Система централизованного управления ИТ-инфраструктурой «РЕД АДМ» (стандартная редакция) версия 2.0.0

Руководство по установке

версия документа 2.0.0-10

Аннотация

1. Система централизованного управления ИТ-инфраструктурой «РЕД АДМ» (далее – РЕД АДМ) является программным продуктом, разработанным компанией «РЕД СОФТ».

2. В настоящем документе описаны действия по развёртыванию РЕД АДМ версии 2.0.0. Данное Руководство предназначено для администраторов, которые будут непосредственно использовать данную систему, и дополняет соответствующее Руководство администратора.

3. Если команда терминала РЕД ОС занимает более чем одну строку, то при написании команды в конце каждой строки (кроме последней) может ставиться обратный слеш «\» и нажимается клавиша «Enter», так что команду можно продолжать набирать в следующей строке. В данном Руководстве все команды, не помещающиеся в одну строку, оформляются именно таким образом, например:

```
   systemctl stop redadm.service rabbitmq-server.service \
redadm-celery-worker.service redadm-celery-beat.service nginx.service
```

4. Если в веб-интерфейсе РЕД АДМ рядом с именем поля находится звёздочка (*) — это поле является обязательным для заполнения.

Содержание

1 Описание дистрибутива

1.1. 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.

1.2. Дистрибутив РЕД АДМ Сервер представляет из себя RPM-пакет.

2 Подготовка окружения

2.1 Компоненты системы

2.1.1. Для развёртывания системы потребуются:

1) Доступ к репозиториям.

2) Сервер с установленной операционной системой РЕД ОС 8 в конфигурации «Сервер», необходимый для установки РЕД АДМ Сервер (сервера подсистемы управления).

3) Развёрнутый контроллер домена (КД). Существующий контроллер домена должен быть на базе Samba или Microsoft Active Directory (MS AD). Особенности работы с КД и его предварительной настройки см. ниже в 2.2.

4) Клиентские машины (клиентские компьютеры, клиенты) в домене. Работа с ними описана в Руководстве администратора.

Клиентское приложение (агент) может быть установлено на клиентских машинах под управлением операционной системы (ОС) РЕД ОС.

2.2 Особенности настройки

Важно! Указания данного подраздела являются обязательными. ▪

2.2.1. Хост, на котором будет развёрнут РЕД АДМ Сервер:
– должен находиться в одной сети с контроллером домена, которым он будет управлять;
– НЕ должен быть в составе домена.

2.2.2. SELinux должен быть переведён в режим `permissive` на машине, где развёртывается РЕД АДМ Сервер.

2.2.3. РЕД АДМ требует прямого доступа по сети между сервером РЕД АДМ и клиентом по TCP-портам 80, 443 и 5000. При использовании `firewalld` эти порты должны быть открыты.

Например, для открытия порта 5000 надо выполнить команду:

```
firewall-cmd --zone=public --add-port=5000/tcp --permanent
```

после чего перезагрузить службу:

```
firewall-cmd --reload
```

Полный перечень портов, используемых системой РЕД АДМ, приведён ниже в 2.3.

2.2.4. Если вы планируете подключать РЕД АДМ к КД на базе MS AD, то убедитесь, что возможно подключение по LDAPS. На самом КД MS AD проверку можно выполнить с помощью утилиты `ldp.exe`.

Для настройки подключения по LDAPS необходимо настроить Центр сертификации (см. Приложение Б).

2.2.5. Для именования вашего локального домена верхнего уровня (TLD) не используйте `.local`, поскольку RFC6762 резервирует этот домен исключительно для использования в MulticastDNS.

2.2.6. Не рекомендуется использовать учётную запись администратора домена для работы в РЕД АДМ. Оптимальным вариантом является настройка прав в ролевой системе РЕД АДМ для других учётных записей в домене.

2.2.7. В целях безопасности все учётные записи 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.

2.2.8. Для совместной работы компонент системы небходимо, чтобы был заранее создан привилегированный пользователь, входящий в группу `wheel`:

– на машине, на которой будет разворачиваться РЕД АДМ Сервер;

– на клиентских машинах.

Для добавления пользователя с именем `your_user` в группу `wheel` выполните команду:

```
usermod -a -G wheel your_user
```

Также можно использовать учётную запись суперпользователя `root` и не создавать новую учётную запись.

2.2.9. Если вы отключаете IPv6 на хосте, где будет развёрнут РЕД АДМ Сервер, то после отключения выполните следующие действия.

1) Отредактируйте файл `/etc/hosts`, удалив оттуда строку:

```
::1 localhost localhost.localdomain localhost6 localhost6.localdomain6
```

2) Отредактируйте файл `/etc/sysconfig/memcached`, удалив из списка значений параметра `OPTIONS` значение `::1`. То есть, строку

```
OPTIONS="-l 127.0.0.1,::1"
```

приведите к виду:

```
OPTIONS="-l 127.0.0.1"
```

2.3 Порты и протоколы, используемые системой

Установка и обновление пакетов ПО из локального репозитория

Источник: локальный репозиторий пакетов.

Приемник: клиентская машина.

Направление передачи: в обе стороны.

Порты и протоколы: 80 TCP, 443 TCP.

Подключение РЕД АДМ Сервер к контроллеру домена

Источник: контроллер домена.

Приемник: РЕД АДМ Сервер.

Направление передачи: в обе стороны.

Порты и протоколы: 389 TCP, 636 TCP, 8200 TCP.

Взаимодействие сервера РЕД АДМ с клиентскими рабочими станциями

Источник: РЕД АДМ Сервер.

Приемник: клиентская машина.

Направление передачи: в обе стороны.

Порты и протоколы: 80 TCP, 443 TCP, 5000 TCP, 5900-5906 TCP/UDP. Для работы с внедоменными компьютерами – 22 TCP.

2.4 Планирование ресурсов сервера РЕД АДМ

Сервер РЕД АДМ развёртывается на отдельной серверной машине, отличной от той, где развёрнут контроллер домена.

На каждый сайт необходим один сервер РЕД АДМ.

Здесь приводятся рекомендации по оптимизации ресурсов в части выбора характеристик серверной машины, на которой установлен РЕД АДМ. Данные ниже оценки приводятся для выделенной серверной машины с установленной операционной системой РЕД ОС 8 «Сервер».

Базовый случай – до 1 000 клиентских машин включительно, для их обслуживания требуются следующие параметры серверной машины:

– ЦПУ – 4 ядра с частотой от 1,6 ГГц;

– объём ОЗУ – 8 Гбайт;

– объём накопителя HDD/SSD – 100 Гбайт (крайне рекомендуется SSD со скоростью передачи данных 600 Мбит/с и выше);

– скорость сети от 1 Гбит/с.

2.4.1 Центральный процессор

Для ЦПУ примерная зависимость от нагрузки следующая:

– не более 1 000 обслуживаемых хостов – 4 ядра;

– если хостов больше 1 000, то используется формула:

$$N_{CPU} = 4 + \left\lceil \frac{N - 1\,000}{500} \right\rceil$$

Квадратные скобки $\lceil \cdots \rceil$ обозначают округление вверх до ближайшего целого.

