F6

ПО «F6 Transaction Fraud Protection»

Инструкция по установке экземпляра ПО

Оглавление

Термины и сокращения

Заказчик	Лицо, использующее программное обеспечение на основании заключенного договора и эксплуатирующее его в своей инфраструктуре
Ноды (nodes)	(«Узлы») Физические или виртуальные машины, на которых в платформе Kubernetes разворачиваются и запускаются контейнеры с приложениями
Операция	Отдельное действие или событие в системе, связанное с выполнением бизнес-процесса или обработкой данных и подлежащее анализу и учету
ПО	Программное обеспечение «F6 Transaction Fraud Protection»
Пользователь	Лицо, взаимодействующее с цифровыми каналами обслуживания Заказчика, в отношении которого применяется антифрод-защита
Разработчик	АО «БУДУЩЕЕ»
СУБД	Система управления базами данных
Транзакция	Зафиксированное финансовое действие, приводящее к изменению денежных средств, финансовых активов или обязательств между субъектами и подлежащее учёту, контролю и подтверждению
API	(Application Programming Interface) Программный интерфейс, который позволяет разным системам обмениваться данными и взаимодействовать друг с другом по заранее определенным правилам
API Connector	Серверный модуль системы, предназначенный для интеграции backend-систем Заказчика с антифрод-платформой через API и обеспечения передачи транзакционных событий и получения результатов их обработки
On-premises	Модель развертывания программного обеспечения, при которой система устанавливается и эксплуатируется в собственной инфраструктуре Заказчика, без использования внешних облачных сервисов

#1 Общие сведения

1.1. Введение

Настоящий документ описывает процесс установки экземпляра программного обеспечения «F6 Transaction Fraud Protection» (далее — ПО, Transaction Fraud Protection).

1.2. Назначение ПО

«F6 Transaction Fraud Protection» — система, предназначенная для защиты пользователей и транзакций в момент их совершения. Она анализирует операции, оценивает риски, выявляет аномалии и маркирует подозрительные действия. Платформа автоматизирует расследования и обеспечивает полный цикл защиты в соответствии с требованиями регуляторов.

#2 Требования к системе

Для корректного функционирования ПО необходим веб-браузер.

ПО поддерживает работу на следующих версиях браузеров:

- Internet Explorer версии 8.0 и выше;
- Google Chrome версии 4.0 и выше;
- Mozilla Firefox версии 3.5 и выше;
- Apple Safari версии 4.0 и выше;
- Opera версии 10.5 и выше;
- iOS Safari версии 3.2 и выше;
- Opera Mobile версии 11.0 и выше;
- Google Chrome for Android версии 11.0 и выше;
- Mozilla Firefox for Android версии 26.0 и выше;
- Windows Internet Explorer Mobile версии 10.0 и выше;
- Яндекс Браузер версии 23.1.1 и выше.

В браузере устройства Заказчика должно быть разрешено исполнение скриптов JavaScript.

2.1. Технические требования к составу оборудования при размещении в инфраструктуре Заказчика

При размещении в инфраструктуре Заказчика требуется выделить следующие минимальные вычислительные мощности для установки системы в промышленную эксплуатацию:

- Серверы приложений (3 шт.):
  - CPU: 4 core, 2Mhz и выше;
  - RAM: 32 GB;
  - HDD: 200 GB;
  - ОС: Ubuntu, РЕД ОС.
- Серверы баз данных (3 шт.):
  - CPU: 4 core, 2Mhz и выше;
  - RAM: 32 GB;
  - HDD: 1 TB;
  - ОС: Ubuntu, РЕД ОС.

Требования для разворачивания предоставленной тестовой среды:

- Среда виртуализации: система управления контейнерами Kubernetes.

2.2. Требования к базам данных

ПО функционирует с использованием следующих СУБД:

- Apache Cassandra 4.0 и выше;
- Elasticsearch 7.0 и выше;
- ClickHouse 20.1 и выше.

#3 Компоненты ПО

Платформа предоставляется в виде On-premises-решения для развертывания в инфраструктуре Заказчика. Взаимодействие с системой осуществляется через API-интерфейс, а результаты обработки операций возвращаются с использованием различных технологий, включая MQ-очереди и API-ответы.

