Установка РЕД АДМ Сервер

Окружение

- **Версия ОС:** 7.3
- **Конфигурация ОС:** 7.3
- **Версия ПО:** redadm-1.1.0

Установка пакета

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.

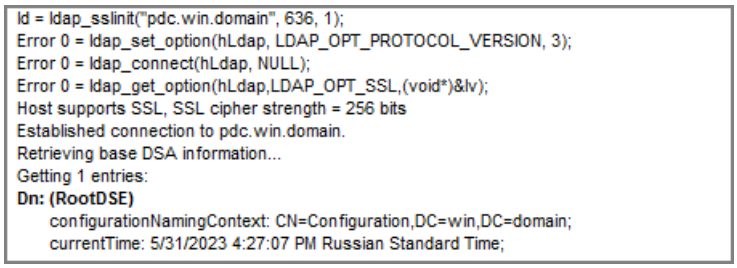
В оснастке «**Сертификаты**» на контроллере домена в разделе «**Доверенные корневые центры сертификации**» импортируйте сертификат **DemoCA.pem**.

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.

Источник: https://redadm.red-soft.ru/base/red-adm/ra-install/ra-1-1-0-install/install-ra-server/