

Инструкция по присоединению рабочей станции под управлением ОС Windows к домену ALD Pro

ALD Pro

Exported on 08/11/2023

Table of Contents

1	Что такое Active Directory?	4
2	Что такое FreeIPA?	5
3	Требования к настройке	6
4	Порядок присоединения.....	7
4.1	Шаг 1. Установите имя хоста в Windows	7
4.2	Шаг 2. Настройте сеть на Windows машине, в данном примере мы установим статический IP адрес.....	7
4.3	Шаг 3. Настройки даты/времени	8
4.4	Шаг 4. Создание нового узла в консоли FreeIPA	11
4.5	Шаг 5. Создание keytab	12
4.6	Шаг 6. Создание пользователя в FreeIPA.....	14
4.7	Шаг 7. Настройте Windows систему на использование FreeIPA	15
4.8	Шаг 8. Войдите в Windows с помощью пользователей FreeIPA	17
4.9	Шаг 9. Проверки.....	18
5	Добавление доменных(ALD Pro) пользователей или групп в локальные группы Windows	20
5.1	Предварительные требования.....	20
5.2	Получить SID пользователя	20
5.3	Получить SID группы.....	21
5.4	Добавить пользователя или группу по SID в локальную группу (запустить PowerShell из под администратора).....	21
5.5	Добавление разрешений на папки доменным пользователям AldPro	21
5.6	Добавление разрешений на папки доменным группам AldPro.....	22

Авторы: [Владимир Кудрявцев](#)¹ [Илья Князев](#)²

v 1.0

Большинство системных администраторов имеют опыт использования компьютеров под управлением ОС Windows в домене Active Directory, но в качестве источника идентификационной информации компьютеры Windows могут использовать и область Kerberos от ALD Pro (FreeIPA).

Способ, которым можно ввести Windows в домен FreeIPA был известен давно, но не получил широкого распространения, т. к. содержал существенный недостаток — внутри операционной системы пользователь действовал от имени локальной учетной записи, которую нужно было создавать заранее. В настоящей инструкции описан способ, который позволяет обеспечить вход в операционную систему именно доменной учетной записью, сохраняя ее SID, участие в группах и Kerberos билеты, что открывает новые возможности по решению задач гибридного развертывания и миграции.

¹ <https://life.astralinux.ru/display/~vkudriavtsev>

² <https://life.astralinux.ru/display/~iknyazev>

1 Что такое Active Directory?

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

2 Что такое FreeIPA?

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

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

AldPro(FreeIPA) может быть интегрирован для работы с Active Directory путем установления доверия между двумя службами. Но в этом руководстве мы настроим систему Windows на использование области FreeIPA для аутентификации пользователей без Active Directory.

Чтобы достичь этого, выполните приведенные ниже шаги для достижения последнего.

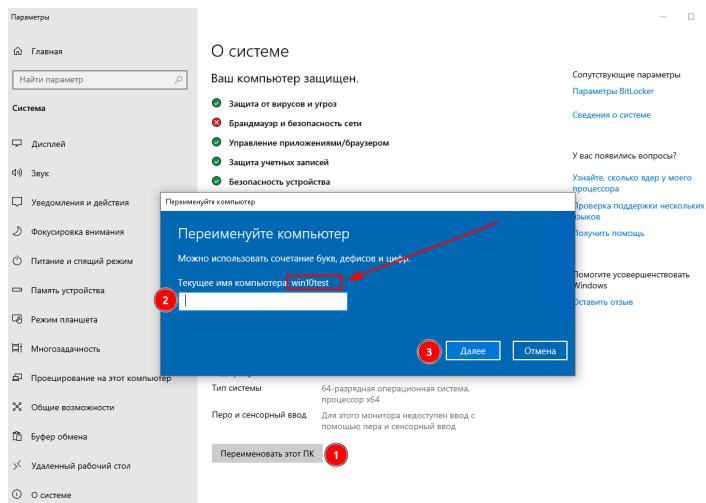
3 Требования к настройке

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

TASK	HOSTNAME	IP_ADDRESS
FreeIPA server(AldPro)	<i>ald01.ald.dom</i>	192.168.88.210
Windows client	<i>Win10test.ald.dom</i>	192.168.88.76

