R-Vision UEBA

Руководство по установке

Настоящий документ является собственностью ООО "Р-Вижн" и защищен законодательством Российской Федерации об авторских правах и интеллектуальной собственности.

Копирование документа либо его фрагментов в любой форме, распространение, в том числе в переводе, а также их передача третьим лицам возможны только с письменного разрешения ООО "Р-Вижн".

СОДЕРЖАНИЕ

1. ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ

В этом разделе представлены технические требования к аппаратной и программной части оборудования.

1.1. О вариантах конфигурации R-Vision UEBA

R-Vision UEBA может быть установлен в двух вариантах:

1. **Моно-инсталляция** предполагает установку всех компонентов системы на одной машине.
2. **Мульти-инсталляция** предполагает установку хранилищ (ClickHouse, PostgreSQL) на отдельной машине.

Тип конфигурации зависит от параметров используемых машин, а также от планируемого количества событий в секунду (Events Per Second, EPS). Рекомендуется устанавливать ClickHouse и PostgreSQL на отдельном сервере при планировании нагрузки от **10000 EPS**.

В разделе Аппаратные требования приведена таблица соответствия EPS разным типам инсталляции с требованиями к оборудованию.

Для повышения производительности вы можете вынести сервис ClickHouse на отдельную машину в ходе эксплуатации.

1.2. Аппаратные требования

Ниже приведена таблица типов установки и требований к аппаратной части в зависимости от планируемого количества передаваемых событий в секунду (EPS):

Событий в секунду	Тип установки	Объем оперативной памяти, ГБ	Количество ядер процессора	Объем SSD (на 6 месяцев)
1000	Моно	26	17	3 ТБ
5000	Моно	34	25	15 ТБ
10000	Узел основных компонентов	14	21	500 ГБ (без срока)
	Узел сервисов хранения данных	40	19	45 ТБ

Событий в секунду	Тип установки	Объем оперативной памяти, ГБ	Количество ядер процессора	Объем SSD (на 6 месяцев)
	(ClickHouse, PostgreSQL)			
15000	Узел основных компонентов	16	25	500 ГБ (без срока)
	Узел сервисов хранения данных (ClickHouse, PostgreSQL)	50	25	60 ТБ
20000	Узел основных компонентов	20	248	500 ГБ (без срока)
	Узел сервисов хранения данных (ClickHouse, PostgreSQL)	62	31	80 ТБ
25000	Узел основных компонентов	22	33	500 ГБ (без срока)
	Узел сервисов хранения данных (ClickHouse, PostgreSQL)	72	38	105 ТБ
30000	Узел основных компонентов	24	37	500 ГБ (без срока)
	Узел сервисов хранения данных (ClickHouse, PostgreSQL)	82	44	120 ТБ
35000	Узел основных компонентов	26	41	500 ГБ (без срока)
	Узел сервисов хранения данных (ClickHouse, PostgreSQL)	94	50	120 ТБ
40000	Узел основных компонентов	28	46	500 ГБ (без срока)
	Узел сервисов хранения данных (ClickHouse, PostgreSQL)	104	57	165 ТБ
45000	Узел основных компонентов	32	50	500 ГБ (без срока)
	Узел сервисов хранения данных (ClickHouse, PostgreSQL)	114	63	180 ТБ
50000	Узел основных компонентов	34	53	500 ГБ (без срока)
	Узел сервисов хранения данных (ClickHouse, PostgreSQL)	124	69	205 ТБ

Для нагрузок выше **5000 EPS** рекомендуется использовать процессоры со следующими характеристиками:

1. AMD, ~3.6 GHz, не старше 2 лет.
2. Intel, ~3.6 GHz, не старше 3 лет.

1.3. Требования к операционной системе

R-Vision UEBA поддерживает следующие операционные системы:

1. Astra Linux SE 1.7;
2. RED OS 7.2;
3. ALT Linux Server 8.2SP и Server 10;
4. Debian 11;
5. Ubuntu 18.04.5 LTS.

Требования к ОС:

1. 64-битная инсталляция.
2. Версия ядра Linux: 4.11 или выше.
3. Iptables: 1.4 или выше.
4. Docker: 17.05.0 или выше.
5. Docker-compose: 1.29.2 или выше.
6. Git: 1.7 или выше.
7. Исполняемый файл `ps`, обычно предоставляемый `procps` или аналогичным пакетом.
8. XZ Utils 4.9 или выше.
9. Правильно смонтированная иерархия `cgroupfs`: одной общей точки монтирования `cgroup` недостаточно для гарантированной работы.

