



ИНСТРУКЦИИ

УСТАНОВКА ДОВЕРИТЕЛЬНЫХ ОТНОШЕНИЙ МЕЖДУ MICROSOFT ACTIVE DIRECTORY И ALD PRO

Версия 2.4.1

Содержание

1	Аннотация	4
2	Предварительные требования	5
2.1	Постановка задачи	5
2.2	Подготовка контролера домена ALD Pro	6
2.3	Подготовка контроллера домена MS	11
2.4	Контрольный список межлесного доверия	12
2.5	Контролеры доверия и агенты доверия (Trust controllers and trust agents)	13
2.5.1	Контролеры доверия	13
2.5.2	Агенты доверия	13
2.6	Проверка доступности портов	14
2.7	Взаимное перенаправление DNS-зон	17
2.8	Настройка DNS - доверительные сети (bind trusted_network)	18
2.9	Настройка времени	19
2.9.1	На стороне ALD Pro	19
2.9.2	На стороне MS AD	22
3	Создание доверительных отношений	23
3.1	Создание двустороннего доверия (Forest Trust)	23
3.2	Создание доверия между двумя доменами (External Trust)	26
3.2.1	Поддержка внешнего доверия к домену из леса MS AD	26
3.2.2	Варианты использования	26
3.2.3	Дизайн	26
3.2.4	Реализация	26
3.2.5	Создание траста (one-way trust using a trust-secret)	28
3.2.6	MS AD доверия с множеством поддоменов	34
4	Проверки работоспособности доверительных отношений	37
4.1	Проверка работоспособности доверия (id-идентификация)	37
4.2	Проверка работоспособности доверия (Kerberos)	39
4.3	Дополнительные проверки	41

4.3.1	Как работает кросс-доверительная аутентификация Kerberos (Kerberos cross-trust authentication)	42
5	Поддержка UPN (User Principal Names) для доверенных доменов (trusted_domains)	45
5.1	Включение поддержки UPN на стороне клиента	45
5.2	Проверка поддержки UPN на стороне сервера	46
5.3	Проверка работоспособности UPN через графику	47
5.4	Проверка работоспособности UPN через SSH	47
6	Настройка SSSD для связи с определенным сайтом MS AD	49
6.1	Настройка сервера ALD Pro (FreeIPA) на определенный сайт MS AD (id, logon)	49
6.2	Настройка клиента на определенный сайт MS AD (id, logon)	50
7	Диагностика SSSD	51
7.1	Настройка журналов отладки для доменов SSSD	51
7.2	Описание уровней логирования SSSD	52
7.3	Описание SSSD журналов событий	53
8	Диагностика Winbind, Samba (smbd), nmbd	56
8.1	Настройка журналов отладки	56
9	Распространенные проблемы SSSD	61
9.1	Проблемы с конфигурационным файлом SSSD.conf	61
9.2	Отсутствие групп при выполнении команды id	62
9.3	Долгое выполнение команды id	63
9.4	SSSD не удается подключиться к MS AD из-за ошибок с GSS-API	63
10	Распространенные проблемы DNS	65
11	Распространенные проблемы Trust Creation (Создание доверительных отношений)	66
12	Настройка производительности SSSD для крупных развертываний доверия	67
12.1	Настройка игнорирования участников групп (ignore_group_members)	67
12.1.1	Предварительное требование	67
12.1.2	Процедура	67
12.2	Настройка таймаута конфигурации для плагина ipa-extdom на ALD Pro (FreeIPA)-серверах	68
12.2.1	Предупреждение	69
12.2.2	Предварительное требование.	69

12.2.3 Процедура	69
12.3 Настройка максимального размера буфера для плагина ipa-extdom на ALD Pro-серверах	70
12.3.1 Предварительное требование.	70
12.3.2 Процедура	70
12.4 Настройка максимального количества экземпляров для плагина ipa-extdom на ALD Pro-серверах	71
12.4.1 Предварительное требование.	71
12.4.2 Процедура	71
12.5 Настройка SSSD в ALD Pro-клиентах для крупных доверительных развертываний IdM-AD	72
12.5.1 Предварительное требование.	72
12.5.2 Процедура	72
12.6 Монтирование кэша SSSD в tmpfs	74
12.6.1 Предварительное требование.	74
12.6.2 Процедура	75
13 Доступ пользователей ALD Pro к ресурсам MS AD	76
13.1 Создание сетевой папки в домене MS AD	76
13.2 Подключение сетевой папки на рабочей станции под управлением Astra Linux	80
13.2.1 Ограничение доступа по SID	82
13.3 Добавление пользователей и групп из ALD Pro домена в домен MS AD.	85
13.3.1 Порядок добавления пользователя или группы	85
14 Доступ пользователей MS Windows к ресурсам ALD Pro	89
15 Установка глобального каталога(в ALD Pro 2.0.0)	90

Аннотация

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.

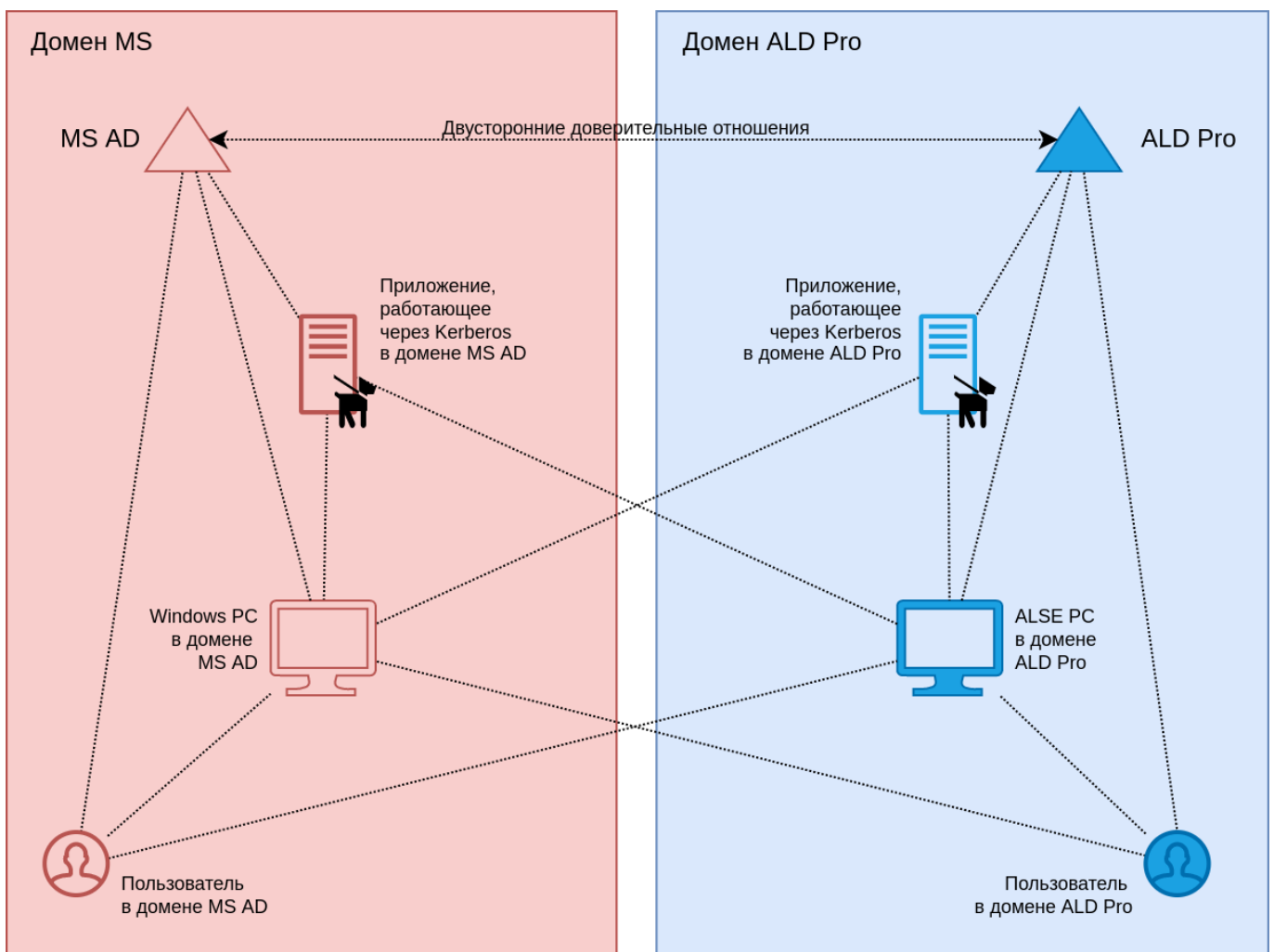
Предварительные требования

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.

Настройка сети

Введите имя этого компьютера.

Имя компьютера -- это одно слово, которое идентифицирует вашу систему в сети. Если вы не знаете каким должно быть имя вашей системы, то посоветуйтесь с администратором вашей сети. Если вы устанавливаете вашу собственную домашнюю сеть, можете выбрать любое имя.

Имя компьютера:

Настройка сети

Имя домена -- это часть вашего Интернет-адреса, справа от имени компьютера. Зачастую она заканчивается на .com, .net, .edu или .org. Если вы настраиваете сеть дома, то можете указать что-нибудь своё, но убедитесь, что используете одинаковое имя домена на всех ваших машинах.

Имя домена:

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.