4 Порядок присоединения

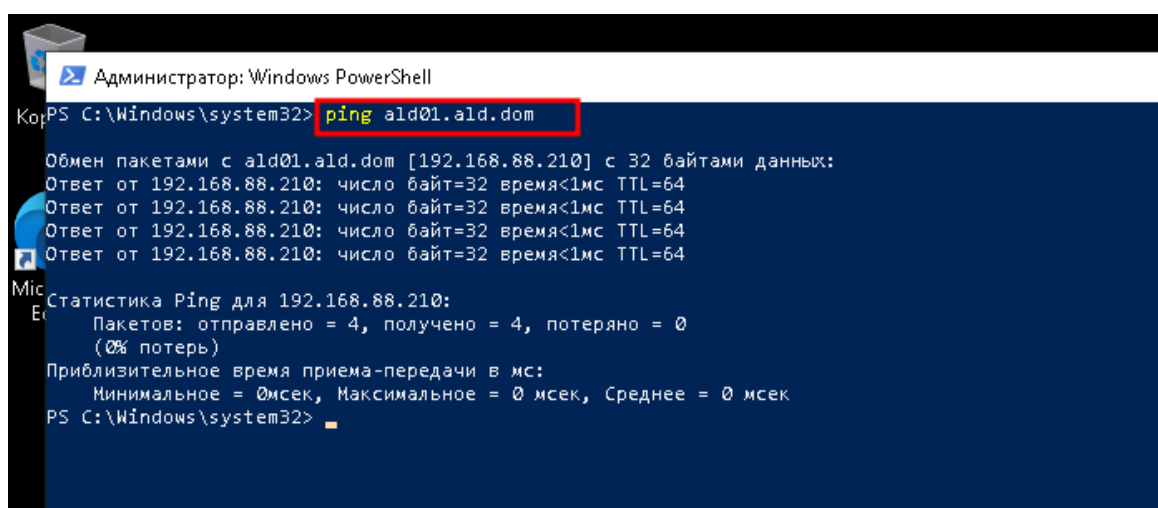
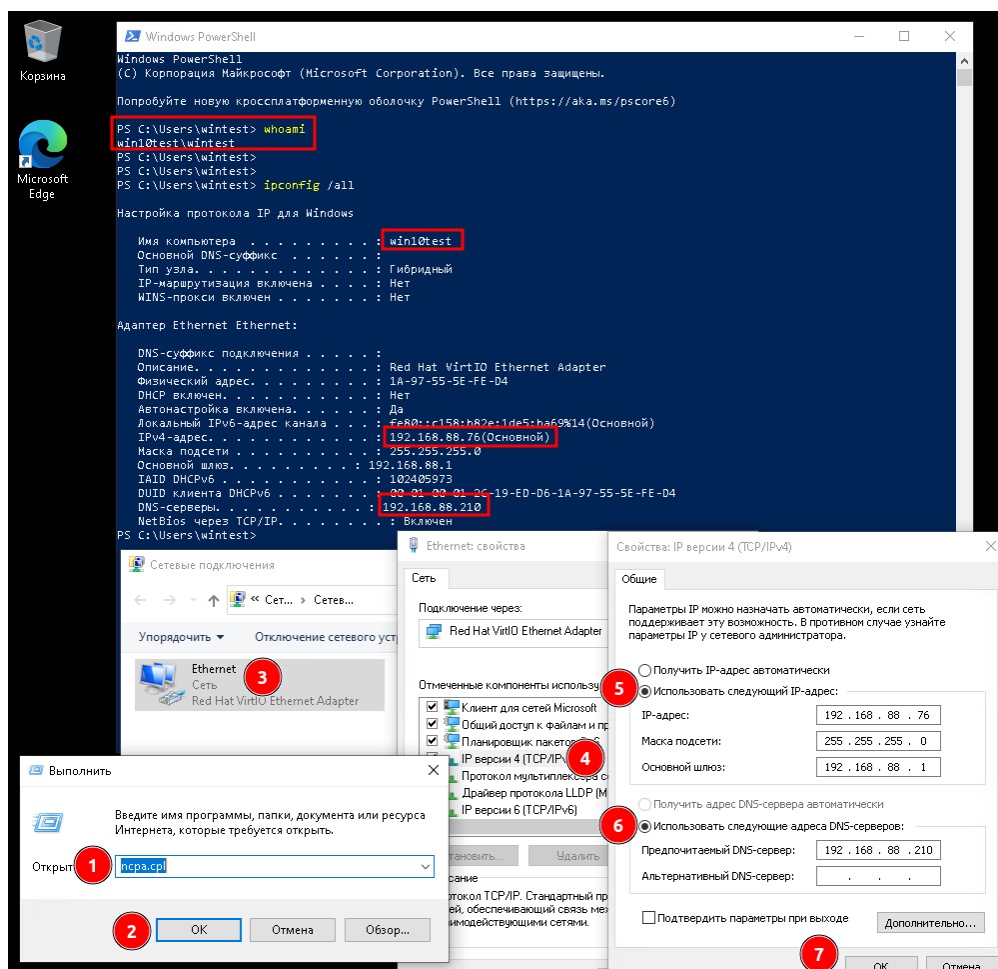
4.1 Шаг 1. Установите имя хоста в Windows



4.2 Шаг 2. Настройте сеть на Windows машине, в данном примере мы установим статический IP адрес.

Нажмите Win+R и запустите **ncpa.cpl** для настройки сети

Сначала мы настроим DNS таким образом, чтобы он мог разрешать имя AldPro(IPA)-сервера.



4.3 Шаг 3. Настройки даты/времени

На стороне ALD Pro(FreelPA) убедитесь, что время не расходится с внешним NTP сервером


```
# chronyc tracking
root@ald01:~# chronyc tracking
Reference ID      : BCE109A7 (188.225.9.167)
Stratum          : 3
Ref time (UTC)   : Tue Jun 13 10:08:13 2023
System time      : 0.000034270 seconds slow of NTP time
Last offset      : -0.000079430 seconds
RMS offset       : 0.000206107 seconds
Frequency        : 9.831 ppm slow
Residual freq    : -0.001 ppm
Skew             : 0.061 ppm
Root delay       : 0.017628554 seconds
Root dispersion  : 0.003091000 seconds
Update interval  : 1040.0 seconds
Leap status      : Normal
root@ald01:~#
root@ald01:~#
root@ald01:~# timedatectl
                Local time: Tue 2023-06-13 13:14:55 MSK
                Universal time: Tue 2023-06-13 10:14:55 UTC
                  RTC time: Tue 2023-06-13 10:14:55
                  Time zone: Europe/Moscow (MSK, +0300)
System clock synchronized: yes
                NTP service: inactive
                RTC in local TZ: no
```

На стороне Windows настраиваем синхронизацию времени с контролером домена в роли NTP сервера. Можно указать несколько значений(FQDN или IP адрес) через запятую, что не обеспечивает возможность автообнаружения контролеров

