База знаний РЕД АДМ

- РЕД АДМ
  - Описание РЕД АДМ
  - Системные требования для РЕД АДМ
  - Подготовка окружения
  - Установка РЕД АДМ Стандартная редакция
    - Установка РЕД АДМ Сервер
    - Установка РЕД АДМ Клиент
  - Обновление РЕД АДМ
    - Обновление РЕД АДМ Сервер версии 1.1.0
    - Обновление РЕД АДМ Сервер версии 1.9.1
    - Обновление РЕД АДМ Клиент
  - Диагностика проблем
  - Полезные статьи
    - Переход с Microsoft Active Directory на РЕД АДМ. Два подхода к миграции ИТ-инфраструктуры
  - Часто задаваемые вопросы (FAQ)

Описание РЕД АДМ

РЕД АДМ Сервер
РЕД АДМ Клиент

###ENV###

РЕД АДМ Сервер

РЕД АДМ Сервер позволяет управлять контроллером домена и автоматизирует типовые задачи администратора с парком рабочих станций и серверов на базе РЕД ОС. Система имеет веб-интерфейс управления.

Продукт имеет модульную структуру и может агрегировать в себе множество модулей администрирования различного назначения.

РЕД АДМ комплексно решает задачи:

- администрирования доменных учетных записей;
- централизованного управления рабочими станциями;
- журналирования операций.

Дистрибутив **РЕД АДМ Сервер** находится в стандартном репозитории РЕД ОС и представляет из себя rpm-пакет.

ВАЖНО!

Техническая поддержка по продукту РЕД АДМ из репозитория предоставляется **только** при действующем сертификате технической поддержки для РЕД ОС конфигурации «**Сервер**».

РЕД АДМ Клиент

РЕД АДМ Клиент – это клиентское приложение для взаимодействия с сервером РЕД АДМ.

РЕД АДМ Клиент необходим для применения распространяемых конфигураций на рабочей станции в автоматическом режиме (режим «pull»), а также для сбора статистики и лога с клиентских рабочих станций.

Дистрибутив **РЕД АДМ Клиент** находится в стандартном репозитории РЕД ОС и представляет из себя rpm-пакет.

Системные требования для РЕД АДМ

###ENV###

Системные требования для РЕД АДМ Сервер

РЕД АДМ Сервер устанавливается на РЕД ОС конфигурации **Сервер** версии **7.3 и выше**. Системные требования для **РЕД ОС Сервер 7.3** см. по ссылке на вкладке «**Системные требования**».

Конфигурация	Минимальные требования
Центральный процессор	4 ядра по 2 ГГц
ОЗУ	4 ГБ
Хранилище	100 ГБ (желательно SSD)

Системные требования для РЕД АДМ Клиент

Минимальные требования к оборудованию совпадают с требованиями к операционной системе, на которую устанавливается **РЕД АДМ Клиент**.

ВАЖНО!

РЕД АДМ Клиент устанавливается и полноценно поддерживается **только на РЕД ОС**.

Требования к веб-управлению

Для доступа к веб-управлению необходимо наличие одного из следующих браузеров:

- **Chromium** версии **90.x** или выше;

- **FireFox** версии **78.x** или выше:
- **Яндекс.Браузер** версии **22.7.5** или выше.

Подготовка окружения

###ENV###

Для развертывания системы РЕД АДМ потребуется:

1. *Установленная операционная система* ***РЕД ОС*** *конфигурации* ***Сервер****, необходимая для установки* ***РЕД АДМ Сервер****.*

Системные требования для **РЕД ОС Сервер 7.3** см. по ссылке на вкладке «**Системные требования**».

Системные требования для **РЕД АДМ Сервер** указаны в разделе «Системные требования».

2. *Развернутый контроллер домена.*

Контроллер домена должен быть на базе *подсистемы службы каталогов РЕД АДМ* (**reddc**), *Samba DC* или *Microsoft Active Directory* (**MS AD**).

В целях безопасности рекомендуется создать *две сервисные учетные* записи:

- первая (**redadm**) — для администрирования РЕД АДМ;
- вторая (имя задается вручную) — для подключения к LDAP-каталогу домена.

Пользователю **redadm** необходимо предоставить права на чтение доменного каталога. С помощью этой учетной записи производится подключение к контроллеру домена и назначение роли администратора другим пользователям. После выполнения всех манипуляций необходимо выйти на сервере РЕД АДМ из этой учетной записи, после чего заблокировать этого пользователя в домене.

Вторая учетная запись, имя которой задается вручную, необходима для чтения LDAP-каталога домена и должна быть всегда активна.

> **Примечание.**
>
> Не рекомендуется использовать сервисную учетную запись для работы в РЕД АДМ. Оптимальным вариантом является настройка прав в ролевой системе РЕД АДМ для других учетных записей в домене.

В целях безопасности учетную запись **redadm** необходимо создавать со сложным паролем длиной **более 8 символов**, содержащим строчные (**a-z**) и

прописные (**A-Z**) буквы, цифры (**0-9**), а также **хотя бы один специальный символ**, иначе во входе в веб-интерфейс РЕД АДМ будет отказано.

3. *Компьютеры (клиентские машины), на которые будет установлен* ***РЕД АДМ Клиент****.*

Эти машины необходимо ввести в ваш домен (к которому подключается РЕД АДМ).

РЕД АДМ требует прямого доступа по сети между сервером РЕД АДМ и клиентом по TCP-портам **22** и **80** (или **443** в случае использования *SSL*).

Клиентское приложение РЕД АДМ можно либо распространить встроенными средствами РЕД АДМ, либо установить из репозитория или rpm-пакета.

Примечание.

При установке **РЕД АДМ Клиент** из репозитория или rpm-пакета необходимо заполнить конфигурационный файл, подробную информацию см. в статье «Установка РЕД АДМ Клиент».

Установка РЕД АДМ Сервер

###ENV###

Установка РЕД АДМ Сервер

Пакеты установки РЕД АДМ поставляются в составе стандартного репозитория.

Для установки **РЕД АДМ Сервер** в терминале перейдите в сеанс пользователя **root**:

```
su -
```

Обновите и перезагрузите систему:

```
dnf update
reboot
```

Здесь и далее команды выполняются с правами пользователя **root**, если не указано иное.

Установка **РЕД АДМ Сервер** из репозитория производится командой:

```
dnf install redadm
```

Для установки **РЕД АДМ Сервер** из RPM-пакета необходимо открыть директорию с RPM-пакетом и выполнить команду:

```
dnf install <имя_пакета>.rpm
```

Настройка после установки

Настройка файла конфигурации сервера

Отредактируйте серверный конфигурационный файл

/etc/redadm/server.conf командой:

```
nano /etc/redadm/server.conf
```

Основные настройки

Секция `[BASE_SETTINGS]` отражает основные настройки РЕД АДМ:

- `CERT_PATH = <путь_к_сертификату>` – сертификат используется для подключения по **ldaps** и **https**. По умолчанию указан демо-сертификат;
- `SECRET_KEY = <ключ>` – автогенерируемый параметр, отображается в зашифрованном виде. Представляет собой ключ приложения, который используется для шифрования паролей и создания токенов авторизации;
- `DEFAULT_SSH_USER = <имя_пользователя>` – в случае автоматического добавления клиентского хоста указанный пользователь будет использоваться для обращения к этому клиенту. Для данного пользователя должны быть заранее распространены ssh-ключи.