1.4. Требования к системе хранения данных

Количество циклов чтения-записи в секунду (IOPS) на системе хранения данных должно составлять не менее 6000.

Проведите тест для проверки вашей системы хранения данных на производительность:

1. Откройте сессию терминала и запустите команду:

```
fio --randrepeat=1 --ioengine=libaio --direct=1 --gtod_reduce=1
--name=fiotest --filename=testfio --bs=4k --iodepth=16 --
   size=1G
--readwrite=randrw --rwmixread=40
```

2. Проверьте количество IOPS на одной сессии, затем запустите еще две сессии с той же командой.

3. Проверьте количество IOPS на трех сессиях, затем запустите еще две сессии с той же командой.

Если при переходах от одной сессии к трем, а затем к пяти сессиям происходит резкое снижение IOPS (в разы), такая система хранения данных может серьезно снизить производительность всей платформы.

1.4.1. Используемые СУБД

В R-Vision UEBA используются следующие СУБД с открытым исходным кодом:

- PostgreSQL 11.14 (postgres:11.14)
- ClickHouse 22.6.8.35 (clickhouse/clickhouse-server:22.6.8.35)

1.5. Требования к Docker

R-Vision UEBA требует следующие параметры Docker для корректной работы:

1. Логирование в формате JSON (`json-file`).
2. Ограничение по количеству (`log-opts.max-file`) и размеру логов (`log-opts.max-size`): максимум 3 файла по 10 мегабайт каждый.
3. Директория Docker (`data-root`) по умолчанию: `/opt/var/docker`.
4. Пользователь системы, работающий с Docker, принадлежит к группе Docker, а также имеет полные права на папку с файлами установки UEBA как sudoer.

2. УСТАНОВКА СИСТЕМЫ

Для установки системы вам могут потребоваться права суперпользователя (`sudo`).

2.1. Подготовка сервера к установке

Ознакомьтесь с техническими требованиями.

1. Проверьте версию ядра Linux:

```
uname -r
```

2. Убедитесь, что установлены все необходимые обновления безопасности и исправления.
3. Убедитесь, что установлен Docker версии не ниже 17.05 со всеми зависимостями:

```
docker -v
```

4. Выделите три точки монтирования:
    1. ОС: `/`
    2. Docker: `/opt/var/docker`

        Предварительно перенесите данные Docker в новую директорию `/opt/var/docker`, чтобы избежать проблем с работой ОС, если на выделенной точке монтирования закончится место.

    3. R-Vision UEBA: `/opt/sense`
5. Убедитесь, что у пользователя есть полные права на Docker (т. е. он состоит в группе `docker`), а также на папку с R-Vision UEBA (т. е. он состоит в группе `sudoers`).

2.2. Шаг 1. Скачивание и распаковка установочных файлов

1. Отправьте запрос в службу клиентской поддержки support@rvision.ru для получения актуальной ссылки на установочный дистрибутив.

2. Перейдите в директорию `/opt`. По умолчанию R-Vision UEBA устанавливается в эту директорию.
3. Загрузите архив и переместите его в директорию `/opt` любым удобным способом.
4. Распакуйте установочные файлы командой:

```
tar -xzvf /opt/sense-<TAG>.tar.gz -C /opt/
```

где <TAG> — это номер версии, который необходимо подставить в команду без пробелов.

> В архиве на верхнем уровне находится директория `sense`. Если указана другая директория для установки продукта, перенесите файлы из директории `sense` в нужную директорию с заменой файлов.

5. Для экономии места на жестком диске вы можете удалить архив из директории `/opt/` после распаковки:

```
rm /opt/sense-<TAG>.tar.gz
```

2.3. Шаг 2. Инициализация настроек

Все внешние настройки и учетные записи содержатся в файлах конфигурации в директориях с постфиксом `_default`.

