

Система обнаружения и предотвращения мошеннических транзакций «Smart Ftaud Detection»

ИНСТРУКЦИЯ ПО УСТАНОВКЕ

ВЕРСИЯ СИСТЕМЫ 3.5

МОСКВА, 2021

Оглавление

Оглавление	1
Введение	2
Назначение документа.....	2
Термины и сокращения	2
Технические требования к составу оборудования	4
Информация о БД	4
Установка ПО «Smart Fraud Detection»	5
Требования к версиям ПО	5
Дополнительные настройки ПО	5
Порядок действий	5
Возможные неисправности и методы их устранения	9
Приложение. Установка тестовой среды ПО «Smart Fraud Detection»	10

Введение

Назначение документа

Документ содержит порядок действий по установке системы для противодействия мошенничеству (Smart Fraud Detection).

Термины и сокращения

ТАБЛИЦА 1. ТЕРМИНЫ.

Термин	Описание
Advanced Adaptive Authentication	Приложение оценки рисков
Advanced Adaptive Authentication Policy	Приложение работы с правилами
Smart Fraud Detection, Система	Комплексная система обнаружения мошенничества в реальном времени методом анализа поступающих транзакций в различных каналах обслуживания клиентов
ExtendeRuleEngine	Приложение обработки транзакций
Банк-эквайер	Сторонняя кредитная организация, являющаяся участником платежной системы и осуществляющая эквайринг.
Банк-эмитент	Кредитная организация, выпустившая платежную карту
Белый список	Список заведомо добросовестных получателей платежа
ДБО	Дистанционное банковское обслуживание – общий термин для технологий предоставления банковских услуг на основании распоряжений, передаваемых клиентом удаленно (то есть без визита в банк), чаще всего с использованием компьютерных и телефонных сетей
Инцидент	Событие, отмеченное в системе как как подозрительное или мошенническое.
Карта	Пластиковая карта, привязанная к одному или нескольким расчётным/лицевым счетам в банке. Используется для оплаты товаров и услуг, в том числе через Интернет, а также снятия наличных.
Клиент	Потребитель услуг, предоставляемых финансовым институтом с помощью различных каналов обслуживания.
Мерчант	Организация торговли и сервиса, торгово-сервисная точка (ТСТ) – Юридическое лицо, либо индивидуальный предприниматель, принимающее банковские карты в качестве средства оплаты товаров (услуг) на основании Договора эквайринга, заключенного с Банком или уполномоченной организацией. Предприятие может иметь

Термин	Описание
	одну торгово-сервисную точку или сеть из двух и более торгово-сервисных точек.
Оценка риска, скоринг	Оценка действий Клиента в числовом выражении, определяющем насколько данная операция отличается от типовых операций Клиента. Значение рассчитывается Системой и является показателем вероятности мошеннических действий в отношении Клиента. Методика расчета является конфиденциальной информацией.
Платежная транзакция	Инициированное клиентом событие, приводящее к финансовой операции (переводы, платежи, погашение кредита и пр.).
Подразделение	Структурное подразделение финансового института, предоставляющее услуги
Сессия	Цикл операций обмена данными, непрерывно выполняющийся от источников запросов к конечным объектам и имеющий некий обобщающий признак (идентификатор) и конечный результат.
Событие (транзакция)	Инициированное клиентом действие, по выполнению платежной или не платежной операции в любых каналах обслуживания.
Сессионная транзакция	Инициированное клиентом событие, не приводящее к финансовым операциям (вход в систему, изменение настроек профиля, получение выписок, смена пароля и пр.).
Сессионные данные	Данные передаваемые в рамках одной сессии.
Чёрный список	Список, содержащий реквизиты мошенников. Разные типы списков отличаются по назначению и структуре реквизитов

Таблица 2. Сокращения

Сокращение	Расшифровка
AAA	Advanced Adaptive Authentication
AAA_Policy	Policy
AAA_Scheduler	Scheduler
DBSave	Database Save
SFD	Smart Ftaud Detection
ДБО	Дистанционное банковское обслуживание
БД	База данных

Технические требования к составу оборудования

Минимальные требования для установки системы в промышленную эксплуатацию:

Сервер приложений:

CPU : 4 core 2Mhz+

RAM: 32 Gb

HDD : 200Gb

OC : Debian, Redhat, CentOS, Alt Linux, Astra Linux

База данных:

CPU : 4 core 2Mhz+

RAM: 8 Gb

HDD : 1Tb

OC : Debian, Redhat, CentOS, Alt Linux, Astra Linux

Требования для разворачивания предоставленной тестовой среды:

Среда виртуализации: VmWare Workstation, VmWare Player, VmWare Fusion, VmWare ESX.

