

Настройка профиля пользователя в терминальной среде Linux

В этом документе описано, как установить NFS-сервер, настроить папку профиля пользователя и терминальный сервер.

В настройке используются:

- NFS-сервер на РЕД ОС 7.3.4;
- терминальный сервер на РЕД ОС 7.3.4;
- Active Directory на Windows Server 2019.

1. Установка NFS-сервера

1. Разверните сервер.
2. Введите сервер в домен с помощью команды:

```
join-to-domain.sh -d 'имя домена' -n 'имя сервера' -u 'у3' -p 'Пароль' -ou  
"CN=Computers" -f -y
```

3. Установите пакеты `nfs-utils` `nfs4-acl-tools` с помощью команды:

```
dnf install nfs-utils nfs4-acl-tools
```

4. Добавьте автостарт с помощью команды:

```
systemctl enable --now nfs-server.service
```

5. Проверьте запуск с помощью команды:

```
systemctl status nfs-server.service
```

После успешного запуска NFS-сервера его статус изменится на «active».

2. Настройка папки для профилей

1. Создайте папку с помощью команды:

```
mkdir -p /srv/nfs/home
```

BASH | □

2. Назначьте права доступа на папку с помощью команд:

```
chgrp 'Пользователи домена' /srv/nfs/home  
chmod g+w /srv/nfs/home
```

BASH | □

3. Настройте доступ к папке с помощью команд:

```
echo "/srv/nfs/home *(rw,sync,no_subtree_check)" | tee -a /etc/exports  
exportfs -vra (работает при su -)
```

BASH | □



Вместо * необходимо прописать IP-адрес или подсеть IP-адресов, с которых будет разрешен доступ.

3. Настройка терминального сервера

1. Установите пакет autoofs с помощью команды:

```
dnf install autoofs
```

BASH | □

2. Скорректируйте конфигурацию auto.master с помощью команды:

```
echo "/- /etc/auto.nfs --timeout=60" | tee -a /etc/auto.master
```

BASH | □

3. Создайте файл конфигурации подключения файловой системы NFS с помощью команды:

```
touch /etc/auto.nfs
```

BASH | □

4. Настройте конфигурацию auto.nfs с помощью команды:

```
echo "/home -rw,hard,sec=sys,intr,acl,nodiratime,sync,noac,lookupcache=none  
$SERVER:/srv/nfs/home" | tee -a /etc/auto.nfs
```

BASH | □

Где:

\$SERVER – FQDN NFS-сервера.

5. Добавьте автостарт с помощью команд:

```
sudo systemctl enable autoofs  
sudo systemctl restart autoofs
```

BASH | □

6. Разрешите процессу mkdirhome права на запись с помощью команд:

```
ausearch -c 'mkhomedir' --raw | audit2allow -M my-mkhomedir  
semodule -X 300 -i my-mkhomedir.pp
```

BASH | □

7. Добавьте разрешение для NFS и SELinux с помощью команды:

```
setsebool -P use_nfs_home_dirs on
```

BASH | □

8. Перезапустите систему с помощью команды:

```
sudo reboot
```

BASH | □

Далее войдите в систему под пользователем, для которого было настроено перенаправление папок и проверьте, что:

- вход выполнен успешно;
- нет ошибок;
- папка создалась на удаленном сервере.

Профили пользователей

1. Настройка профиля пользователя в терминальной среде Windows

Перенаправление папок позволяет пользователям и администраторам вручную или с помощью групповой политики перенаправлять путь к определенной папке в новое расположение. Новым расположением может быть папка на терминальном сервере или каталог на файловом сервере. Пользователи будут работать с данными в перенаправленной папке.

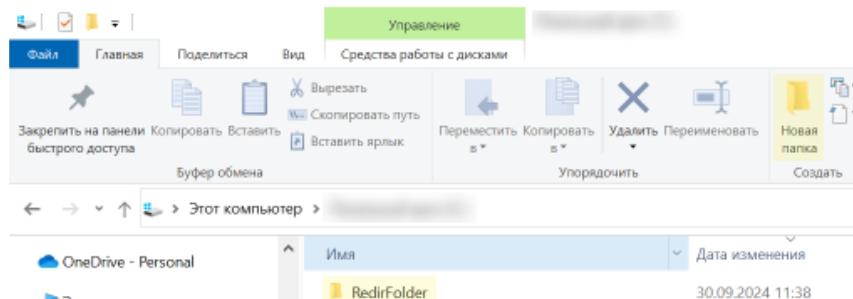
В этом документе описано, как настроить перенаправления папок (folder redirection) на компьютерах пользователей в домене Active Directory (AD) с помощью групповых политик (GPO) для группы доступа пользователей домена.