2.4.2 Оперативная память

Для ОЗУ примерная зависимость объёма от нагрузки следующая:
– не более 1 000 обслуживаемых хостов — 8 Гбайт ОЗУ;
– если хостов больше 1 000, то используется формула:

$$V_{RAM}(min)\ (\text{Гбайт}) = 8 + \left\lceil \frac{N - 1\,000}{500} \right\rceil$$

2.4.3 Жёсткий диск

Для жёсткого диска примерная зависимость объёма от нагрузки следующая:
– не более 1 000 обслуживаемых хостов – 100 Гбайт;
– для каждых следующих 1 000 хостов – плюс 100 Гбайт.
Если выразить зависимость через формулу, то для N хостов:

$$V_{DS}(min)\ (\text{Гбайт}) = 100 + 100 \cdot \left\lceil \frac{N - 1\,000}{1\,000} \right\rceil$$

Здесь уже учтено, что сама операционная система с установленным дистрибутивом РЕД АДМ Сервер занимает около 10 Гбайт.

2.4.4 Сетевой интерфейс

Для всей области применимости РЕД АДМ достаточна пропускная способность сетевой карты, равная 1 Гбит/с.

2.4.5 Примеры масштабирования

Ниже приведена сводная таблица с результатами оценки требуемых значений параметров сервера (ЦПУ, объёмов ОЗУ и жёсткого диска) для успешной работы с указанным количеством обслуживаемых клиентских машин (хостов). Оценка производится со значительным запасом по ресурсам: для теоретического случая с одновременным запуском на всех хостах по 100 задач.

Количество клиентских машин	Ядра ЦПУ, штук	Объём памяти ОЗУ, Гбайт	Объём жёсткого диска, Гбайт
100	4	8	100
500	4	8	100
1 000	4	8	100
2 000	6	10	200

2.5 РЕД АДМ Клиент

2.5.1. РЕД АДМ Клиент необходим для взаимодействия сервера РЕД АДМ и компьютеров в инфраструктуре. Развёртывание клиентского агента на компьютеры описано в разделе «Работа с компьютерами» Руководства администратора.

2.5.2. Минимальные и рекомендуемые требования к оборудованию совпадают с требованиями к операционной системе, на которую устанавливается РЕД АДМ Клиент – это РЕД ОС в конфигурации «Рабочая станция» версий 7 или 8.

2.5.3. В таблице ниже приведены минимальные требования к оборудованию.

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

2.6 Требования к веб-управлению

2.6.1. 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.

3 Развёртывание РЕД АДМ

3.1 Установка

Операции по установке и настройке выполняются в терминале в сеансе пользователя `root`, вход в который из сеанса текущего пользователя осуществляется командой

```
su -
```

Перед обновлением всех пакетов и установкой пакета для РЕД АДМ сервер – проверьте доступность репозиториев.

3.1.1 Обновление системы

Обновите все установленные пакеты:

```
dnf makecache && dnf update -y
```

При необходимости перезагрузите компьютер:

```
reboot
```

3.1.2 Установка РЕД АДМ Сервер

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

```
dnf install -y redadm-⟨версия_пакета⟩.rpm
```

3.2 Дополнительные настройки

Важно! Операции, описанные в 3.2.1 – обязательны.
Операции, описанные в 3.2.2 и 3.2.3 – обязательными не являются. ■

3.2.1 DNS и синхронизация времени

Убедитесь, что в системе установлен правильный DNS-сервер, разрешающий A-записи DNS контроллера домена. Установить DNS-сервер можно в настройках сетевого адаптера.

Проверить корректность установки в РЕД ОС 7 можно, просмотрев файл `/etc/resolv.conf` – IP-адрес доменного DNS-сервера должен быть указан первым в списке; в РЕД ОС 8 проверку можно выполнить командой `resolvectl status`. Обычно DNS-сервер расположен непосредственно на контроллерах домена.

Также следует проверить синхронизацию времени с контроллером домена. Это необходимо для обеспечения работоспособности, в том числе при обеспечении защищённого подключения к домену.

3.2.2 Редактирование файла конфигурации

Настроив параметры сервера РЕД АДМ, можно отредактировав конфигурационный файл сервера (см. Приложение А). В случае изменения этого файла, для применения внесённых изменений необходимо перезапустить следующие службы:

```
systemctl restart redadm.service rabbitmq-server.service \
redadm-celery-worker.service redadm-celery-beat.service nginx.service \
memcached.service
```

После перезапуска проверьте статус служб:

```
systemctl status redadm.service rabbitmq-server.service \
redadm-celery-worker.service redadm-celery-beat.service nginx.service \
memcached.service
```

При успешной установке сервера все необходимые службы должны иметь статус `active (running)`.

3.2.3 Изменение стандартного порта для подключения к клиентам по SSH

По умолчанию используется порт 22. Для его изменения выполните следующие действия.

3.2.3.1. Измените порт в настройках SSH.

1) Создайте конфигурационный файл:

```
touch /home/redadm_local_service_user/.ssh/config
```

Вставьте в файл следующее содержание:

```
Host 10.10.*.*
Port 33
```

В данном примере указаны значения:
– `10.10.*.*` – ваша подсеть,
– `33` – новый порт для SSH.

2) Перезапустите службу SSH:

```
systemctl restart sshd.service
```

3.2.3.2. Измените порт в настройках Ansible, в файле `/etc/ansible/ansible.cfg`:

```
[defaults]
ansible_port = 33
remote_port = 33
```

3.3 Первоначальная настройка

Подсистема управления (РЕД АДМ Сервер) настраивается через веб-интерфейс.

3.3.1. **Важные замечания по настройке сетевых параметров в ходе первоначальной настройки:**

1) Применив настройки параметров сети сервера РЕД АДМ и контроллера домена (если он создаётся), проверьте доступность репозиториев для этих хостов.

2) При настройке (развёртывании) сервера РЕД АДМ и при вводе его в домен: при редактировании сетевых настроек сервера РЕД АДМ в поле «DNS-серверы» сначала укажите IP-адрес существующего контроллера домена, а затем, через запятую, можно указать адрес второго контроллера домена (локального или внешнего). Например:

```
192.168.0.20, 8.8.8.8
```

3.3.2. Для подключения к веб-интерфейсу откройте браузер на любой машине, с которой доступен IP-адрес сервера РЕД АДМ, и впишите в адресную строку адрес в следующем формате:

```
https://⟨IP-адрес_РЕД_АДМ⟩
```

Например:

```
https://10.1.0.2
```

Примечание. После запуска сервисов веб-интерфейс доступен не сразу. В случае ошибки 502 при загрузке страницы, подождите несколько минут и перезагрузите страницу.

3.3.3. Откроется приветственный экран (рисунок 1), где для продвижения на следующий шаг необходимо принять лицензионное соглашение – поставить галочку в соответствующем чекбоксе и нажать кнопку «Продолжить».