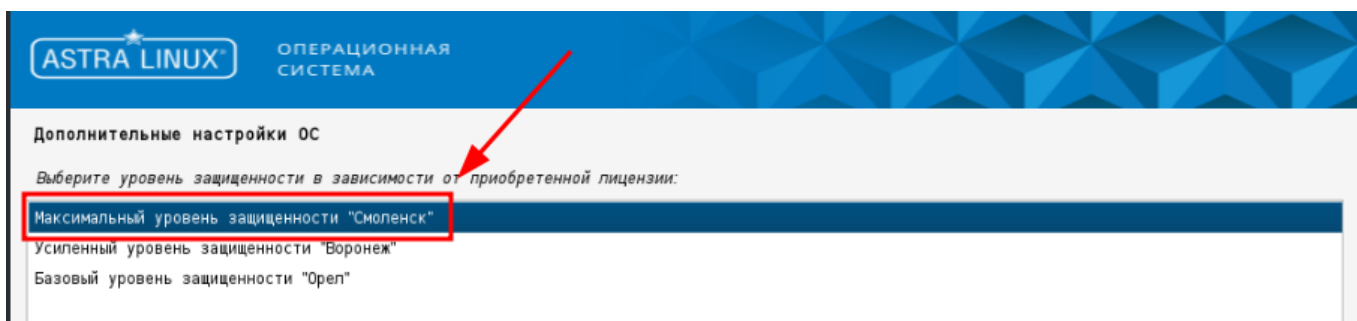
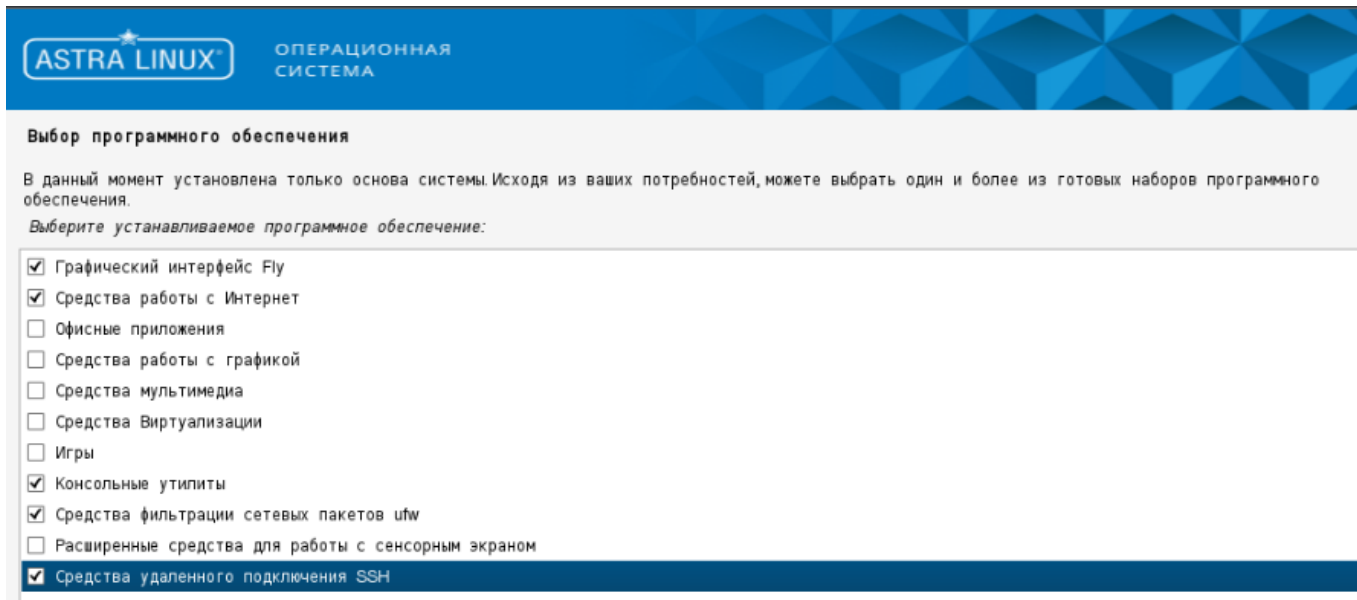
Имя учётной записи администратора:

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



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
```

(продолжение на следующей странице)

```

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
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 статическому 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
```

#Обновление файла для продвижения /etc/network/interfaces установка
→статического 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 контролера домена
set +o history
/opt/rbta/alddpro/mp/bin/alddpro-server-install.sh --setup_gc --setup_syncer -
↪d 'alldomain.lan' -n 'alddc01' -p 'Astra123' --no-reboot >/var/log/
↪promotion_alddpro_domain-controler.log
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 контролера 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 контролере домена

```
#Переименовать контролер 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 контролера домена Active Directory в новом лесу
Install-ADDSForest -DomainName windomain.lan -DomainNetBIOSName WINDOMAIN -
↪InstallDNS

#Установка forwarder на а 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 контролера доверия до агента доверия.

2.6. Проверка доступности портов

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

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

```
$Servers = "localhost#", "adcc02" #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)
```

(продолжение на следующей странице)

```

        $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)"
            }
        $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  
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

Для работы доверительных отношений с компьютеров в домене alldomain.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 alldomain.lan необходимо:

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

```
Add-DnsServerConditionalForwarderZone -Name "alldomain.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 alldomain.lan необходимо выполнить следующие команды:

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

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

- Запустить команду на контролере домена **alddc01.alldomain.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;
* };
*/

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) контролере 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□
```

(продолжение на следующей странице)

```
↪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
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 [ * ]
↪
```

Создание доверительных отношений

3.1. 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: alldomain.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.alldomain.lan
Контролёры отношений доверия AD IPA: alddc01.alldomain.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
```

(продолжение на следующей странице)


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

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:~#  
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 посмотреть, какие контролеры 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  
Контролёры 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 лесу 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.

3.2. Создание доверия между двумя доменами (External Trust)

3.2.1. 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.

3.2.2. 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.

3.2.3. 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.

3.2.4. 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)
```

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

3.2.5. 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).

3.2.5.1. Создание доверия на стороне MS AD

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:
 1. 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 «ipr trust-add»

The screenshot shows the Active Directory Domains and Trusts console with 'windomain.lan' selected. The 'windomain.lan Properties' dialog is open, with the 'General' tab selected. A green box highlights the 'New Trust...' button at the bottom left, with a red circle containing the number '2' next to it. A red circle containing the number '1' is next to the 'windomain.lan Properties' title bar. The 'New Trust Wizard' dialog is also open, with the 'Trust Name' step selected. A green box highlights the 'Name' text box containing 'alldomain.lan', with a red circle containing the number '3' next to it. The wizard provides instructions on how to create a trust and includes example names for NetBIOS and DNS.

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.



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.



Sides of Trust

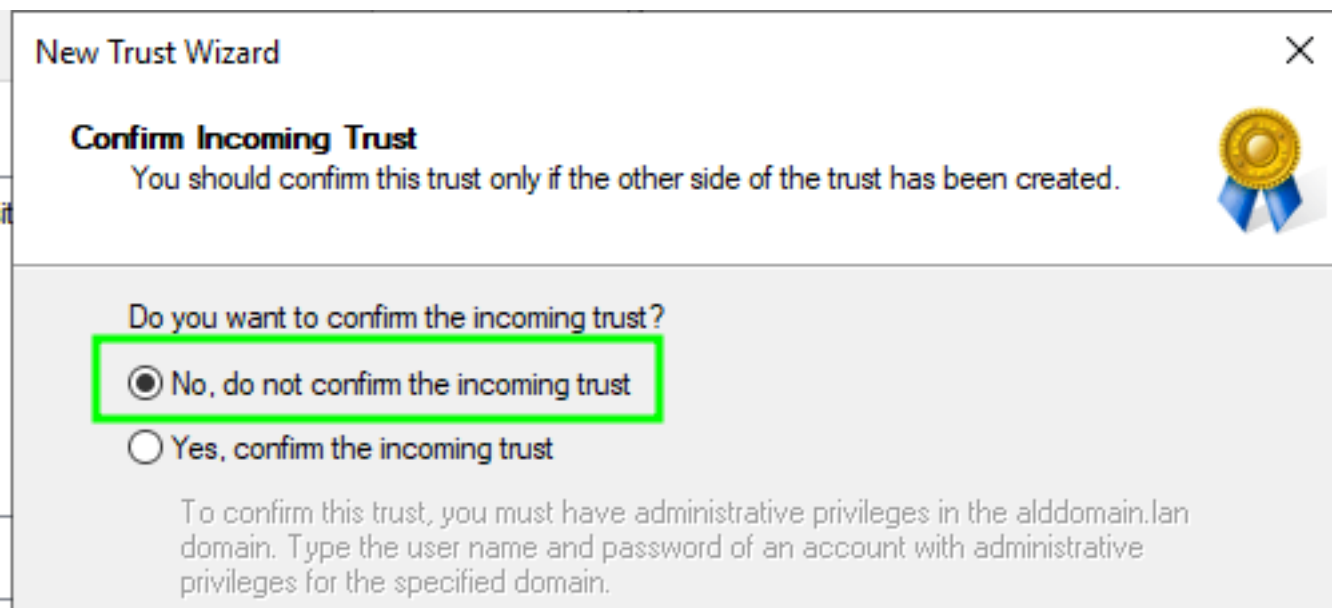
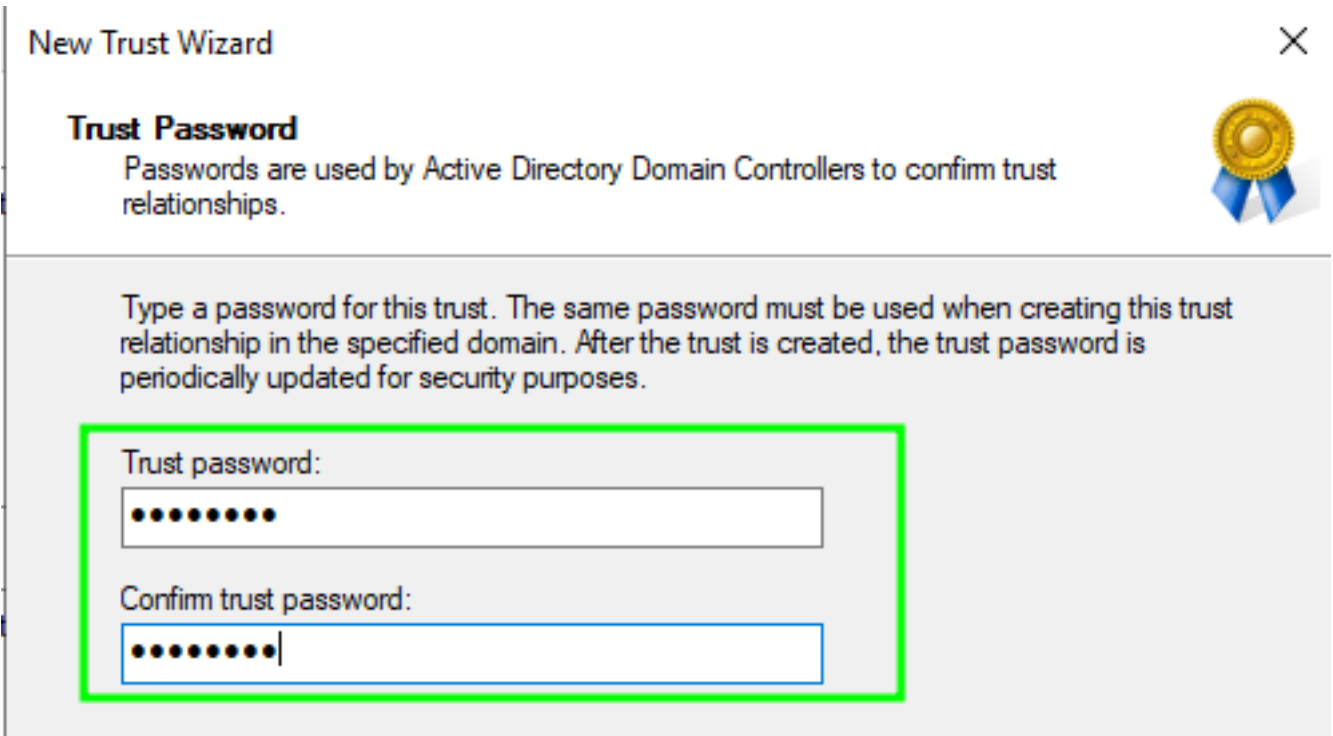
If you have appropriate permissions in both domains, you can create both sides of the trust relationship.



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.



3.2.5.2. Создание доверия на стороне ALD Pro

