режим продолжения операции (не останавливать поиск при ошибках)
-E [!]ext[=extparam]	Указывает расширения поиска. Знак '!' обозначает критичность расширения. Общие расширения: [!]domainScope (диапазон домена) !dontUseCopy [!]mv=<filter> (RFC 3876 фильтр совпавших значений) [!]pr=<size>[/prompt|noprompt] (RFC 2696 постраничный вывод результатов/запрос вывода) [!]sss=[-]<attr[:OID]>[/[-]<attr[:OID]>...] (RFC 2891 сортировка на стороне сервера) [!]subentries[=true|false] (RFC 3672 подзаписи) [!]sync=ro[/<cookie>] (RFC 4533 LDAP Sync refreshOnly) [!]sync=rp[/<cookie>][/<slimit>] (LDAP Sync refreshAndPersist) [!]vlv=<before>/<after>(/<offset>/<count>|:<value>) (ldapv3-vlv-09 вид виртуального списка) [!]deref=derefAttr:attr[,...][;derefAttr:attr[,...][;...]] [!]<oid>[=:<b64value>] (общий контроль; нет обработки ответа)
-f file	Считать серию строк из файла ***file*** и выполнить по одному поиску LDAP для каждой строки. В этом случае заданный в командной строке фильтр ***filter*** интерпретируется как шаблон, в котором первое и только первое вхождение ***%s*** заменяется строкой из файла ***file***. Любые

Параметр	Описание
	другие вхождения символа % в шаблоне будут рассматриваться как ошибка. Если требуется, чтобы в поисковом фильтре присутствовал символ %, он должен быть закодирован как \25 (смотрите RFC 4515). Если в качестве значения ***file*** указан символ «-», то строки считываются со стандартного ввода.
-F prefix	URL-префикс для временных файлов (по умолчанию: file://path, где **path** либо **/tmp/.private/<user>**, либо значение, указанное в параметре ***-T***)
-l limit	Ограничение на время поиска (в секундах). Значение 0 (ноль) или none означает, что ограничений нет. Значение max означает максимальное допустимое протоколом значение (целое число)
-L[LL]	Управление выводом результатов поиска в формате обмена данными LDAP (LDAP Data Interchange Format): ***-L*** — вывести ответы в формате LDIFv1, ***-LL*** — отключить вывод комментариев, ***-LLL*** — отключить вывод версии LDIF.
-M[M]	Включить элемент управления Manage DSA IT. ***-MM*** делает этот элемент управления критичным.
-P {2|3}	Версия протокола LDAP (по умолчанию 3)
-s {base|one|sub|children}	Задает область поиска. Может принимать одно из следующих значений: base, one, sub (по умолчанию) или children, что означает поиск только по базовому объекту, на одном уровне, по всему поддереву и по дочерним записям соответственно
-S attr	Отсортировать возвращаемые записи по атрибуту ***attr***. По умолчанию возвращаемые записи не сортируются. Если в качестве ***attr*** задана строка нулевой длины ("""), записи сортируются по компонентам их уникального имени Distinguished Name. По умолчанию **ldapsearch** выводит записи по мере их получения. При использовании параметра ***-S*** все данные сначала получаются, потом сортируются, потом выводятся.
-t[t]	При указании одного ***-t*** полученные непечатаемые значения записываются в набор временных файлов (полезно при работе со значениями, содержащими несимвольные данные, такими как jpegPhoto или audio). При указании второго ***-t*** все полученные значения записываются в файлы.
-T path	

Параметр	Описание
	Временные файлы записываются в указанный в ***path*** каталог (по умолчанию **/tmp/.private/<user>**)
-u	Включить в вывод форму удобного для пользователя имени (User Friendly Name, UFN) уникального имени (Distinguished Name, DN)
-z limit	Ограничить количество возвращаемых в результате поиска записей значением **limit**. Значение 0 (ноль) или none означает, что ограничений нет. Значение max означает максимальное допустимое протоколом значение (целое число).
Общие параметры	
-d debuglevel	Установить уровень отладки LDAP
-D binddn	Использовать указанное в ***binddn*** уникальное имя Distinguished Name при подсоединении к каталогу LDAP. При SASL-подсоединениях сервер будет игнорировать это значение.
-e [!]ext[=extparam]	Указывает общие расширения. Знак '!' обозначает критичность расширения. Общие расширения: • [!]assert=<filter> (RFC 4528; фильтр RFC 4515) • [!]authzid=<authzid> (RFC 4370; "dn:<dn>" или "u:<user>") • [!]chaining[=<resolveBehavior>[/<continuationBehavior>]] • [!]manageDSAit (RFC 3296) • [!]noop • ppolicy • [!]postread[=<attrs>] (RFC 4527; разделённый запятыми список атрибутов) • [!]preread[=<attrs>] (RFC 4527; разделённый запятыми список атрибутов) • [!]relax • [!]sessiontracking • abandon, cancel, ignore (сигнал SIGINT посылает abandon/cancel, либо в ответ на него посылается ignore; если расширение помечено как критичное, сигнал SIGINT не принимается; ненастоящие элементы управления
-h host	Сервер LDAP
-H URI	Указывает URI (возможно, несколько), ссылающийся на LDAP-сервер (серверы). В URI допускаются поля: протокол/хост/порт.

Параметр	Описание
-I	Использовать интерактивный режим SASL.
-n	Демонстрируется, что будет сделано, но реальный поиск не выполняется. Используется для отладки совместно с параметром ***-v***
-N	Не использовать обратное разрешение DNS для получения канонического имени хоста SASL.
-O props	Параметры безопасности SASL
-o opt[=optparam]	Указывает опции общего назначения. Возможные опции: - nettimeout=<timeout> (в секундах, либо «none» или «max») - ldif-wrap=<width> (в символах, либо «no» для предотвращения переноса строк)
-p порт	Порт, на котором сервер LDAP принимает запросы. Номер порта по умолчанию — 389. Если номер порта не задан, и указан параметр ***-Z***, то применяется номер порта LDAP SSL по умолчанию, равный 636.
-Q	Использовать тихий режим SASL. Запросы не выводятся никогда.
-R realm	Задаёт realm аутентификационного идентификатора для SASL. Форма realm зависит от того, какой механизм аутентификации в действительности используется.
-U authcid	Идентификатор аутентификации SASL. Форма идентификатора зависит от того, какой механизм аутентификации в действительности используется.
-v	Запустить в подробном режиме (диагностические сообщения посылаются в стандартный вывод)
-V[V]	Вывести информацию о версии. При указании ***-VV***, после вывода информации о версии осуществляется выход. При указании ***-V***, после вывода информации о версии выполняется поиск согласно заданным критериям.
-w passwd	Использовать указанное значение ***passwd*** в качестве пароля для простой аутентификации.
-W	