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

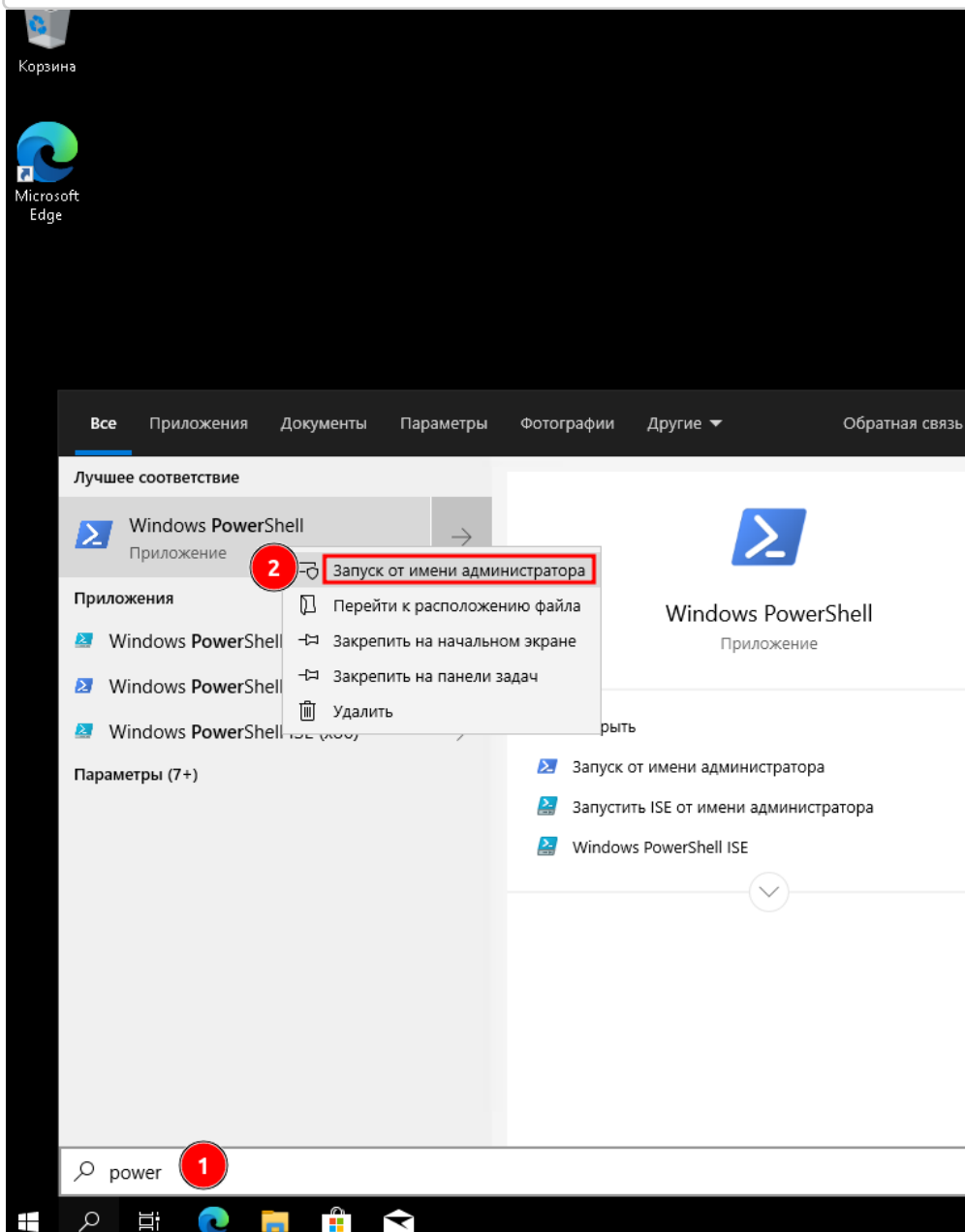
```
net start w32time

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

Результат проверки времени

```
PS C:\Users\Administrator> w32tm /stripchart /computer:ald01.ald.dom
Tracking ald01.ald.dom [192.168.88.210:123].
The current time is 4/13/2023 1:40:55 PM.
```

```
13:40:55, d:+00.0091883s o:-00.0110417s  
[ * ]  
13:40:57, d:+00.0093593s o:-00.0111335s  
[ * ]  
13:40:59, d:+00.0099441s o:-00.0112867s  
[ * ]  
13:41:01, d:+00.0100102s o:-00.0113176s  
[ * ]
```



В данном примере, мы указали IP адрес

```

Администратор: Windows PowerShell
Windows PowerShell
(C) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

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

PS C:\Windows\system32> w32tm /config /reliable:yes /syncfromflags:manual /manualpeerlist:"192.168.88.210" /update
Обнаружена следующая ошибка: Служба не запущена. [0x80070426]
PS C:\Windows\system32> net start w32time
Служба "Служба времени Windows" запускается.
Служба "Служба времени Windows" успешно запущена.

PS C:\Windows\system32> w32tm /config /reliable:yes /syncfromflags:manual /manualpeerlist:"192.168.88.210" /update
Команда выполнена успешно.
PS C:\Windows\system32> net stop w32time
Служба "Служба времени Windows" останавливается.
Служба "Служба времени Windows" успешно остановлена.

PS C:\Windows\system32> net start w32time
Служба "Служба времени Windows" запускается.
Служба "Служба времени Windows" успешно запущена.

