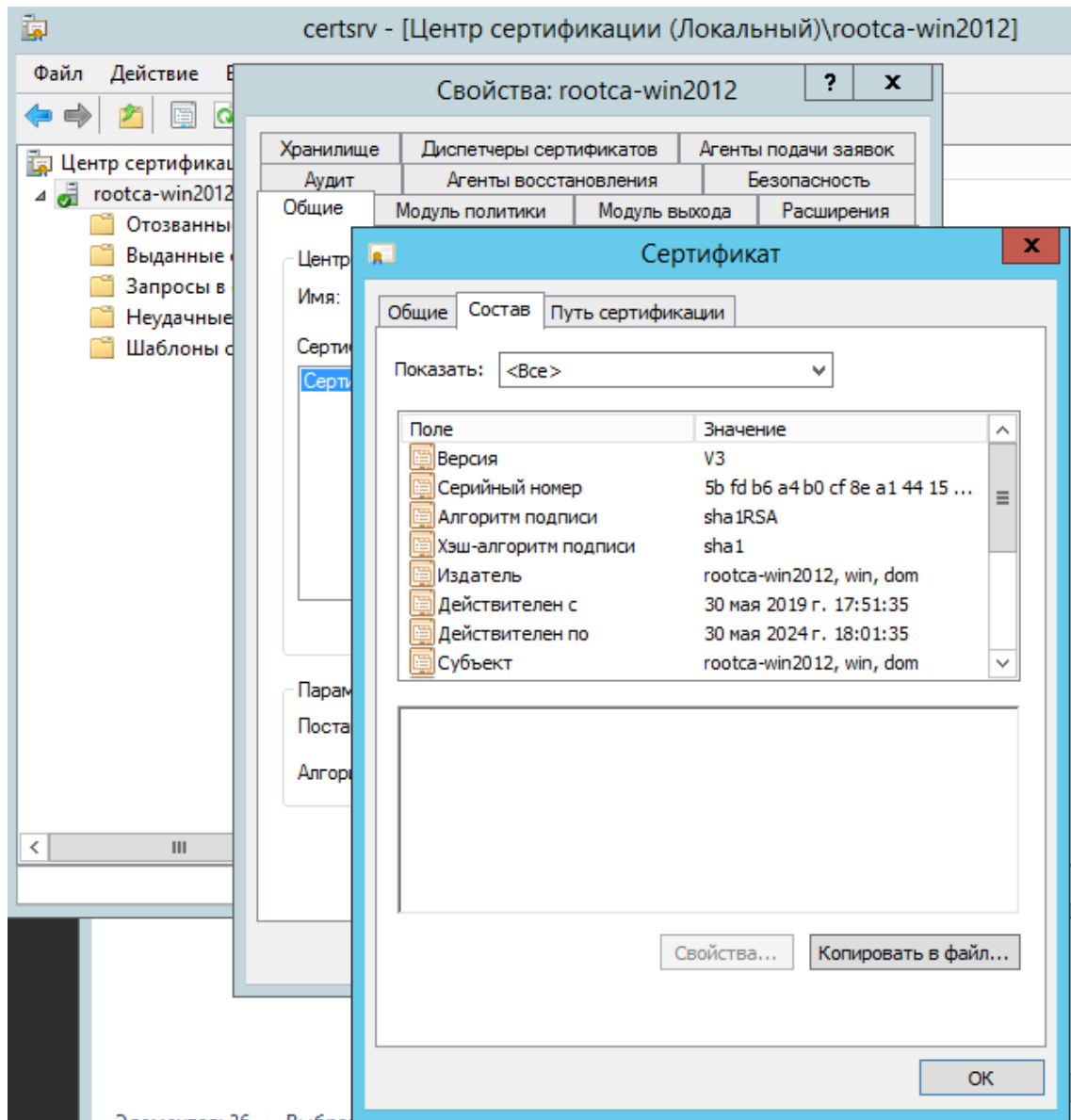


Миграция пользователей из AD DS 2012 в FreeIPA

1 Настройка на WS 2012

1.1 Экспорт сертификата корневого центра

На WS должна быть настроена Служба сертификации Active Directory. Необходимо сделать экспорт сертификата корневого центра с Windows Server для сервера FreeIPA. Для этого запускаем оснастку certsrv.msc и копируем в файл **winrootca.cer** сертификат (в кодировке Base-64) :

