Система централизованного управления ИТ-инфраструктурой РЕД АДМ

Руководство по установке

Оглавление

1 Введение

Система централизованного управления ИТ-инфраструктурой «РЕД АДМ» (далее – РЕД АДМ) является программным продуктом, полностью разработанным компанией «РЕД СОФТ». РЕД АДМ имеет модульную структуру и агрегирует в себе множество модулей администрирования различного назначения.

В настоящем документе описаны действия по установке РЕД АДМ. Данное Руководство предназначено для администраторов, которые будут непосредственно использовать данную систему, и дополняет соответствующее Руководство администратора.

2 Описание дистрибутива

2.1 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.

2.2 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 выполнения конфигураций с клиентских рабочих станций.

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

3 Системные требования

3.1 РЕД АДМ Сервер

РЕД АДМ Сервер устанавливается на РЕД ОС в конфигурации «Сервер» версии 7.3 и выше.

В таблице ниже приведены минимальные требования к оборудованию.

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

3.2 РЕД АДМ Клиент

Минимальные и рекомендуемые 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. ■

3.3 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.

4 Подготовка окружения

Для развертывания системы потребуются:

1. Установленная операционная система РЕД ОС в конфигурации «Сервер», необходимая для установки РЕД АДМ Сервер.

Системные требования для РЕД ОС Сервер 7.3 см. на официальном сайте компании-производителя в разделе «Системные требования».

Системные требования для РЕД АДМ Сервер указаны в подразделе 3.1 «РЕД АДМ Сервер» настоящего руководства.

2. Развернутый контроллер домена.

Контроллер домена должен быть на базе подсистемы службы каталогов РЕД АДМ (reddc) 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 дать 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).

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 подразделе 6.1 «Установка» настоящего руководства.

РЕД АДМ требует прямого доступа по сети между сервером РЕД АДМ и клиентом по TCP-портам 22 и 80 (или 443). Полный перечень портов, используемых системой РЕД АДМ, приведен в таблице ниже.

Протокол (служба)	**Номер порта**
Взаимодействие с клиентом	
SSH	22
VNC	5900-5906
HTTP	80
HTTPS	443
Взаимодействие с контроллером домена	
DNS	53
LDAP	389
LDAPS	636
Взаимодействие с браузером	
HTTP	80
HTTPS	443

5 РЕД АДМ Сервер

5.1 Установка

5.1.1 Обновление системы

Предварительно необходимо обновить систему:

```
dnf makecache && dnf upgrade -y
```

При необходимости перезагрузите компьютер:

```
reboot
```

5.1.2 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 -
```

Установка РЕД АДМ Сервер из репозитория производится командой:

```
dnf install -y redadm
```

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

```
dnf install -y <имя_пакета>.rpm
```

5.2 Настройка после установки

5.2.1 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 домена (по умолчанию используется порт 636);
- `LDAP_DOMAIN_NAME = <имя>` – ldap-имя 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. Установить DNS-сервер можно в настройках сетевого адаптера, проверить – в файле `/etc/resolv.conf`, IP-адрес доменного DNS-сервера должен быть указан первым в списке. Обычно DNS-сервер расположен непосредственно на контроллерах домена.

Также следует проверить синхронизацию времени с контроллером домена, это необходимо для обеспечения шифрованного подключения к LDAP-каталогу домена. ■

Примечание. Сценарий установки РЕД АДМ Сервер автоматически настроит параметры Ansible в файле конфигурации `/etc/ansible/ansible.cfg`.

Подробную информацию о параметрах Ansible см. в разделе 2 «Настройка перед началом работы» Руководства администратора.

5.2.2 Настройка файла конфигурации клиента

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

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

Важно! Синтаксис файла конфигурации чувствителен к регистру! ■

```
[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>
```

5.2.3 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
```

5.2.4 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 перемещены в автоматически созданный каталог, в имени которого указаны текущие дата и время.

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
```

5.3 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;
- сертификат создаётся самостоятельно.

5.3.1 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
```

5.3.2 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 остнастке «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 так, как представлено на рисунке 1.