```
# ipa trust-add --type=ad <DomainName> --trust-secret  
root@alldc01:~# ipa trust-add --type=ad windomain.lan --trust-secret  
Общий секрет для отношения доверия:
```

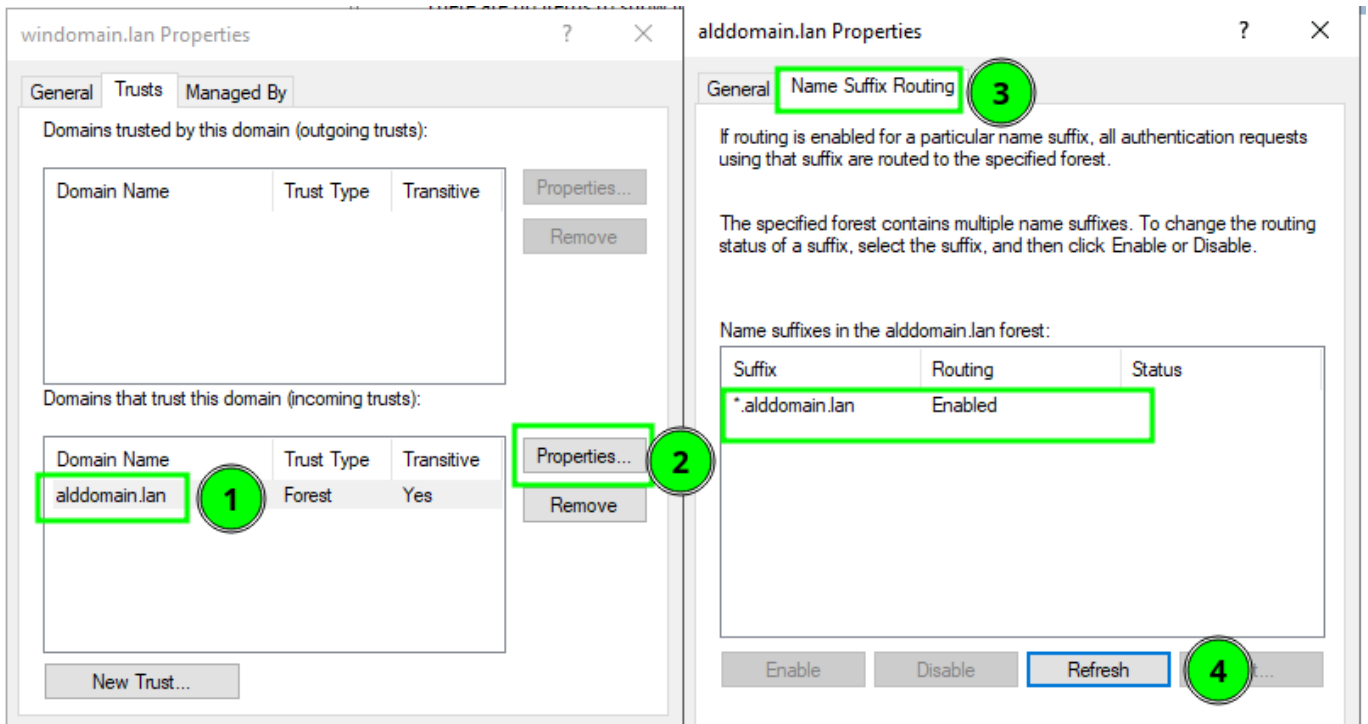
↪ --

Добавлено отношение доверия MS AD для области (realm) "windomain.lan"

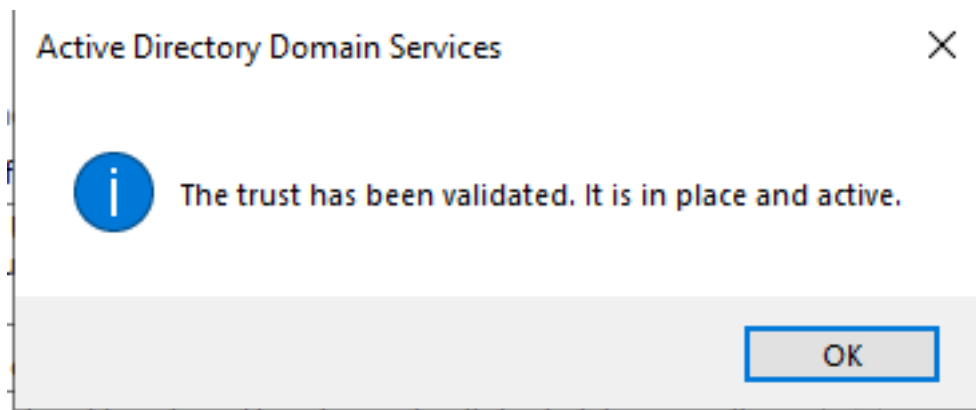
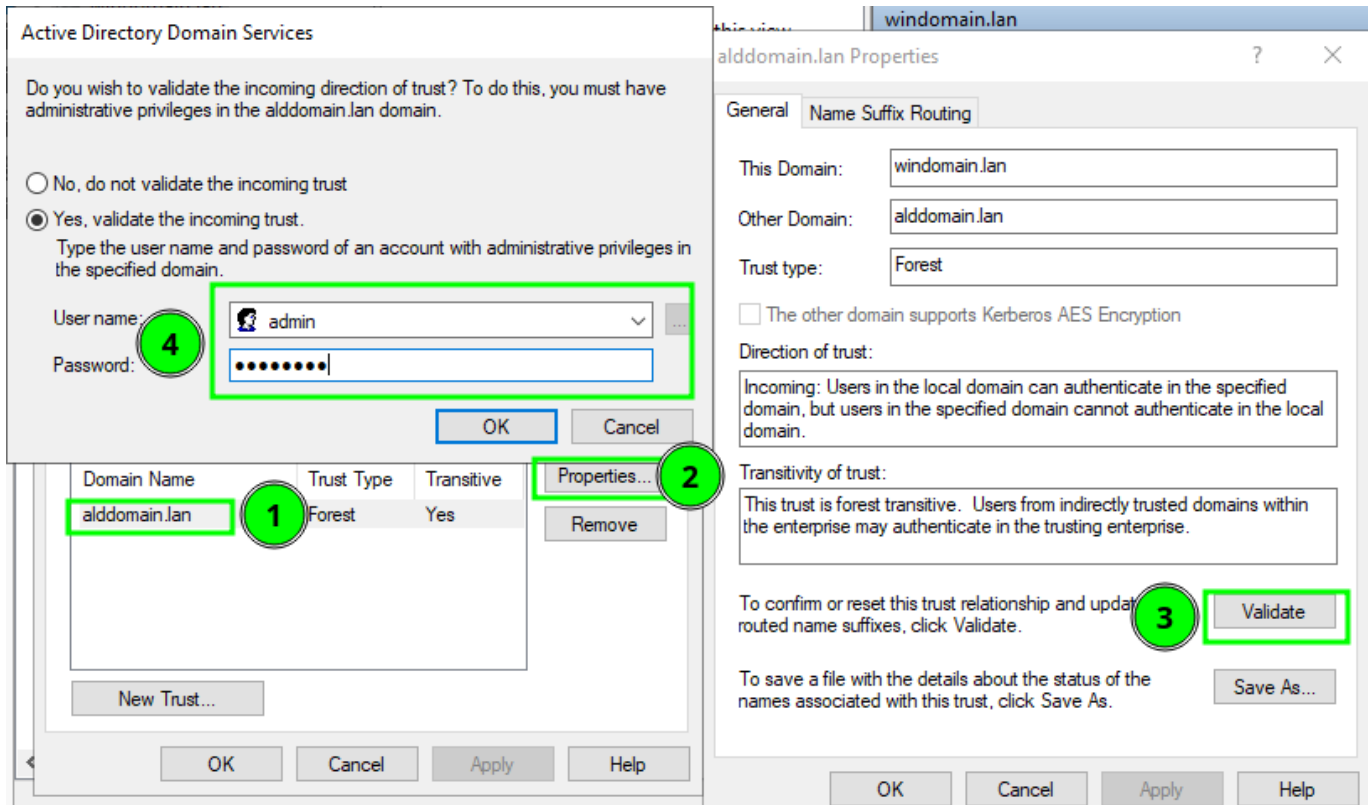
(продолжение на следующей странице)

Имя области (realm): windomain.lan
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 двустороннее доверие, то команды будут 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)

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
```