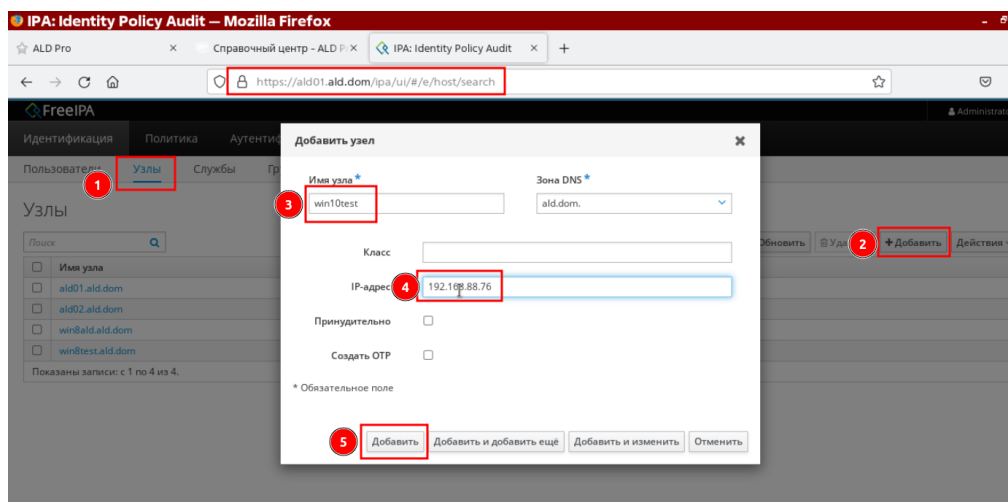
PS C:\Windows\system32> w32tm /resync
Отправка команды синхронизации на локальный компьютер
Команда выполнена успешно.
PS C:\Windows\system32> w32tm /monitor /computers:"192.168.88.210"
192.168.88.210[192.168.88.210:123]:
ICMP: 0ms задержка
NTP: +0.9840959s смещение относительно локального времени
RefID: (неизвестный) [0xA709E18C]
Страта: 3

Предупреждение:
Рекомендуется использовать обратное разрешение имен. Возможно, оно выполнено
неверно, так как поле RefID в пакетах времени различается в
разных реализациях NTP и может не использовать IP-адреса.
PS C:\Windows\system32> w32tm /stripchart /computer:192.168.88.210
Отслеживание 192.168.88.210 [192.168.88.210:123].
Текущее время - 14.06.2023 9:58:36.
09:58:36, d:+00.0002039s o:+00.9840817s [ * ]
09:58:38, d:+00.0003147s o:+00.9841296s [ * ]
09:58:40, d:+00.0003431s o:+00.9841122s [ * ]
09:58:42, d:+00.0004024s o:+00.9840443s [ * ]
PS C:\Windows\system32>
    
```

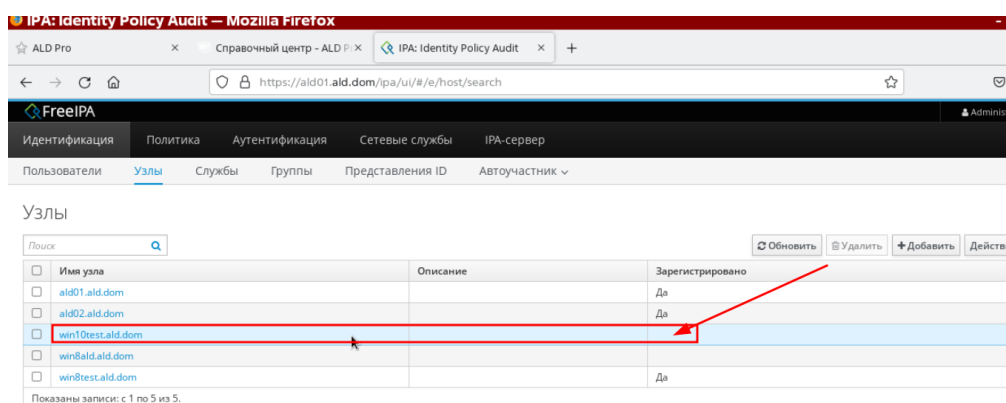
4.4 Шаг 4. Создание нового узла в консоли FreeIPA

В веб-консоли перейдите на вкладку хосты и нажмите кнопку Добавить.

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



Клиент был добавлен, но еще не зарегистрирован.



4.5 Шаг 5. Создание keytab

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

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

Вернитесь в командную строку FreeIPA и добавьте клиент. Сначала сгенерируйте билет(Выполните аутентификацию) с помощью команды:

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

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

Для получения поддерживаемых типов шифрования выполните команду указанную ниже:

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

Добавьте участника, используя команду с приведенным ниже синтаксисом. Помните, что вам необходимо включить типы шифрования:

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

В приведенной выше команде:

-s указывает сервер FreeIPA

-e определяет шифрование

-k путь до существующего или нового keytab файла

-p указывает нового участника, который будет добавлен

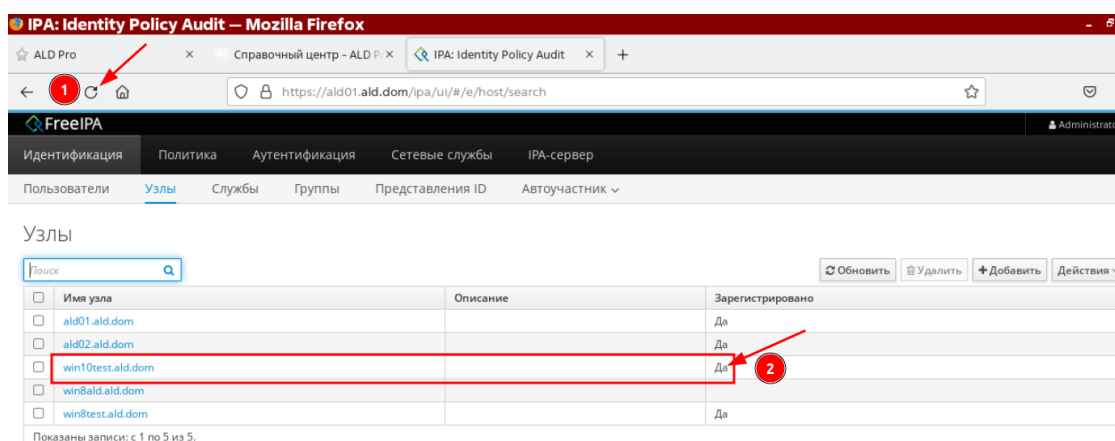
-P устанавливает пароль (**не забудьте, так как он будет использоваться при настройке клиента позже**)

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

Проверьте, был ли добавлен ключ:

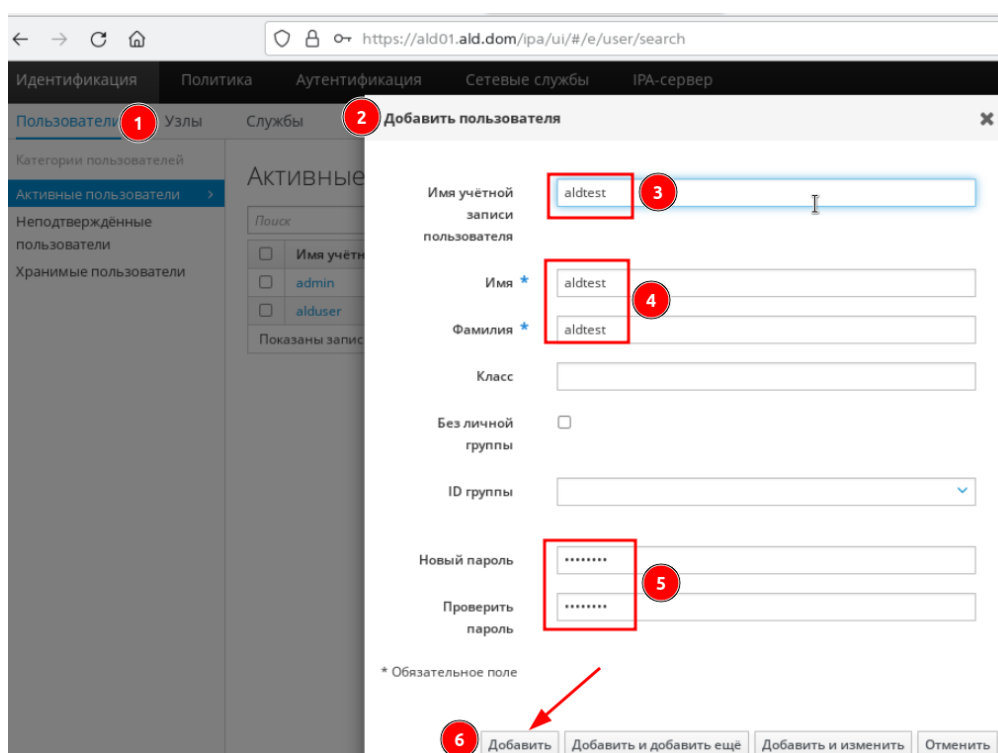
```
root@ald01:~# klist -k /etc/krb5.keytab.windows
Keytab name: FILE:/etc/krb5.keytab.windows
KVNO Principal
-----
  1 host/win8test.ald.dom@ALD.DOM
  1 host/win8test.ald.dom@ALD.DOM
  1 host/win8test.ald.dom@ALD.DOM
  1 host/win8test.ald.dom@ALD.DOM
  1 host/win8test.ald.dom@ALD.DOM
  1 host/win8test.ald.dom@ALD.DOM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

