Файл конфигурации сервера

Окружение

- **Версия ОС:** РЕД ОС 8
- **Конфигурация ОС:** РЕД ОС 8
- **Версия ПО:** redadm-2.0.0

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
```

Основные настройки

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.

Настройки SSL-подключения

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

-- клиентскими агентами,

-- подсистемами РЕД АДМ.

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 разделе «Настройки в домене MS AD».

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.

Настройки подключения к базе данных

Не используется в текущей редакции.

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).

Настройки подключения к домену

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.

Дополнительные настройки

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.

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.

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.

4. Секция [CLIENT] определяет параметры подключения между сервером и

клиентскими агентами РЕД АДМ:

-- CLIENT_AGENT_PORT -- порт для подключения (по умолчанию -- 5000).

Шифрование пароля

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
```

Источник: https://redadm.red-soft.ru/base/red-adm/ra-admin/ra-2-0-0-admin/ra-2-0-0-server-config/