|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |

**Сервисная интеграционная шина** «Аметум ESB»

**Руководство администратора**

листов 61

Москва, 2023

**СОДЕРЖАНИЕ**

[1. ВВЕДЕНИЕ 5](#_Toc153651357)

[1.1. Полное наименование Интеграционной шины и ее обозначение 5](#_Toc153651358)

[1.1.1. Полное наименование Интеграционной шины 5](#_Toc153651359)

[1.1.2. Условное обозначение Интеграционной шины 5](#_Toc153651360)

[1.2. Область применения Интеграционной шины 5](#_Toc153651361)

[1.3. Краткое описание возможностей Интеграционной шины 5](#_Toc153651362)

[1.4. Уровень подготовки обслуживающего персонала Интеграционной шины 6](#_Toc153651363)

[1.5. Перечень эксплуатационной документации, с которой необходимо ознакомиться обслуживающему персоналу Интеграционной шины 6](#_Toc153651364)

[2. НАЗНАЧЕНИЕ И УСЛОВИЯ ПРИМЕНЕНИЯ 7](#_Toc153651365)

[3. ПОДГОТОВКА К РАБОТЕ 8](#_Toc153651366)

[3.1. Состав и содержание носителя данных, содержащего запускаемые программы и данные 8](#_Toc153651367)

[3.2. Требования к ресурсам и программному обеспечению 9](#_Toc153651368)

[3.2.1. Требования к ресурсам и программному обеспечению прокси-сервера 9](#_Toc153651369)

[3.2.2. Требования к ресурсам и программному обеспечению сервера баз данных 9](#_Toc153651370)

[3.2.3. Требования к ресурсам и программному обеспечению сервера приложения 10](#_Toc153651371)

[3.2.4. Требования к ресурсам и программному обеспечению сервера для обслуживания очереди сообщений 10](#_Toc153651372)

[3.3. Порядок загрузки программ и данных 10](#_Toc153651373)

[3.4. Порядок проверки работоспособности 10](#_Toc153651374)

[4. ОПИСАНИЕ ОПЕРАЦИЙ 12](#_Toc153651375)

[4.1. Первоначальная установка и настройка Интеграционной шины 12](#_Toc153651376)

[4.1.1. Установка серверной части 12](#_Toc153651377)

[4.1.2. Установка клиентского рабочего места 21](#_Toc153651378)

[4.1.3. Определение пути доступа по сети к серверу 22](#_Toc153651379)

[4.1.4. Установка программного обеспечения клиентского рабочего места 22](#_Toc153651380)

[4.1.5. Загрузка необходимых компонентов системы 22](#_Toc153651381)

[4.1.6. Проверка функционирования программно-технического комплекса 22](#_Toc153651382)

[4.1.7. Настройка серверной части 23](#_Toc153651383)

[4.1.8. Настройка клиентской части 44](#_Toc153651384)

[4.2. Проверка работоспособности сервисов Интеграционной шины 44](#_Toc153651385)

[4.3. Функции администрирования при эксплуатации системы 47](#_Toc153651386)

[4.3.1. Управление правами доступа 48](#_Toc153651387)

[4.3.2. Управление прикладными системами, взаимодействующими между собой и с системами ФОИВ посредством Интеграционной шины 51](#_Toc153651388)

[4.3.3. Введение перечня ФОИВ и информационных систем 54](#_Toc153651389)

[4.3.4. Протоколирование действий пользователей 56](#_Toc153651390)

[4.3.5. Мониторинг работоспособности сервисов Интеграционной шины 57](#_Toc153651391)

[4.3.6. Работа с сервером приложений Tomcat 57](#_Toc153651392)

[5. АВАРИЙНЫЕ СИТУАЦИИ 60](#_Toc153651393)

**ПЕРЕЧЕНЬ СОКРАЩЕНИЙ**

|  |  |
| --- | --- |
| **Термин (сокращение)** | **Определение** |
| БД | База данных |
| Интеграционная шина | Сервисная интеграционная шина «Аметум ESB» (Enterprise Service Bus) |
| ОС Линукс | Операционная система AstraLinux СE версии 2.12 и выше |
| Разработчик, ЦИТ | Общество с ограниченной ответственностью «Центр Информационных Технологий» |
| СМЭВ | Система межведомственного электронного взаимодействия |
| ФОИВ | Федеральный орган исполнительной власти |
| ЭС | Электронное сообщение |
| HTTP | (от англ. «HyperText Transfer Protocol») – протокол передачи гипертекста |

# ВВЕДЕНИЕ

## Полное наименование Интеграционной шины и ее обозначение

### Полное наименование Интеграционной шины

Сервисная интеграционная шина Аметум ESB

### Условное обозначение Интеграционной шины

Ametum ESB.