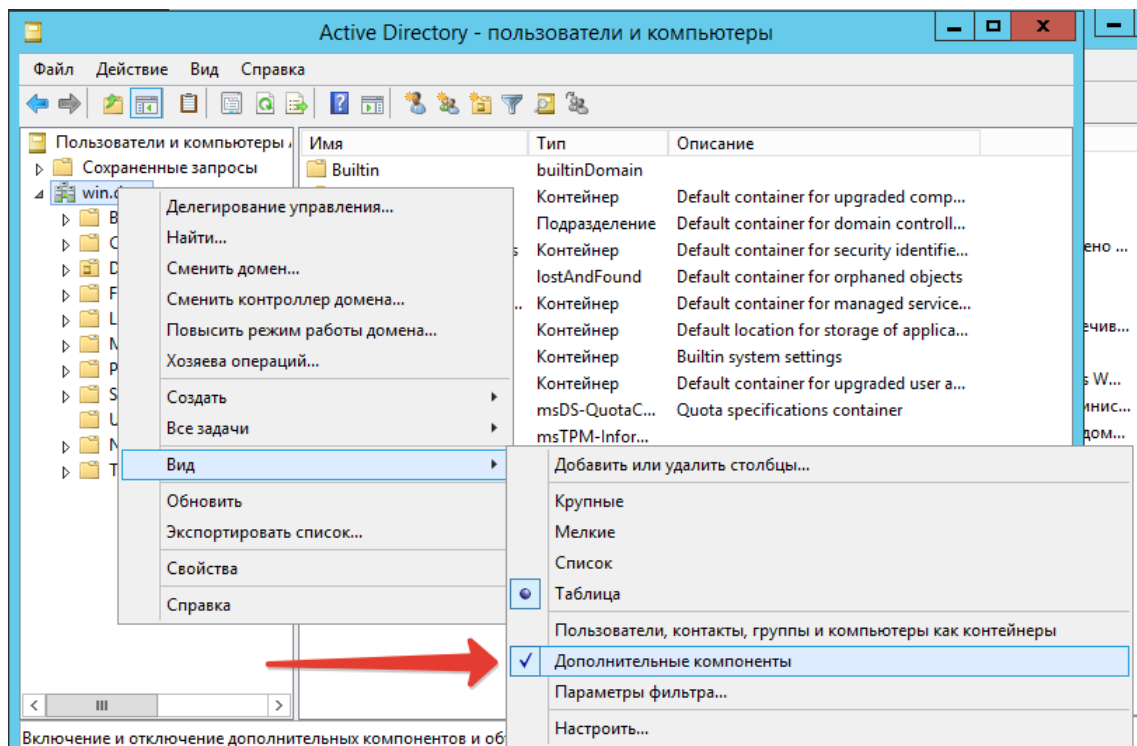


1.2 Создание пользователя для синхронизации

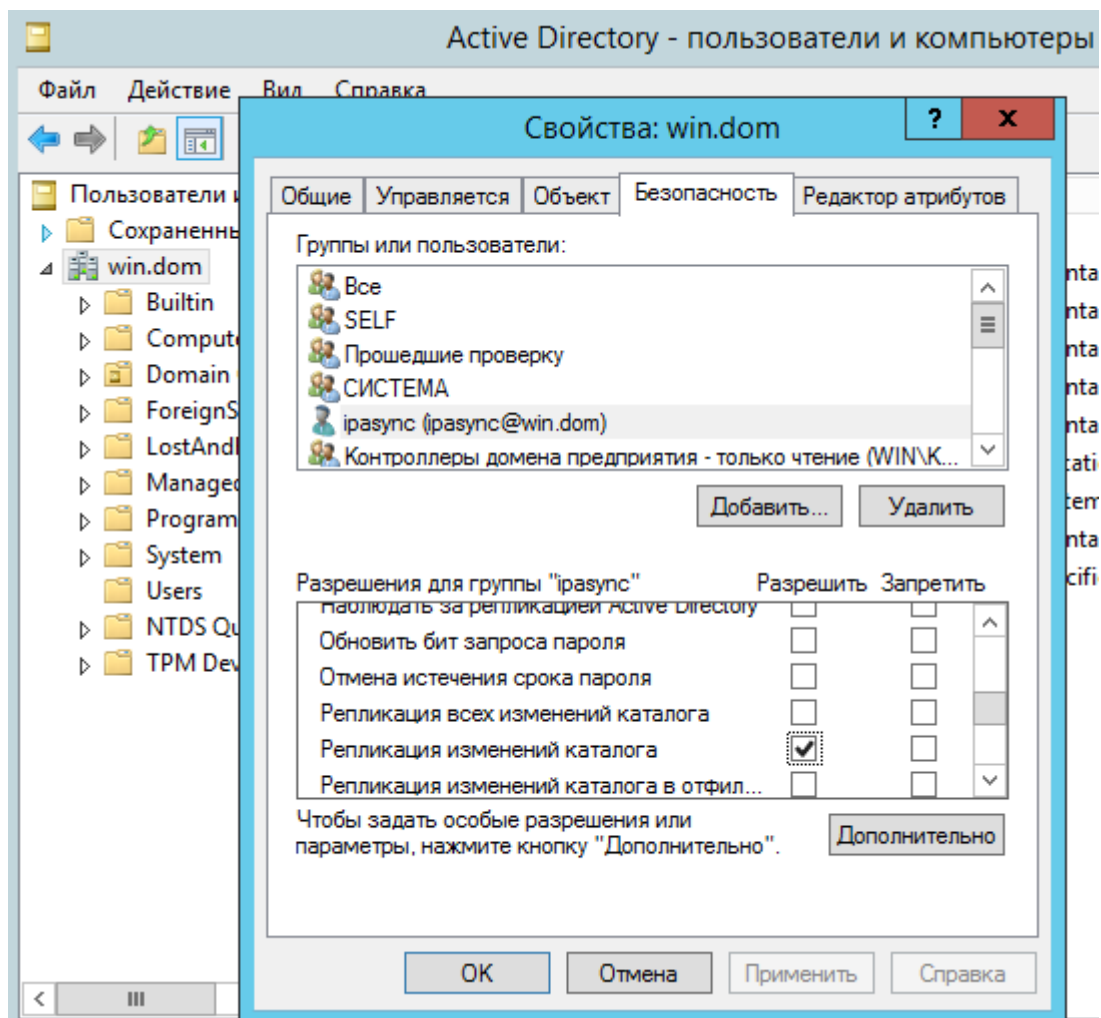
Далее на Windows Server создаем пользователя "ipasync" для синхронизации с FreeIPA. Данный пользователь должен быть включен в группы:

- "Контроллеры домена предприятия - только чтение"
- "Операторы учета"
- "Пользователи домена"

Включаем отображение "Дополнительные компоненты" :



В свойствах домена, добавляем пользователя ipasync и разрешаем репликацию изменений каталога.