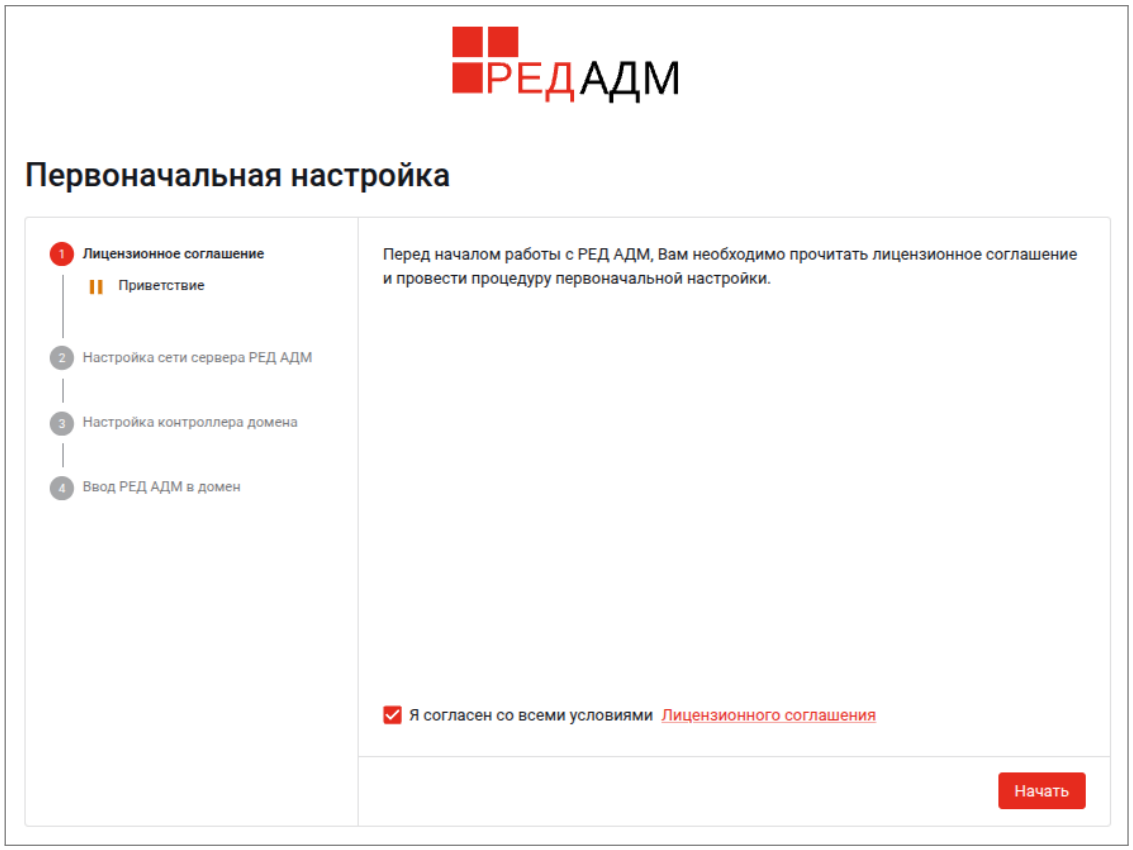

Рисунок 1 – Принятие лицензионного соглашения

3.3.4. На странице «Ввод данных пользователя» (рисунок 2) Вам необходимо ввести логин и пароль для настроенной ранее локальной учётной записи привилегированного пользователя и нажать на кнопку «Продолжить».

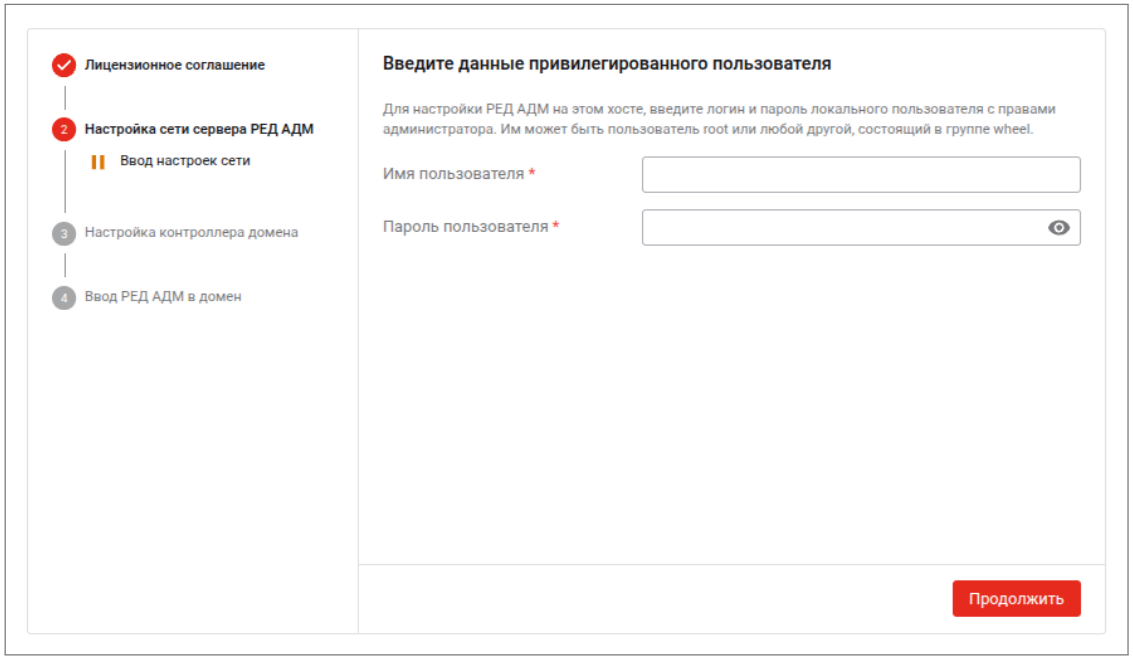

Рисунок 2 – Ввод данных пользователя

Если всё успешно, то выведется всплывающее сообщение «Указанный пользователь имеет sudo права» и вы перейдёте на страницу «Параметры сети» (рисунок 3).