Секция `[LDAP]` отражает настройки подключения к вашему домену:

- `LDAP_URL = ldaps://<IP-адрес>:<порт>` – LDAP-адрес контроллера домена (по умолчанию используется *порт 636*);
- `LDAP_DOMAIN_NAME = <имя>` – LDaP-имя контроллера домена;
- `LDAP_DC_END = <имя>` – имя в формате DC;
- `USERNAME_LDAP = <имя_пользователя>` – имя доменного пользователя, с помощью которого РЕД АДМ будет совершать LDAP-запросы на чтение. Используется для работы механизма распространения конфигураций;
- `PASSWORD_LDAP = <пароль_доменного_пользователя>` – пароль доменного пользователя.

Для шифрования пароля доменного пользователя после сохранения конфигурационного файла выполните команду:

```
/opt/redadm/.venv/bin/python /opt/redadm/scripts/encrypt_config.py -a
"PASSWORD_LDAP"
```

Дополнительные настройки

Секция `[SYSLOG]` отражает настройки ведения журналов:

- `SYSLOG_ENABLE` – включение syslog;

- SYSLOG_DEFAULT – директория для хранения логов;
- SYSLOG_IP – IP-адрес сервера syslog (должен быть настроен syslog backend и закомментирована строка с SYSLOG_DEFAULT);
- SYSLOG_PORT – порт сервера syslog.

Секция [OTHER] содержит дополнительные настройки:

- PULL_NUMBER_TASKS = *<число>* – число запросов на получение конфигураций в режиме «pull», которые **РЕД АДМ Сервер** будет обслуживать одновременно.

ВАЖНО!

Убедитесь, что в системе установлен правильный DNS-сервер, разрешающий A-записи DNS контроллера домена. Проверку разрешения A-записи можно запустить командой:

```
nslookup <имя_контроллера_домена>
```

либо

```
ping <имя_контроллера_домена>
```

При правильной настройке DNS-сервера в ответе команды будет выведена информация с IP-адресом домена, а запросы обработаны.

Установить DNS-сервер можно в настройках сетевого адаптера, проверить – в файле **/etc/resolv.conf**. Подробную информацию по настройке и проверке корректности конфигурации DNS-сервера см. в наших инструкциях «Настройка сетевого адаптера» и «Настройка DNS».

Также следует проверить синхронизацию времени с контроллером домена, это необходимо для обеспечения шифрованного подключения к LDAP-каталогу домена. Подробнее см. инструкцию «Настройка синхронизации времени».

Примечание.

Сценарий установки **РЕД АДМ Сервера** настроит параметры *Ansible* в файле конфигурации **/etc/ansible/ansible.cfg**.

Параметр **forks** отвечает за максимальное количество потоков, которые *Ansible* будет использовать для выполнения задач на целевых хостах. Это количество используется при распространении клиентского агента и VNC, а также в ручном режиме применения конфигураций.

Параметр **timeout** отвечает за время ожидания по умолчанию для подключающихся клиентов. Возникает в случаях недоступности клиентского хоста.

Для установки или обновления *Ansible* до версии **6.X** воспользуйтесь инструкцией «Ansible - система автоматизации настройки и развертывания ПО».

Настройка файла конфигурации клиента

Отредактируйте конфигурационный файл клиента **/etc/redadm/client.conf**.

ВАЖНО!

Синтаксис файла конфигурации **чувствителен** к регистру!

```
nano /etc/redadm/client.conf
```

```
[SETTINGS]
 # IP-адрес вашего сервера РЕД АДМ, к которому будут подключаться клиенты
 IP=10.1.1.2
 # порт, к которому будут подключаться клиенты РЕД АДМ
 # по умолчанию используется порт 80
 PORT=80
 # использование https для обращения клиентов к серверу
 # по умолчанию используется значение False
 ENABLED_SECURE=False
 # путь к сертификату сервера РЕД АДМ на клиентской машине
 SECURE_CERTIFICATE=<путь_к_сертификату>
```

Запуск служб

После редактирования файлов конфигурации сервера и клиента для применения внесенных изменений необходимо запустить и добавить в автозагрузку следующие службы:

```
systemctl enable --now redadm.service redis.service redadm-celery-worker.service redadm-celery-beat.service nginx.service
```

Настройка HTTPS

Для настройки подключения с использованием **HTTPS** необходимо выполнить некоторые дополнительные настройки.

Самоподписанные сертификаты

Если центр сертификации отсутствует, можно использовать демо-сертификаты.

Для этого необходимо перейти в каталог с сертификатами:

```
cd /opt/redadm/configs/ssl
```

Здесь для дальнейшей работы потребуется непосредственно сам сертификат (**redadm-server.crt**) и ключ сервера (**redadm-server.key**), а также сертификат центра сертификации **DemoCA.pem**, который необходимо установить в качестве доверенного для браузера, где используется веб-интерфейс РЕД АДМ.

Если потребуется сгенерировать новые демо-сертификаты, необходимо запустить скрипт генерации из каталога **/opt/redadm/configs/ssl** командой:

```
./generate\_DemoCA.sh
```

После выполнения скрипта в выводе будут отображены полные пути сертификата и ключа, которые нужно прописать в конфигурационные файлы. Пример их заполнения приведен ниже.

Примечание.

При каждой новой генерации сертификата все имеющиеся в каталоге файлы будут зарезервированы в каталог с текущей датой.

Сторонний центр сертификации

Сгенерируйте сертификат для сервера РЕД АДМ в вашем центре сертификации. Требования к сертификату:

- значение параметра `cn` должно совпадать с доменным именем сервера РЕД АДМ;
- должны присутствовать поля `alt_names`, где прописаны все IP-адреса и DNS-имена, на которых будет доступен РЕД АДМ.

Пример конфигурационного файла параметров генерации для **openssl** можно просмотреть в файле **/opt/redadm/configs/ssl/ssl-conf.ext**.

Разместите сгенерированные сертификаты в каталог **/opt/redadm/configs/ssl**.

Настройка конфигурационных файлов

Настройте **nginx** в файле **/etc/nginx/nginx.conf**. Для этого закомментируйте секцию `[HTTP]`:

```
#[HTTP server]
 #
 # server {
 # listen 80;
 # ...
 #}
```

Затем раскомментируйте секцию `[HTTPS]`:

```
[HTTPS server]
 server {
 listen 443 ssl;
 server_name localhost;
 ssl_certificate /opt/redadm/configs/ssl/redadm-server.crt;
 ssl_certificate_key /opt/redadm/configs/ssl/redadm-server.key;
 ...
 }
```

В файле конфигурации сервера **/etc/redadm/server.conf** укажите путь к

сгенерированному сертификату в поле CERT_PATH.

В файле конфигурации клиента **/etc/redadm/client.conf** отредактируйте следующие параметры:

- PORT = 443;
- ENABLE_SECURE = True;
- SECURE_CERTIFICATE = *<путь_к_сертификату_на_клиентской_машине>*.

Перезапустите службы **redadm** и **nginx**:

```
systemctl restart redadm.service nginx.service
```

Дополнительные настройки при использовании домена MS AD

В данном подразделе описано создание сертификатов для обеспечения безопасных подключений по **SSL** между **сервером РЕД АДМ** и контроллером домена **Microsoft Active Directory**. Здесь рассмотрены два случая:

- в домене уже имеется центр сертификации: например, эту роль выполняет контроллер домена Active Directory;
- сертификат создаётся самостоятельно.