1. Общие параметры конфигурации и переменные окружения: /opt/sense/config/envs_default.
2. Общие настройки прокси-сервера: /opt/sense/config/envoy/config.
3. Настройки внутреннего прокси: /opt/sense/config/envs/balancer.
4. Демонстрационные SSL-сертификаты: /opt/sense/config/envoy/certs_default.
5. Файлы конфигурации ClickHouse (при использовании): /opt/sense/config/clickhouse.

При первичной установке R-Vision UEBA:

1. Скопируйте директорию `/opt/sense/config/envs_default` как `/opt/sense/config/envs`:

```
cp -R /opt/sense/config/envs_default /opt/sense/config/envs
```

2. Скопируйте директорию `/opt/sense/config/config_default` как `/opt/sense/config/config`:

```
cp -R  /opt/sense/config/envoy/config_default
   /opt/sense/config/envoy/config
```

3. Скопируйте директорию `/opt/sense/config/envoy/certs_default` как `/opt/sense/config/envoy/certs`:

```
cp -R  /opt/sense/config/envoy/certs_default
   /opt/sense/config/envoy/certs
```

4. При использовании ClickHouse скопируйте в директорию `/opt/sense/config/clickhouse` одну из стандартных директорий, в зависимости от вашего вида установки:

   a. `/opt/sense/config/clickhouse_mono_default` для монолитной установки.

   b. `/opt/sense/config/clickhouse_cluster_default` для кластерной установки.

После копирования стандартных файлов конфигурации приступите к их настройке.

2.4. Шаг 3. Изменение конфигурационных файлов окружения

При необходимости измените конфигурационные файлы в директории `opt/sense/config/envs`. Здесь вы можете ввести имена хостов, порты, названия БД и пароли к ним, ключи шифрования, порты коннекторов и т. д.

Переменные, обязательные для изменения:

1. В файле /opt/sense/config/envs/backend:
   - **FRONTEND_URL**: адрес, на котором будет располагаться UI.
   - **JWT_ACCESS_TOKEN_SECRET**: приватный ключ для выпуска JWT access-токена.
   - **JWT_REFRESH_TOKEN_SECRET**: приватный ключ для выпуска JWT refresh-токена.

- **CREDENTIAL_KEY**: мастер-ключ для шифрования паролей.

2. В файле /opt/sense/config/envs/gateway:

   1. **SERVER_NAME_LIST**: список имен хостов, совпадающий с сертификатом SSL. Указывается через пробел.

2.5. Шаг 4. Установка ограничений по ресурсам и масштабирование сервисов

Типы сервисов R-Vision UEBA, их ограничения для RAM и CPU, а также возможности масштабирования описаны в инструкции по установке ограничений ресурсов.

2.6. Шаг 5. Организация работы с envoy-gateway прокси

Параметры точек входа в систему (например, коннекторы) указаны в файлах директории `/opt/sense/config/envoy/config`. Для внесения изменений в параметры точек входа отредактируйте файлы в поддиректориях:

1. /opt/sense/config/envoy/config/clusters
2. /opt/sense/config/envoy/config/listeners

> Например, если вы не используете QRadar, удалите соответствующие файлы из обеих директорий. При необходимости добавьте новые точки входа в обе директории.

После любого изменения точек входа перезагрузите контейнер `gateway` при помощи docker-compose.

2.7. Шаг 7. Настройка SSL

В процессе установки распаковываются демо-сертификаты SSL. Для дальнейшей работы с сертификатами воспользуйтесь инструкцией по настройке SSL.

2.8. Шаг 8. Установка UEBA

Установка системы после инициализации настроек производится в автоматическом режиме.

В директории `/opt/sense` выполните скрипт инсталляции **install.sh**. Скрипт автоматически загрузит все Docker-образы, необходимые для работы R-Vision UEBA, и запустит контейнеры.

2.9. Шаг 9. Проверка работоспособности

После установки проверьте наличие ошибок в запущенных сервисах:

1. изучите логи запуска и работы с помощью команды:

```
docker logs -t --tail 1000 <имя_контейнера>
```

2. Проверьте работоспособность контейнеров через сервис Warden, используя следующий URL: `http://<ip-address>/api/warden/health`где `<ip-address>` - адрес веб-интерфейса UEBA.

Если в логах не наблюдается ошибок, перейдите в веб-интерфейс R-Vision UEBA по адресу `http://<ip-address>` или `http://<dns-name>`, если есть внутреннее доменное имя. Данные для входа по умолчанию:

1. Логин: **admin**.
2. Пароль: **admin**.