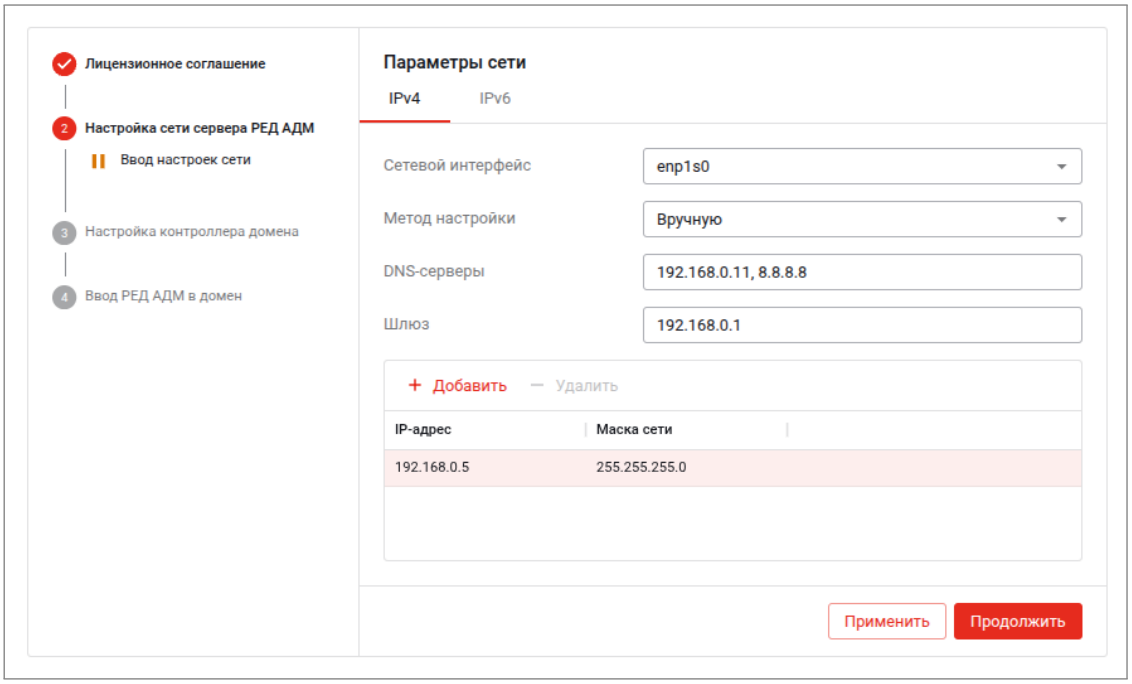

Рисунок 3 – Сервер РЕД АДМ: настройка сети

При необходимости выполните настройки сети: настройки можно выполнить как для IPv4 так и для IPv6. Можно выбрать сетевой интерфейс (если необходимый отличается от выставленного автоматически), а также режим настройки – «Автоматически» (настройки выставлены при установке системы), «Вручную» или «Отключено» (режим «Отключено» нельзя установить для IPv4).

В ручном режиме (рисунок 3) можно задать DNS-серверы и шлюз, добавить или удалить пары из IP-адреса и маски подсети (про правила указания значений IP-адресов DNS сказано в начале подраздела).

Закончив установку настроек, для их применения нажмите на кнопку «Применить», и в случае успеха нажмите на кнопку «Продолжить». Не забудьте проверить доступность репозиториев.

3.3.5. Далее нужно подключить РЕД АДМ Сервер к существующему домену (рисунок 4). Введите параметры домена и данные служебного доменного пользователя (администратора) и нажмите кнопку «Продолжить».

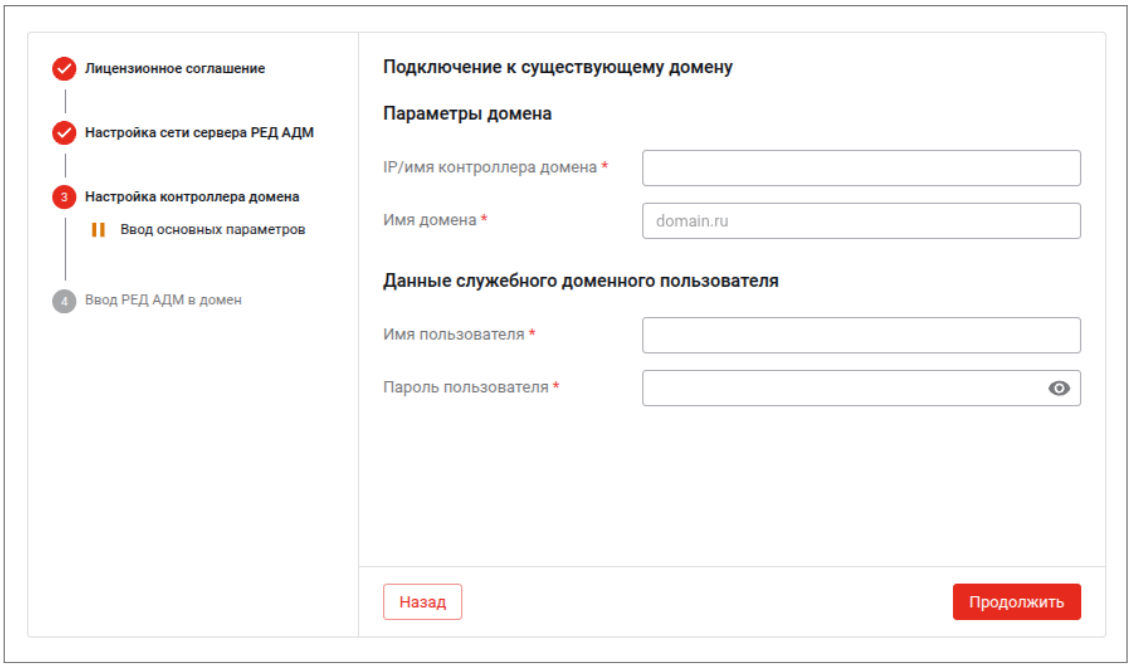

Рисунок 4 – Подключение сервера РЕД АДМ к имеющемуся контроллеру домена

3.3.6. На следующем этапе производится ввод РЕД АДМ в домен (рисунок 5).

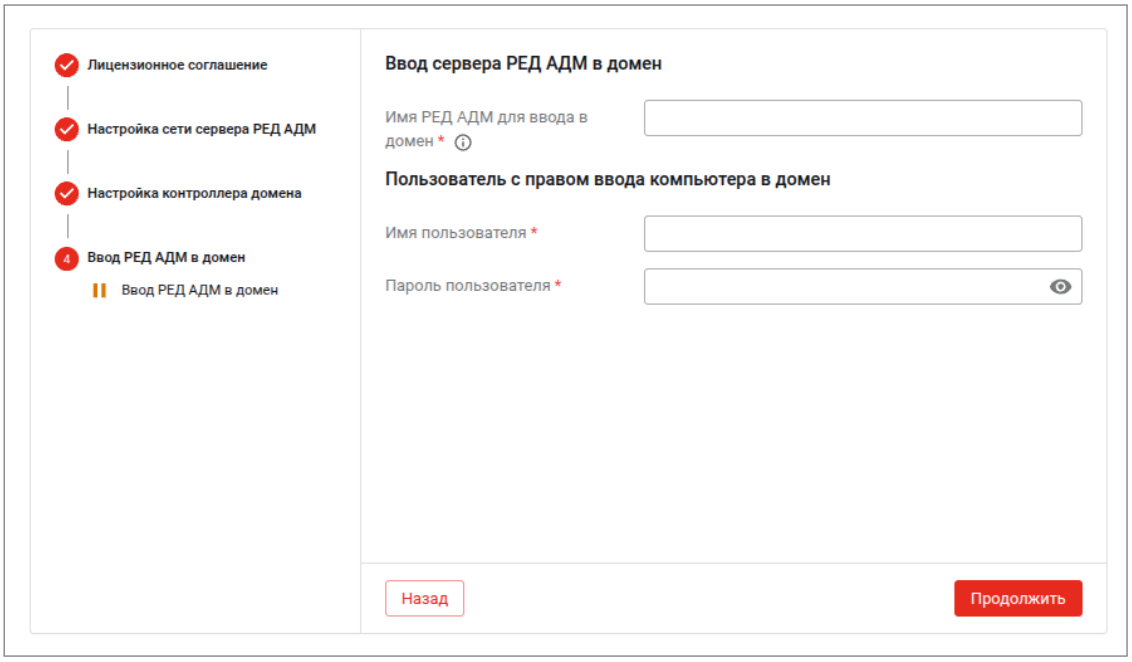

Рисунок 5 – Указание параметров домена

Нужно указать:

– имя хоста, на котором развёртывается РЕД АДМ сервер (без указания домена – например, `redadm`);

– имя и пароль привилегированного доменного пользователя (администратора домена). Если Вы разворачивали новый домен, имя пользователя с необходимыми правами – `administrator`.