3.2.6. MS AD доверия с множеством поддоменов

В больших организациях, 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
```

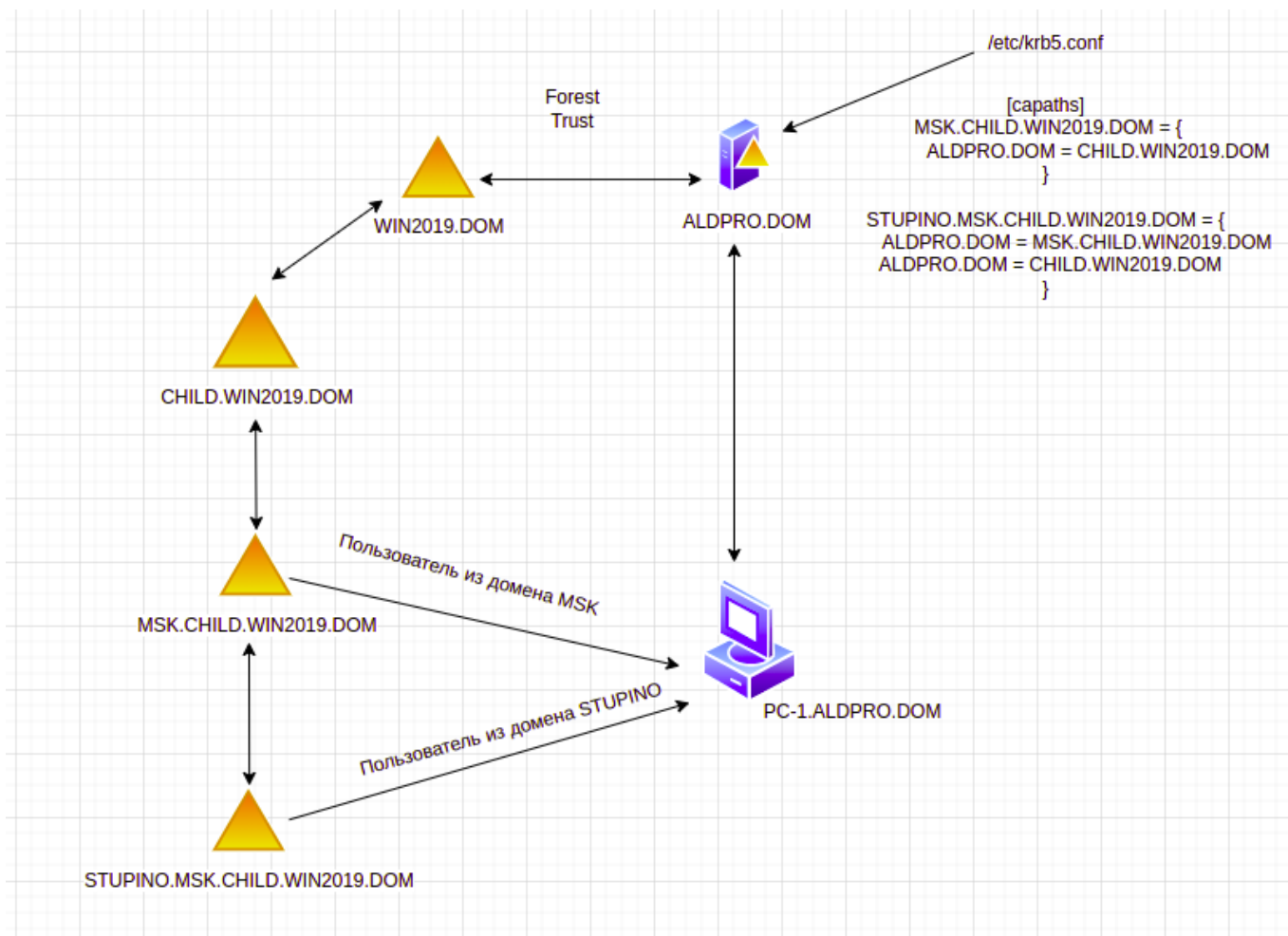
```
}
```

```
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>)

```

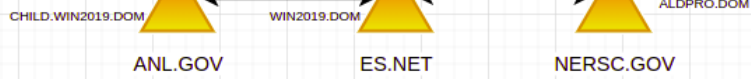
[capaths]
ANL.GOV = {
  TEST.ANL.GOV = .
  PNL.GOV = ES.NET
  NERSC.GOV = ES.NET
  ES.NET = .
}
TEST.ANL.GOV = {
  ANL.GOV = .
}
NERSC.GOV = {
  ANL.GOV = ES.NET
}
ES.NET = {
  ANL.GOV = .
}

```

```

[capaths]
NERSC.GOV = {
  ANL.GOV = ES.NET
  TEST.ANL.GOV = ES.NET
  TEST.ANL.GOV = ANL.GOV
  ES.NET = .
}
ANL.GOV = {
  NERSC.GOV = ES.NET
}
ES.NET = {
  NERSC.GOV = .
}
TEST.ANL.GOV = {
  NERSC.GOV = ANL.GOV
  NERSC.GOV = ES.NET
}

```



```

[capaths]
ALDPRO.DOM = {
  CHILD.WIN2019.DOM = WIN2019.DOM
  MSK.CHILD.WIN2019.DOM = WIN2019.DOM
  MSK.CHILD.WIN2019.DOM = CHILD.WIN2019.DOM
  WIN2019.DOM = .
}
CHILD.WIN2019.DOM = {
  ALDPRO.DOM = WIN2019.DOM
}
WIN2019.DOM = {
  ALDPRO.DOM = .
}
MSK.CHILD.WIN2019.DOM = {
  ALDPRO.DOM = CHILD.WIN2019.DOM
  ALDPRO.DOM = WIN2019.DOM
}

```

```

MSK.CHILD.WIN2019.DOM = {
  ALDPRO.DOM = CHILD.WIN2019.DOM
}

```

```

STUPINO.MSK.CHILD.WIN2019.DOM = {
  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
  }
}

```

TEST.ANL.GOV

systemctl restart krb5-kdc && systemctl restart sssd

Проверки работоспособности доверительных отношений

4.1. 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, поскольку во время проверки подлинности должен быть задан правильный набор групп, запрос на проверку подлинности также должен выполнить поиск идентификатора, обычно операцию initgroups, перед проверкой подлинности:

1. Убедиться, что все AldPro контролеры отображаются при выполнении команды **ipa trustconfig-show**

```
#Выполнить аутентификацию
kinit admin
#Показать какие контролеры 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
```

(продолжение на следующей странице)

```
GUID домена: 7a522ccc-a0d7-4eac-a46a-46b12c93fa0e
Резервная основная группа: Default SMB Group
Агенты отношений доверия AD IPA: alddc01.alldomain.lan alddcXX.alldomain.lan
Контролёры отношений доверия AD IPA: alddc01.alldomain.lan alddcXX.alldomain.
↳lan
#Показать созданный траст
ipa trust-find windomain.lan
#Показать Направление отношения доверия
ipa trust-show windomain.lan
```

Если контролер AldPro не указан в списке, то требуется проверить наличие ошибок в логах на проблемном контролере

```
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)
```

4.2. 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 принцепала).

```
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
↳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
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
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
```

4.3. 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.
↳alldomain.lan
kvno host/alddc01.alldomain.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
```

(продолжение на следующей странице)

```

#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_B4jH9C0
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

```

4.3.1. 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 иностранного домена. Чтобы продемонстрировать, как выполняются запросы тикетов в разных доверительных системах, в этом разделе основное внимание уделяется *semperis* (лабораторный лес).

4.3.1.1. Терминология Kerberos

TGT (Ticket Granting Ticket) = Билет, выдающий билет, предоставляется DC прошедшему проверку подлинности пользователю. TGT используется для запроса билетов на обслуживание. Может использоваться для аутентификации в сервисах.

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

4.3.1.2. Kerberos cross-trust authentication



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)

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 Kerberos 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 principal), даже если его домен Active Directory назван REGION.EXAMPLE.COM.

5.1. 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/sss/sss.conf
```

```
[domain/windomain.lan]
```

(продолжение на следующей странице)

```
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
```

5.2. 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 enterprise 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 контролер видит необходимый суффикс

```
#Выполняем аутентификацию
kinit admin

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

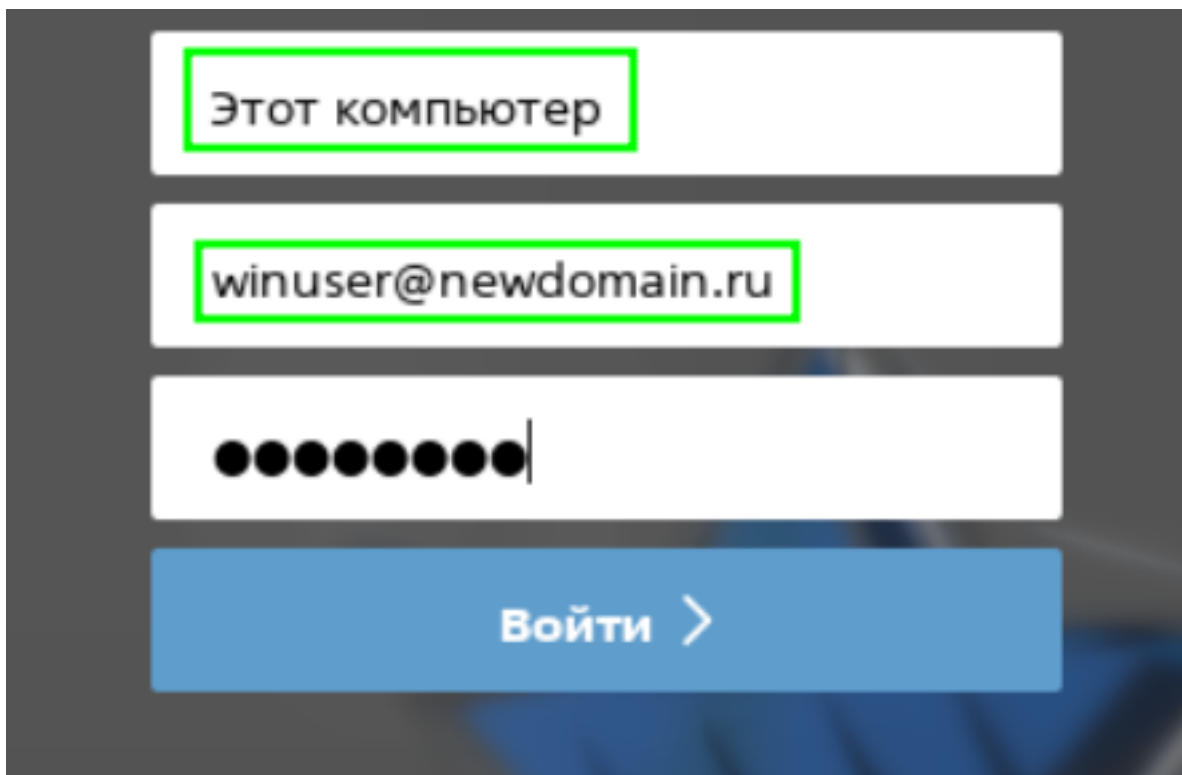
#Получить информацию по домену
ipa trustdomain-find

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

#Пример результата
```

```
root@a1ddc01:~# 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
```