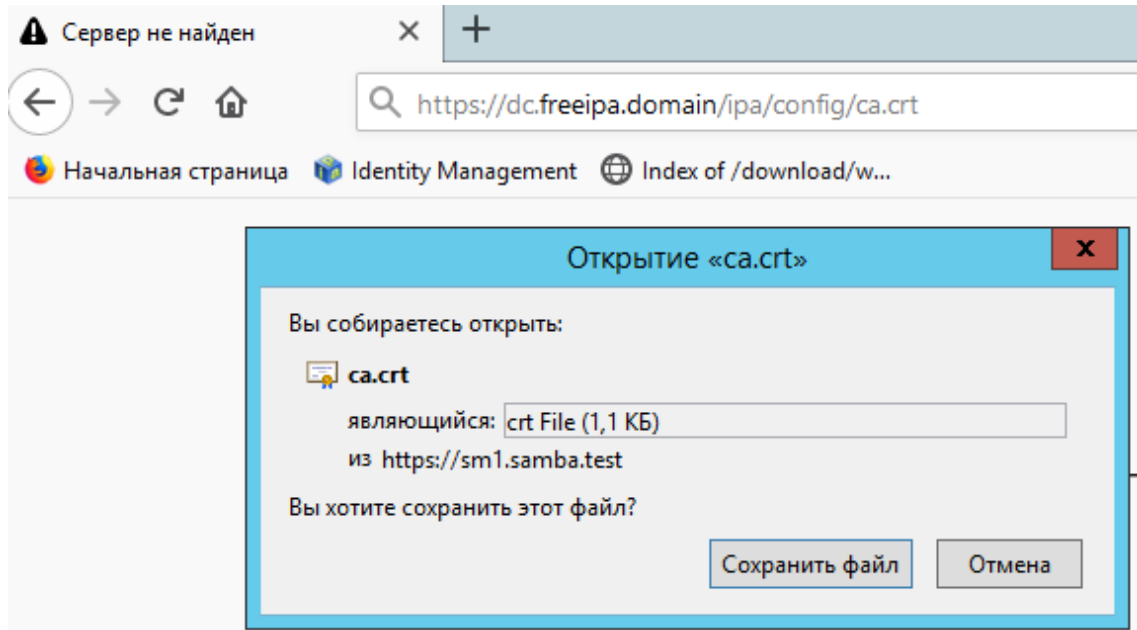


1.3 Сохранение сертификата с сервера FreeIPA

Необходимо зайти браузером (например Firefox) с Windows Server по адресу :

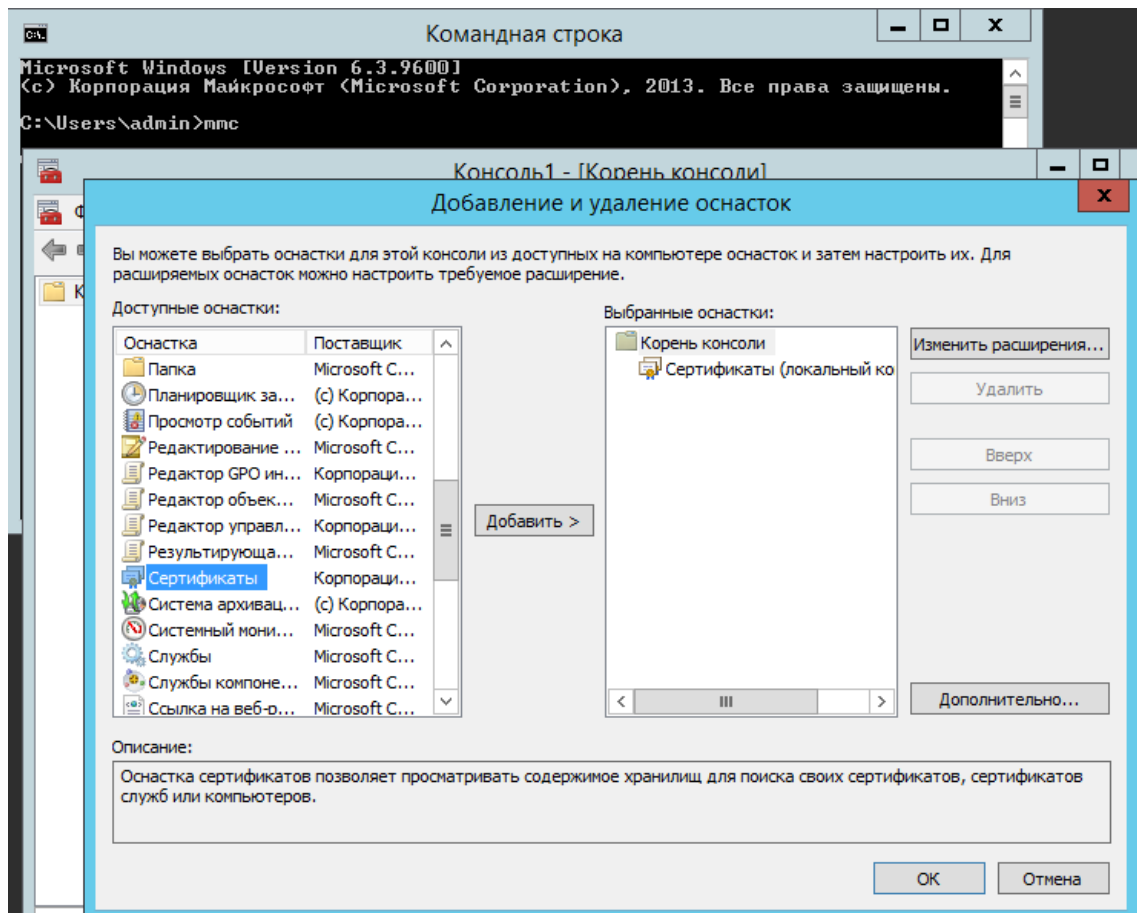
<https://dc.freeipa.domain/ipa/config/ca.crt>

