ALD Pro

ИНСТРУКЦИИ

ДОВЕРИТЕЛЬНЫЕ ОТНОШЕНИЯ

Версия 3.0.0

Содержание

Модуль доверия между доменами ALD Pro

1.1. Особенности установки при использовании Astra Linux версии 1.7.6 и выше

При использовании **Astra Linux** версией 1.7.6 и выше установка дополнительных пакетов не требуется, так как реализация доверительных отношений **ALD Pro** встроена в пакеты системы.

Чтобы настроить модуль **Доверие между доменами ALD Pro**, необходимо:

1. На контроллере домена нужно установить пакет `libipa-aldpro` командами:

```
sudo apt update
sudo apt install libipa-aldpro
```

2. В файл `/usr/share/aldpro/updates/92-aldpro-extdom-extop-plugin.update` нужно добавить следующие строки для расширения схемы каталога:

```
dn: cn=ipa_extdom_extop,cn=plugins,cn=config
only:changetype: add
only:objectclass: top
only:objectclass: nsSlapdPlugin
only:objectclass: extensibleObject
only:cn: ipa_extdom_extop
only:nsslapd-pluginpath: libaldpro_extdom_extop
only:nsslapd-plugininitfunc: ipa_extdom_init
only:nsslapd-plugintype: extendedop
only:nsslapd-pluginenabled: on
only:nsslapd-pluginid: ipa_extdom_extop
only:nsslapd-pluginversion: 1.0
only:nsslapd-pluginvendor: AstraLinux
only:nsslapd-plugindescription: Support resolving IDs in trusted domains to
↪names and back
only:nsslapd-plugin-depends-on-type: database
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
only:nsslapd-basedn: $SUFFIX
```

3. Выполнить обновление схемы каталога и перезапустить службы следующими командами:

```
sudo ipa-ldap-updater /usr/share/aldpro/updates/92-aldpro-extdom-extop-plugin.
↪update
sudo net conf setparm global "passdb backend" "aldprosam:ldapi://%2fvar%2frun
↪%2fslapd-$(hostname -d | sed 's/\./-/g; s/.*/\U&/').socket"
sudo aldproctl restart
```

Полный перечень обновляемых пакетов:

- libipa-hbac-dev
- libipa-hbac0
- libnss-sss
- libpam-sss
- libsss-certmap-dev
- libsss-certmap0
- libsss-idmap-dev
- libsss-idmap0
- libsss-nss-idmap-dev
- libsss-nss-idmap0
- libsss-simpleifp-dev
- libsss-simpleifp0
- libsss-sudo
- libwbclient-sssd
- libwbclient-sssd-dev
- python3-libipa-hbac
- python3-libsss-nss-idmap
- python3-sss
- sssd
- sssd-ad

- sssd-ad-common
- sssd-common
- sssd-dbus
- sssd-ipa
- sssd-kcm
- sssd-krb5
- sssd-krb5-common
- sssd-ldap
- sssd-proxy
- sssd-tools

1.2. Установка при использовании Astra Linux версии ниже 1.7.6

Если планируется устанавливать доверительные отношения между доменами ALD Pro, необходимо установить модуль доверия между доменами ALD Pro.

Для установки доверительных отношений между доменами ALD Pro предъявляются следующие технические требования:

1. Установку пакетов и выполнение инструкций по настройке модуля доверия необходимо выполнять на обоих контроллерах домена, между которыми настраивается доверие.

2. Установку необходимо выполнять от имени учетной записи администратора системы с высоким уровнем целостности.

3. На обоих контроллерах домена должно быть установлено обновление ALD Pro 2.5.0.

Внимание: При установке модуля доверия между доменами ALD Pro для компонентов SSSD будет выполнено понижение версий (даунгрейд) до 2.5.0-1astra.se8-aldpro1 из состава срочного оперативного обновления операционной системы Astra Linux Special Edition 1.7.3.UU.2.

Порядок установки модуля на контроллерах домена ALD Pro:

1. Подключить репозиторий, содержащий необходимые для функционирования модуля обновления:

   - Примонтировать iso-образ *ALDPro-2.5.0-trust.iso*, выполнив команду:

```
sudo mkdir /mnt/aldpro_2.5.0_trust
sudo mount -o loop /distr/ALDPro-2.5.0-trust.iso /mnt/aldpro_2.5.0_trust

Где:

   - ``mount`` -- утилита обеспечивает монтирование файловой системы;

   - ``-o loop`` -- ключ позволяет связать свободное петлевое устройство (/
 ↪dev/loopN) с указанным iso-образом;

   - ``/distr/ALDPro-2.5.0-trust.iso`` -- параметр определяет абсолютный
 ↪путь к iso-образу;

   - ``/mnt/aldpro_2.5.0_trust`` -- параметр определяет точку монтирования.

* Создать файл ``/etc/apt/sources.list.d/trust.list`` со следующим
 ↪содержимым:

.. code-block:: console

   deb file:///media/cdrom 2.5.0 aldpro
```

1. Добавить в файл */etc/apt/preferences.d/aldpro* следующее содержимое:

```
Package: *
Pin: release n=2.5.0
Pin-Priority: 1000
```

3. Выполнить команды:

```
sudo apt update
sudo apt dist-upgrade
sudo apt install libipa-aldpro
```

4. Добавить в файл */usr/share/aldpro/updates/92-aldpro-extdom-extop-plugin.update*:

```
dn: cn=ipa_extdom_extop,cn=plugins,cn=config
only:changetype: add
only:objectclass: top
only:objectclass: nsSlapdPlugin
only:objectclass: extensibleObject
only:cn: ipa_extdom_extop
only:nsslapd-pluginpath: libaldpro_extdom_extop
only:nsslapd-plugininitfunc: ipa_extdom_init
only:nsslapd-plugintype: extendedop
only:nsslapd-pluginenabled: on
only:nsslapd-pluginid: ipa_extdom_extop
only:nsslapd-pluginversion: 1.0
only:nsslapd-pluginvendor: AstraLinux
only:nsslapd-plugindescription: Support resolving IDs in trusted domains to
 ↪names and back
only:nsslapd-plugin-depends-on-type: database
only:nsslapd-basedn: $SUFFIX
```

5. **Последовательно** выполнить команды, каждую **после завершения** предыдущей:

```
sudo ipa-ldap-updater /usr/share/aldpro/updates/92-aldpro-extdom-extop-plugin.
 ↪update

sudo net conf setparm global "passdb backend" "aldprosam:ldapi://%2fvar%2frun
 ↪%2fslapd-$(hostname -d | sed 's/\./-/g; s/.*/\U&/').socket"

sudo ipactl restart
```

Для автоматизации процесса установки модуля «Доверие между доменами ALD Pro» на **клиентах** домена ALD Pro рекомендуется создать репозиторий из ISO-образа *ALDPro-2.5.0-trust.iso* и с помощью задания автоматизации произвести установку модуля.

Описание процесса создания репозитория из ISO-образа приведено в repo_from_ISO. Описание порядка создания и запуска заданий автоматизации приведено в Справочном центре ALD Pro.

Порядок установки модуля на **Клиентах** ALD Pro:

Внимание: Следующие действия актуальны при использовании ОС Astra Linux версией ниже 1.7.6. Если на клиентах установлена ОС Astra Linux версии 1.7.6, см. os_1_7_6.

1. Подключить репозиторий, содержащий необходимые для функционирования модуля обновления:

   - Примонтировать ISO-образ *ALDPro-2.5.0-trust.iso*, выполнив команду:

```
sudo mkdir /mnt/ald_pro_2.5.0_trust
sudo mount -o loop /distr/ALDPro-2.5.0-trust.iso /mnt/ald_pro_2.5.0_trust
```

   Где:

   - `mount` – утилита обеспечивает монтирование файловой системы;
   - `-o loop` – ключ позволяет связать свободное петлевое устройство (/dev/loopN) с указанным iso-образом;
   - `/distr/ALDPro-2.5.0-trust.iso` – параметр определяет абсолютный путь к iso-образу;
   - `/mnt/ald_pro_2.5.0_trust` – параметр определяет точку монтирования.
   - Создать файл `/etc/apt/sources.list.d/aldpro_trust.list` со следующим содержимым:

```
deb file:///mnt/ald_pro_2.5.0_trust 2.5.0 aldpro
```

2. Добавить в файл `/etc/apt/preferences.d/aldpro` следующее содержимое для настройки приоритетов:

```
Package: *
Pin: release n=2.5.0
Pin-Priority: 1000
```

3. Выполнить команды:

```
sudo apt update
sudo apt dist-upgrade
```

Инструкция по установке доверительных отношений между Microsoft Active Directory и ALD Pro

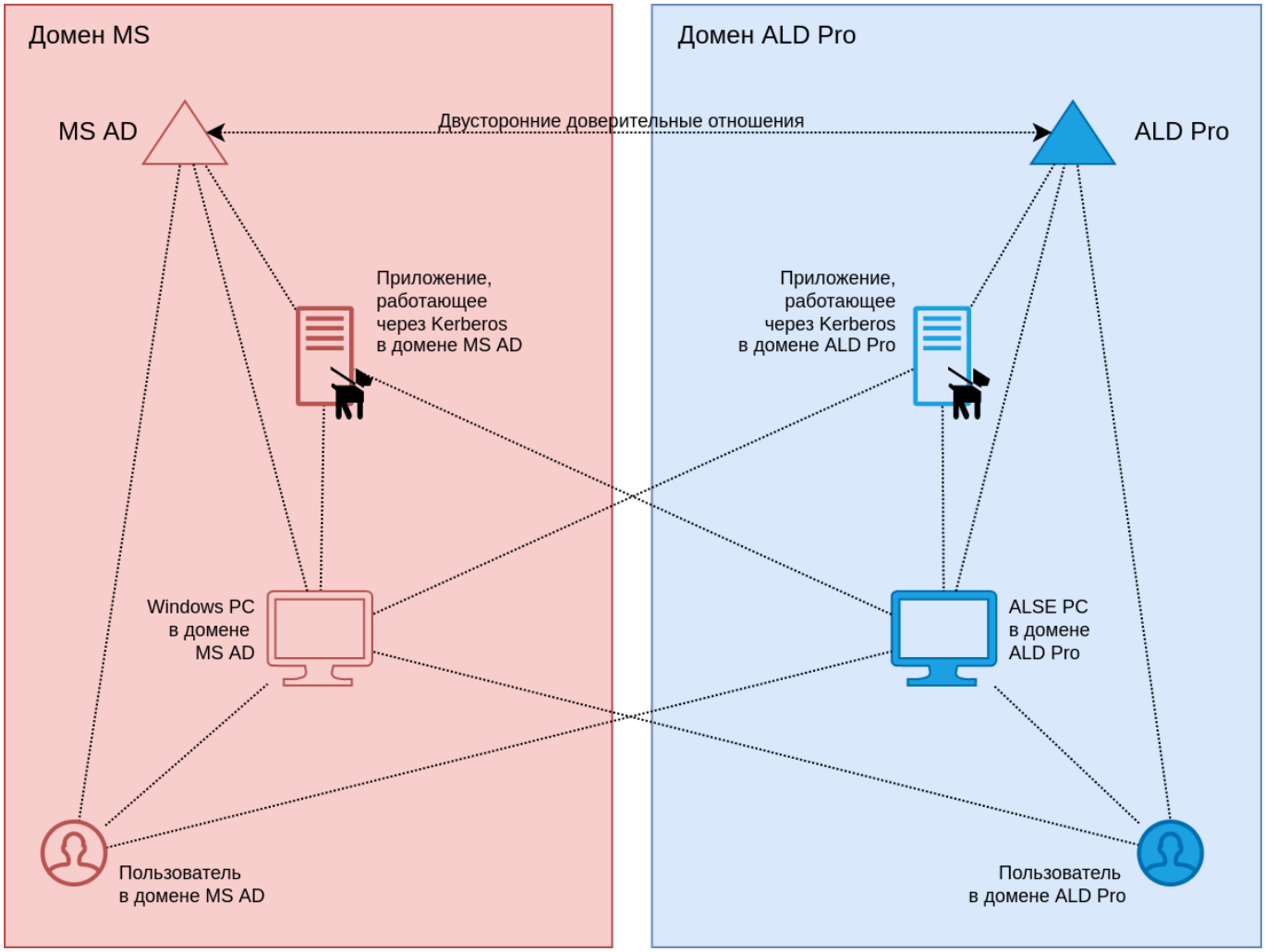
В настоящей инструкции представлены рекомендации по настройке доверительных отношений между доменами ALD Pro и Microsoft Active Directory (далее по тексту MS AD), которые позволяют пользователям одного домена проходить прозрачную аутентификацию на контроллерах другого домена. Эти возможности актуальны в переходный период, когда часть пользователей и сервисов работают уже в новом домене, а часть остаются в старом.

Подготовленная VM windc01 –для домена windomain.lan (Win2019)

Подготовленная VM alddc01 –для домена alddomain.lan (ALD Pro 2.1.0)

2.1. Постановка задачи

Ранее организация работала в домене MS AD (**windomain.lan**) и в рамках миграции был развернут домен ALD Pro (**alddomain.lan**). В соответствии с составленным планом предполагается постепенный перевод сервисов и пользователей на работу в новом домене, поэтому необходимо в течение некоторого времени обеспечить гибридную работу пользователей сразу в двух доменах с помощью механизма доверительных отношений.



Данные отношения называются «доверительными» (Domain Trust), т. к. контроллеры доверяющего домена напрямую не аутентифицируют пользователей доверенного домена, а только принимают доказательство об успешной аутентификации этих пользователей от контроллеров из доверенного домена. Невозможность выполнить аутентификацию напрямую объясняется тем, что у доверяющего домена просто нет учетных данных пользователей из доверенного домена.

Порядок работы аутентификации с использованием доверительных отношений (Domain Trust):

1. Пользователю доверенного домена ALD Pro нужно пройти аутентификацию в службе из доверяющего домена MS AD.

2. Пользователь ALD Pro успешно проходит аутентификацию на контроллере ALD Pro и получает от него TGT билет.

3. Пользователь ALD Pro обращается к своему контроллеру за сервисным билетом к службе из доверяющего домена MS AD. Контроллер ALD Pro видит, что служба

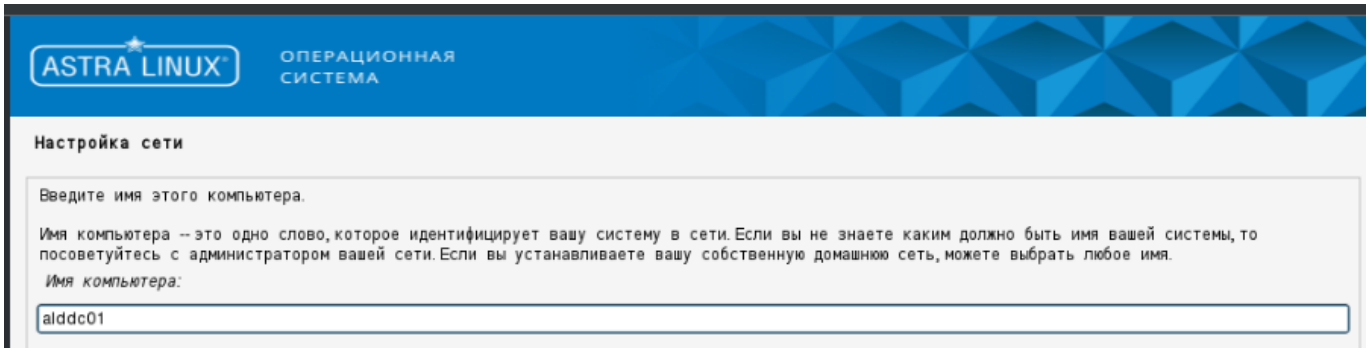
находится в доверяющем домене MS AD, поэтому выписывает билет на выполнение рекурсивного Kerberos запроса к контроллеру из доверяющего домена MS AD. Билет зашифрован паролем служебной учетной записи, соответствующей доверительному отношению. Таким образом, пользователь получает своего рода сервисный билет на доступ к службе распространения ключей доверяющего домена (Key Distribution Center, KDC).

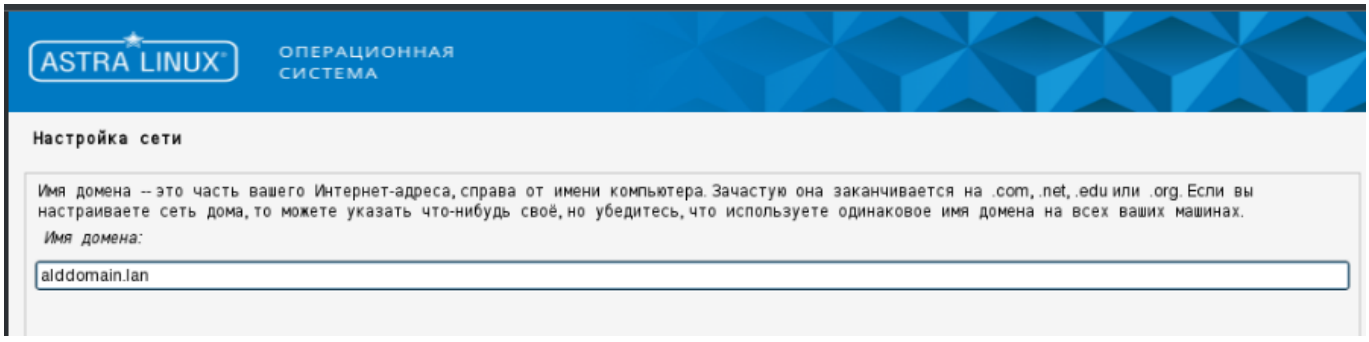
4. Пользователь ALD Pro обращается с полученным билетом к контроллеру доверяющего MS AD, совершая рекурсивный Керберос запрос. Контроллер MS AD расшифровывает билет, используя пароль учетной записи, соответствующей доверительному отношению, и, доверяя контроллеру ALD Pro, что тот выполнил проверку аутентичности пользователя должным образом, выписывает пользователю сервисный билет на доступ к своей службе.

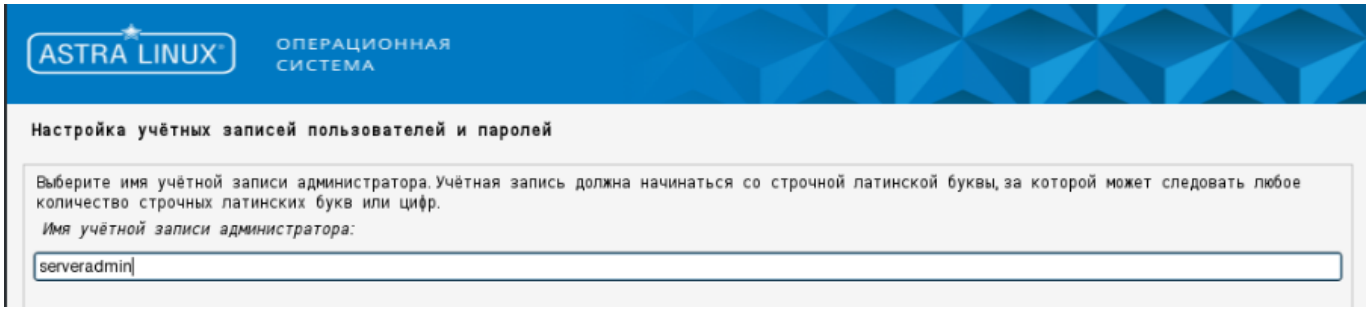
5. Клиент идет к службе из домена MS AD, используя сервисный билет, полученный от контроллера из этого же домена.

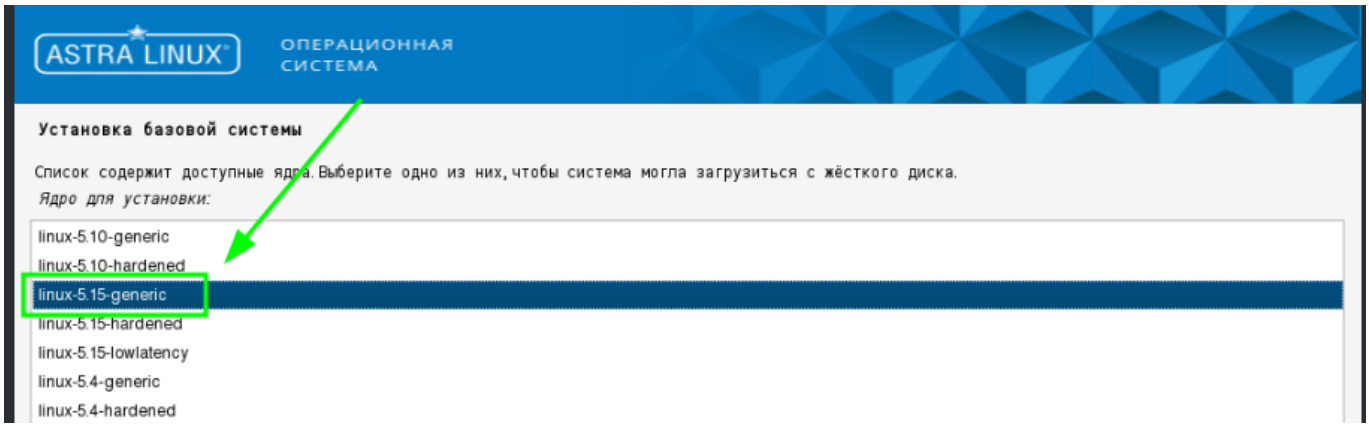
2.2. Подготовка контроллера домена ALD Pro

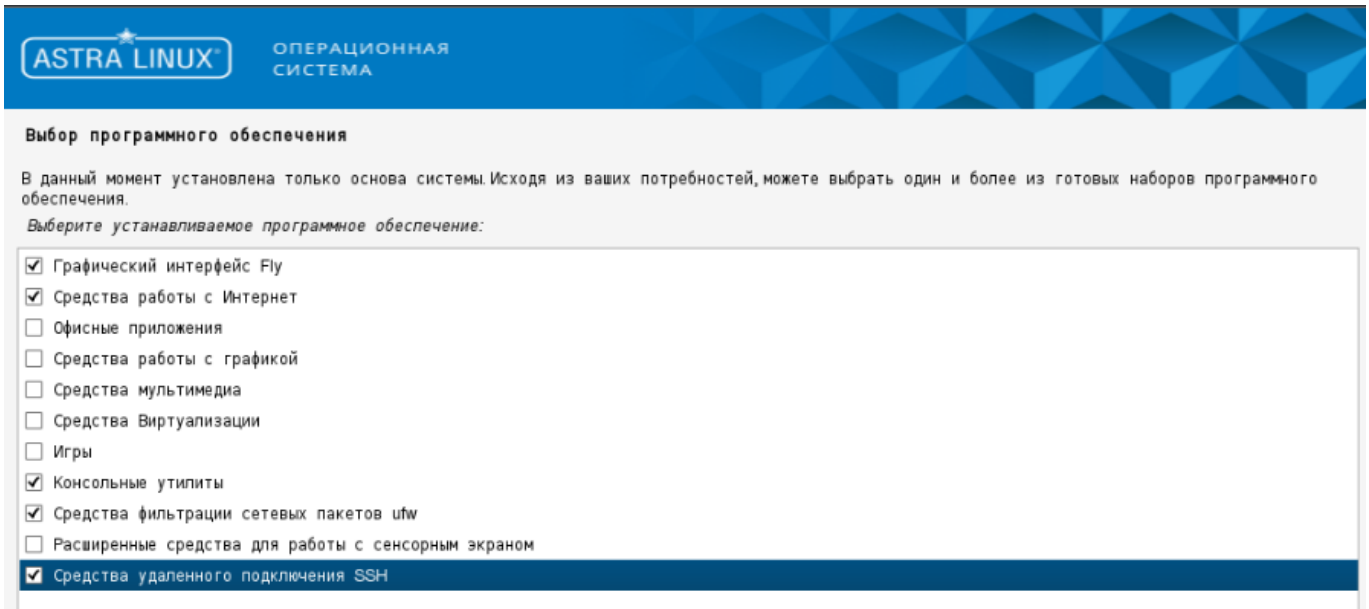
Для взаимодействия между компьютерами будет использована сеть 192.168.88.0/24.

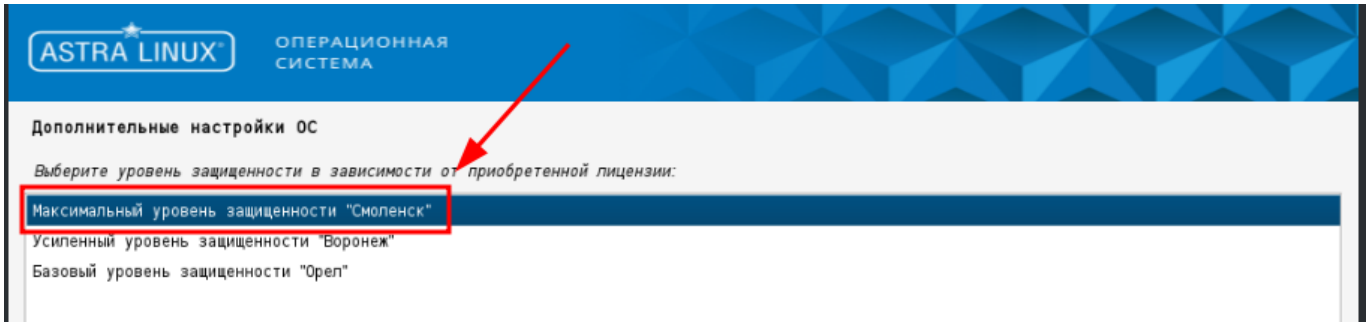





ASTRA LINUX
ОПЕРАЦИОННАЯ СИСТЕМА
Настройка учётных записей пользователей и паролей
Выберите имя учётной записи администратора. Учётная запись должна начинаться со строчной латинской буквы, за которой может следовать любое количество строчных латинских букв или цифр.
Имя учётной записи администратора:
serveradmin


ASTRA LINUX
ОПЕРАЦИОННАЯ СИСТЕМА
Установка базовой системы
Список содержит доступные ядра. Выберите одно из них, чтобы система могла загрузиться с жёсткого диска.
Ядро для установки:
linux-5.10-generic
linux-5.10-hardened
linux-5.15-generic
linux-5.15-hardened
linux-5.15-lowlatency
linux-5.4-generic
linux-5.4-hardened


ASTRA LINUX
ОПЕРАЦИОННАЯ СИСТЕМА
Выбор программного обеспечения
В данный момент установлена только основа системы. Исходя из ваших потребностей, можете выбрать один и более из готовых наборов программного обеспечения.
Выберите устанавливаемое программное обеспечение:
Графический интерфейс Fly
Средства работы с Интернет
Офисные приложения
Средства работы с графикой
Средства мультимедиа
Средства Виртуализации
Игры
Консольные утилиты
Средства фильтрации сетевых пакетов ufw
Расширенные средства для работы с сенсорным экраном
Средства удаленного подключения SSH


ASTRA LINUX
ОПЕРАЦИОННАЯ СИСТЕМА
Дополнительные настройки ОС
Выберите уровень защищенности в зависимости от приобретенной лицензии:
Максимальный уровень защищенности "Смоленск"
Усиленный уровень защищенности "Воронеж"
Базовый уровень защищенности "Орел"

Для первоначальной настройки сети необходимо выполнить **поочередно** нижеперечисленные команды под пользователем root (sudo -i).

```
#Смена имени
hostnamectl set-hostname alddc01

#Закомментировать все строки в основном файле sources.list
sed -i '/^deb.*/s/^/#/' /etc/apt/sources.list

#Создание отдельного frozen.list
cat <<EOF > /etc/apt/sources.list.d/frozen.list
deb https://dl.astralinux.ru/astra/frozen/1.7_x86-64/1.7.4/repository-base/ 1.
↪7_x86-64 main contrib non-free
deb https://dl.astralinux.ru/astra/frozen/1.7_x86-64/1.7.4/repository-
↪extended/ 1.7_x86-64 main contrib non-free
EOF

#Создание отдельного aldpro.list
cat <<EOF > /etc/apt/sources.list.d/aldpro.list
deb https://dl.astralinux.ru/aldpro/stable/repository-main/ 2.1.0 main
deb https://dl.astralinux.ru/aldpro/stable/repository-extended/ generic main
EOF

#Настройка приоритетов пакета aldpro
cat <<EOF > /etc/apt/preferences.d/aldpro
Package: *
Pin: release n=generic
Pin-Priority: 900
EOF

#Остановка NetworkManager сервиса, в дальнейшем будет использоваться
↪Networking + resolvconf
systemctl stop NetworkManager.service && systemctl disable NetworkManager.
↪service

#Обновление файла /etc/hosts, указание ip адреса и FQDN,hostname
cat <<EOF > /etc/hosts
127.0.0.1 localhost
192.168.88.80 alddc01.alddomain.lan alddc01
# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
EOF

#Обновление файла /etc/network/interfaces установка статичного адреса,маски,
 ↪шлюза,dns сервера и поискового домена
cat <<EOF > /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).
source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
        address 192.168.88.80
        netmask 255.255.255.0
        gateway 192.168.88.1
        dns-nameservers 77.88.8.8
        dns-search alddomain.lan
EOF

#Установка пакета resolvconf
apt update && apt install resolvconf
#Перезагрузка сервера, после перезагрузки сервер будет доступен по
 ↪указанному статичному IP адресу
reboot now
```

Теперь система готова к установке ALD Pro. Для этого необходимо выполнить **поочередно** команды под пользователем root (sudo -i)

```
#Установка обновлений
apt update && astra-update -A -r -T

#Установка пакетов ALD Pro
DEBIAN_FRONTEND=noninteractive apt-get install -y -q aldpro-mp aldpro-gc
 ↪aldpro-syncer
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
#Обновление файла для продвижения /etc/network/interfaces установка
 ↪статичного адреса,маски,шлюза,dns сервера и поискового домена
cat <<EOF > /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).
source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
        address 192.168.88.80
        netmask 255.255.255.0
        gateway 192.168.88.1
        dns-nameservers 192.168.88.80
        dns-search alddomain.lan
EOF

#Перезагрузка networking.service для обновления измененного dns-nameservers
systemctl restart networking.service

#Перезагрузка сервера
reboot now

#Отключение dnssec-validation в файле /etc/bind/named.conf.options
sed -i "s/dnssec-validation.*\$/dnssec-validation no;/g" /etc/bind/named.conf.
 ↪options

#Перезапуск службы bind9.service
systemctl restart bind9.service

#Продвижение контроллера домена
set +o history
/opt/rbta/aldpro/mp/bin/aldpro-server-install.sh --setup_gc --setup_syncer -
 ↪d 'alddomain.lan' -n 'alddc01' -p 'Astra123'  --no-reboot >/var/log/
 ↪promotion_aldpro_domain-controler.log
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
set -o history
#Отключение dnssec-validation в файле /etc/bind/ipa-options-ext.conf
sed -i "s/dnssec-validation.*\$/dnssec-validation no;/g" /etc/bind/ipa-
↪options-ext.conf

#Перезагрузка контроллера домена
reboot now
```

2.3. Подготовка контроллера домена MS

Продвижением называют процедуру, в ходе которой выполняется настройка служб сервера для его использования в качестве контроллера домена. Для корректной работы контроллера требуется соблюдение следующих условий:

- Статичный IP адрес
- Разрешение имен через собственный DNS-сервер
- Имя хоста в соответствии с именем сервера в домене

Необходимо выполнить следующие команды в **powershell** на контроллере домена

```
#Переименовать контроллер домена
Rename-Computer -NewName windc01
Restart-Computer

#Установить IP адрес,маску подсети и основной шлюз (настройки tcp/ipv4)
New-NetIPAddress -IPAddress 192.168.88.85 -PrefixLength 24 -DefaultGateway
↪192.168.88.1 -InterfaceIndex (Get-NetAdapter).InterfaceIndex

#Установить DNS сервер  (настройки tcp/ipv4)
Set-DnsClientServerAddress -InterfaceIndex (Get-NetAdapter).InterfaceIndex -
↪ServerAddresses "192.168.88.85"

#Установка необходимых компонентов
Install-WindowsFeature -name AD-Domain-Services -IncludeManagementTools

#Установка первого контроллера домена Active Directory в новом лесу
Install-ADDSForest -DomainName windomain.lan -DomainNetBIOSName WINDOMAIN -
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
 ↪InstallDNS

#Установка forwarder на a DNS сервер
Set-DnsServerForwarder -IPAddress "77.88.8.8" -PassThru
```

2.4. Контрольный список межлесного доверия

1. Проверка доступности портов
2. Взаимное перенаправление DNS-зон
3. Настройка времени

2.5. Контроллеры доверия и агенты доверия (Trust controllers and trust agents)

2.5.1. Контроллеры доверия

Это ALD Pro контроллеры, которые могут выполнять поиск идентификационных данных на контроллерах домена AD. Они также запускают Samba suite, чтобы установить доверительные отношения с MS AD. Контроллеры домена MS AD связываются с контроллерами доверия при установлении и проверке доверия к MS AD. Компьютеры, зарегистрированные в MS AD, взаимодействуют с контроллерами доверия ALD Pro для запросов аутентификации Kerberos.

Первый контроллер доверия создается при настройке доверия. Если есть несколько контроллеров домена в разных географических местоположениях, необходимо использовать команду `ipa-adtrust-install` , чтобы назначить серверы ALD Pro доверенными контроллерами по этим местоположениям.

Контроллеры доверия управляют большим количеством сетевых служб, чем агенты доверия и таким образом, представляют большую площадь для атак потенциальных злоумышленников.

Контроллер доверия - это мастер FreeIPA, который запускает следующие службы:

- Сервер LDAP с плагинами sigden, extdom и ldap
- KDC с драйвером IPA
- Samba сконфигурирован с помощью модуля ipasam PASSDB
- SSSD с ipa_server_mode=True
- Экземпляр глобального каталога (отдельный экземпляр LDAP с AD-совместимой схемой)

2.5.2. Агенты доверия

Это серверы ALD Pro, которые могут разрешать запросы идентификационных данных от клиентов Astra Linux к контроллерам домена MS AD, используя SSSD. В отличие от контроллеров доверия, агенты доверия не могут обрабатывать запросы на аутентификацию Kerberos.

Доверительный агент - это мастер FreeIPA, который запускает следующие сервисы:

- Сервер LDAP с подключаемыми модулями siding и ext dom
- KDC с драйвером IPA
- SSSD с ipa_server_mode=True

Важно: Нельзя понизить статус существующего контроллера доверия до агента доверия.

2.6. Проверка доступности портов

Для проверки доступности портов контроллера домена **alddc01**.alddomain.lan необходимо:

- Получить список всех контроллеров ALD Pro (FreeIPA) **ipa trustconfig-show | grep -i Контроллеры**
- Запустить PowerShell скрипт на контроллере домена **windc01**.windomain.lan (MS AD)

```
$Servers = "localhost"#,"addc02" #Контроллеры домена Active Directory
$Ports   =  "80",
            "443",
#UDP        "123",
            "135",
#UDP        "137",
#UDP        "138",
            "139",
            "464",
            "389",
            "636",
            "3268",
            "3269",
            "53",
            "445",
            "88"

$Destination = "192.168.88.80" #Контроллер домена ALD Pro
$Results = @()
$Results = Invoke-Command $Servers {param($Destination,$Ports)
                $Object = New-Object PSCustomObject
                $Object | Add-Member -MemberType NoteProperty -Name
↪"ServerName" -Value $env:COMPUTERNAME
                $Object | Add-Member -MemberType NoteProperty -Name
↪"Destination" -Value $Destination
                    Foreach ($P in $Ports){
                        $PortCheck = (Test-NetConnection -Port $p -
↪ComputerName $Destination ).TcpTestSucceeded
                        If($PortCheck -notmatch "True|False"){$PortCheck =
↪"ERROR"}
                        $Object | Add-Member Noteproperty "$("Port " + "$p")
↪" -Value "$($PortCheck)"
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
                    }
                $Object
        } -ArgumentList $Destination,$Ports | select * -ExcludeProperty
↪runspaceid, pscomputername

$Results | Out-GridView -Title "Testing Ports"

$Results | Format-Table -AutoSize
```

([см. подробнее](https://learn.microsoft.com/ru-ru/troubleshoot/windows-server/identity/config-firewall-for-ad-domains-and-trusts))

```
Server              Port Service
123/UDP         W32Time
135/TCP         RPC Endpoint Mapper
137/UDP         netbios-ns
138/UDP         NetBIOS Datagram Service
464/TCP/UDP          Kerberos password change
49152-65535/TCP    RPC for LSA, SAM, NetLogon
389/TCP/UDP          LDAP
636/TCP         LDAP SSL
3268/TCP             LDAP GC
3269/TCP             LDAP GC SSL
53/TCP/UDP           DNS
445/TCP         SMB
49152-65535/TCP    FRS RPC, DFSR RPC
88/TCP/UDP          Kerberos
```

Для проверки доступности портов контроллера домена **windc01**.windomain.lan необходимо:

- Получить список всех MS AD контроллеров домена – запустить в PowerShell

```
Get-ADDomainController -Filter * | ft Hostname,IPv4Address,OperatingSystem,
↪Enabled
```

- Установить nmap и запустить команду на контроллере домена **alddc01**.alddomain.lan (ALD Pro)

```
apt update && apt install nmap -y
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
nmap -sT -sU -p 123,135,137,138,464,389,636,3268,3269,53,445,88 192.168.88.
↪85 #Указать IP всех контроллеров домена Active Directory
```

Список портов контроллера домена **ALD Pro**

```
Server              Port Service
80/TCP              Http
443/TCP             Https
123/UDP          W32Time
135/TCP          RPC Endpoint Mapper
137/UDP          netbios-ns
138/UDP          NETBIOS Datagram Service
139/TCP/UDP         NETBIOS Session Service
464/TCP/UDP          Kerberos password change
49152-65535/TCP     RPC for LSA, SAM, NetLogon
389/TCP/UDP          LDAP
636/TCP          LDAP SSL
3268/TCP             LDAP GC
3269/TCP             LDAP GC SSL
53/TCP/UDP           DNS
445/TCP/UDP          SMB
49152-65535/TCP     FRS RPC, DFSR RPC
88/TCP/UDP          Kerberos
1024-1300/TCP       Epmap listener range
```

2.7. Взаимное перенаправление DNS-зон

Важно: Все контроллеры домена MS AD должны разрешать DNS-запросы к контроллерам домена ALD Pro (прямая и обратная зоны).