## Область применения Интеграционной шины

Интеграционная шина предназначена для обеспечения взаимодействия прикладных систем между собой, а также с информационными системами федеральных органов исполнительной власти (ФОИВ) без создания каждый раз новой инфраструктуры взаимодействия.

Взаимодействие пользователей с Интеграционной шиной осуществляется посредством пользовательского интерфейса Модуля мониторинга Интеграционной шины.

## Краткое описание возможностей Интеграционной шины

Интеграционная шина предоставляет следующие возможности:

создание транспортной инфраструктуры как совокупности узлов с произвольной топологией и возможностью маршрутизации информационного взаимодействия;

1) унификация информационного взаимодействия между прикладными информационными системами на основе единых правил для всех участников (синхронного и асинхронного на основе протоколов MQ и HTTP);

2) трансформация данных в потоковом и пакетном режиме;

3) создание адаптеров к информационным системам, не имеющим возможности подключиться по единым правилам взаимодействия;

4) создание шлюзов в другие интеграционные шины

5) интеграция транспортной инфраструктуры со СМЭВ

Интеграционная шина, обеспечивая информационное взаимодействие между прикладными системами, а также с системами ФОИВ, осуществляет:

1. получение запроса от любой прикладной системы и передачу его в другую прикладную систему или в ФОИВ в синхронном режиме;
2. получение ответа на ранее направленный запрос и передачу ответа в любую прикладную систему организации в синхронном режиме.
3. получение запроса от любой прикладной системы и передачу в другую прикладную систему или в ФОИВ в асинхронном режиме;
4. получение ответа на ранее направленный запрос и передачу ответа в любую прикладную систему в асинхронном режиме;
5. получение запроса от ФОИВ и передачу его в любую прикладную систему в синхронном режиме;
6. получение ответа от любой прикладной системы на ранее направленный запрос и передачу ответа в ФОИВ в синхронном режиме;
7. получение запроса от ФОИВ и передачу его в любую прикладную систему в асинхронном режиме;
8. получение ответа от любой прикладной системы организации на ранее направленный запрос и передачу ответа в ФОИВ в асинхронном режиме;
9. журналирование (логирование) всех выполняемых операций.

## Уровень подготовки обслуживающего персонала Интеграционной шины

Квалификация обслуживающего персонала Интеграционной шины должна быть достаточной для:

администрирования общесистемного ПО: Astra Linux 2.12 и выше

сервера приложений: Apache Tomcat 7.0 или выше (из состава дистрибутива Astra Linux);

СУБД: PostgreSQL 10.6 или выше (из состава дистрибутива Astra Linux);

прокси-сервера (при необходимости): HAProxy 1.8 или выше;

1. проведения резервного копирования и восстановления данных;
2. сопровождения специального программного и информационного обеспечения Интеграционной шины;
3. проведения технического обслуживания комплекса технических средств Интеграционной шины.

## Перечень эксплуатационной документации, с которой необходимо ознакомиться обслуживающему персоналу Интеграционной шины

Перед началом эксплуатации Интеграционной шины обслуживающему персоналу Интеграционной шины необходимо ознакомиться с настоящим документом, а также с документом «Руководство пользователя».

# НАЗНАЧЕНИЕ И УСЛОВИЯ ПРИМЕНЕНИЯ

Интеграционная шина предназначен для обеспечения унифицированного взаимодействия прикладных систем между собой, а также с информационными системами ФОИВ без создания каждый раз новой инфраструктуры взаимодействия.

Для мониторинга и контроля взаимодействия прикладных систем между собой, а также с системами ФОИВ используется Модуль мониторинга Интеграционной шины.

Для обеспечения взаимодействия с Интеграционной шиной со стороны прикладных систем должны быть разработаны и внедрены сервисы синхронной либо асинхронной отправки и получения данных.

