Программа для ЭВМ «ExeReport»

Руководство по установке

Листов: 9

Санкт-Петербург, 2025

ГЛОССАРИЙ

ТЕРМИН	ОПРЕДЕЛЕНИЕ
Docker	Программное обеспечение для автоматизации развёртывания и управления приложениями в средах с поддержкой контейнеризации, контейнеризатор приложений.
DNS	Система доменных имен
OpenSSL	Криптографическая библиотека с открытым исходным кодом.
TLS	Протокол защиты транспортного уровня
ОС	Операционная система
ПО	Программное обеспечпение
ПЭВМ	Программа для электронной вычислительной машины
БД	База данных
СУБД	Система управления базами данных
ЭВМ	Электронная вычислительная машина

Содержание

1 Введение

1.1 Область применения программы для ЭВМ «ExeReport»

Программа для ЭВМ «ExeReport» (далее по тексту – ExeReport или Система) предназначена для обработки и представления данных о деятельности предприятия в виде различных отчетов и аналитических панелей.

1.2 Краткое описание возможностей

ExeReport – сервер отчетов, предоставляющий следующие возможности:

- загрузка и хранение макетов отчетов в формате frx;
- настройка и хранение конфигурации отчетов;
- предоставление отчетов пользователю по запросу в различных форматах;
- экспорт отчетов в различные форматы.

ExeReport может использоваться как самостоятельное средство визуализации производственной отчетности, так и встраиваться в различные пользовательские порталы.

1.3 Уровень подготовки пользователя

Требования к квалификации специалиста, отвечающего за установку ПО ExeReport согласно настоящему документу:

- опыт работы с ОС семейства Linux;
- опыт администрирования СУБД PostgreSQL;
- опыт работы с Docker;
- понимание принципов шифрования передачи данных и функционирования протокола TLS;
- знание настоящего Руководства по установке.

2 Подготовка к установке

2.1 Получение доступа и распаковка инсталляционного пакета

Для установки вспомогательных компонентов для запуска ExeReport, виртуальная машина, на которую производиться установка ПО должна иметь доступ в интернет. После установки и запуска ExeReport, доступ в интернет можно отключить.

2.2 Установка Docker

ПО ExeReport устанавливается и запускается в docker.

Для установки docker, в терминале ОС Debian необходимо последовательно выполнить команды, используя учетную запись с правами администратора.

Для обновления пакетов apt выполните команду:

sudo apt update

Далее выполните команду:

sudo apt install apt-transport-https ca-certificates curl gnupg2 software-properties-common

Далее необходимо установить ключ в ОС для подключения официального репозитория Docker:

curl -fsSL https://download.docker.com/linux/debian/gpg | sudo apt-key add -

Подключите репозиторий Docker:

sudo add-apt-repository "deb [arch=amd64] https://download.docker.com/linux/debian $(lsb_release -cs) stable"

Обновите список пакетов:

sudo apt update

Запустите установку последней версии Docker:

sudo apt install docker-ce

Проверьте статус службы Docker:

sudo systemctl status docker

Последняя команда показывает состояние docker. Состояние должно быть active(running).

Детальную информацию по установке Docker также можно найти на сайте Вендора - https://docs.docker.com/engine/install/.

2.3 Установка Guardant Control Center и Guardant SLK

Для корректной работы ExeReport требуется установить следующее ПО на один из компьютеров в сети с docker, который будет выполнять функцию сервера лицензирования ExeReport:

- Guardant Control Center;
- Guardant SLK.

Дистрибутивы указанного выше ПО находятся в архиве ExeReport в папке gcc.

После установки ПО Guardant необходимо активировать лицензию ExeReport с использованием ПО Мастер лицензий Guardant (входит в состав Guardant SLK).

Для активации необходимо использовать ключ лицензии (Серийный номер), предоставленный Вендором.

Детальные инструкции по установке ПО Guardant и активации лицензии представлены на сайте вендора ПО Guardant по ссылке: https://dev.guardant.ru/display/GSLK/Guardant+Control+Center.

2.4 Установка сертификатов

Для использования защищенных протоколов https ssl, необходимо сгенерировать и сконвертировать сертификаты для вашего домена.

Адреса сервисов:

[ip адрес виртуальной машины] postgres.[домен]

[ip адрес виртуальной машины] keycloak.[домен]

[ip адрес виртуальной машины] report.[домен]

Адреса сервисов должны быть добавлены в DNS, либо прописаны в локальных hosts файлах клиентов.

Для создания и конвертации сертификатов необходимо установить openssl. Детальная инструкция по установке доступна по ссылке https://wiki.openssl.org/index.php/Binaries.