Использование существующего центра сертификации

Если вы подключаете РЕД АДМ к Microsoft Active Directory, и в домене уже поднята роль «**Центр сертификации**», убедитесь, что параметр CNGHashAlgorithm имеет значение SHA256, иначе в браузере потребуется подтвердить ненадежное SSL-соединение.

Для проверки параметра CNGHashAlgorithm требуется в командной строке Windows (где располагается *Центр сертификации*) выполнить:

```
certutil -getreg ca\csp\CNGHashAlgorithm
```

Опционально: для установки SHA256 и пересоздания (!) нового корневого сертификата в командной строке требуется выполнить:

```
```

```
certutil -setreg ca\csp\CNGHashAlgorithm SHA256
net stop CertSvc
net start CertSvc
certutil -renewCert ReuseKeys
net stop CertSvc
net start CertSvc
```

Далее для выпуска SSL-сертификатов требуется:

1. На Windows (где располагается *Центр сертификации*) запустите оснастку **Сертификаты**.

В командной строке или в окне «**Выполнить**» введите команду:

```
certmgr.msc
```

2. Правой клавишей мыши щелкните по пункту «**Личное**», и далее перейдите по элементам «**Все задачи**» — «**Дополнительные операции**» — «**Создать настраиваемый запрос...**».

3. Выберите значения параметров:

- *Настраиваемый запрос*: Продолжить без политики регистрации;
- *Шаблон*: Ключ CNG (без шаблона);
- *Формат запроса*: PKCS #10;

4. Раскройте выпадающее меню «**Подробности**» и выберите «**Свойства**». Рассмотрим заполнение свойств на примере домена **wind.lan**.

> **Примечание.**
>
> Сервер РЕД АДМ может и не быть членом домена. Но обязательно должна быть создана A-запись в службе DNS с указанием IP-адреса сервера РЕД АДМ и именем, используемым в сертификате.

Общие

- *Имя*: redadm.wind.lan;
- *Описание*: SSL Certificate.

Субъект

- *Имя субъекта (Тип: Общее имя)*: redadm.wind.lan;

- *Дополнительное имя (Тип: Служба DNS)*: redadm.wind.lan;
- *Дополнительное имя (Тип: IP-адрес (v4))*: впишите IP-адрес сервера РЕД АДМ.

Закрытый ключ

- *Поставщик службы шифрования*: RSA, Microsoft Software Key Storage Provider;
- *Параметры ключа*:
  - *Размер*: 2048;
  - Сделать закрытый ключ экспортируемым.

- *Выберите хэш-алгоритм*: По умолчанию.

5. Сохраните файл запроса в формате **Base64**. Например: **C:\requests\redadm.wind.lan.req**.

6. Выпустите сертификат командой:

```
certreq -submit -attrib "CertificateTemplate:webserver"
C:\requests\redadm.wind.lan.req C:\requests\redadm.wind.lan.cer
```

7. Добавьте выпущенный сертификат **redadm.wind.lan.cer** в «**Личное**».

Дважды щелкните по файлу сертификата, перейдите во вкладку «**Состав**» и нажмите «**Копировать в файл...**».

В открывшемся окне нажмите «**Далее**», выберите «**Да, экспортировать закрытый ключ**» и установите пароль.

Укажите путь и сохраните сертификат с расширением **pfx**. Например, **redadm.wind.lan.pfx**.

8. Экспортируйте корневой сертификат сервера, он понадобится для организации защищенного соединения между РЕД АДМ и компьютерами.

Перейдите на вкладку «**Доверенные корневые центры сертификации**» и нажмите на элемент «**Сертификаты**».

Дважды щелкните по корневому сертификату, перейдите во вкладку «**Состав**» и нажмите «**Копировать в файл...**».

Примечание.

У контроллера домена с именем **windc1.wind.lan** сертификат имеет вид **wind-WINDC1-CA**).

В открывшемся окне нажмите «**Далее**», выберите формат: **Файлы X.509 (.CER) в кодировке DER**.

Укажите путь и сохраните корневой сертификат с расширением **cer**. Например, **ca.cer**.

9. Загрузите файл полученного сертификата **pfx** и корневого сертификата **cer** на сервер с установленным РЕД АДМ и выполните следующие команды для извлечения сертификата и ключа. Потребуется вводить пароль, установленный на предыдущем шаге.

Извлеките сертификат:

```
openssl pkcs12 -in redadm.wind.lan.pfx -clcerts -nokeys -out redcert.crt
```

Извлеките ключ:

```
openssl pkcs12 -in redadm.wind.lan.pfx -nocerts -out temp.key
```

Удалите пароль с ключа:

```
openssl rsa -in temp.key -out redserver.key
```

Преобразуйте корневой сертификат в формат **crt**:

```
openssl x509 -inform DER -in ca.cer -out ca.crt
```

Скопируйте полученный сертификат в **/opt/redadm/configs/ssl/**:

```
cp redcert.crt /opt/redadm/configs/ssl/
cp redserver.key /opt/redadm/configs/ssl/
```

Установите владельца и права доступа:

```
chown redadm_local_service_user:redadm_local_service_user
/opt/redadm/configs/ssl/redcert.crt
chown redadm_local_service_user:redadm_local_service_user
/opt/redadm/configs/ssl/redserver.key
chmod 644 /opt/redadm/configs/ssl/redcert.crt
chmod 600 /opt/redadm/configs/ssl/redserver.key
```

Скопируйте преобразованный корневой сертификат **ca.crt** на клиентский компьютер в **/opt/redclient/**.

10. Откройте файл **/etc/nginx/nginx.conf** на сервере РЕД АДМ и закомментируйте секцию [HTTP server]:

```
# [HTTP server]
# server
# listen 80;
# ...
#
```

11. Раскомментируйте секцию [HTTPS server]:

```
# [HTTPS server]
server {
  listen 443 ssl;
  server_name redadm.wind.lan;
  ssl_certificate /opt/redadm/configs/ssl/redcert.crt;
  ssl_certificate_key /opt/redadm/configs/ssl/redserver.key;
  ...
}
```

12. В файле конфигурации сервера **/etc/redadm/server.conf** укажите путь к сгенерированному сертификату в поле CERT_PATH:

```
CERT_PATH=/opt/redadm/configs/ssl/redcert.crt
```

13. В файле конфигурации клиента **/etc/redadm/client.conf** отредактируйте следующие параметры:

```
PORT = 443
ENABLED_SECURE = True
SECURE_CERTIFICATE = /opt/redclient/ca.crt
```

14. Перезапустите службы **redadm** и **nginx**:

```
systemctl restart redadm.service nginx.service
```

15. Проверьте статус служб:

```
systemctl status redadm.service nginx.service
```

Самостоятельное создание сертификатов

Если у вас нет собственного центра сертификации, вы можете создать сертификат без ЦС и подписать его в РЕД АДМ. Для этого выполните следующие шаги:

1. Создайте в любом текстовом редакторе файл **request.inf** со следующим содержимым:

```
[Version]
 Signature="$Windows NT$
 [NewRequest]
 Subject = "CN=<DC_fqdn>"; укажите полное имя вашего домена
 KeySpec = 1
 KeyLength = 1024
 ; Can be 1024, 2048, 4096, 8192, or 16384.
 ; Larger key sizes are more secure, but have
 ; a greater impact on performance.
 Exportable = TRUE
 MachineKeySet = TRUE
 SMIME = False
 PrivateKeyArchive = FALSE
 UserProtected = FALSE
 UseExistingKeySet = FALSE
 ProviderName = "Microsoft RSA SChannel Cryptographic Provider"
 ProviderType = 12
 RequestType = PKCS10
 KeyUsage = 0xa0
 [EnhancedKeyUsageExtension]
 OID=1.3.6.1.5.5.7.3.1 ; this is for Server Authentication
```

2. Сгенерируйте запрос на подпись через консоль **PowerShell**:

```
certreq -new request.inf request.csr
```

Поместите полученный сертификат на сервер РЕД АДМ в каталог **/opt/redadm/configs/ssl**.

