

DRE Defender

Руководство по установке

Индекс	DREDefender-IG
Конфиденциальность	Публичный - L0
Ревизия	1.0
Статус	Согласован

Содержание

1. Аннотация	3
2. Термины и сокращения	4
3. Требования к квалификации установщика	5
4. Системные требования	6
4.1. Аппаратное обеспечение	6
4.2. Программное обеспечение	6
5. Предварительные действия	7
5.1. Установка и настройка PostgreSQL	7
5.2. Установка и настройка Redis	7
6. Установка и настройка системы	8
7. Использование Minio для аудита	9

1. Аннотация

Документ предназначен для технических специалистов, занимающихся установкой, настройкой и поддержкой сервиса. Документ рассчитан на инженеров, обладающих специальными навыками и знаниями в области инсталляции программного обеспечения.

i Данный документ опубликован исключительно для изучения системных требований при установке продукта, а также ознакомления с последовательностью и деталями процесса установки. Реальная установка продукта производится с использованием внутренних репозиторийв ООО "Цифра", доступ к которым предоставляется заказчику по запросу.

2. Термины и сокращения

Термин\Сокращение	Определение\Расшифровка
БД	База данных.
DRE Defender	Сервис маршрутизации запросов, продукт ООО "Цифра".
AGS	API Gateway Server, рабочее название продукта DRE Defender.

3. Требования к квалификации установщика

Для установки системы сотрудник обязан:

- иметь базовые представления и практические навыки работы с системой оркестрации Kubernetes (<https://kubernetes.io/docs/tutorials/kubernetes-basics/>) и пакетным менеджером Helm.
- иметь навыки работы с ОС семейства Linux, а именно:
 - установка пакетов;
 - создание и настройка сетевых подключений;
 - запуск служб, настройка автозапуска служб;
 - установка и настройка PostgreSQL;
 - создание и работа с БД под управлением PostgreSQL.
- иметь знания о DNS.
- иметь базовые представления и практические навыки работы с Git.
- иметь навыки работы с ssl-сертификатами.

4. Системные требования

4.1. Аппаратное обеспечение

Рекомендации по минимальной конфигурации серверного обеспечения:

Число пользователей - до 10 000:

1. Сервер с 4 ГБ RAM и 4 ядрами (без Rancher)
2. Сервер с 8 ГБ RAM и 8 ядрами (при наличии Rancher).

Число пользователей - до 5 000 000:

1. 2 x Сервер с 8 ГБ RAM и 8 ядрами.
2. 5 x Сервер с 16 ГБ RAM и 4 ядрами
3. 2 x Сервер с 16 ГБ RAM и 8 ядрами
4. 1 x Сервер 4 GB RAM и 4 ядрами

4.2. Программное обеспечение

Для установки необходимо предварительно выполнить следующие условия:

1. Установить и настроить кластер Kubernetes.

Так как развертывание производится в кластере k8s, то необходим config file для доступа к кластеру.

- Если пользователь выполнял развертывание Kubernetes самостоятельно, то он сам должен создать config file (см. документацию Kubernetes).
- Если Kubernetes был развернут сторонними людьми, то необходимо получить config file у администратора кластера.

Установкой и администрированием системы Kubernetes занимаются сотрудники Отдела поддержки инфраструктуры.

2. Установить kubectl (<https://kubernetes.io/docs/tasks/tools/install-kubectl/>).

3. Установить helm (<https://helm.sh/ru/docs/intro/install/>).

Helm необходим в случае ручной установки элементов системы в кластер k8s. При стандартной установке с использованием gitlab-ci использование helm не предполагается.

4. Развернуть DNS-сервер, преобразование имен DNS-зоны настроить на мастера k8s (созданы А записи на зону DNS).

5. Развернуть кластер БД (Кластер высокой доступности PostgreSQL (High-Availability Cluster)) - ссылка на документ по развертыванию предоставляется Заказчику по Запросу

- Для корректной работы системы AGS необходим доступ к следующим ресурсам:

- GS Labs chartmuseum: (ссылка предоставляется Заказчику по запросу)
- GS Labs gitlab: (ссылка предоставляется Заказчику по запросу)
- Необходим доступ к репозиторию, содержащему helmfile для развертывания AGS. Helm файл содержит инструкции, с помощью которых осуществляются настройки устанавливаемых компонентов. Сами компоненты поставляются в виде чартов (charts), из которых развертываются Kubernetes Pods. Данные берутся из gitlab (gitlab)

5. Предварительные действия

i Начиная с релиза AGS ver. 1.2, появилась база данных Redis. Для использования этой базы требуется установить и настроить Redis. Сама БД развертывается с помощью CI/CD (аналогично другим компонентам AGS).

Можно работать как в Standalone режиме, так и в кластерном режиме.

5.1. Установка и настройка PostgreSQL

Рекомендуется использовать расширение TimescaleDB для работы с Time-series - партиционирование таблиц, функции агрегации и т.д.

После установки PostgreSQL выполнить действия:

1. Развернуть пулер соединений перед PostgreSQL (опционально для тестовых зон).
2. Установить расширение TimescaleDB.
3. Создать БД для AGS.
4. Создать пользователя с доступом только к этой БД.
5. Записать артефакты конфигурации для последующей настройки AGS:
 - IP-адрес и порт мастера (пулера).
 - Имя БД.
 - Логин и пароль пользователя.
 - Имя схемы, используемой в БД (по умолчанию - "public").

5.2. Установка и настройка Redis

В соответствии с Системными требованиями, для корректной работы системы AGS требуется поднять базу данных Redis. Все Redis'ы должны быть доступны из кластера.

Процедура установки Redis описана здесь: <https://redis.io/docs/getting-started/>

Параметры работы с Redis'ами настраиваются в конфигурационных файлах сервисов AGS.

Конфигурацию самих Redis менять не требуется.

6. Установка и настройка системы

Конфигурация и утилиты helm для разворачивания AGS находятся в репозитории (ссылка и права доступа предоставляются по запросу заказчика).

7. Использование Minio для аудита

Audit — это один из сервисов AGS. Аудит запросов пользователей, использующих AGS для доступа к целевым сервисам, предполагает контроль и мониторинг активности пользователей на сервере хранения данных. Этот процесс включает в себя проверку логов, анализ запросов и действий пользователей с целью обеспечения безопасности, целостности и конфиденциальности информации, а также выявления возможных нарушений или несанкционированных действий.

MinIO — это объектное хранилище данных с совместимым интерфейсом Amazon S3. Оно используется в качестве хранилища для сервиса storage. Сервис storage необходим для проведения аудита, он сохраняет файлы из запросов пользователей.

© ООО "Цифра", 2023-2025.

Документация "DRE Defender. Руководство по установке" является объектом авторского права. Воспроизведение всего произведения или любой его части воспрещается без письменного разрешения правообладателя.