API Connector — это серверный модуль Transaction Fraud Protection, предназначенный для прямого подключения backend-систем Заказчика. Модуль интегрируется с внутренней архитектурой защищаемого сервиса и обеспечивает защиту транзакций, инициированных из различных каналов, включая веб-каналы, мобильные приложения и API.

ПО осуществляет сбор и анализ данных об операциях, поступающих из защищаемых систем Заказчика, и направляет их на обработку в аналитическую платформу Разработчика. При выявлении признаков мошенничества в транзакции (аномалии в реквизитах, подозрительные паттерны) система незамедлительно направляет Заказчику уведомление, на основании которого Заказчик может предпринять действия по блокировке операции либо провести дополнительную проверку.

Пример тестовой инсталляции со встроенными тестовыми модулями доступен по ссылке https://taf.fp.f6.security

#4 Установка тестовой версии ПО

4.1. Базовый вариант установки ПО в инфраструктуре Заказчика (On-premises)

Тестовая среда представляет собой сборку образов Docker-контейнеров с предустановленным системным и прикладным ПО.

Конфигурация оборудования должна соответствовать требованиям, описанным в разделе 2 «Требования к системе».

Пошаговая инструкция по установке ПО в инфраструктуре Заказчика:

1. Скачать тестовый образ ПО по ссылке: https://taf.fp.f6.security/demo.tar;
2. Установить следующие приложения из официальных репозиториев:
   - Kubernetes v1.24.x, доступен по ссылке:
     - https://github.com/kubernetes/kubernetes/tree/release-1.24;

     Для установки приложения используйте команду:

     ```
     sudo yum install -y kubelet-1.24.8-0 kubeadm-1.24.8-0 kubectl-1.24.8-0 --disableexcludes=kubernetes
     ```
   - Containerd, актуальный дистрибутив доступен по ссылке:
     - https://github.com/containerd/containerd/releases;
   - Calico, доступен по ссылке:
     - https://github.com/projectcalico/calico/releases/tag/v3.25.1;

     Для установки приложения используйте команду:

     ```
     curl https://raw.githubusercontent.com/projectcalico/calico/v3.25.1/manifests/calico.yaml -O
     ```
3. Установить FluxCD и выполнить bootstrap с репозиторием манифестов. Ссылки на инструменты:
   - https://fluxcd.io/flux/get-started/;
   - https://getbootstrap.com/docs/5.3/getting-started/download/.

   Для установки приложений используйте команду:

   ```
   curl -s https://fluxcd.io/install.sh | sudo bash
   https://getbootstrap.com/docs/4.5/getting-started/download/
   ```
4. На развернутые ноды необходимо прописать лейблы:

Роль	Параметр	Taint-конфигурация
Пользовательский интерфейс	`rabbit-admin=true` `bucket=sb-admin`	

Backend	`bucket=sb-main`
	`main-broker-sb-main=true`
	`sb-micro=true`
	`micro-sb-main=true`
	`zookeeper=true`	

	`ingress-host=true`
	`roles=back_ns`
	`fpm1=true`
	`vault=true`	

База данных Cassandra	`cassandra=true`	`PreferNoSchedule` `cassandra-only=true`
База данных Elasticsearch	`elastic=true`	`PreferNoSchedule` `elastic-only=true`
База данных ClickHouse	`clickhouse=true`	`PreferNoSchedule` `clickhouse-only=true`
Мониторинг	`monitoring=true`	

Пример команд:

```
kubectl label node nodename elastic=true
kubectl taint node nodename cassandra-only=true:PreferNoSchedule
kubectl taint node nodename elastic-only=true:PreferNoSchedule
```

5. После выполнения всех перечисленных выше действий система считается готовой к эксплуатации. В случае возникновения проблем следует обратиться по телефону +7 495 984-33-64 или по электронной почте fp-support@f6.ru.

#5 Поддержание функционирования ПО

Поддержание функционирования ПО заключается в контроле настроек, проведенных в рамках установки ПО. Иных регламентных мероприятий со стороны Заказчика ПО не требует.

При возникновении любых проблем или вопросов обратитесь к сотрудникам Разработчика:

- **Коровин Дмитрий Сергеевич, юрист**
  - **по электронной почте: d.korovin@f6.ru;**
  - **по номеру телефона: +7 915 067-08-90**