Миграция пользователей из AD DS 2012 в FreeIPA

1 Настройка на WS 2012

1.1 Экспорт сертификата корневого центра

Ha 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) :

| ī. | certsrv - | [Центр сертиф | икации (Л | Іокаль | ьный)\rootca-win20 | 12] |
|--|--------------------------------------|---|---|---|--|-----|
| Файл Действие В | | Свойства: го | ootca-win2 | 2012 | ? X | |
| ↓ Центр сертификац ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ | Хранилище Аудит Общие Центр | Диспетчеры серт Агенты восста Модуль политики | ификатов новления Модуль вы Серт | Агенть Б хода ГИФИК | а подачи заявок резопасность Расширения ат | x |
| 🤗 Неудачные 🎦 Шаблоны с | Серти | Общие Состав Пу Показать: Состав Пу | ть сертифика | Зирия | × | |
| | Парам Поста | Версия Серийный номер Алгоритм подпи Хэш-алгоритм п Издатель Действителен п Действителен п Субъект | о іси одписи : : 10 | V3 Sb fd b sha 1R: sha 1 rootca 30 mas rootca | ние 56 a4 b0 cf 8e a1 44 15 SA -win2012, win, dom a 2019 г. 17:51:35 a 2024 г. 18:01:35 -win2012, win, dom | |
| < | Алгорі | | C | зойства | Копировать в файл | 1 |
| 2 | D Coul | | | | 0 | |

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.

| | Active Directory - пользователи и компьютер | ры |
|---|---|---|
| Файл Действие | Вил Справка | 1 |
| 🗢 🔿 🔁 🖬 | Свойства: win.dom ? 🗙 | |
| Пользователи и Сохраненны № Пользователи и № Сохраненны № Вuiltin № Domain № Domain № ForeignS № LostAndi № Nanageo № Program № System № System № NTDS Qu № TPM Dev | Общие Управляется Объект Безопасность Редактор атрибутов Группы или пользователи: | nta nta nta :ati :em nta cifi |
| < 111 | ОК Отмена Применить Справка | |

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: |
|---|-----------|-------|
|---|-----------|-------|

| А Сервер не найден | × + |
|---------------------------|--|
| ← → ⊂ ŵ | Q https://dc. freeipa.domain /ipa/config/ca.crt |
| ۏ Начальная стран | ица 🛭 📦 Identity Management 🛛 Index of /download/w |
| | Открытие «ca.crt» |
| | Вы собираетесь открыть: Гасти являющийся: crt File (1,1 КБ) из https://sm1.samba.test Вы хотите сохранить этот файл? Сохранить файл |

1.4 Импорт сертификата FreeIPA

Добавляем оснастку "Сертификаты" и импортируем сертификат FreeIPA:

| C:4. | | 1 | Kon | иандная стро | ка | _ 🗆 X |
|------------------------------|---|------------------------------------|--------------|--------------------------------------|---|-----------------------|
| Micros (c) Koj C:\Use: | icrosoft Windows [Version 6.3.9600] с) Корпорация Майкрософт (Microsoft Corporation), 2013. Все права защищены. ∷\Users\admin>mmc | | | | | |
| | | | к До | Консоль1 - [Ки бавление и у, | орень консоли] даление оснасток | = = × |
| | Вы можете выбрать осна расширяемых оснасток м | астки для этой к южно настроить | онс о тре | оли из доступных ебуемое расширен | на компьютере оснасток и затем нас ие. | троить их. Для |
| | Доступные оснастки: | | _ | 7 | Выбранные оснастки: | , [|
| | Оснастка | Поставщик | ^ | | Корень консоли | Изменить расширения |
| | Папка | Microsoft C | | | Сертификаты (локальный ко | Удалить |
| | Планировщик за | (c) Kopnopa | | | | |
| | Редактирование | Microsoft C | | | | Pasau |
| | Редактор GPO ин | Корпораци | | | | вверх |
| | 🗐 Редактор объек | Microsoft C | | | | Вниз |
| | 🗾 Редактор управл | Корпораци | ≡ | Добавить > | | |
| | 🗐 Результирующа | Microsoft C | | | | |
| | 🙀 Сертификаты | Корпораци | | | | |
| | 🌆 Система архивац | (с) Корпора | | | | |
| | 🔊 Системный мони | Microsoft C | | | | |
| | 🔍 Службы | Microsoft C | | | | |
| | 🖲 Службы компоне | Microsoft C | | | | Пополнитольно |
| | 🔮 Ссылка на веб-р | Microsoft C | ~ |] | | дополнительно |
| | Описание: | | | | | |
| | Оснастка сертификатов | в позволяет про | смат | гривать содержим | ое хранилищ для поиска своих серти | фикатов, сертификатов |
| | служб или компьютеров | 3. | | | • | |
| | | | | | | |
| | | | | | | |
| | | | | | | ОК Отмена |
| | | | | | | |

