Установка Ekassir Identity Platform в Docker

В статье рассмотрена ручная установка в Docker Swarm. В промышленной среде рекомендовано использовать средства автоматизации, например ansible.

Требования

1. Образ Access Manager.
2. Linux дистрибутив с установленным Docker.
3. База данных (MariaDB или Oracle MySQL (Community Edition)).

Получение дистрибутива

1. Компания eKassir передает дистрибутив программного обеспечения

Состав поставки

1. deploy.yml - compose файл для Docker.
2. appsettings.json - основной файл, содержащий настройки приложения.
3. cert.pem - Файл с сертификатами доверенных Удостоверяющих Центров (УЦ).
4. localhost.pfx - PFX-контейнер, содержащий транспортный TLS сертификат и закрытый ключ. Веб-сервер Kestrel использует pfx-контейнер для установки TLS-соединения.
5. localhost-sig.pfx - PFX-контейнер, содержащий подписывающий сертификат и закрытый ключ. Access Manager использует данный pfx для подписи исходящих данных.
6. dataprotectionkey.xml - DataProtectionKey, содержит ключ шифрования чувствительной информации в базе данных.

Конфигурация

deploy.yml

Конфигурация сервиса

1. Задать имя сервиса (services:{{service_name}})
2. Указать название образа программного обеспечения (services:{{service_name}}:image)
3. Выбрать сеть в docker (services:{{service_name}}:networks)
4. Загрузить конфигурацию программного обеспечения через Docker secrets (следующая секция).

Docker secrets

Приложение расположено в папке /app внутри Docker-контейнера.

Через механизм Docker secrets в docker-контейнер загружаются следующие данные.

#	Параметр	Расположение	Описание
1	appsettings.json	/app/appsettings.json	Статическая конфигурация Access Manager
2	DataProtectionKey	/app/keys/dataprotectionkey.xml	Содержит ключ шифрования чувствительной информации в базе данных
3	CA-bundle	/app/bundle/rootCA.crt	Файл с сертификатами доверенных Удостоверяющих Центров.
4	TLS-сертификат	/app/localhost.pfx	Транспортный TLS-сертификат для web-сервера Kestrel
5	Sign-сертификат	/app/localhost-sig.pfx	Подписывающий сертификат. Используется для подписи исходящих сообщений.

appsettings.json

Параметр	Тип	Default	Описание
DatabaseType	string	null	Тип базы данных Access Manager: • "MySQL" - БД MySQL или MariaDB
ekassir.am_configuration_mysql	string	null	Параметры подключения к БД MySQL. Полный список параметров по ссылке MySqlConnectionConnectionString Пример: "Server=10.0.1.1;Database=am23;Uid=username;Pwd=password;Allow User Variables=true;MinimumPoolSize=1;MaximumPoolSize=100;Connection Lifetime=60;Connection Timeout=10;"
BasePath	string	null	Базовый URL, если Access Manager установлен за proxy-сервером. Если AM доступен по URL https://example.ru/am, необходимо установить значение параметра "/am". Пример: "/am"
Path	string	null	Путь внутри docker до PFX-контейнера. Пути заданы в параметрах TSL-сертификат и Sign-сертификат файла deploy.yml
Password	string	null	Пароль от PFX-контейнера

cert.pem

Содержит сертификаты доверенных УЦ. Необходимо добавить сертификат внутреннего УЦ, развернутого внутри компании, если он используется.

localhost.pfx и localhost-sig.pfx

Рекомендуется сгенерировать данные файлы локальным удостоверяющим центром или приобрести у доверенного УЦ. Требования к сертификатам

Использование ключа (англ. key usage) OID 2.5.29.15 (См. *IETF RFC 5280, раздел 4.2.1.3*):

- Цифровая подпись (англ. digital signature), т.е. установлен бит 0 в поле сертификата **KeyUsage**
- Шифрование ключей (англ. key encipherment), т.е. установлен бит 2 в поле сертификата **KeyUsage**
- Шифрование данных (*англ*. data encipherment), т.е. установлен бит 3 в поле сертификата **KeyUsage**

Расширенное использование ключа (англ. extended key usage) [*прим.* в ОС Windows используется термин «*Улучшенный ключ*»] или Прикладные политики (англ. Application policies):

- Аутентификация сервера (англ. server authentication) *[прим.* в ОС Windows используется термин *«Проверка подлинности сервера*»] OID 1.3.6.1.5.5.7.3.1 (см. *RFC 3280*)
- Аутентификация клиента (англ. client authentication) [прим. в ОС Windows используется термин «*Проверка подлинности клиента*»] OID 1.3.6.1.5.5.7.3.2 (см. RFC 3280)

dataprotectionkey.xml

Можно использовать файл из поставки AM для целей тестирования. Для промышленной эксплуатации необходимо сгенерировать отдельный Data Protection Key с помощью утилиты Access Manager Cli.

Запуск сервиса

Скопировать файлы в папку на сервер с установленным docker и выполнить команду:

```
docker stack deploy -c deploy.yml {{stack_name}}
```