3. Подпишите сертификат с помощью корневого сертификата РЕД АДМ (**DemoCA.pem**):

```
openssl x509 -req -in request.csr -CA DemoCA.pem -CAkey DemoCA.key -
CAcreateserial -out request.crt -days 365 -sha256
```

4. Подписанный сертификат **request.crt** и корневой сертификат **DemoCA.pem** необходимо передать на контроллер домена Active Directory.

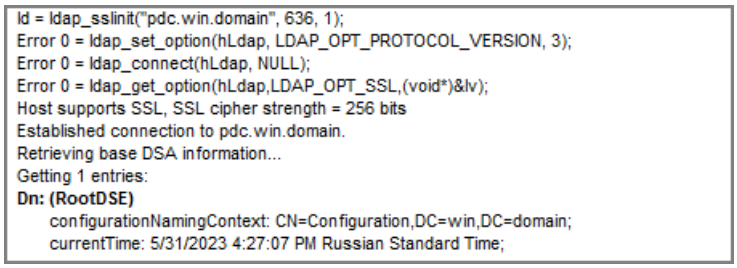
В оснастке «**Сертификаты**» на контроллере домена в разделе «**Доверенные корневые центры сертификации**» импортируйте сертификат **DemoCA.pem**.

Далее необходимо принять сертификат **request.crt**:

```
certreq -accept request.crt
```

Проверить работу **LDAPS** можно утилитой **ldp.exe**.

5. В меню «**Connections**» выберите «**Connect**», укажите *имя* вашего домена, *порт* 636 и наличие *SSL*. Вывод должен выглядеть примерно следующим образом:



6. Перезапустите сервер РЕД АДМ:

```
systemctl restart redadm.service
```

Подробную информацию о генерации сертификатов можно посмотреть в официальной документации Microsoft.

Установка РЕД АДМ Клиент

###ENV###

Примечание.

Установка **РЕД АДМ Клиент** (клиентского приложения) возможна двумя способами:

- из веб-интерфейса РЕД АДМ;
- с помощью rpm-пакета.

Подробную информацию об установке **РЕД АДМ Клиент** из веб-интерфейса см. в *Руководстве администратора*.

Примечание.

При распространении клиентского приложения РЕД АДМ через веб-интерфейс дополнительных настроек в файле **/opt/redclient/client.conf** производить не требуется, т.к. в данном случае все настройки определяются сервером.

Для ручной установки **РЕД АДМ Клиент** в терминале перейдите в сеанс пользователя **root**:

```
su -
```

Установка **РЕД АДМ Клиент** из репозитория производится командой:

```
dnf install redadm-client
```

Для установки **РЕД АДМ Клиент** из RPM-пакета необходимо открыть директорию с RPM-пакетом и выполнить команду:

```
dnf install <имя_пакета>.rpm
```

Для настройки **РЕД АДМ Клиент** отредактируйте конфигурационный файл **/opt/redclient/client.conf**:

```
nano /opt/redclient/client.conf
```

```
[SETTINGS]
# IP-адрес вашего сервера РЕД АДМ, к которому будут подключаться клиенты
IP=10.1.1.2
# порт, к которому будут подключаться клиенты РЕД АДМ
# по умолчанию используется порт 80
PORT=80
# использование https для обращения клиентов к серверу
# по умолчанию используется значение False
ENABLED_SECURE=False
# путь к сертификату сервера РЕД АДМ на клиентской машине
SECURE_CERTIFICATE=<путь_к_сертификату>
```

Запустите клиентскую службу и добавьте ее в автозагрузку:

```
systemctl enable redclient-daemon.service --now
```

Получение конфигураций с сервера РЕД АДМ происходит при выполнении команды **gpupdate** на клиенте. Данная команда автоматически прописывается при установке пакета в сценарий запуска сессии пользователей. В случае с GDM — это **/etc/gdm/PreSession/Default**.

Если вы хотите получать конфигурации по расписанию, пропишите команду **gpupdate &** в crontab-файл.

Например, для получения конфигураций в 10 и 40 минут каждого часа, впишите следующую строку:

```
10,40 * * * * root /bin/gpupdate &
```

Обновление РЕД АДМ Сервер версии 1.1.0

###ENV###

Для обновления **РЕД АДМ Сервер** версии 1.1.0 перейдите в сеанс пользователя **root**:

```
su -
```

Остановите активные службы:

```
systemctl stop redadm.service redadm-celery-worker.service redadm-celery-beat.service nginx.service
```

Выполните команду обновления:

```
dnf update redadm
```

Запустите остановленные службы:

```
systemctl start redadm.service redadm-celery-worker.service redadm-celery-beat.service nginx.service
```

ВАЖНО!

После обновления РЕД АДМ Сервер необходимо также обновить версии клиентских приложений на всех подключенных клиентах путем их повторного распространения.

Также клиентские приложения необходимо заново распространять после каждого изменения конфигурационного файла клиента **/etc/redadm/client.conf**.

Решение проблем после обновления

Если после обновления наблюдаются проблемы с наполнением журнала или неточности в настроенных конфигурациях, выполните нижеприведенные действия и сохраните их вывод для анализа проблемы.

Обновите базу данных командами:

```
sudo -u redadm_local_service_user /opt/redadm/.venv/bin/python3
/opt/redadm/manage.py makemigrations
sudo -u redadm_local_service_user /opt/redadm/.venv/bin/python3
/opt/redadm/manage.py migrate
sudo -u redadm_local_service_user /opt/redadm/.venv/bin/python3
/opt/redadm/manage.py create_grouppolicy
sudo -u redadm_local_service_user /opt/redadm/.venv/bin/python3
/opt/redadm/manage.py update_grouppolicy
sudo -u redadm_local_service_user /opt/redadm/.venv/bin/python3
/opt/redadm/manage.py update
sudo -u redadm_local_service_user /opt/redadm/.venv/bin/python3
/opt/redadm/manage.py update_1_9_2
```

Шаблонные файлы конфигурации можно найти в каталоге **/opt/redadm/configs**.

Для редактирования прав на файлы РЕД АДМ измените владельца следующих директорий:

```
chown -R redadm_local_service_user. /opt/redadm
chown -R redadm_local_service_user. /var/log/redadm
chown -R redadm_local_service_user. /etc/redadm
```

Обновление РЕД АДМ Сервер версии 1.9.1

###ENV###

Для обновления **РЕД АДМ Сервер** версии 1.9.1 перейдите в сеанс пользователя **root**:

```
su -
```

Остановите активные службы:

```
systemctl stop redadm.service redadm-celery-worker.service redadm-celery-beat.service
```

Выполните команду обновления:

```
dnf update redadm
```

Отредактируйте файлы конфигурации сервера и клиента в соответствии с рекомендациями, описанными в пункте «Настройка после установки» в инструкции «Установка РЕД АДМ Сервер».