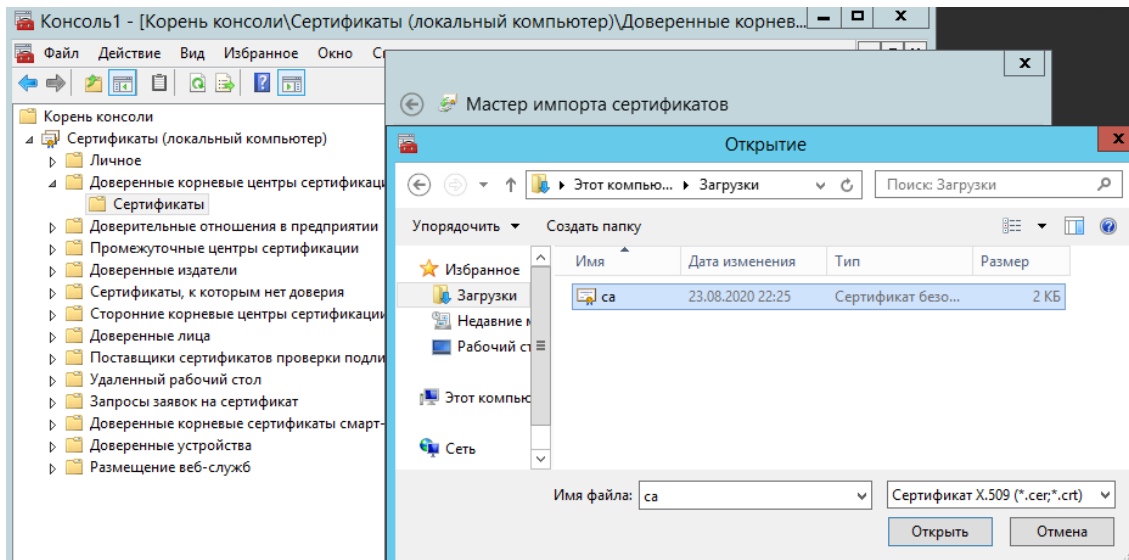
И сохранить файл:



1.4 Импорт сертификата FreeIPA

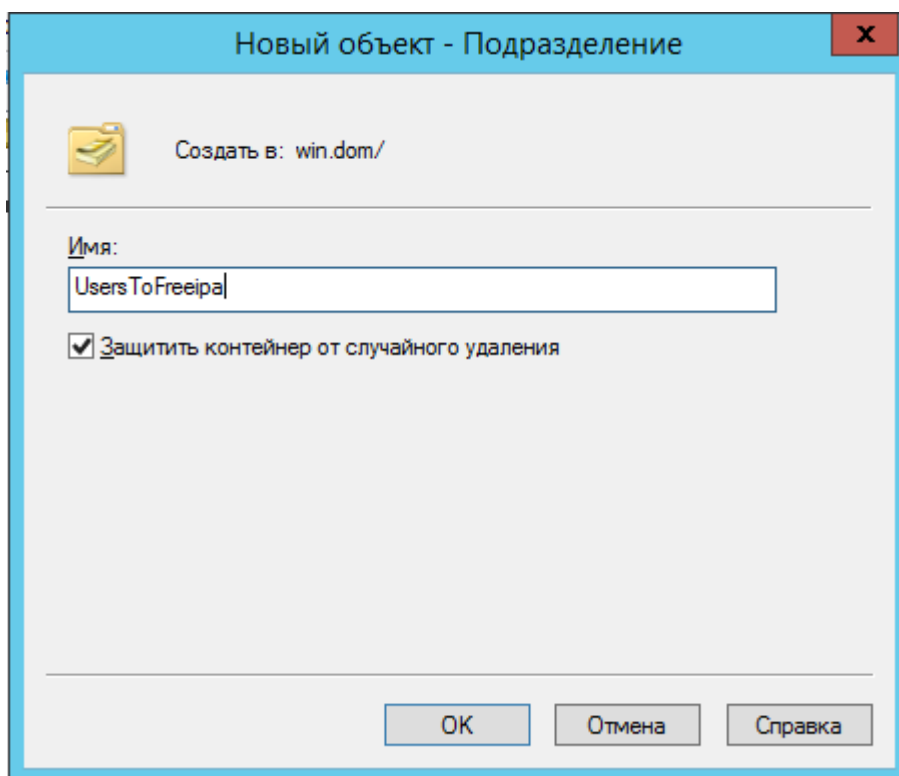
Добавляем оснастку "Сертификаты" и импортируем сертификат FreeIPA:





1.5 Создание контейнера для синхронизации пользователей

В Active Directory необходимо создать контейнер (OU) через который будут синхронизироваться/переноситься пользователи:



2 Настройка сервера FreeIPA

2.1 Импорт сертификата Windows Server

Кладем ранее сохраненный корневой сертификат с Windows Server на КД FreeIPA в `/etc/ssl/Microsoft/winrootca.cer` (Предварительно создав папку `/etc/ssl/Microsoft`)

2.2 Создание соглашения о синхронизации

Используется команда `ipa-replica-manage connect` с параметрами:

Параметры	Описание
<code>--winsync</code>	Ключ для установки синхронизацию с Active Directory
<code>--binddn</code>	Пользователь в формате DN, который используется для работы синхронизации между FreeIPA и Active Directory. Необходимо предварительно создать учетную запись в домене Active Directory и наделить разрешением на репликацию, чтение, поиск и записей в Active Directory.
<code>--bindpw</code>	Пароль для пользователя синхронизации.
<code>--passync</code>	Задаёт пароль для дополнительной учетной записи специального пользователя "passync", которая используется службой Password Synchronization на Windows Server.
<code>--cacert</code>	Полный путь к файлу сертификата центра сертификации Active Directory.
<code>--win-subtree</code>	Указывается DN поддерева домена в Active Directory, в котором находятся учетные записи пользователей для синхронизации.

Если параметр **"--win-subtree"** не задан, то по умолчанию используется значение `cn = Users, $ SUFFIX` и после начала действия соглашения о синхронизации ТОЛЬКО НОВЫЕ пользователи в OU "Users" будут скопированы из Active Directory в FreeIPA. А если задать специальный OU "UsersToFreeipa", то синхронизироваться будут пользователи, которые копируются или создаются в этом Контейнере.

Перед настройкой синхронизации необходимо удалить существующие Kerberos билеты, командой: `kdestroy`

И далее выполнить команду создания соглашения о синхронизации: `admin@dc:/$ sudo ipa-replica-manage connect --winsync --binddn cn=ipasync,cn=Users,dc=win,dc=dom --bindpw 12345678 --win-subtree "OU=UsersToFreeipa,DC=win,DC=dom" --passsync 12345678 --cacert /etc/ssl/Microsoft/winrootca.cer w2012r2.win.dom` Результат удачной настройки синхронизации должен быть таким:

```
admin@dc:/$ sudo ipa-replica-manage connect --winsync --binddn
cn=ipasync,cn=Users,dc=win,dc=dom --bindpw 12345678 --win-subtree
"OU=UsersToFreeipa,DC=win,DC=dom" --passsync 12345678 --cacert
/etc/ssl/windows/winrootca.cer w2012r2.win.dom
Directory Manager password:

Added CA certificate /etc/ssl/windows/winrootca.cer to certificate
database for dc.freeipa.domain
The user for the Windows PassSync service is
uid=passsync,cn=sysaccounts,cn=etc,dc=freeipa,dc=domain
Windows PassSync system account exists, not resetting password
Starting replication, please wait until this has completed.

Update succeeded

Connected 'dc.freeipa.domain' to 'w2012r2.win.dom'
admin@dc:/$
```

Во время настройки синхронизации на сервере FreeIPA автоматически создается дополнительная учетная запись "**passsync**" для работы службы Password Synchronization на Windows Server.

При настройке синхронизации производится проверка существования учетной записи PassSync и выводится сообщение о результате.