CPU : 2 core 2Mhz+

RAM: 16 Gb

HDD : 22Gb

Информация о БД

Система Smart Fraud Detection может работать с одной из следующих СУБД:

- apache cassandra 3.11
- Oracle Database 11g2 и новее
- PostgreSQL 12 и новее

Тестовый образ системы, предоставленный по ссылке https://www.fzlabs.ru/wp-content/uploads/SmartFraudDetection3_5.zip работает с СУБД PostgreSQL 13.

Установка ПО «Smart Fraud Detection»

Требования к версиям ПО

№	Наименование	Версия
1	Java Environment	jdk1.8.0_144
2	Apache Cassandra Database	apache-cassandra-3.11.0
3	PostgreSQL Database	PostgreSQL 12+

Дополнительные настройки ПО

№	ПО	Файл настроек	Начальная настройка	Изменённая настройка
1	Apache Cassandra	/opt/apache-cassandra-3.11.0/conf/cassandra.yaml	read_request_timeout_in_ms: 5000	read_request_timeout_in_ms: 10000
2	Apache Cassandra	/opt/apache-cassandra-3.11.0/conf/cassandra.yaml	write_request_timeout_in_ms: 2000	write_request_timeout_in_ms: 60000
3	PostgreSQL	postgresql.conf	-	max_connections = 10000
4	Linux max open files	/etc/security/limits.conf	-	sfd soft nofile 1000000 sfd hard nofile 1000000
5	Linux pending signals count	/etc/security/limits.conf	-	sfd soft sigpending 96289 sfd hard sigpending 96289

Порядок действий

№	Действия	Сделано
---	----------	---------

1	Скопировать папки admin app db-deploy profile tmp из папки поставки в /opt/sfd/	
	Работы на БД	
2	Выполнить скрипты из папки db-deploy	
2.1	Необходимо перейти в папку со скриптами ~/db-deploy	
2.2	Заполнить параметры в конфигурационном файле config.properties в соответствии с комментариями	
2.3	Запустить скрипт по развёртыванию БД: bash install.sh	
3	Работы на серверах приложений	
4	Настройка конфигурационных файлов в папке profile/config/	
4.1	<p>Файл env.conf задать параметры в соответствии с комментариями:</p> <p>JAVA_HOME (при установке openjdk директорию в которой установлена java можно определить командой update-alternatives --display java. Пример: /usr/lib/jvm/java-1.8.0-openjdk-1.8.0.292.b10-1.el7_9.x86_64)</p> <p>AdvancedAA_HOSTLIST</p> <p>AdvancedAA_DBSave_HOSTLIST</p> <p>AdvancedAA_Scheduler_HOSTLIST</p> <p>AdvancedAA_Policy_HOSTLIST</p> <p>AdvancedAA_Policy_Calculation_HOSTLIST</p> <p>AdvancedAA_Policy_Dynamic_HOSTLIST</p> <p>ExtendedRuleEngineAsync_HOSTLIST</p> <p>AFD_DATA_ANALYZER_HOSTLIST</p> <p>AFD_UI_HOSTLIST</p>	

4.2	<p>Файлы ignite-data-analyzer.xml – конфиг Ignite кластера приложения AFD_DATA_ANALYZER</p> <p>В теге <code><property name="addresses"></code> в list необходимо перечислить все хосты входящие в кластер приложения . Пример:</p> <pre><property name="addresses"> <list> <value>hostname1:48500</value> <value>hostname2:48500</value> </list> </property></pre> <p>Указываемый порт для каждого конфига уже есть в примере по умолчанию в конфиге.</p> <p>Так же его можно взять в части:</p> <pre><bean class="org.apache.ignite.spi.discovery.tcp.TcpDiscoverySpi"> <property name="localPort" value="48500"/></pre>	
4.3	<p>В файле afd_config.properties(конфиг приложения AAA) необходимо заполнить параметры:</p> <ul style="list-style-type: none"> • <code>aaa.ignite.nodeList</code> - список серверов входящие в кластер Ignite приложения AAA • <code>cache.profile.backups</code> - Количество бекапов профилей, которые хранятся в распределённых кешах \leq количество серверов кластера Ignite – 1 • <code>cache.profile.def.maxSize</code> - максимальный размер памяти доступной для кэша в байтах и в конце добавить L; • <code>afd.aaap.tcp.hosts</code> – хосты где установлено приложение AAAP для отправки в него запросов. 	
4.4	<p>В файле afd_eea_config.properties(конфиг приложения ЕЕА) необходимо заполнить параметры:</p> <ul style="list-style-type: none"> • <code>afd.dictionary.ignite.nodeList</code> - список серверов входящие в кластер Ignite приложения ЕЕА • <code>afd.tcp.hosts</code> – хосты где установлено приложение ААА для отправки в него запросов 	
4.5	<p>В файле afd_aaap_config.properties(конфиг приложения AAAP) необходимо заполнить параметры:</p> <ul style="list-style-type: none"> • <code>aaap.ignite.nodeList</code> – список серверов входящие в кластер Ignite AAAP • <code>aaap.list.distributed.numBackups</code> - Количество бекапов элементов списков, которые хранятся в распределённых кешах \leq количество серверов кластера Ignite – 1 	