| \overline Консоль1 - [Корень консоли\Сертификаты (локальный компьютер)\Доверенные корнев 💻 🗖 🗙 | | | | |
|--|---|-----|--|--|
| 🖀 Файл Действие Вид Избранное Окно Со | К мастер импорта сертификатов | | | |
| Корень консоли Сертификаты (локальный компьютер) Паниное | С Открытие Открытие | c | | |
| Доверенные корневые центры сертификаци Сертификаты | |] | | |
| ▷ ☐ Доверительные отношения в предприятии ▷ ☐ Промежуточные центры сертификации ▷ ☐ Доверенные издатели | Упорядочить Создать папку ВП Создать папку ВП | | | |
| ▷ Сертификаты, к которым нет доверия ▷ Cropoнние корневые центры сертификации ▷ Absepenные лица ▷ Crasщики сертификатов проверки подли | Загрузки Са 23.08.2020 22:25 Сертификат безо 2 КБ В Недавние и В абочий ст ≡ В або | | | |
| Удаленный рабочий стол Запросы заявок на сертификат Доверенные корневые сертификаты смарт- Доверенные устройства Доверенные рабосложба | ј∰ Этот компькс | | | |
| | Имя файла: са v Сертификат X.509 (*.cer;*.crt) v Открыть Отмена | .41 | | |

1.5 Создание контейнера для синхронизации пользователей

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

| Новый объект - Подразделение 🛛 🗙 |
|---|
| Создать в: win.dom/ |
| <u>И</u> мя: |
| UsersToFreeipa |
| Защитить контейнер от случайного удаления |
| |
| |
| |
| |
| |
| |
| ОК Отмена Справка |

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 | | | |
|--|---|--|--|--|
| winsync | Ключ для установки синхронизацию с Active Directory | | | |
| binddn | 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. | | | |
| bindpw | Пароль для пользователя синхронизации. | | | |
| passync | Задает пароль для дополнительной учетной записи специального пользователя "passsync", которая используется службой Password Synchronization на Windows Server. | | | |
| cacert | Полный путь к файлу сертификата центра сертификации Active Directory. | | | |
| win-subtree | Указывается DN поддерева домена в Active Direcoty, 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 Direcoty 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 ipareplica-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 <u>fedoraproject.org</u> последнюю версию программы 389-PassSync :

https://directory.fedoraproject.org/docs/389ds/download.html#windows-passwordsynchronization

И настраиваем подключение к серверу FreeIPA, пример:

| 谩 | 389 Directory Password Sync Setup |
|--|--|
| Password Synchron Please enter your p | nization Information assword synchronization information |
| <u>H</u> ost Name: <u>P</u> ort Number: <u>U</u> ser Name: | dc.freeipa.domain 636 uid=passsync,cn=sysaccounts,cn=etc,dc=freeipa,dc=dom |
| Password: Cert Token: | |
| <u>S</u> earch Base: | cn=users,cn=accounts,dc=freeipa,dc=domain |
| | < Back Next > Cancel |

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

4 Проверка синхронизации

В Active Directory создаем нового пользователя или переносим существующего, в ранее созданное Подразделении "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 выполнятся не будет, в логах появится ошибка - "не указан атрибут sn".

| | Acti | ve Directory - пользователи и компьн | | | |
|---------------------------------|---|--------------------------------------|--|--|--|
| Файл | Копировать о | бъект - Пользователь 🛛 🗙 – | | | |
| | | | | | |
| <mark>⊇</mark> ⊓o ▷ 篇 ⊿ 💏 | 🔏 Создать в: win.dom/ | /Users | | | |
| | Имя: | Инициалы: | | | |
| | Фамилия: winuser2 | | | | |
| Þ | Полное имя: winuser2 | | | | |
| | Имя входа пользователя: | | | | |
| Þ | winuser2 | @win.dom v | | | |
| Þ | Имя входа пользователя (пред-Windows 2000); | | | | |
| Þ | WIN\ | winuser2 | | | |
| | | | | | |
| | | | | | |
| | | < Назад Далее > Отмена н | | | |
| L | | , T | | | |