Групповая политика применяется к пользователю или компьютеру в зависимости от расположения объектов пользователя и компьютера в AD. В некоторых случаях пользователям могут потребоваться политики, применяемые на основе расположения как объекта пользователя, так и объекта компьютера, либо только расположения объекта компьютера. Для этого можно использовать функцию замыкания групповой политики (Loopback), чтобы применить объекты групповой политики (GPO).

Подробнее о Loopback можно прочесть [на официальном сайте Microsoft](#).

- Создайте в домене AD группу и добавьте в нее пользователей с помощью консоли Active Directory Users and Computers (ADUC).
- Создайте и опубликуйте на файловом сервере сетевую папку, в которой будут храниться перенаправленные папки с помощью проводника Windows:
 - На файловом сервере, где будет размещена общая папка, создайте новую папку и назовите ее, например «RedirFolder».



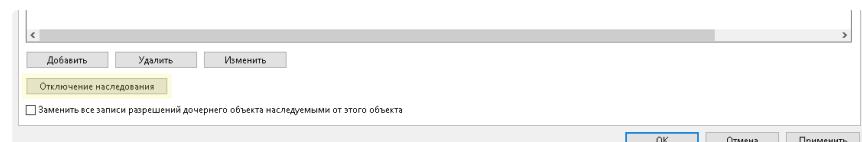
- Нажмите правой кнопкой мыши по папке, разверните **Предоставить доступ к (Give Access to)** и выберите **Отдельные люди (Specific people)**.



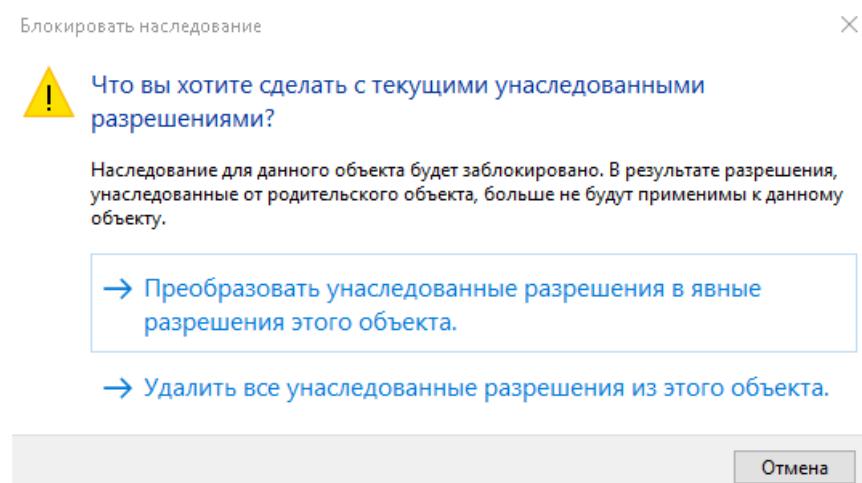
- с. Предоставьте полный доступ (чтение/запись) для **Authenticated users**.
- d. Нажмите **Поделиться > Готово (Share > Done)**.

3. Для того чтобы обеспечить каждому пользователю доступ только к его файлам, необходимо настроить правильные разрешения NTFS для папки:

- a. В свойствах папки перейдите на вкладку **Безопасность (Security)**, нажмите [**Дополнительно**] ([**Advanced**]), затем нажмите [**Отключение наследования**] ([**Disable Inheritance**]).