Варианты реализации:

- Хранение в Active Directory;
- Ручное добавление.

Для работы доверительных отношений с компьютеров в домене alddomain.lan должны разрешаться имена компьютеров домена windomain.lan и наоборот. Для этого необходимо выполнить взаимное перенаправление DNS-зон.

Для создания перенаправителя (ConditionalForwarder) из домена windomain.lan в alddomain.lan необходимо:

- Запустить PowerShell на контроллере домена **windc01**.windomain.lan (MS AD)

```
Add-DnsServerConditionalForwarderZone -Name "alddomain.lan" -
↪ReplicationScope "Forest" -MasterServers 192.168.88.80

#Вывести список всех созданных ConditionalForwarder
$DNSServer = "windc01"
$Zones = Get-WMIObject -Computer $DNSServer -Namespace "root\MicrosoftDNS" -
↪Class "MicrosoftDNS_Zone"
$Zones | Select-Object Name,MasterServers,DsIntegrated,ZoneType | where {$_.
↪ZoneType -eq "4"} | ft -AutoSize
```

Для проверки доступности домена alddomain.lan необходимо выполнить следующие команды:

```
ping alddc01.alddomain.lan
Resolve-DnsName _ldap._tcp.alddomain.lan -Type SRV
Resolve-DnsName _kerberos._tcp.alddomain.lan -Type SRV
```

Для создания перенаправителя (ConditionalForwarder) из домена alddomain.lan в windomain.lan необходимо:

- Запустить команду на контроллере домена **alddc01**.alddomain.lan (ALD Pro)

```
kinit admin
ipa dnsforwardzone-add windomain.lan --forwarder=192.168.88.85 --forward-
↪policy=only

#Показать параметры зоны windomain.lan
ipa dnsforwardzone-show windomain.lan
```

Для проверки доступности домена windomain.lan необходимо выполнить следующие команды:

```
ping windc01.windomain.lan
dig SRV _ldap._tcp.windomain.lan
dig SRV _kerberos._tcp.windomain.lan
```

2.8. Настройка DNS - доверительные сети (bind trusted_network)

В случаях необходимости ограничения DNS-запросов из определенных сетей на каждом ALD Pro (FreeIPA) контроллере, необходимо внести изменения в файл /etc/bind/ipa-ext.conf:

```
p/* User customization for BIND named
*
* This file is included in /etc/bind/named.conf and is not modified during
↪IPA
* upgrades.
*
* "options" settings must be configured in /etc/bind/ipa-options-ext.conf.
*
* Example: ACL for recursion access:
*
* acl "trusted_network" {
*   localnets;
*   localhost;
*   234.234.234.0/24;
*   2001::co:ffee:babe:1/48;
* };
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
*/

acl "trusted_network" {
localnets;
localhost;
192.168.88.0/24;
172.19.3.0/24;
172.19.4.0/24;
};
```

Для активации дополнительных опций DNS Bind, на каждом ALD Pro (FreeIPA) контроллере необходимо внести изменения в файл **/etc/bind/ipa-options-ext.conf:**

```
/* User customization for BIND named
*
* This file is included in /etc/bind/named.conf and is not modified during
 ↪IPA
* upgrades.
*
* It must only contain "options" settings. Any other setting must be
* configured in /etc/bind/ipa-ext.conf.
*
* Examples:
* allow-recursion { trusted_network; };
* allow-query-cache { trusted_network; };
*/

allow-recursion { trusted_network; };
allow-query-cache { trusted_network; };

/* turns on IPv6 for port 53, IPv4 is on by default for all ifaces */
listen-on-v6 { any; };

/* dnssec-enable is obsolete and 'yes' by default */
dnssec-validation no;
```

2.9. Настройка времени

Перед установлением межлесного доверия необходимо выполнить дополнительную настройку даты/времени и убедиться, что настройки часового пояса и даты/времени на обоих серверах совпадают.

2.9.1. На стороне ALD Pro

1. Статус сервиса времени

```
systemctl status chrony.service
```

2. Проверка источника времени

```
chronyc sources -v
210 Number of sources = 4

.-- Source mode  '^' = server, '=' = peer, '#' = local clock.
/ .- Source state '*' = current synced, '+' = combined , '-' = not combined,
| /   '?' = unreachable, 'x' = time may be in error, '~' = time too variable.
||                                                 .- xxxx [ yyyy ] +/- zzzz
||      Reachability register (octal) -.           |  xxxx = adjusted offset,
||      Log2(Polling interval) --.      |          |  yyyy = measured offset,
||                                \     |          |  zzzz = estimated error.
||                                 |    |           \
MS Name/IP address         Stratum Poll Reach LastRx Last sample
===============================================================================
^- 82.142.168.18                 3  10   377   760   +597us[ +579us] +/-  
 ↪64ms
^* ntp.ix.ru                     1  10   377   106   -135us[ -153us] +/-
 ↪5999us
^- ground.corbina.net            2  10   377   148  -6714us[-6731us] +/-  
 ↪44ms
^- cello.corbina.net             2  10   377  1007  -6747us[-6765us] +/-  
 ↪38ms
```

3. Подробная статистика по источникам времени

```
chronyc sourcestats -v
210 Number of sources = 4
                             .- Number of sample points in measurement set.
                             /    .- Number of residual runs with same sign.
                           |    /    .- Length of measurement set (time).
                           |    |    /      .- Est. clock freq error (ppm).
                           |    |    |      /           .- Est. error in freq.
                           |    |    |     |           /         .- Est. offset.
                           |    |    |     |          |          |   On the -.
                           |    |    |     |          |          |   samples. \
                           |    |    |     |          |          |             |
Name/IP Address            NP  NR  Span  Frequency  Freq Skew  Offset  Std
 ↪Dev
==============================================================================
82.142.168.18              14   8  224m     +0.020      0.065   -215us
 ↪229us
ntp.ix.ru                  18  13  361m     +0.000      0.030    +29ns
 ↪186us
ground.corbina.net         16   9  258m     +0.012      0.053  -8380us
 ↪228us
cello.corbina.net          25  15  430m     +0.055      0.035  -7950us
 ↪334us
```

4. Проверка расхождение времени

```
chronyc tracking
```

Пример результата

```
admin@aldpro01:~$ chronyc tracking
Reference ID    : BC5D6802 (188.93.104.2)
Stratum         : 3
Ref time (UTC)  : Thu Apr 13 10:21:39 2023
System time     : 0.000400797 seconds slow of NTP time
Last offset     : +0.000018209 seconds
RMS offset      : 0.000149458 seconds
Frequency       : 17.812 ppm slow
Residual freq   : +0.000 ppm
Skew            : 0.136 ppm
Root delay      : 0.014107514 seconds
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
Root dispersion : 0.019041860 seconds
Update interval : 515.2 seconds
Leap status     : Normal
```

Текущий конфиг можно посмотреть в файле:

```
less /etc/chrony/chrony.conf
```

2.9.2. На стороне MS AD

Для настройки синхронизации времени с внешним NTP-сервером (настраивается только на PDC в корневом домене) необходимо выполнить следующие команды:

```
w32tm /config /reliable:yes /syncfromflags:manual /manualpeerlist:"ntp.msk-ix.
 ↪ru" /update
net stop w32time
net start w32time
w32tm /resync
w32tm /monitor /computers:"ntp.msk-ix.ru"
w32tm /stripchart /computer:ntp.msk-ix.ru
```

Пример результата

```
PS C:\Users\Administrator> w32tm /stripchart /computer:ntp.msk-ix.ru
Tracking ntp.msk-ix.ru [194.190.168.1:123].
The current time is 4/13/2023 1:40:55 PM.
13:40:55, d:+00.0091883s o:-00.0110417s  [                         *      ]
 ↪                     ]
13:40:57, d:+00.0093593s o:-00.0111335s  [                         *      ]
 ↪                     ]
13:40:59, d:+00.0099441s o:-00.0112867s  [                         *      ]
 ↪                     ]
13:41:01, d:+00.0100102s o:-00.0113176s  [                         *      ]
 ↪                     ]
13:41:03, d:+00.0101050s o:-00.0112696s  [                         *      ]
 ↪                     ]
```

2.9.2.1. Создание доверительных отношений

2.10. Создание двустороннего доверия (Forest Trust)

Во всех инструкциях создание доверия начинают с выполнения команды `ipa-adtrust-install` , которая подготавливает домен FreeIPA к работе с доверительными отношениями, в частности, добавляет атрибут для хранения windows security identifier (SID). В случае с ALD Pro это не требуется. Команда `trustconfig-show` показывает, что домен уже готов к работе с доверительными отношениями:

```
# ipa trustconfig-show
Домен: alddomain.lan
Идентификатор безопасности: S-1-5-21-1307086432-2724870100-1147875473
Имя NetBIOS: ALDDOMAIN
GUID домена: 7a522ccc-a0d7-4eac-a46a-46b12c93fa0e
Резервная основная группа: Default SMB Group
Агенты отношений доверия AD IPA: alddc01.alddomain.lan
Контроллеры отношений доверия AD IPA: alddc01.alddomain.lan
```

Доверие может быть добавлено на стороне ALD Pro из командной строки. При появлении проблем рекомендуется использовать ключи -d и -v для получения дополнительной информации об ошибках.

Перед созданием доверительных отношений нужно запросить Kerberos-билет для учетной записи **admin:**

```
root@alddc01:~# kinit admin
Password for admin@ALDDOMAIN.LAN:
root@alddc01:~#
root@alddc01:~# klist
Ticket cache: KEYRING:persistent:0:0
Default principal: admin@ALDDOMAIN.LAN

Valid starting       Expires              Service principal
22.10.2023 14:55:39  23.10.2023 14:55:36  krbtgt/ALDDOMAIN.LAN@ALDDOMAIN.LAN


#ipa -d -v trust-add --type=ad <DomainName> --admin administrator --password -
↪-two-way=true
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
ipa -d -v trust-add --type=ad windomain.lan --admin administrator --password -
↪-two-way=true

--------------------------------------------------------------------------------
↪--
Добавлено отношение доверия Active Directory для области (realm) "windomain.
↪lan"
--------------------------------------------------------------------------------
↪--
Имя области (realm): windomain.lan
Имя домена NetBIOS: WINDOMAIN
Идентификатор безопасности домена: S-1-5-21-292663598-2229028806-4201728183
Направление отношения доверия: Двустороннее отношение доверия
Тип отношения доверия: Домен Active Directory
Состояние отношения доверия: Установлено и проверено
```

Если в этот момент отслеживать сетевой трафик, то можно будет увидеть, что аутентификация в Windows-домене выполняется по Kerberos, а установление доверия выполняется по транспортному протоколу SMB2 путем вызова удаленных команд RPC. В то же время билет на доступ к службе `krbtgt` в Windows домене не сохраняется в кеше sssd службы, поэтому команда `klist` после установления доверия не покажет дополнительных билетов.

После создания доверия можно посмотреть информацию о созданном доверии командами `trust-find` и `trust-show` :

```
root@alddc01:~# ipa trust-find
----------------------------
найдено 1 отношение доверия
----------------------------
Имя области (realm): windomain.lan
Имя домена NetBIOS: WINDOMAIN
Идентификатор безопасности домена: S-1-5-21-292663598-2229028806-4201728183
Тип отношения доверия: Домен Active Directory
----------------------------------
Количество возвращённых записей 1
----------------------------------
root@alddc01:~#
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
root@alddc01:~# ipa trust-show  windomain.lan
Имя области (realm): windomain.lan
Имя домена NetBIOS: WINDOMAIN
Идентификатор безопасности домена: S-1-5-21-292663598-2229028806-4201728183
Направление отношения доверия: Двустороннее отношение доверия
Тип отношения доверия: Домен Active Directory
```

Так же можно просмотреть, какие контроллеры ALD Pro обрабатывают запросы при работе с доверительными отношениями:

```
root@alddc01:~# ipa trustconfig-show
Домен: alddomain.lan
Идентификатор безопасности: S-1-5-21-1307086432-2724870100-1147875473
Имя NetBIOS: ALDDOMAIN
GUID домена: 7a522ccc-a0d7-4eac-a46a-46b12c93fa0e
Резервная основная группа: Default SMB Group
Агенты отношений доверия AD IPA: alddc01.alddomain.lan
Контроллеры отношений доверия AD IPA: alddc01.alddomain.lan
```

С помощью команд `trust-fetch-domains` и `trustdomain-find` можно подгрузить информацию о дочерних доменах леса и доменах, с которыми у доверенного домена, в свою очередь, построены доверительные отношения. Они потребуются, если позднее в лесе MS AD появятся новые дочерние домены или будут созданы транзитивные доверительные отношения с другими MS AD доменами. При добавлении информации о домене MS AD в каталог ALD Pro каждому домену назначается диапазон POSIX идентификаторов.

2.11. Создание доверия между двумя доменами (External Trust)

2.11.1. Поддержка внешнего доверия к домену из леса MS AD

Внешнее доверие - это доверительные отношения между доменами MS AD, которые находятся в разных лесах MS AD. В то время как для обеспечения доверия к лесу всегда требуется установить доверие **между корневыми доменами** лесов MS AD, внешнее доверие может быть установлено к любому домену в лесу.

2.11.2. Варианты использования

Администратор домена MS AD хочет установить доверие между ALD Pro и своим доменом. Доверие между ALD Pro и внешним доменом MS AD будет непереходным, поскольку никакие пользователи или группы из других доменов MS AD не будут иметь доступа к ресурсам ALD Pro.

2.11.3. Дизайн

Внешнее доверие между доменами MS AD по определению является нетранзитивным и обеспечивает фильтрацию SID между границами домена. Это означает, что только пользователи и группы с SID из доверенного домена могут использовать ресурсы и быть видимыми в системах ALD Pro. Никому из других пользователей и групп из доменов, которым доверенный домен доверяет в своем собственном лесу MS AD, или других доменов, которым доверяют извне, не будет разрешен доступ к ресурсам ALD Pro.

2.11.4. Реализация

Функция внешнего доверия повторно использует существующую инфраструктуру лесного доверия. Существуют изменения, позволяющие поддерживать внешнее доверие:

- Нетранзитивность: поскольку внешнее доверие является нетранзитивным по определению, любая попытка установить функцию транзитивности доверительной ссылки с помощью команды **LSA SetInformationTrustedDomain()** завершится

неудачей. Таким образом, нет необходимости устанавливать транзитивность для внешнего доверия.

- Атрибуты доверия: внешнее доверие может быть обнаружено путем проверки отсутствия атрибута `ipaNTTrustAttributes` LDAP-объекта доверенного домена.

Траст можно добавить на стороне ALD Pro из командной строки. При появлении проблем рекомендуется использовать ключи -d и -v для получения дополнительной информации об ошибках.

Перед созданием доверительных отношений запрашивается Kerberos-билет для учетной записи **admin**:

```
root@alddc01:~# kinit admin
Password for admin@ALDDOMAIN.LAN:
root@alddc01:~#
root@alddc01:~# klist
Ticket cache: KEYRING:persistent:0:0
Default principal: admin@ALDDOMAIN.LAN

Valid starting       Expires              Service principal
22.10.2023 15:10:49  23.10.2023 15:10:46  krbtgt/ALDDOMAIN.LAN@ALDDOMAIN.LAN



ipa -d -v trust-add --type=ad <DomainName> --external=true --admin
 ↪administrator --password --two-way=true

ipa -d -v trust-add --type=ad windomain.lan --external=true --admin
 ↪administrator --password --two-way=true
```

Пример результата:

```
------------------------------------------------------------------------------
 ↪--
Добавлено отношение доверия Active Directory для области (realm) "windomain.
 ↪lan"
------------------------------------------------------------------------------
 ↪--
Имя области (realm): windomain.lan
Имя домена NetBIOS: WINDOMAIN
Идентификатор безопасности домена: S-1-5-21-292663598-2229028806-4201728183
```

(продолжение на следующей странице)

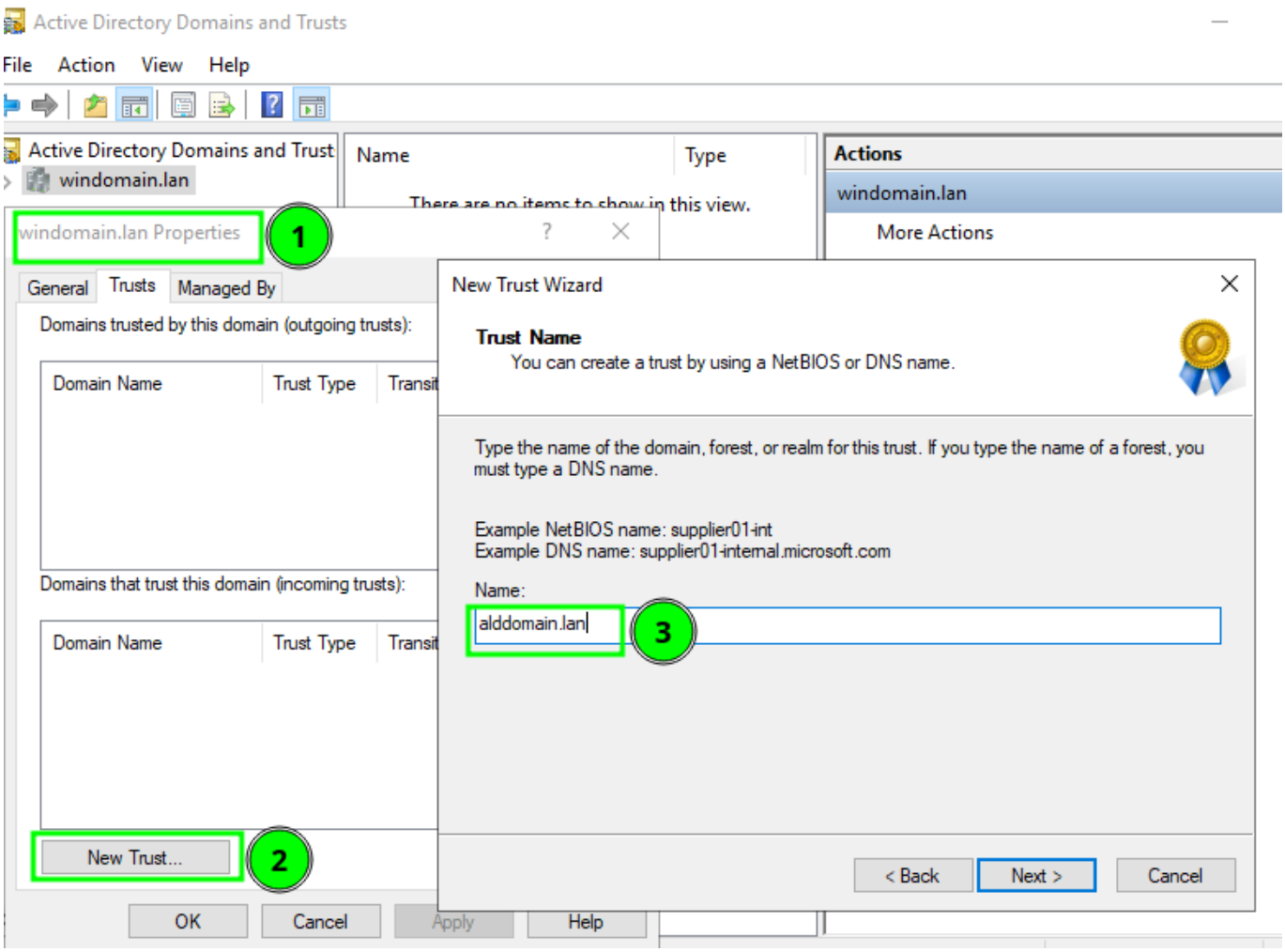
(продолжение с предыдущей страницы)

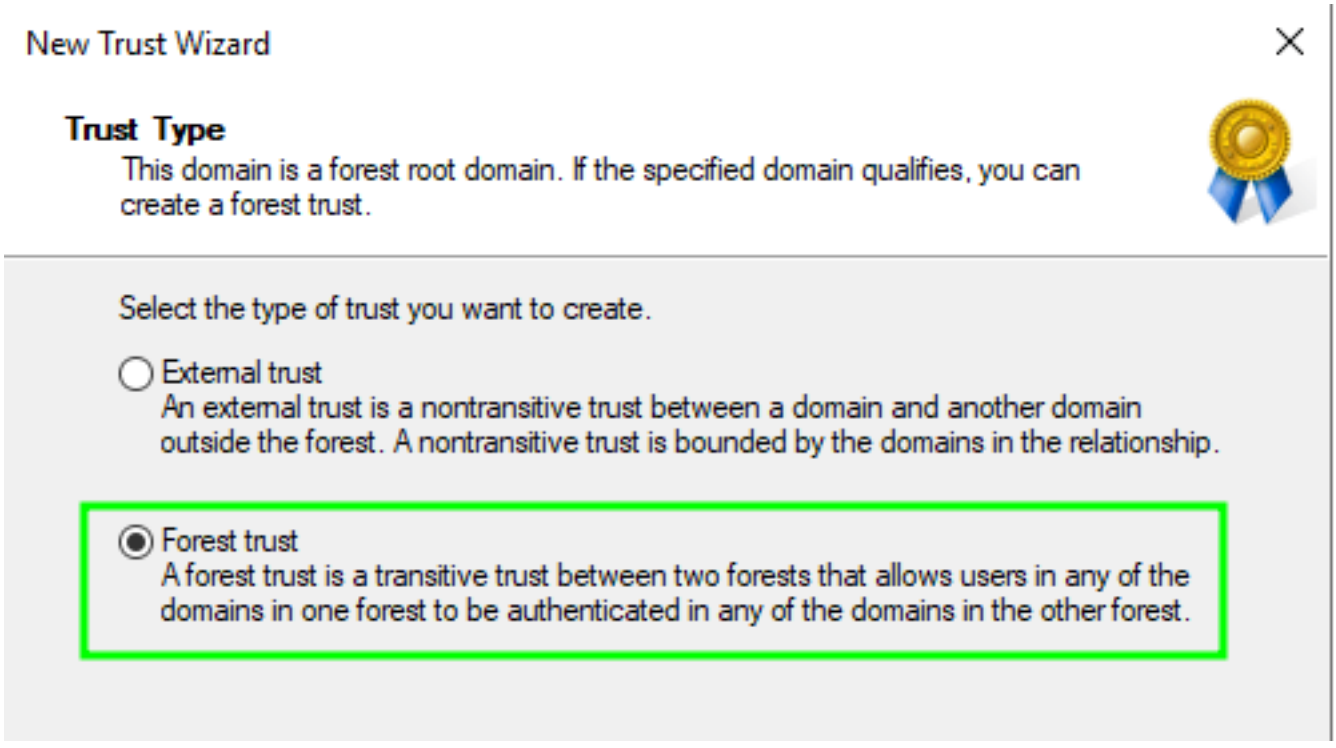
```
Направление отношения доверия: Двустороннее отношение доверия
Тип отношения доверия: Нетранзитивное внешнее отношение доверия с доменом в
 ↪другом лесу Active Directory
Состояние отношения доверия: Установлено и проверено
```

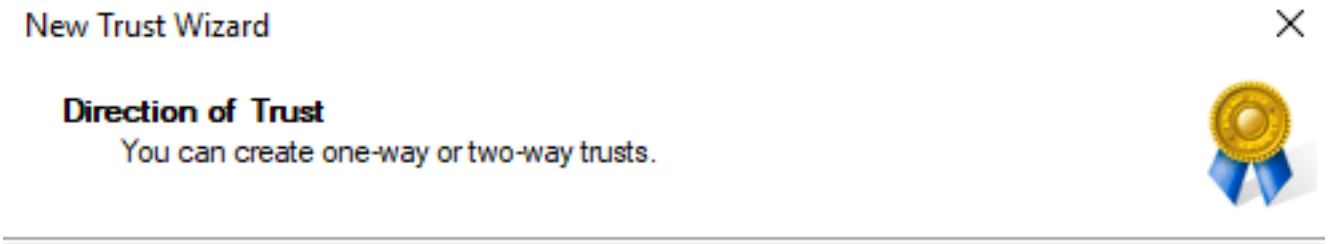
2.11.5. Создание траста (one-way trust using a trust-secret)

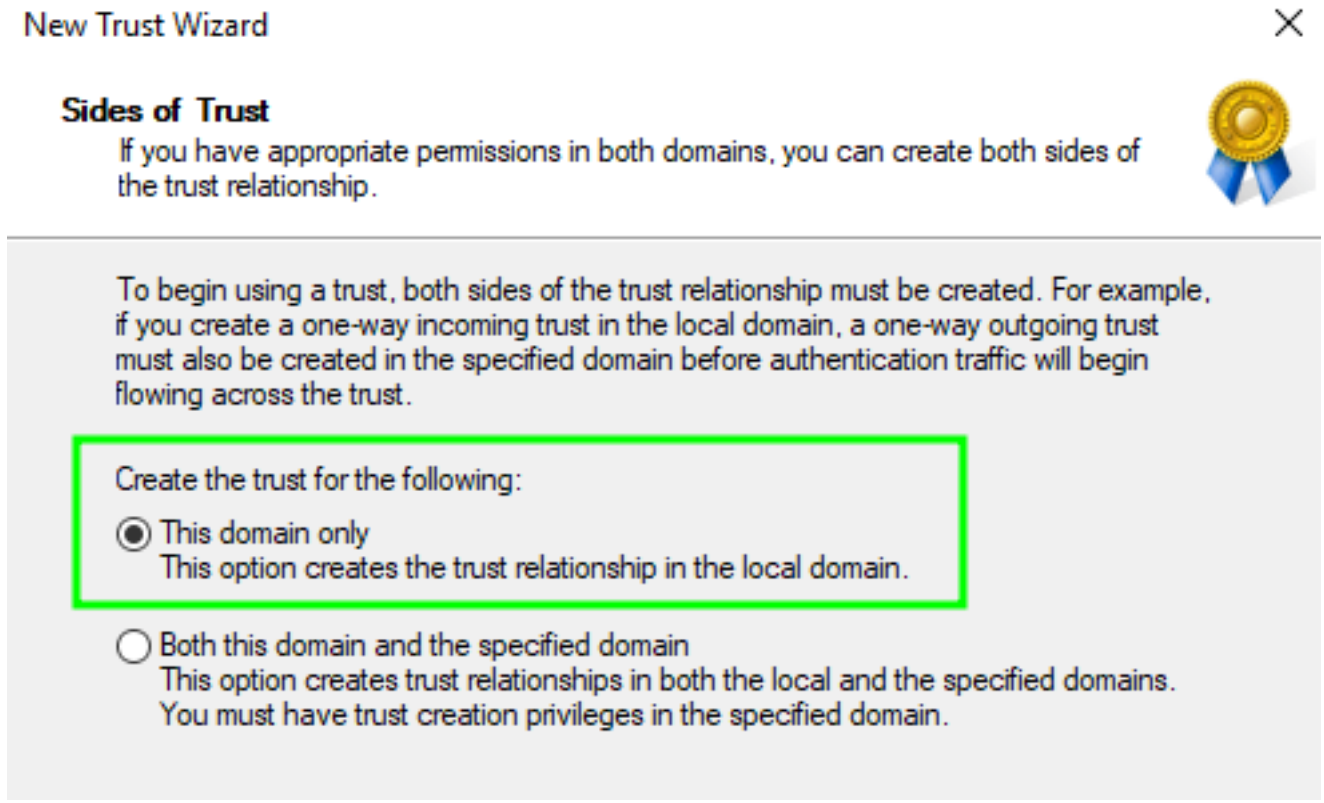
Для создания доверительных отношений, используя секрет доверия, требуется предварительно создать доверие на стороне MS AD (win.company.local).

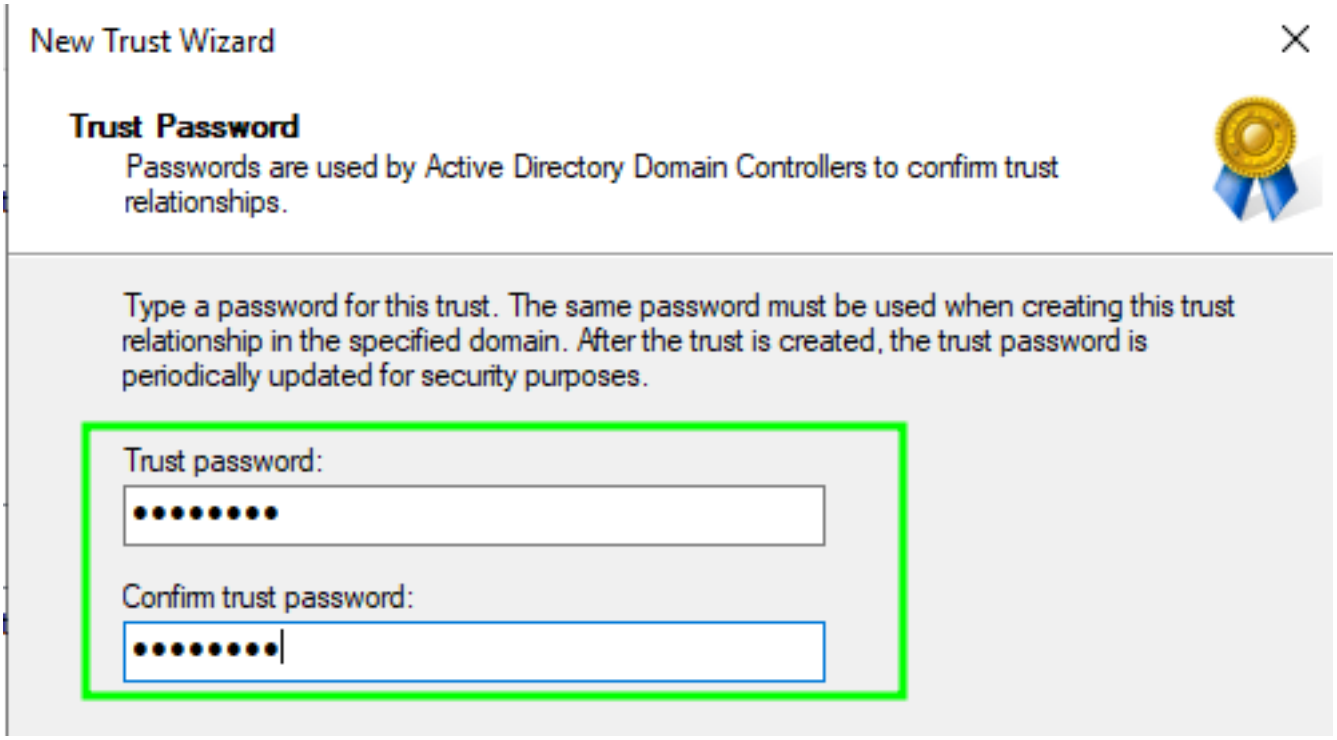
1. На стороне Windows открыть MS AD Domain and Trusts tool
2. Открыть свойства для леса Windows
3. Выбрать вкладку «Трасты» и нажать «Создать траст»
4. Перейти к мастеру создания доверия, введя: - Название ALD Pro-леса, затем «следующий»
5. Выбрать «Лесное доверие» на странице «Тип доверия»
6. Выбрать «Односторонний: входящий» на странице «Направление доверия»
7. Выбрать «Только для этого домена» по бокам страницы доверия
8. Ввести тот же общий секрет, который использовался на шаге (1), с помощью «ipa trust-add»

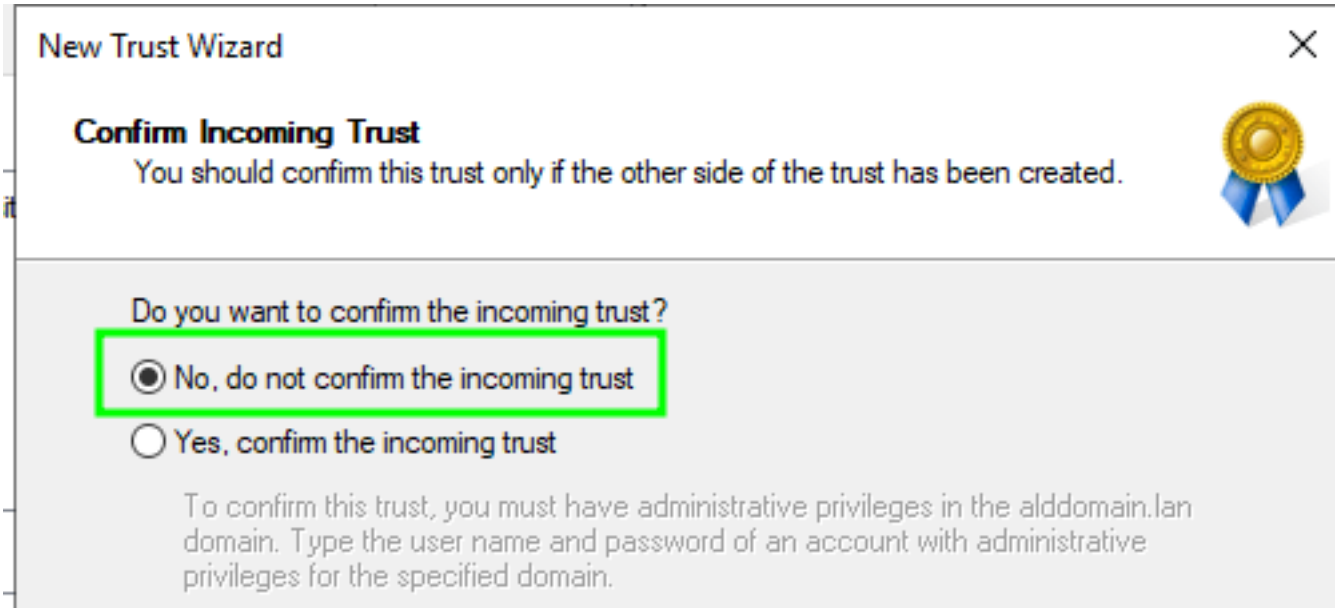

Active Directory Domains and Trusts
File Action View Help
Active Directory Domains and Trust
windomain.lan
Name
Type
There are no items to show in this view.
Actions
windomain.lan
More Actions
windomain.lan Properties
1
General Trusts Managed By
Domains trusted by this domain (outgoing trusts):
Domain Name
Trust Type
Transit
Domains that trust this domain (incoming trusts):
Domain Name
Trust Type
Transit
New Trust...
2
OK
Cancel
Apply
Help
New Trust Wizard
Trust Name
You can create a trust by using a NetBIOS or DNS name.
Type the name of the domain, forest, or realm for this trust. If you type the name of a forest, you must type a DNS name.
Example NetBIOS name: supplier01-int
Example DNS name: supplier01-internal.microsoft.com
Name:
alddomain.lan
3
< Back
Next >
Cancel


New Trust Wizard
Trust Type
This domain is a forest root domain. If the specified domain qualifies, you can create a forest trust.
Select the type of trust you want to create.
External trust
An external trust is a nontransitive trust between a domain and another domain outside the forest. A nontransitive trust is bounded by the domains in the relationship.
Forest trust
A forest trust is a transitive trust between two forests that allows users in any of the domains in one forest to be authenticated in any of the domains in the other forest.


New Trust Wizard
Direction of Trust
You can create one-way or two-way trusts.
Select the direction for this trust.
Two-way
Users in this domain can be authenticated in the specified domain, realm, or forest, and users in the specified domain, realm, or forest can be authenticated in this domain.
One-way: incoming
Users in this domain can be authenticated in the specified domain, realm, or forest.
One-way: outgoing
Users in the specified domain, realm, or forest can be authenticated in this domain.


New Trust Wizard
Sides of Trust
If you have appropriate permissions in both domains, you can create both sides of the trust relationship.
To begin using a trust, both sides of the trust relationship must be created. For example, if you create a one-way incoming trust in the local domain, a one-way outgoing trust must also be created in the specified domain before authentication traffic will begin flowing across the trust.
Create the trust for the following:
This domain only
This option creates the trust relationship in the local domain.
Both this domain and the specified domain
This option creates trust relationships in both the local and the specified domains.
You must have trust creation privileges in the specified domain.