После успешного ввода в домен производится генерация сертификатов и установка обновлений. По окончанию процесса откроется окно авторизации.

3.4 Авторизация в веб-интерфейсе

Авторизация в веб-интерфейсе выполняется через учётную запись доменного администратора или служебного доменного пользователя, созданного в ходе первоначальной настройки.

Примечание. РЕД АДМ может производить смену пароля пользователя при авторизации, для этого сервер РЕД АДМ должен быть в домене.

3.4.1. Для входа в веб-интерфейс в открывшейся форме авторизации (рисунок 6) выполните авторизацию доменным администратором или созданным служебным доменным пользователем.

В поле «Имя пользователя» впишите имя доменного администратора (`administrator`) или служебного доменного пользователя.

В поле «Пароль» впишите, соответственно, пароль этого пользователя, и нажмите кнопку «Войти».

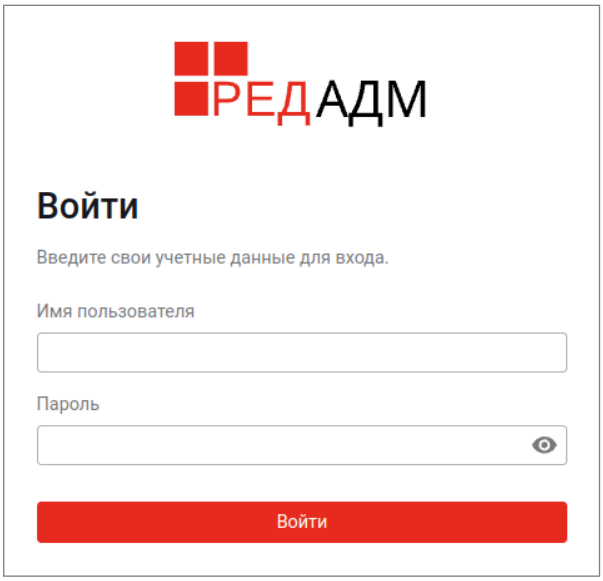

Рисунок 6 – Страница авторизации

После успешного входа вы попадёте на страницу мониторинга (рисунок 7).

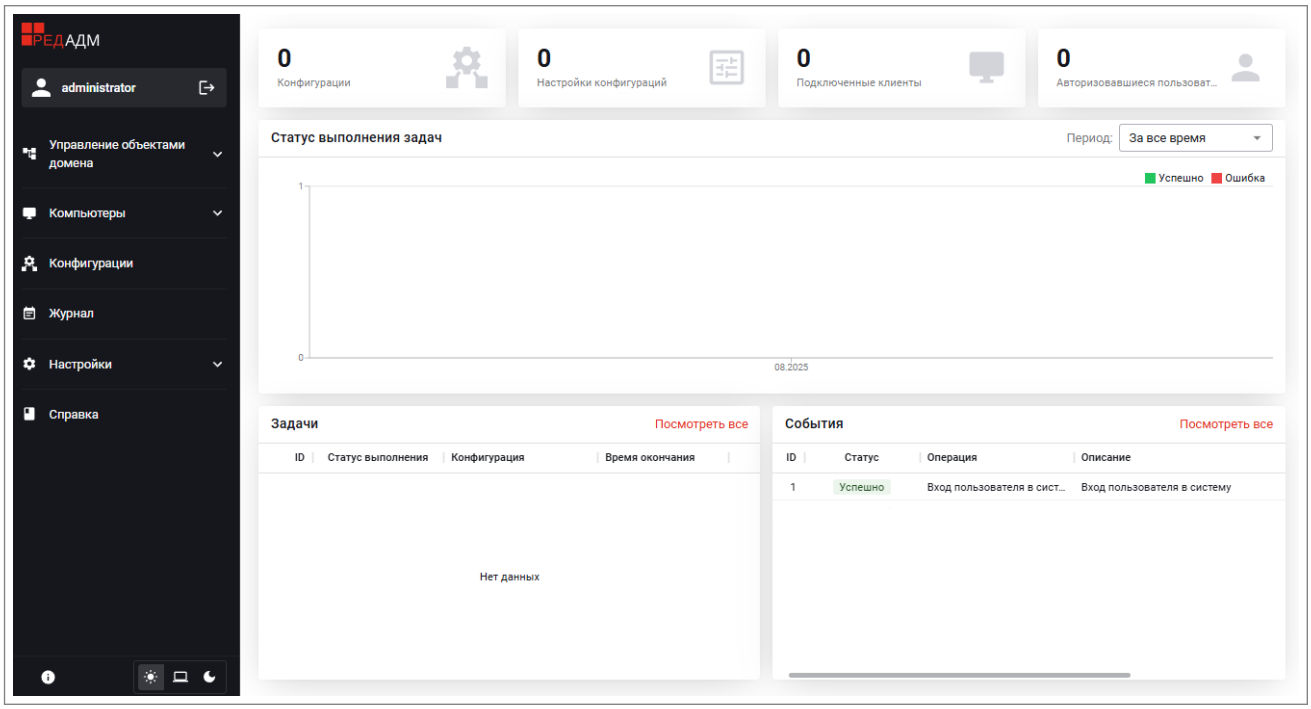

Рисунок 7 – Страница мониторинга системы

4 Обновление РЕД АДМ

Здесь рассмотрена процедура обновления для РЕД АДМ с версии ниже 2.0 до версии 2.0.

4.1 Обновление сервера РЕД АДМ

4.1.1. Выполните команду обновления:

```
dnf update redadm -y
```

4.1.2. Проверьте статусы служб:

```
systemctl status redadm.service rabbitmq-server.service \
redadm-celery-worker.service redadm-celery-beat.service nginx.service
```

4.2 Обновление клиентских агентов РЕД АДМ

4.2.1. В веб-интерфейсе РЕД АДМ перейдите по пути «Настройки» → «Общие» → «Обновление клиентских агентов».

4.2.2. Откроется страница со списком подключённых к РЕД АДМ компьютеров (узлов). При выделении такого узла в списке станет активна кнопка «Обновить клиентский агент». Выберите все узлы и нажмите на эту кнопку.