5.3. Проверка работоспособности UPN через графику



5.4. 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) □
```


(продолжение с предыдущей страницы)

```
↪ группы=1524001110(winuser@windomain.lan),1524000513(domain users@windomain.  
↪lan)
```

Настройка SSSD для связи с определенным сайтом MS AD

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/sss/sss.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/sss/sss.conf`. Заголовки разделов доверенного домена соответствуют этому шаблону:

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

6.1. 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**.

6.2. 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]
allowed_uids = 0, 33, 114, fly-dm, ipaapi
[secrets]
[session_recording]
[domain/alddomain.lan/windomain.lan]
ad_site = Default-First-Site-Name
```

Диагностика SSSD

Расположение конфигурационных файлов

```
SSSD
/etc/sss/sss.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
```

7.1. 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/sss/sss.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/alldomain.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
```

7.2. 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.

7.3. Описание SSSD журналов событий

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

SSSD создает файл журнала для каждого домена, а также файл *sssdl_pam.log* и *sssdl_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.

sssdl_<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.

sssdl_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/sss/sss.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 контролеру Active Directory подключен Winbind
wbinfo --dsgetdcname=windomain.lan
#Проверка активных подключений через Winbind
wbinfo --online-status

#Проверка работоспособности службы SSSD
sss -d4 -i
#Вывести список доменов которые видит SSSD
sssctl domain-list
```

(продолжение на следующей странице)

```
#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/sss/*
#Удаление всего кеша с контролера 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
↳Inforpipe 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
```


Диагностика Winbind, Samba (smbd), nmbd

8.1. 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 **перепрет** 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 2,2М
-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 команда 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
```

(продолжение на следующей странице)

```
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 интерактивно 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 acs: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

```

Распространенные проблемы SSSD

9.1. Проблемы с конфигурационным 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
```

```
[sssд] [ldb] (3): server_sort:Unable to register control with rootdse!
```

```
[sssд] [confdb_get_domains] (0): No domains configured, fatal error!
```

```
[sssд] [get_monitor_config] (0): No domains configured.
```

Необходимо отредактировать файл /etc/sssд/sssд.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:

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

Необходимо отредактировать файл /etc/sssд/sssд.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/sssд/sssд.conf. Если службы перечислены в нескольких записях, SSSD распознает только последнюю запись.

SSSD также требует, чтобы для /etc/sssд/sssд.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]
[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/sss/sss.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/sss/sss.conf:

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

9.2. 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
```

Если количество превышает 200 000 – выполнить расширение диапазона

```
#Показать текущие диапазоны (idrange) для всех доменов
# Произвести аутентификацию
kinit admin
#Вывести список доступных диапазонов
ipa idrange-find
#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 контролера домена и перезапуск службы sssd
rm -f /var/lib/sss/db/* /var/lib/sss/mc/* && systemctl restart sssd
```

9.3. Долгое выполнение команды id

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

Решение. Одной из причин может быть большая вложенность групп

```
#Выполните команду id с параметром -G(вывести все ID групп)- эта команда  
→игнорирует вложенность групп  
id -G winuser@windomain.lan  
  
#Если команда отработывает быстро то требуется добавить в существующую  
→секцию в /etc/sss/sss.conf на каждом контролере 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
```

9.4. 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/AEXAMPLE]  
debug_level = 0xFFF0  
id_provider = ad  
ad_server = 172.16.0.1  
ad_domain = example.com
```

(продолжение на следующей странице)


```
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.

Распространенные проблемы DNS

AldPro(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 контролере 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 контролере домена ALD Pro (FreeIPA) /etc/bind/ipa-options-ext.conf Пример: allow-recursion { trusted_network; }; allow-query-cache { trusted_network; };

Распространенные проблемы Trust Creation (Создание доверительных отношений)

№ Проблема	Решение
<p>Ошибка 3221225485 при создании доверительных отношений:</p> <p>ipr: 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»)</p>	<p>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 ipr-adtrust-instal, предварительно сделав копию файла конфигурации smb.conf cp smb.conf{,_bkr}, так как он будет перезаписан из шаблона.</p>

Настройка производительности SSSD для крупных развертываний доверия

12.1. 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).

12.1.1. Предварительное требование

Необходимы права root для редактирования конфигурационного файла `/etc/sss/sss.conf`.

12.1.2. Процедура

1. Открыть конфигурационный файл `/etc/sss/sss.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 закрыть файл `/etc/sss/sss.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 `sss.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.

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

Клиенты AldPro 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).

12.2.1. 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.

12.2.2. Предварительное требование.

Пароль менеджера каталогов LDAP (LDAP Directory Manager password)

12.2.3. 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
```

(продолжение на следующей странице)

```
↪ipaExtDomMaxNssTimeout: 20000
```

12.3. 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).

12.3.1. Предварительное требование.

Пароль менеджера каталогов LDAP (LDAP Directory Manager password)

12.3.2. 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
```

12.4. 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/sss/sss_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]
→(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.

12.4.1. Предварительное требование.

Пароль менеджера каталогов LDAP (LDAP Directory Manager password)

12.4.2. 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 AldPro и, если она не улучшится, повторить эту процедуру и отрегулировать значение переменной `ipaExtdomMaxInstances`.

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

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

12.5.1. Предварительное требование.

Нужны права `root` для редактирования конфигурационного файла `/etc/sss/sss.conf`.

12.5.2. Процедура

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

a) Очистить кэш SSD на AldPro-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 войнb 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/sss/sss.conf` в текстовом редакторе.

3. Добавить следующие параметры в раздел [домен] для домена MS AD. Установить параметры `ram_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 [ram]:

```
[ram]
ram_id_timeout = 9
```

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

6. Перезапустить службу SSSD, чтобы загрузить изменения конфигурации.