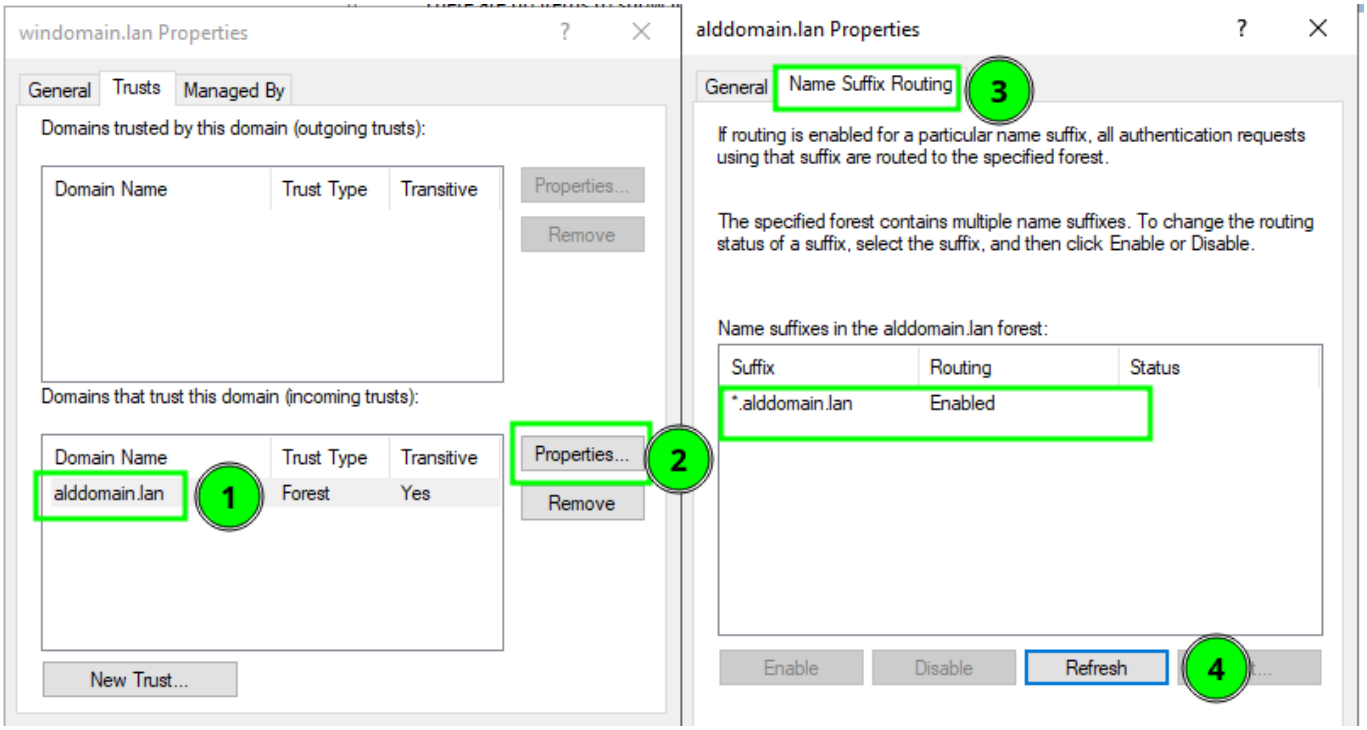

```
# ipa trust-add --type=ad  <DomainName> --trust-secret
root@alddc01:~# ipa trust-add --type=ad  windomain.lan --trust-secret
Общий секрет для отношения доверия:
-------------------------------------------------------------------------------
 ↪--
Добавлено отношение доверия MS AD для области (realm) "windomain.lan"
-------------------------------------------------------------------------------
 ↪--
Имя области (realm): windomain.lan
```

(продолжение на следующей странице)

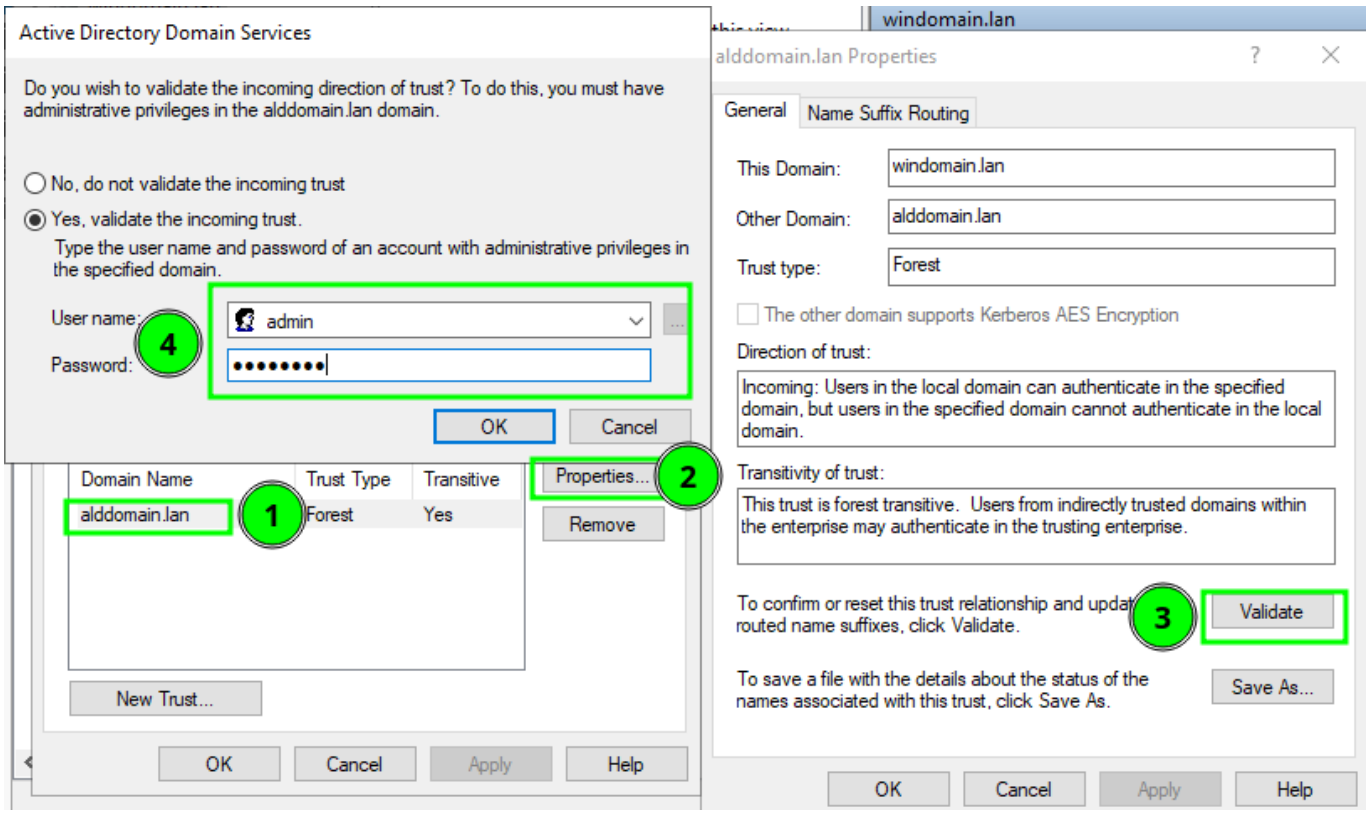
(продолжение с предыдущей страницы)

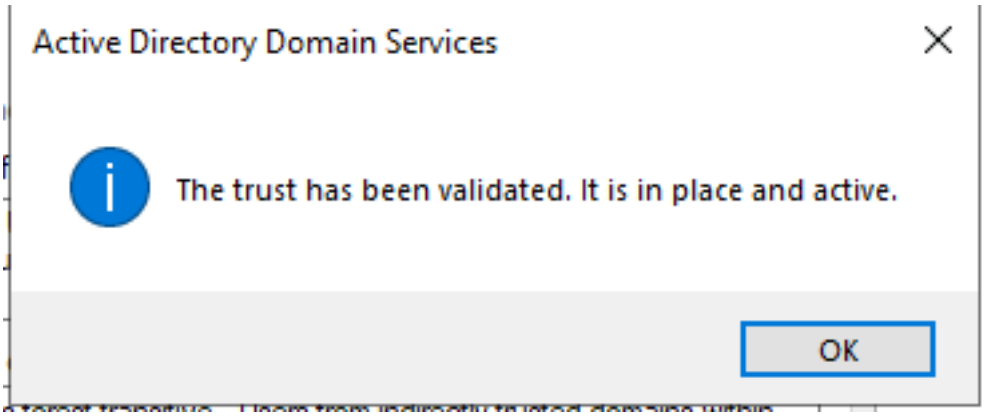
```
Имя домена NetBIOS: WINDOMAIN
Идентификатор безопасности домена: S-1-5-21-292663598-2229028806-4201728183
Направление отношения доверия: Доверяющий лес
Тип отношения доверия: Домен MS AD
Состояние отношения доверия: Ожидание подтверждения удалённой стороной
```

На стороне MS AD необходимо убедиться, что появился суффикс роутинг



Провести валидацию доверия





Если требуется установить двусторонее доверие, то команды будет выглядеть следующим образом:

```
# ipa trust-add --type=ad <DomainName>--trust-secret  --two-way=true

ipa trust-add --type=ad windomain.lan --trust-secret  --two-way=true


#root@aldpro01:~# ipa trust-add --type=ad windomain.lan --trust-secret  --two-
↪way=true
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
Общий секрет для отношения доверия:
--------------------------------------------------------------------------------
 ↪------
Добавлено отношение доверия Active Directory для области (realm) "win.company.
 ↪local"
--------------------------------------------------------------------------------
 ↪------
Имя области (realm): windomain.lan
Имя домена NetBIOS: WINDOMAIN
Идентификатор безопасности домена: S-1-5-21-292663598-2229028806-4201728183
Направление отношения доверия: Двустороннее отношение доверия
Тип отношения доверия: Домен Active Directory
Состояние отношения доверия: Ожидание подтверждения удалённой стороной
```

Для удаление траста необходимо выполнить команду:

```
ipa trust-del windomain.lan
```

2.11.6. MS AD доверие с множеством поддоменов

В больших организация, где поддоменов MS AD более одного, требуется производить дополнительные действия.

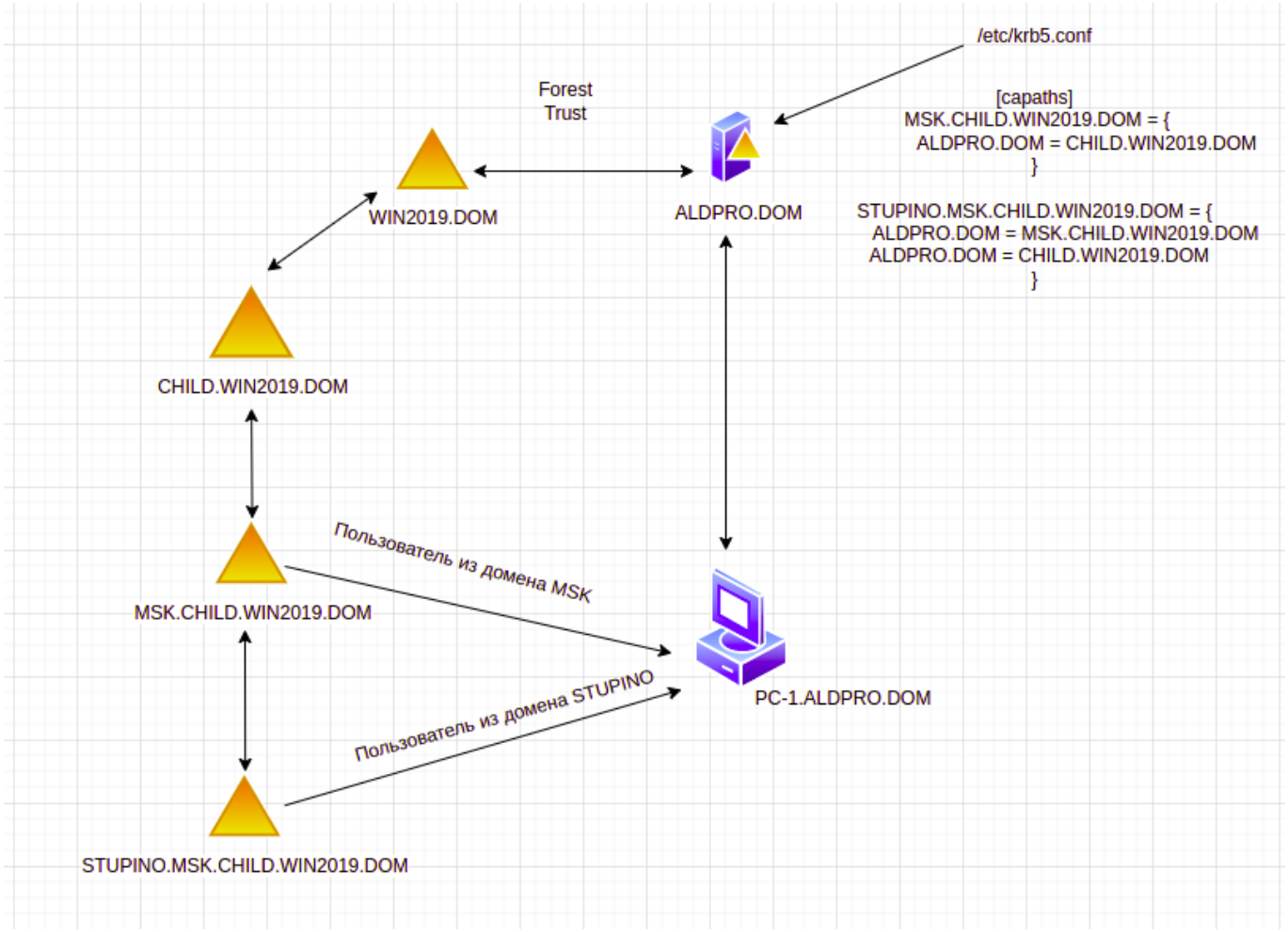
Чтобы выполнить прямую (неиерархическую) аутентификацию между областями, необходима база данных для построения путей аутентификации между областями. В этом разделе определяется нужная база данных.

Клиент использует этот раздел, чтобы найти путь аутентификации между своей областью и областью сервера. Сервер использует этот раздел для проверки пути аутентификации, используемого клиентом, путем проверки поля «Пройдено» в полученном билете. ([см. подробнее](https://web.mit.edu/kerberos/krb5-1.5/krb5-1.5.4/doc/krb5-admin/capaths.html)).

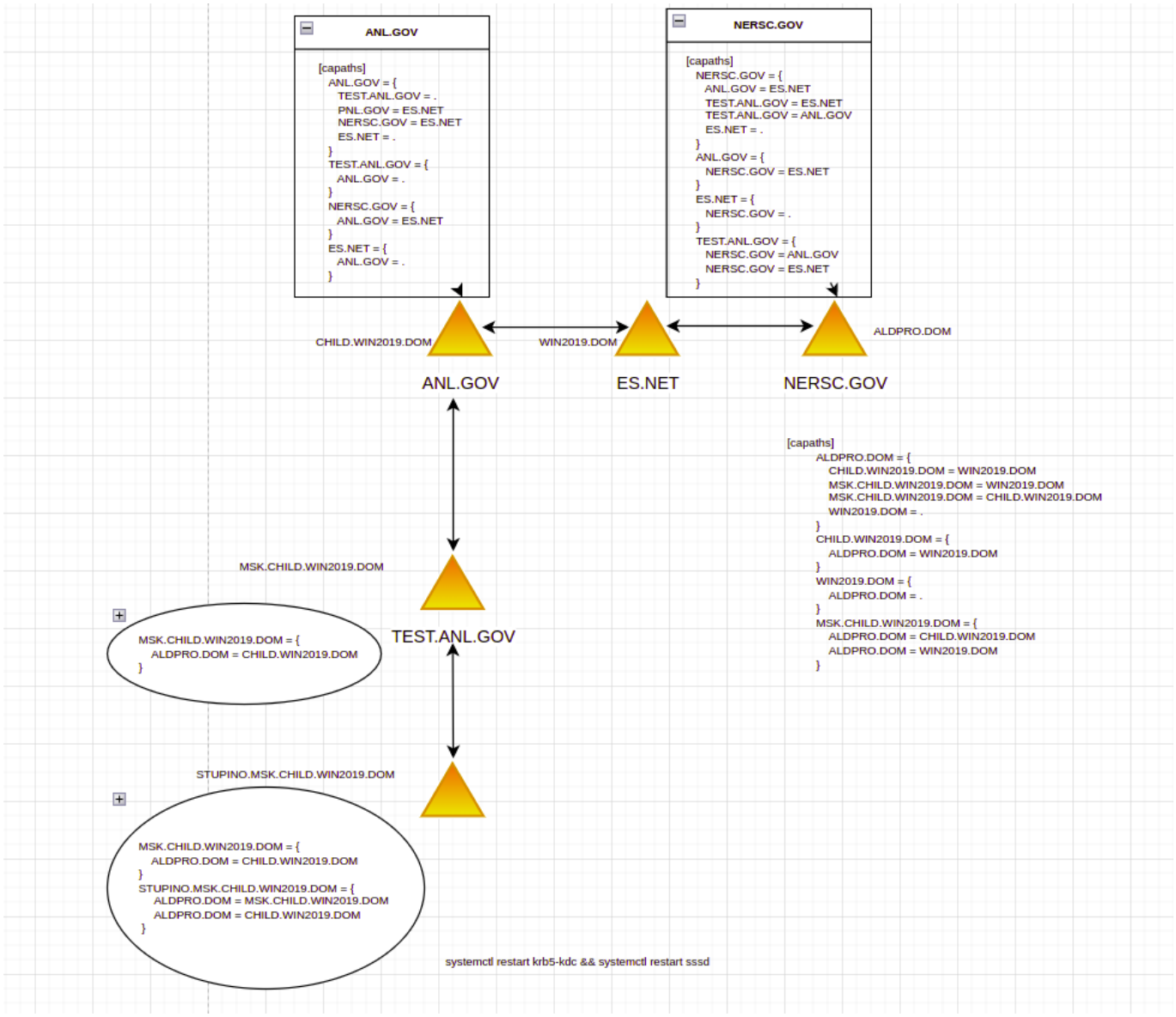
Далее приведен упрощенный визуализированный пример.

Пример многодоменной инфраструктуры, в данном примере для того, чтобы пользователи из поддоменов **msk.child.win2019.dom** и **stupino.msk.child.win2019.dom** смогли войти на PC-1.ALDPRO.DOM. Необходимо добавить в файл **/etc/krb5.conf** следующую информацию:

```
[capaths]

MSK.CHILD.WIN2019.DOM = {

ALDPRO.DOM = CHILD.WIN2019.DOM

}

STUPINO.MSK.CHILD.WIN2019.DOM = {

ALDPRO.DOM = MSK.CHILD.WIN2019.DOM

ALDPRO.DOM = CHILD.WIN2019.DOM

}
```



Пример визуализации официальной статьи
(https://web.mit.edu/kerberos/krb5-1.5/krb5-1.5.4/doc/krb5-admin/capaths.html)



2.11.6.1. Проверки работоспособности доверительных отношений

2.12. Проверка работоспособности доверия (id-идентификация)

Два основных типа запросов, которые может выполнять клиент - это поиск идентификационных данных (id) и аутентификация (login). Для пользователей IPA поиск идентификационных данных представляет собой обычный поиск по протоколу LDAP **на IPA-сервере**, а аутентификация выполняется с помощью внутреннего инструмента, подобного kinit, также подключающегося к IPA-серверу.

Доверенные пользователи MS AD (Trusted AD users) работают по-другому. Поиск идентификационных данных (id) с клиентских компьютеров подключается к IPA-серверу с помощью расширенной операции LDAP. Плагин extdom сервера IPA запрашивает у экземпляра SSSD, запущенного на сервере, информацию о пользователе AD, экземпляр SSSD выполняет поиск на сервере MS AD с использованием протокола LDAP и передает данные обратно клиенту IPA. Для запросов аутентификации на основе пароля (**login**) клиенты IPA подключаются **непосредственно к серверам AD** с помощью Kerberos.

Важно помнить, что во время проверки подлинности должен быть задан правильный набор групп. Поскольку это требование существует, запрос на проверку подлинности также должен выполнить поиск идентификатора (обычно операцию initgroups) перед проверкой подлинности:

1. Убедиться, что все ALD Pro контроллеры отображаются при выполнении команды **ipa trustconfig-show**

```
#Выполнить аутентификацию
kinit admin
#Показать какие контроллеры домена могут обрабатывать Trust с Active
 ↪Directory
ipa trustconfig-show
root@alddc01:~# ipa trustconfig-show
Домен: alddomain.lan
Идентификатор безопасности: S-1-5-21-1307086432-2724870100-1147875473
Имя NetBIOS: ALDDOMAIN
GUID домена: 7a522ccc-a0d7-4eac-a46a-46b12c93fa0e
Резервная основная группа: Default SMB Group
Агенты отношений доверия AD IPA: alddc01.alddomain.lan alddcXX.alddomain.lan
Контроллеры отношений доверия AD IPA: alddc01.alddomain.lan alddcXX.alddomain.
 ↪lan
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
#Показать созданный траст
ipa trust-find windomain.lan
#Показать Направление отношения доверия
ipa trust-show windomain.lan
```

Если контроллер ALD Pro не указан в списке, то требуется проверить наличие ошибок в логах на проблемном контроллере

```
root@alddc02:~# grep -insRH --color=auto "ipa-ad" /var/log
/var/log/ipaserver-install.log:162:2023-05-11T14:56:28Z DEBUG The ipa-adtrust-
 ↪install command failed, exc
eption: ScriptError: Unrecognized error during check of admin rights: 'member_
 ↪user'
```

В данном случае нужно вручную повторно запустить команду **ipa-adtrust-install** на alddc02 контроллере.

2. Проверка топологии репликации суффикса

```
root@alddc01:~# ipa topologysuffix-verify --help
Usage: ipa [global-options] topologysuffix-verify NAME [options]

Проверка топологии репликации для суффикса.

Проверки, которые выполняются:
1. проверка того, не отключена ли топология (иначе говоря, имеются ли пути
 ↪репликации между всеми серверами).
2. проверка того, не превышено ли рекомендованное количество соглашений о
 ↪репликации между серверами.
Options:
-h, --help  show this help message and exit
#
root@alddc01:~# ipa topologysuffix-verify domain
----------------------------------------------------------------------
Топология репликации суффикса "domain" соответствует требованиям.
----------------------------------------------------------------------
```

3. Проверка работоспособности траста с помощью команды **id** (**Требуется выполнить на каждом ALD Pro (FreeIPA) контроллере** домена)

SSSD предоставляет две основные функции: получение информации о пользователях и аутентификацию пользователей. Каждый из них подключается к разным системным API и должен рассматриваться отдельно. Однако успешная аутентификация (**login**) может быть выполнена **только тогда, когда может быть получена информация о пользователе (id).** Поэтому, если аутентификация не работает, важно убедиться, что можно, по крайней мере, получить информацию о пользователе с помощью id.

```
#Очистка всего доступного кеша и перезапуск службы sssd
rm -f /var/lib/sss/db/* /var/lib/sss/mc/* && systemctl restart sssd
#Получение информации о пользователе в домене windomain.lan
id 'windomain\administrator'
#Или
id administrator@windomain.lan

#Пример результата
root@alddc01:~# id administrator@windomain.lan
uid=1131400500(administrator@windomain.lan)
 ↪gid=1131400500(administrator@windomain.lan)
 ↪группы=1131400500(administrator@windomain.lan),1131400520(group policy
 ↪creator
owners@windomain.lan),1131400513(domain users@windomain.lan),
 ↪1131400519(enterprise admins@windomain.lan),1131400518(schema
 ↪admins@windomain.lan),1131400512(domain admi
ns@windomain.lan)
```

2.13. Проверка работоспособности доверия (Kerberos)

Ниже представлены примеры запросов Kerberos-билетов

https://web.mit.edu/kerberos/krb5-1.12/doc/user/user_commands/kinit.html

Запрос Kerberos-билета для примера из домена windomain.lan

Запрос KINIT (kinit получает и кэширует первоначальный билет, предоставляющий право на получение билета для принципала).

```
root@alddc01:~# KRB5_TRACE=/dev/stderr kinit administrator@windomain.lan
[30804] 1698829046.855690: Resolving unique ccache of type KEYRING
[30804] 1698829046.855691: Getting initial credentials for
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
↪administrator@windomain.lan
[30804] 1698829046.855693: Sending unauthenticated request
[30804] 1698829046.855694: Sending request (195 bytes) to windomain.lan
[30804] 1698829046.855695: Initiating TCP connection to stream 192.168.88.
↪85:88
[30804] 1698829046.855696: Sending TCP request to stream 192.168.88.85:88
[30804] 1698829046.855697: Received answer (198 bytes) from stream 192.168.88.
↪85:88
[30804] 1698829046.855698: Terminating TCP connection to stream 192.168.88.
↪85:88
[30804] 1698829046.855699: Response was from master KDC
[30804] 1698829046.855700: Received error from KDC: -1765328359/Additional
↪pre-authentication required
[30804] 1698829046.855703: Preauthenticating using KDC method data
[30804] 1698829046.855704: Processing preauth types: PA-PK-AS-REQ (16), PA-PK-
↪AS-REP_OLD (15), PA-ETYPE-INFO2 (19), PA-ENC-TIMESTAMP (2)
[30804] 1698829046.855705: Selected etype info: etype aes256-cts, salt "WIN-
↪F8I3I8FPJ70Administrator", params ""
[30804] 1698829046.855706: PKINIT client has no configured identity; giving
↪up
[30804] 1698829046.855707: PKINIT client has no configured identity; giving
↪up
[30804] 1698829046.855708: Preauth module pkinit (16) (real) returned: 22/
↪Недопустимый аргумент
Password for administrator@windomain.lan:
```

KLIST перечисляет участника Kerberos и билеты Kerberos, хранящиеся в кэше учетных данных или ключи, хранящиеся в файле keytab.

https://web.mit.edu/kerberos/krb5-1.12/doc/user/user_commands/klist.html

```
root@alddc01:~# klist
Ticket cache: KEYRING:persistent:0:krb_ccache_6c40ahD
Default principal: Administrator@WINDOMAIN.LAN

Valid starting       Expires              Service principal
24.10.2023 13:48:50  24.10.2023 23:48:50  krbtgt/WINDOMAIN.LAN@WINDOMAIN.LAN
        renew until 25.10.2023 13:48:44
```

Запрос KVNO (kvno получает служебный билет для указанных участников Kerberos)

https://web.mit.edu/kerberos/krb5-devel/doc/user/user_commands/kvno.html

```
root@alddc01:~# kvno -S CIFS windc01.windomain.lan
CIFS/windc01.windomain.lan@WINDOMAIN.LAN: kvno = 3
root@alddc01:~#
root@alddc01:~# klist
Ticket cache: KEYRING:persistent:0:krb_ccache_6c40ahD
Default principal: Administrator@WINDOMAIN.LAN

Valid starting       Expires              Service principal
24.10.2023 14:17:17  24.10.2023 23:48:50  CIFS/windc01.windomain.
 ↪lan@WINDOMAIN.LAN
24.10.2023 13:48:50  24.10.2023 23:48:50  krbtgt/WINDOMAIN.LAN@WINDOMAIN.LAN
        renew until 25.10.2023 13:48:44
```

2.14. Дополнительные проверки

```
#Выполняем аутентификацию пользователя из домена AD DS, получаем TGT-билет
 ↪от контроллера AD DS
kinit administrator@windomain.lan
#Получаем для пользователя Cross realm TGT билет у контроллера AD DS для
 ↪сквозной аутентификации на контроллерах ALD Pro
kvno krbtgt/ALDDOMAIN.LAN@WINDOMAIN.LAN
#Используя Cross realm TGT билет получаем у контроллера ALD Pro сервисный
 ↪билет для аутентификации на хосте из домена ALD Pro с fqdn именем alddc01.
 ↪alddomain.lan
kvno host/alddc01.alddomain.lan@ALDDOMAIN.LAN

#Получаем для пользователя Cross realm TGT билет у контроллера ALD Pro для
 ↪сквозной аутентификации на контроллерах Active Directory
kvno krbtgt/WINDOMAIN.LAN@ALDDOMAIN.LAN
#Используя Cross realm TGT билет получаем у контроллера Active Directory
 ↪сервисный билет для аутентификации на хосте из домена Active Directory
kvno host/windc01.windomain.lan@WINDOMAIN.LAN

#Конечный результат
root@alddc01:~# klist
Ticket cache: KEYRING:persistent:0:krb_ccache_B4jH9CO
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
Default principal: Administrator@WINDOMAIN.LAN

Valid starting       Expires              Service principal
24.10.2023 14:41:04  25.10.2023 00:22:09  host/windc01.windomain.
 ↪lan@WINDOMAIN.LAN
24.10.2023 14:39:55  25.10.2023 00:22:09  krbtgt/WINDOMAIN.LAN@ALDDOMAIN.LAN
24.10.2023 14:28:13  25.10.2023 00:22:09  host/alddc01.alddomain.
 ↪lan@ALDDOMAIN.LAN
24.10.2023 14:25:15  25.10.2023 00:22:09  krbtgt/ALDDOMAIN.LAN@WINDOMAIN.LAN
24.10.2023 14:22:09  25.10.2023 00:22:09  krbtgt/WINDOMAIN.LAN@WINDOMAIN.LAN
        renew until 25.10.2023 14:22:04
```

2.14.1. Как работает кросс-доверительная аутентификация Kerberos (Kerberos cross-trust authentication)

Чтобы пройти аутентификацию в службе через доверительное управление с использованием Kerberos, необходим реферал (также известный как билет на получение реферального билета [TGT]). Это билет, запрошенный у локального контроллера домена (DC) для стороннего домена. Чтобы продемонстрировать, как выполняются запросы тикетов в разных доверительных системах, в этом разделе основное внимание уделяется semperis (лабораторный лес).

TGT (Ticket Granting Ticket) = это билет, выдаваемый контроллером домена (DC) после успешной аутентификации пользователя. Он позволяет запрашивать билеты на обслуживание (Service Tickets, ST) для доступа к конкретным сервисам в домене.

TGS(Ticket Granting Service) - это компонент KDC, который выдает запрос на обслуживание, когда участник запрашивает подключение к службе Kerberos. Изначально должен быть билет на предоставление доступа (TGT) для домена (MS AD), прежде чем будет выдан билет на обслуживание в этом домене MS AD.

PAC(Privilege Attribute Certificate) = Сертификат атрибута привилегий. Содержится в TGT, скопирован в служебный билет. Сообщает службе, каким пользователем вы являетесь и в каких группах состоите, на основе идентификаторов безопасности (SID).

Пример SID: S-1-5-21-3286968501-24975625-1618430583-512

1. Пользовательский NTLM hash для запроса TGT
2. TGT зашифрованный krbtgt hash
3. Запрос TGS для server.ad.local
4. TGT зашифрованный Inter Realm trust key krbtgt/MSK.CHILD.ALD.DOM@MSK.CHILD.ALD.DOM
5. Клиент запрашивает TGT krbtgt/CHILD.ALD.DOM@MSK.CHILD.ALD.DOM
6. Cross-realm ticket granting ticket krbtgt/CHILD.ALD.DOM@MSK.CHILD.ALD.DOM
7. С помощью билета krbtgt/CHILD.ALD.DOM@MSK.CHILD.ALD.DOM клиент запрашивает билет krbtgt/ALD.DOM@CHILD.ALD.DOM для пересечения границ (cross-realm ticket)
8. Cross-realm ticket granting ticket krbtgt/ALD.DOM@CHILD.ALD.DOM
9. С помощью билета krbtgt/ALD.DOM@CHILD.ALD.DOM клиент запрашивает билет krbtgt/AD.LOCAL@ALD.DOM для пересечения границ (cross-realm ticket)
10. Cross-realm ticket granting ticket krbtgt/AD.LOCAL@ALD.DOM
11. С помощью билета krbtgt/AD.LOCAL@ALD.DOM, выданного KDC области ALD.DOM, клиент запрашивает у KDC области AD.LOCAL (TGS) билет для участника обслуживания (service principal) в области AD.LOCAL.

12. TGS ticket granting service билет service/server@AD.LOCAL, требовалось получить три промежуточных (cross-realm tickets) билета для разных областей.

После этого кэш учетных данных содержит заявки для:

- krbtgt/MSK.CHILD.ALD.DOM@MSK.CHILD.ALD.DOM,
- krbtgt/CHILD.ALD.DOM@MSK.CHILD.ALD.DOM,
- krbtgt/ALD.DOM@CHILD.ALD.DOM,
- krbtgt/AD.LOCAL@ALD.DOM и service/hostname@AD.LOCAL.

13. TGS ticket granting service билет service/server@AD.LOCAL (AP REQ включающий TGS для доступа)

14. AP REP (SERVER считывает учетные данные безопасности пользователя и соответствующим образом создает токен доступа)

2.14.1.1. Поддержка UPN (User Principal Names) для доверенных доменов (trusted_domains)

Основное имя пользователя (UPN) в MS AD является основной формой обращения к пользователям. UPN имеет структуру «**имя пользователя@суффикс**», где как имя пользователя, так и части суффикса могут различаться. По умолчанию суффикс совпадает с доменным именем MS AD, но администраторы MS AD могут создавать дополнительные суффиксы имен и связывать их с конкретными пользователями. Эти дополнительные UPN для пользователей затем могут использоваться для проверки подлинности Kerbers в доменах MS AD.

Альтернативные UPN часто используются, когда несколько компаний с развертываниями MS AD объединяются и хотят предоставить единое пространство имен для входа в систему.

Цель - разрешить использование альтернативных UPN, связанных с пользователями MS AD, при доступе к ресурсам в домене ALD Pro.

Пример:

Пользователь MS AD хочет войти в систему, используя свое **имя пользователя@EXAMPLE** (user pricipal), даже если его домен Active Directry назван REGION.EXAMPLE.COM.

2.15. Включение поддержки UPN на стороне клиента

SSSD уже поддерживает вход в систему с помощью UPN, запрашивая у KDC принятие корпоративных имен для входа. По умолчанию использование корпоративных участников **отключено**, поэтому в sssd.conf необходимо добавить **krb5_use_enterprise_principal = True** чтобы включить его.

```
root@pc-1:~# nano /etc/sssd/sssd.conf

[domain/windomain.lan]

id_provider = ipa
ipa_server = _srv_, alddc01.windomain.lan
ipa_domain = ald.dom
ipa_hostname = pc-1.windomain.lan
auth_provider = ipa
chpass_provider = ipa
access_provider = ipa
cache_credentials = True
ldap_tls_cacert = /etc/ipa/ca.crt
krb5_store_password_if_offline = True
krb5_use_enterprise_principal = True
```

2.16. Проверка поддержки UPN на стороне сервера

IPA KDC действительно понимает несколько доменов, связанных с доверенным лесом AD. Однако, поскольку информация о суффиксах имен, связанных с лесом, недоступна, он не может учитывать их при обработке имен входа enteprise для выдачи ссылок в правильную область. Необходимо добавить поддержку, позволяющую ALD Pro (FreeIPA) KDC искать суффиксы имен, связанные с доверенным лесом.