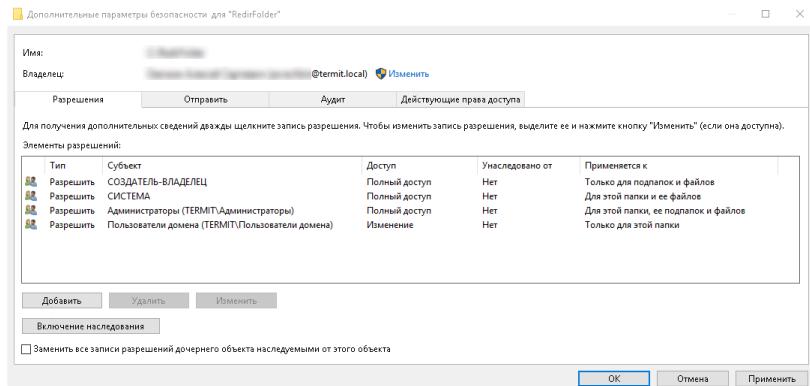


- b. В открывшемся окне выберите **Преобразовать унаследованные разрешения в явные разрешения этого объекта (Convert inherited permissions into explicit permissions on the object)**.



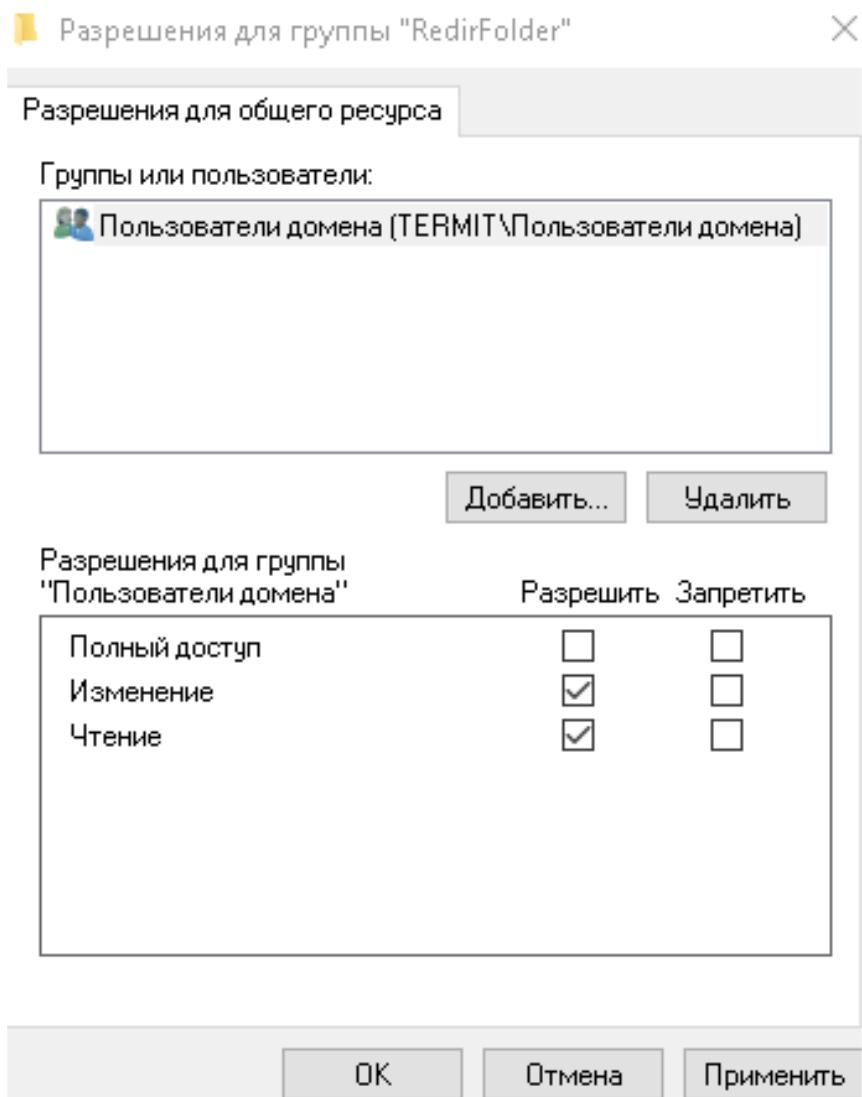
- c. В списке разрешений NTFS оставьте права:

- СОЗДАТЕЛЬ-ВЛАДЕЛЕЦ (Полный доступ, Только для подпапок и файлов) (CREATOR OWNER (Full control, Subfolders and files only))
- СИСТЕМА (Полный доступ, Для этой папки, ее подпапок и файлов) (SYSTEM (Full control, This folder, subfolders and files))
- Администраторы (Полный доступ, Для этой папки, ее подпапок и файлов) (Administrators (Full control, This folder, subfolders and files))
- Пользователи домена (Изменение, Чтение и выполнение, Запись, Только для этой папки) (Domain users (Modify, Read & execute, Write, This folder))



- d. На файловом сервере в свойствах сетевой папки перейдите на вкладку **Доступ (Sharing)**, нажмите **Расширенная настройка > Разрешения (Advanced Sharing: > Permissions)** и активируйте опцию **Полный доступ (Full Control)**.