```
systemctl restart sssd
```

12.6. 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.

12.6.1. Предварительное требование.

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

12.6.2. 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:sss_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.

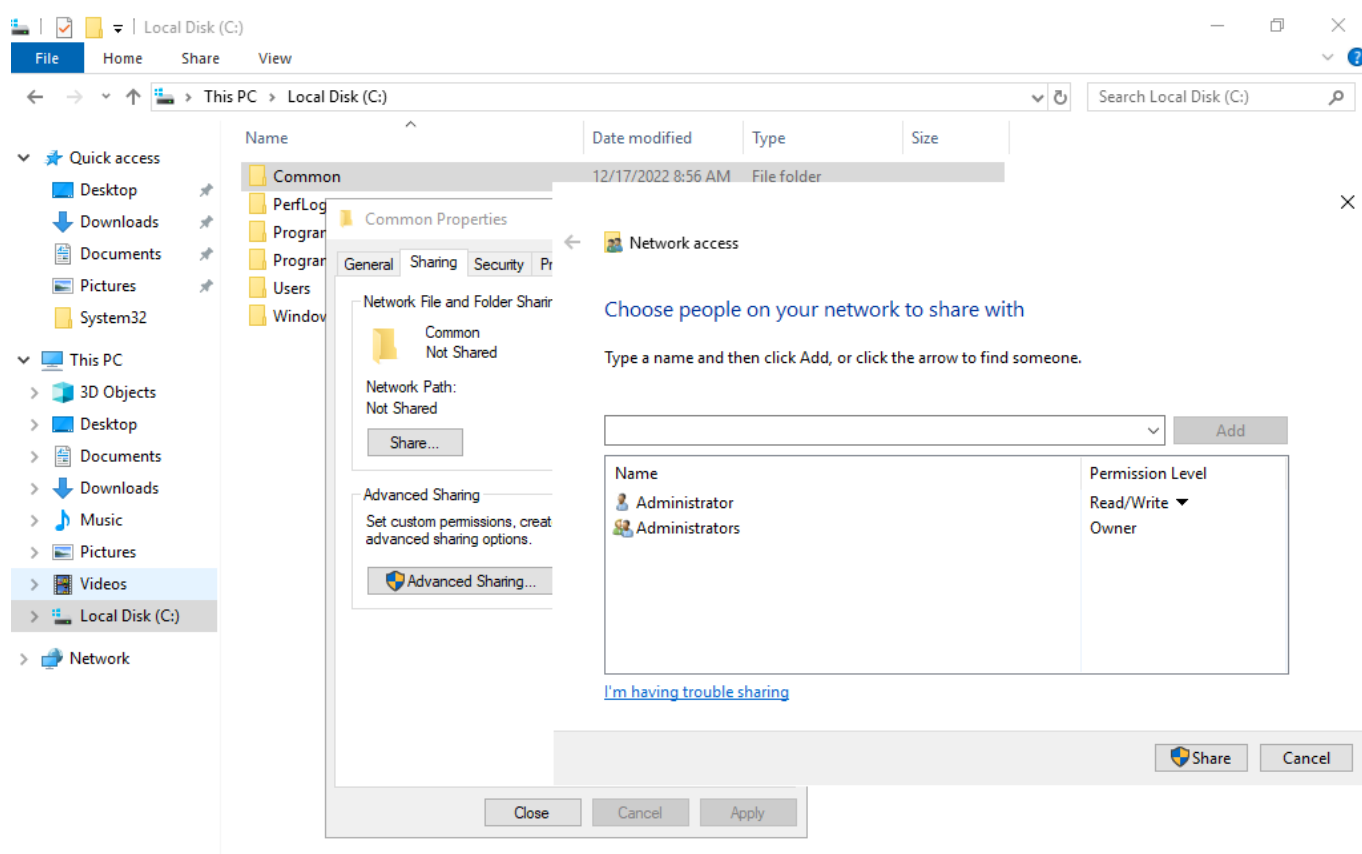
Минусы: Кэш не сохраняется при перезагрузках. Это означает, что кэш должен быть восстановлен после перезагрузки компьютера, но также и то, что `cachedpassword` теряются после перезагрузки.

Доступ пользователей ALD Pro к ресурсам MS AD

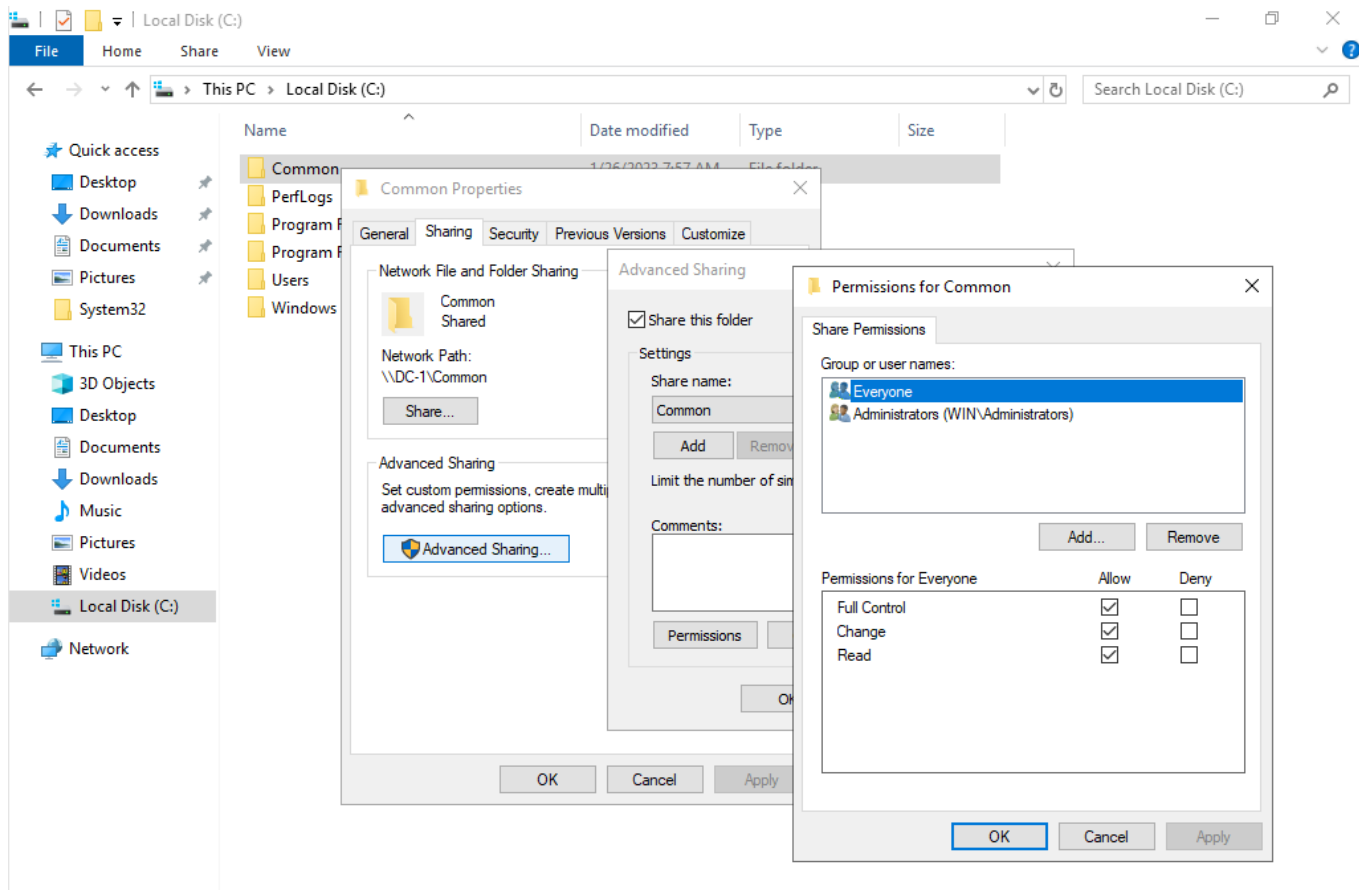
13.1. Создание сетевой папки в домене MS AD

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

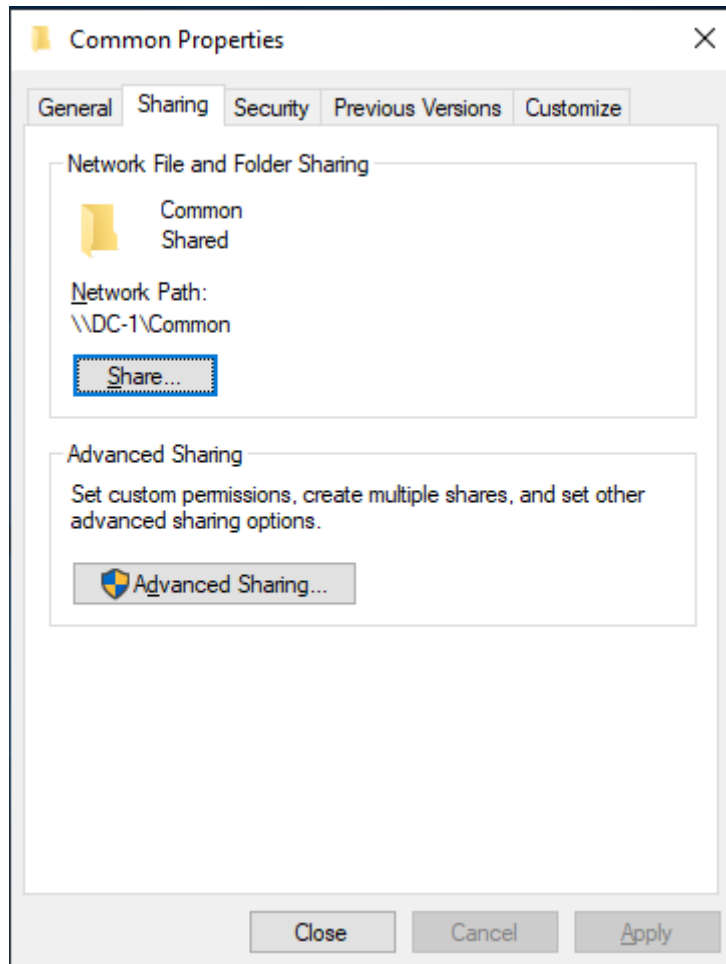
Создать папку C:Common, в свойствах на закладке «Sharing» выбрать «Share» и в окне «Network access» выбрать «Share», оставив все по умолчанию.

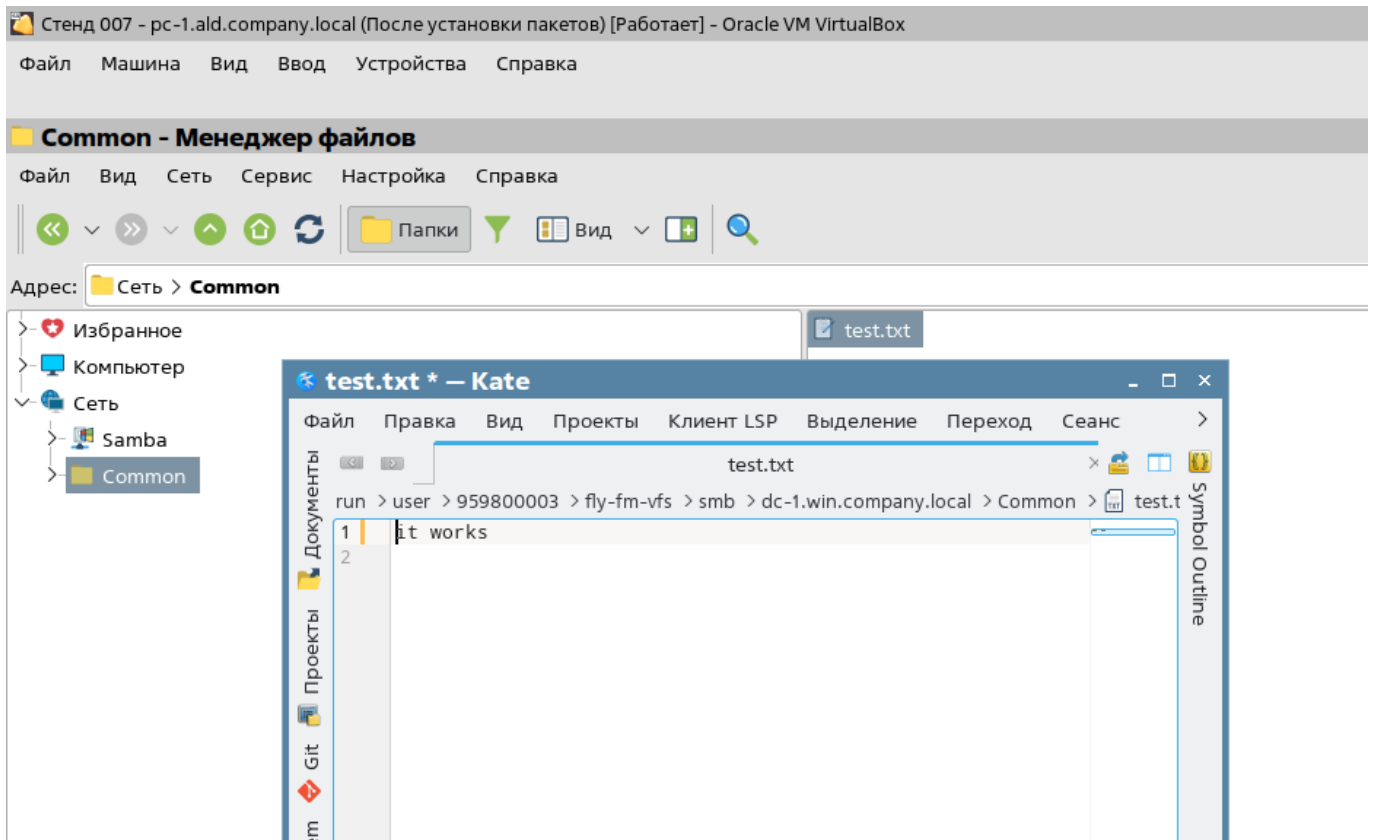
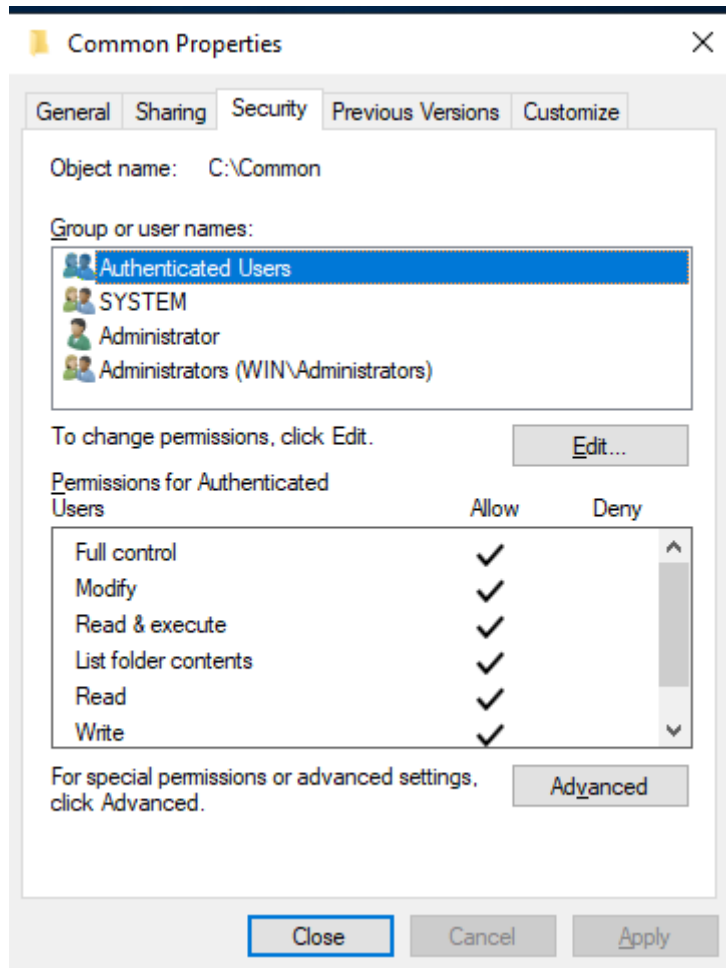


Если открыть окно «Common PropertiesSharingAdvanced SettingsPermissions», то будет видно, что по умолчанию на уровне SMB все пользователи имеют полные права.



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.