Теперь вернемся к веб-интерфейсу, клиент должен быть зарегистрирован.

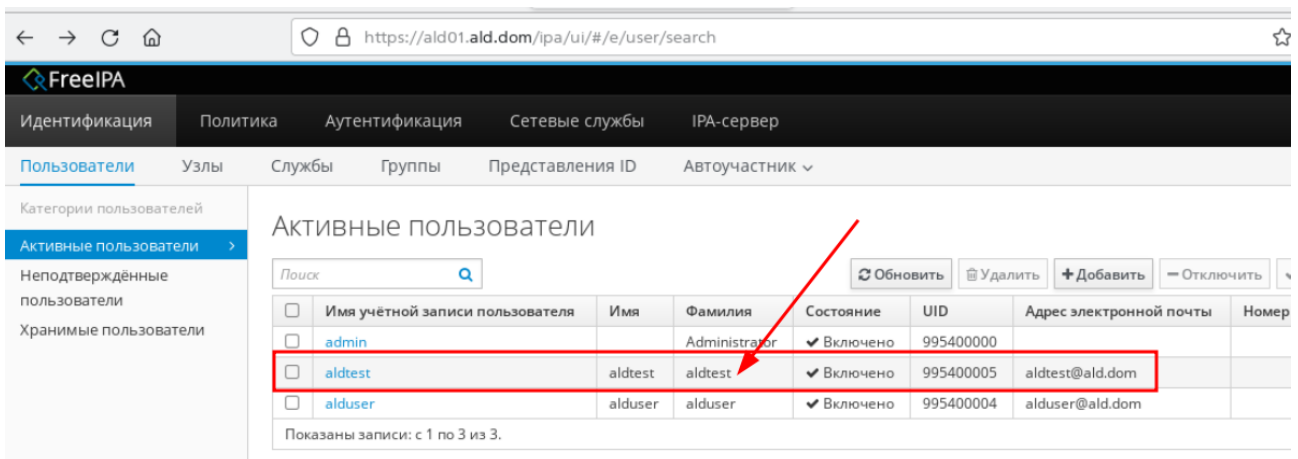


4.6 Шаг 6. Создание пользователя в FreeIPA

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



Указанный пароль при создании пользователя **вам придется сменить при первом входе в систему**. Добавленный пользователь появится, как показано на рисунке.