После настройки разрешения пользователи смогут создавать папки в каталоге, а доступ к содержимому вложенных папок будет только у владельцев-пользователей.



4. Создайте в домене групповую политику перенаправления папок для пользователей. Для этого:
- Запустите консоль управления групповой политикой (GPMC).
 - Создайте новую GPO и назначьте на Organizational Unit с пользователями.

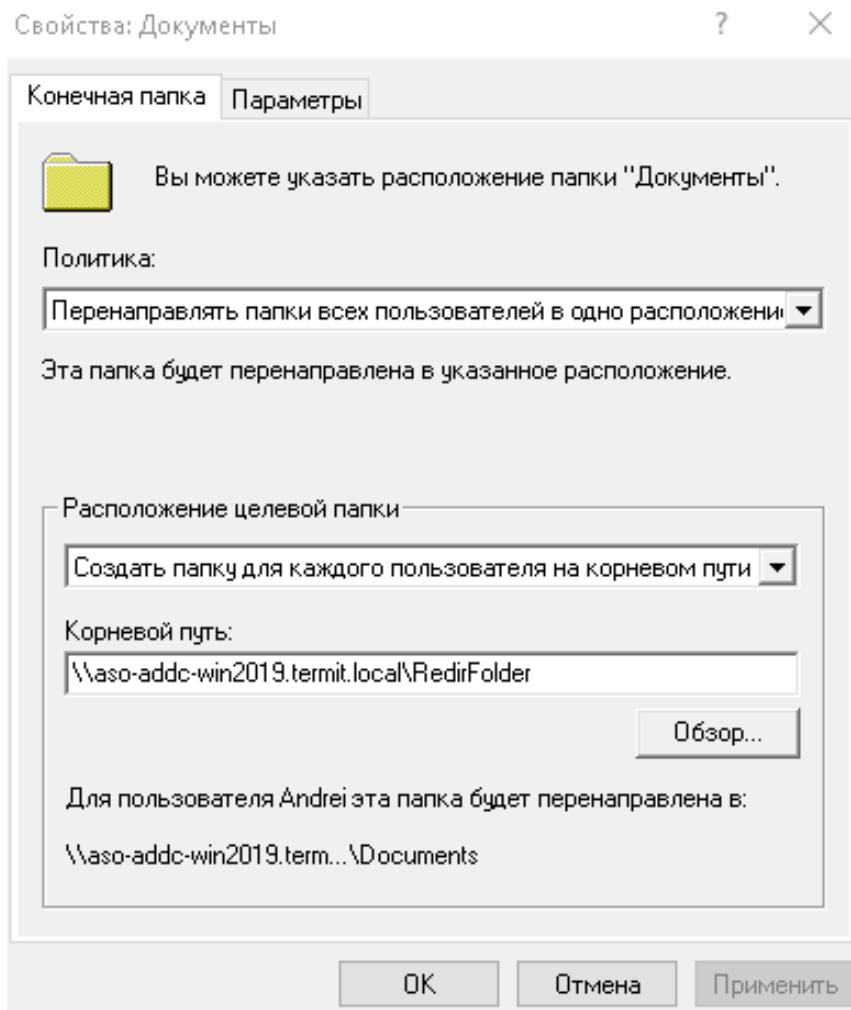
5. В редакторе управления групповыми политиками разверните **Конфигурация пользователя > Политики > Конфигурация Windows > Перенаправление папки** (**User Configuration > Policies > Windows Settings > Folder Redirection**).



В разделе **Перенаправление папки (Folder Redirection)** находятся опции для перенаправления различных папок профиля пользователя. В этом примере приведена настройка перенаправления только для папки **Документы (Documents)**. Остальные папки можно настроить таким же образом.

6. Откройте свойства **Документы (Documents)** и на вкладке **Корневая папка (Target)** укажите следующие параметры перенаправления каталога:

- **Политика (Settings)** – Перенаправлять папки всех пользователей в одно расположение (Basic, Redirect everyone's folder to the same location);
- **Расположение целевой папки (Target folder location)** – Создать папку для каждого пользователя на корневом пути (Create a folder for each user under the root path);
- **Корневой путь (Root path)** – \\lasso-addc-win2019.termit.local\\RedirFolder.