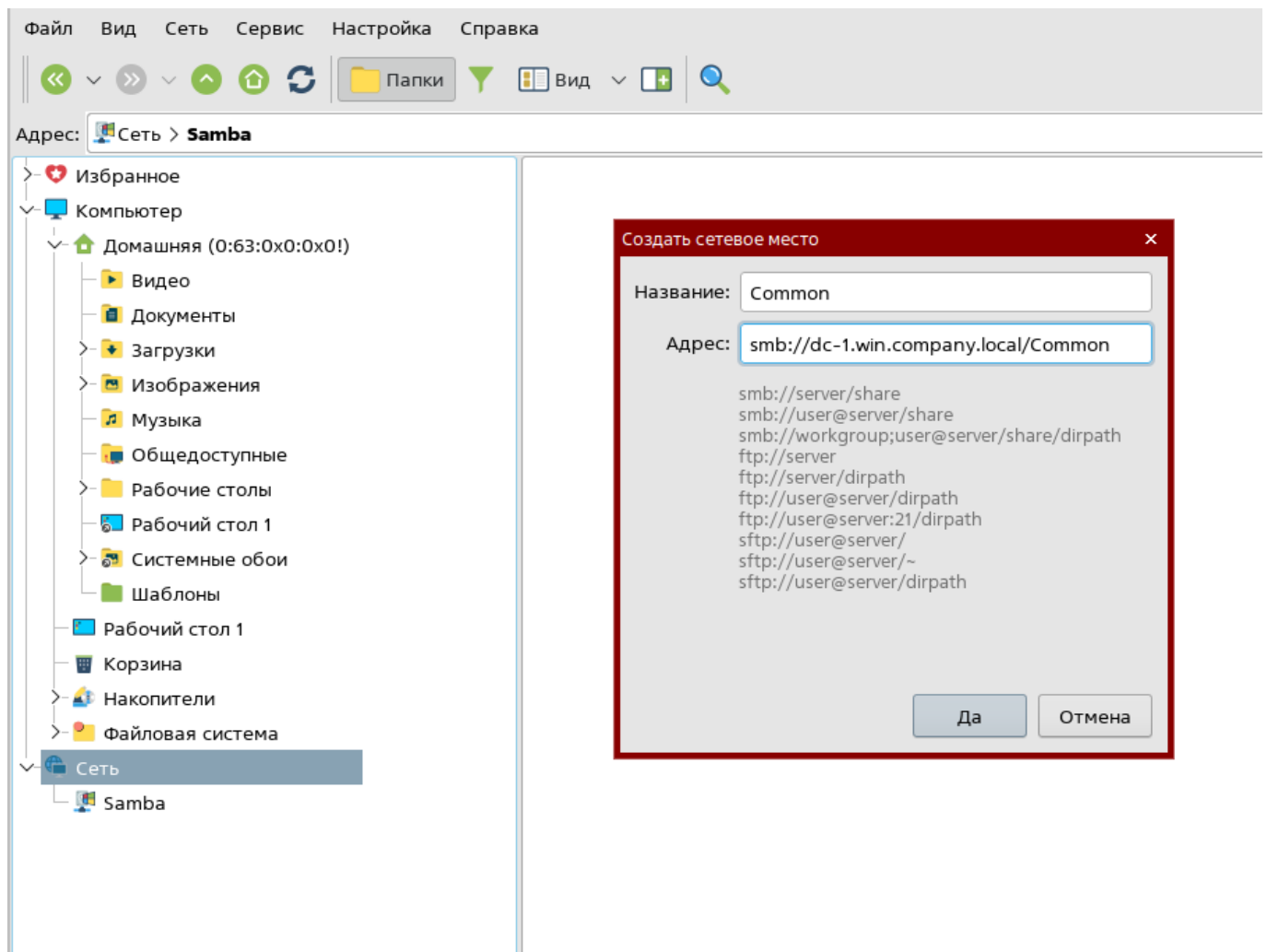
13.2. Подключение сетевой папки на рабочей станции под управлением Astra Linux

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/sss/sss.conf нужно добавить параметр krb5_use_fast = never

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

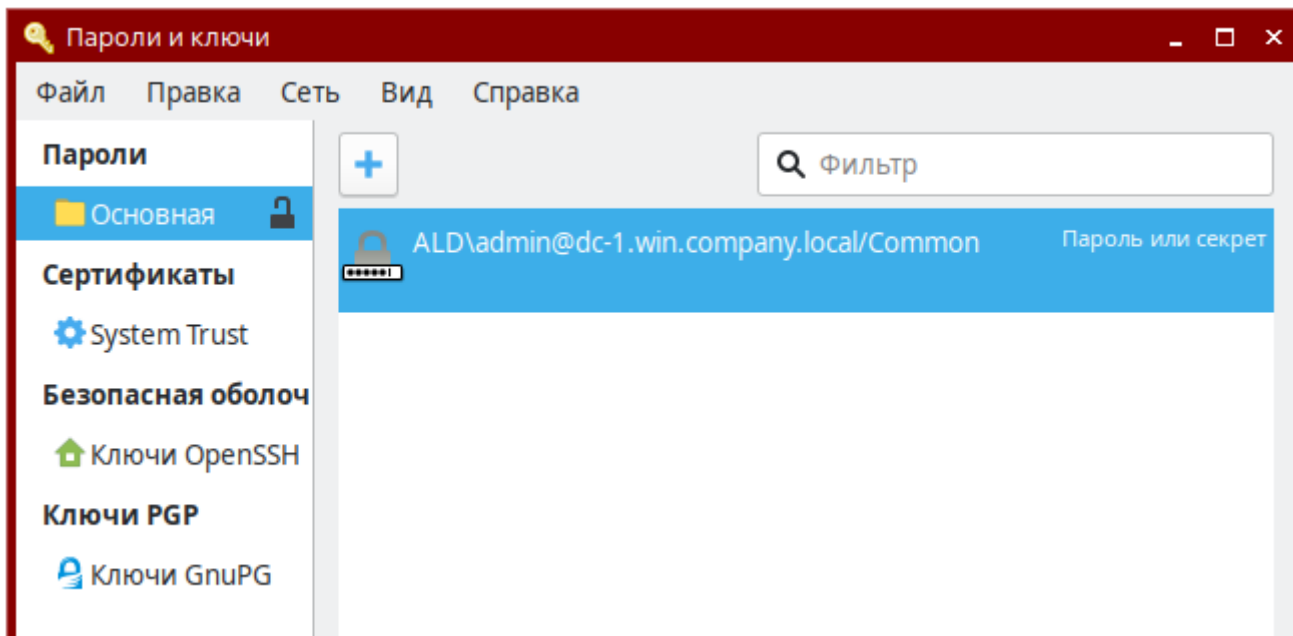
На стороне контроллера домена ALD Pro в файле /etc/krb5.conf.d/freeipa закомментировать параметр spake_preauth_groups. При установке модуля глобального каталога скриптом ipa-gc-install.py отключение этого параметра будет выполнено автоматически с помощью ключа –disable-fast-preauth.

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 участников 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 «ALDadmin» в формате «ДОМЕНИмя_пользователя».

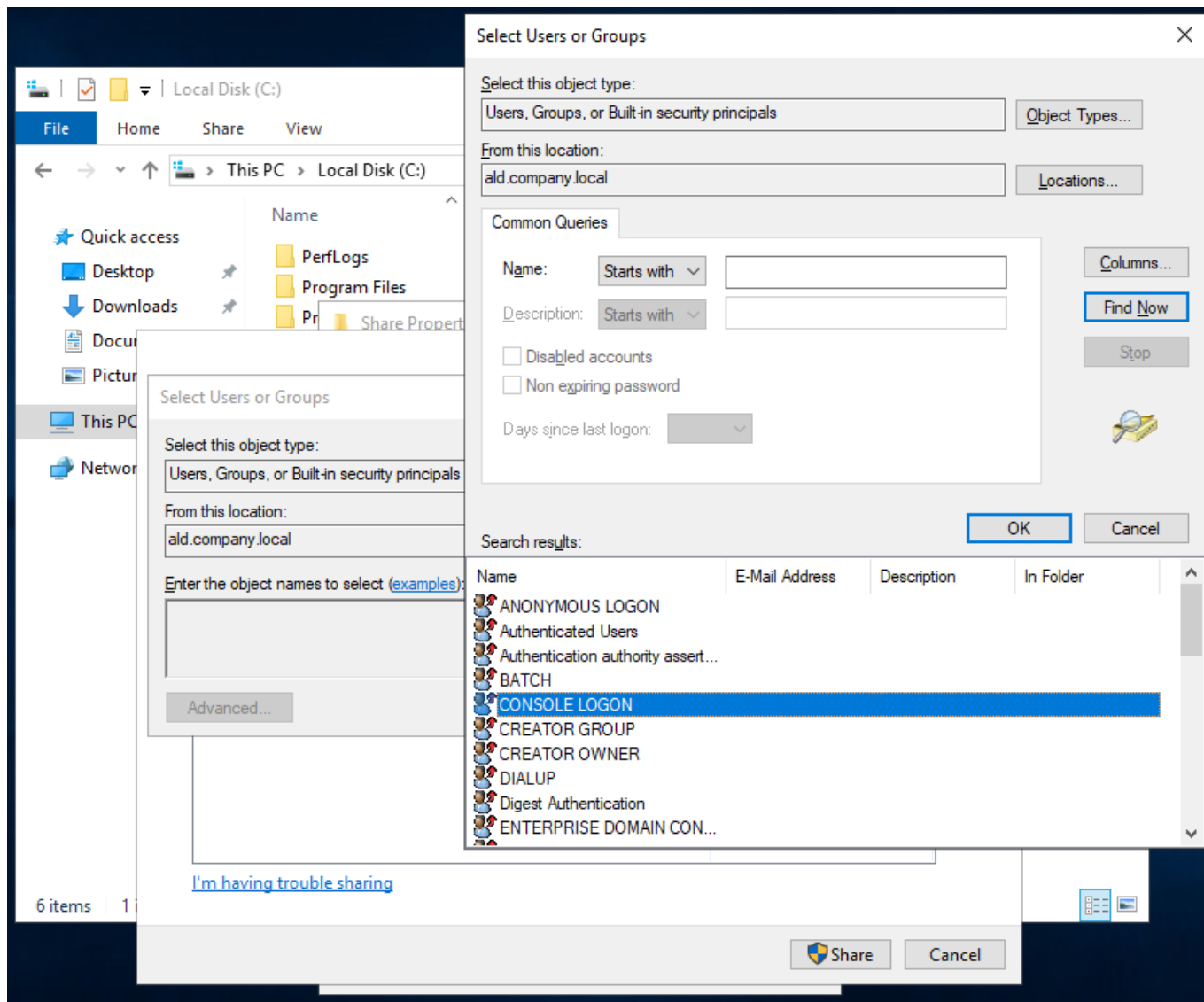
Система предложит сохранить учетные данные в связке ключей, для работы с которой можно воспользоваться приложением seahorse «Пароли и ключи»

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



13.2.1. 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 удастся.



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 контролере 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».