4.7 Шаг 7. Настройте Windows систему на использование FreeIPA

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

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

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

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

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

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

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

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

ВАЖНО!

Пароль учётной записи компьютера не отображается в реестре или в качестве выходных данных команды `ksetup`.

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

В инструкциях встречается указание, что необходимо выполнить команду **`ksetup /mapuser **`**

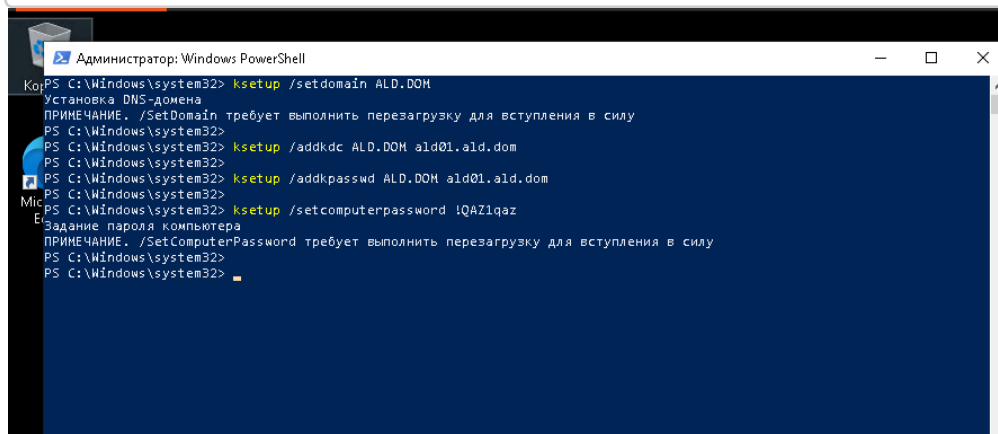
`ksetup /mapuser * *` - Чтобы сопоставить все учётные записи в области ALD.DOM Kerberos с любой существующей учётной записью с тем же именем на этом компьютере.

Поскольку в нашем случае используются доменные учётные записи пользователей, нам нет необходимости сопоставлять им локальные учётки.

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

Выполните поочередно следующие команды (**Не перезагружайте компьютер**)

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



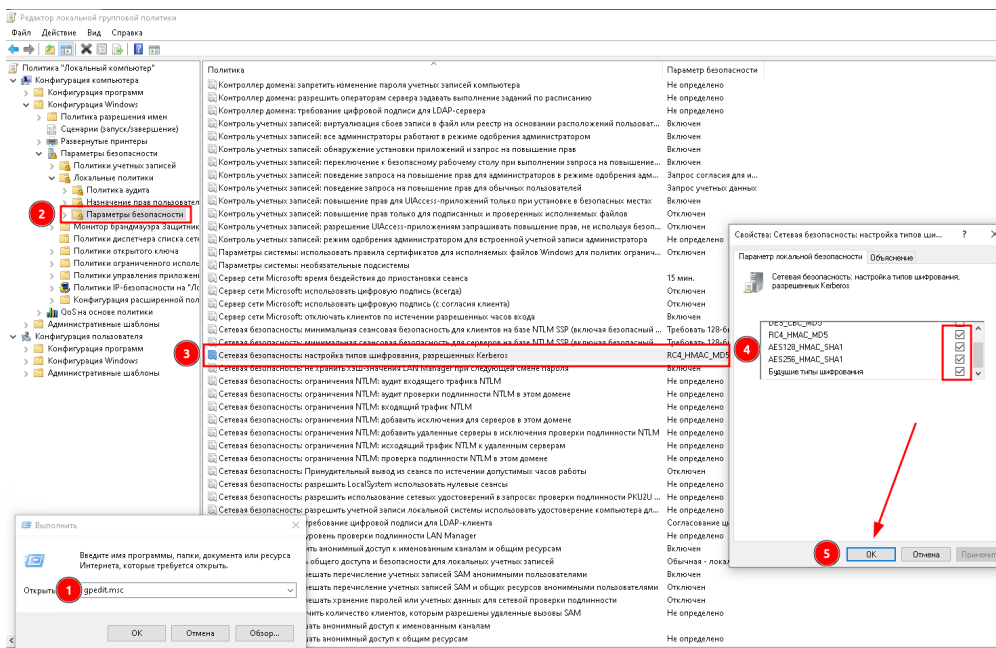
Теперь запустите **gpedit.msc**, нажав клавишу Windows + R.

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

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

Укажите следующие типы шифрования:

RC4_HMAC_MD5, AES128_HMAC_SHA1, AES256_HMAC_SHA1, Будущие типы шифрования



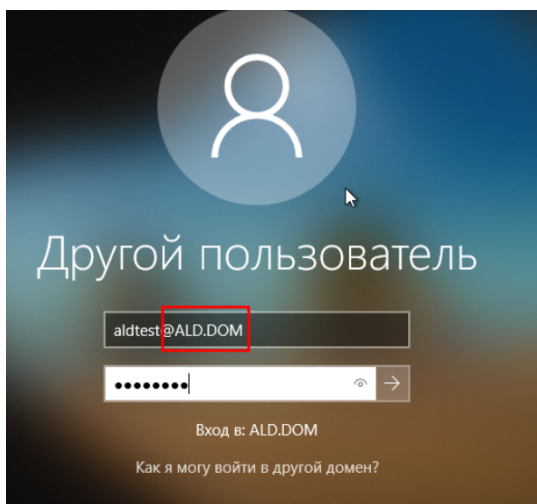
Примените, нажмите кнопку OK и перезагрузите систему.