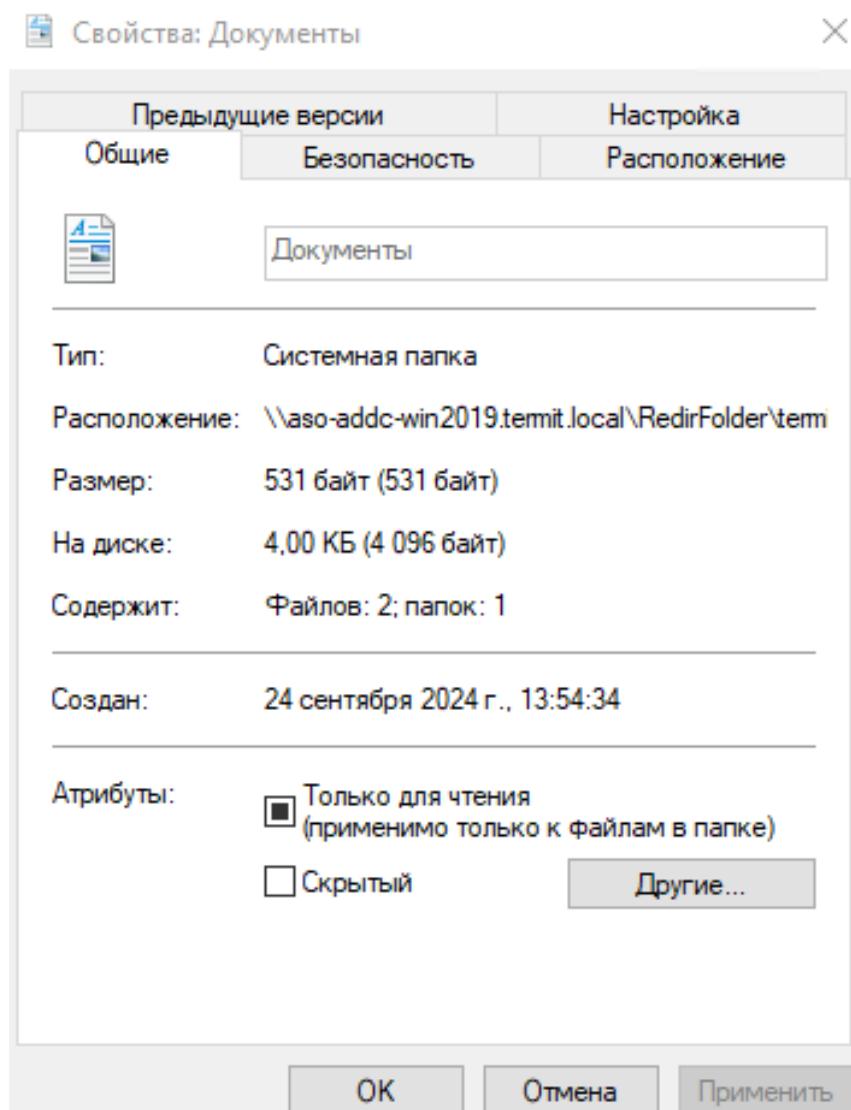


! Добавьте адрес файлового сервера и/или домен в список доверенных зон, используя групповую политику **Список назначений зоны для веб-сайтов (GPO Site to Zone Assignment List)** в Конфигурация компьютера > Административные шаблоны > Компоненты Windows > Internet Explorer > Панель управления Интернетом > Страница безопасности (в Computer Configuration > Administrative Templates > Windows Components > Internet Explorer > Internet Control Panel > Security Page).

Иначе при запуске ярлыков и исполняемых файлов из перенаправленного каталога могут появляться предупреждения системы безопасности Windows.

7. Проверьте работу групповой политики перенаправления папки. Для этого:

- a. Запустите **десктоп-клиент Termit** > **рабочий стол**.
- b. Откройте свойства папки **Документы (Documents)** и убедитесь, что в параметре **Расположение (Location)** указан UNC-путь к вашему файловому серверу.



Вы можете создавать файлы и папки в **Документы (Documents)**. И они будут доступны пользователю с любого компьютера в вашем домене.