Параметр	Описание
	Запрашивать ввод пароля для простой аутентификации (используется для того, чтобы не указывать пароль в командной строке).
-x	Использовать простую аутентификацию
-X authzid	Идентификатор авторизации SASL ("dn:<dn>" или "u:<user>")
-y file	Считать пароль из файла ***file***. В качестве пароля используется всё содержимое файла. Поэтому файл не должен содержать символа переноса строки.
-Y mech	Задаёт механизм SASL, который будет использоваться для аутентификации. Если параметр не указан, программа выберет лучший из известных серверу механизмов.
-Z[Z]	Запустить запрос TLS (***-ZZ*** для запроса успешного ответа)

7.11.5.1. Фильтр

Фильтр должен быть указан в строковом формате фильтров LDAP (см. RFC 4515). Если фильтр не указан, используется фильтр по умолчанию (objectClass=*).

Синтаксис LDAP-фильтра имеет вид:

```
<Атрибут><оператор сравнения><значение>
```

Вместо имени атрибута можно использовать его идентификатор (Attribute-Id). Тело фильтра должно быть заключено в скобки.

Таблица 7.14. Примеры LDAP-фильтров

Запрос	LDAP фильтр
Все пользователи:	(sAMAccountType=805306368)
Отключенные (Disabled) пользователи:	(&(sAMAccountType=805306368)(useraccountcontrol:1.2.840.113556.1.4.803:=2))
Заблокированные (Locked) пользователи:	(&(sAMAccountType=805306368)(badPwdCount>=4))
Пользователи, у которых в настройках указано «Пароль никогда не истекает»	(&(objectCategory=person)(objectClass=user)(userAccountControl:1.2.840.113556.1.4.803:=65536))
Пользователи которые не меняли пароль с 5 мая 2023 года (см. https://www.epochconverter.com/ldap для преобразования даты во временную метку Windows)	(&(objectCategory=person)(pwdLastSet<=133278047990000000))
Пользователи с незаполненным полем mail	(&(objectCategory=group)(!(mail=*)))

Запрос	LDAP фильтр
Пользователи, которые должны сменить пароль при следующем входе в систему	(&(sAMAccountType=805306368)(pwdLastSet=0))
Пользователи с ограниченным сроком действия учетной записи	(&(sAMAccountType=805306368)(accountExpires>=1)(accountExpires<=9223372036854775806))
Пользователи, созданные за определенный период (формат даты: YYYY MM DD HH mm ss.s Z)	(&(sAMAccountType=805306368)(whenCreated>=20230401000000.0Z<=20230701000000.0Z))
Все компьютеры	(objectCategory=computer)
Все контроллеры домена	(&(objectCategory=computer)(userAccountControl:1.2.840.113556.1.4.803:=8192))
Контроллеры домена, доступные только для чтения	(&(objectCategory=computer)(userAccountControl:1.2.840.113556.1.4.803:=67108864))
Группы в которых нет пользователей	(&(objectCategory=group)(!(member=*)))
Группы с ключевым словом admin в имени	(&(objectCategory=group)(samaccountname=*admin*))
Все группы безопасности (Security)	(&(objectCategory=group)(groupType:1.2.840.113556.1.4.803:=2147483648))
Все члены группы Sales (без учёта вложенности)	(memberOf=CN=Sales,CN=Users,DC=test,DC=alt)
Все члены группы Sales (с учётом вложенности)	(memberOf:1.2.840.113556.1.4.1941:=CN=Sales,CN=Users,DC=test,DC=alt)
Все группы, в которые входит пользователь testldap	(&(objectCategory=group)(member=CN=testldap,CN=Users,DC=test,DC=alt)))
Все подразделения (OU)	(objectCategory=organizationalUnit)
Все объекты групповой политики	(objectCategory=groupPolicyContainer)
Все отношения доверия	(objectClass=trustedDomain)
Объекты связанные с ролями FSMO	(fsMORoleOwner=*)
PDC Emulator	(&(objectClass=domainDNS)(fSMORoleOwner=*))
RID Master	(&(objectClass=rIDManager)(fSMORoleOwner=*))
Объект AD с определенным SID	(objectSID=S-1-5-21-1723588197-2340999690-1379671080-1105)

7.11.5.2. Формат вывода

Если найдена одна или несколько записей, то каждая запись передается в поток вывода в следующем формате:

```
Отличительное имя (DN)
имя_атрибута: значение
имя_атрибута: значение
имя_атрибута: значение
…
```

Записи разделяются пустыми строками.

Если задан параметр ***-t*** вместо реальных значений атрибутов будут выводиться URI временных файлов, в которые эти значения помещаются. Если задан параметр ***-A*** будут выводиться только имена атрибутов.

Примечание

Значение атрибута записывается в 7-битной кодировке ASCII и отделяется от его имени символом «:». Значения, не подходящие под эту кодировку, записываются в кодировке base64 и отделяются от имени атрибута символами «::»:

```
имя_атрибута:: base64_значение_атрибута
```

Например:

```
dn::
Q0490JfQsNC50YbQtdCy0LAg0J7Qu9GM0LPQsCxDTj1Vc2VycyxEQz10ZXN0LERDPWFsdA==
cn:: 0JfQsNC50YbQtdCy0LAg0J7Qu9GM0LPQsA==

…
$  echo "0JfQsNC50YbQtdCy0LAg0J7Qu9GM0LPQsA==" | base64 -d
Зайцева Ольга
```

Чтобы отобразить строки в кодировке base64 можно использовать следующую команду:

```
$ ldapsearch -LLL -D testldap@test.alt -x -W | perl -MMIME::Base64 -
MEncode=decode -n -00 -e 's/\n
+//g;s/(?<=:: )(\S+)/decode("UTF-8",decode_base64($1))/eg;print'
```