13.3. 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.](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.)


13.3.1. 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

Object	Security	Attribute Editor	
General	Members	Member Of	Managed By

 Contoso-Group-DL

Group name (pre-Windows 2000):

Description:

E-mail:

Group scope

Domain local

Global

Universal

Group type

Security

Distribution

Notes:

3. На стороне MS AD на контролере 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'

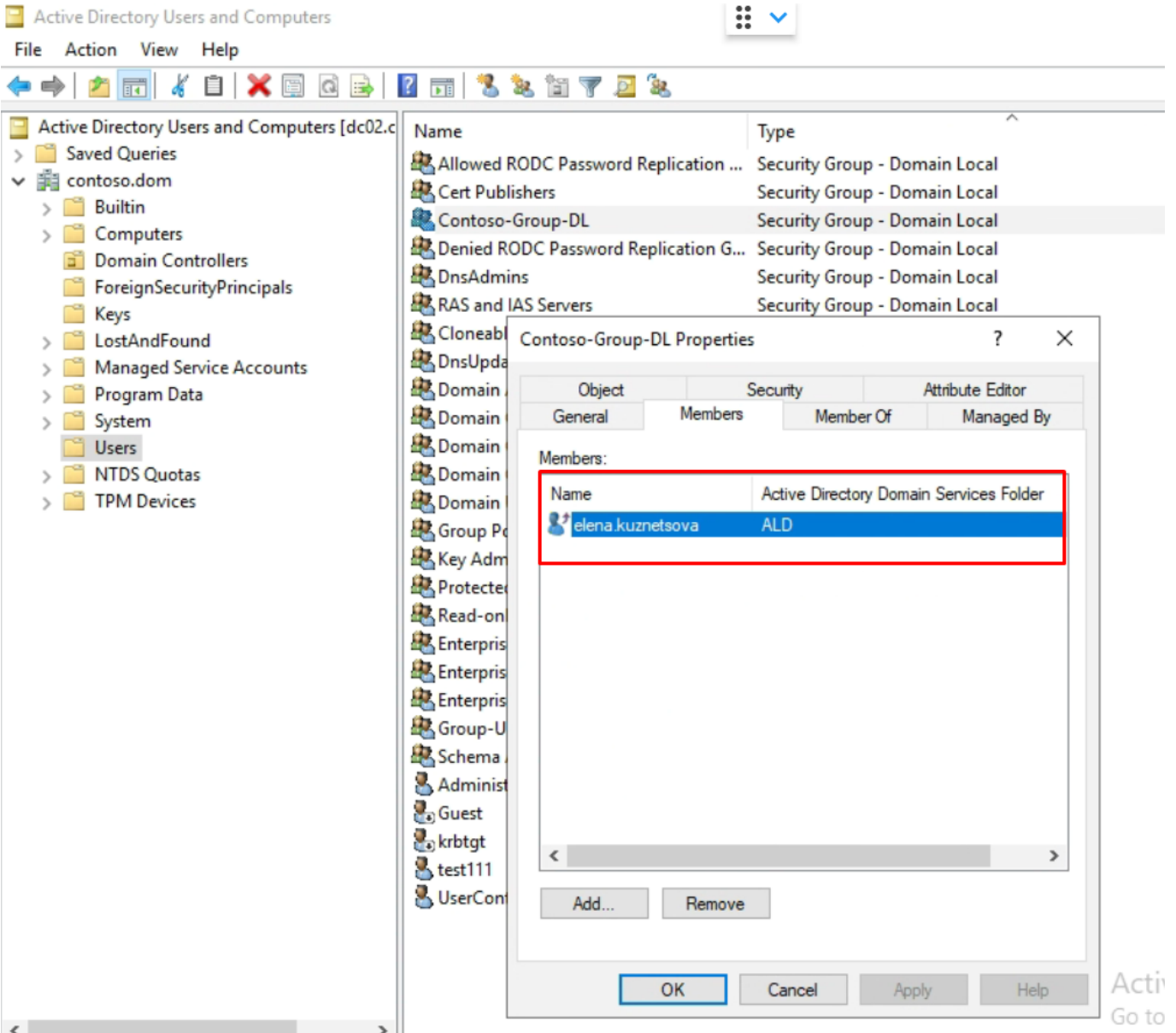
#Domain Local Group из леса Active Directory
$DomainLocalGroupDN = 'CN=Contoso-Group-DL,CN=Users,DC=contoso,DC=dom'

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

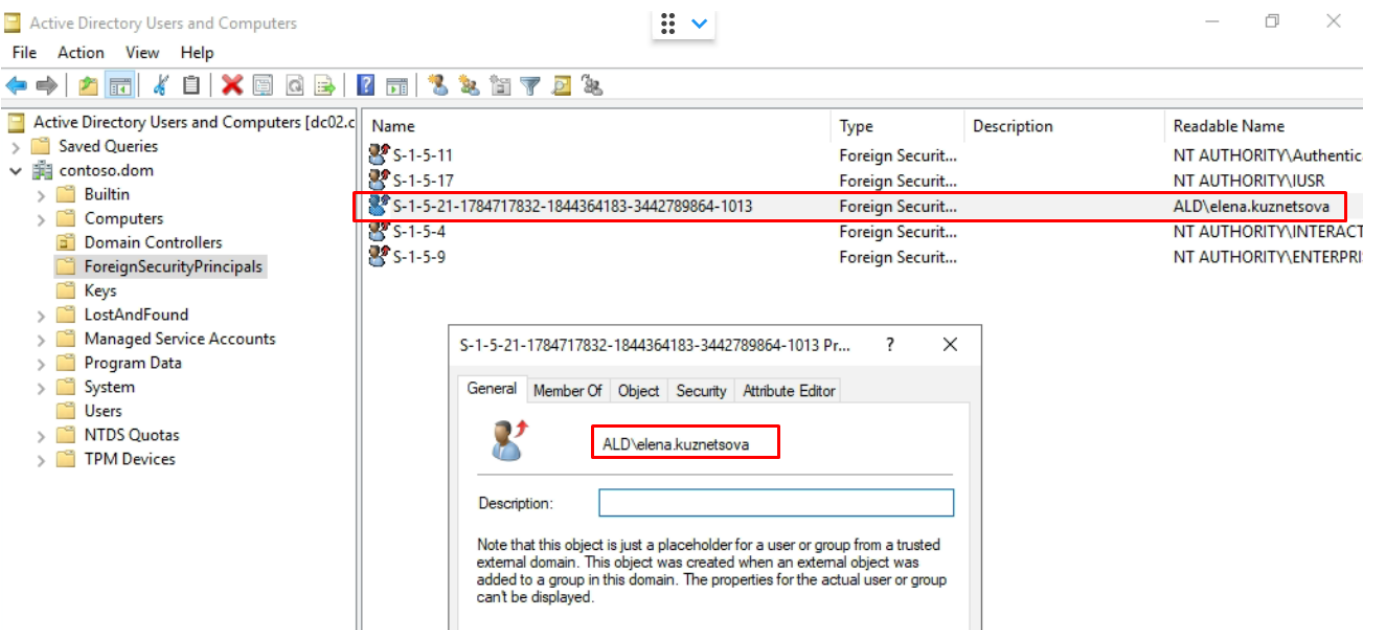
#Добавление AldSid в DomainLocal группы
[void]$group.member.Add("<SID=$AldSid>")
$group.CommitChanges()
$group.Close()
```

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.



Acti
Go to



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.

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/...](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.