Первым делом необходимо убедиться, что ALD Pro контроллер видит необходимый суффикс

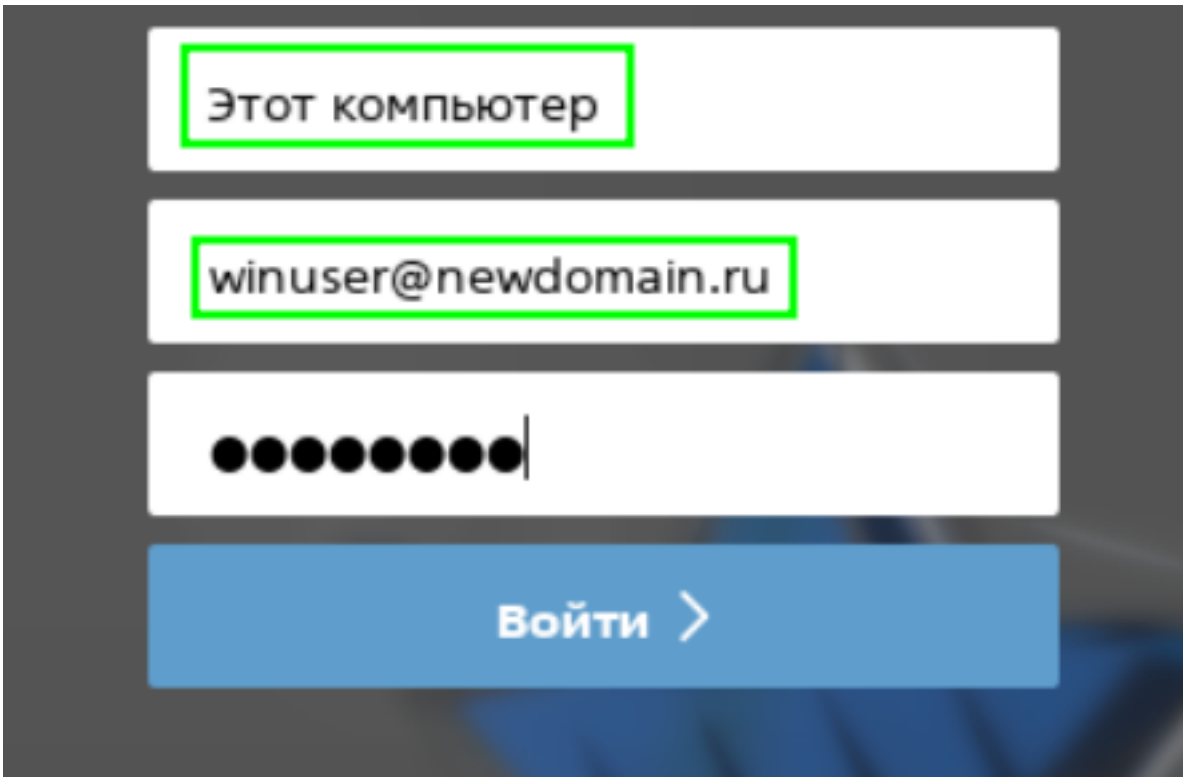
```
#Выполняем аутентификацию
kinit admin

```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
#Обновляем список надежных доменов
ipa trust-fetch-domains windomain.lan

#Получить информацию по домену
ipa trustdomain-find

#Обновляем информацию по Trust windomain.lan
ipa trust-show windomain.lan

#Пример результата
root@alddc01:~# ipa trust-show windomain.lan
Имя области (realm): windomain.lan
Имя домена NetBIOS: WINDOMAIN
Идентификатор безопасности домена: S-1-5-21-292663598-2229028806-4201728183
Направление отношения доверия: Двустороннее отношение доверия
Тип отношения доверия: Домен Active Directory
Суффиксы UPN: newdomain.ru
```

2.17. Проверка работоспособности UPN через графику



2.18. Проверка работоспособности UPN через SSH

```
ssh winuser@newdomain.lan@pc-1
winuser@windomain.lan@pc-1:~$ whoami
winuser@windomain.lan
winuser@windomain.lan@pc-1:~$ id winuser@newdomain.lan
uid=1524001110(winuser@windomain.lan) gid=1524001110(winuser@windomain.lan)
 ↪группы=1524001110(winuser@windomain.lan),1524000513(domain users@windomain.
 ↪lan)
```

Администратор может отключить автоматическое обнаружение серверов и сайтов MS AD в доверенном домене MS AD и вместо этого вручную перечислить серверы, сайты или и то, и другое, чтобы ограничить список серверов MS AD, с которыми взаимодействует SSSD. Например, это позволит избежать обращения к сайтам, которые недоступны.

Эта процедура описывает ручную настройку серверов MS AD, к которым подключается SSSD, путем редактирования файла **/etc/sssd/sssd.conf**.

Если SSSD-клиенты напрямую подключены к домену MS AD, процедура выполняется на всех клиентах.

В настройке ограничение доступа к контроллерам домена MS AD(DCs) или сайтам также настраивает SSSD-клиенты для подключения к определенному серверу или сайту для проверки подлинности.

Если SSSD-клиенты находятся в домене ALD Pro (FreeIPA), который находится в доверительном управлении с MS AD, процедура выполняется только на сервере управления идентификацией ALD Pro (FreeIPA).

Важно убедиться, что у ALD Pro (FreeIPA) домена есть **отдельный раздел [domain]** в **/etc/sssd/sssd.conf**. Заголовки разделов доверенного домена соответствуют этому шаблону:

```
[domain/ald.example.com/ad.example.com]
```

2.19. Настройка сервера ALD Pro (FreeIPA) на определенный сайт MS AD (id, logon)

```
[domain/alddomain.lan/windomain.lan]
ad_site = Default-First-Site-Name
```

В этой настройке ограничение (Restricting) сайтов MS AD выполняется **только для** идентификации (команда **id**), для аутентификации (**logon**) в указанном сайте MS AD требуется выполнить вышеуказанную настройку на **каждом клиенте**.

2.20. Настройка клиента на определенный сайт MS AD (id, logon)

```
[[domain/alddomain.lan]
id_provider = ipa
ipa_server = _srv_, alddc01.alddomain.lan
ipa_domain = alddomain.lan
ipa_hostname = alddc01.alddomain.lan
auth_provider = ipa
chpass_provider = ipa
access_provider = ipa
cache_credentials = True
ldap_tls_cacert = /etc/ipa/ca.crt
krb5_store_password_if_offline = True
debug_level = 9
[sssd]
services = ifp
domains = alddomain.lan
[nss]
homedir_substring = /home
[pam]
[sudo]
[autofs]
[ssh]
[pac]
[ifp]
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
allowed_uids = 0, 33, 114, fly-dm, ipaapi
[secrets]
[session_recording]
[domain/alddomain.lan/windomain.lan]
ad_site = Default-First-Site-Name
```

Расположение конфигурационных файлов

```
SSSD
/etc/sssd/sssd.conf
PAM
/etc/pam.d/system-auth or
/etc/pam.d/system-auth-ac (with authconfig)
NSS
/etc/nsswitch.conf
DNS
/etc/resolv.conf
Samba
/etc/samba/smb.conf
Winbind
/etc/security/pam_winbind.conf
Kerberos
/etc/krb5.conf
```

2.21. Настройка журналов отладки для доменов SSSD

Каждый домен устанавливает свой собственный уровень журнала отладки. Увеличение уровня журнала может предоставить больше информации о проблемах с SSSD или с конфигурацией домена.

Чтобы изменить уровень ведения журнала, существует 2 способа:

A) Установить параметр **debug_level** для каждого раздела в файле /etc/sssd/sssd.conf, для которого будут создаваться дополнительные журналы, перезапустите сервис SSSD.

```
systemctl restart sssd.service
```

Данный способ **будет работать даже после перезапуска сервиса SSSD**.

Пример:

```
[domain/alddomain.lan]
debug_level = 9
[sssd]
debug_level = 9
[nss]
debug_level = 9
[pam]
debug_level = 9
```

В) Установить дополнительный пакет и включить необходимый уровень логирования. **Все изменения применяются «на лету» ко всем разделам**, вносить вручную в sssd.conf файл не требуется.

Данный способ работает **до перезапуска службы SSSD**.

```
apt update && apt install sssd-tools

sss_debuglevel 6
```

2.22. Описание уровней логирования SSSD

Описание уровней сообщений в журналах SSSD:

0 Фатальные сбои: Любые сбои, которые могли бы помешать запуску SSSD или привести к его остановке.

1 Критические сбои: Ошибка, которая не останавливает SSSD, но указывает на то, что как минимум одна основная функция не будет работать должным образом.

2 Серьезные сбои: Ошибка, объявляющая, что определенный запрос или операция завершился неудачей.

3 Мелкие сбои: Это ошибки, которые могли бы привести к сбою операции с уровнем 2.

4 Настройки конфигурации: Сообщения, связанные с настройками конфигурации.

5 Данные о функции: Информация о функциях и данных, связанных с ними.

6 Сообщения трассировки для функций операций: Сообщения, предназначенные для отслеживания выполнения определенных операций.

7 Сообщения трассировки для внутренних управляющих функций: Сообщения, связанные с внутренними функциями управления SSSD.

8 Содержимое внутренних переменных функций, которое может быть интересным: Отладочная информация, связанная с переменными внутри функций.

9 Информация с очень низким уровнем трассировки: Экстремально низкоуровневая отладочная информация.

2.23. Описание SSSD журналов событий

SSDD использует ряд файлов журнала для представления информации о своей работе, расположенных в каталоге **/var/log/sssd/**.

SSSD создает файл журнала для каждого домена, а также файл sssd_pam.log и sssd_nss.log.

krb5_child.log: (short-lived helper process) содержит информацию, связанную с аутентификацией Kerberos, которая используется для безопасной аутентификации в сетевой среде.

ldap_child.log: (short-lived helper process) Этот журнальный файл связан с службами LDAP (Lightweight Directory Access Protocol), участвующего в обмене данными с сервером LDAP (MS AD).

selinux_child.log: (short-lived helper process) SELinux (Security-Enhanced Linux) - это функция безопасности в Linux. Этот журнальный файл содержит информацию, связанную с событиями и активностью, связанной с SELinux.

sssd_<ALD Domain Name>.log: Эти журнальные файлы специфичны для службы SSSD (System Security Services Daemon) и обычно именуются именем домена MS AD, с которым взаимодействует SSSD.

sssd_ifp.log: Этот журнальный файл относится к службе InfoPipe (IFP) в SSSD, обеспечивает интерфейс общей шины, доступный по системной шине.

sssd.log: Файл журнала для SSSD, взаимодействующего со своими процессами-ответчиками.

sssd_nss.log: Этот журнальный файл фокусируется на компоненте Name Service Switch (NSS) SSSD, которая обрабатывает разрешение имен пользователей и групп (выполнение команды id).

sssd_pac.log: Этот журнальный файл содержит информацию, связанную с Privilege Attribute Certificate (PAC) в контексте SSSD и аутентификации. Определяет, как SSSD работает с Kerberos для управления пользователями и группами MS AD.

sssd_pam.log: Этот журнальный файл связан с службой Pluggable Authentication Module (PAM) в SSSD, отвечающей за аутентификацию и авторизацию.

sssd_ssh.log: Этот журнальный файл специфичен для действий, связанных с SSH в рамках SSSD, особенно в отношении аутентификации SSH.

Кроме того, в файле /var/log/secure регистрируются сбои аутентификации и причина сбоя.

```
### Все тесты необходимо выполнять на контроллере домена ALD Pro(FreeIPA)
#Установка sssd-tools на контроллер домена
apt update && apt install sssd-tools

#Проверка сервисов контроллера домена ALD Pro (FreeIPA)
ipactl status
#Проверка конфигурационного файла /etc/sssd/sssd.conf на ошибки
sssctl config-check

#Проверка доступности Winbind
wbinfo --ping
#Проверка  NETLOGON соединения с контроллером ALD Pro (FreeIPA)
wbinfo --ping-dc
#Показать к какому контроллеру Active Directory подключен Winbind
wbinfo --dsgetdcname=windomain.lan
#Проверка активных подключений через Winbind
wbinfo --online-status

#Проверка работоспособности службы SSSD
sssd -d4 -i
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
#Вывести список доменов которые видет SSSD
sssctl domain-list
#Проверка активных подключений через SSSD(предварительно выполните id
 ↪Administrator@windomain.lan)
sssctl domain-status windomain.lan

# Включение уровня логирования
sss_debuglevel 6
# Обнуление журналов по необходимости
truncate -s 0 /var/log/sssd/*
#Удаление всего кеша с контроллера домена и перезапуск службы sssd
rm -f /var/lib/sss/db/* /var/lib/sss/mc/* && systemctl restart sssd

#identity lookups(id) проверка способ 1
id winuser@windomain.lan
#identity lookups(id) проверка способ 2
id 'windomain\winuser'
#Все ошибки id будут фиксироваться в 2 журнала sssd_nss.log и sssd_<ALD
 ↪Domain Name>.log
#Команда отображает пользовательские данные, доступные через NSS и ответчик
 ↪Infopipe для интерфейса D-Bus. Отображаемые данные показывают, авторизован
 ↪ли пользователь для входа в систему с помощью служб system-auth PAM.
sssctl user-checks winuser@windomain.lan
```

2.24. Настройка журналов отладки

Вся конфигурация Samba располагается в двух местах, стандартный файл конфигурации располагается по пути ./etc/samba/smb.conf, этот файл не рекомендуется изменять, при проблемах с доверием в некоторых случаях потребуется повторно выполнить команду **ipa-adtrust-install** которая **перетрет** все внесенные изменения в указанный файл, а также обнулит и запишет из шаблона по умолчанию параметры реестра в файл /var/lib/samba/registry.tdb, так же команду **ipa-adtrust-install** потребуется сделать, если база данных, содержащая реестр параметров для Samba (/var/lib/samba/registry.tdb), была удалена.

```
#root@dc1:/var/lib/samba# ls -lh
итого 2,2M
-rw-------  1 root root          412K ноя 14 16:20 account_policy.tdb
-rw-r--r--  1 root root           225 ноя 17 10:41 browse.dat
drwxr-xr-x  4 root root          4,0K ноя 13 15:52 DriverStore
-rw-------  1 root root          416K ноя 14 17:33 group_mapping.tdb
-rw-------  1 root root           12K ноя 17 09:15 netsamlogon_cache.tdb
drwxr-xr-x 11 root root          4,0K ноя 13 15:52 printers
drwxr-xr-x  2 root root          4,0K ноя 14 10:33 printing
drwxr-xr-x  3 root root          4,0K ноя 13 16:04 private
-rw-------  1 root root          516K ноя 14 17:32 registry.tdb
-rw-------  1 root root          412K ноя 14 16:20 share_info.tdb
drwxrwx--T  2 root sambashare    4,0K ноя 13 15:52 usershares
-rw-------  1 root root           32K ноя 17 08:47 winbindd_cache.tdb
-rw-r--r--  1 root root          412K ноя 14 17:45 winbindd_idmap.tdb
drwxr-x---  2 root winbindd_priv 4,0K ноя 17 08:47 winbindd_privileged
```

account_policy.tdb Основное предназначение заключается в хранении настроек политики учетных записей для пользователей на сервере Samba. Эти настройки включают параметры, связанные с политикой паролей, блокировкой учетных записей и другие параметры безопасности.

browse.dat Файл в директории /var/lib/samba в Samba используется для хранения информации о браузере (Browser Information). Этот файл содержит данные о доступных ресурсах и службах в сети, которые могут быть предоставлены сервером Samba.

group_mapping.tdb Файл в директории /var/lib/samba в Samba используется для хранения отображений между группами в системе Samba и соответствующими группами в сетевой службе, например, в Microsoft Active Directory.

netsamlogon_cache.tdb Файл в директории /var/lib/samba в Samba представляет собой базу данных TDB, которая используется для кэширования информации, связанной с обработкой запросов NetLogon в рамках протокола аутентификации в сетевых службах, таких как Microsoft Active Directory.

registry.tdb - это файл TD (Trivial Database), используемый Samba, который представляет собой реализацию протокола Server Message Block (SMB) с открытым исходным кодом. Файл registry.tdb специально хранит данные конфигурации в формате ключ-значение, аналогичном кусту реестра Windows.

В контексте Samba файл registry.tdb **используется для хранения параметров**

конфигурации, относящихся к реестру Windows. Сюда входит информация о системе, сетевых настройках и других параметрах конфигурации, необходимых для функционирования сервера Samba.

share_info.tdb Файл в директории /var/lib/samba в Samba представляет собой базу данных TDB, используемую для хранения информации о совместно используемых ресурсах (шарах) в Samba.

winbindd_cache.tdb Файл в директории /var/lib/samba в Samba представляет собой базу данных TDB, используемую для кэширования данных и запросов, выполняемых службой Winbind в рамках протокола аутентификации и авторизации в среде Samba.

winbindd_idmap.tdb Файл в директории /var/lib/samba в Samba представляет собой базу данных TDB, используемую для хранения информации о сопоставлении (маппинге) идентификаторов безопасности (SID) и POSIX UID/GID в процессе аутентификации и авторизации через Winbind.

Для просмотра содержимого файлов XXXX.tdb в Samba используется утилита tdbtool. Пример команды для просмотра содержимого registry.tdb:

tdbtool registry.tdb dump

Эта команда выводит содержимое registry.tdb в формате ключ-значение. Важно убедиться, что каманда выполняется с правами пользователя, достаточными для чтения файла registry.tdb.

Для более удобного просмотра всех настроек Samba, **включая реестр**, можно использовать команду **net conf list**

Команда net conf list в Samba используется для отображения текущей конфигурации Samba. Она выводит различные параметры и настройки, связанные с работой Samba, включая параметры глобальной секции smb.conf, информацию о доменах, настройки Kerberos и другие параметры.

Более подробную информацию о реестре можно найти по адресу

https://www.samba.org/~obnox/presentations/linux-kongress-2008/lk2008-obnox.pdf

Каждая служба устанавливает свой собственный уровень журнала отладки. Увеличение уровня журнала может предоставить больше информации о проблемах с Winbind,Samba(smbd) или nmbd

Чтобы изменить уровень ведения журнала, существует 2 способа:

1. Увеличение уровня ведения журнала winbind или samba без перезапуска служб

```
#Проверяем текущие настройки для сервисов smdb и winbind
smbcontrol smbd debuglevel
smbcontrol winbind debuglevel
#smbcontrol nmbd debuglevel

#Устанавливаем уровень логирования(на лету) 100 для сервисов smdb и winbind
smbcontrol smbd debug 100
smbcontrol winbind debug 100
#smbcontrol nmbd debug 100
```

Настройка журналов без перезапуска демона также полезно в тех случаях, когда перезапуск службы временно устраняет проблему на неопределенный период времени. Недостатком является то, что увеличение количества журналов после возникновения проблемы может привести к отсутствию информации, но это не требуется в тех случаях, когда известно, как воспроизвести проблему.

2. Увеличение уровня ведения журнала winbind или samba с перезапуском служб

```
#Остановите службы smb и winbind.
systemctl stop smbd.service winbind.service

#Установите уровень логирования для служб smb и winbind
net conf setparm global 'log level' 100

#Удалите предыдущие журналы samba
rm /var/log/samba/log.*
#Запустите службы smb и winbind
systemctl start smbd.service winbind.service
#Проведите необходимые тесты и создайте архив с журналами
tar -cvf debugging-smb_winbind.tar  /var/log/samba/log.*
```

Выключение режима повышенного журналирования (Disable debugging)

```
#Остановите службы smb и winbind.
systemctl stop smbd.service winbind.service
#Установите уровень логирования для служб smb и winbind
net conf setparm global 'log level' 0
#Запустите службы smb и winbind
systemctl start smbd.service winbind.service
```

3. Так же можно интерективно смотреть, что происходит с winbind в момент старта службы для этого выполните поочередно команды ниже:

```
systemctl stop  winbind.service
winbindd -i -d 100
```

4. Если требуется повысить логирование только для определенного сервиса, в данном примере логирование включено «1» для всех сервисов, кроме winbind - для него включен уровень «100» . **/etc/samba/smb.conf**

```
### Added by IPA Installer ###
#         DO NOT EDIT         #
[global]
debug pid = yes
state directory = /var/lib/samba
cache directory = /var/lib/samba
include = registry
log level = 1 winbind:100

[gluster-aldpro-volume01]
comment = For samba share of volume aldpro-volume01
vfs objects = glusterfs
glusterfs:volume = aldpro-volume01
glusterfs:logfile = /var/log/samba/glusterfs-aldpro-volume01.%M.log
glusterfs:loglevel = 7
path = /
read only = no
guest ok = yes
~
~
~
```

```
smbcontrol winbind debuglevel
PID 26871: all:1 tdb:1 printdrivers:1 lanman:1 smb:1 rpc_parse:1 rpc_srv:1
 ↪rpc_cli:1 passdb:1 sam:1 auth:1 winbind:100 vfs:1 idmap:1 quota:1 acls:1
 ↪locking:1 msdfs:1 dmapi:1 registry:1 scavenger:1 dns:1 ldb:1 tevent:1 auth_
 ↪audit:1 auth_
json_audit:1 kerberos:1 drs_repl:1 smb2:1 smb2_credits:1 dsdb_audit:1 dsdb_
 ↪json_audit:1 dsdb_password_audit:1 dsdb_password_json_audit:1 dsdb_
 ↪transaction_audit:1 dsdb_transaction_json_audit:1 dsdb_group_audit:1 dsdb_
 ↪group_json_audit:1
```

2.25. Проблемы с конфигурационном файлом SSSD.conf

Проблема: не удается запустить SSSD.

Решение. SSSD требует, чтобы файл конфигурации был правильно настроен со всеми необходимыми записями, прежде чем демон запустится. Для запуска службы SSSD требуется по крайней мере один правильно настроенный домен. Без домена попытка запустить SSSD возвращает ошибку о том, что домены не настроены:

```
# sssd -d4 -i

[sssd] [ldb] (3): server_sort:Unable to register control with rootdse!
[sssd] [confdb_get_domains] (0): No domains configured, fatal error!
[sssd] [get_monitor_config] (0): No domains configured.
Необходимо отредактировать файл /etc/sssd/sssd.conf и создать хотя бы один
↪домен.
```

SSSD также требует наличия по крайней мере одного доступного поставщика услуг, прежде чем он запустится. Если проблема связана с конфигурацией поставщика услуг, сообщение об ошибке указывает на то, что службы не настроены:

```
[sssd] [get_monitor_config] (0): No services configured!
```

Необходимо отредактировать файл /etc/sssd/sssd.conf и настроить по крайней мере одного поставщика услуг.

Важно: SSSD требует, чтобы поставщики услуг были настроены в виде списка, разделенного запятыми, в одной записи служб в файле /etc/sssd/sssd.conf. Если службы перечислены в нескольких записях, SSSD распознает только последнюю запись.

SSSD также требует, чтобы для /etc/sssd/sssd.conf были правильно установлены права собственности и разрешения. Если владелец или разрешения установлены неправильно, попытка запустить SSSD возвращает эти сообщения об ошибках:

```
[sssd] [confdb_ldif_from_ini_file] (0x0020): Permission check on config file
↪failed.
[sssd] [confdb_init_db] (0x0020): Cannot convert INI to LDIF [1]: [Operation
↪not permitted]
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
[sssd] [confdb_setup] (0x0010): ConfDB initialization has failed [1]:
↪Operation not permitted
[sssd] [load_configuration] (0x0010): Unable to setup ConfDB [1]: Operation
↪not permitted
[sssd] [main] (0x0020): Cannot read config file /etc/sssd/sssd.conf. Please
↪check that the file is accessible only by the owner and owned by root.root.
```

Необходимо установить правильное имя владельца и разрешения для файла /etc/sssd/sssd.conf:

```
chmod 600 /etc/sssd/sssd.conf
chown root:root /etc/sssd/sssd.conf
```

2.26. Отсутствие групп при выполнении команды id

Проблема: нет групп при выполнении команды id username@FQDN_WindowsDomain или членов группы с getent group.

Решение. Проверить количество объектов в домене MS AD

```
# В Домене Active directory запустить Powershell и выполнить команду ниже
(Get-ADObject -Filter *).count
```

Проверить диапазоны идентификаторов пользователей домена MS AD:

```
# Для вывода списка доменных пользователей и их SID в домене Active
↪Directory запустить Powershell и выполнить команду ниже
Get-ADUser -Filter * -Property SID | Select-Object Name, SID
```

Если количество объектов или последняя часть SID некоторых доменных пользователей MS AD превышает 200 000 – выполнить расширение диапазона:

```
#Показать текущие диапазоны (idrange) для всех доменов
# Произвести аутентификацию
kinit admin
#Вывести список доступных диапозонов
ipa idrange-find
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
#Изменить id_range для домена windomain.lan к примеру до 500 000
ipa idrange-mod WINDOMAIN.LAN_id_range --range-size=500000
#Удаление всего кеша с контроллера домена и перезапуск службы sssd
rm -f /var/lib/sss/db/* /var/lib/sss/mc/* && systemctl restart sssd
```

2.27. Долгое выполнение команды id

Проблема: Выполнение команды id занимает много времини или прерывается по таймауту.

Решение. Одной из причин может быть большая вложенность групп

```
#Выполните команду id с параметром -G(вывести все ID групп)- эта каманда
 ↪игнорирует вложенность групп
id -G  winuser@windomain.lan

#Если команда отрабатывает быстро то требуется добавить в существующую
 ↪секцию в /etc/sssd/sssd.conf на каждом контроллере домена -игнорирование
 ↪вложенных групп
[domain/alddomain.lan]
...
ignore_group_members = true
subdomain_inherit = ignore_group_members

#Выполнить очистку кеша и произвести перезапуск службы sssd
rm -f /var/lib/sss/db/* /var/lib/sss/mc/* && systemctl restart sssd
```

2.28. SSSD не удается подключиться к MS AD из-за ошибок с GSS-API

Проблема: поставщик удостоверений MS AD правильно настроен в файле sssd.conf, но SSSD не удается подключиться к нему с ошибками GSS-API.

Решение. SSSD может подключаться только к поставщику MS AD, используя его имя хоста. Если имя хоста не указано, SSSD-клиент не может разрешить IP-адрес хоста, и аутентификация завершается неудачей.

Например, при такой конфигурации:

```
[domain/ADEXAMPLE]
debug_level = 0xFFF0
id_provider = ad
ad_server = 172.16.0.1
ad_domain = example.com
krb5_canonicalize = False
```

SSSD-клиент возвращает этот сбой GSSAPI, и запрос аутентификации завершается неудачей:

```
(Fri Jul 27 18:27:44 2012) [sssd[be[ADTEST]]] [sasl_bind_send] (0x0020): ldap_
 ↪sasl_bind failed (-2)[Local error]
(Fri Jul 27 18:27:44 2012) [sssd[be[ADTEST]]] [sasl_bind_send] (0x0080):
 ↪Extended failure message: [SASL(-1): generic failure: GSSAPI Error:
 ↪Unspecified GSS failure.  Minor code may provide more information (Cannot
 ↪determine realm for numeric host address)]
```

Чтобы избежать этой ошибки, необходимо установить для ad_server значение имени узла MS AD или использовать ключевое слово _srv_ для использования обнаружения службы DNS.

ALD Pro(FreeIPA) использует BIND в качестве интегрированного DNS-сервера. Если есть подозрения, что с DNS что-то не так, необходимо проверить журналы, сгенерированные BIND.

```
journalctl -u bind9-pkcs11.service
```

Если требуется создать tcp dump, необходимо воспользоваться командой:

```
tcpdump -i eth0 -w /home/${USER}/$(date +%Y-%m-%d_%H-%M)_$(hostname).pcap
```

№	Проблема	Решение

1	Не работает DNS resolving имен из новой подсети	Необходимо добавить новую подсеть в **trusted_network** на каждом контроллере домена ALD Pro (FreeIPA)
		/etc/bind/**ipa-ext.conf**
		Пример:
		`.....`
		`acl "trusted_network" {`
		`  localnets;`
		`  localhost;`
		`  192.168.88.0/24;`
		`  172.19.3.0/24;`
		`  172.19.4.0/24;`
		`  <НОВАЯ Подсеть>;`
		`};`

2	Не работают рекурсивные запросы	Необходимо включить дополнительные опции на каждом контроллере домена ALD Pro (FreeIPA)
		/etc/bind/**ipa-options-ext.conf**
		Пример:
		`allow-recursion { trusted_network; };`
		`allow-query-cache { trusted_network; };`

№	Проблема	Решение
	Ошибка 3221225485 при создании доверительных отношений: **ipa: ERROR: Ошибка обмена данными с сервером CIFS: код «3221225485», сообщение «An invalid parameter was passed to a service or function.» (оба значения могут быть «None»)**	Проверить, что параметры реестра /var/lib/samba/registry.tdb – существуют и не были удалены. Для проверки выполнить команду **net conf list**. Если вывод пустой или есть уверенность, что файл был поврежден, требуется повторно выполнить команду ipa-adtrust-instal, предварительно сделав копию файла конфигурацуии smb.conf **cp smb.conf{,_bkp}**, так как он будет перезаписан из шаблона.

2.29. Настройка игнорирования участников групп (ignore_group_members)

Извлечение информации о пользователях (id <username@<ADdomain>) и группах является трудоемкой операцией для демона служб системной безопасности (SSSD), особенно при развертывании ALD Pro с доверием к большому домену MS AD. Улучшить производительность можно, настроив, какую информацию и как долго SSSD извлекает из поставщиков удостоверений (identity providers).

2.29.1. Предварительное требование

Необходимы права root для редактирования конфигурационного файла **/etc/sssd/sssd.conf**.

2.29.2. Процедура

1. Открыть конфигурационный файл /etc/sssd/sssd.conf в текстовом редакторе.
2. Добавить следующие параметры в раздел [домен] для домена MS AD. Если доменного раздела для домена MS AD еще нет, необходимо создать его.

```
[domain/ald.example.com]
ignore_group_members = true
subdomain_inherit = ignore_group_members
...
```

3. Сохранить и закрыт файл /etc/sssd/sssd.conf на сервере.
4. Перезапустить службу SSSD, чтобы загрузить изменения конфигурации.

```
systemctl restart sssd
```

ignore_group_members

Наиболее трудоемкой операцией является загрузка групп, включая их участников. Обычно на начальном этапе важно, членом каких групп является пользователь (id aduser@ad_domain), а не какие участники входят в конкретные группы (getent group adgroup@ad_domain). При установке для параметра ignore_group_members значения **True**, все группы отображаются как пустые, таким образом загружается только информация о самих объектах группы, а не об их членах, что обеспечивает значительное повышение производительности. Важно обратить внимание, что идентификатор aduser@ad_domain все равно вернет все правильные группы.

subdomain_inherit_inherit

Вышеуказанные параметры могут быть переданы в конфигурацию доверенных доменов MS AD. На данный момент единственным поддерживаемым методом является использование опции subdomain_inherit в разделе домена sssd.conf. Имена любого из двух приведенных выше параметров могут быть указаны в качестве значения subdomain_inherit,

и они будут применяться как к основному домену (IPA), так и к поддомену MS AD.

2.30. Настройка таймаута конфигурации для плагина ipa-extdom на ALD Pro (FreeIPA)-серверах

Клиенты ALD Pro не могут напрямую получать информацию о пользователях и группах из MS AD, поэтому серверы ALD Pro используют плагин **ipa-extdom** для получения информации о пользователях и группах MS AD, и эта информация пересылается запрашивающему клиенту.

Плагин **ipa-extdom** отправляет запрос в SSSD на получение данных о пользователях MS AD. Если информации нет в кэше SSSD, SSSD запрашивает данные у контроллера домена MS AD (DC). Можно настроить значение таймаута конфигурации, которое определяет, как долго подключаемый модуль **ipa-extdom** ожидает ответа от **SSSD**, прежде чем подключаемый модуль отменит соединение и вернет вызывающей стороне сообщение об ошибке таймаута. Значение по умолчанию равно 10000 миллисекунд (10 секунд).

В следующем примере время ожидания настройки устанавливается равным 20 секундам (20000 миллисекунд).

2.30.1. Предупреждение

Необходимо соблюдать осторожность при настройке таймаута конфигурации:

Если задается слишком малое значение, например 500 миллисекунд, у **SSSD может не хватить времени для ответа**, и запросы всегда будут возвращать таймаут.

Если задается слишком большое значение, например 30000 миллисекунд (30 секунд), **один запрос может заблокировать подключение к SSSD на этот промежуток времени**. Поскольку **только один поток может подключаться к SSSD одновременно**, все остальные запросы от подключаемого модуля должны ждать.

Если ALD Pro-клиенты отправляют много запросов, они могут заблокировать все доступные рабочие процессы, настроенные для сервера каталогов на ALD Pro-сервере. Как следствие, сервер может быть не в состоянии ответить на какой-либо запрос в течение некоторого времени.

Изменять время ожидания конфигурации рекомендуется только в следующих

ситуациях:

- Если клиенты ALD Pro при запросе информации о пользователях и группах Ms AD часто получают ошибки таймаута до истечения их собственного таймаута поиска. Значение таймаута конфигурации слишком мало.
- Если сервер каталогов на ALD Pro-сервере часто блокируется, а утилита **pstack** сообщает, что многие или все рабочие потоки в это время обрабатывают запросы **ipa-extdom**. Значение слишком велико.

2.30.2. Предварительное требование.

Пароль менеджера каталогов LDAP (LDAP Directory Manager password)

2.30.3. Процедура

Используется следующая команда, чтобы настроить время ожидания настройки на 20000 миллисекунд:

```
# ldapmodify -D "cn=directory manager" -W dn: cn=ipa_extdom_extop,cn=plugins,
 ↪cn=config changetype: modify replace: ipaExtdomMaxNssTimeout
 ↪ipaExtdomMaxNssTimeout: 20000
```

2.31. Настройка максимального размера буфера для плагина ipa-extdom на ALD Pro-серверах

Клиенты ALD Pro не могут напрямую получать информацию о пользователях и группах из MS AD, поэтому серверы IdM используют плагин ipa-extdom для получения информации о пользователях и группах MS AD, и эта информация пересылается запрашивающему клиенту.

Можно настроить максимальный размер буфера для плагина ipa-extdom, который регулирует размер буфера, в котором SSSD может хранить полученные данные. Если буфер слишком мал, SSSD возвращает ошибку ERANGE, и подключаемый модуль повторяет запрос с буфером большего размера. Размер буфера по умолчанию составляет 134217728 байт (128 МБ).

В следующем примере максимальный размер буфера устанавливается равным 256 МБ (268435456 байт).

2.31.1. Предварительное требование.

Пароль менеджера каталогов LDAP (LDAP Directory Manager password)

2.31.2. Процедура

Используется следующая команда, чтобы установить максимальный размер буфера равным 268435456 байтам:

```
# ldapmodify -D "cn=directory manager" -W dn: cn=ipa_extdom_extop,cn=plugins,
 ↪cn=config changetype: modify replace: ipaExtdomMaxNssBufSize
 ↪ipaExtdomMaxNssBufSize: 268435456
```

2.32. Настройка максимального количества экземпляров для плагина ipa-extdom на ALD Pro-серверах

Поскольку клиенты ALD Pro не могут напрямую получать информацию о пользователях и группах из MS AD, серверы ALD Pro используют плагин **ipa-extdom** для получения информации о пользователях и группах MS AD, а затем пересылают эту информацию запрашивающему клиенту.

По умолчанию плагин **ipa-extdom** настроен на использование до **80%** рабочих потоков LDAP для обработки запросов от ALD Pro-клиентов. Если служба SSSD на ALD Pro-клиенте запросила большой объем информации о пользователях и группах **AD trust**, эта операция **может остановить службу LDAP**, если она использует большинство потоков LDAP. Если данная проблема возникла, можно увидеть аналогичные ошибки в файле журнала SSSD для домена MS AD, **/var/log/sssd/sssd__your-ad-domain-name.com_.log**:

```
(2022-05-22  5:00:13): [be[ad.example.com]] [ipa_s2n_get_user_done]
 ↪(0x0040): s2n exop request failed.
(2022-05-22  5:00:13): [be[ad.example.com]] [ipa_s2n_get_user_done]
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
↪(0x0040): s2n exop request failed.
(2022-05-22  5:00:13): [be[ad.example.com]] [ipa_s2n_exop_done] (0x0040):
↪ldap_extended_operation result: Server is busy(51), Too many extdom
↪instances running.
```

Можно настроить максимальное количество экземпляров ipa-extdom, установив значение для параметра ipaExtdomMaxInstances, которое должно быть целым числом больше 0 и меньше общего числа рабочих потоков.

2.32.1. Предварительное требование.

Пароль менеджера каталогов LDAP (LDAP Directory Manager password)

2.32.2. Процедура

1. Извлечь общее количество рабочих потоков.

```
# ldapsearch -xLLLD cn=directory\ manager -W -b cn=config -s base nsslapd-
↪threadnumber
Enter LDAP Password:
dn: cn=config
nsslapd-threadnumber: 16
```

Это означает, что текущее значение для ipaExtdomMaxInstances равно 13.

2. Отрегулировать максимальное количество экземпляров. В этом примере значение изменяется на 14:

```
# ldapmodify -D "cn=directory manager" -W
dn: cn=ipa_extdom_extop,cn=plugins,cn=config
changetype: modify
replace: ipaExtdomMaxInstances
ipaExtdomMaxInstances: 14
```

3. Следить за производительностью сервера каталогов ALD Pro и, если она не улучшится, повторить эту процедуру и отрегулировать значение переменной ipaExtdomMaxInstances.

2.33. Настройка SSSD в ALD Pro-клиентах для крупных доверительных развертываний IdM-AD

Эта процедура применяет параметры настройки к конфигурации службы SSSD в ALD Pro-клиенте, чтобы увеличить время отклика при получении информации из большой среды MS AD.

2.33.1. Предварительное требование.

Нужны права **root** для редактирования конфигурационного файла **/etc/sssd/sssd.conf**.

2.33.2. Процедура

1. Определить, сколько секунд занимает один незакешированный вход в систему.

a) Очистить кэш SSD на ALD Pro-клиенте client.example.com

Требуется предварительная установка **apt install sssd-tools**

```
[root@client ~]# sss_cache -E
```

b) Измерить сколько времени требуется для входа в систему в качестве пользователя MS AD с помощью команды time. В этом примере из клиента ALD Pro client.example.com войnb на тот же хост, что и пользователь ad-user из **ad**.example.com AD Domain

```
[root@client ~]# time ssh ad-user@ad.example.com@client.example.com
```

Ввести пароль как можно скорее.