# ПОДГОТОВКА К РАБОТЕ

## Состав и содержание носителя данных, содержащего запускаемые программы и данные

Дистрибутив распространяется в виде набора файлов и папок. Содержание дистрибутива имеет следующую структуру:

/src

/dist

/lib

/scripts

/conf

/log\_confs.

Таблица 1. Состав файлов дистрибутива Интеграционной шины

| Наименование | Описание |
| --- | --- |
| /src | исходные коды |
| /dist | war-файлы:   1. пользовательские инструменты:  * admin.war; * operator.war;  1. внутренние сервисы:  * interaction.war; * sender.war; * router.war; * mq-Interaction.war; * mq-Sender.war;  1. внешние сервисы:  * smev3-receiver.war; * smev3-sender.war; * smev3-requester.war |
| /lib | библиотеки и компоненты Интеграционной шины |
| /scripts | скрипты для автоматической очистки устаревших данных |

Примеры конфигурационных файлов размещены в папке conf. Конфигурационные файлы для настройки логирования размещены в папке /log\_confs.

* 1. **Требования к ресурсам и программному обеспечению**
     1. **Требования к ресурсам и программному обеспечению прокси-сервера**

1. Необходимое ПО: ОС Линукс.
2. Требования к аппаратному обеспечению для продуктивного контура:

CPU 2 ядра,

2 Gb RAM,

60 Gb HDD.

* + 1. **Требования к ресурсам и программному обеспечению сервера баз данных**

1. Интеграционная шина должна использоваться СУБД, отвечающая требованиям импортозамещения и функционирующая на базе программного обеспечения «с открытым кодом».
2. Необходимое ПО: ОС Линукс, PostgreSQL 10.6.
3. Требования к аппаратному обеспечению:

для продуктивного контура:

* узел Master кластера основной базы данных: для основного сервера – CPU 4 ядра, 8 Gb RAM, 400 Gb HDD (разделение на логические диски – 100 Gb – под системный раздел, 300 Gb – под размещение базы данных);
* узел Slave кластера основной базы данных: для вспомогательного сервера – CPU 4 ядра, 8 Gb RAM, 350 Gb HDD (разделение на логические диски – 50 Gb – под системный раздел, 300 Gb – под размещение базы данных);
* для тестового контура:
* сервер базы данных: CPU 2 ядра, 4 Gb RAM, 250 Gb HDD (разделение на логические диски – 50 Gb – под системный раздел, 100 Gb – под размещение базы данных).
  + 1. **Требования к ресурсам и программному обеспечению сервера приложения**

1. Требования к программному обеспечению:

ОС Линукс,

JDK 8 update 191,

Apache Tomcat 7.0.54.

1. Требования к аппаратному обеспечению для тестового и продуктивного контура:

CPU 2 ядра,

4 Gb RAM,

60 Gb HDD.

* + 1. **Требования к ресурсам и программному обеспечению сервера для обслуживания очереди сообщений**

Для работы c Интеграционной шиной нет необходимости в установке дополнительного ПО на рабочие места пользователей. Минимальным требованием является 32- или 64-разрядная ОС не ниже Windows 7.

## Порядок загрузки программ и данных

Для запуска Интеграционной шины требуется выполнить ввод в адресной строке запущенного web-браузера адреса сервера приложений.

## Порядок проверки работоспособности

После установки и настройки компонентов Интеграционной шины должны быть доступны web-интерфейсы Модуля мониторинга и Модуля администрирования Интеграционной шины. Для запуска Интеграционной шины требуется выполнить ввод в адресной строке запущенного web-браузера адреса модуля Интеграционной шины. Система работоспособна, если в результате действий пользователя, на экране монитора отобразилась форма авторизации в клиентском приложении без выдачи пользователю сообщений о сбое в работе.

# ОПИСАНИЕ ОПЕРАЦИЙ

## Первоначальная установка и настройка Интеграционной шины

### Установка серверной части

#### **Подготовка ОС Линукс**

Действия выполняются на обоих узлах.

Необходимо проверить наличие настроек для использования DNS серверов.