2. Настройка профиля пользователя в терминальной среде Linux

В этом документе описано, как установить NFS-сервер, настроить папку профиля пользователя и терминальный сервер.

В настройке используются:

- NFS-сервер на РЕД ОС 7.3.4;
- терминальный сервер на РЕД ОС 7.3.4;
- Active Directory на Windows Server 2019.

2.1. Установка NFS-сервера

1. Разверните сервер.
2. Введите сервер в домен с помощью команды:

```
join-to-domain.sh -d 'имя домена' -n 'имя сервера' -u 'УЗ' -p 'Пароль' -ou  
"CN=Computers" -f -y
```

3. Установите пакеты nfs-utils nfs4-acl-tools с помощью команды:

```
dnf install nfs-utils nfs4-acl-tools
```

4. Добавьте автостарт с помощью команды:

```
systemctl enable --now nfs-server.service
```

5. Проверьте запуск с помощью команды:

```
systemctl status nfs-server.service
```

После успешного запуска NFS-сервера его статус изменится на «active».

2.2. Настройка папки для профилей

1. Создайте папку с помощью команды:

```
mkdir -p /srv/nfs/home
```

2. Назначьте права доступа на папку с помощью команд:

```
BASH | ↗  
chgrp 'Пользователи домена' /srv/nfs/home  
chmod g+w /srv/nfs/home
```

3. Настройте доступ к папке с помощью команд:

```
BASH | ↗  
echo "/srv/nfs/home *(rw,sync,no_subtree_check)" | tee -a /etc/exports  
exportfs -vra (работает при su -)
```



Вместо * необходимо прописать IP-адрес или подсеть IP-адресов, с которых будет разрешен доступ.

2.3. Настройка терминального сервера

1. Установите пакет autoofs с помощью команды:

```
BASH | ↗  
dnf install autoofs
```

2. Скорректируйте конфигурацию auto.master с помощью команды:

```
BASH | ↗  
echo "/- /etc/auto.nfs --timeout=60" | tee -a /etc/auto.master
```

3. Создайте файл конфигурации подключения файловой системы NFS с помощью команды:

```
BASH | ↗  
touch /etc/auto.nfs
```

4. Настройте конфигурацию auto.nfs с помощью команды:

```
BASH | ↗  
echo "/home -rw,hard,sec=sys,intr,acl,nodiratime,sync,noac,lookupcache=none  
$SERVER:/srv/nfs/home" | tee -a /etc/auto.nfs
```

Где:

\$SERVER — FQDN NFS-сервера.

5. Добавьте автостарт с помощью команд:

```
BASH | ↗  
sudo systemctl enable autoofs  
sudo systemctl restart autoofs
```

6. Разрешите процессу mkdirhome права на запись с помощью команд:

```
BASH | ↗  
ausearch -c 'mkhomedir' --raw | audit2allow -M my-mkhomedir  
semodule -X 300 -i my-mkhomedir.pp
```

7. Добавьте разрешение для NFS и SELinux с помощью команды:

```
setsebool -P use_nfs_home_dirs on
```

BASH | □

8. Перезапустите систему с помощью команды:

```
sudo reboot
```

BASH | □

Далее войдите в систему под пользователем, для которого было настроено перенаправление папок и проверьте, что:

- вход выполнен успешно;
- нет ошибок;
- папка создалась на удаленном сервере.



Ошибка "Cannot authenticate using при настройке ovirt-engine-extension-aaa-ldap-setup"

1. Вопрос

При настройке подключения zVirt к Active Directory (уровень домена 2016, уровень леса 2016, контроллеры домена MS Windows Server 2016, роль управления сертификатами СА, доменный пользователь **searchuser**) с помощью **virt-engine-extension-aaa-ldap-setup** возникает ошибка:

```
[ INFO ] Resolving SRV record 'srasu.local'  
[ INFO ] Connecting to LDAP using 'ldap://srasu-s-dc01.srasu.local:389'  
[ INFO ] Executing startTLS  
[ INFO ] Connection succeeded  
Enter search user DN (for example  
uid=username,dc=example,dc=com or leave empty for anonymous):  
uid=searchuser,dc=srasu,dc=local  
Enter search user password:  
[ INFO ] Attempting to bind using 'uid=searchuser,dc=srasu,dc=local'  
[ ERROR ] Cannot authenticate using 'uid=searchuser,dc=srasu,dc=local':  
{'msgtype': 97, 'msgid': 3, 'result': 49, 'desc': 'Invalid credentials',  
'ctrls': [], 'info': '80090308: LdapErr: DSID-0C090447, comment:  
AcceptSecurityContext error, data 52e, v3839'}
```

На **Engine** скопирован **root-ca.pem**.