7.11.5.3. Примеры

Вывести всех пользователей, фамилия которых начинается с буквы «К»:

```
$ ldapsearch -LLL -H ldap://192.168.0.122:389 \
-D testldap@test.alt -b "dc=test,dc=alt" \
-x -W "(&(sAMAccountName=*)(sn=K*))" cn sn
```

где:

- ***-H ldap://192.168.0.122:389*** — сервер LDAP;
- ***-D testldap@test.alt*** — пользователь с правом чтения в каталоге LDAP;
- ***-b "dc=test,dc=alt"*** — контейнер AD, в котором будет выполняться поиск;

- ***-x*** — использовать простую аутентификацию;
- ***-W*** — спросить пароль;
- ***"(&(sAMAccountName=*)(sn=K*))"*** — выражение, по которому будут отфильтрованы результаты;
- ***cn sn*** — поля, которые необходимо вывести;

Параметры по умолчанию можно задать в файле **/etc/openldap/ldap.conf**, например:

```
BASE    dc=test,dc=alt
URI     ldap://dc1.test.alt
```

Команда с использованием базы поиска и URI по умолчанию:

```
$ ldapsearch -LLL -D testldap@test.alt \
-x -W "(&(sAMAccountName=*)(sn=K*))" cn sn
```

Вывести фамилию и электронную почту всех пользователей, из подразделения OU, у которых непустое поле mail:

```
$ ldapsearch -LLL -H ldap://192.168.0.122:389 \
-D testldap@test.alt -b "ou=OU,dc=test,dc=alt" -s one \
-x -W "(&(sAMAccountName=*)(mail=K*))" sn mail
```

В данном примере не будут выведены записи только из подразделения OU, но не из его дочерних подразделений.

Считать последовательность строк из файла **new.filter** и выполнить функцию поиска LDAP для каждой строки:

```
$ ldapsearch -H ldap://192.168.0.122:389 \ -D testldap@test.alt -b
"dc=test,dc=alt" -x -W -f new.filter "(samaccountname=%s)" cn
```

Содержимое файла **new.filter**:

```
z*
ivanov
k*
*k
```

Команда выполняет поиск по поддереву для каждого фильтра, начиная с samaccountname=z*. Когда этот поиск завершается, начинается поиск для фильтра cn=ivanov и т.д. Пример вывода вышеуказанной команды с параметром ***-n***:

```
 LDAPv3
# base <dc=test,dc=alt> with scope subtree
# filter pattern: (samaccountname=%s)
# requesting: dn
#

#
# filter: (samaccountname=z*)
#
```

```
#
# filter: (samaccountname=ivanov)
#

#
# filter: (samaccountname=k*)
#

#
# filter: (samaccountname=*k)
#
```

7.11.6. sssctl

sssctl — это инструмент командной строки, который предоставляет унифицированный способ получения информации о состоянии Security System Services Daemon (SSSD).

Утилиту **sssctl** можно использовать для сбора информации:

- состоянии домена;
- аутентификации пользователя;
- доступа пользователей к клиентам определенного домена;
- информация о кэшированном содержимом.

С помощью утилиты **sssctl** можно:

- управлять кэшем SSSD;
- управлять журналами;
- проверить конфигурационные файлы.

Таблица 7.15. Основные команды sssctl

Команда	Описание
Статус SSSD	
domain-list	Вывести список доступных доменов
domain-status домен	Вывести информацию о домене
user-checks пользователь	Вывести информацию о пользователе и проверить аутентификацию
access-report домен	Создание отчёта о правилах управления доступом для домена, которые применяются к клиентскому компьютеру (работает только для домена FreeIPA)
Информация о кэшированном содержимом	
user-show пользователь	Информация о кэше пользователя
group-show группа	Информация о кэше группы
netgroup-show группа	Информация о кэше сетевой группы
Инструменты для работы с локальными данными	

Команда	Описание
client-data-backup	Резервное копирование локальных данных
client-data-restore	Восстановление локальных данных из резервной копии
cache-remove	Резервное копирование локальных данных и удаление кэшированного содержимого
cache-upgrade	Выполнить обновление кеша
cache-expire	Сделать недействительными кешированные объекты
cache-index действие	Управление индексами кеша
Инструменты для управления журналированием	
logs-remove	Удалить существующие файлы журналов SSSD
logs-fetch файл	Архивировать файлы журналов SSSD в tarball
debug-level [уровень]	Изменить или вывести уровень журналирования SSSD
analyze	Анализ зарегистрированных данных
Инструменты для проверки файлов конфигурации	
config-check	Выполнить статический анализ конфигурации SSSD
Инструменты, связанные с сертификатом	
cert-show сертификат	Вывести информацию о сертификате
cert-map сертификат	Показать пользователей, привязанных к сертификату

Получить дополнительную информацию можно на справочной странице sssctl(8) (**`man sssctl`**).

Пример получения дополнительной информации о подкоманде:

```
# sssctl user-show --usage
```

или

```
# sssctl user-show --help
```

Получение информации о домене:

```
# sssctl domain-status TEST.ALT
Online status: Online

Active servers:
AD Global Catalog: dc1.test.alt
AD Domain Controller: dc1.test.alt

Discovered AD Global Catalog servers:
- dc1.test.alt

Discovered AD Domain Controller servers:
- dc1.test.alt
```

Показать информацию о кэше пользователя:

```
# sssctl user-show kim
Name: kim
Cache entry creation date: 12/28/22 13:39:46
Cache entry last update time: 06/19/23 09:55:29
Cache entry expiration time: Expired
Initgroups expiration time: Expired
Cached in InfoPipe: No
```

Показать данные авторизации пользователя:

```
# sssctl user-checks kim
user: kim
action: acct
service: system-auth

SSSD nss user lookup result:
 - user name: kim
 - user id: 1187401107
 - group id: 1187400513
 - gecos: Олег Ким
 - home directory: /home/TEST.ALT/kim
 - shell: /bin/bash

SSSD InfoPipe user lookup result:
 - name: kim
 - uidNumber: 1187401107
 - gidNumber: 1187400513
 - gecos: Олег Ким
 - homeDirectory: not set
 - loginShell: not set

testing pam_acct_mgmt

pam_acct_mgmt: Success

PAM Environment:
 - no env -
```

7.11.7. testparm

С помощью команды **`testparm`** можно проверить содержимое файла конфигурации **`/etc/samba/smb.conf`**.