5 Удаление РЕД АДМ

5.1. Для удаления РЕД АДМ Сервер сначала остановите активные службы:

```
systemctl stop redadm.service rabbitmq-server.service \
redadm-celery-worker.service redadm-celery-beat.service nginx.service
```

Затем выполните команду удаления:

```
dnf remove redadm
```

Удалите директории `/opt/redadm` и `/etc/redadm`:

```
rm -rf /opt/redadm /etc/redadm
```

Приложения

A Файл конфигурации сервера

Для редактирования конфигурационного файла сервера `/etc/redadm/server.conf` выполните команду:

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

При внесении изменений в файл конфигурации вручную, после сохранения файла необходимо перезагрузить службы:

```
systemctl restart redadm.service rabbitmq-server.service \
redadm-celery-worker.service redadm-celery-beat.service nginx.service \
memcached.service
```

A.1 Основные настройки

A.1.1. Секция `[BASE_SETTINGS]` отражает основные настройки РЕД АДМ:

– `SECRET_KEY = ⟨ключ⟩` – генерируется автоматически, 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 клиентской машины указанный пользователь будет использоваться для обращения к этому клиенту. Для данного пользователя должны быть заранее распространены SSH-ключи;

– `JWT_ACCESS_EXPIRATION_SECONDS` – пользовательская переменная, используемая для указания времени истечения срока действия JSON Web Tokens (JWT) в секундах (по умолчанию – 3600). Например, если установлено значение 3600 (1 час), то JWT-токен доступа, выданный пользователю, будет действителен в течение одного часа с момента его создания. После истечения срока действия токена пользователю потребуется повторно аутентифицироваться, чтобы получить новый токен;

– `JWT_REFRESH_EXPIRATION_SECONDS` – пользовательская переменная, которая указывает время истечения срока действия для JSON Web Token (JWT) обновления (по умолчанию – 7200). JSON Web Token Refresh Token (или просто Refresh Token) используется для

обновления устаревших или истекших JWT access token без необходимости повторной аутентификации пользователя. При истечении срока действия Refresh Token пользователь должен повторно аутентифицироваться для получения нового Refresh Token и нового Access Token. Таким образом, Refresh Token предоставляет удобный механизм для обновления токена доступа без необходимости запрашивать у пользователя логин и пароль каждый раз, когда Access Token истекает.

А.2 Настройки SSL-подключения

А.2.1. Безопасное подключение по SSL осуществляется с помощью Wildcard-сертификатов между сервером РЕД АДМ и:

– клиентскими агентами,

– подсистемами РЕД АДМ.

А.2.2. При использовании Центра сертификации выпустите указанные ниже сертификаты и ключи к ним:

– Wildcard-сертификат,

– сертификат для сервера РЕД АДМ,

– корневой сертификат Центра сертификации.

Далее поместите их на сервер РЕД АДМ, и в конфигурационном файле `server.conf` укажите абсолютные пути к ним.

Имена сертификатов и пути к ним могут быть любыми.

> **Важно!** У пользователя `redadm_local_service_user` должно быть право на чтение этих сертификатов и ключей. ■

Действия в том случае, если Центр сертификации развёрнут на сервере MS AD, описаны в Приложении Б.

А.2.3. Секция `[SSL]` определяет настройки подключения по SSL:

– `SSL_RA_PRIVATE_KEY_PATH` – абсолютный путь к закрытому ключу, выпущенному для сервера РЕД АДМ;

– `SSL_RA_PROPAGATION_CERT_PATH` – абсолютный путь к сертификату удостоверяющего центра (CA), который распространяется вместе с Wildcard-сертификатами на подсистемы РЕД АДМ и на клиентские агенты;

– `SSL_RA_NGINX_CERT_PATH` – абсолютный путь к сертификату для сервера NGINX;

– `SSL_MS_WILDCARD_PRIVATE_KEY_PATH` – абсолютный путь к закрытому ключу Wildcard-сертификата;

– `SSL_MS_WILDCARD_CERT_PATH` – абсолютный путь к Wildcard-сертификату.

А.3 Настройки подключения к базе данных

Не используется в текущей редакции.

А.3.1. Секция [DATABASE] определяет настройки подключения к базе данных:
– DB_HOST – IP-адрес сервера с установленной и запущенной базой данных;
– DB_PORT – порт (по умолчанию – 3050);
– DB_NAME – абсолютный путь к файлу созданной ранее базы данных (/db/redadm.fdb);
– DB_TYPE – тип базы данных;
– DB_USER – ранее созданный пользователь этой базы данных (redadm);
– DB_PASSWORD – пароль этого пользователя (redadm).

А.4 Настройки подключения к домену

А.4.1. Секция [LDAP] отражает настройки подключения к вашему домену:
– LDAP_URL – LDAP-ссылка на контроллер домена в формате ldaps://⟨имя⟩:⟨порт⟩, где ⟨имя⟩ – имя или IP-адрес контроллера домена; ⟨порт⟩ – по умолчанию используется порт 636;
– LDAP_DOMAIN_NAME = ⟨имя⟩ – LDAP-имя домена;
– LDAP_DC_END = ⟨имя⟩ – имя в формате DC;
– USERNAME_LDAP – имя пользователя с правом на чтение каталога LDAP;
– PASSWORD_LDAP – пароль указанного пользователя с правом на чтение каталога LDAP;
– LDAP_PAGE_SIZE – максимальное количество отображаемых в интерфейсе РЕД АДМ учетных записей LDAP (по умолчанию – 1000);
– CACHE_REQUEST_LDAP – время кэширования LDAP запросов;
– TIMEOUT_CONNECTION_LDAP – время переподключения пользователя к LDAP.

А.5 Дополнительные настройки

А.5.1. 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.

А.5.2. Секция [OTHER] содержит дополнительные настройки:
– PULL_NUMBER_TASKS = ⟨число⟩ – число запросов на получение конфигураций в режиме «pull», которые РЕД АДМ Сервер будет обслуживать одновременно.

А.5.3. Секция [DOWNLOAD_FOLDERS] определяет расположение дистрибутивов РЕД АДМ и REDDC, предназначенных для развёртывания кластера:
– PATH_DOWNLOAD_REDADM = /opt/redadm/rpm/redadm – директория с дистрибутивом РЕД АДМ;
– PATH_DOWNLOAD_REDDC = /opt/redadm/rpm/reddc – директория с дистрибутивом reddc.

А.5.4. Секция [CLIENT] определяет параметры подключения между сервером и клиентскими агентами РЕД АДМ:
– CLIENT_AGENT_PORT – порт для подключения (по умолчанию – 5000).

А.6 Шифрование пароля

А.6.1. Пароль при развёртывании системы шифруется автоматически. При необходимости шифрование можно выполнить и самим (например, если файл конфигурации `/etc/redadm/server.conf` редактировался вручную). Для шифрования пароля доменного пользователя после сохранения конфигурационного файла выполните команды:

```
cd /opt/redadm/
source .venv/bin/activate
```

Откроется командная строка виртуального окружения `(.venv)`. Введите в ней команду:

```
python scripts/encrypt_config.py -a "PASSWORD_LDAP"
```

Для выхода из виртуального окружения введите команду:

```
deactivate
```

Б Настройки в домене MS AD

В данном Приложении описана работа в Центре сертификации MS CA с Wildcard-сертификатами, используемыми для реализации безопасного SSL-соединения сервера РЕД АДМ с клиентскими агентами и подсистемами РЕД АДМ.

Необходимо выпустить указанные ниже сертификаты и ключи к ним:

– Wildcard-сертификат,

– сертификат для сервера РЕД АДМ,

– корневой сертификат Центра сертификации.

Важно! Значение `RenewalKeyLength` должно быть не меньше, чем **2048**. ■

Далее поместите их на сервер РЕД АДМ, и в конфигурационном файле `server.conf` укажите абсолютные пути к ним.