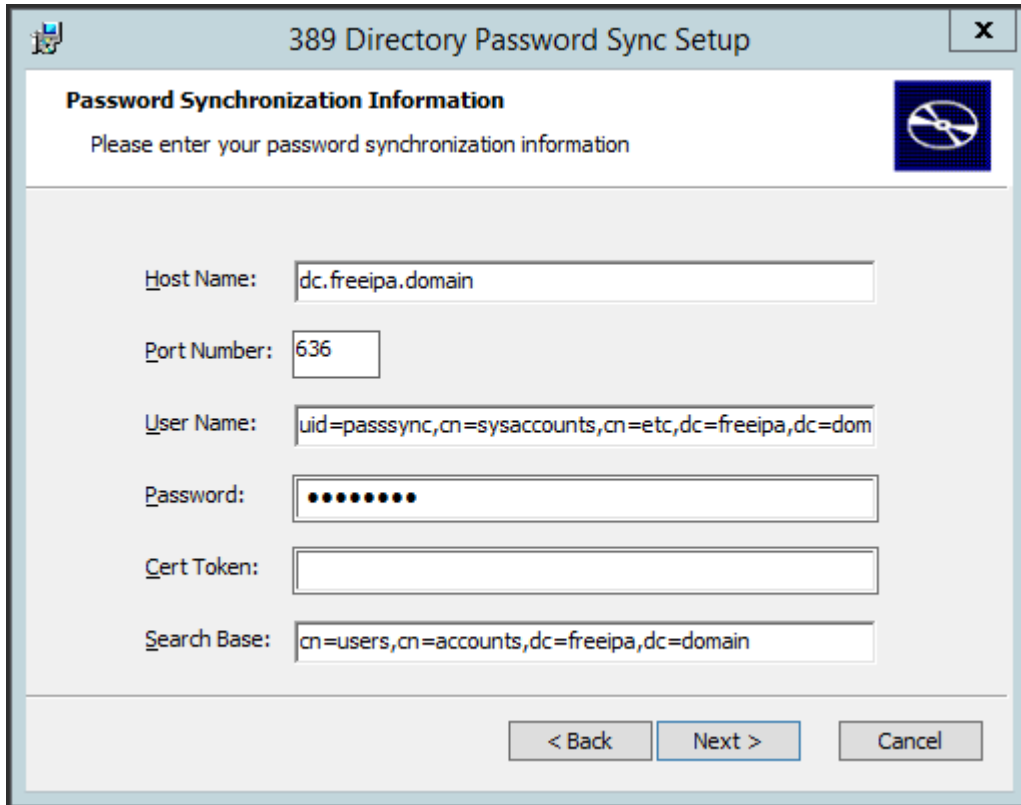
По умолчанию uid=passsync,cn=sysaccounts,cn=etc,dc=freeipa,dc=domain . Пароль, задается через параметр "**--passsync**", при создании соглашения о синхронизации.

3 Установка ПО на WS 2012 для синхронизации паролей

Далее устанавливаем с сайта fedoraproject.org последнюю версию программы 389-PassSync :

<https://directory.fedoraproject.org/docs/389ds/download.html#windows-password-synchronization>

И настраиваем подключение к серверу FreeIPA, пример:



```
cd "c:\Program Files\389 Directory Password Synchronization"  
certutil.exe -d . -A -n "DC.FREEIPA.DOMAIN IPA CA" -t "CT,," -a -i  
ipaca.crt
```

Делаем проверку сертификата:

```
certutil.exe -d . -L -n "DC.FREEIPA.DOMAIN IPA CA"
```

Дополнительно можно ориентироваться на инструкцию с сайта RedHat:

https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html-single/windows_integration_guide/index#setting-up-pass-sync

4 Проверка синхронизации

В Active Directory создаем нового пользователя или переносим существующего, в ранее созданное Подразделение "UsersToFreeipa" и через 1-3 минуты он появится в списке пользователей в FreeIPA.

Необходимо обратить внимание на заполнение полей пользователя (минимальный набор полей с которым выполняется синхронизация)
Например, если поле Фамилия не указан, то синхронизация выполняться не будет, в логах появится ошибка - "не указан атрибут sn".

Active Directory - пользователи и компьютеры

Копировать объект - Пользователь

Создать в: win.dom/Users

Имя: Инициалы:

Фамилия:

Полное имя:

Имя входа пользователя: @win.dom

Имя входа пользователя (пред-Windows 2000):

< Назад Далее > Отмена