4.6	<p>В файле afd_aaap_calculation.properties (конфигурационный файл приложения AAAPC) заполнить параметры:</p> <ul style="list-style-type: none"> • <code>afd.ignite.maxMemoryBytes</code> – максимальный размер памяти на данном сервере который может использовать Ignite кластер данного приложения • <code>aaap.ignite.nodeList</code> – список серверов входящие в кластер Ignite AAAPC • <code>aaap.list.distributed.numBackups</code> - Количество бекапов элементов списков, которые хранятся в распределённых кешах \leq количество серверов кластера Ignite – 1 • <code>aaap.calculation.history.numBackups</code> - Количество бекапов исторических данных, которые хранятся в распределённых кешах \leq количество серверов кластера Ignite – 1. 	
4.7	<p>В файле afd_aaap_dynamic.properties (конфигурационный файл приложения AAAPD) заполнить параметры:</p> <ul style="list-style-type: none"> • <code>afd.ignite.maxMemoryBytes</code> – максимальный размер памяти на данном сервере который может использовать Ignite кластер данного приложения • <code>aaap.dynamic.ignite.nodeList</code> – список серверов входящие в кластер Ignite AAAPD • <code>aaap.dynamic.list.distributed.numBackups</code> - Количество бекапов элементов списков, которые хранятся в распределённых кешах \leq количество серверов кластера Ignite – 1 • <code>aaap.dynamic.elements.numBackups</code> - Количество бекапов исторических данных, которые хранятся в распределённых кешах \leq количество серверов кластера Ignite – 1. 	
4.8	<p>В файле afd_scheduler.properties (конфигурационный файл приложения Scheduler) необходимо заполнить параметры:</p> <ul style="list-style-type: none"> • <code>scheduler.master.host</code> – хостнейм мастер ноды приложение Scheduler; • <code>scheduler.ignite.nodeList</code> - список серверов входящие в кластер Ignite Scheduler. • <code>scheduler.resolution.aaap.client.hosts</code> – если приложения Scheduler и AAAP стоят на разных серверах, то тут необходимо перечислить все сервера AAAP, как указано в комментарии 	
4.9	<p>В файле dbconnection.properties необходимо прописать настройки соединения к мастер БД:</p> <pre>jdbc.url= jdbc:postgresql://{server_db_hostname}/sfd} jdbc.username={db_login} jdbc.password={db_password}</pre>	
5	Дополнительные действия	
5.1	<p>Создать ключ для управления через ssh:</p> <pre>ssh-keygen -f /opt/sfd/profile/config/mgmt.key -q -N ""</pre>	

5.2	Прописать во все сервера публичную часть ключа: cat /opt/sfd/profile/config/mgmt.key.pub >> /opt/sfd/.ssh/authorized_keys	
-----	--	--

Возможные неисправности и методы их устранения

В случае проблем со входом в Web-интерфейс следует проверить следующее:

1. Виртуальная машина получила IP адрес:

- После полной загрузки системы необходимо ввести данные пользователя и пароль на Операционную систему: user/sfdrootXCB
- Выполнить команду: **sudo ifconfig -a**:

```
user@sfd-3-5-demo:~$ sudo ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.16.23.143 netmask 255.255.255.0 broadcast 172.16.23.255
    inet6 fe80::20c:29ff:fe5b:15e5 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:fb:15:e5 txqueuelen 1000 (Ethernet)
    RX packets 62 bytes 6142 (5.9 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 21 bytes 2167 (2.1 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

user@sfd-3-5-demo:~$ _
```

- Проверить правильность выданного адреса, в случае если адрес не выдан или сетевой интерфейс в состоянии “DOWN” устранить проблему самостоятельно или обратиться в поддержку компании «Фаззи Лоджик Лабс» для получения консультации.