Имена сертификатов и пути к ним могут быть любыми.

Важно! У пользователя `redadm_local_service_user` должно быть право на чтение этих сертификатов и ключей. ■

Б.1 Выпуск Wildcard-сертификата

Для выпуска Wildcard-сертификата на сервере Центра сертификации выполните по очереди следующие операции:

1) Последовательно нажмите «Пуск» → «Выполнить» (или сочетание клавиш «Win» + «R»).

В открывшейся командной строке введите `mmc` и нажмите «Enter». Откроется Консоль управления (MMC).

2) Последовательно нажмите «Файл» → «Добавить или удалить оснастку...».

3) В списке доступных оснасток выберите «Сертификаты» и нажмите «Добавить».

4) В открывшемся окне «Оснастка диспетчеров сертификатов» выберите «учетной записи компьютера» и нажмите кнопку «Далее».

5) На следующей странице для параметра «Эта оснастка всегда управляет» выберите «локальным компьютером» и нажмите кнопку «Готово».

Вернувшись в окно «Добавление и удаление оснасток», нажмите кнопку «OK».

6) В корне Консоли управления выберите «Сертификаты (локальный компьютер)» и кликните ПКМ по «Личное».

В открывшемся контекстном меню последовательно выберите «Все задачи» («All Tasks») → «Дополнительные операции» («Advanced Operations») → «Создать настраиваемый запрос...» («Create Custom Request»).

7) Откроется окно «Регистрация сертификатов». Нажмите кнопку «Далее».

На следующей странице производится выбор политики регистрации сертификатов. В секции «Настраиваемый запрос» («Custom Request») выберите «Продолжить без политики регистрации» («Proceed without enrollment policy») и нажмите кнопку «Далее».

8) Откроется страница «Пользовательский запрос».

Установите параметры:

– «Шаблон» – «Старый ключ (без шаблона)» («(No template) Legacy key»)

– «Формат запроса» – «PKCS #10»

Нажмите кнопку «Далее».

9) Откроется страница «Сведения о сертификате».

Для создаваемого запроса нажмите на значок «Подробности» («Details») – отобразятся более подробные сведения. Нажмите кпопку «Свойства» («Properties»).

10) Откроется окно «Свойства сертификата».

Во вкладке «Общие» («General») задайте параметры (здесь и далее *вводимые* значения приведены для примера):

– «Понятное имя» («Friendly name») – `*.red.adm`

– «Описание» («Description»): `my wildcard`

Перейдите на вкладку «Субъект» («Subject»):

В секции «Имя субъекта» («Subject name») выберите указанный тип параметра, задайте значение параметра, после чего добавьте (выберите) параметр, нажав кнопку «Добавить» справа (в дальнейшем добавление параметров осуществляется аналогичным образом):

– тип – «Общее имя» («Common name»), значение – `*.red.adm`

В секции «Дополнительное имя» («Alternative name») добавьте (выберите) параметр:

– тип – «Служба DNS», значение – `*.red.adm`

11) Перейдите на вкладку «Расширения» («Extensions»).

В секции «Использование ключа» («Key Usage») в списке «Доступные параметры» («Available options») выберите параметры:

– «Цифровая подпись» («Digital Signature»)

– «Шифрование ключей» («Key Encipherment»)

В секции «Расширенное использование ключа (политики применения)» («Extended Key Usage (application policies)») выберите параметр «Проверка подлинности сервера» («Server Authentication»).

12) Перейдите на вкладку «Закрытый ключ» («Private key»).

В секции «Параметры ключа» («Key options») установите параметры:

– в выпадающем меню «Размер ключа» («Key size») – выберите «2048»;

– установите чекбокс «Сделать закрытый ключ экспортируемым» («Make private key exportable»).

13) Нажмите кнопку «ОК» для применения и сохранения настроек, окно «Свойства сертификата» закроется. Вы продолжите работу в окне «Регистрация сертификатов» на странице «Сведения о сертификате», где будут отображены добавленные выше свойства.

Нажмите кнопку «Далее». Откроется страница сохранения. Укажите расположение и имя файла, формат файла выберите «Base 64». Нажмите кнопку «Готово».

14) В браузере Internet Explorer откройте страницу `https://localhost/certsrv`

Последовательно нажмите «Request a certificate» → «advanced certificate request», и в поле «Saved Request» вставьте содержимое сохранённого файла запроса.

Выберите тип – «Base 64», шаблон сертификата («Certificate template») – «Web-server». Нажмите «Download certificate».

15) В корне Консоли управления выберите «Сертификаты (локальный компьютер)» и кликните ПКМ по «Личное».

В открывшемся контекстном меню последовательно выберите «Все задачи» → «Импорт» и добавьте созданный сертификат.

16) Произведите экспорт открытого и закрытого ключей. По возможности, везде выбирайте формат `Base 64`. При экспорте закрытого ключа обязательно установите пароль (далее, при конвертации, он будет убран).

17) Загрузите ключи на хост с сервером РЕД АДМ.

Б.2 Выпуск сертификата для сервера РЕД АДМ

Для выпуска сертификата для сервера РЕД АДМ на сервере центра сертификации выполните следующие действия:

1) Последовательно нажмите «Пуск» → «Выполнить» (или сочетание клавиш «Win» + «R»).

В открывшейся командной строке введите `mmc` и нажмите «Enter». Откроется Консоль управления (MMC).

2) Последовательно нажмите «Файл» → «Добавить или удалить оснастку...».

3) В списке доступных оснасток выберите «Сертификаты» и нажмите «Добавить».

4) В открывшемся окне «Оснастка диспетчеров сертификатов» выберите «учетной записи компьютера» и нажмите кнопку «Далее».

5) На следующей странице для параметра «Эта оснастка всегда управляет» выберите «локальным компьютером» и нажмите кнопку «Готово».

Вернувшись в окно «Добавление и удаление оснасток», нажмите кнопку «ОК».

6) В корне Консоли управления выберите «Сертификаты (локальный компьютер)» и перейдите в логическое хранилище «Личное».

7) В панели «Тип объекта» кликните ПКМ (правой кнопкой мыши) на свободном месте, и в открывшемся контекстном меню последовательно выберите «Все задачи» («All Tasks») → «Дополнительные операции» («Advanced Operations») → «Создать настраиваемый запрос...» («Create Custom Request»).

8) Откроется окно «Регистрация сертификатов». Нажмите кнопку «Далее».

На следующей странице производится выбор политики регистрации сертификатов. В секции «Настраиваемый запрос» («Custom Request») выберите «Продолжить без политики регистрации» («Proceed without enrollment policy») и нажмите кнопку «Далее».

9) Откроется страница «Пользовательский запрос».

Установите параметры:

– «Шаблон» – «Старый ключ (без шаблона)» («(No template) Legacy key»);

– «Формат запроса» – «PKCS #10».

Нажмите кнопку «Далее».

10) Откроется страница «Сведения о сертификате».

Для создаваемого запроса нажмите на значок «Подробности» («Details») – отобразятся более подробные сведения. Нажмите кпопку «Свойства» («Properties»).

11) Откроется окно «Свойства сертификата».