```
Password:
Last login: Sat Jan 23 06:29:54 2021 from 10.0.2.15
[ad-user@ad.example.com@client ~]$
```

c) Выйти из системы как можно скорее, чтобы отобразить прошедшее время. В этом примере один некэшированный вход в систему занимает около 9 секунд.

```
[ad-user@ad.example.com@client /]$ exit
logout
Connection to client.example.com closed.

real 0m8.755s
user    0m0.017s
sys     0m0.013s
```

2. Открыть конфигурационный файл /etc/sssd/sssd.conf в текстовом редакторе.

3. Добавить следующие параметры в раздел [домен] для домена MS AD. Установить параметры pam_id_timeout и krb5_auth_timeout на количество секунд, которое занимает некэшированная логика. Если доменного раздела для домена MS AD еще нет, создать его.

```
[domain/example.com/ad.example.com]
krb5_auth_timeout = 9
ldap_deref_threshold = 0
...
```

4. Добавить следующую опцию в раздел [pam]:

```
[pam]
pam_id_timeout = 9
```

5. Сохранить и закрыть файл **/etc/sssd/sssd.conf** на сервере.

6. Перезапустить службу SSSD, чтобы загрузить изменения конфигурации.

```
systemctl restart sssd
```

2.34. Монтирование кэша SSSD в tmpfs

Демон служб системной безопасности (SSSD) постоянно записывает объекты LDAP в свой кэш. Эти внутренние транзакции SSSD записывают данные на диск, что намного медленнее, чем чтение и запись из оперативной памяти (RAM).

Чтобы повысить производительность, необходимо смонтировать кэш SSSD в оперативной памяти.

Кэшированная информация не сохраняется после перезагрузки, если кэш SSSD находится в оперативной памяти.

Это изменение безопасно выполнять на серверах ALD Pro, поскольку экземпляр SSSD на сервере ALD Pro не может потерять соединение с сервером каталогов на том же хосте.

Если выполнить эту настройку на ALD Pro-клиенте, и он потеряет подключение к серверам ALD Pro, пользователи не смогут пройти проверку подлинности после перезагрузки, пока не будет восстановлено подключение.

2.34.1. Предварительное требование.

Нужны права root для редактирования файла конфигурации **/etc/fstab**.

2.34.2. Процедура

Довольно много времени, затрачиваемого на обработку запроса, уходит на запись объектов LDAP в кэш. Поскольку кэш поддерживает полные свойства ACID, он выполняет синхронизацию диска с каждой внутренней транзакцией SSSD, что приводит к записи данных на диск. С положительной стороны, это гарантирует, что кэш всегда доступен в случае сбоя сети и будет доступен для использования после сбоя компьютера, но, с другой стороны, запись данных требует времени. Можно смонтировать кэш на **ramdisk**, сократив затраты на ввод-вывод с диска, добавив в **/etc/fstab** в виде одной строки следующее:

```
tmpfs /var/lib/sss/db/ tmpfs size=300M,mode=0700,rootcontext=system_u:object_
↪r:sssd_var_lib_t:s0 0 0
```

Затем необходимо подключить каталог и перезапустить sssd после этого:

```
mount /var/lib/sss/db/

systemctl restart sssd
```

Важно настроить параметр размера в соответствии с требуемым IPA и размером каталога объявлений. Как правило, можно использовать **100 Мб на 10000 записей LDAP**.

Выполнение этого изменения на ALD-сервере немного безопаснее, чем на ALD-клиентах, поскольку экземпляр SSSD на сервере никогда не потеряет подключение к ALD-серверу, поэтому кэш всегда можно перестроить. Но в случае, если кэш был потерян после перезагрузки, и MS AD был недоступен из-за сетевой ошибки или аналогичного состояния, узел не смог бы вернуться к кэшированным данным о MS AD пользователях.

Плюсы: Операции ввода-вывода в кэше выполняются намного быстрее.

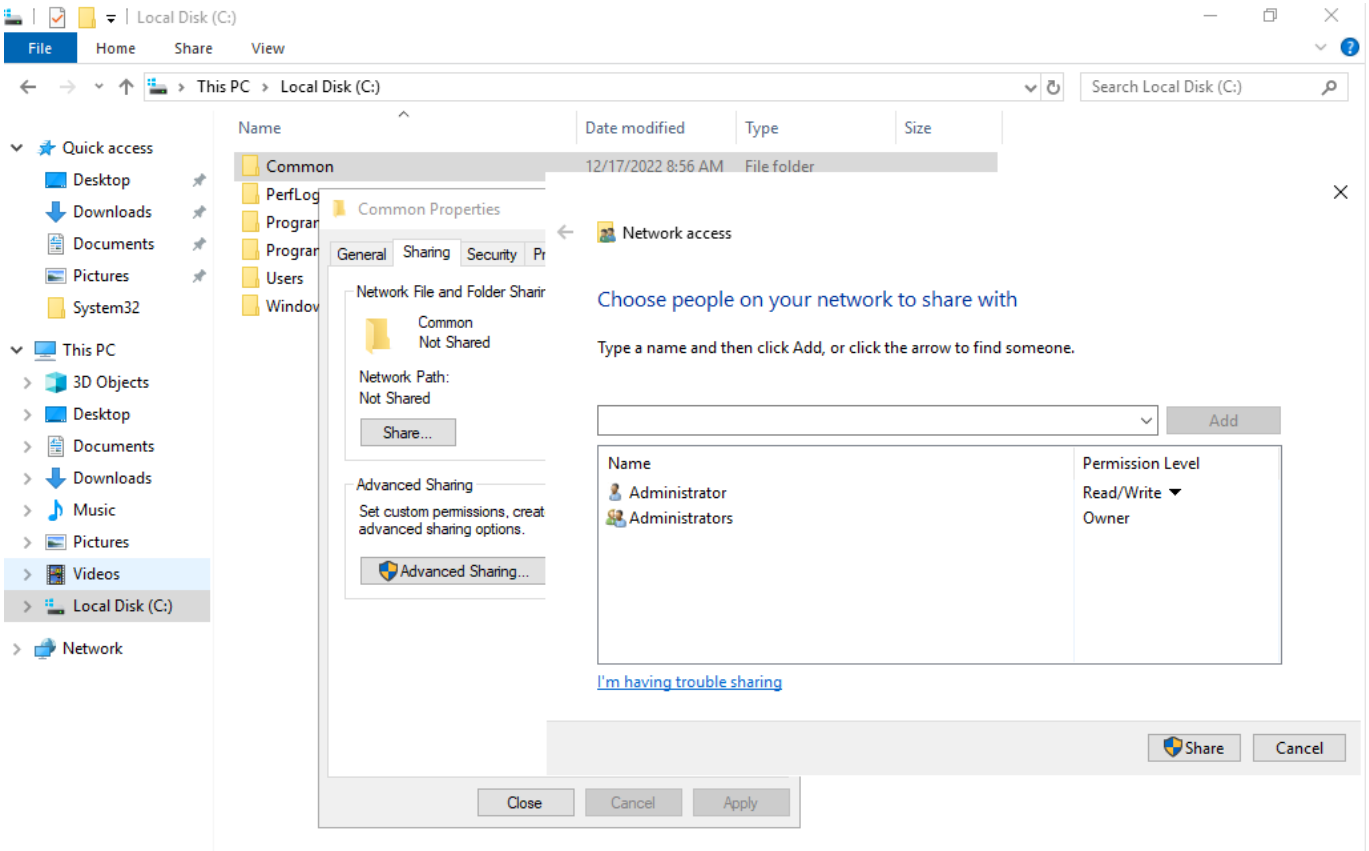
Минусы: Кэш не сохраняется при перезагрузках. Это означает, что кэш должен быть восстановлен после перезагрузки компьютера, но также и то, что cachedpassword теряются после перезагрузки.

2.34.2.1. Доступ пользователей ALD Pro к ресурсам MS AD

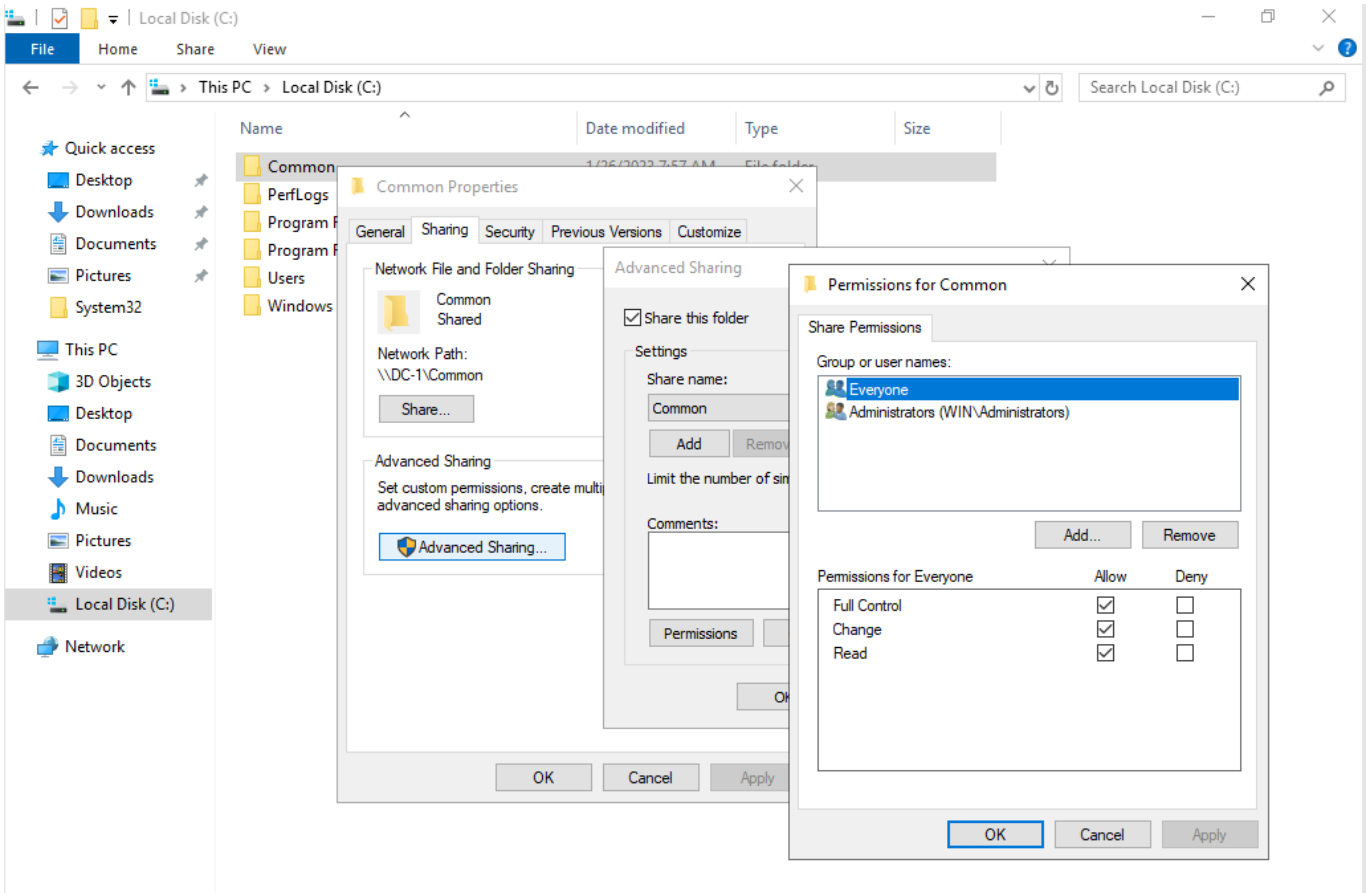
2.35. Создание сетевой папки в домене MS AD

Контроллер домена не рекомендуется использовать для создания общих сетевых ресурсов. Он используется в примере для упрощения процесса.

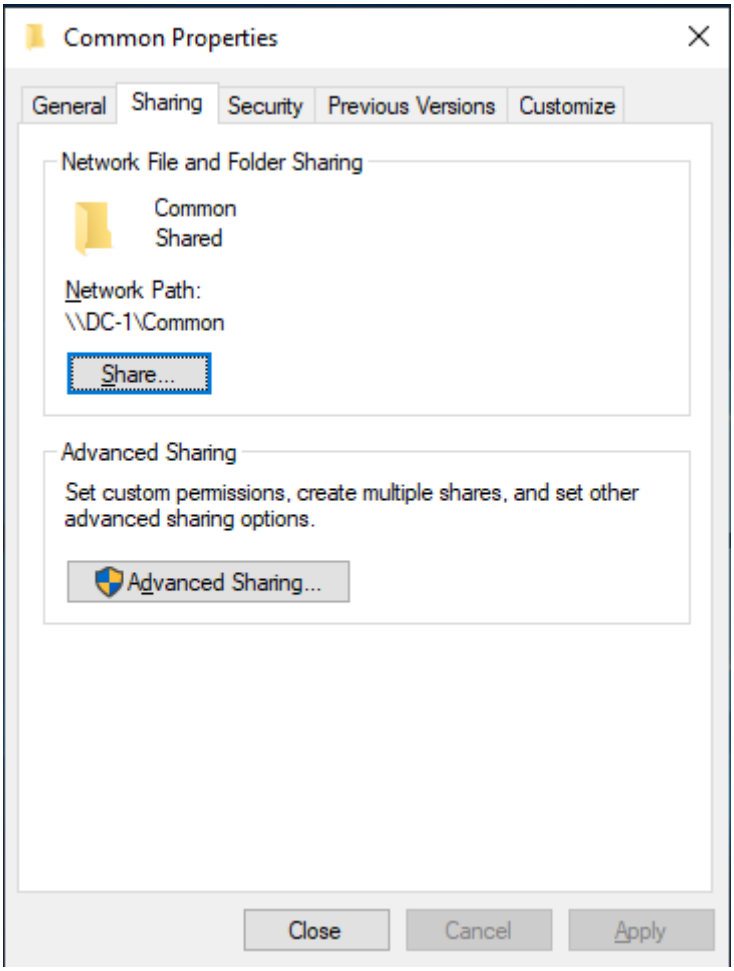
Создать папку C:Common, в свойствах на закладке «Sharing» выбрать «Share» и в окне «Network access» выбрать «Share», оставив все по умолчанию.

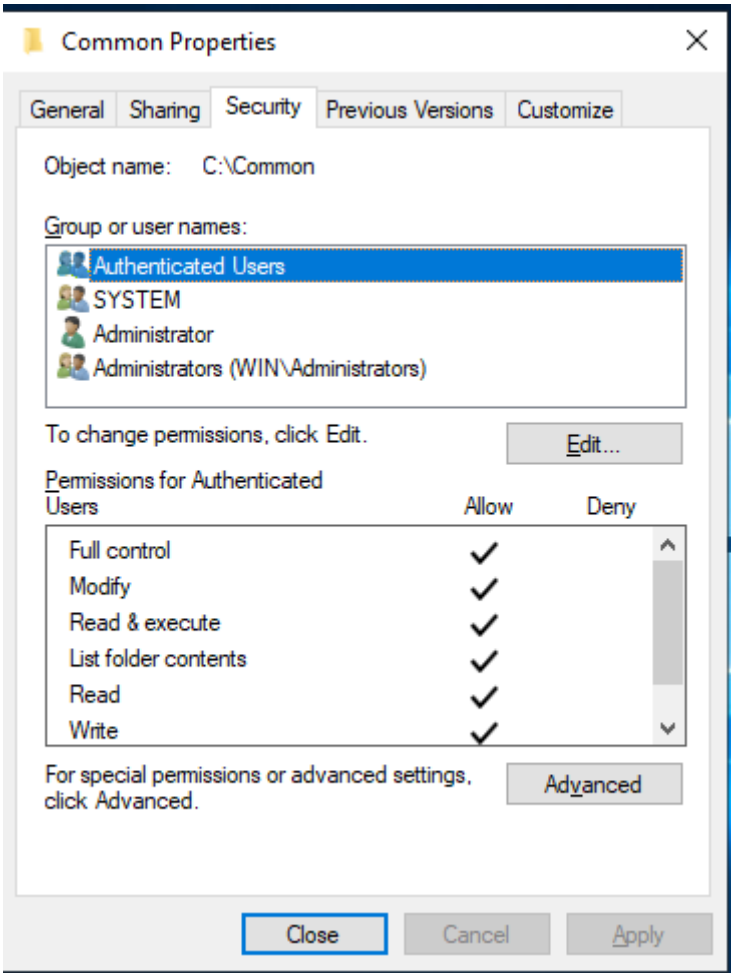


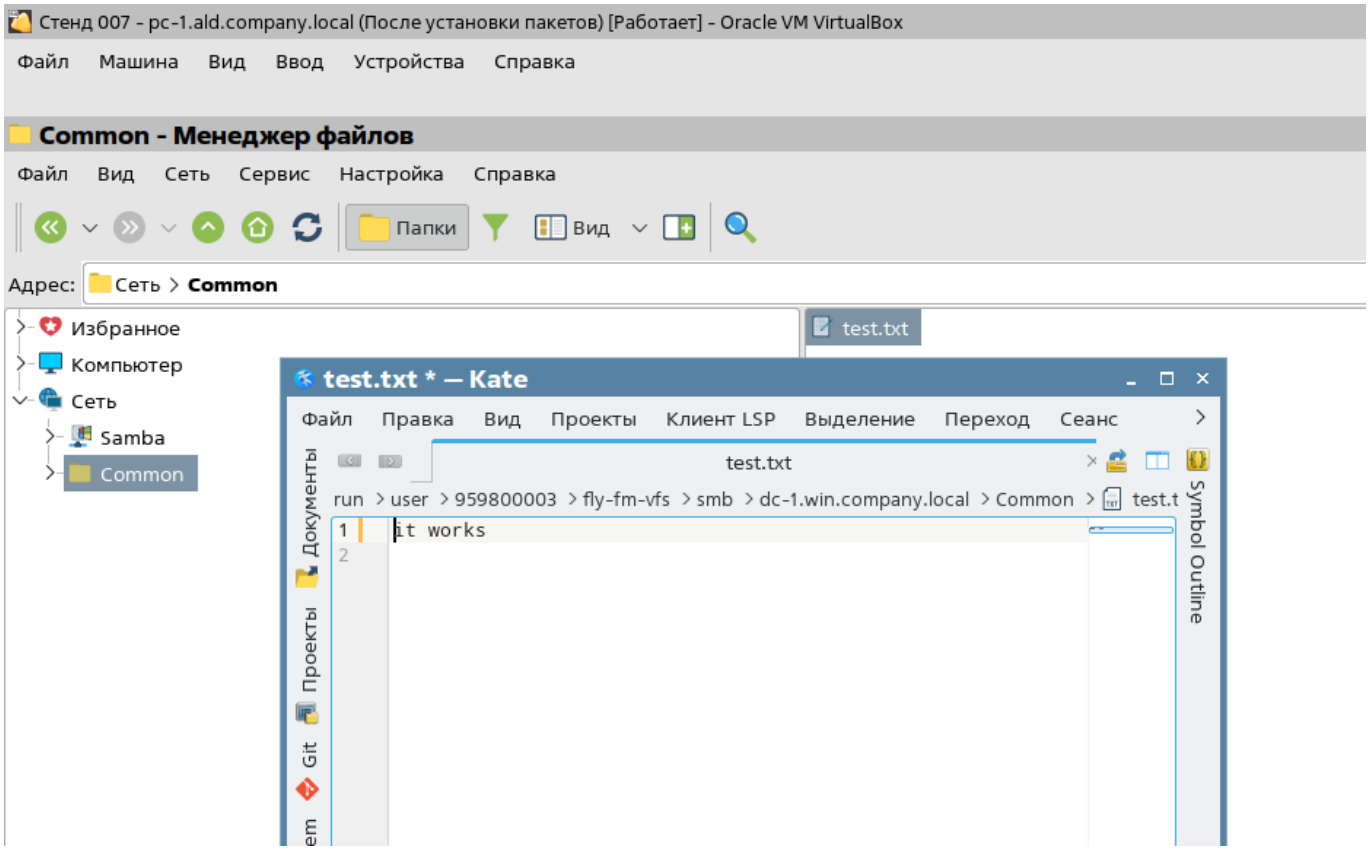
Если открыть окно «Common PropertiesSharingAdvanced SettingsPermissions», то будет видно, что по умолчанию на уровне SMB все пользователи имеют полные права.



Но доступ к файлам регулируется также на уровне NTFS разрешений, которые настраиваются на вкладке «Common PropertiesSecurity». Можно предоставить доступ к общей папке всем аутентифицированным пользователям, и это позволит пользователям ALD Pro редактировать файлы в папке, доказывая работу доверительных отношений в направлении MS → ALD.




Common Properties
General
Sharing
Security
Previous Versions
Customize
Object name: C:\Common
Group or user names:
Authenticated Users
SYSTEM
Administrator
Administrators (WIN\Administrators)
To change permissions, click Edit.
Edit...
Permissions for Authenticated Users
Allow
Deny
Full control
Modify
Read & execute
List folder contents
Read
Write
For special permissions or advanced settings, click Advanced.
Advanced
Close
Cancel
Apply


Стенд 007 - pc-1.ald.company.local (После установки пакетов) [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
Common - Менеджер файлов
Файл Вид Сеть Сервис Настройка Справка
Папки
Вид
Адрес: Сеть > Common
Избранное
Компьютер
Сеть
Samba
Common
test.txt
test.txt * — Kate
Файл Правка Вид Проекты Клиент LSP Выделение Переход Сеанс
test.txt
run > user > 959800003 > fly-fm-vfs > smb > dc-1.win.company.local > Common > test.t
1 it works
2
Документы
Проекты
Git
Symbol Outline

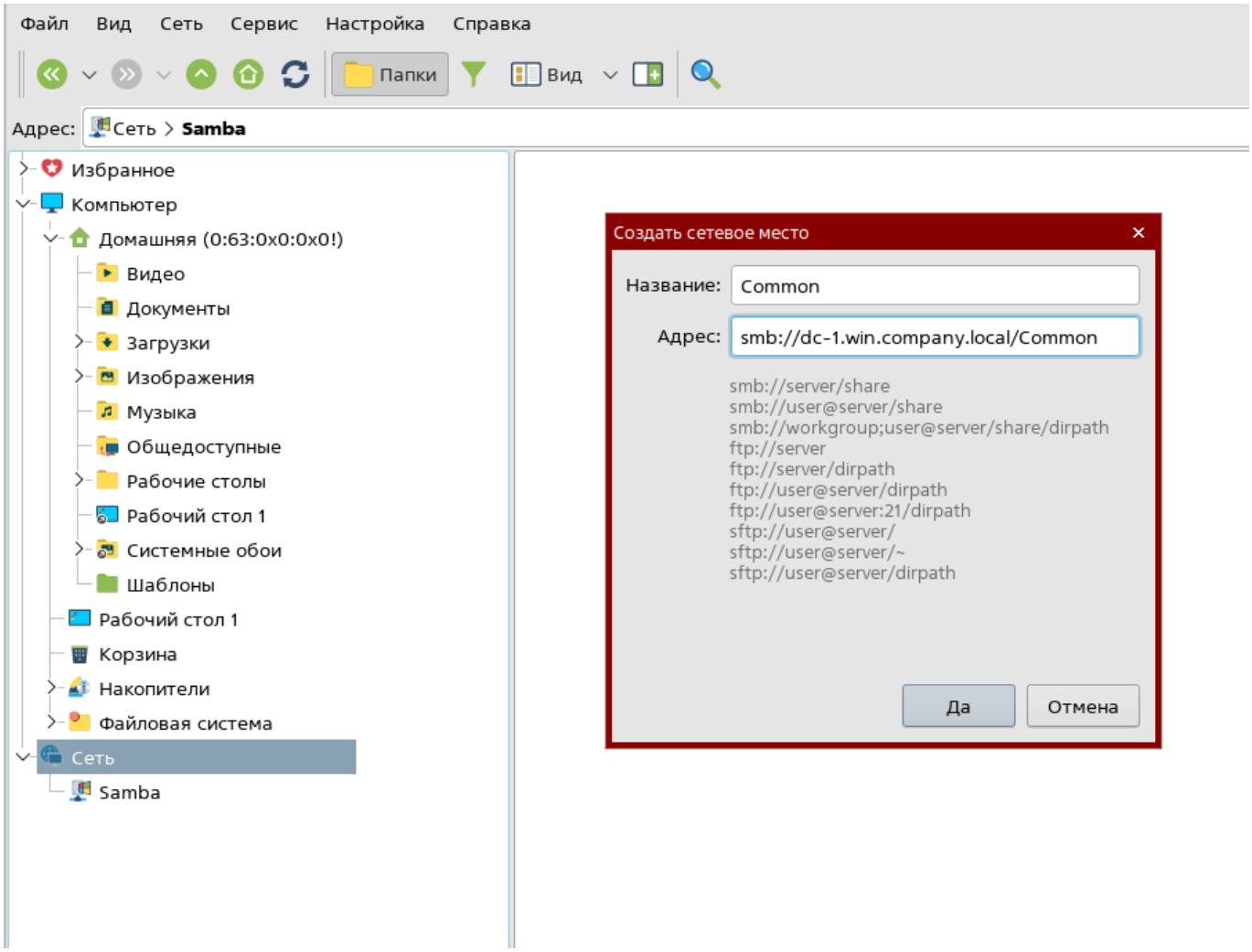
2.36. Подключение сетевой папки на рабочей станции под управлением Astra Linux

Для подключения сетевой папки из домена MS AD в Astra Linux необходимо открыть проводник, кликнуть правой кнопкой мыши по узлу «Сеть» и выбрать команду «Новое место». Задать следующие параметры подключения:

В примере Windows Domain Controller именуется как **dc-1**.win.company.local

- Название: Common (любое)
- Адрес: smb://dc-1.win.company.local/Common

формат протокол://имя_сервера/название_общей_папки



Для того, чтобы при подключении сетевого ресурса аутентификация прошла прозрачно по протоколу Kerberos, на стороне Astra Linux нужно отключить SPAKE и FAST. Метод предварительной аутентификации SPAKE был добавлен в MIT Kerberos с версии 1.17 и

использует методы криптографии с открытым ключом для защиты от атак по словарю паролей (password dictionary attacks), что не поддерживается со стороны MS AD.

На стороне клиента Astra Linux, с которого выполняется подключение к диску MS, в файле /etc/sssd/sssd.conf нужно добавить параметр krb5_use_fast = never

```
[domain/ald.company.local]
...
krb5_use_fast = never
```

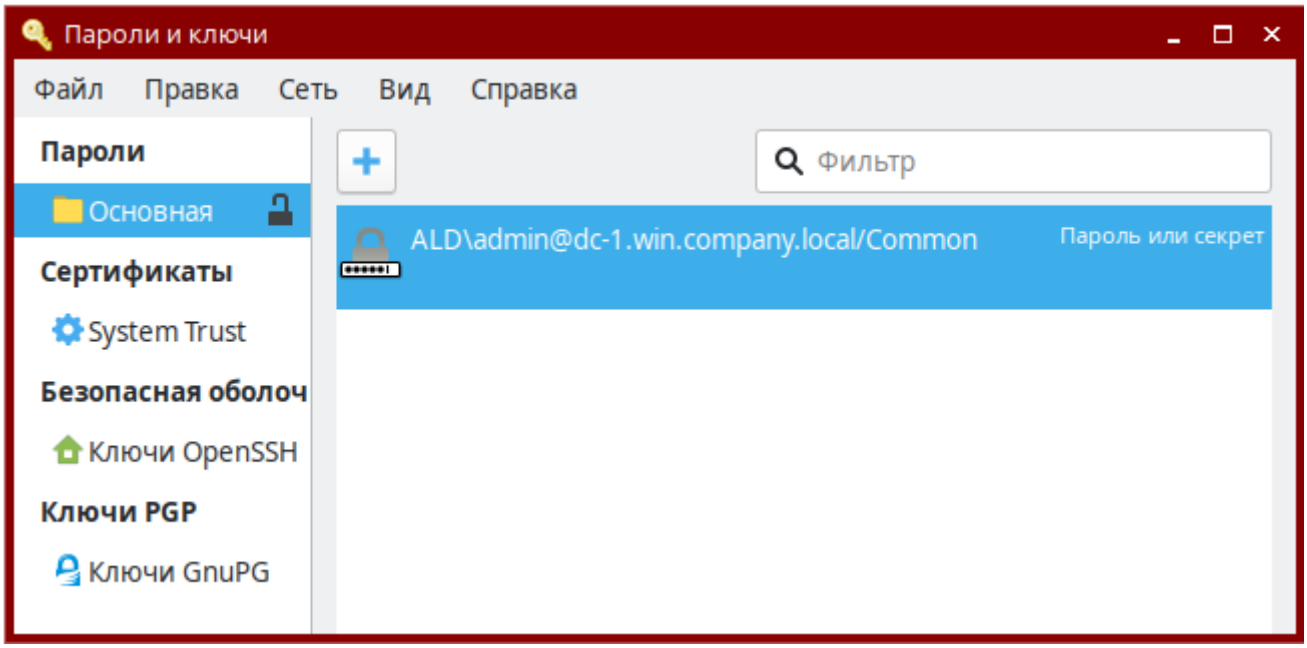
После этих действий нужно перезагрузить контроллер и клиентский компьютер ALD Pro и обязательно проверить, что время на контроллерах MS AD и ALD Pro синхронизировано, т. к. для работы протокола Kerberos нужно, чтобы время всех участниках расходилось не более, чем на 5 минут.

Если FAST/SPAKE не выключить, то при монтировании сетевой папки файловый менеджер не сможет пройти аутентификацию по билету Kerberos и запросит учетные данные, чтобы попробовать аутентификацию по NTLM. Если нет необходимости настраивать прозрачную аутентификацию, то можно указать имя пользователя в формате:

```
#имя пользователя
ALD\admin
#в формате
ДОМЕН\имя_пользователя
```

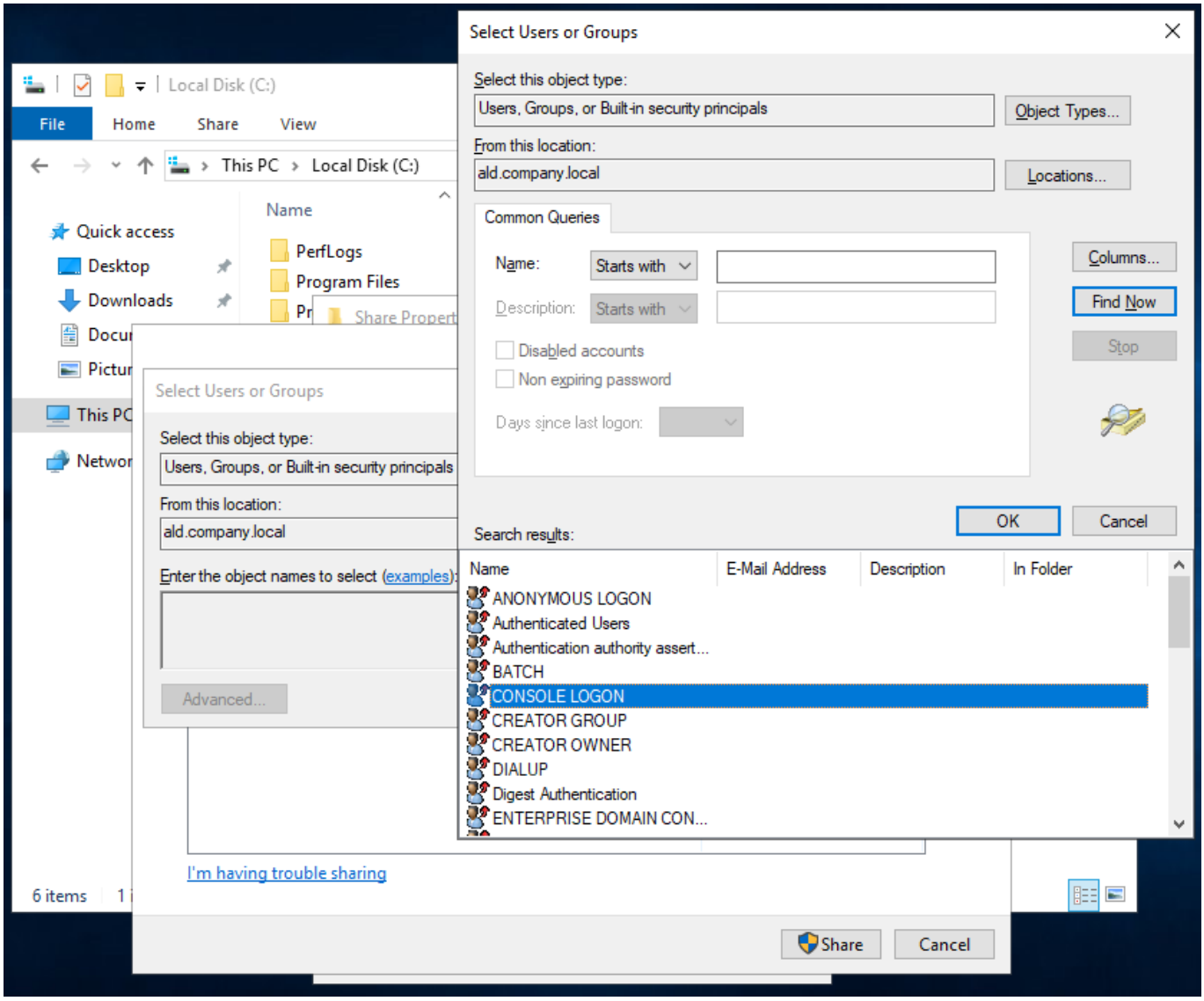
Система предложит сохранить учетные данные в связке ключей, для работы с которой можно воспользоваться приложением seahorse «Пароли и ключи»

```
# apt-get install seahorse
# seahorse
```



2.36.1. Ограничение доступа по SID

Сценарий, когда доступ к сетевому ресурсу предоставляется всем пользователям домена, является крайне редким. На практике обычно требуется предоставить доступ только строго ограниченной группе пользователей. Если воспользоваться окном «Select Users or Groups», можно обнаружить, что объекты доверенного домена ALD Pro найти не удается.



Стандартный механизм поиска объектов из доверенного домена работает через глобальный каталог, которого в обычной FreeIPA нет. Глобальный каталог — это еще один LDAP-каталог, который должен быть доступен на порту 3268 и предоставлять данные обо всех объектах леса в определенной схеме данных. Не имея этой службы на стороне FreeIPA, доступ конкретным пользователям можно предоставить только по SID через PowerShell.

Посмотреть SID пользователя ALD Pro можно с помощью утилиты wbinfo на ALD Pro контроллере домена:

Используя wbinfo

```
root@aldpro01:~# wbinfo -n 'ald\admin'
S-1-5-21-896088827-1417987318-1335504985-500 SID_USER (1)
```

Используя ipa command

```
root@ald01:~# ipa user-show admin --all | grep ipantsecurityidentifier
ipantsecurityidentifier: S-1-5-21-896088827-1417987318-1335504985-500
```

Назначить права доступа можно командой ICACLS (Integrity Control Access Control List)

Наиболее популярные разрешения:

r = чтение

rx = Чтение, Выполнение, Список содержимого папки

rxm = Чтение, Выполнение, Список содержимого папки, Запись, Изменение

f = Полный доступ

(OI) = Для этой папки и её файлов

(CI) = Для этой папки и её подпапок

Таким образом, чтобы дать обычные права на чтение и запись на папку, используются разрешения (OI)(CI)rxm. Тогда команда будет выглядеть так:

```
PS C:\Users\Administrator> ICACLS "C:\Temp" /grant "*S-1-5-21-896088827-
↪1417987318-1335504985-500:(OI)(CI)rxm"
```

После добавления объектов в ACL, в стандартном окне безопасности они будут отображаться даже не по своим SID, а по привычным именам, т. к. для разрешения имен глобальный каталог не требуется.

Для упрощения администрирования в MS AD можно создать вспомогательные группы. Например, для администраторов ALD Pro в MS AD создается группа «WINALD_Pro_Administrators», в эту группу добавляются SID группы «ALDAdmins» из доверенного домена ALD Pro. Далее при назначении прав доступа на общий сетевой ресурс можно будет использовать группу «WINALD_Pro_Administrators».

2.37. Добавление пользователей и групп из ALD Pro домена в домен MS AD.

Процесс добавления пользователей из одного домена в другой осуществляется через доверительные отношения между доменами. По умолчанию в доверенных доменах MS AD используется Global Catalog для поиска пользователя или группы, однако ALD Pro версии ниже 2.0.0 по умолчанию не имеет глобальный каталог, по этой причине для добавления пользователя или группы из домена без глобального каталога в домен MS AD с глобальным каталогом, используется PowerShell скрипт.

При добавлении пользователя или группы в домене MS AD будет создан специальный объект Foreign Security Principal.

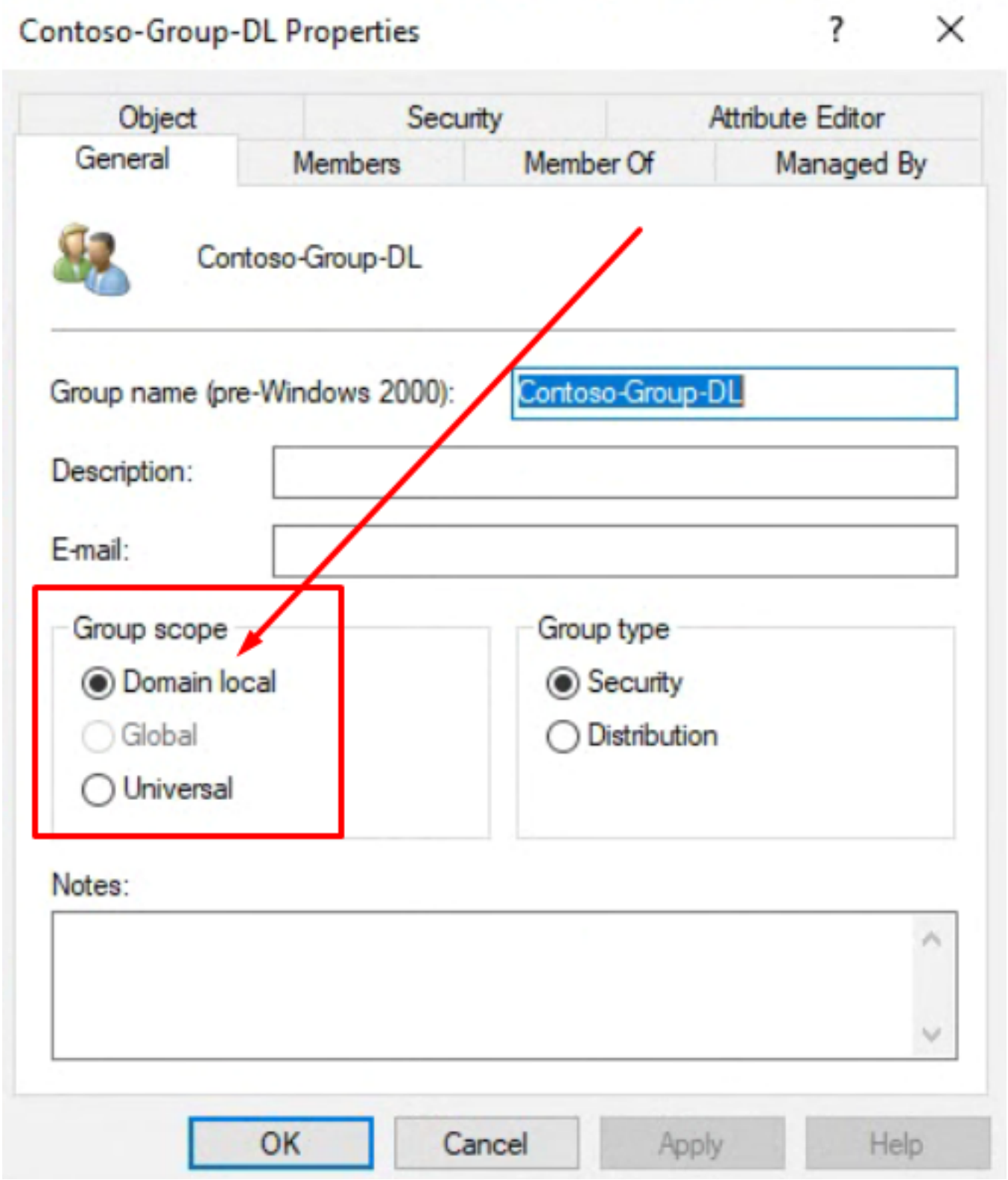
https://social.technet.microsoft.com/wiki/contents/articles/51367.active-directory-foreign-security-principals-and-special-identities.aspx#:~:text=A%20Foreign%20Security%20Principal%20(FSP,security%20groups%20and%20granted%20permissions.

2.37.1. Порядок добавления пользователя или группы

1. Посмотреть SID пользователя ALD Pro можно с помощью утилиты ldapsearch:

```
root@aldpro01:~# wbinfo -n 'ald\elena.kuznetsova'
S-1-5-21-1784717832-1844364183-3442789864-1013 SID_USER (1)
```

2. На стороне MS AD необходимо создать Domain Local группу, куда можно добавит SID из домена ALD Pro



3. На стороне MS AD на контроллере домена необходимо запустить скрипт

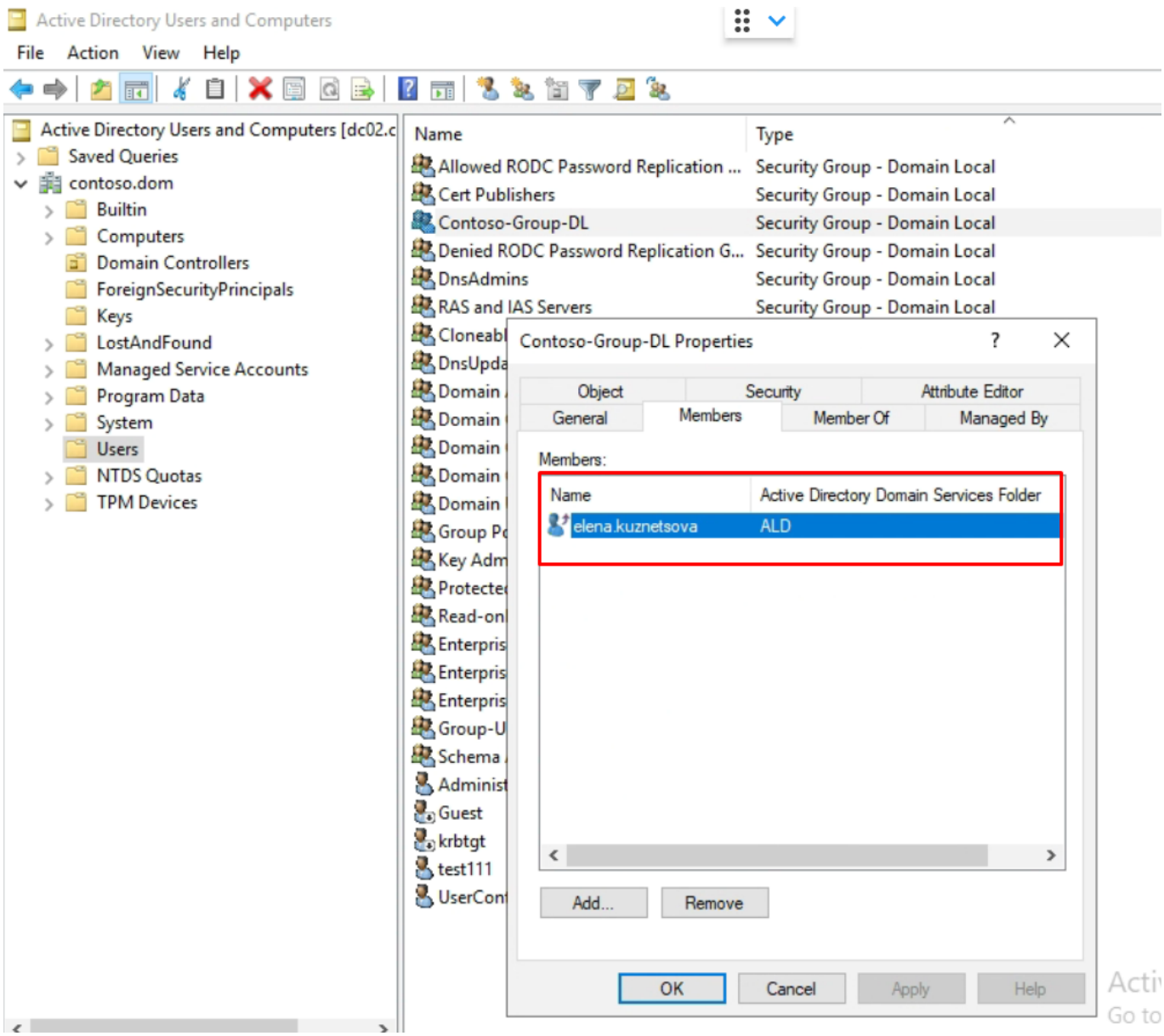
<S-1-5-21-1784717832-1844364183-3442789864-1013>– SID пользователя или группы

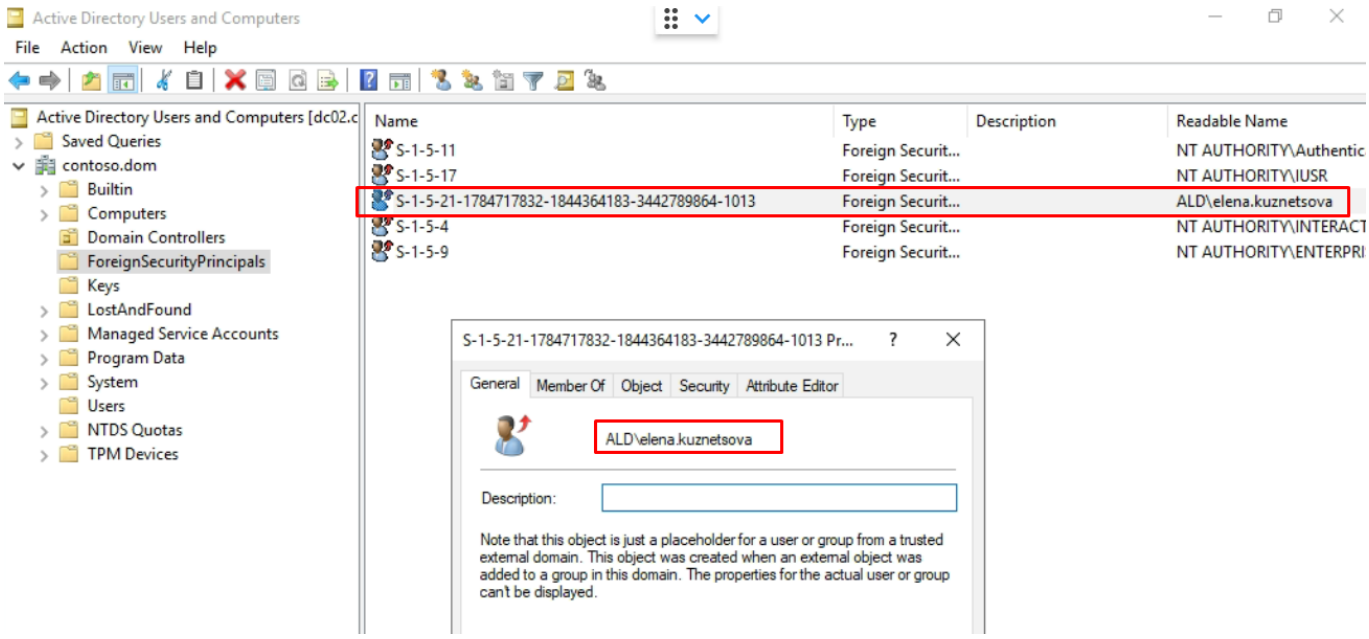
<CN=Contoso-Group-DL,CN=Users,DC=contoso,DC=dom >- Distinguished Name группы

```
#SID Из леса ALD_Pro(Пользователь или группа)
$AldSid = 'S-1-5-21-1784717832-1844364183-3442789864-1013'

#Domain Local Group из леса Active Directory
$DomainLocalGroupDN = 'CN=Contoso-Group-DL,CN=Users,DC=contoso,DC=dom'

#Создание нового Directory Entry
$group = New-Object DirectoryServices.DirectoryEntry("LDAP://$(
 ↪$DomainLocalGroupDN)")

#Добавление AldSid в DomainLocal группу
[void]$group.member.Add("<SID=$AldSid>")
$group.CommitChanges()
$group.Close()
```

После выполнения скрипта пользователь будет добавлен в группу и соответствующий объект Foreign Security Principal будет создан автоматически.

Теперь можно назначить Domain Local группу, к примеру, на файловые ресурсы, и все пользователи или группы внутри нее будут иметь доступ к ресурсу в домене MS AD.


Active Directory Users and Computers
File Action View Help
Active Directory Users and Computers [dc02.c
Saved Queries
contoso.dom
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Keys
LostAndFound
Managed Service Accounts
Program Data
System
Users
NTDS Quotas
TPM Devices
Name
Type
Allowed RODC Password Replication ...
Security Group - Domain Local
Cert Publishers
Security Group - Domain Local
Contoso-Group-DL
Security Group - Domain Local
Denied RODC Password Replication G...
Security Group - Domain Local
DnsAdmins
Security Group - Domain Local
RAS and IAS Servers
Security Group - Domain Local
Contoso-Group-DL Properties
Object
Security
Attribute Editor
General
Members
Member Of
Managed By
Members:
Name
Active Directory Domain Services Folder
elena.kuznetsova
ALD
Add...
Remove
OK
Cancel
Apply
Help


Active Directory Users and Computers
File Action View Help
Active Directory Users and Computers [dc02.c
Saved Queries
contoso.dom
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Keys
LostAndFound
Managed Service Accounts
Program Data
System
Users
NTDS Quotas
TPM Devices
Name
Type
Description
Readable Name
S-1-5-11
Foreign Securit...
NT AUTHORITY\Authentic
S-1-5-17
Foreign Securit...
NT AUTHORITY\IUSR
S-1-5-21-1784717832-1844364183-3442789864-1013
Foreign Securit...
ALD\elena.kuznetsova
S-1-5-4
Foreign Securit...
NT AUTHORITY\INTERACT
S-1-5-9
Foreign Securit...
NT AUTHORITY\ENTERPRI
S-1-5-21-1784717832-1844364183-3442789864-1013 Pr...
General
Member Of
Object
Security
Attribute Editor
ALD\elena.kuznetsova
Description:
Note that this object is just a placeholder for a user or group from a trusted external domain. This object was created when an external object was added to a group in this domain. The properties for the actual user or group can't be displayed.

2.37.1.1. Доступ пользователей MS Windows к ресурсам ALD Pro

Доступ к ресурсам ALD Pro пользователям из доверенного домена MS AD предоставляется через внешние группы.

На стороне ALD Pro пользователям из доверенного домена MS AD предоставляется доступ к ресурсам через внешние группы.

```
# ipa group-add 'ad_administrators_external' --desc='Внешняя группа
↪администраторов из MS AD' --external
# ipa -n group-add-member 'ad_administrators_external' --external 'WIN.
↪COMPANY.LOCAL\Domain Admins'
```

Внешние группы не имеют gid (являются не POSIX-группами), поэтому их нельзя использовать напрямую для предоставления доступа к сетевым файлам. Следует создать еще одну обычную POSIX-группу и включить в нее группу ad_administrators.

Важно отметить, что добавление двустороннего доверия возможно в обычной инсталляции FreeIPA, даже не имея поддержки глобального каталога.

2.37.1.2. Установка глобального каталога(в ALD Pro 2.0.0)

Склонировать репозиторий:

```
# git clone --branch AD-39377-mvp1 https://git.astralinux.ru/scm/ad/aldpro-
↪backend-global-catalog.git /opt/gc/
```

где

- git clone — команда для клонирования репозитория
- AD-39377-mvp1 — имя ветки, в которой содержатся необходимые исходные коды
- https://git.astralinux.ru/… - адрес репозитория с кодом глобального каталога
- /opt/gc/ - имя папки, в которую нужно клонировать репозиторий

Запустить скрипт, который выполнит настройку глобального каталога в системе:

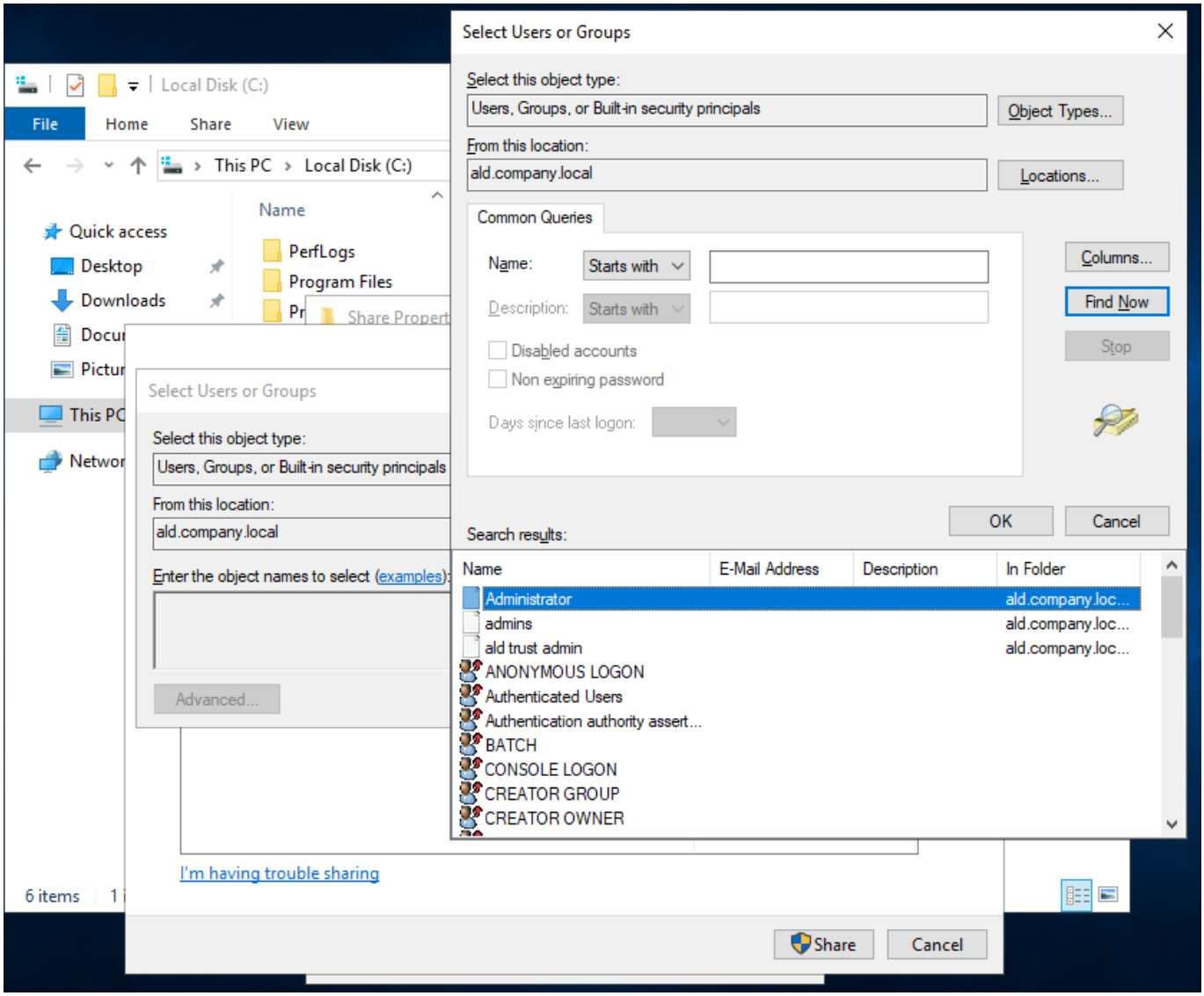
```
# /opt/gc/ipa-gc-install.py --gc-cert-file /etc/ssl/freeipa/server.p12 --gc-
↪pin 'AstraLinux_172' --disable-fast-preauth
```

где

- ipa-gc-install.py — имя файла со скриптом для настройки GC
- server.p12 — контейнер с сертификатом удостоверяющего центра и сервера
- gc-pin — пароль к контейнеру p12, совпадает с паролем доменного админа на момент установки IPA

Для настройки глобального каталога требуется контейнер p12 с сертификатом сервера и удостоверяющего центра. Используется уже существующий контейнер p12, который был создан FreeIPA при установке. Паролем к этому контейнеру является пароль доменного администратора, который использовался в момент продвижения сервера до контроллера домена.

После выполнения указанных действий на контроллере домена WINDC-1 при назначении прав доступа на сетевые ресурсы, стандартная оснастка «Select Users or Groups» начнет находить пользователей и группы из доверенного домена ald.company.local. Если уже придпринималась попытка обращения к глобальному каталогу, которая закончилась неудачно, необходимо очистить кеш и перезагрузить Windows сервер.



2.38. Инструкция по работе двусторонних доверительных отношений между MS AD и ALD Pro

2.38.1. Введение

Для удобства администрирования в организации может быть несколько доменов.

Например, домен MS AD и домен ALD Pro. В домене MS AD будут находится компьютеры с операционной системой Windows. Домен ALD Pro будут содержать компьютеры с AstraLinux.

Для корректной работы необходима возможность гибридной работы пользователей сразу в двух доменах с помощью механизма доверительных отношений.

Ранее в ALD Pro уже были реализованы доверительные отношения MS AD –> ALD Pro. Но для полноценной работы, необходимы двусторонние доверительные отношения.

Популярный кейс:

Ранее организация работала в домене MS AD, и в рамках миграции инфраструктур был развернут домен ALD Pro (ald.company.lan). Для беспрерывной работы предполагается постепенный перевод сервисов и пользователей на работу в новом домене. В течение некоторого времени необходимо обеспечивать гибридную работу пользователей сразу в двух доменах с помощью механизма доверительных отношений.

2.38.2. Как работали доверительные отношения MS AD и ALD Pro ранее

До внедрения функционала глобального каталога и двусторонних доверительных отношений, было реализовано в полном объеме только одностороннее доверие. Домен ALD Pro полностью доверял домену под управлением MS AD, следовательно пользователи MS AD имели возможность доступа на клиентские компьютеры и сетевые ресурсы в домене ALD Pro.

Доступ на клиентские машины в домене MS AD осуществляется только с машинами под ОС Windows. Доступ через SSSD-client осуществляется только путем ввода машины в два домена, что возможно и без доверия.

При разграничении доступа к ресурсам не было возможности сопоставить пользователя ALD Pro с атрибутом, и осуществлять поиск пользователей.

2.38.3. Как работают теперь

1. Версии Windows Server работающие с глобальным каталогом ALD Pro

    - Windows Server 2008 R2
    - Windows Server 2012
    - Windows Server 2012 R2
    - Windows Server 2016
    - Windows Server 2019

2. ALD Pro должен быть версии 2.1.0 и выше, с установленным глобальным каталогом.

3. Версия Astra Linux не ниже 1.7.4.

Для работы с глобальным каталогом, его необходимо установить согласно разделу gc_syncer.

Механизм работы глобального каталога

В лесу Active Directory может быть много поддоменов, и, чтобы ускорить поиск нужной информации, разработчики Microsoft придумали такую роль, как **глобальный каталог** (англ. Global Catalog, GC).

Контроллер домена MS AD, которому назначена роль глобального каталога, с помощью штатной процедуры репликации извлекает из всех поддоменов краткую информацию об объектах (англ. Partial Attribute Set, PAT) и предоставляет ее приложениям по запросу.

В FreeIPA нет глобального каталога, что становится проблемой при работе в доверительных отношениях с доменом MS AD, т.к. из-за этого Windows-администраторы не могу назначить права доступа пользователям доверенного домена FreeIPA с помощью стандартных оснасток (просто не работает поиск объектов из доверенного домена). Для решения этой проблемы в ALD Pro была реализована функция глобального каталога в виде дополнительного модуля.

Глобальный каталог ALD Pro – это отдельный экземпляр LDAP-сервера, в котором содержится копия всех объектов домена в схеме данных Active Directory. Глобальный каталог обеспечивает возможность поиска объектов (пользователей и групп) из стандартных оснасток Windows, что нужно для добавления субъектов доверенного домена в списки доступа на стороне Windows.

ГК состоит из следующих компонентов:

- Экземпляр LDAP-каталога (`dirsrv@GLOBAL-CATALOG`), работающий на стандартном для глобального каталога MS AD порту *3268/TCP*.
- Модуль синхронизации (`ipa-gcsyncd`) – служба, обеспечивающая синхронизацию объектов домена из обычного каталога в базу глобального каталога на том же контроллере домена.
- Модуль проверки целостности глобального каталога (`aldpro-gc-inspector`) – служба для выявления конфликтов синхронизации.

Для того чтобы клиенты MS AD могли обнаружить контроллеры домена ALD Pro, выполняющие функцию глобального каталога, в домене создаются SRV-записи вида:

- _gc._tcp.fqdn_имя_домена
- _gc._tcp.Default-First-Site-Name._sites.fqdn_имя_домена
- _ldap._tcp.Default-First-Site-Name._sites.gc._msdcs.fqdn_имя_домена
- _ldap._tcp.gc._msdcs.fqdn_имя_домена

Синхронизация работает на основе механизма репликации syncrepl. Служба ipa-gcsyncd извлекает информацию о пользователях и группах из основного LDAP-каталога, модифицирует ее с учетом схемы AD DS, которую ожидают увидеть клиенты Windows, и сохраняет в базу глобального каталога. Модификация учетных записей пользователей при синхронизации глобального каталога выполняется по шаблону `/opt/gc/templates/gcsync/gc_user_template.tmpl`:

```
{% macro first_val(attr) -%}
   {{ entry[attr][0] }}
{%- endmacro %}
dn: cn={{ first_val('uid') }},cn=users,{{ suffix }}
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: ad-top
objectClass: ad-organizationalPerson
objectClass: user
objectClass: securityPrincipal
objectClass: posixAccount
objectClass: inetUser
objectClass: gcobject
cn: {{ first_val('uid') }}
sn: {{ first_val('sn') }}
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
{%- if entry['givenname'] %}
givenName: {{ first_val('givenname') }}
{%- endif %}
instanceType: 4
{%- if entry['displayname'] %}
displayName: {{ entry.single_value['displayname'] }}
{%- endif %}
name: {{ first_val('cn') }}
objectGUID:: {{ guid }}
userAccountControl: 66048
primaryGroupID: 513
objectSid:: {{ sid }}
sAMAccountName: {{ pkey }}
sAMAccountType: 805306368
{%- if entry['krbcanonicalname'] %}
userPrincipalName: {{ entry.single_value['krbcanonicalname'] }}
{%- else %}
userPrincipalName: {{ first_val('krbprincipalname') }}
{%- endif %}
objectCategory: CN=Person,CN=Schema,CN=Configuration,{{ suffix }}
{%- if entry['mail'] %}
mail: {{ first_val('mail') }}
{%- endif %}
uidnumber: {{ first_val('uidnumber') }}
gidnumber: {{ first_val('gidnumber') }}
{%- for uid in entry['uid'] %}
uid: {{ uid }}
{%- endfor %}
homeDirectory: {{ first_val('homedirectory') }}
{%- for group in entry['memberof'] %}
memberof: {{ group }}
{%- endfor %}
nTSecurityDescriptor: D:(A;;RPWPCRCCDCLCLORCWOWDSDDTSW;;;DA)(A;;
 ↪RPWPCRCCDCLCLORCWOWDSDDTSW;;;SY)(A;;RPLCLORC;;;AU)(OA;;WP;736e4812-af31-
 ↪11d2-b7df-00805f48caeb;bf967ab8-0de6-11d0-a285-00aa003049e2;CO)(A;;SD;;;CO)
gcuuid: {{ entryuuid }}
```

Модификация групп пользователей выполняется по шаблону `/opt/gc/templates/gcsync/gc_group_template.tmpl`:

```
{% macro first_val(attr) -%}
   {{ entry[attr][0] }}
{%- endmacro %}
dn: cn={{ pkey }},cn=users,{{ suffix }}
objectClass: top
objectClass: ad-top
objectClass: group
objectClass: securityprincipal
objectClass: nsmemberof
objectClass: gcobject
objectClass: posixGroup
cn: {{ pkey }}
instanceType: 4
name: {{ pkey }}
objectGUID:: {{ guid }}
objectSid:: {{ sid }}
sAMAccountName:  {{ pkey }}
sAMAccountType: 268435456
objectCategory: CN=Group,CN=Schema,CN=Configuration,{{ suffix }}
ntsecuritydescriptor: D:(A;;RPWPCRCCDCLCLORCWOWDSDDTSW;;;DA)(A;;
 ↪RPWPCRCCDCLCLORCWOWDSDDTSW;;;SY)(A;;RPLCLORC;;;AU)(A;;
 ↪RPWPCRCCDCLCLORCWOWDSDDTSW;;;AO)(A;;RPLCLORC;;;PS)(OA;;CR;ab721a55-1e2f-
 ↪11d0-9819-00aa0040529b;;AU)
{%- for member in entry['member'] %}
member: {{ member }}
{%- endfor %}
{%- for group in entry['memberof'] %}
memberof: {{ group }}
{%- endfor %}
gidnumber: {{ gidnumber }}
groupType: {{ groupType }}
gcuuid: {{ entryuuid }}
```

Одним из наиболее важных атрибутов для синхронизации объектов глобального каталога является **ipaNTSecurityIdentifier**, который определяет уникальный идентификатор субъектов безопасности Windows. Этот атрибут генерируется плагином **sidgen** и есть у всех пользователей и групп ALD Pro. При синхронизации глобального каталога значение текстового атрибута **ipaNTSecurityIdentifier** записывается в бинарный атрибут **ObjectSid**, который, собственно, и используется при добавлении субъектов безопасности в списки доступа на стороне Windows.

Механизм поиска и добавления субъектов ALD Pro в списки ACL на стороне Windows работает следующим образом:

1. Windows-администратор при добавлении пользователя/группы в ACL с помощью стандартной оснастки выполняет поиск объектов в доверенном домене ALD Pro. Запрос направляется к глобальному каталогу на порт 3268/TCP (LDAP) с аутентификацией по Kerberos. Если Kerberos-аутентификация по какой-либо причине не сработает (например, время в доменах отличается более, чем на 5 минут), то оснастка Windows попытается выполнить NTLM-аутентификацию, поэтому пользователь увидит окно для ввода учетных данных.

2. После успешного поиска появится список объектов ALD Pro с отображением их `uid` (в случае пользователя) или `cn` (в случае группы).

3. При добавлении субъекта в список доступа, система безопасности Windows выполнит еще один запрос к контроллеру домена ALD Pro по протоколу SMB для дополнительной проверки, существует ли субъект с таким SID в домене.

4. Для успешного выполнения указанного запроса на контроллере ALD Pro должны работать службы smbd и winbind. Обработка запроса выполняется с использованием библиотеки **ipasam** (или **aldprosam** в случае доверительных отношений между доменами ALD Pro).

5. После получения поодтверждения, что субъект с указанным SID существует в домене ALD Pro, система Windows добавит его в редактируемый список доступа.

2.38.4. Настройка двусторонних доверительных отношений

Для работы доверительных отношений с компьютеров из домена ALD.company.lan должны разрешаться имена компьютеров из домена WIN.company.lan и наоборот, нужно сделать взаимное перенаправление DNS-зон.

Настройка ALD Pro

Добавление зоны перенаправления можно сделать из графического интерфейса «Роли и службы сайта Служба разрешения имен Перенаправление запросов».

1. Имя зоны = имя домена MS AD.

2. Глобальные перенаправители = IP-адрес контроллера домена MS AD, с которым устанавливаются доверительные отношения.

3. Остальные поля и параметры оставить без изменений.

После на каждом контроллере домена необходимо выполнить команды:

```
sudo net conf setparm global "restrict anonymous" "0"
sudo aldproctl restart -i
```

Настройка MS AD

Настройка контроллера домена MS AD осуществляется согласно официальным инструкциям к MS AD. (Пуск → Оснастка “DNS”):

1. Контекстное меню к “Серверы условной пересылки” → Создать сервер условной пересылки.
2. В поле “DNS-домен” ввести имя домена ALD Pro.
3. Добавить IP-адрес контроллера домена ALD Pro в блоке “IP-адреса основных серверов:”.

Создание двусторонних доверительных отношений осуществляется на портале управления ALD Pro на вкладке **Управление доменом** → **Интеграция с доменом** → **Доверительные отношения** (см. Справочный центр на портале или Руководство пользователя).

Выполнение данных команд предоставляет УЗ Администратора доступ к атрибуту krbPrincipalKey у сервисного принципала cifs, что необходимо для успешного создания двусторонних доверительных отношений.

При создании доверительных отношений с доменом MS AD необходимо указать диапазон идентификаторов для доверенного домена MS AD.

На всех контроллерах домена ALD Pro и файловых серверах в конфигурационный файл `samba` необходимо добавить следующие параметры:

```
idmap config <netbios домена MS AD> : range = 261600000 - 261800000
idmap config <netbios домена MS AD> : backend = sss
```

Диапазон идентификаторов выводится с помощью команды:

```
ipa idrange-find
```

Пример:

```
astr@dc01:~$ ipa idrange-find
------------------
найдено 4 диапазона
------------------
Имя диапазона: MSAD.DOMEN.RU_id_range
Первый идентификатор POSIX диапазона: 618600000
Количество идентификаторов в диапазоне: 200000
Первый RID соответствующего диапазона RID: 0
SID доверенного домена: S-1-5-21-3537296142-1636428635-2476405179
Тип диапазона: Active Directory domain range
Имя диапазона: MVPWIN16.DOMEN.RU_id_range
Первый идентификатор POSIX диапазона: 261600000
Количество идентификаторов в диапазоне: 200000
Первый RID соответствующего диапазона RID: 0
SID доверенного домена: S-1-5-21-3894048104-315847931-183599100
Тип диапазона: Active Directory domain range
```

Из этого:

```
idmap config <netbios домена MS AD> : range = <Первый идентификатор POSIX
 ↪диапазона> - <Первый идентификатор POSIX диапазона> + <Количество
 ↪идентификаторов в диапазоне>
```

После указания диапазонов идентификаторов необходимо перезапустить `samba`:

```
sudo systemctl restart smbd winbind
```

Необходимо обратить внимание на созданный диапазон идентификаторов, чрезвычайно важно чтобы в созданный диапазон доверенного домена входили RID пользователей этого домена. В противном случае диапазон необходимо расширить или пересоздать двусторонние доверительные отношения с параметром `--range-size=<количество идентификаторов в диапазоне>`.

Важно: После создания двусторонних доверительных отношений через некоторое время (в зависимости от того сколько реплик MS AD) может возникнуть ошибка с добавлением объектов через групповые политики. В этом случае необходимо удалить, а затем заново создать доверительные отношения. При этом записи с диапазона идентификаторов для доверенного домена и конфигурационный файл с `samba` оставить как есть (не удалять).

Для доступа к ресурсам windows с аутентификацией по kerberos (IIIS, cifs, принтеры с общим доступом по smb) необходимо отключить у клиентских компьютеров FAST аутентификацию, так как windows её не поддерживает. Для этого на всех клиентах ALD Pro, где предполагается доступ, необходимо настроить глобальную политику **Групповые политики → Параметры компьютеров → Безопасность → FAST аутентификация**. Выставить параметр never.

Важно: Установка этого параметра понижает безопасность.

При первом применении может понадобиться перезагрузка сервиса sssd.

Проверить двусторонние доверительные отношения можно следующими способами:

1. авторизация на компьютере домена MS AD;
2. авторизация на компьютере домена ALD Pro;
3. создание общей папки.

Авторизация на компьютере домена MS AD

Необходимо авторизоваться на компьютере домена MS AD, используя учетную запись пользователя ALD Pro. Логин должен быть указан полностью, включая имя домена:

```
<имя_пользователя ALD Pro>@<имя_домена>
```

В результате пользователь под учетной записью ALD Pro авторизуется на компьютере домена MS AD.

Авторизация на компьютере домена ALD Pro

Необходимо выбрать нужный домен MS AD и авторизоваться на компьютере домена ALD Pro, используя учетную запись пользователя MS AD. В поле **Имя пользователя** необходимо указать имя пользователя, без имени домена.

В результате пользователь под учетной записью MS AD авторизуется на компьютере домена ALD Pro.

Создание общей папки

1. Создание общей папки на компьютере домена MS AD.

Необходимо создать папку **C:Common** и добавить в нее хотя бы один файл. Открыть доступ к созданной папке из контекстного меню **Sharing → Share → Network access**. Настройки оставить по умолчанию.

В окне **Common PropertiesSharingAdvanced SettingsPermissions** будет отображена информация, что по умолчанию на уровне SMB все пользователи, включая пользователей ALD Pro, имеют полные права.

Но доступ к файлам регулируется также на уровне NTFS разрешений, которые настраиваются на вкладке **Common PropertiesSecurity**. Можно предоставить доступ к общей папке всем аутентифицированным пользователям.

В результате пользователи ALD Pro могут редактировать файлы, находящиеся в папке **Common**.

2. Создание общей папки на компьютере домена ALD Pro.

Необходимо создать новое сетевое место, которое соответствует папке **Common** в файловом менеджере. Для этого выбрать **Сеть → Создать сетевое место**. Указать **Название** и **Адрес** в формате:

```
smb://<полное наименование контроллера домена MS AD, на котором создана папка>
↪/<Наименование папки из MS AD>
```

В результате пользователи MS AD могут редактировать файлы, находящиеся в папке **Common**.

2.38.5. Заключение

Благодаря внедрению ряда решений, включая глобальный каталог ALD Pro, есть возможность настраивать двусторонние доверительные отношения. В отличие от MS AD, в ALD Pro направления доверия MS AD → ALD Pro и ALD Pro → MS AD реализованы разными механизмами.

Двусторонние доверительные отношения, предоставляют возможность общаться доменам ALD Pro и MS AD, решая ряд важных задач:

- Авторизация пользователей доверенных доменах на рабочих станциях;
- Доступ к сетевым ресурсам пользователей доверенного домена (веб сервер, файловый сервер, базы данных и т.д.);

- Разграничение доступа к ресурсам доверенных доменов.

2.39. Инструкция по присоединению системы Windows к FreeIPA Realm без Active Directory

Большинство системных администраторов имеют опыт использования компьютеров под управлением ОС Windows в домене Active Directory, но в качестве источника идентификационной информации компьютеры Windows могут использовать и область Kerberos от ALD Pro (FreeIPA). Способ, которым можно ввести Windows в домен FreeIPA был известен давно, но не получил широкого распространения, т. к. содержал существенный недостаток — внутри операционной системы пользователь действовал от имени локальной учетной записи, которую нужно было создавать заранее. В настоящей инструкции описан способ, который позволяет обеспечить вход в операционную систему именно доменной учетной записью, сохраняя ее SID, участие в группах и Kerberos билеты, что открывает новые возможности по решению задач гибридного развертывания и миграции.

2.39.1. Что такое Active Directory

Active Directory - это база данных специального назначения со службами, которые позволяют пользователям подключаться к привязанным к ней сетевым ресурсам. В этой базе данных хранится важная информация о вашей среде, такая как пользователь и компьютеры, которым разрешено устанавливать подключения. Поскольку Active Directory является продуктом Microsoft, он часто используется в среде Windows.Он обеспечивает эти функциональные возможности путем хранения пользовательских, групповых, хостовых и любых других данных, необходимых для управления безопасностью сетевых компьютеров. Что делает этот инструмент более совершенным, так это его простой и понятный в использовании веб-интерфейс, а также командная строка для администрирования.

2.39.2. Что такое FreeIPA

FreeIPA - это бесплатное интегрированное решение для управления информацией о безопасности с открытым исходным кодом, спонсируемое RedHat. Он сочетает в себе MIT Kerberos, Dogtag (систему сертификатов), NTP, DNS и сервер каталогов 389. Основная цель состоит в том, чтобы обеспечить функциональность, аналогичную Active Directory. Его можно использовать для обеспечения централизованной аутентификации, авторизации и получения информации об учетной записи.

FreeIPA не является повторной реализацией Microsoft Active Directory и может работать независимо. Основное различие между ними заключается в том, что FreeIPA ориентирована на Linux и другие системы, соответствующие стандартам POSIX, в то время как Active Directory является инструментом Windows.

ALD Pro(FreeIPA) может быть интегрирован для работы с Active Directory путем установления доверия между двумя службами. Но в этом руководстве настраивается система Windows на использование области FreeIPA для аутентификации пользователей без Active Directory.

Чтобы достичь этого, необходимо выполнить приведенные ниже шаги.

2.39.3. Требования к настройке

В этом руководстве будут настроены две системы со статическими IP-адресами и именами хостов:

TASK	HOSTNAME	IP_ADDRESS
FreeIPA server(ALD Pro)	ald01.ald.dom	192.168.88.210
Windows client	Win10test.ald.dom	192.168.88.76

2.39.4. Порядок присоединения

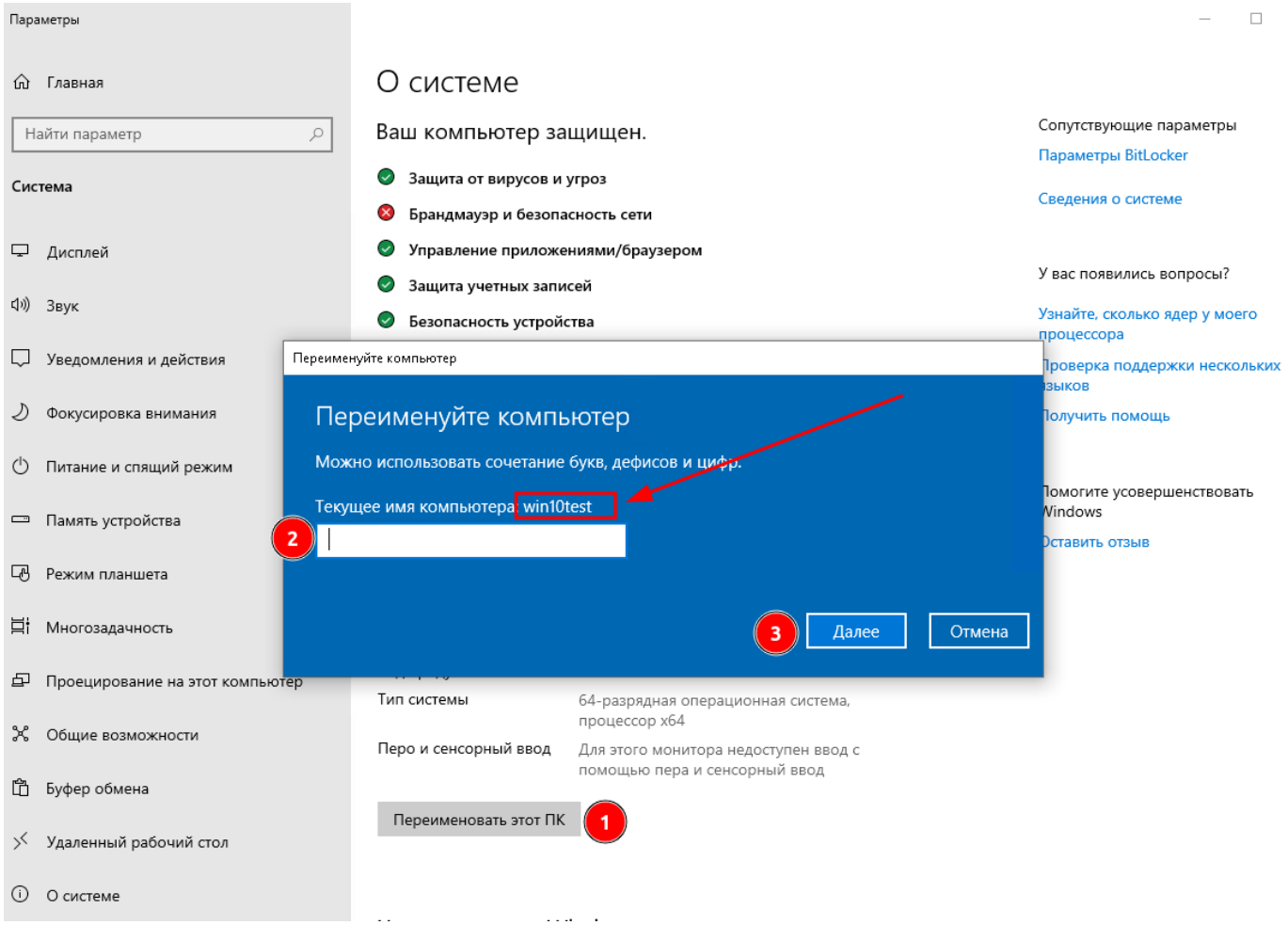


Рисунок 2.1 – Установка имени хоста

Нажать Win+R и запустить ncpa.cpl для настройки сети. Сначала настраивается DNS таким образом, чтобы он мог разрешать имя ALD Pro(IPA)-сервера.

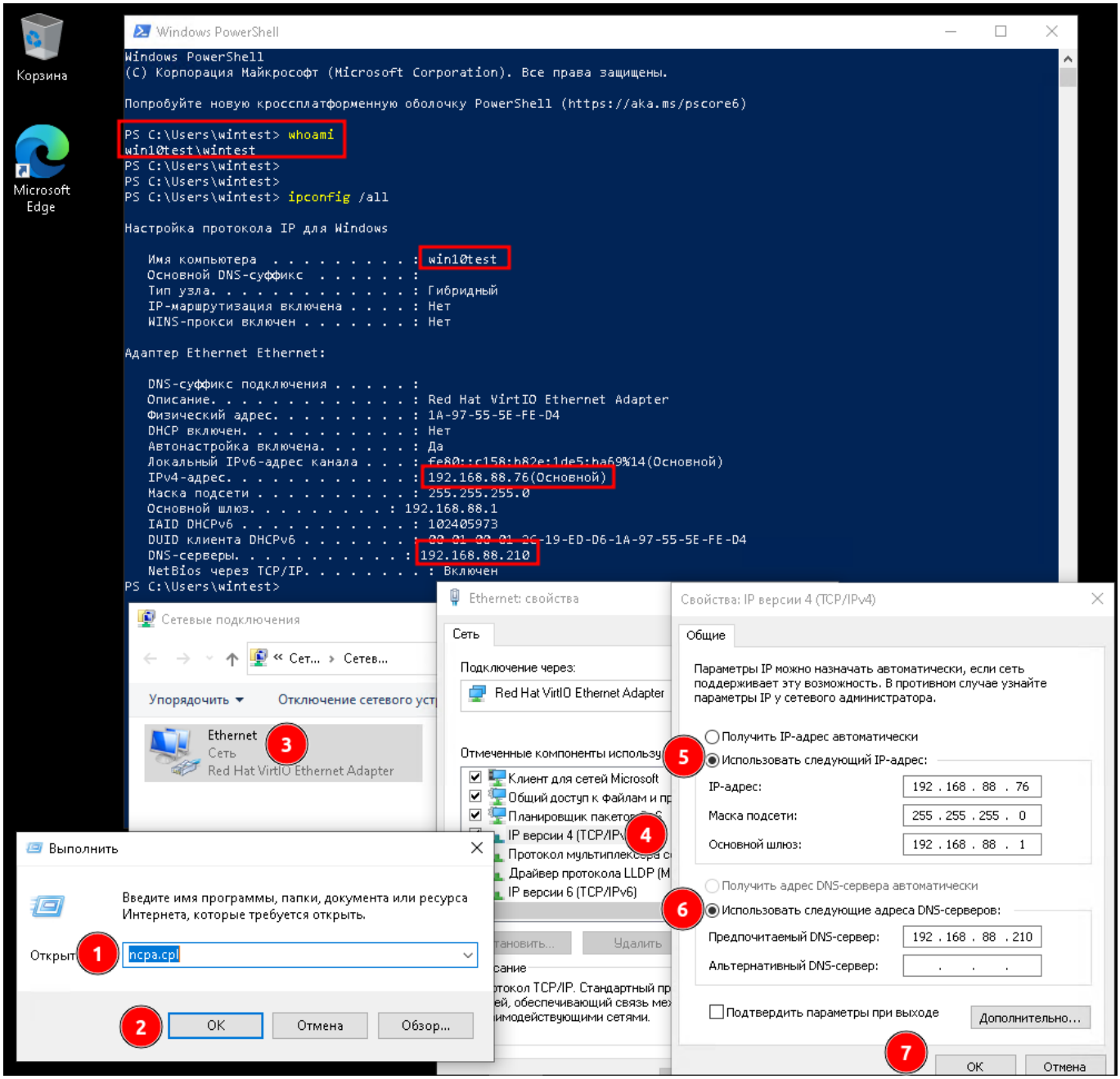


Рисунок 2.2 – Настройка сети на Windows машине 1

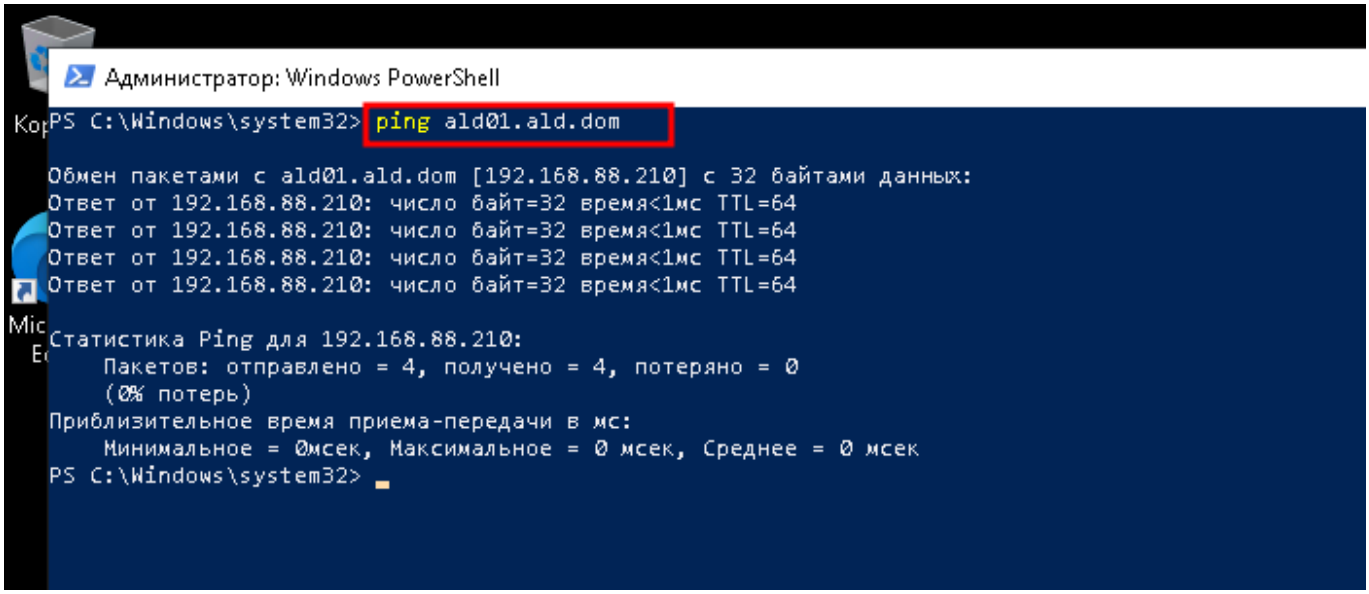


Рисунок 2.3 – Настройка сети на Windows машине 2

На стороне ALD Pro(FreeIPA) необходимо убедиться, что время не расходится с внешним NTP сервером

```
# chronyc tracking
root@ald01:~# chronyc tracking
Reference ID    : BCE109A7 (188.225.9.167)
Stratum         : 3
Ref time (UTC)  : Tue Jun 13 10:08:13 2023
System time     : 0.000034270 seconds slow of NTP time
Last offset     : -0.000079430 seconds
RMS offset      : 0.000206107 seconds
Frequency       : 9.831 ppm slow
Residual freq   : -0.001 ppm
Skew            : 0.061 ppm
Root delay      : 0.017628554 seconds
Root dispersion : 0.003091000 seconds
Update interval : 1040.0 seconds
Leap status     : Normal
root@ald01:~#
root@ald01:~#
root@ald01:~# timedatectl
               Local time: Tue 2023-06-13 13:14:55 MSK
           Universal time: Tue 2023-06-13 10:14:55 UTC
                 RTC time: Tue 2023-06-13 10:14:55
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
               Time zone: Europe/Moscow (MSK, +0300)
System clock synchronized: yes
              NTP service: inactive
          RTC in local TZ: no
```

На стороне Windows настраивается синхронизация времени с контроллером домена в роли NTP сервера. Можно указать несколько значений (FQDN или IP адрес) через запятую, что не обеспечивает возможность автообнаружения контроллеров

```
w32tm /config /reliable:yes /syncfromflags:manual /manualpeerlist:"<NTPServer>
 ↪" /update
```

```
net start w32time

w32tm /config /reliable:yes /syncfromflags:manual /manualpeerlist:"ald01.ald.
 ↪dom" /update
net stop w32time
net start w32time
w32tm /resync
w32tm /monitor /computers:"ald01.ald.dom"
w32tm /stripchart /computer:ald01.ald.dom
```

Результат проверки времени

```
PS C:\Users\Administrator> w32tm /stripchart /computer:ald01.ald.dom
Tracking ald01.ald.dom [192.168.88.210:123].
The current time is 4/13/2023 1:40:55 PM.
13:40:55, d:+00.0091883s o:-00.0110417s  [                              *      □
 ↪                     ]
13:40:57, d:+00.0093593s o:-00.0111335s  [                              *      □
 ↪                     ]
13:40:59, d:+00.0099441s o:-00.0112867s  [                              *      □
 ↪                     ]
13:41:01, d:+00.0100102s o:-00.0113176s  [                              *      □
 ↪                     ]
```

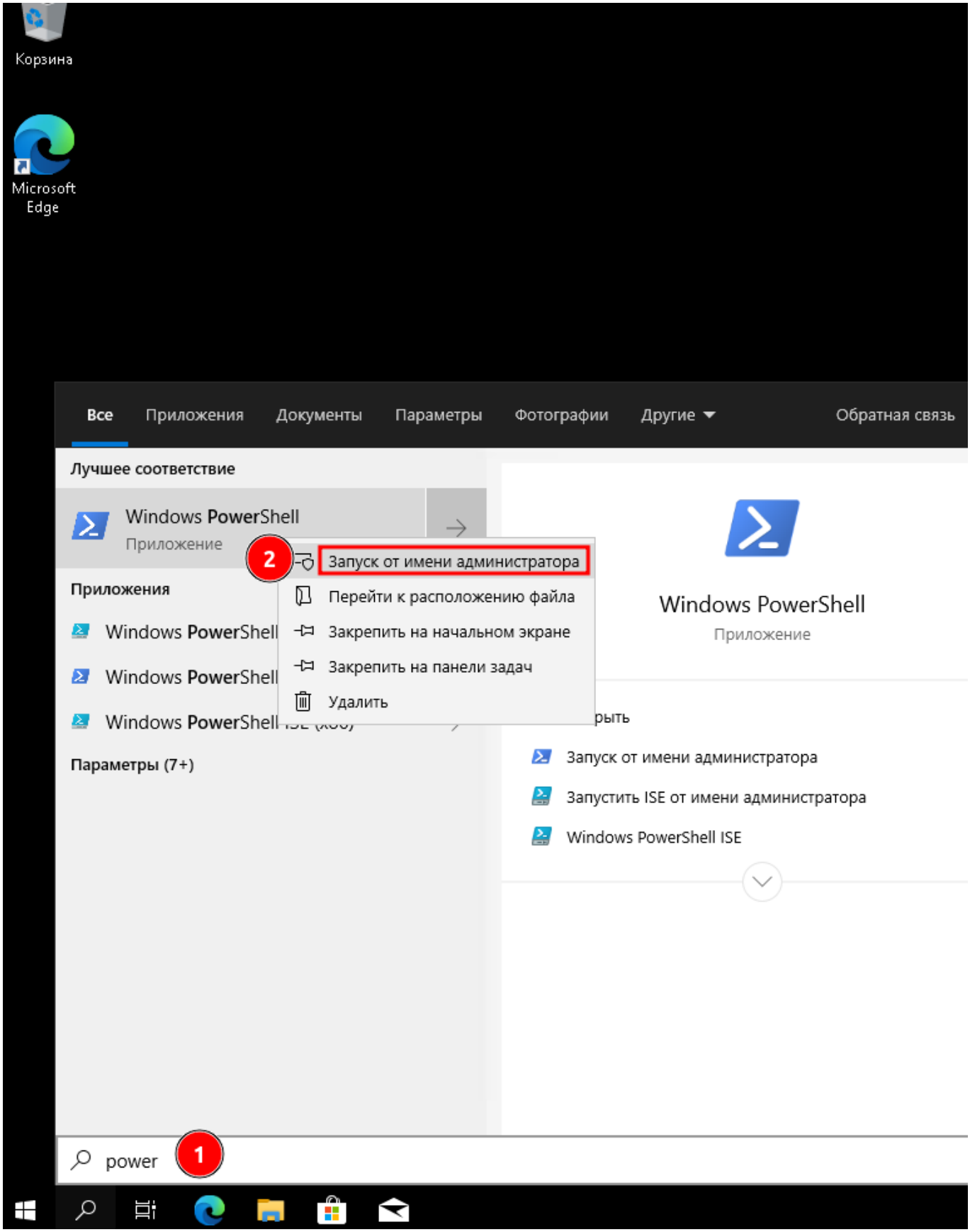


Рисунок 2.4 – Настройки даты/времени 1

В данном примере указан IP адрес

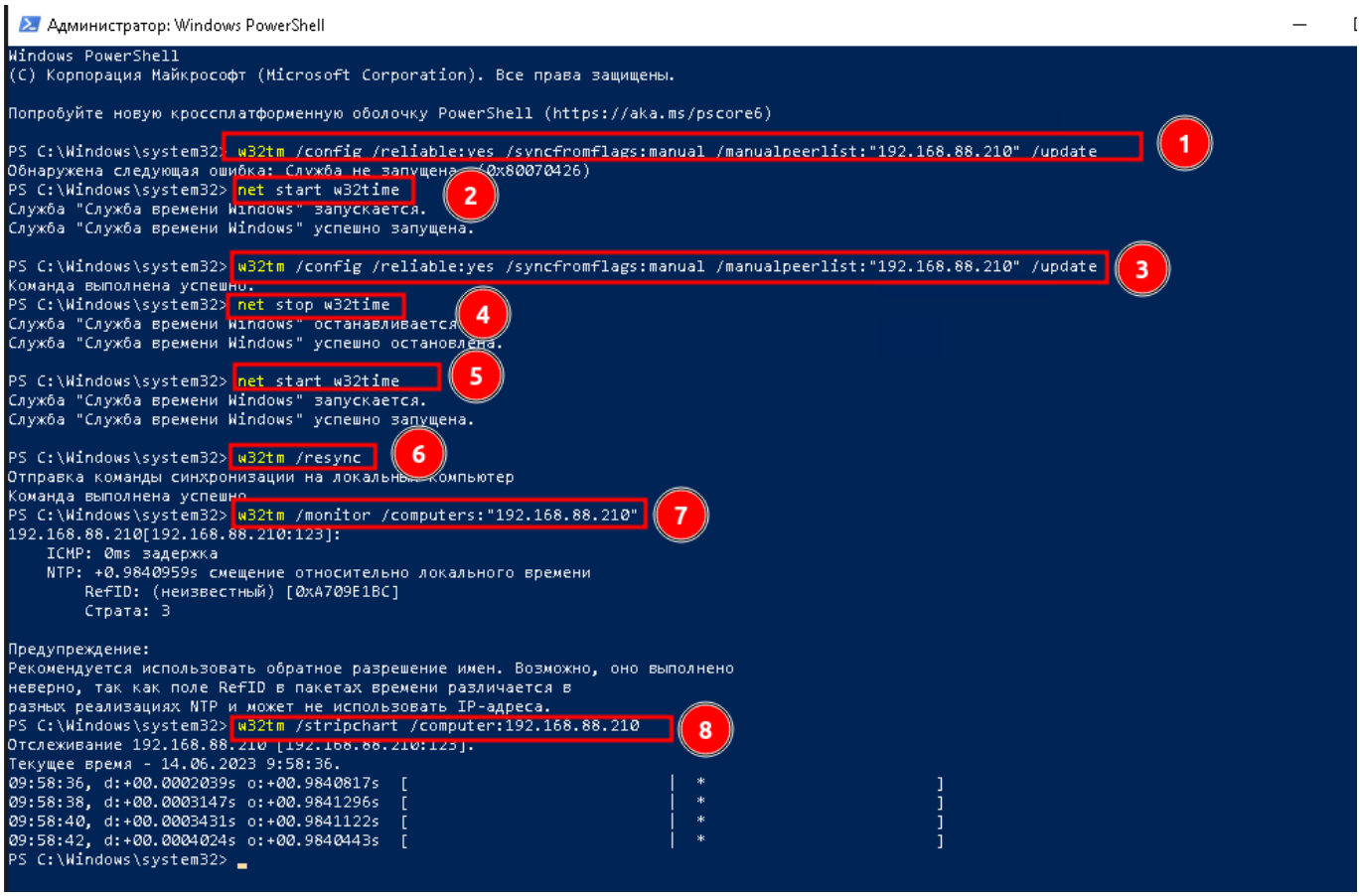


Рисунок 2.5 – Настройки даты/времени 2

В веб-консоли перейти на вкладку хосты и нажать кнопку Добавить.

Указать имя хоста и IP-адрес клиента Windows, как показано на рисунке.

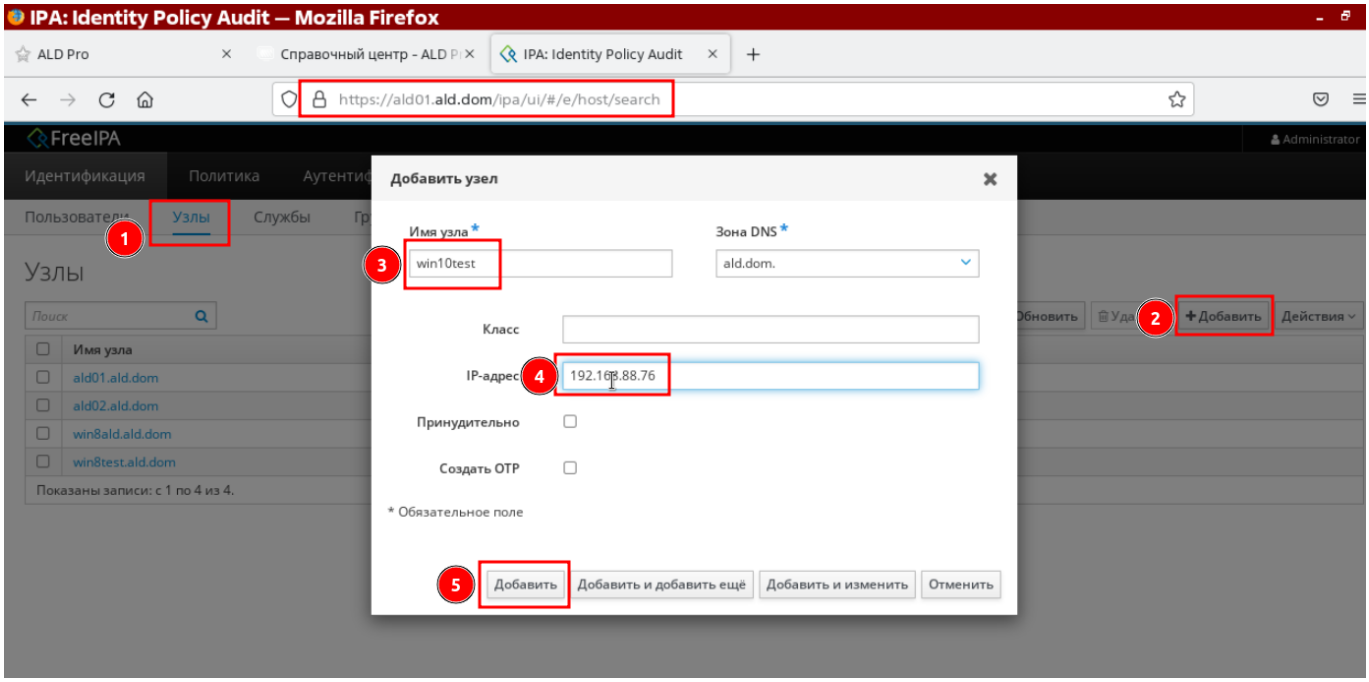


Рисунок 2.6 – Создание нового узла в консоли FreeIPA 1

Клиент был добавлен, но еще не зарегистрирован.

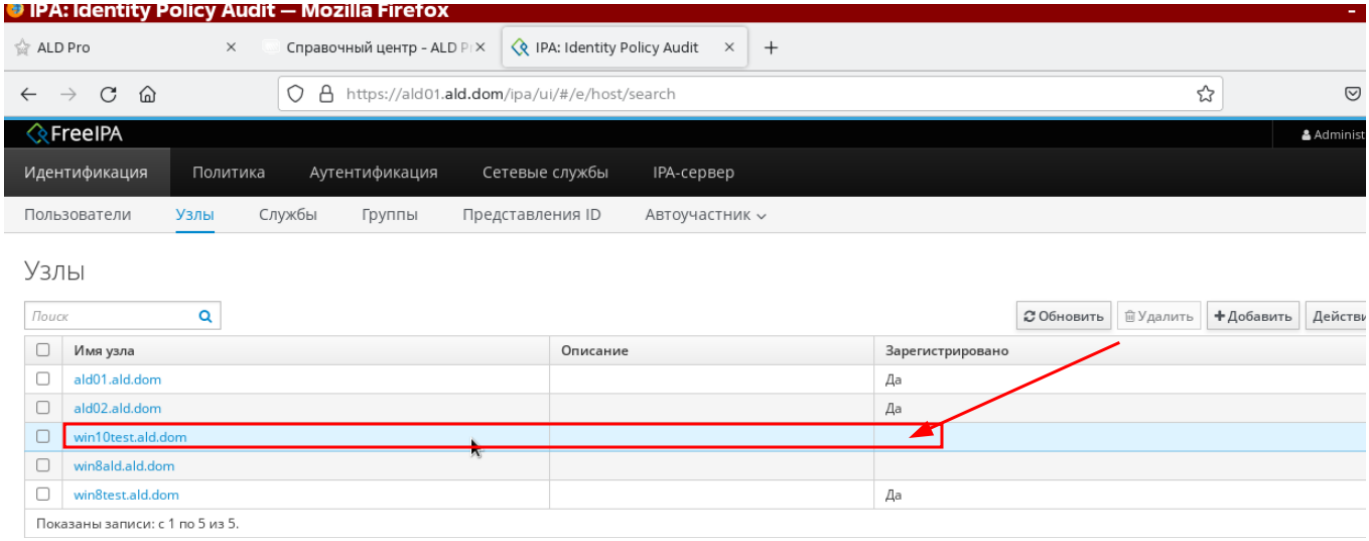


Рисунок 2.7 – Создание нового узла в консоли FreeIPA 2

Таблица ключей(keytab) - это файл, содержащий пары участников Kerberos и зашифрованные ключи (которые являются производными от пароля Kerberos).

Аутентификация(Authentication) - это процесс проверки личности зарегистрированного пользователя или процесса перед предоставлением доступа к защищенным сетям и системам.

В командной строке FreeIPA добавить клиента.

Сначала генерируется билет (Выполните аутентификацию) с помощью команды:

```
root@ald01:~#kinit admin
root@ald01:~#kinit admin
Password for admin@ALD.DOM:
root@ald01:~#
root@ald01:~#
root@ald01:~# klist
Ticket cache: KEYRING:persistent:0:krb_ccache_sN0WuVv
Default principal: admin@ALD.DOM

Valid starting     Expires            Service principal
06/13/23 13:36:28  06/14/23 13:36:24  krbtgt/ALD.DOM@ALD.DOM
```

Для получения поддерживаемых типов шифрования выполнить команду:

```
root@ald01:~# ipa-getkeytab --permitted-enctypes
Failed to load translations
Supported encryption types:
AES-256 CTS mode with 96-bit SHA-1 HMAC
AES-128 CTS mode with 96-bit SHA-1 HMAC
AES-256 CTS mode with 192-bit SHA-384 HMAC
AES-128 CTS mode with 128-bit SHA-256 HMAC
Triple DES cbc mode with HMAC/sha1
ArcFour with HMAC/md5
Camellia-128 CTS mode with CMAC
Camellia-256 CTS mode with CMAC
```

Добавить участника, используя команду с приведенным ниже синтаксисом. Необходимо включить типы шифрования:

```
root@ald01:~#ipa-getkeytab -s ald01.ald.dom -p host/win10test.ald.dom@ALD.
 ↪DOM -e aes256-cts,aes128-cts,aes256-sha2,aes128-sha2,camellia256-cts-cmac,
 ↪camellia128-cts-cmac -k /etc/krb5.keytab.windows -P
```

В приведенной выше команде:

-s указывает сервер FreeIPA;

-e определяет шифрование;

-k путь до существующего или нового keytab файла;

-p указывает нового участника, который будет добавлен;

-P устанавливает пароль (**не забудьте, так как он будет использоваться при настройке клиента позже**).