2.4.1 Генерация key файла

Для генерации key файла необходимо выполнить команду:

openssl genrsa -out wildcard.[домен].key 2048

2.4.2 Генерация crt файла

Для генерации файла crt используется файл key, сгенерированный ранее и файл cnf. Файл cnf содержит конфигурационную информацию и имеет следующую структуру:

[req]

default_bits = 20482

distinguished_name = req_distinguished_name

req_extensions = req_ext

prompt = no

[req_distinguished_name]
C = RU
ST = Russia
L = [локация - город]
O = [организация]
CN =[домен]

[req_ext]
subjectAltName = @alt_names
extendedKeyUsage = serverAuth, clientAuth
basicConstraints=CA:TRUE

[alt_names]
DNS.1 = keycloak.[домен]
DNS.2 = report.[домен]
DNS.3 = *.[домен]
Для генерации crt файла необходимо выполнить команду:

openssl req -x509 -nodes -newkey rsa:4096 -extensions req_ext -keyout wildcard.[домен].key -out wildcard.[домен].crt -days [срок действия сертификата в днях] -config wildcard.[домен].cnf

2.4.3 Конвертация в PFX

Для конвертации сертификатов в формат PFX необходимо воспользоваться следующей командой:

openssl pkcs12 -export -out wildcard.[домен].pfx -inkey wildcard.[домен].key -in wildcard.[домен].crt

После выполнения команды openssl запросит ввести новый пароль и подтвердить его, после чего, будет создан сертификат в формате pfx.

Получившийся сертификат необходимо скопировать и переименовать:

cp wildcard.[домен].pfx EXEReport.pfx

2.5 Изменение docker-compose.yaml

Для корректного подключения сертификатов необходимо внести их названия в файл docker-compose.yaml.

В файле заложены шаблоны, которые нужно изменить в соответствии с названием домена.

Пример шаблона:

source: ./crt/wildcard.[домен].crt

Для pfx сертификатов, необходимо изменить пароль в следующих строках:

ASPNETCORE_Kestrel__Certificates__Default__Password: "123456"

указав пароль, который использовался при создании pfx сертификатов, п. 2.4.3.

При отсутствии DNS сервера необходимо сконфигурировать адресацию по именам. Для этого в файле docker-compose.yaml нужно добавить в конфигурацию каждого из контейнеров Exereport следующий ключ:

extra_hosts:

- "keycloak.[домен] report.[домен]:[IP адрес виртуальной машины]"

Для доступа контейнеров ExeReport к ПО Guardant необходимо сконфигурировать следующую переменную в файле docker-compose

GCCSettings:Remotehosts:”[IP-адрес]”

указав ip-адрес компьютера, на котором было установлено ПО Guardant, п. 2.3.

3 Установка и запуск ExeReport

3.1 Установка и запуск ExeReport

Сначала необходимо перейти в каталог с распакованным архивом ExeReport. Скопировать в папку ./crt полученные на предыдущих шагах сертификаты (см. раздел 2.4) и изменить файл docker-compose.yaml как описано в разделе 2.5. Далее необходимо в терминале ОС перейти в каталог с распакованным архивом ExeReport и выполнить команду:

./install-exereport.sh

при этом произойдет загрузка образов, копирование данных и запуск сервисов.

ВНИМАНИЕ: Если файл не запускается, измените права на этот файл командой:

chmod +x install-exereport.sh

3.2 Проверка корректности установки

Проверить, что сервисы запустились, можно перейдя в браузере по адресу, указанному при установке: https:// [ip адрес виртуальной машины]:9200.

В случае корректной установки ПО ExeReport в браузере должно открыться стартовое окно приложения ExeReport.

Работа с приложением ExeReport описана в документе Руководство пользователя ExeReport.

Прочие настройки расположены в файле docker-compose.yaml.

4 Обновление ExeReport

Для обновления ПО ExeReport с версии 1.1.0 или 1.2.0 до версии 1.4 необходимо:

- установить ПО Guardant;
- удалить старые и запустить новые контейнеры ExeReport.

4.1 Установка и настройка ПО Guardant

При обновлении ExeReport с версии 1.1.0 на версию 1.2.0 или выше необходимо установить и настроить ПО Guardant в соответствии с требованиями раздела 2.3.

4.2 Запуск контейнеров ExeReport 1.4

Для запуска контейнеров ExeReport версии 1.4, необходимо предварительно остановить и удалить существующие контейнер ExeReport.

ВАЖНО: т.к. Keycloak и ExeReport хранят конфигурацию в БД, при удалении контейнера конфигурация не будет потеряна, внесенные настройки сохранены в БД и будут использованы новой версией контейнера.

В случае использования вновь сгенерированных сертификатов необходимо выполнять запуск ExeReport 1.4 по текущему документу, начиная с раздела 2.4.

В случае использования существующих сертификатов, которые использовались в версии ExeReport 1.1.0 или 1.2.0, запуск ExeReport 1.4 необходимо производить по текущему документу, начиная с раздела 2.5.

При успешном запуске должен запуститься контейнер ExeReport.

По окончанию обновления ExeReport необходимо проверить его работоспособность как описано в разделе 3.2.