Запустите остановленные службы:

```
systemctl start redadm.service redadm-celery-worker.service redadm-celery-beat.service
```

Запустите и добавьте в автозагрузку службу веб-сервера:

```
systemctl enable --now nginx.service
```

ВАЖНО!

После обновления РЕД АДМ Сервер необходимо также обновить версии клиентских приложений на всех подключенных клиентах путем их повторного распространения.

Также клиентские приложения необходимо заново распространять после каждого изменения конфигурационного файла клиента **/etc/redadm/client.conf**.

Решение проблем после обновления

Если после обновления наблюдаются проблемы с наполнением журнала или неточности в настроенных конфигурациях, выполните нижеприведенные действия и сохраните их вывод для анализа проблемы.

Обновите базу данных командами:

```
sudo -u redadm_local_service_user /opt/redadm/.venv/bin/python3
/opt/redadm/manage.py makemigrations
sudo -u redadm_local_service_user /opt/redadm/.venv/bin/python3
/opt/redadm/manage.py migrate
sudo -u redadm_local_service_user /opt/redadm/.venv/bin/python3
/opt/redadm/manage.py create_grouppolicy
sudo -u redadm_local_service_user /opt/redadm/.venv/bin/python3
/opt/redadm/manage.py update_grouppolicy
sudo -u redadm_local_service_user /opt/redadm/.venv/bin/python3
/opt/redadm/manage.py update
sudo -u redadm_local_service_user /opt/redadm/.venv/bin/python3
/opt/redadm/manage.py update_1_9_2
```

Шаблонные файлы конфигурации можно найти в каталоге **/opt/redadm/configs**.

Для редактирования прав на файлы РЕД АДМ измените владельца следующих директорий:

```
chown -R redadm_local_service_user. /opt/redadm
chown -R redadm_local_service_user. /var/log/redadm
chown -R redadm_local_service_user. /etc/redadm
```

Обновление РЕД АДМ Клиент

###ENV###

Обновить РЕД АДМ Клиент можно из веб-интерфейса, заново распространив клиентское приложение с обновленной версии сервера.

Примечание.

После обновления РЕД АДМ Клиента до версии **1.9.1 и выше** таблица подключенных узлов будет пуста.

Таблица будет заполнена значениями после распространения новой версии клиентского приложения либо при обращении клиента к серверу (при выполнении команды `gpupdate`).

Для обновления **РЕД АДМ Клиент** вручную перейдите в сеанс пользователя **root**:

```
su -
```

Остановите клиентскую службу:

```
systemctl stop redclient-daemon.service
```

Обновите пакет **РЕД АДМ Клиент**:

```
dnf update redadm-client
```

Проверьте параметры в файле **/opt/redclient/client.conf**.

```
[SETTINGS]
 # IP-адрес вашего сервера РЕД АДМ, к которому будут подключаться клиенты
 IP=10.1.1.2
 # порт, к которому будут подключаться клиенты РЕД АДМ
 # по умолчанию используется порт 80
 PORT=80
 # использование https для обращения клиентов к серверу
 # по умолчанию используется значение False
 ENABLED_SECURE=False
```

```
# путь к сертификату сервера РЕД АДМ на клиентской машине
SECURE_CERTIFICATE=<путь_к_сертификату>
```

Запустите клиентскую службу:

```
systemctl start redclient-daemon.service
```

Диагностика проблем

###ENV###

При сбоях в функционировании приложения РЕД АДМ в первую очередь стоит проверить статус сервиса **redadm**. Для этого выполните команду:

```
systemctl status redadm.service
```

В статусе должно отображаться **active (running)**.

Также можно просмотреть файл логов на предмет ошибок, выполнив команду:

```
cat /var/log/redadm/redadm.log
```

В случае возникновения проблем с распространением SSH-ключа просмотрите соответствующие логи, выполнив команды:

```
cat /var/log/redadm/ssh1.log
cat /var/log/redadm/ssh_key.log
```

В случае возникновения проблем с распространением конфигураций необходимо проверить статус служб, выполнив команды:

```
systemctl status redis.service
systemctl status redadm-celery-worker.service
```

В статусе должно отображаться **active (running)**.

В случае остановки служб необходимо перезапустить их, выполнив команды:

```
systemctl restart redis.service
systemctl restart redadm-celery-worker.service
```

Далее необходимо проверить корректность заполнения файла конфигурации клиентского приложения **/opt/redclient/client.conf**:

```
cat /opt/redclient/client.conf
```

В нем должны быть указаны *IP-адрес* и *порт* РЕД АДМ Сервер — параметры `IP` и `port` соответственно.

Переход с Microsoft Active Directory на РЕД АДМ. Два подхода к миграции ИТ-инфраструктуры

###ENV###

В рамках текущей статьи будет рассмотрено *два подхода* к переносу ИТ-инфраструктуры на отечественную систему централизованного управления, а именно – обзор возможностей и пошаговая инструкция, подготовка домена к миграции, установка доверительных отношений или создание параллельной инфраструткуры.

В РЕД АДМ используется подход «*в центре всего есть контроллер*». Далее будет подробнее рассмотрен процесс перехода от инфраструктуры на базе продуктов Microsoft Windows на решения РЕД СОФТ.

Существует несколько сценариев миграции. Следует понимать, что все эти сценарии «сферические в вакууме», их нужно **адаптировать** для каждого конкретного случая, однако, общие подходы необходимо рассмотреть. Часть из этих сценариев рассмотрены в нашем обучающем курсе, другие будут добавлены в курс в будущем.

Примечание.

Обратите внимание, что изменения в инфраструктуре необходимо **сначала** проверять **в тестовой среде** и только потом реализовывать изменения в продуктовой среде!

Репликация

Рассмотрим ситуацию, когда в организации существует контроллер на базе MS AD. К контроллеру подключены клиентские машины на базе ОС Windows, предоставлены различные сервисы – файловое хранилище, возможность централизованной установки ОС на новые машины, получение клиентскими машинами настроек с помощью GPO.

Репликация — один из самых удобных способов выполнения миграции с MS AD. При этом, в отличие от описанных далее способов, при репликации нет необходимости настраивать параллельный доступ к используемым сервисам из двух доменов. Необходимо просто добавить новый контроллер домена РЕД АДМ в домен, проверить работоспособность инфраструктуры и сервисов, и, по готовности, вывести контроллер домена Windows из эксплуатации.

Перед вводом новых контроллеров в домен следует убедиться, что в нем отсутствуют ошибки репликации, а также пройден чек-лист «здоровье домена». Каждый системный администратор должен иметь такой чек-лист и периодически проверять «здоровье» вверенного ему домена.