2. Запуск базы данных Postgres:

- После запуска виртуальной машины, выполнить под root команду «**sudo systemctl status postgresql-13**», в результате выполнения команды среди строк статуса должна содержаться строка:

Active: active (running)

- В случае если статус другой проанализировать лог файлы в:

/var/lib/pgsql/13/data/log/postgresql-.log*

На наличие ошибок

3. В случае, если при старте одно из приложений сообщит об ошибке, необходимо проанализировать логи:

/opt/sfd/profile/log/afd-front.log

/opt/sfd/profile/log/afd-eea.log

/opt/sfd/profile/log/afd-aaap.log

/opt/sfd/profile/log/afd-aaap-calculation.log

/opt/sfd/profile/log/afd-aaap-dynamic.log

/opt/sfd/profile/log/afd-data-analyzer.log

/opt/sfd/profile/log/afd-ui.log

/opt/sfd/profile/log/afd-scheduler.log

/opt/sfd/profile/log/afd-db-save.log

Либо прислать их на анализ в поддержку компании «Фаззи Лоджик Лабс».

Приложение. Установка тестовой среды ПО «Smart Fraud Detection»

Тестовая среда представляет собой виртуальную машину VmWare с предустановленным системным и прикладным ПО. Использование предоставленной виртуальной машины возможно в средах виртуализации VmWare Workstation, VmWare Player, VmWare Fusion, VmWare ESX.

Ссылка для скачивания образа: https://www.fzlabs.ru/wp-content/uploads/SmartFraudDetection3_5.zip.

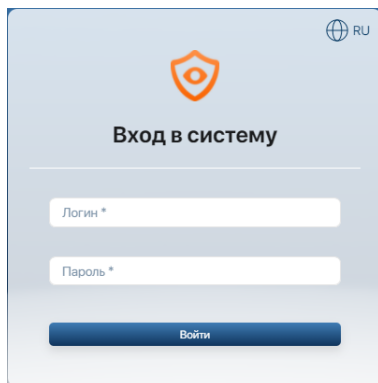
Для установки необходимо выполнить следующие действия:

1. Скопировать предоставленный архив SmartFraudDetection3_5.zip на сервер или рабочую станцию, где размещена среда виртуализации и разархивировать штатными средствами. Необходимое дисковое пространство составляет 22Гб и оперативной памяти не менее 16Гб.
2. Открыть основной файл для импорта виртуальной машины SFD_3.5.vmx непосредственно из среды виртуализации (меню File-Open). Виртуальная машина Smart Fraud Detection появится в списке существующих виртуальных машин с идентификатором «SFD_3.5».

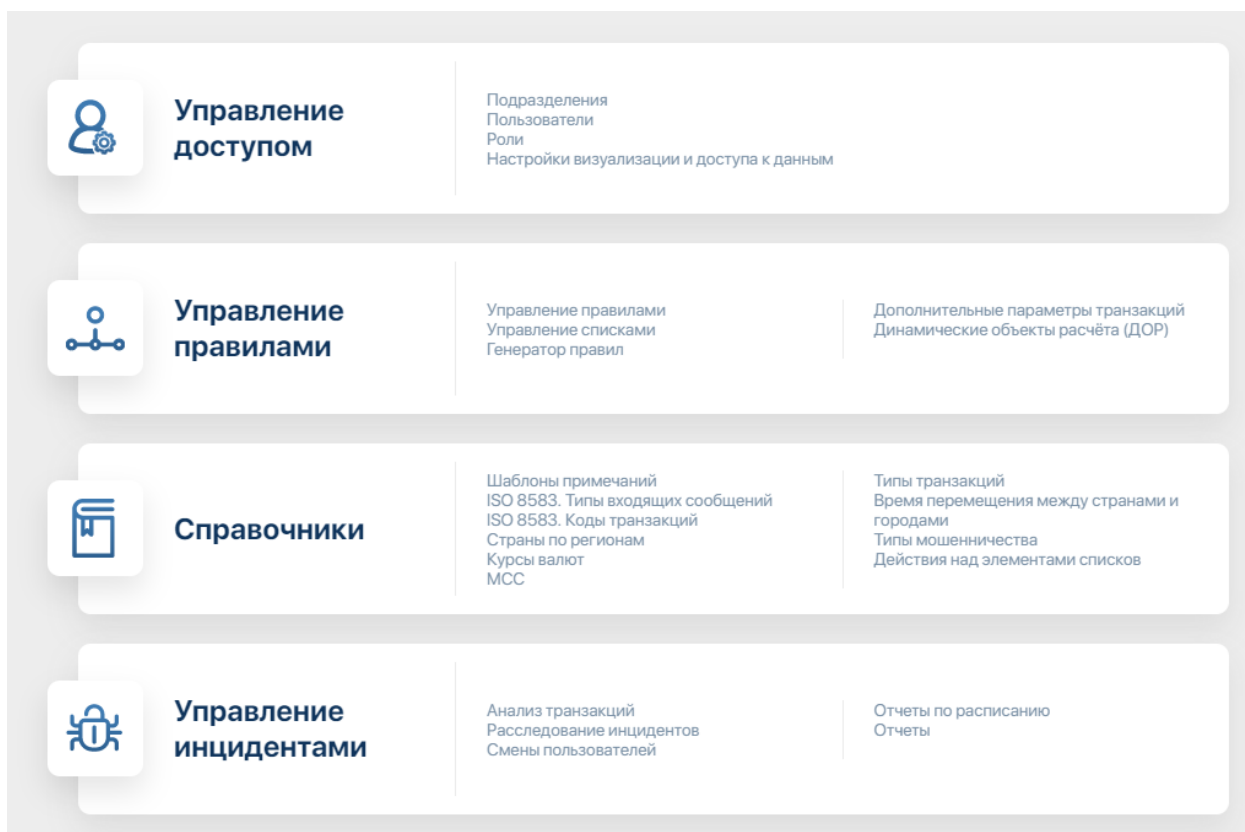
3. Запустить виртуальную машину в среде виртуализации. Для этого в меню виртуальной машины выбрать опцию «RUN». В появившемся диалоговом окне «Where did you get this machine?» выбрать «I move it».
4. Запустить само приложение, подключившись к виртуальной машине по протоколу SSH либо через консоль виртуализации под пользователем sfd с паролем XCBSfd!!
5. Выполнить команду: «**/opt/sfd/admin/send_all.sh start**» в подключённой консоли и дождаться окончания выполнения скрипта.