```
root@ald01:~# kinit admin
Password for admin@ALD.DOM:
root@ald01:~#
root@ald01:~# ipa-getkeytab -s ald01.ald.dom -p host/win10test.ald.dom@ALD.
 ↪DOM -e aes256-cts,aes128-cts,aes256-sha2,aes128-sha2,camellia256-cts-cmac,
 ↪camellia128-cts-cmac -k /etc/krb5.keytab.windows -P
Failed to load translations
New Principal Password:
Verify Principal Password:
Keytab successfully retrieved and stored in: /etc/krb5.keytab.windows
```

Проверка, был ли добавлен ключ:

```
root@ald01:~# klist -k /etc/krb5.keytab.windows
Keytab name: FILE:/etc/krb5.keytab.windows
KVNO Principal
---- --------------------------------------------------------------------------
 ↪-
   1 host/win8test.ald.dom@ALD.DOM
   1 host/win8test.ald.dom@ALD.DOM
   1 host/win8test.ald.dom@ALD.DOM
   1 host/win8test.ald.dom@ALD.DOM
   1 host/win8test.ald.dom@ALD.DOM
   1 host/win8test.ald.dom@ALD.DOM
   1 host/win10test.ald.dom@ALD.DOM
   1 host/win10test.ald.dom@ALD.DOM
   1 host/win10test.ald.dom@ALD.DOM
   1 host/win10test.ald.dom@ALD.DOM
   1 host/win10test.ald.dom@ALD.DOM
   1 host/win10test.ald.dom@ALD.DOM
```

Вернуться к веб-интерфейсу FreeIPA, клиент должен быть зарегистрирован.

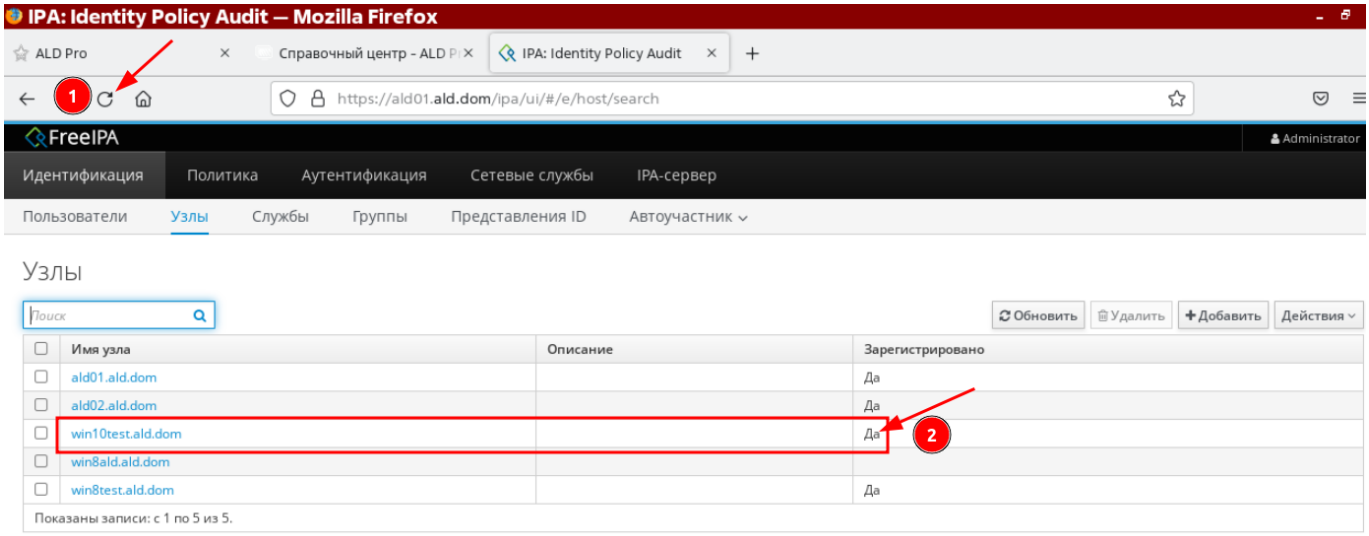


Рисунок 2.8 – Создание keytab 1

Чтобы иметь возможность использовать FreeIPA для аутентификации в Windows, необходимо создать пользователя в FreeIPA. На FreeIPA странице перейти на вкладку Пользователи и добавить пользователя, как показано на рисунке:

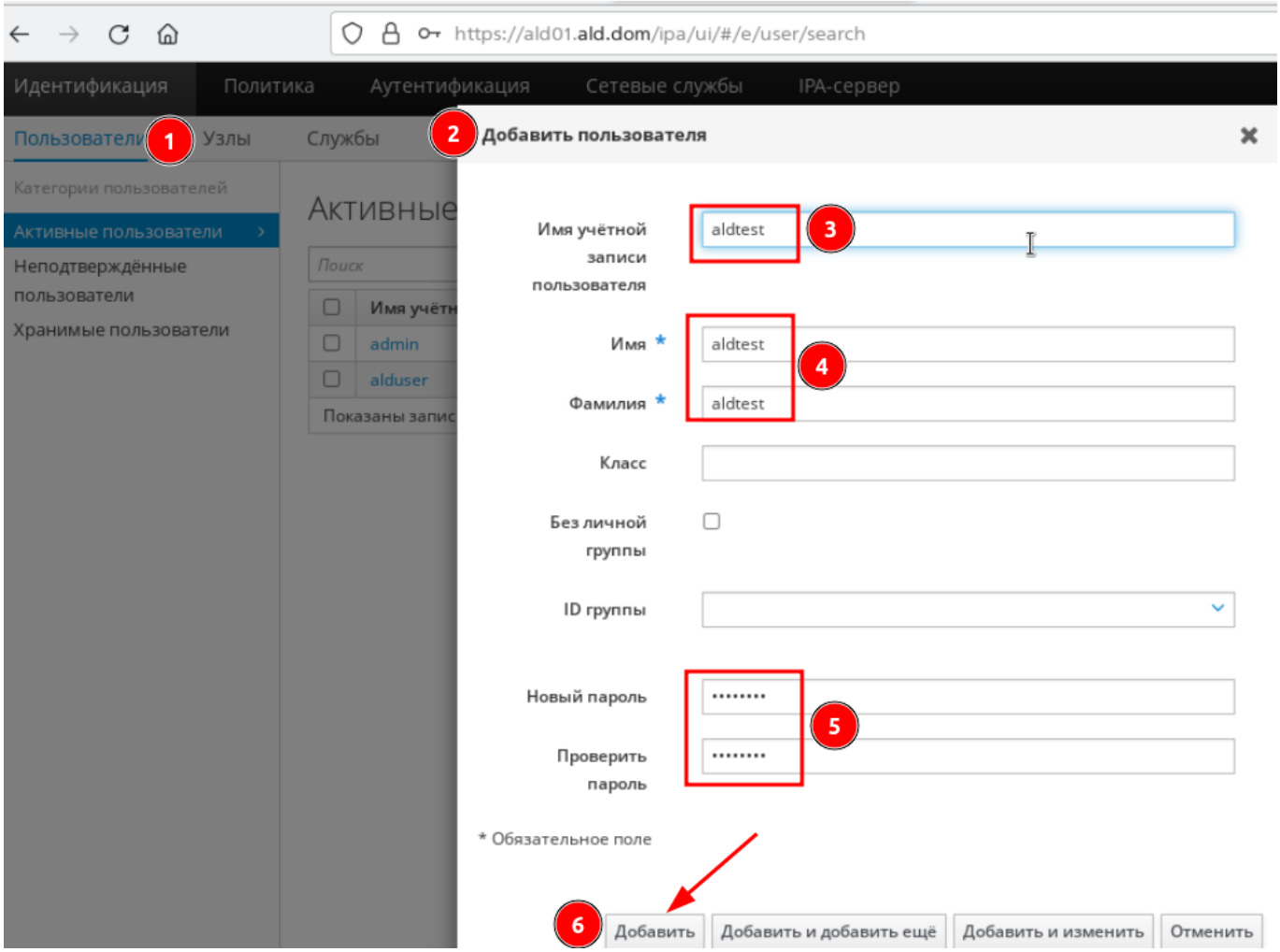


Рисунок 2.9 – Создание пользователя в FreeIPA

Указанный пароль при создании пользователя необходимо сменить при первом входе в систему.

Добавленный пользователь появится, как показано на рисунке.

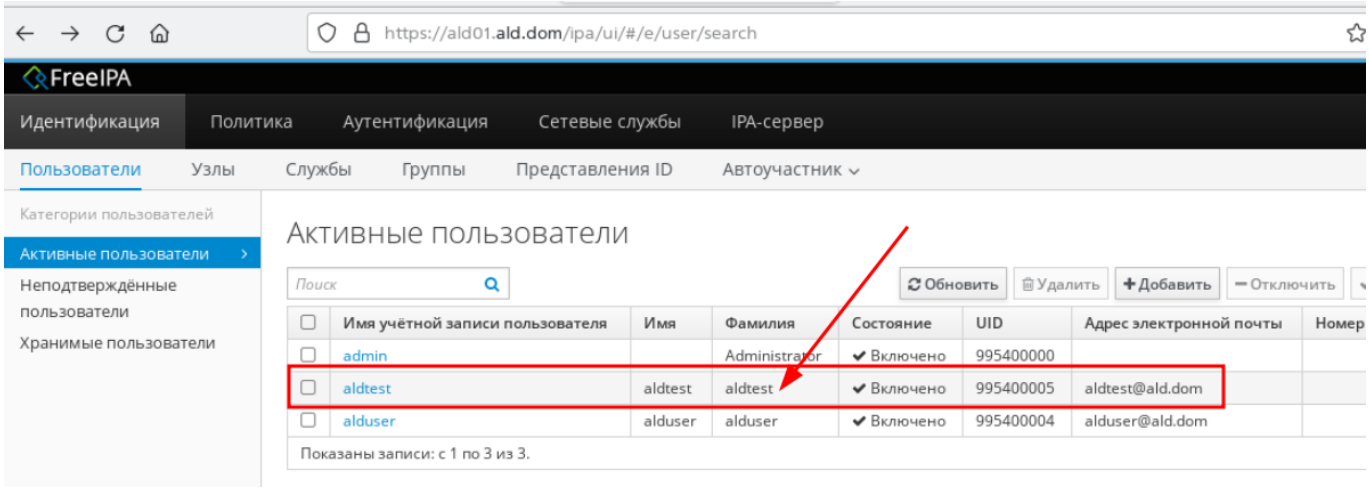


Рисунок 2.10 – Добавленный пользователь

```
ksetup /setdomain [REALM NAME]
ksetup /addkdc [REALM NAME] [kdc DNS name]
ksetup /addkpasswd [REALM NAME] [kdc DNS name]
ksetup /setcomputerpassword [MACHINE_PASSWORD] #(пароль из шага 5 при
 ↪генерировании keytab)
# ksetup /mapuser * *
```

`ksetup /setdomain` - Задает доменное имя для всех операций Kerberos.

https://learn.microsoft.com/ru-ru/windows-server/administration/windows-commands/ksetup-domain

`ksetup /addkdc` - Добавляет адрес центра распространения ключей (KDC) для заданной области Kerberos.

https://learn.microsoft.com/ru-ru/windows-server/administration/windows-commands/ksetup-addkdc

`ksetup addkpasswd` - Добавляет адрес сервера kerberos password (kpasswd) для области.

https://learn.microsoft.com/ru-ru/windows-server/administration/windows-commands/ksetup-addkpasswd

`ksetup /setcomputerpassword` - Задает пароль для локального компьютера. Эта команда влияет только на учетную запись компьютера и требует перезагрузки, чтобы изменение пароля вступило в силу.

Примечание: Пароль учетной записи компьютера не отображается в реестре или в качестве выходных данных команды ksetup.

https://learn.microsoft.com/ru-ru/windows-server/administration/windows-commands/ksetup-setcomputerpassword

В инструкциях встречается указание, что необходимо выполнить команду ksetup /mapuser, чтобы сопоставить все учетные записи в области ALD.DOM Kerberos с любой существующей учетной записью с тем же именем на этом компьютере.

Благодаря использованию доменных учётных записей пользователей, нет необходимости сопоставлять им локальные “учётки”.

https://learn.microsoft.com/ru-ru/windows-server/administration/windows-commands/ksetup-mapuser

Выполнить поочередно следующие команды (Не перезагружать компьютер):

```
ksetup /setdomain ALD.DOM
ksetup /addkdc ALD.DOM ald01.ald.dom
ksetup /addkpasswd ALD.DOM ald01.ald.dom
ksetup /setcomputerpassword !QAZ1qaz (укажите свой пароль)
```

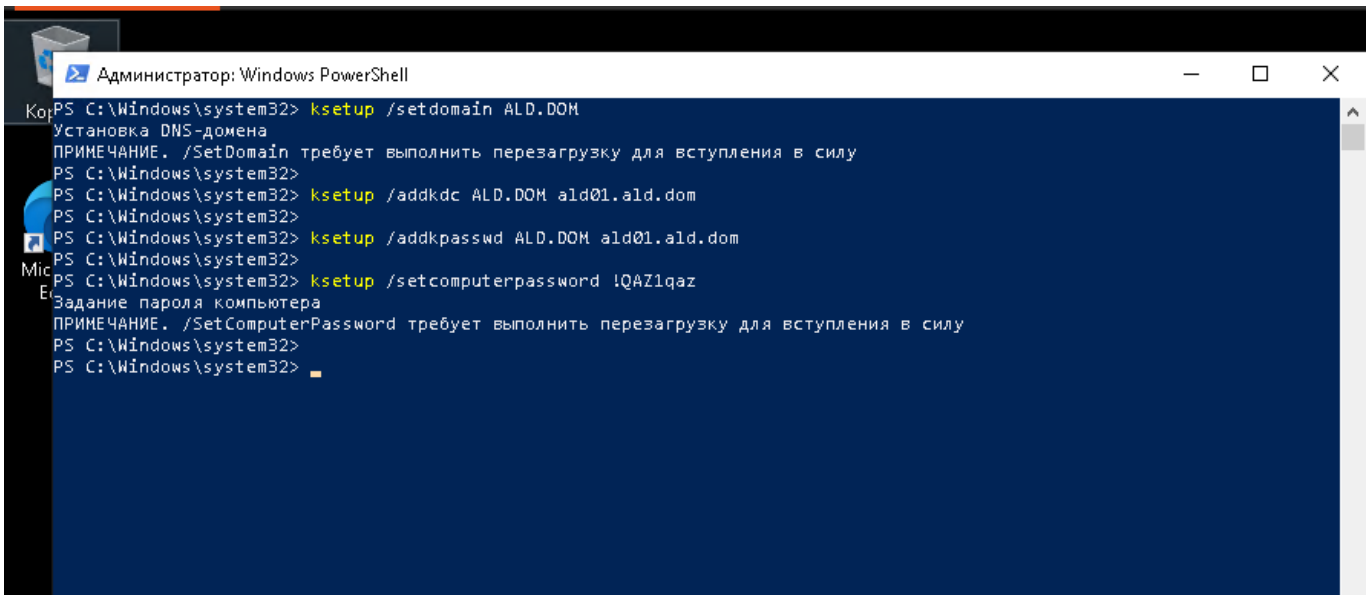


Рисунок 2.11 – Результат выполнения команд

Теперь запустить **gpedit.msc**, нажав клавишу Windows + R.

Конфигурация Windows > Параметры безопасности, Локальные политики, Параметры Безопасности > Сетевая безопасность: настройка типов шифрования, разрешенных Kerberos

Windows Settings > Security Settings > Local Policies > Security Options > Network Security: Configure encryption types allowed for Kerberos

Указать следующие типы шифрования:

RC4_HMAC_MD5,AES128_HMAC_SHA1,AES256_HMAC_SHA1,Будущие типы шифрования

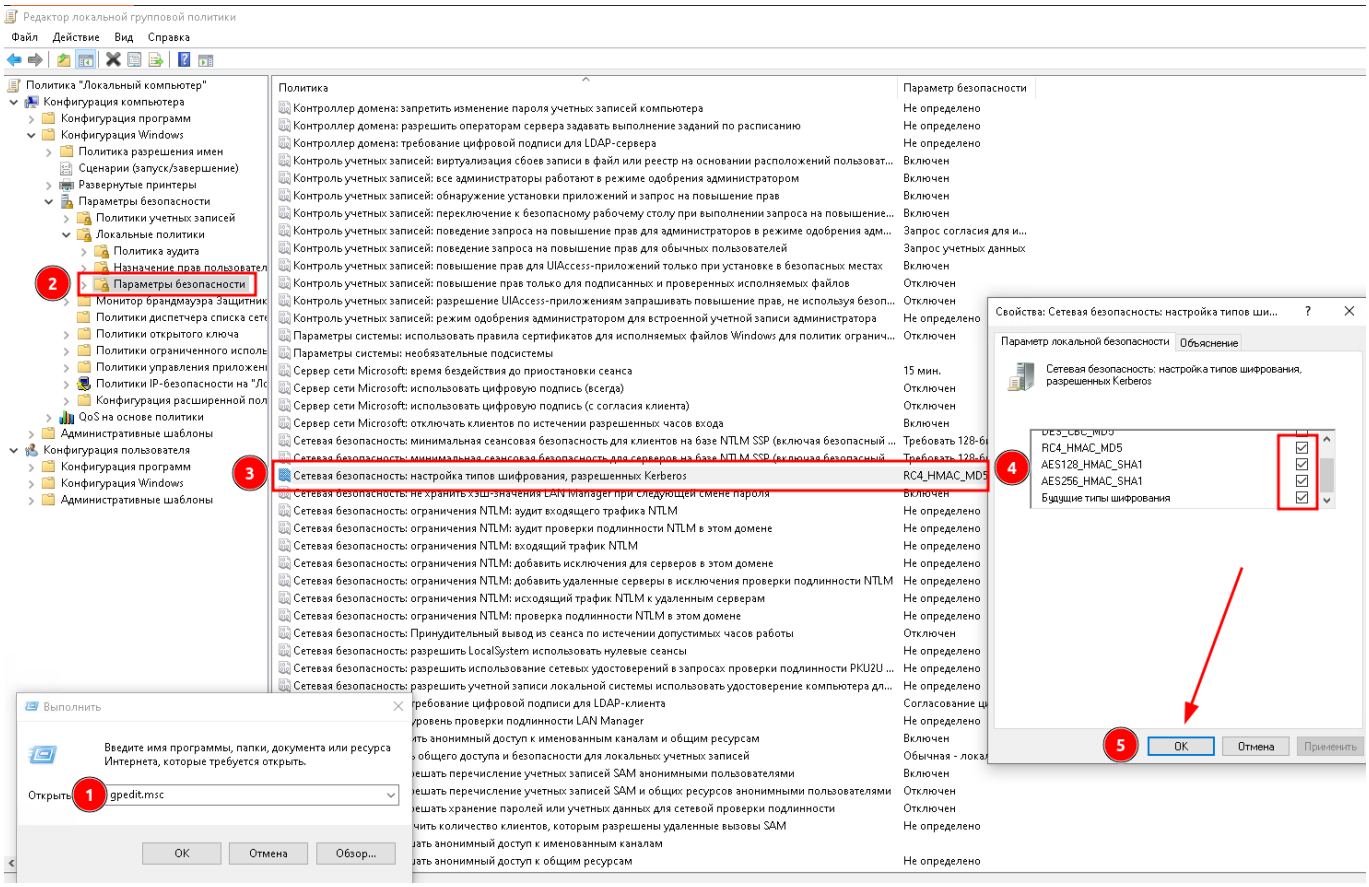


Рисунок 2.12 – Типы шифрования

Применить, нажав кнопку ОК, и перезагрузить систему.

Имя Пользователя@REALM aldtest@ALD.DOM

Когда система перезагрузится, войти в систему с помощью пользователя FreeIPA, как показано на рисунке:

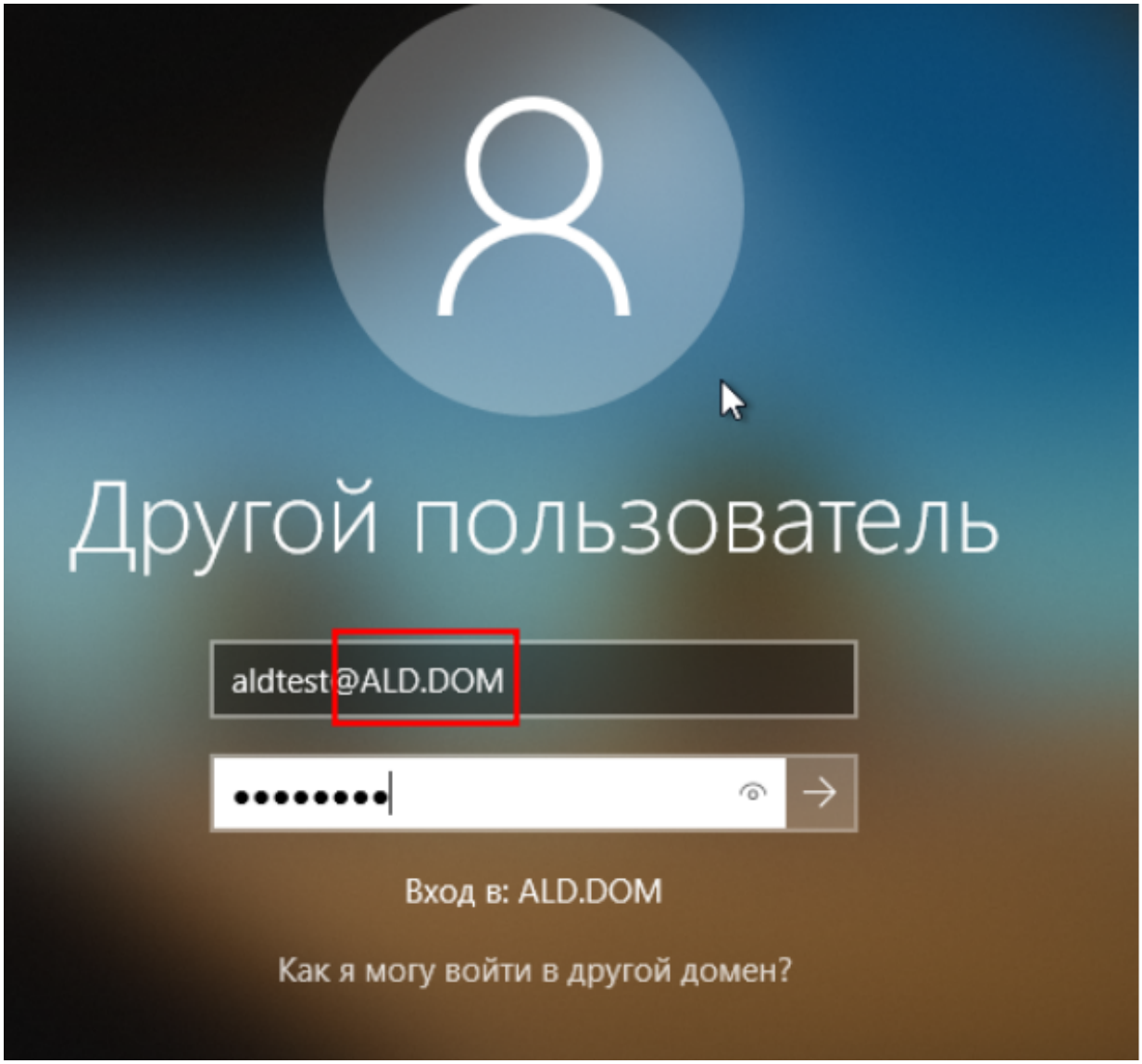


Рисунок 2.13 – Вход в систему

Будет предложено изменить пароль для пользователя IPA.

Выполнить следующие команды в PowerShell или CMD:

```
whoami
klist
```

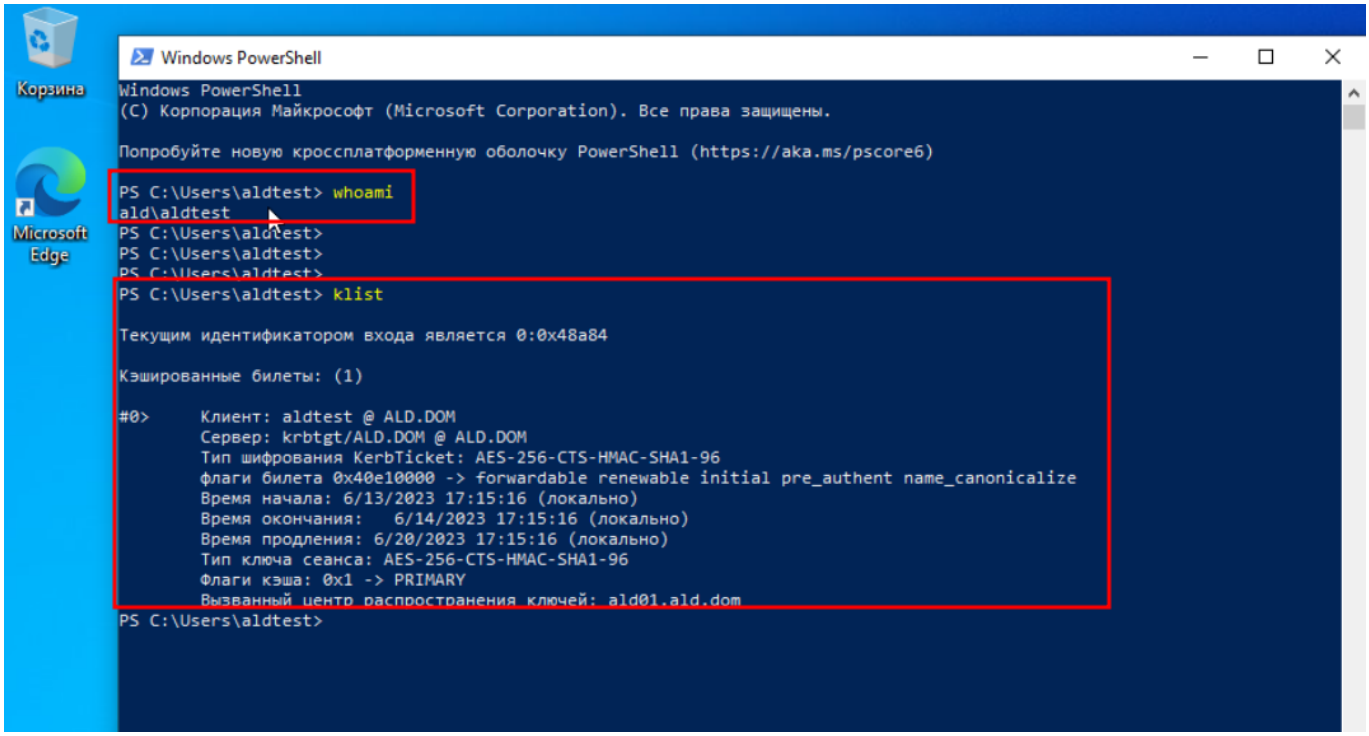


Рисунок 2.14 – Проверки 1

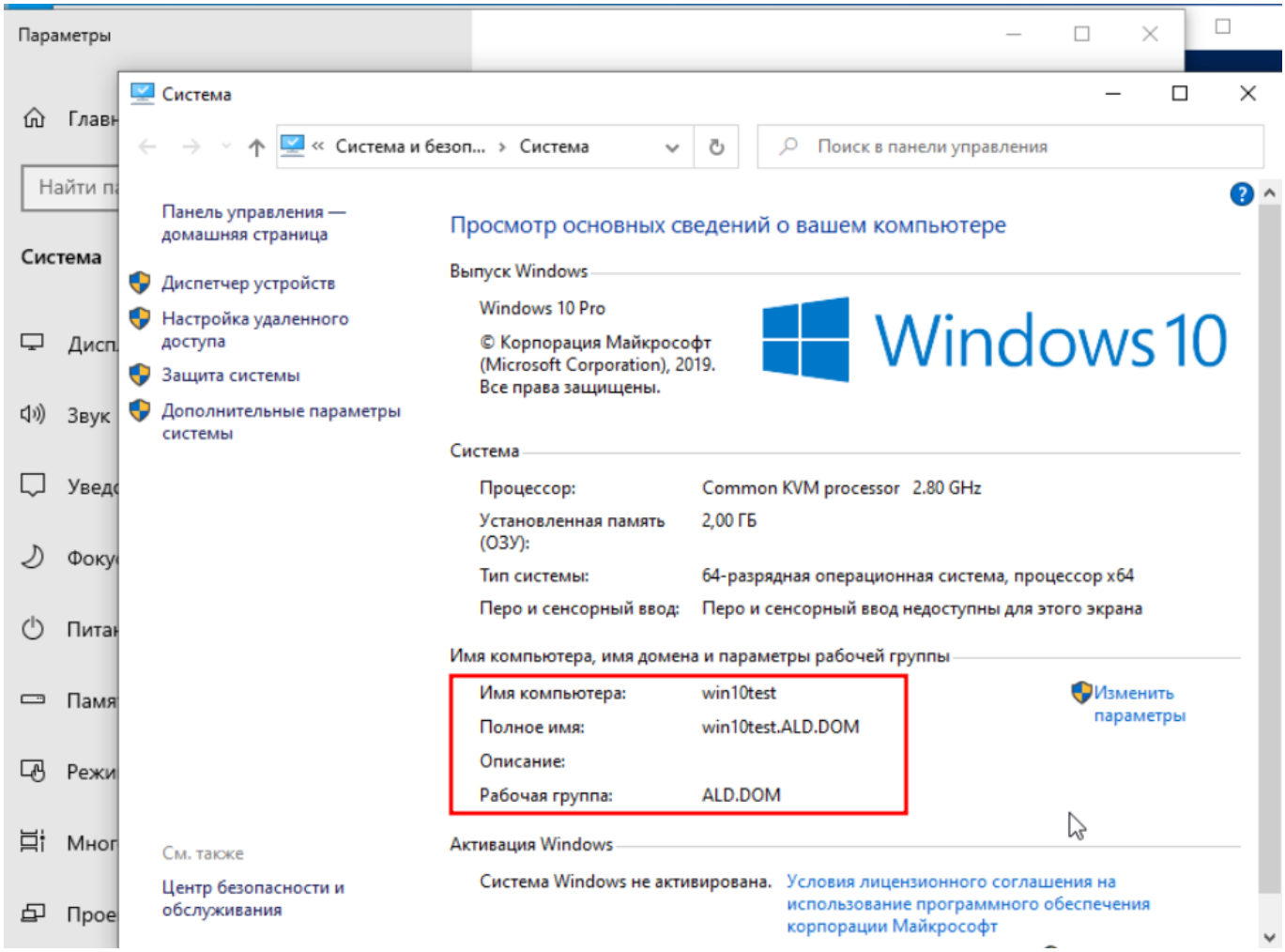


Рисунок 2.15 – Проверки 2

На Ald Pro сервере создать общую тестовую папку и попробовать зайти:

```
root@ald01:~# nano /etc/samba/smb.conf
[testshare]
path = /srv/testshare
browseable = yes
valid users = aldtest
admin users = aldtest
writable = yes
```

```
root@ald01:~# systemctl reload smbd.service
```

После успешного входа klist будет содержать дополнительный билет:

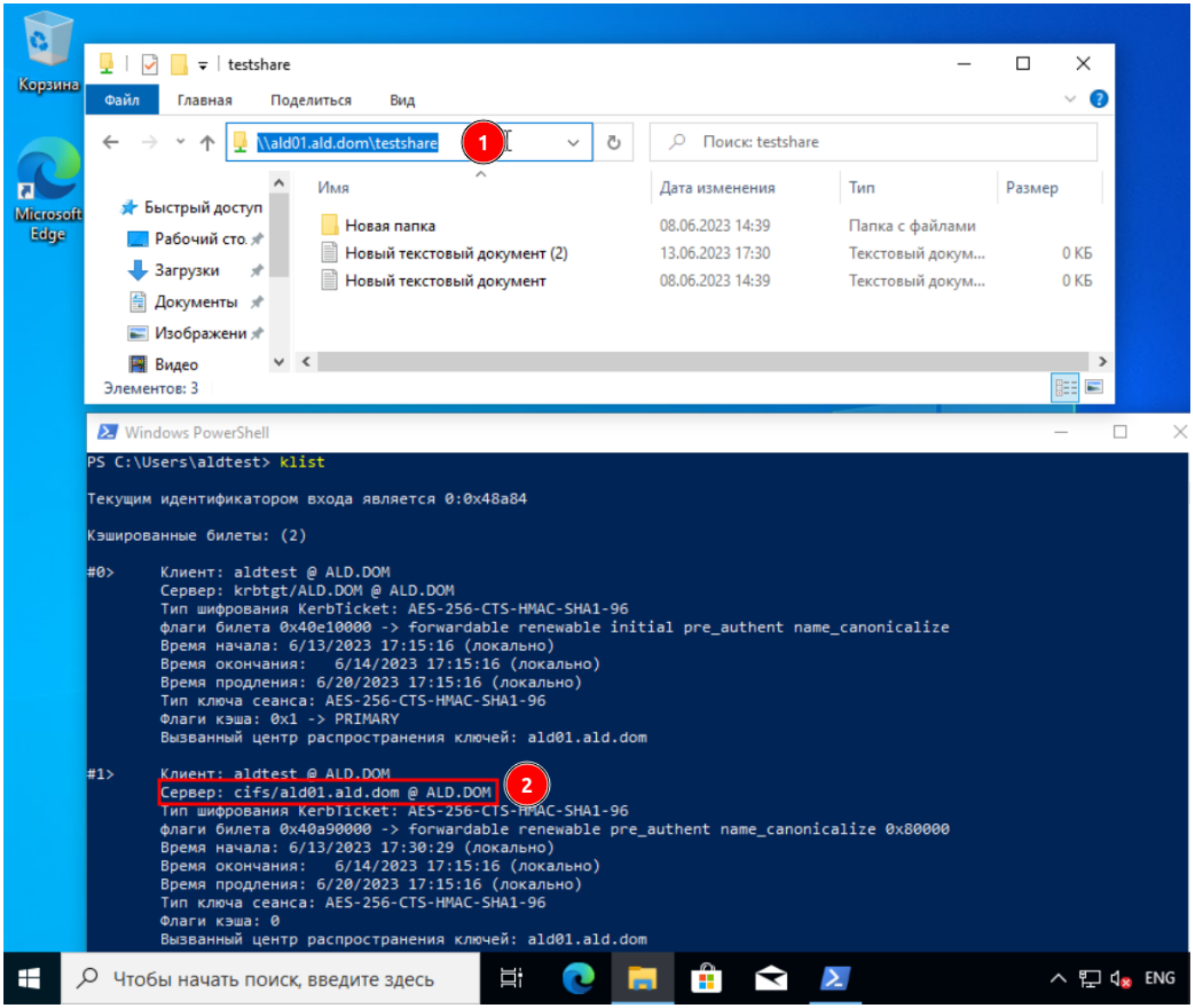


Рисунок 2.16 – Билет Kerberos

2.39.5. Добавление доменных(ALD Pro) пользователей или групп в локальные группы Windows

Скачать пакет WMF 5.1 для той операционной системы и архитектуры, в которой будет производиться установка.

Операционная система	Предварительные требования	Ссылка на пакеты
Windows Server 2012 R2		Win8.1AndW2K12R2-KB3191564-x64.msu
Windows Server 2012		W2K12-KB3191565-x64.msu
Windows Server 2008 R2	.NET Framework 4.5.2	Win7AndW2K8R2-KB3191566-x64.ZIP
Windows 8.1	x64:Win8.1AndW2K12R2-KB3191564-x64.msu, x86:Win8.1-KB3191564-x86.msu	
Windows 7 с пакетом обновления 1 (SP1)	.NET Framework 4.5.2	x64:Win7AndW2K8R2-KB3191566-x64.ZIP, x86:Win7-KB3191566-x86.ZIP

https://learn.microsoft.com/ru-ru/powershell/scripting/windows-powershell/wmf/setup/install-configure?view=powershell-7.3#download-and-install-the-wmf-51-package

Используя wbinfo

```
root@ald01:~# wbinfo -n "ald\admin"
S-1-5-21-109148531-2531787706-4107538291-500 SID_USER (1)
```

Используя ipa command

```
root@ald01:~# ipa user-show admin --all | grep ipantsecurityidentifier
  ipantsecurityidentifier: S-1-5-21-109148531-2531787706-4107538291-500
```

Используя ipa command

```
root@ald01:~# ipa group-show group_high --all | grep ipantsecurityidentifier
  ipantsecurityidentifier: S-1-5-21-109148531-2531787706-4107538291-1007
root@ald01:~#
root@ald01:~# ipa group-show group_high --all
  dn: cn=group_high,cn=groups,cn=accounts,dc=ald,dc=dom
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
  Имя группы: group_high
  ID группы: 995400007
  Группы-участники: group_low
  Пользователи с непрямым участием: alduser, aldtest
  ipantsecurityidentifier: S-1-5-21-109148531-2531787706-4107538291-1007
  ipauniqueid: d1410fd4-0a8c-11ee-9d12-422c2492509f
  objectclass: top, groupofnames, nestedgroup, ipausergroup, ipaobject, x-ald-
↪audit-policy, rbta-unit, posixgroup, ipantgroupattrs
```

```
Windows PowerShell (C) Корпорация Майкрософт (Microsoft Corporation). Все
↪права защищены.

Попробуйте новую кроссплатформенную оболочку PowerShell (https://aka.ms/
↪pscore6)

PS C:\Windows\system32> Add-LocalGroupMember -Group 'Пользователи удаленного
↪рабочего стола' -Member 'S-1-5-21-109148531-2531787706-4107538291-500'
```

Наиболее популярные разрешения:

r = чтение

rx = Чтение, Выполнение, Список содержимого папки

rxm = Чтение, Выполнение, Список содержимого папки, Запись, Изменение

f = Полный доступ

(OI) = Для этой папки и её файлов

(CI) = Для этой папки и её подпапок

Таким образом, чтобы дать обычные права на чтение и запись на папку, используются разрешения (OI)(CI)rxm. То есть результирующая команда будет выглядеть так:

PowerShell или CMD

```
ICACLS "C:\Temp" /grant "*S-1-5-21-109148531-2531787706-4107538291-
↪500:(OI)(CI)rxm"
```

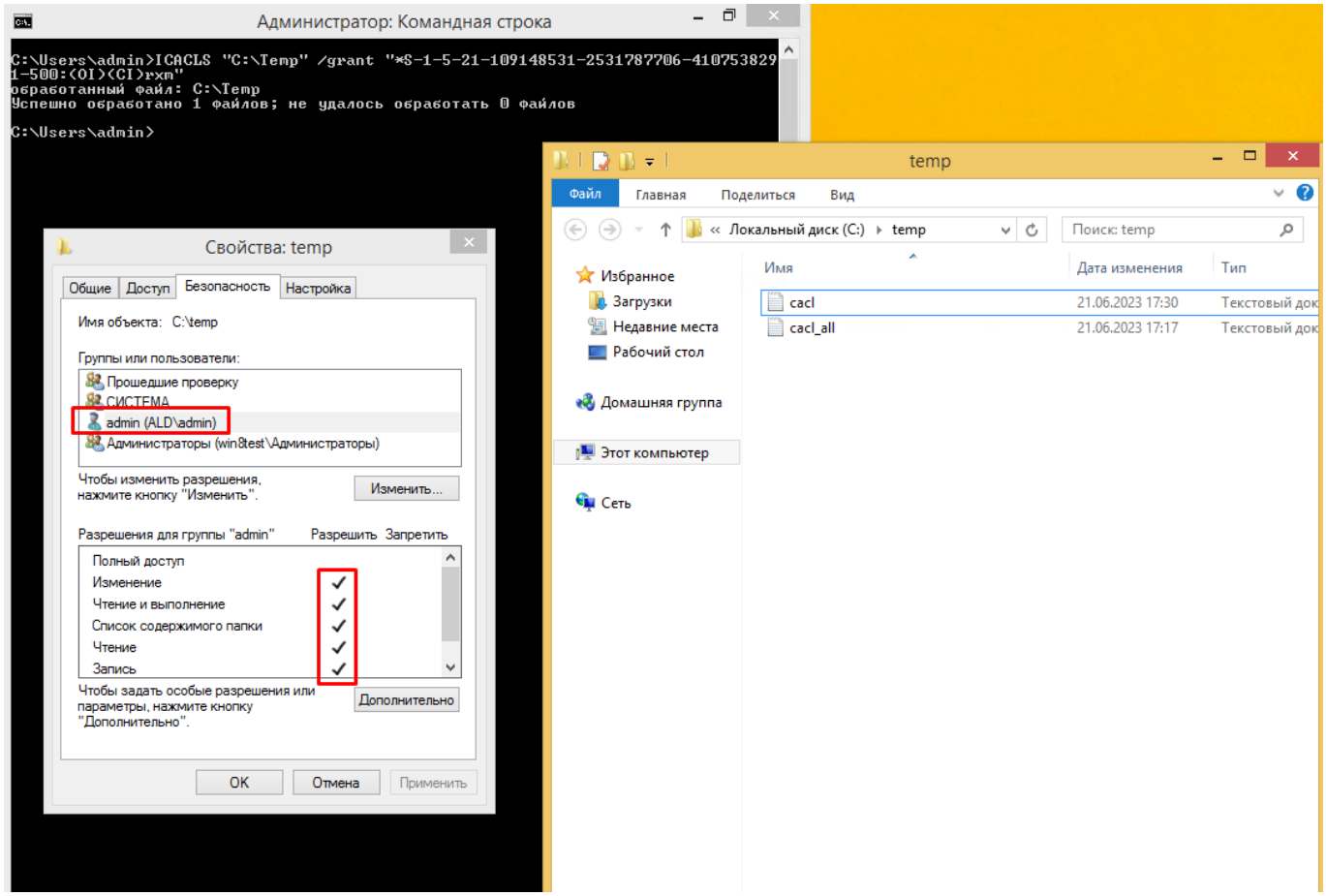


Рисунок 2.17 – Результат работы команд

Более детальная информация может быть найдена на сайте Microsoft:

https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/icacls

К сожалению в текущей реализации не поддерживается прямое добавление доменных групп в дискретные списки доступа (DACL).

Для того, чтобы обойти это ограничение:

1. Создать соответствующую доменной локальную группу.
2. В локальную группу добавить SID доменной группы (см. Добавление доменных(ALD Pro) пользователей или групп в локальные группы Windows).
3. Добавить в безопасность папки или файла локальную группу, которую создали в п. 1.

```
Alddom_fs_c_temp_r

Alddom_fs_c_temp_rw
```