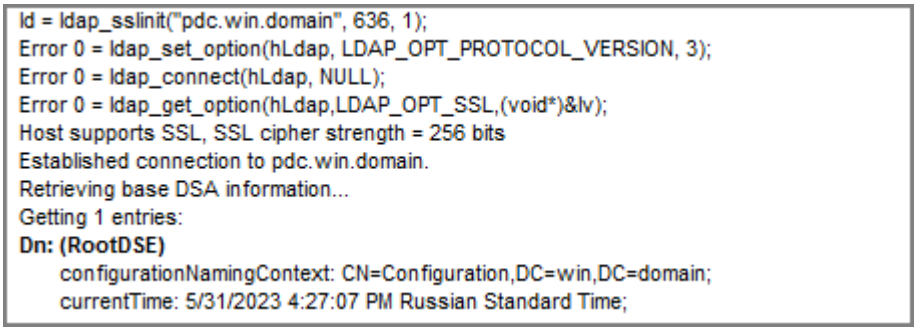

Рисунок 1 – Проверка подключения

6. Перезапустите сервер РЕД АДМ:

```
systemctl restart redadm.service
```

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

5.4 Обновление РЕД АДМ Сервер версии 1.9

Для обновления РЕД АДМ Сервер **версии 1.9** необходимо:

1. Остановить активные службы:

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

2. Выполнить команду обновления:

```
dnf update redadm
```

3. Отредактировать файл конфигурации сервера РЕД АДМ в соответствии с указаниями п. 5.2.1 «Настройка файла конфигурации сервера» настоящего руководства.

4. Привести файл конфигурации клиента к виду, описанному в п. 5.2.2 «Настройка файла конфигурации клиента» настоящего руководства.

5. Запустить остановленные службы:

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

6. Запустить и добавить 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`.

5.5 Обновление РЕД АДМ Сервер версии 1.10

Для обновления РЕД АДМ Сервер **версии 1.10** необходимо:

1. Остановить активные службы:

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

2. Выполнить команду обновления:

```
dnf update redadm
```

3. Запустить 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`.

5.6 Обновление РЕД ОС 7.3 до РЕД ОС 8

В случае если требуется обновить РЕД ОС 7.3, на которой установлен РЕД АДМ Сервер, до РЕД ОС 8, необходимо:

1. Остановить активные службы:

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

2. Выполнить обновление ОС в соответствии с документацией от технической поддержки.

3. Проверить наличие обновлений для РЕД АДМ с помощью команды:

```
dnf update redadm
```

4. Запустить остановленные службы РЕД АДМ и проверить их статус:

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

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

Если пользователь, для которого распространялся ssh-ключ, не является `root`, этого пользователя необходимо добавить в группу `root` на клиентских хостах.

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

5.7 Решение проблем

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
```

5.8 Удаление

Для удаления РЕД АДМ Сервер сначала остановите активные службы:

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

Затем выполните команду удаления:

```
   dnf remove redadm
```

6 РЕД АДМ Клиент

6.1 Установка

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 -y redadm-client
```

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

```
dnf install -y <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 --now redclient-daemon.service
```

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 &
```

6.2 Обновление

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

> **Примечание.** После обновления РЕД АДМ Клиент до **версии 1.9.1** и выше таблица подключенных узлов будет пуста (подробнее см. раздел 5 «Добавление клиентских машин» в Руководстве администратора).
>
> 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 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`.

```
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:

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

6.3 Удаление

Для удаления РЕД АДМ Клиент остановите клиентскую службу:

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

Удалите пакет командой:

```
dnf remove redadm-client
```

Проверьте файл `/etc/gdm/PreSession/Default` на отсутствие вызова команды `gpupdate`.

Если вы вписывали `gpupdate` в файлы конфигураций `crontab`, отредактируйте их.

7 Проверка успешности установки

Для успешной установки сервера РЕД АДМ проверьте статусы всех необходимых служб командой:

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

Если все службы запущены успешно (имеют статус `active (running)`), выполните авторизацию доменным администратором или пользователем `redadm`, который является служебным пользователем и должен быть создан в домене заранее.

Примечание. РЕД АДМ не может производить смену пароля пользователя при авторизации, поэтому не создавайте сервисного пользователя с необходимостью смены пароля при первом входе или смените его при авторизации с рабочей станции.