Пример проверки настройки Samba:

```
$ testparm
Load smb config files from /etc/samba/smb.conf
Loaded services file OK.
Weak crypto is allowed

Server role: ROLE_ACTIVE_DIRECTORY_DC

Press enter to see a dump of your service definitions

# Global parameters
```

```
[global]
    dns forwarder = 8.8.8.8
    ldap server require strong auth = No
    passdb backend = samba_dsdb
    realm = TEST.ALT
    server role = active directory domain controller
    workgroup = TEST
    rpc_server:tcpip = no
    rpc_daemon:spoolssd = embedded
    rpc_server:spoolss = embedded
    rpc_server:winreg = embedded
    rpc_server:ntsvcs = embedded
    rpc_server:eventlog = embedded
    rpc_server:srvsvc = embedded
    rpc_server:svcctl = embedded
    rpc_server:default = external
    winbindd:use external pipes = true
    idmap_ldb:use rfc2307 = yes
    idmap config * : backend = tdb
    map archive = No
    vfs objects = dfs_samba4 acl_xattr

[dfs]
    msdfs root = Yes
    path = /media/dfsroot

[sysvol]
    path = /var/lib/samba/sysvol
    read only = No

[netlogon]
    path = /var/lib/samba/sysvol/test.alt/scripts
    read only = No

[free]
    guest ok = Yes
    path = /mnt/win/free
    read only = N
```

7.12. Конфигурационные файлы

7.12.1. smb.conf

`/etc/samba/smb.conf` — файл конфигурации Samba.

7.12.2. krb5.conf

`/etc/krb5.conf` — файл конфигурации Kerberos.

7.12.3. sssd.conf

`/etc/sssd/sssd.conf` — файл конфигурации SSSD.

Для работы с Active Directory в SSSD имеется специальный AD-провайдер *sssd-ad*.

Минимальный конфигурационный файл (**`/etc/sssd/sssd.conf`**) для sssd-ad:

```
[sssd]
config_file_version = 2
services = nss, pam

# Managed by system facility command:
## control sssd-drop-privileges unprivileged|privileged|default
user = _sssd

# SSSD will not start if you do not configure any domains.

domains = TEST.ALT
[nss]

[pam]
[domain/TEST.ALT]
id_provider = ad
auth_provider = ad
chpass_provider = ad
access_provider = ad
default_shell = /bin/bash
fallback_homedir = /home/%d/%u
debug_level = 0
;cache_credentials = true
ad_gpo_ignore_unreadable = true
ad_gpo_access_control = permissive
ad_update_samba_machine_account_password = true
```

Получить подробную информацию можно на справочной странице sssd.conf(5) (**`man sssd.conf`**).

7.12.4. resolv.conf

`/etc/resolv.conf` — файл конфигурации ресолвера (механизма преобразования имен хостов в адреса IP).

Файл конфигурации ресолвера (resolver) содержит информацию, которая считывается функциями разрешения имён при первом их вызове процессом. Файл разработан в удобочитаемом формате, и содержит список ключевых слов со значениями, которые предоставляют различного рода информацию для функций разрешения имён. Файл настройки считается надёжным источником информации DNS (например, информация об AD-бите DNSSEC будет возвращаться в неизменном виде из этого источника).

Если этот файл не существует, то будет опрашиваться только служба имён на локальной машине; доменное имя определяется из имени узла, а список поиска будет содержать это доменное имя.

Обычно в файле **`/etc/resolv.conf`** указан как минимум 1 сервер имен, на который будут перенаправляться все DNS запросы:

```
# Generated by resolvconf
# Do not edit manually, use
# /etc/net/ifaces/<interface>/resolv.conf instead.
nameserver 192.168.197.241
```

Важно

> Файл **/etc/resolv.conf** не должен редактироваться. Его автоматически генерирует **resolvconf**. Редактировать можно файл **/etc/net/ifaces/<interface>/resolv.conf**

Поддерживаются следующие параметры настройки:

nameserver IP-адрес сервера имён

Интернет-адрес сервера имён, на который надо переправлять все запросы, либо адрес IPv4 (в точечной нотации), либо адрес IPv6 в нотации с двоеточием (и, возможно, с точками) в соответствии с RFC 2373. Может быть указано до **MAXNS** (в настоящее время 3) серверов имён, ключевое слово должно быть указано для каждого сервера. Если указано несколько серверов, библиотека распознавателя запрашивает их в указанном порядке. Если в файле нет строк ***nameserver***, по умолчанию используется сервер имён на локальном компьютере. Используемый алгоритм заключается в том, чтобы попробовать обратиться к первому указанному серверу имён, и, если время ожидания запроса истекло, попробовать обратиться к следующему серверу, и т.д. пока не будет исчерпан список серверов, а затем повторять попытки, пока не будет сделано максимальное количество повторных попыток.

options

Позволяют изменять некоторые внутренние переменные функций определения имён. Синтаксис:

```
options параметр …
```

где **параметр** может иметь следующие значения:

attempts:n

Задаёт количество попыток, которое преобразователь предпримет, отправляя запрос на свои серверы имён, прежде чем закончить работу и вернуть ошибку. По умолчанию используется RES_DFLRETRY (в настоящее время равно 2). Значение этого параметра скрыто ограничено числом 5.

debug

Устанавливает RES_DEBUG в _res.options (эффективно, только если glibc был собран с поддержкой отладки; см. **resolver(3)**).

edns0 (начиная с *glibc 2.6*)

Задаёт значение RES_USE_EDNSO в _res.options. Включает поддержку расширений DNS, описанных в RFC 2671.

inet6

Задаёт значение RES_USE_INET6 в _res.options. Это приводит к выполнению запроса AAAA перед запросом A внутри функции **gethostbyname(3)**, и отображению ответов IPv4 в «туннелированной форме» IPv6, если записи AAAA не были найдены, но существует набор записей A. Начиная с *glibc 2.25*, эта опция устарела; приложения должны использовать **getaddrinfo(3)**, а не **gethostbyname(3)**.