Чек-лист проверки «здоровья домена»

Для проверки «здоровья» домена необходимо выполнить следующий алгоритм действий:

1. Проверить состояние репликации, выполнив:

```
repadmin /replsum
repadmin /showrepl
```

2. Проверить состояние служб домена, выполнив:

```
dcdiag /q
```

Проверить, что все контроллеры домена (если их несколько) используют **DFS-R** для репликации **SYSVOL**:

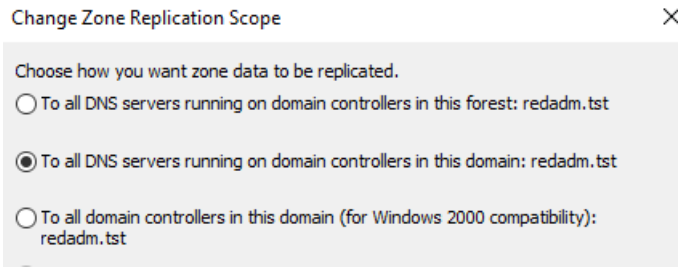
```
dfsrmig /getmigrationstate
```

Провести миграцию репликации **SYSVOL** на **DFS-R**, если она не была проведена ранее. Миграция необходима, если изначально домен был развернут с уровнем домена леса **2008 или ниже**, т.к. до уровня 2008 для репликации каталога **SYSVOL** использовался механизм **FRS**.

Провести диагностический отчет по репликации **DFS-R** («Оснастка DFS

management» — «Replication» — «Create Diagnostic Report»). При наличии ошибок необходимо их устранить.

3. В оснастке DNS проверить свойства прямых и обратных зон («Свойства зоны» — вкладка «General» — «Replication»).



Должен быть установлен один из первых двух вариантов.

Проверьте зону `_msdcs` на присутствие записей старых контроллеров, в случае необходимости — удалите старые записи от несуществующих контроллеров.

4. Проверьте, что все **FSMO** роли находятся на действующих контроллерах домена:

```
netdom query fsmo
```

5. Проведите анализ логов контроллера MS AD и убедитесь в отсутствии ошибок («Application and Services Logs» — «Directory Service»).

6. Проведите анализ логов DNS и убедитесь в отсутствии ошибок («Application and Services Logs» — «DNS Server»).

Настройка управления групповыми политиками

Вы можете подключить к контроллеру домена MS AD клиентские машины на базе РЕД ОС. Но может возникнуть вопрос — как ими управлять, ведь групповые политики MS AD могут управлять только рабочими станциями на базе ОС Windows. Для управления рабочими станциями на базе РЕД ОС можно использовать такой инструмент, как *Ansible*. При использовании инструмента *Ansible* может потребоваться подготавливать плейбуки вручную, не говоря уже о том, что этот инструмент работает только в режиме **push**.

Благодаря клиентскому приложению в РЕД АДМ, можно легко управлять групповыми политиками и использовать конфигурации как в формате **push**, так и в формате **pull**:

- *push-режим* позволяет отправить конфигурации непосредственно с РЕД АДМ — данный способ не всегда удобен, т.к. часть машин может быть выключена, или настройки должны быть доставлены в момент входа пользователя в

систему;

- с помощью *pull-режима* конфигурация будет применена по запросу клиентской машины, а чтобы клиентская машина вовремя запросила нужные данные с сервера, доступен клиентский агент РЕД АДМ.

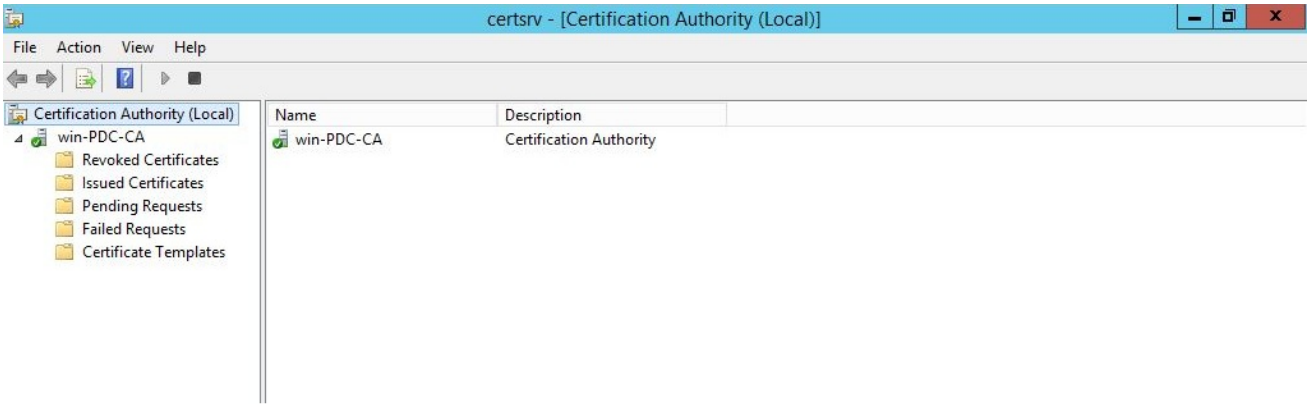
Ввод контроллера домена РЕД АДМ

Следующим действием станет ввод контроллера домена РЕД АДМ в существующий домен на базе MS AD. Данную процедуру можно выполнить из графического интерфейса РЕД АДМ.

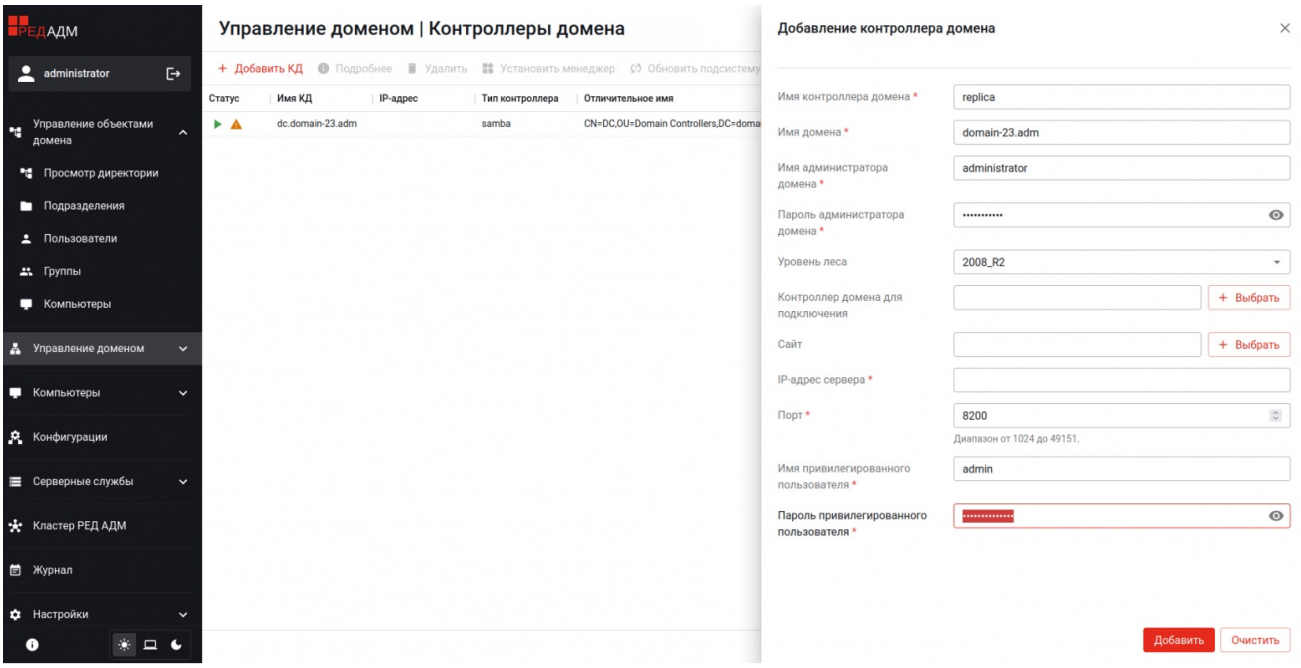
1. Сначала необходимо установить РЕД АДМ и создать локальную базу данных.