В домене Microsoft Active Directory пользователя можно создать только с атрибутом «отключенная учетная запись», и уже после создания включить учетную запись.

Для доступа на веб-портал откройте браузер на любой машине, с которой доступен IP-адрес сервера РЕД АДМ. Впишите в адресную строку браузера адрес страницы в следующем формате:

```
http(s)://<IP-адрес(имя_хоста)_РЕД_АДМ>:<указанный_порт>
```

По умолчанию используется порт 80. Пример готового адреса веб-портала приведен ниже:

```
http://10.1.0.2:80
```

После загрузки веб-портала будет открыта форма авторизации.

В поле «Имя входа пользователя» впишите `redadm` или имя доменного администратора.

В поле «Пароль» впишите пароль, установленный пользователю `redadm` при создании, или пароль доменного администратора и нажмите кнопку «Войти» (рисунок 2).

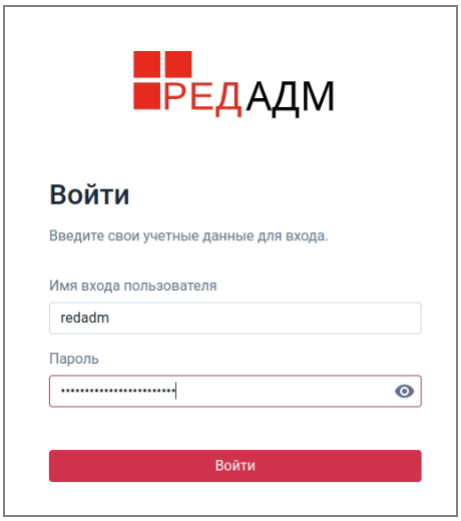

Рисунок 2 – Окно авторизации

После успешного входа вы попадете на страницу мониторинга (рисунок 3).

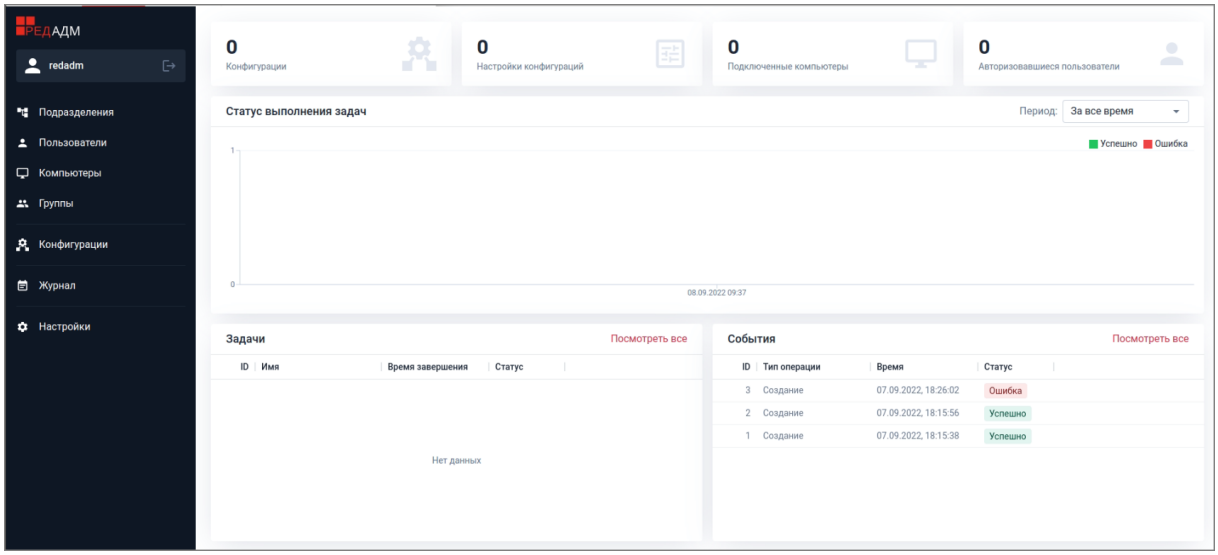

Рисунок 3 – Страница мониторинга системы

На этом установка системы РЕД АДМ закончена.