По соображениям безопасности рекомендуется изменить логин и пароль после установки.

Для перезапуска R-Vision UEBA введите команду

```
docker-compose -f /opt/sense/docker-compose.prod.yml restart
```

2.10. Перемещение корневой директории Docker и настройка лог-файлов

Перед установкой системы необходимо настроить лог-файлы Docker.

1. Остановите Docker-демон:

```
service docker stop
```

2. Для Docker должны быть установлены следующие ограничения по файлам журналов: формат JSON, размер журнала до 10 МБ.

   Создайте конфигурационный файл **/etc/docker/daemon.json** со следующим содержимым:

```
{
    "data-root": "/opt/var/docker",
    "log-driver": "json-file",
    "log-opts": {
        "max-size": "10m",
        "max-file": "3"
    }
}
```

3. Рекомендуется перенести данные Docker в новую директорию `/opt/var/docker`, чтобы избежать проблем с работой ОС, если на выделенной точке монтирования закончится место.

   Скопируйте текущие данные Docker в новую директорию и переименуйте старую Docker-директорию:

```
cp -rp /var/lib/docker/* "/opt/var/docker"
mv /var/lib/docker /var/lib/docker.old
```

4. Перезапустите Docker-демон:

```
service docker start
```

5. Удалите старую Docker-директорию:

```
rm -rf /var/lib/docker.old
```

2.11. Установка ограничений по ресурсам и масштабирование сервисов

Все сервисы R-Vision UEBA подразделяются на четыре категории.

1. **Хранилища** могут разворачиваться в виде отдельного кластера для увеличения доступных ресурсов хранения и увеличения производительности:

   a. **ClickHouse** (clickhouse) — хранилище данных для инструментов анализа и обучения.

   b. **PostgreSQL** (postgres) — хранилище пользовательских конфигураций.

2. **Stateful** и **stateless-сервисы** не могут масштабироваться, доступно только ограничение по ресурсам:
    1. **Gateway** — фронт-прокси и балансировщик нагрузки внешнего TCP- и HTTP-трафика.
    2. **Balancer** - балансировщик нагрузки внутреннего TCP- и HTTP трафика
    3. **Backend** — обеспечивает доступ к функционалу сервисов по GraphQL API.
    4. **Correlation rules** - система обработки фильтров простых правил.
    5. **Jm** — сервис программных экспертов.
    6. **NATS** — брокер сообщений.
    7. **Notifier** — система обработки уведомлений пользователей.
    8. **Mailer** — интеграция с серверами электронной почты.
    9. **SOAR Integration** — интеграция с R-Vision SOAR.
    10. **Dkron** — планировщик задач и запросов.
    11. **Frontend** — сервис nginx для вывода статических страниц.
    12. **Change Log** — сервис для журналирования изменений в пользовательских данных и конфигурациях.
    13. **DGA Domain Checker** — подсервис программных экспертов.
    14. **Lookalike Domain Checker** — подсервис программных экспертов.
    15. **Analyst** — сервис управления лицензиями.
    16. **LDAP** — сервис синхронизации с Active Directory.
    17. **Migrate** — сервис миграции при обновлении.
3. Для **коннекторов** и **нормализаторов** доступно как ограничение по ресурсам, так и масштабирование.
    1. **vector** — основной обработчик всего потока событий.
4. Для **сервисов для сбора и отображения метрик и журналов логов элементов инсталляции** доступно только ограничение по ресурсам:

1. **Prometheus** — система мониторинга и хранения метрик в виде временных рядов.
2. **Warden** — система проверки состояния сервисов и поэкземплярного восстановления их работы, а также сбора метрик.
3. **Vector Container Logs** - система сбора логов контейнеров в единую таблицу в ClickHouse.
4. **Vector Raw Log Collector** - система сбора дампов входящих сообщений, отправленных на специальные порты.

NATS может запускаться в нескольких экземплярах как отдельные сервисы, основанные на одном и том же образе. Сформируйте из всех развернутых экземпляров отдельный кластер по инструкции. Используйте имена сервисов в качестве доменных имен. Сконфигурируйте массив имен экземпляров для всех сервисов, использующих NATS, чтобы в случае падения одного из экземпляров