Во вкладке «Общие» («General») задайте параметры:

– «Понятное имя» («Friendly name») – `redadm.red.adm`;

– «Описание» («Description»): `my server certificate`.

Перейдите на вкладку «Субъект» («Subject»):

В секции «Имя субъекта» («Subject name») добавьте (выберите) параметр:

– тип – «Общее имя» («Common name»), значение – `redadm.red.adm`

В секции «Дополнительное имя» («Alternative name») добавьте (выберите) параметры:

– тип – «Служба DNS», значение – `redadm.red.adm`

– тип – «IP-адрес (v4)», значение – `10.10.10.10`

12) Перейдите на вкладку «Расширения» («Extensions»).

В секции «Использование ключа» («Key Usage») в списке «Доступные параметры» («Available options») выберите параметры:

– «Цифровая подпись» («Digital Signature»)

– «Шифрование ключей» («Key Encipherment»)

В секции «Расширенное использование ключа (политики применения)» («Extended Key Usage (application policies)») выберите параметр «Проверка подлинности сервера» («Server Authentication»).

13) Перейдите на вкладку «Закрытый ключ» («Private key»).

В секции «Параметры ключа» («Key options») установите параметры:

– в выпадающем меню «Размер ключа» («Key size») – выберите «2048»;

– установите чекбокс «Сделать закрытый ключ экспортируемым» («Make private key exportable»).

14) Нажмите кнопку «OK» для применения и сохранения настроек, окно «Свойства сертификата» закроется. Вы продолжите работу в окне «Регистрация сертификатов» на странице «Сведения о сертификате», где будут отображены добавленные выше свойства.

Нажмите кнопку «Далее». Откроется страница сохранения. Укажите расположение и имя файла, формат файла выберите «Base 64». Нажмите кнопку «Готово».

15) В браузере Internet Explorer откройте страницу `https://localhost/certsrv`

Последовательно нажмите «Request a certificate» → «advanced certificate request», и в поле «Saved Request» вставьте содержимое сохранённого файла запроса.

Выберите тип – «Base 64», шаблон сертификата («Certificate template») – «Web-server». Нажмите «Download certificate».

16) В корне Консоли управления выберите «Сертификаты (локальный компьютер)» и кликните ПКМ по «Личное».

В открывшемся контекстном меню последовательно выберите «Все задачи» → «Импорт» и добавьте созданный сертификат.

17) Произведите экспорт открытого и закрытого ключей. По возможности, везде выбирайте формат `Base 64`. При экспорте закрытого ключа обязательно установите пароль (далее, при конвертации, он будет убран).

18) Загрузите ключи на хост с сервером РЕД АДМ.

Б.3 Корневые ключи центра сертификации

Для экспорта корневого ключа центра сертификации на сервере центра сертификации выполните следующие действия:

1) Последовательно нажмите «Пуск» → «Выполнить» (или сочетание клавиш «Win» + «R»).

В открывшейся командной строке введите `mmc` и нажмите «Enter». Откроется Консоль управления (MMC).

2) Последовательно нажмите «Файл» → «Добавить или удалить оснастку...».

3) В списке доступных оснасток выберите «Сертификаты» и нажмите «Добавить».

4) В открывшемся окне «Оснастка диспетчеров сертификатов» выберите «учетной записи компьютера» и нажмите кнопку «Далее».

5) На следующей странице для параметра «Эта оснастка всегда управляет» выберите «локальным компьютером» и нажмите кнопку «Готово».

Вернувшись в окно «Добавление и удаление оснасток», нажмите кнопку «ОК».

6) В корне консоли нажмите на «Сертификаты (локальный компьютер)» и перейдите в логическое хранилище «Личное».

7) Откройте корневой сертификат и последовательно нажмите «Детали» → «Копировать в файл».

Выполните экспорт закрытого ключа в формат `pfx`, обязательно установите пароль.

Выполните экспорт открытого ключа в формат `cer Base 64`.

8) Загрузите ключи на хост с сервером РЕД АДМ.

Б.4 Преобразование ключей для сервера РЕД АДМ

1) Создайте резервную копию директории `/opt/redadm/configs/ssl`

2) Загрузите в директорию `/root` следующие сертификаты, полученные в Центре сертификации MS CA:

- `wildcard-public.cer`
- `wildcard-private.pfx`
- `redadm-server-public.cer`
- `redadm-server-private.pfx`
- `ca-public.cer`
- `ca-private.pfx`

3) Выполните преобразование и переименование ключей:

```
cd /root
```

```
openssl pkcs12 -in wildcard-private.pfx -nocerts -nodes \
-out wildcard_cert.key
openssl pkcs12 -in wildcard-private.pfx -nocerts -nodes \
-out wildcard-key.pem
openssl x509 -in wildcard-public.cer -out wildcard-cert.pem
openssl x509 -in wildcard-public.cer -out wildcard_cert.crt
```

```
   openssl x509 -in redadm-server-public.cer -out redadm-server.crt
   openssl pkcs12 -in redadm-server-private.pfx -nocerts -nodes \
-out redadm-server.key
```

```
   openssl x509 -in ca-public.cer -out redadm-ca.pem
   openssl x509 -in ca-public.cer -out ca.crt
   openssl pkcs12 -in ca-private.pfx -nocerts -nodes -out ca.key
```

```
   cp wildcard_cert.crt /opt/redadm/configs/ssl/pki/issued/
   cp wildcard-cert.pem /opt/redadm/configs/ssl/pki/issued/
   cp redadm-server.crt /opt/redadm/configs/ssl/pki/issued/
```

```
   cp redadm-server.key /opt/redadm/configs/ssl/pki/private/
   cp wildcard_cert.key /opt/redadm/configs/ssl/pki/private/
   cp wildcard-key.pem /opt/redadm/configs/ssl/pki/private/
```

```
   cp ca.crt /opt/redadm/configs/ssl/pki/
```

```
   cp redadm-ca.pem /opt/redadm/configs/ssl/
   cp redadm-server.crt /opt/redadm/configs/ssl/
   cp redadm-server.key /opt/redadm/configs/ssl/
```

```
   chown -R redadm_local_service_user:redadm_local_service_user \
/opt/redadm/configs/ssl/pki/issued/
   chown -R redadm_local_service_user:redadm_local_service_user \
/opt/redadm/configs/ssl/pki/private/
   chown redadm_local_service_user:redadm_local_service_user \
/opt/redadm/configs/ssl/pki/ca.crt
   chown redadm_local_service_user:redadm_local_service_user \
/opt/redadm/configs/ssl/redadm-ca.pem
   chown redadm_local_service_user:redadm_local_service_user \
/opt/redadm/configs/ssl/redadm-server.crt
   chown redadm_local_service_user:redadm_local_service_user \
/opt/redadm/configs/ssl/redadm-server.key
```

4) Добавьте корневой сертификат в хранилище доверенных сертификатов:

```
   cp redadm-ca.pem /etc/pki/ca-trust/source/anchors/
```

```
   update-ca-trust
```

```
   update-ca-trust extract
```

5) Перезагрузите службы сервера РЕД АДМ:

```
   systemctl restart redadm.service rabbitmq-server.service \
redadm-celery-worker.service redadm-celery-beat.service nginx.service \
memcached.service
```