В результате выполнения процедуры установки по ссылке *http://<ip адрес, полученный виртуальной машиной>:18080* станет доступен интерфейс системы Smart Fraud Detection

Для входа в интерфейс модуля необходимо ввести логин\пароль: *admin\admin123!*

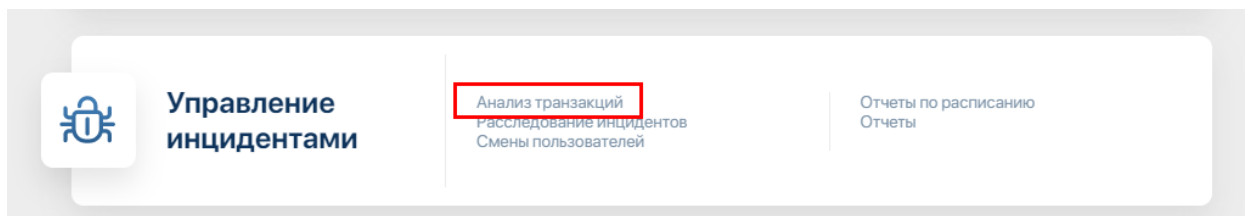


После успешной аутентификации предоставляется полный доступ к интерфейсу системы SFD:



В системе есть несколько загруженных тестовых событий.

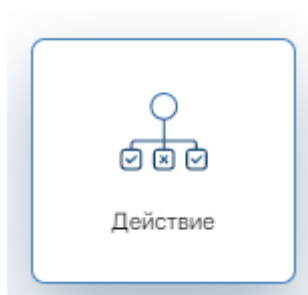
Их можно посмотреть перейдя в анализ транзакций:



Далее выбрать «поиск транзакций»



И выбрать действие



Выставить следующие даты и действия

Данные за период

С 30.08.2021 00:01 По 31.08.2021 00:00

Обязательные параметры

Действие Антифрод *

☒ ALLOW ☒ DENY ☒ REVIEW

И нажать кнопку «Применить»

Отобразятся следующие транзакции:

Дата и время транзакции	ID транзакции	ID клиента	Описание т
30.08.2021 13:43:52	e29fbf8fb8e44f9c958a20b...	00002030	Привязка м
30.08.2021 13:44:25	64d860a5243d4f05af21f9f...	00002030	Перевод с
30.08.2021 13:45:12	30f13a26a0204cfeb1e7cc6...	00002030	Перевод с
30.08.2021 13:45:53	395bd1eefcda4ea9b24e66...	00002030	Перевод с
30.08.2021 13:46:24	f9909cb627c14c8f8c448b...	00002030	Перевод с

Попасть в каждую из них можно двойным нажатием курсора по ним