ip6-bytestring (с *glibc 2.3.4* до *glibc 2.24*)

Задаёт значение RES_USE_BSTRING в _res.options. Это приводит к поиску обратной записи IPv6, с использованием формата значимых битов, описанного в RFC 2673; если этот параметр не установлен (по умолчанию), то используется формат полубайта. Эта опция была удалена в *glibc 2.25*, так как она полагалась на несовместимое с предыдущими версиями расширение DNS.

ip6-dotint/no-ip6-dotint (с *glibc 2.3.4* до *glibc 2.24*)

Устанавливает/сбрасывает значение RES_NOIP6DOTINT в _res.options. Если указан сброс (ip6-dotint), то выполняется поиск обратной записи IPv6 в зоне ip6.int; если задана установка (no-ip6-dotint), то по умолчанию выполняется поиск обратной записи IPv6 в зоне ip6.arpa. Эти параметры доступны в версиях *glibc* до 2.24, где по умолчанию используется no-ip6-dotint. Поскольку ip6-dotint перестала поддерживаться, эти опции были удалены в *glibc 2.25*.

ndots:n

Задаёт минимальное количество точек, которые должны обязательно присутствовать в имени, переданном функции res_query(3) (см. **`resolver(3)`**), прежде чем будет сделан первоначальный абсолютный запрос. По умолчанию **`n`** равно 1, поэтому если в имени есть точки, сначала имя пытаются разрешить как абсолютное, прежде чем добавлять к нему элементы из списка поиска. Значение этой опции скрыто ограничено числом 15.

no-check-names

Задаёт значение RES_NOCHECKNAME в _res.options, что приводит к отключению в современном BIND проверки в поступающих именах узлов и почтовых именах недопустимых символов, таких как символы подчёркивания (_), не-ASCII или управляющие символы.

no-reload (начиная с *glibc 2.16*)

Задаёт значение RES_NORELOAD в _res.options. Эта опция отключает автоматическую перезагрузку измененного файла конфигурации.

no-tld-query (начиная с *glibc 2.14*)

Задаёт значение RES_NOTLDQUERY в _res.options. Этот параметр указывает res_nsearch() не пытаться разрешить неполное имя, как если бы оно было доменом верхнего уровня. Данный параметр может привести к проблемам, если в качестве TLD указано «localhost», а не localhost в одном или более элементах списка поиска. Данный параметр не действует, если не установлен RES_DEFNAMES или RES_DNSRCH.

rotate

Задаёт значение RES_ROTATE в _res.options, что приводит к циклическому выбору указанных серверов имён. Без этой опции распознаватель всегда будет запрашивать первый сервер имён в списке и использовать последующий сервер имён только в случае сбоя первого. Эта опция позволяет распределить нагрузку между разными серверами имён.

single-request-reopen (начиная с *glibc 2.9*)

Задаёт RES_SNGLKUPREOP в _res.options. Для разрешения имён используется единый сокет для запросов A и AAAA. Некоторое оборудование ошибочно возвращает только один ответ. Когда это происходит, клиент продолжает ждать второго ответа.

Указание этого параметра изменяет это поведение так, что если два запроса с одного порта не обрабатываются правильно, то сокет будет закрыт и открыт новый перед посылкой второго запроса.

single-request (начиная с *glibc 2.10*)

Задаёт значение RES_SNGLKUP в _res.options. По умолчанию, *glibc* начиная с версии 2.9 выполняет поиск по IPv4 и IPv6 параллельно.

Некоторые приложения DNS-серверов не могут обработать такие запросы должным образом и делают паузу между ответами на запрос. Этот параметр отключает данное поведение, что заставляет *glibc* делать запросы IPv6 и IPv4 последовательно (за счет некоторого замедления процесса разрешения имени).

timeout:n

Задаёт промежуток времени, который функции определения имён будут ждать ответа от удалённого сервера имён перед тем как повторить запрос другому серверу имён. Это время может не совпадать с общим временем, затраченным на любой вызов API-интерфейса преобразователя, и нет гарантии, что один вызов API-интерфейса преобразователя соответствует одному тайм-ауту. Измеряется в секундах, значение по умолчанию — RES_TIMEOUT (в настоящее время равно 5). Значение этой опции скрыто ограничено числом 30.

trust-ad (начиная с *glibc 2.31*)

Задаёт значение RES_TRUSTAD в _res.options. Этот параметр управляет поведением бита AD распознавателя-заглушки. Если проверяющий преобразователь устанавливает в ответе бит AD, это означает, что данные в ответе были проверены в соответствии с протоколом DNSSEC. Чтобы полагаться на бит AD, локальная система должна доверять как распознавателю, проверяющему DNSSEC, так и сетевому пути к нему, поэтому требуется явное согласие. Если активна опция ***trust-ad***, тупиковый распознаватель устанавливает бит AD в исходящих DNS-запросах (чтобы включить поддержку бита AD) и сохраняет бит AD в ответах. Без этой опции бит AD в запросах не устанавливается и всегда удаляется из ответов, прежде чем они будут возвращены приложению. Это означает, что приложения могут доверять биту AD в ответах, если параметр ***trust-ad*** установлен правильно.

В *glibc* версии 2.30 и более ранних AD не устанавливается автоматически в запросах и без изменений передается приложениям в ответах.

use-vc (начиная с *glibc 2.14*)

Задаёт значение RES_USEVC в _res.options. Данный параметр включает принудительное использование TCP для запросов DNS.

search список поиска

По умолчанию список поиска содержит одну запись — имя локального домена. Он определяется по локальному имени хоста, возвращаемому функцией **`gethostname(2)`**; локальным доменным именем считается всё, что следует после первого знака «.». Если имя хоста не содержит «.», предполагается, что корневой домен является именем локального домена.