2. На этапе подключения или создания нового контроллера домена необходимо выбрать «Подключиться к существующему». При подключении по доменному имени нужно проверить, что контроллер доступен по доменному имени с хоста, где установлен РЕД АДМ (проверить настройки DNS).

3. Для подключения РЕД АДМ к контроллеру домена на базе MS AD необходимо разрешить возможность подключения по **ldaps**. Для этого создайте на MS AD роль центра сертификации (если по каким-либо причинам данный вариант не подходит, рекомендуется воспользоваться документацией — в ней описано, как подключиться к MS AD без роли центра сертификации).



4. Затем необходимо создать новый контроллер и присоединить его к существующему. Сделать это можно через «Управление доменом в РЕД АДМ». Нажмите на кнопку «Добавить КД» и укажите — на каком хосте этот контроллер будет развернут и к какому контроллеру его нужно присоединить — все остальные настройки будут подобраны автоматически.



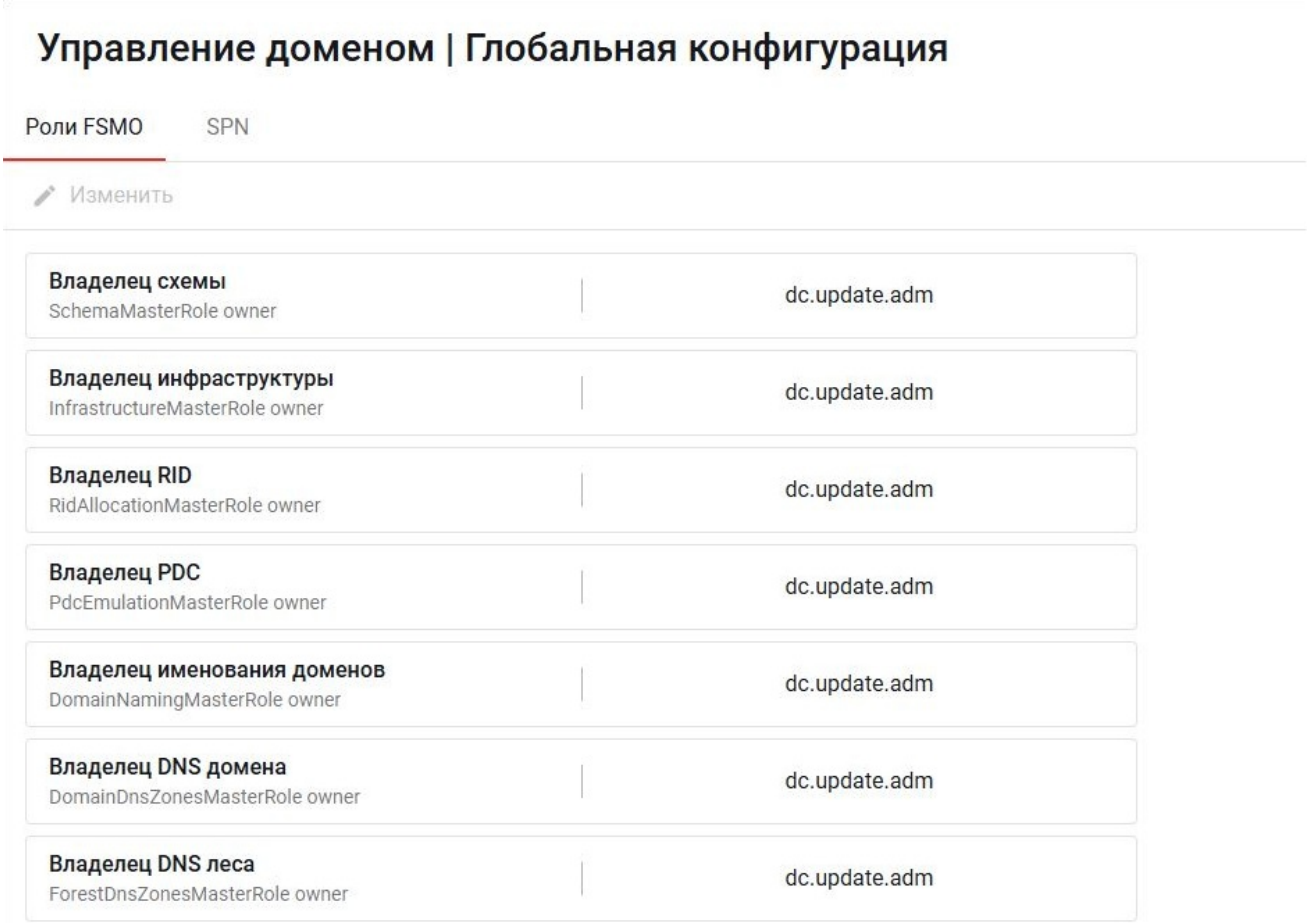
Миграция клиентских машин

Теперь в инфраструктуре работают два контроллера домена, причем один из них может управлять машинами на базе РЕД ОС. Далее необходимо начать процесс перевода парка клиентских машин на РЕД ОС. Управление РЕД ОС будет производиться с помощью конфигураций из РЕД АДМ.

Если в домене будет организована *гетерогенная среда* (будут использоваться как машины на базе ОС Windows, так и машины на базе РЕД ОС) необходимо выполнить некоторые подготовительные действия:

1. Выполнить репликацию каталога **SYSVOL**. Данное действие необходимо для того, чтобы все групповые политики, которые были созданы для хостов на базе ОС Windows, продолжили работать. Подробную информацию о данном этапе можно просмотреть в документации.

2. После репликации каталога **SYSVOL** следует передать роли **FSMO** с контроллера MS AD на контроллер РЕД АДМ. Для этого нужно перейти в «Управление доменом» — «Глобальная конфигурация».



3. Для управления реплицированными политиками потребуется машина с Windows, на которую необходимо установить **RSAT**.

4. Далее необходимо выключить контроллер на базе Windows, проверить работоспособность групповых политик, понизить роль первого контроллера и вывести его из эксплуатации.

Примечание.

Обратите внимание, что РЕД АДМ пока **не работает** с почтовым сервером **MS Exchange**. Поэтому, если такое решение еще используется в вашей инфраструктуре, полностью отказываться от контроллеров на базе MS Windows не рекомендуется. Однако можно рассмотреть варианты аналогичных сервисов от российских вендоров.

После выполненных действий в инфраструктуре нет контроллеров на базе MS AD. Клиентские машины постепенно мигрируют с Windows на РЕД ОС.

Построение параллельной инфраструктуры

Бывают ситуации, когда невозможно произвести никаких действий с существующим доменом. В этом случае можно построить параллельную инфраструктуру на базе РЕД АДМ и выстроить между доменами доверительные отношения.

Плюсы такого решения — проводить миграцию можно длительное время, постепенно перемещая сопутствующие сервисы на новые решения. При этом не так важно, насколько корректно работает ваш исходный домен — например, в нем могут возникать какие-либо ошибки, которые нельзя оперативно решить. Также в этом случае можно полностью избавится от унаследованных проблем в доменной инфраструктуре, создав всё заново.

Развертывание нового домена

Далее будет кратко рассмотрен процесс настройки доверительных отношений. для получения подробной информации см. документацию. В примерах будет использоваться исходных домен на MS AD — **windows.red** и новый домен на РЕД АДМ **example.tst**.

