Инструкция по установке

Magnus ID

Оглавление

Введение

Данный документ представляет собой руководство по развертыванию системы Magnus ID для проведения тестирования, а также описание необходимых настроек и действия, которые необходимо выполнить для тестового запуска системы.

1. Исполнение в программном комплексе

1.1 Аппаратные требования

Требования к устройству для запуска и тестирования:

- Соединение с сетью Интернет;
- Устройство с минимальными характеристиками:
  - CPU – 8 ядер;
  - RAM – 16 Гб;
  - Диск – 40 Гб.
- ПО, установленное на устройстве:

  Дистрибутив Linux (Debian любой актуальной версии https://www.debian.org/releases/).

- Минимальные поддерживаемые версии браузер:
  - Yandex browser 25.8.5 или выше;
  - Microsoft Edge 140.0.3485.24 или выше;
  - Google Chrome 140.x или выше;
  - Mozila firefox 142.0 или выше;
  - Opera 121.0.5600.20 или выше;
  - Safari 18.6 или выше.

1.2 Подготовка среды

- Для установки **Docker** необходимо последовательно выполнить команды от пользователя `root`:

  1. `apt update`
  2. `apt install apt-transport-https ca-certificates curl`
  3. `curl -fsSL https://download.docker.com/linux/debian/gpg -o /etc/apt/keyrings/docker.asc`
  4. `echo "deb [arch=$(dpkg --print-architecture) signed-by=/etc/apt/keyrings/docker.asc] https://download.docker.com/linux/debian $(lsb_release -cs) stable" > /etc/apt/sources.list.d/docker.list`
  5. `apt update`
  6. `apt install docker-ce`
  7. `docker -v`

В случае успешной установки будет получена версия Docker.

Пример сообщения об успешной установке Docker:

```
Docker version 28.4.0, build d8eb465
```

- Для работы Magnus ID необходим SSL сертификат. При отсутствии доверенного сертификата возможно сгенерировать самоподписанный, для этого потребуется пакет OpenSSL. Установить пакет и сгенерировать самоподписанный сертификат можно следующими командами:

```
1. apt install openssl
2. openssl req -x509 -newkey rsa -days 365 -noenc -keyout privkey.pem -
   out cert.pem -subj "/CN=example.com" -addext
   "subjectAltName=DNS:example.com,DNS:*.example.com,IP:10.0.0.1"
```

1.3 Установка на физическое оборудование

Тестовая лицензия для использования программного комплекса Magnus ID не требуется. Данный комплекс имеет полную функциональность, не ограничиваясь лицензиями.

- Архив дистрибутива необходимо распаковать в директорию, из которой будет запускаться ПО, заменив в команде `/path/to/dir` на путь до директории установки:

```
1. tar -zxf magnusid-dist.tar.gz -C /path/to/dir
```

- Скопировать предварительно выпущенный или созданный самоподписанный сертификат и приватный ключ в файлах `ssl/cert.pem` и `ssl/privkey.pem` соответственно.

- Отредактировать файл конфигурации `.env` в директории установки. Список параметров конфигурации:

  - `IDM_HOSTNAME` — адрес хоста, на котором будет работать ПО. Можно указать DNS имя или IP адресс;

  - `IDM_FRONT_CLIENT_ID` — ID клиента в системе, для авторизации через веб-интерфейс;

  - `IDM_FRONT_CLIENT_SECRET` — секретный ключ клиента в системе, для авторизации через веб-интерфейс;

- PGP_ENCRYPTION_KEY — ключ шифрования паролей в БД;
- CAS_WEBFLOW_CRYPTO_SIGNING_KEY — ключ длинной не менее 64 байт, закодированный в Base64 для подписи передаваемых данных. Можно сгенерировать следующей командой:
  - `head -c 64 /dev/urandom | base64`
- CAS_WEBFLOW_CRYPTO_ENCRYPTION_KEY — ключ длинной 16 байт, закодированный в Base64 для шифрования передаваемых данных. Можно сгенерировать следующей командой:
  - `head -c 16 /dev/urandom | base64`
- CAS_AUTHN_TOKEN_CRYPTO_SIGNING_KEY — ключ длинной 32 байта, закодированный в Base64 для подписи токенов авторизации. Можно сгенерировать следующей командой:
  - `head -c 32 /dev/urandom | base64`
- CAS_AUTHN_TOKEN_CRYPTO_ENCRYPTION_KEY — ключ длинной 32 байта, закодированный в Base64 для шифрования токенов авторизации. Можно сгенерировать следующей командой:
  - `head -c 32 /dev/urandom | base64`
- MGNS_SECURITY_TOTP_SECRET_KEY — ключ для генерации временных одноразовых паролей;
- MAIL_HOST — адрес почтового сервера;
- MAIL_USERNAME — имя пользователя на почтовом сервере;
- MAIL_PASSWORD — пароль для авторизации на почтовом сервере;
- DATABASE_USER — имя создаваемого пользователя во внутренней СУБД для работы ПО;
- DATABASE_PASSWORD — пароль для создаваемого пользователя во внутренней СУБД;
- DATABASE_NAME — имя создаваемой БД во внутренней СУБД;
- REDIS_PASSWORD — пароль внутреннего Redis сервера;

    - `POSTGRES_SUPERUSER_PASSWORD` — пароль суперпользователя во внутренней СУБД, может потребоваться в случае выполнения административных задач с СУБД;

- Загрузить прилагаемые образы в хранилище Docker:

```
1. docker image load -i images/services.tar
2. docker image load -i images/distrib.tar
```

- Запустить все Docker контейнеры в директории с распакованным дистрибутивом ПО:
    - `docker compose up -d`
- Для входа в интерфейс Magnus ID нужно в браузере перейти по адресу `https://<hostname>/`. Где `<hostname>` — это адрес сервера, на котором развёрнут дистрибутив.

2. Контактная информация

Компания ООО «МАГНУС ТЕХ» (ОГРН 1217700002959).

Адрес: 105082, г. Москва, ул. Большая Почтовая, д 36 стр. 1

Контакты:

По вопросам поддержки обращайтесь:

- На официальный сайт: Magnus-tech.ru
- На электронную почту: support@Magnus-tech.ru
- По телефону: +7(800)550-27-84

Отзыв по документации:

Если вы нашли ошибки в документации или у Вас есть предложения, свяжитесь с нами по адресу support@Magnus-tech.ru.

3. Информация о компании

Magnus Tech - специализируется на разработке инновационных систем и комплексных решений для эффективного управления бизнес-процессами в современных условиях. В основе деятельности компании лежит активное внедрение передовых технологий, с особым акцентом на вопросах безопасности и защиты данных.

Одним из направлений работы является создание надежного программного обеспечения для защищенного файлового обмена и организации совместной работы. Такие решения становятся важным элементом успешной цифровой трансформации рабочего пространства, что позволяет предлагать партнерам высококачественные продукты, соответствующие самым строгим требованиям информационной безопасности.

Разработки компании не только решают сложные бизнес-задачи, но и обеспечивают полную сохранность данных, становясь незаменимыми инструментами в стратегии цифровизации рабочих процессов. Постоянное совершенствование продуктов позволяет соответствовать актуальным потребностям рынка и обеспечивать максимальную эффективность работы партнеров.