Это поведение можно изменить, перечислив имена доменов, в которых нужно вести поиск, после ключевого слова ***`search`*** через пробел или символ табуляции. При разрешении запросов имён, в которых меньше точек чем указано в **`ndots`** (по умолчанию 1), будет использован каждый компонент пути поиска пока не будет найдено соответствующее имя. Для сред с несколькими субдоменами см. параметры **`ndots:n`**, чтобы избежать атак типа «человек посередине» и ненужного трафика для корневых DNS-серверов. Обратите внимание, что этот процесс может быть медленным и будет генерировать много сетевого трафика, если серверы для перечисленных доменов не являются локальными, и что время ожидания запросов истечет, если сервер для одного из доменов недоступен.

При наличии нескольких директив ***`search`*** используется только список поиска из последнего экземпляра.

Список поиска может содержать не более шести доменов и не может быть длиннее 256 символов. В *glibc 2.25*и более ранних версиях список поиска мог содержать не более шести доменов и не мог быть длиннее 256 символов. Начиная с *glibc 2.26* список поиска не ограничен.

Директива ***`domain`*** — это устаревшее название директивы ***`search`***, которая обрабатывает только одну запись в списке поиска.

sortlist

Позволяет сортировать адреса, возвращаемых функцией **`gethostbyname(3)`**. Список сортировки задается в виде пар IP-адрес/сетевая маска. Маску сети указывать не обязательно, по умолчанию используется естественная маска сети. IP-адрес и маска сети разделяются косой чертой. В списке можно указывать до 10 пар. Пример:

```
sortlist 130.155.160.0/255.255.240.0 130.155.0.0
```

Ключевое слово ***`search`*** системного файла **`resolv.conf`** можно переопределить для каждого процесса, задав для переменной среды LOCALDOMAIN список доменов поиска, разделенных пробелами.

Ключевое слово ***`options`*** системного файла **`resolv.conf`** можно переопределить для каждого процесса, задав для переменной среды RES_OPTIONS список параметров преобразователя, разделенных пробелами.

Любые изменения, внесенные вручную в файл конфигурации **`/etc/resolv.conf`**, обязательно будут перезаписаны при изменениях в сети или перезагрузке системы.

Ключевое слово и значение должны находиться в одной строке, и кроме того, строка должна начинаться с ключевого слова (например, ***`nameserver`***). Значение следует за ключевым словом, разделенным пробелом.

Строки, начинающиеся с точки с запятой (;) или решетки (#), считаются комментариями.

Resolvconf – это платформа для обновления системной информации о серверах DNS. Он настраивается как посредник между программами, которые предоставляют эту информацию и программами, которые используют эту информацию.

Обновить файл **/etc/resolv.conf**, чтобы внести изменения в DNS:

```
# resolvconf -u
```

Пример файла **/etc/resolv.conf**:

```
search test.alt example.test
nameserver 192.168.0.122
nameserver 8.8.8.8
```

Запись search позволяет использовать в качестве адреса только хост-имя для компьютеров в домене test.alt. Например, чтобы обратиться системе work.test.alt, пользователь должен ввести в качестве адреса только хост-имя, work. Когда преобразователь пытается разрешить доменное имя, например work, он сначала формирует полное доменное имя, используя имя домена test.alt, в work.test.alt и выполняет DNS-запрос, используя это полное доменное имя. Если это не удается, то преобразователь пробует следующий в очереди домен и запрашивает IP-адрес work.example.test.

При этом, когда преобразователь пытается разрешить доменное имя work.ru, он сначала запросит work.ru как абсолютное доменное имя. Если DNS не сможет разрешить его, то только тогда преобразователь объединит его с поисковым доменом, чтобы сформировать work.ru.test.alt, и повторит запрос.

Решение о том, выполняется ли первый запрос как абсолютное доменное имя или нет, полностью зависит от количества точек, присутствующих в доменном имени. По умолчанию доменное имя, содержащее по крайней мере 1 точку, заставит преобразователь запрашивать его дословно, не объединяя его с какими-либо поисковыми доменами. Количество точек для первого запроса абсолютного доменного имени настраивается в значении параметра ***ndots*** (см. описание параметров выше).

Глава 8. Примечания

8.1. Настройка беспарольного доступа по ssh

Генерация SSH-ключа (на DC1):

```
# ssh-keygen -t ed25519
```

На вопрос о файле для сохранения ключа нажать **Enter** (по умолчанию). На вопрос о пароле к ключу также нажать **Enter** (не указывать пароль)

Скопировать публичную часть SSH-ключа на второй контроллер домена (DC2) для пользователя user:

```
# ssh-copy-id -i ~/.ssh/id_ed25519.pub user@dc2.test.alt
```

Скопировать публичную часть SSH-ключа на второй контроллер домена (DC2) для администратора. Для этого подключаемся к DC2 и под root копируем публичную часть ключа:

```
# ssh user@dc2.test.alt
[user@dc2 ~]$ su -
Password:
[root@dc2 ~]# cat /home/user/.ssh/authorized_keys >>.ssh/authorized_keys
[root@dc2 ~]# exit
выход
[user@dc2 ~]$ exit
выход
Connection to dc2 closed.
```

Теперь есть возможность удалённо выполнять команды на DC2 с привилегиями администратора.

8.2. Центр управления системой

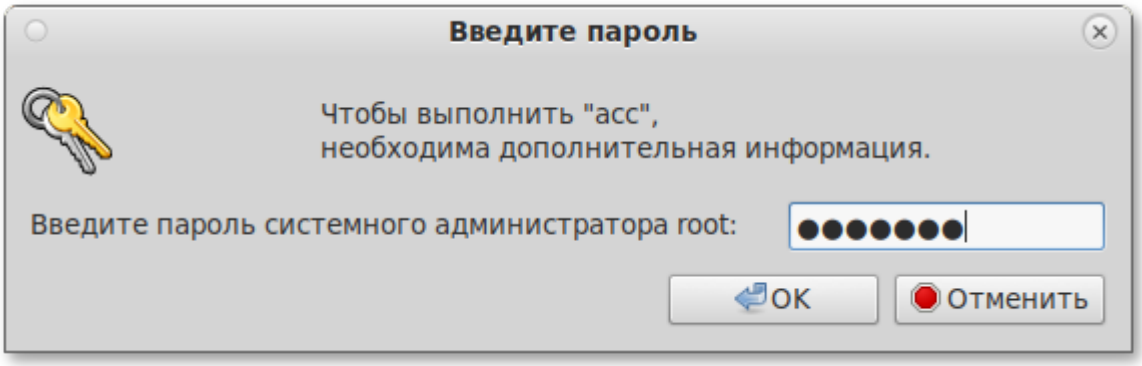
Центр управления системой (ЦУС, альтератор) представляет собой удобный интерфейс для выполнения наиболее востребованных административных задач: добавление и удаление пользователей, настройка сетевых подключений, просмотр информации о состоянии системы и т.п.