Рекомендуется в файле /etc/hosts прописать имена серверов кластера Postgres.

ntpq -p

На обоих узлах проверить, что в качестве локали установлена UTF8 (файл /etc/locale.conf)

База данных прикладной системы под управлением СУБД PostgreSQL должна содержаться в отдельном созданном каталоге:

**Директории с БД и backup должны располагаться на отдельных смонтированной файловых системах:**

VG – vg\_pgdata

LV – lvpgdata точка монтирования /pgdata/ файловой системы ext4

/pgdata/

VG – vg\_pgbackup

LV – lvpgbackup точка монтирования /pgdata/backups файловой системы ext4

Файлы данных БД PostgreSQL разместить в дочерней директории каталога:

/pgdata/data/ - для данных БД

/pgdata/tmp/ **-** директория хранения lock-файлов кластера БД

/pgdata/backup/ – директория для хранения backup файлов БД

#### **Установка JDK**

Действия необходимо выполнять на серверах приложений.

Скопировать дистрибутив JDK и Tomcat из каталога lib, поставляемой с настоящей инструкцией в каталог /opt:

jdk-8u191-linux-x64.rpm

apache-tomcat-7.0.54.tar.gz

apr-1.6.5.tar.gz

1. Перейти в каталог /opt и выполнить установку rpm пакета

cd /opt

rpm -ivh jdk-8u191-linux-x64.rpm

1. Сконфигурировать установленную Java как версию по умолчанию. Для выбора только что установленной версии в появившемся списке необходимо выбрать 2.

alternatives --install /usr/bin/java java /usr/java/jdk1.8.0\_191-amd64/bin/java 2

alternatives --config java

1. Проверить, что установилась нужная версия java:

java -version

javac -version

1. Установить переменную среды JAVA\_HOME в файле /etc/profile.d/java.sh:

export JAVA\_HOME=/usr/java/latest

1. Выполнить команду для изменения прав доступа к скрипту:

chmod +x /etc/profile.d/java.sh

#### **Установка СУБД PostgreSQL**

Установку PostgreSQL необходимо выполнять из централизованного распределенного репозитория для операционных систем Линукс и RHEL (описание репозитория доступно по ссылке http://link.rzd/2495)

Требуется подключить репозиторий PostgreSQL-10

Добавить файл pgsql.repo в директорию /etc/yum.repos.d

Вписать в файл:

[pg]

name=pg

baseurl=http://rzd-repo-02.rzd/pulp/repos/Default\_Organization/Library/custom/PostgreSQL\_10/rhel-7Server-x86\_64\_/

gpgcheck=0

enable=1

1. Postgresql10, postgresql10-server, postgresql10-contrib, postgresql10-libs на обоих узлах, предназначенных для СУБД.

yum install postgresql10 postgresql10-server postgresql10-contrib postgresql10-libs

1. Выполнить смену пароля пользователю postgres на обоих узлах:

passwd postgres

1. Необходимо дать права на созданную директорию для пользователя postgres на обоих узлах:

chown -R postgres:postgres /pgdata

chmod -R 700 /pgdata

1. Необходимо перенастроить файлы на обоих узлах:

/var/lib/pgsql/.bash\_profile :

Заменить значение PGDATA=/pgdata/data

/usr/lib/systemd/system/postgresql-10.service

Заменить значение Environment=PGDATA=/pgdata/data/

1. Выполнить инициализацию БД на master

/usr/pgsql-10/bin/postgresql-10-setup initdb

После данной операции файлы BD развернутся в ранее созданных директориях.

1. Получить полномочия пользователя postgres на master:

su - postgres

1. Настроить основной конфигурационный файл БД. Ниже приведен пример настроек конфигурационных файлов СУБД PostgreSQL:

/pgdata/data/postgresql.conf

Shared\_buffers = 128MB (зависит от требований разработчика)

listen\_addresses = '\*'

port = 5432

wal\_level = hot\_standby (настройка необходимая при использовании кластера).

max\_wal\_senders = 3 (максимальное количество подключений от резервных серверов или клиентов потокового резервного копирования).

max\_replication\_slots = 3 (Задаёт максимальное число слотов репликации, которое сможет поддерживать сервер. Значение по умолчанию — ноль).

hot\_standby = on (Определяет, можете ли Вы подключиться для выполнения запросов к серверу во время восстановления).

1. Настроить файл доступа к БД /pgdata/data/pg\_hba.conf отталкиваясь от примера:

Разрешить локальные подключения всем пользователям ко всем базам

local" is for Unix domain socket connections only

local all all peer

# IPv4 local connections:

host all all x.x.x.x/24 md5

# Allow replication connections from localhost, by a user with the

# replication privilege.

host replication replica node1/32 md5

host replication replica node2/32 md5

1. Выйти из под пользователя postgres и запустить PostgreSQL на master.

systemctl start postgresql-10.service

1. Снова получить полномочия postgres

su – postgres

1. Создать пользователя репликации и слот репликации.

psql -U postgres -c "create user replica with replication encrypted password 'pass'"

где 'pass'" меняем на пароль для пользователя репликации.