4.8 Шаг 8. Войдите в Windows с помощью пользователей FreeIPA

Имя Пользователя@REALM

aldtest@ALD.DOM(see page 3)

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

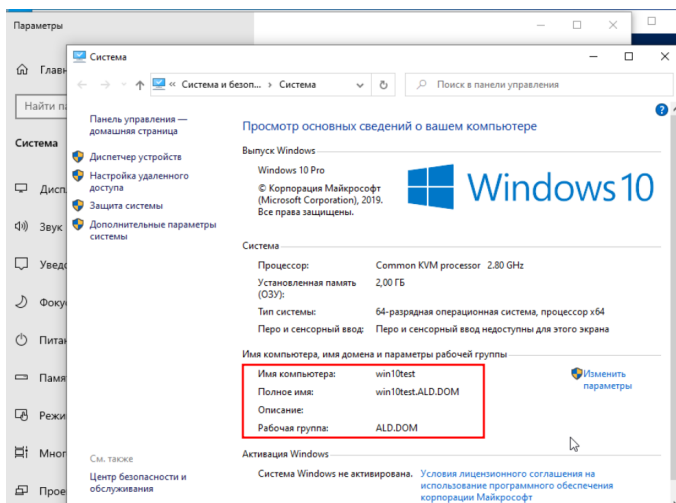
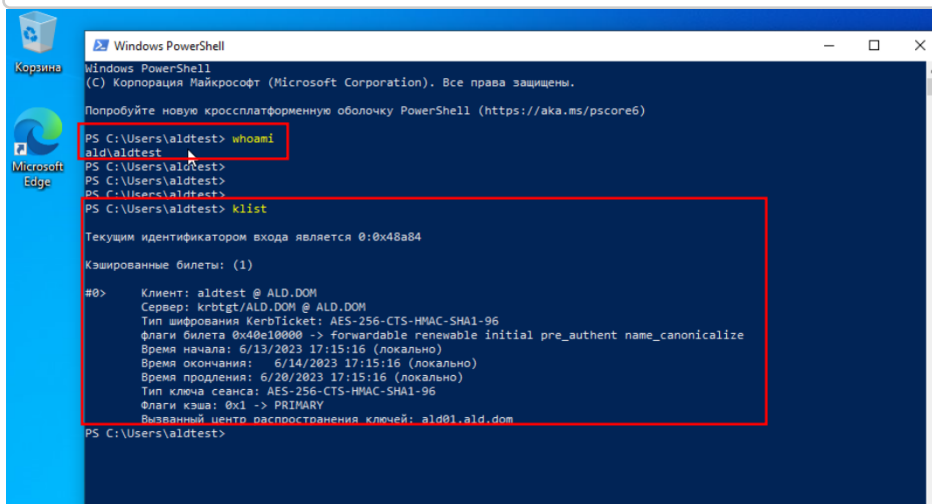


Вам будет предложено изменить пароль для пользователя IPA

4.9 Шаг 9. Проверки

Выполните следующие команды в PowerShell или CMD:

```
whoami
klist
```



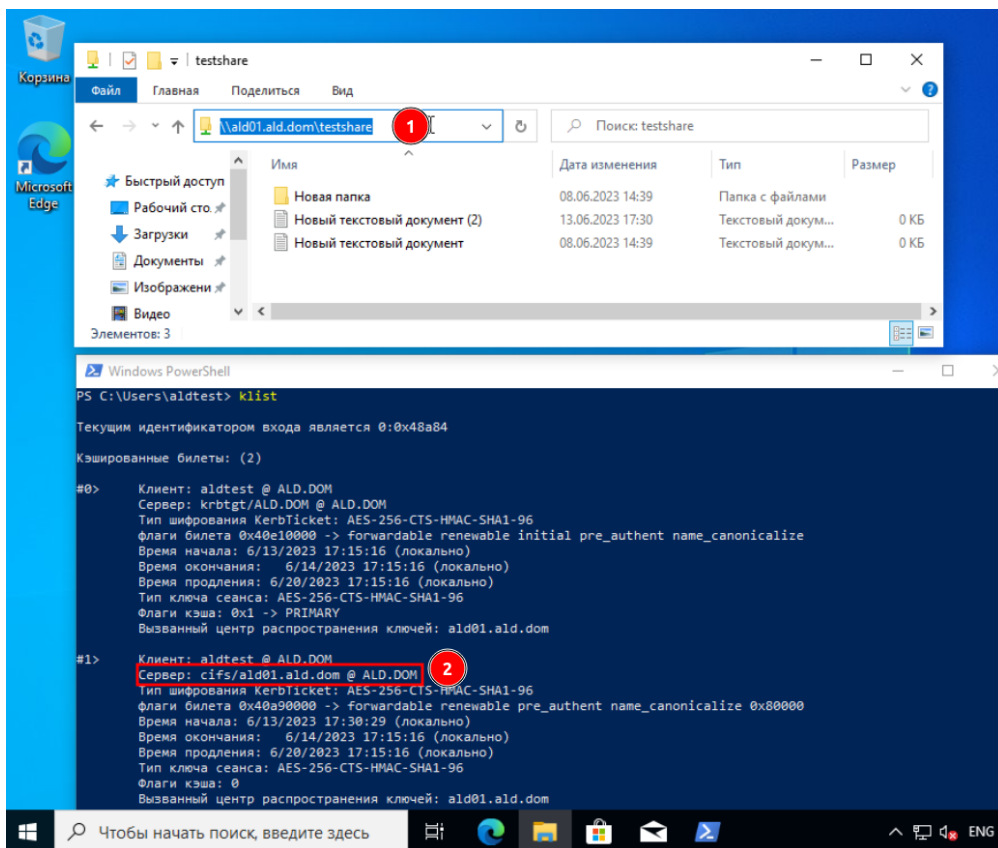
На Ald Pro сервере создайте общую тестовую папку и попробуйте зайти:

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

```
writable = yes
```

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

После успешного входа klist будет содержать дополнительный билет:



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

5.1 Предварительные требования

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

Операционная система	Предварительные требования	Ссылки на пакеты
Windows Server 2012 R2		Win8.1AndW2K12R2-KB3191564-x64.msu ³
Windows Server 2012		W2K12-KB3191565-x64.msu ⁴
Windows Server 2008 R2	.NET Framework 4.5.2 ⁵	Win7AndW2K8R2-KB3191566-x64.ZIP ⁶
Windows 8.1		x64: Win8.1AndW2K12R2-KB3191564-x64.msu ⁷ x86: Win8.1-KB3191564-x86.msu ⁸
Windows 7 с пакетом обновления 1 (SP1)	.NET Framework 4.5.2 ⁹	x64: Win7AndW2K8R2-KB3191566-x64.ZIP ¹⁰ x86: Win7-KB3191566-x86.ZIP ¹¹

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

5.2 Получить SID пользователя

Используя wbinfo

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

3 <https://go.microsoft.com/fwlink/?linkid=839516>

4 <https://go.microsoft.com/fwlink/?linkid=839513>

5 <https://www.microsoft.com/download/details.aspx?id=42642>

6 <https://go.microsoft.com/fwlink/?linkid=839523>

7 <https://go.microsoft.com/fwlink/?linkid=839516>

8 <https://go.microsoft.com/fwlink/?linkid=839521>

9 <https://www.microsoft.com/download/details.aspx?id=42642>

10 <https://go.microsoft.com/fwlink/?linkid=839523>

11 <https://go.microsoft.com/fwlink/?linkid=839522>

Используя ipa command

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

5.3 Получить SID группы

Используя ipa command

```
root@ald01:~# ipa group-show group_high --all | grep ipantsecurityidentifier
ipantsecurityidentifier: S-1-5-21-109148531-2531787706-4107538291-1007
root@ald01:~#
root@ald01:~# ipa group-show group_high --all
dn: cn=group_high,cn=groups,cn=accounts,dc=ald,dc=dom
Имя группы: group_high
ID группы: 995400007
Группы-участники: group_low
Пользователи с непрямым участием: alduser, aldtest
ipantsecurityidentifier: S-1-5-21-109148531-2531787706-4107538291-1007
ipauniqueid: d1410fd4-0a8c-11ee-9d12-422c2492509f
objectclass: top, groupofnames, nestedgroup, ipausergroup, ipaobject, x-ald-audit-policy, rbta-unit, posixgroup, ipantgroupattrs
```

5.4 Добавить пользователя или группу по SID в локальную группу (запустить PowerShell из под администратора)

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

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

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

5.5 Добавление разрешений на папки доменным пользователям AldPro

Наиболее популярные разрешения:

r = чтение

rx = Чтение, Выполнение, Список содержимого папки

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

f = Полный доступ

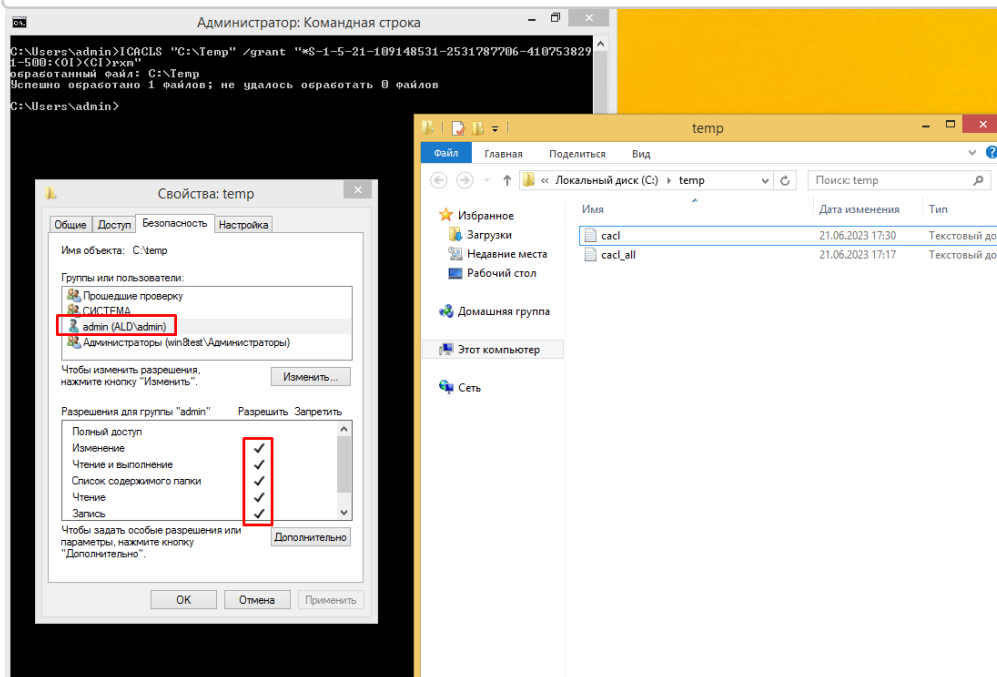
(OI) = Для этой папки и её файлов

(CI) = Для этой папки и её подпапок

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

PowerShell или CMD

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



Более детальная информация может быть найдена на сайте Microsoft

<https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/icaccls>

5.6 Добавление разрешений на папки доменным группам AldPro

К сожалению в текущей реализации не поддерживается прямое добавление доменных групп в дискретные списки доступа (DACL). Для того, чтобы обойти это ограничение мы:

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

```
Alldom_fs_c_temp_r  
Alldom_fs_c_temp_rw
```