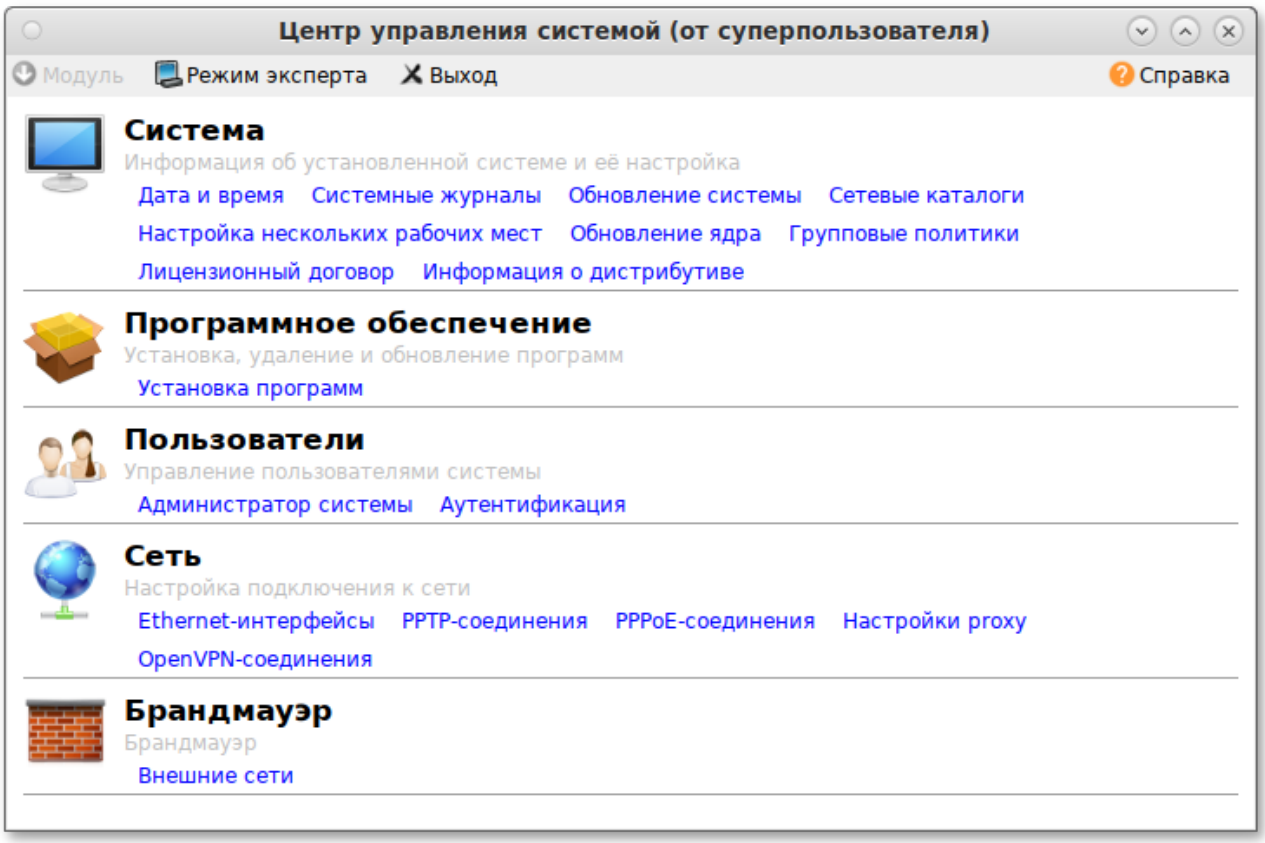
ЦУС состоит из независимых диалогов-модулей. Каждый модуль отвечает за настройку определённой функции или свойства системы.

Запустить ЦУС в графической среде можно следующими способами:

- в графической среде MATE: **Система** → **Администрирование** → **Центр управления системой**;
- в графической среде XFCE, KDE: **Меню запуска приложений** → **Настройки** → **Центр управления системой**;
- из командной строки: командой **`acc`**.

Запуск ЦУС требует административных прав, и если запустить его от обычного пользователя, он запросит пароль администратора системы (root):





ЦУС имеет также веб-ориентированный интерфейс, позволяющий управлять сервером с любого компьютера сети.

Для запуска веб-ориентированного интерфейса, должен быть установлен пакет *alterator-fbi*:

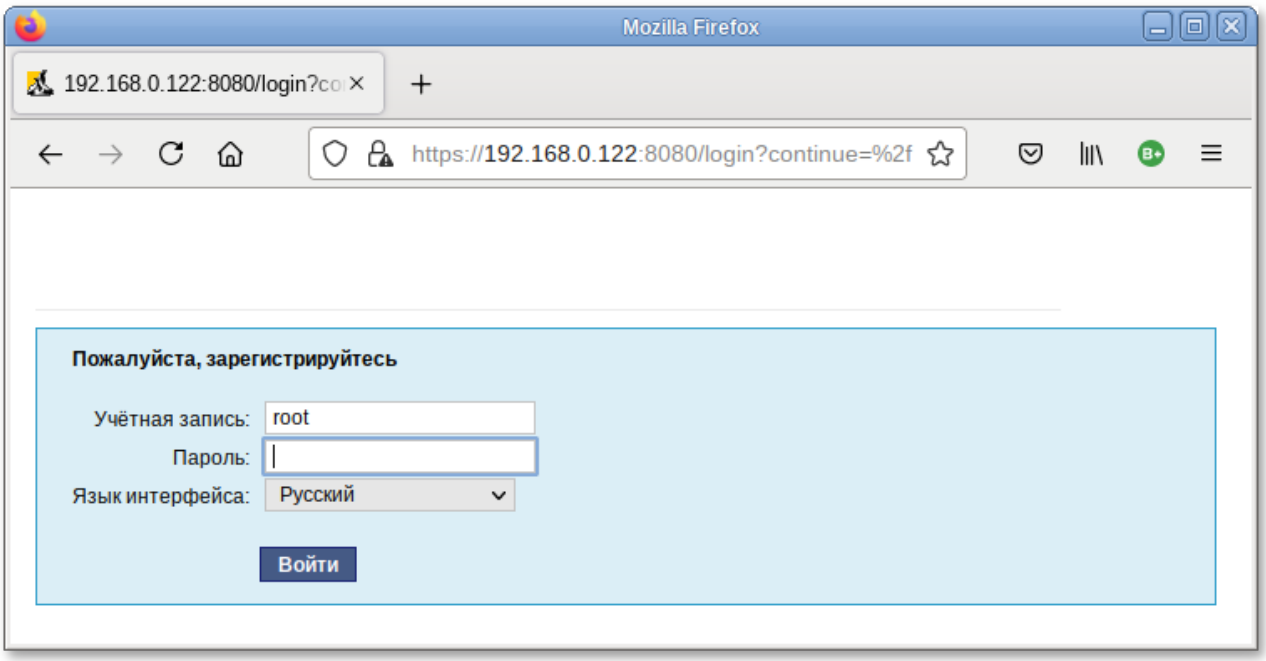
```
# apt-get install alterator-fbi
```

И запущены сервисы **`ahttpd`** и **`alteratord`**:

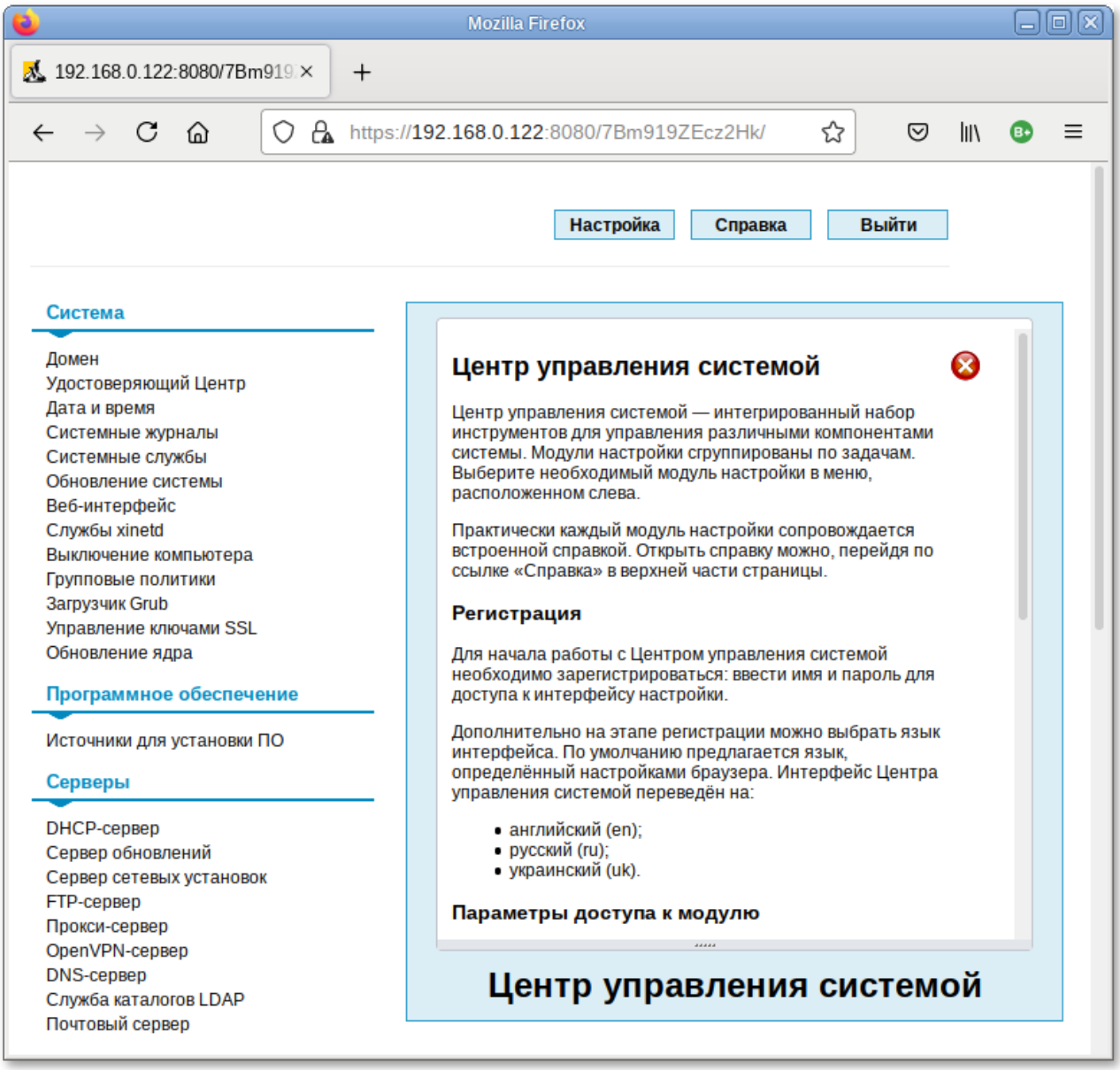
```
# systemctl enable --now ahttpd
# systemctl enable --now alteratord
```

Работа с ЦУС может происходить из любого веб-браузера. Для начала работы необходимо перейти по адресу **`https://ip-адрес:8080/`**.

При запуске центра управления системой необходимо ввести в соответствующие поля имя пользователя (**root**) и пароль пользователя:



После этого будут доступны все возможности ЦУС на той машине, к которой было произведено подключение через веб-интерфейс.



Установленные пакеты, которые относятся к ЦУС, можно посмотреть, выполнив команду:

```
rpm -qa | grep alterator*
```

Прочие пакеты для ЦУС можно найти, выполнив команду:

```
apt-cache search alterator*
```

Модули можно дополнительно загружать и удалять как обычные программы:

```
# apt-get install alterator-net-openvpn
# apt-get remove alterator-net-openvpn
```