1. Настройка доверительных отношений происходит после установки контроллера РЕД АДМ, поэтому сначала необходимо установить РЕД АДМ и развернуть новый домен.

2. На контроллере РЕД АДМ необходимо отредактировать файл **/etc/named.conf** и после корневой зоны «**.**» добавить зону пересылки запросов в доверенный домен:

```
zone "windows.red" IN {
 type forward;
 forwarders { 192.168.100.5; };
 };
```

где в параметре `forwarders` необходимо указать адрес контроллера домена MS AD, с которым необходимо установить доверительные отношения.

3. На контроллере домена РЕД АДМ также необходимо отредактировать файл **/etc/krb5.conf** и в секции `[realms]` и `[domain_realm]`.

```
[realms]
 EXAMPLE.TST = {
 kdc = dc1.example.tst
 admin_server = dc1.example.tst
 }
```

```
WINDOWS.RED = {
kdc = windc.windows.red
admin_server = windc.windows.red
}
[domain_realm]
.example.tst = EXAMPLE.TST
example.tst = EXAMPLE.TST
.windows.red = WINDOWS.RED
windows.red = WINDOWS.RED
```

4. Далее на РЕД АДМ необходимо перезапустить службы:

```
systemctl restart reddc named
```

5. На контроллере домена MS AD необходимо настроить сервер условной пересылки.

Установка доверительных отношений

Теперь можно приступить к настройке доверительных отношений, предварительно проверив доступность контроллеров друг с другом, командой:

```
nslookup <имя_КД>
```

Если сервера доступны, создайте доверительные отношения командой:

```
samba-tool domain trust create windows.red --type=external --direction=both --create-location=both -U Administrator@WINDOWS
```

где:

- `type` — тип доверительных отношений - `external` (внешнее) — РЕД АДМ поддерживает тип отношений `external`;
- `direction` — направление доверительных отношений, со следующими возможными значениями:
    - `both` — двухсторонние доверительные отношения. Контроллер домена РЕД АДМ будет доверять контроллеру домена Active Directory и наоборот — обе стороны смогут обмениваться аутентификационной информацией и ресурсами;

- outgoing — односторонние доверительные отношения только для исходящих запросов: например, контроллер домена Active Directory будет доверять контроллеру домена РЕД АДМ, например, при получении запросов на аутентификацию от пользователей из СК РЕД АДМ, но не наоборот;

- incoming — односторонние доверительные отношения только для входящих запросов: например, контроллер домена РЕД АДМ будет доверять контроллеру домена Active Directory, например, при получении запросов на аутентификацию от пользователей из домена Active Directory, но не наоборот.

В случае успешного создания доверительных отношений, в конце вывода результатов работы команды в терминале должно быть выведено сообщение success.

После построения доверительных отношений необходимо еще раз перезапустить службы **reddc** и **named** и проверить установленные доверительные отношения при помощи команды:

```
samba-tool domain trust list
```

Для того чтобы убедиться в корректности выполненных выше команд, рекомендуется проверить целостность получения файла **PAC dump** при помощи следующей команды (запуск следует выполнять с правами суперпользователя **root**):

```
net ads kerberos pac dump -U Administrator@WINDOWS.RED
```

Часто задаваемые вопросы (FAQ)

Не удаётся получить доступ к web-интерфейсу РЕД АДМ

Проверьте статус сервиса **redadm** на сервере РЕД АДМ, скорее всего он не запущен. Запустите его следующей командой:

```
systemctl status redadm
systemctl enable redadm --now
```

Не запускаются сервисы redadm-celery-worker и redadm-celery-beat

1) Остановите сервисы:

```
systemctl stop redadm-celery-worker.service redadm-celery-beat.service
```

2) Выполните перезагрузку машины:

```
reboot
```

3) Выполните откат версии пакета **python3-click** до **7.1.2**:

```
dnf downgrade python3-click
```

4) Выполните запуск сервисов:

```
systemctl start redadm-celery-worker.service redadm-celery-beat.service
```

Какие принтеры можно подключить через конфигурацию РЕД АДМ?

Подключить через конфигурацию «**Установить принтер**» можно принтеры доступные по протоколу **ipp**.

Почему на вкладке «Конфигурации» видны не все подразделения?

Создание конфигураций допускается только в подразделениях, имеющих тип **Organization Unit - OU**.

Почему на вкладке «Настройки» - «Подключение узлов» не отображаются клиентские машины в домене?

Для того чтобы хост появился в списке и отображался его статус, клиентская машина должна находиться в домене и быть добавлена через соответствующее меню, вызываемое на кнопку «**Добавить**».

Не получается распространить конфигурацию «Подключение локального репозитория»

Возможно на клиентской машине не установлен пакет **redos-kernels-release**. Адрес локального репозитория вносится в уже существующий файл репозитория. Создайте конфигурацию для установки пакета **redos-kernels-release**.

Работает ли РЕД АДМ с доменом FreeIPA?

На данный момент РЕД АДМ работает только с доменами **Samba DC** и **Microsoft AD**. Добавление функционала взаимодействия с **FreeIPA** планируется в будущих обновлениях.

Машина с сервером РЕД АДМ должна быть введена в домен?

Нет, для работы РЕД АДМ и его взаимодействия с контроллером домена достаточно, чтобы в настройках сети был прописан **DNS-сервер**, разрешающий А-записи контроллера домена, и указан «**Поисковой домен**».

Влияет ли расположение конфигурации в дереве на что-то кроме того, что будет располагаться в области применения после ее создания?

Расположение конфигурации в древе влияет только на то, какое подразделение будет указано во вкладке «**Область применения**» по умолчанию.

Что необходимо прописывать в настройке конфигурации «Подключение локального репозитория»? (формат записи)

В полях конфигурации «**Подключение локального репозитория**» указываются URL-ссылки на ваши локальные репозитории.

В какой момент запускается выполнение конфигурации на клиентской машине?

Клиент запрашивает доступные конфигурации после выполнения команды **gpupdate**.

Команду **gpupdate** можно выполнить несколькими способами:

1. Вручную в терминале.

2. Добавив в автозапуск по расписанию, например, через **crontab**.

3. При входе в сессию под доменным пользователем - команда **gpupdate** добавляется в скрипт входа **gdm** после установки клиентской части.

Пользователю домена назначена роль, имеющая доступ к управлению учетными записями домена, но при создании подразделения/пользователя/компьютера появляется ошибка. Почему?

Роли в РЕД АДМ влияют только на доступность тех или иных модулей в веб-интерфейсе. Права на изменение объектов домена задаются на контроллере домена или добавлением пользователя в группу администраторов домена.

Не появляются записи на вкладке «Журналы» - «Задачи».

Записи в данном разделе появляются только после выполнения конфигураций на клиентских машинах. В них содержится результат их выполнения.

В конфигурации «Подключение сетевого каталога» необходимо задавать полный путь к каталогу?

Для конфигурации «**Подключение сетевого каталога**» в поле «**Сервер**» укажите доменное имя сервера с опубликованным сетевым каталогом, а в поле «**Сетевой каталог**» — имя директории на удалённом сервере.

Где создаётся каталог после выполнения конфигурации «Параметры пользователя» - «Системные настройки» - «Создание каталога»?

Каталог создаётся в домашнем каталоге пользователя с правами доступа для всех.