2. Решение

Необходимо корректно указать:

```
cn=searchuser,dc=srasu,dc=local
```

вместо

```
uid=searchuser,dc=srasu,dc=local
```

Ошибка "Cannot resolve principal" при попытке подключения к внешнему серверу аутентификации AD

1. Вопрос

Если попытка подключения к внешнему серверу аутентификации AD заканчивается неудачно и в логе есть запись вида

```
Cannot resolve principal 'ovirtadm@domain.local'
```

2. Проверка

Это говорит о работе службы глобального каталога не на порту **3268**, а **389**. Следует проверить сервисные записи DNS. Для этого перейдите в терминал (подключитесь по SSH) к менеджеру управления и введите (где **example.com** - адрес домена):

```
dig _ldap._tcp.gc._msdcs.example.com SRV  
dig _ldap._tcp.example.com SRV
```

Корректный результат вывода команды `dig _ldap._tcp.gc._msdcs.example.com SRV`:

```
# dig _ldap._tcp.gc._msdcs.domain.local SRV  
  
; <>> DiG 9.11.36-RedHat-9.11.36-3.el8 <>> _ldap._tcp.gc._msdcs.domain.local  
SRV  
;; global options: +cmd  
;; Got answer:  
;; WARNING: .local is reserved for Multicast DNS  
;; You are currently testing what happens when an mDNS query is leaked to DNS  
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8991  
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 2  
  
;; OPT PSEUDOSECTION:  
; EDNS: version: 0, flags:; udp: 4000  
;; QUESTION SECTION:  
;_ldap._tcp.gc._msdcs.domain.local. IN SRV  
  
;; ANSWER SECTION:
```

```

_ldap._tcp.gc._msdcs.domain.local. 600 IN SRV      0 100 3268
myserver.domain.local.

;; ADDITIONAL SECTION:
myserver.domain.local. 3600 IN A      172.25.1.19

;; Query time: 3 msec
;; SERVER: 172.25.1.19#53(172.25.1.19)
;; WHEN: Fri Dec 02 09:24:05 MSK 2022
;; MSG SIZE  rcvd: 121

```

Корректный результат вывода команды dig _ldap._tcp.example.com SRV :

```

# dig _ldap._tcp.domain.local SRV

; <>> DiG 9.11.36-RedHat-9.11.36-3.el8 <>> _ldap._tcp.domain.local SRV
;; global options: +cmd
;; Got answer:
;; WARNING: .local is reserved for Multicast DNS
;; You are currently testing what happens when an mDNS query is leaked to DNS
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44159
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;_ldap._tcp.domain.local.           IN      SRV

;; ANSWER SECTION:
_ldap._tcp.domain.local. 600      IN      SRV      0 100 389
myserver.domain.local.

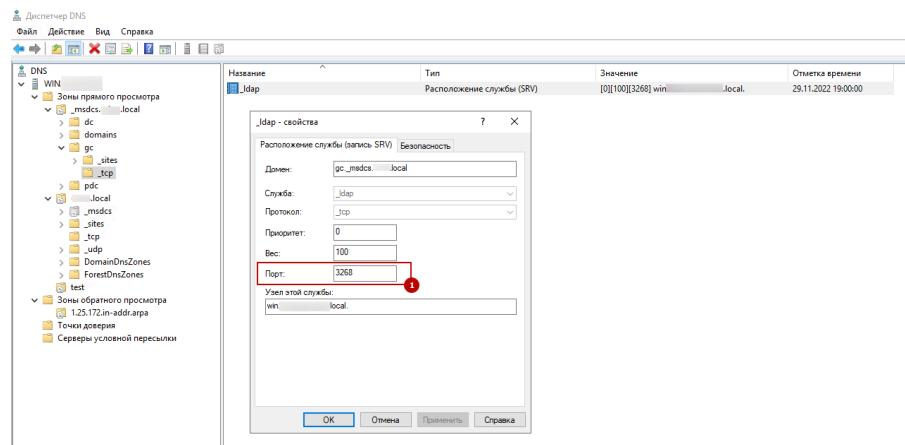
;; ADDITIONAL SECTION:
myserver.domain.local. 3600 IN A      172.25.1.19

;; Query time: 2 msec
;; SERVER: 172.25.1.19#53(172.25.1.19)
;; WHEN: Fri Dec 02 09:24:42 MSK 2022
;; MSG SIZE  rcvd: 111

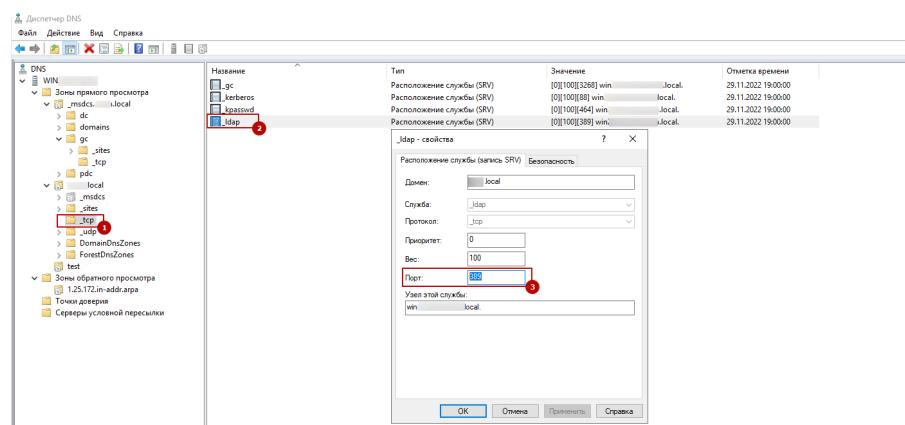
```

В графическом виде можно проверить используемые порты можно по путям:

1. Оснастка DNS – Имя DNS сервера – Зоны прямого просмотра – _msdcs.domain.name – gc – _tcp – _ldap .



2. Оснастка DNS – Имя DNS сервера – Зоны прямого просмотра – domain.name – _tcp – _ldap .



3. Решение

Измените значения текущих портов, на значения по умолчанию. По умолчанию LDAP работает на порту 389, GC на порту 3268.

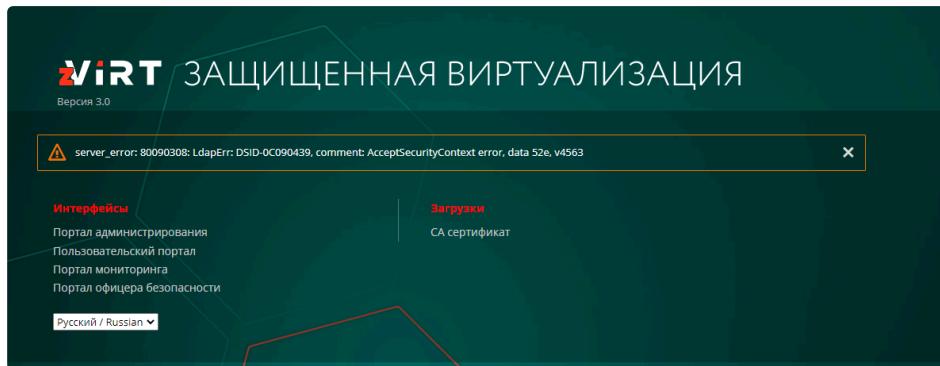


Ошибка "server error data 52e" при авторизации

1. Ошибка

При авторизации по протоколу LDAP:

```
server_error: 80090308: LdapErr: DSID-0C090439, comment: AcceptSecurityContext error, data 52e, v4563
```



2. Решение

Ошибка возникает из-за неверного логина/пароля в файле `/etc/ovirt-engine/aaa/domain.properties`, где `domain` имя Вашего домена.

Необходимо ввести корректный логин в переменную `vars.user` и корректный пароль `vars.password`. Например:

```
include = <ad.properties>

vars.domain = test.local
vars.user = CN=Qwerty_Qwerty,CN=Users,DC=test,DC=local
vars.password = mypassword

pool.default.auth.simple.bindDN = ${global:vars.user}
pool.default.auth.simple.password = ${global:vars.password}
pool.default.serverset.type = srvrecord
pool.default.serverset.srvrecord.domain = ${global:vars.domain}
```