/usr/pgsql-10/bin/psql -U postgres -c "SELECT pg\_create\_physical\_replication\_slot('standby\_slot') "

1. Необходимо выполнить копирование БД и настроек на slave-сервер от пользователя postgres:

su - postgres

pg\_basebackup -h pg1 -U replica -D /pgdata/data -X s

где pg1 – имя master хоста

1. Выйти из-под пользователя postgres и выключить PostgreSQL на master.

#### **Установка и настройка кластера БД в режиме master-slave**

В случае логической порчи данных в БД потребуется восстановление из резервной копии.

1. Необходимо выполнить установку кластерного ПО на всех нодах кластера:

yum install pcs

1. Сменить пароль пользователю hacluster на всех нодах кластера (пользователь создается в системе автоматически)

passwd hacluster

**PostgreSQL**

Заменить файл /usr/lib/ocf/resource.d/heardbeat/pgsql на предоставленный организацией. Выполнить на обеих нодах.

В файле /usr/lib/ocf/resource.d/heardbeat/pgsql требуется заменить значение в файле pgsql:

OCF\_RESKEY\_tmpdir\_default="/pgdata/tmp"

1. Стартовать и активировать сервисы кластера на всех нодах кластера

systemctl start pcsd.service; systemctl is-active pcsd.service; systemctl enable pcsd.service; systemctl is-enabled pcsd.service

1. C одного из узлов выполнить первоначальную авторизацию кластерного ПО

pcs cluster auth pg1 pg2

Имена хостов указываются те, которые прописаны в DNS или /etc/hosts

1. C одного из узлов серверов БД выполнить первоначальную конфигурацию кластерного ПО

pcs cluster setup --start --name cluster\_name pg1 pg2

1. Выполнить настройку ресурсов кластера согласно данных настроек на одной из нод:

pcs property set no-quorum-policy="ignore"

pcs property set stonith-enabled="false"

pcs resource defaults resource-stickiness="1000"

pcs resource defaults migration-threshold="3"

pcs resource create vip-master IPaddr2 \

ip="x.x.x.x"\ ## Виртуальный кластерный IP

nic="ens160"\

cidr\_netmask="xx"\ ## пример 24

op start timeout="60s" interval="0s" on-fail="restart"\

op monitor timeout="60s" interval="10s" on-fail="restart"\

op stop timeout="60s" interval="0s" on-fail="block"

pcs resource create pgsql pgsql \ ## Является <resource\_id>

pgctl="/usr/pgsql-10/bin/pg\_ctl"\

psql="/usr/pgsql-10/bin/psql"\

pgdata="/pgdata/data/"\

rep\_mode="sync"\

node\_list="pg1 pg2"\

primary\_conninfo\_opt="keepalives\_idle=60 keepalives\_interval=5 keepalives\_count=5 password=pass" \ ## Пароль репликации

repuser=replica replication\_slot\_name=standby\_slot2 \

master\_ip="x.x.x.x"\ ## Виртуальный кластерный IP

op start timeout="60s" interval="0s" on-fail="restart"\

op monitor timeout="60s" interval="4s" on-fail="restart"\

op monitor timeout="60s" interval="3s" on-fail="restart" role="Master"\

op promote timeout="60s" interval="0s" on-fail="restart"\

op demote timeout="60s" interval="0s" on-fail="stop"\

op stop timeout="60s" interval="0s" on-fail="block"\

op notify timeout="60s" interval="0s"

pcs resource master msPostgresql pgsql \ ## Является <resource\_id>

master-max=1 master-node-max=1 clone-max=2 clone-node-max=1 notify=true

pcs resource group add master-group vip-master

pcs constraint colocation add master-group with Master msPostgresql INFINITY

pcs constraint order promote msPostgresql then start master-group symmetrical=false score=INFINITY

pcs constraint order demote msPostgresql then stop master-group symmetrical=false score=0

1. Выполнить перезапуск ресурсов на всех нодах кластера

pcs resource cleanup

#### **Установка Apache Tomcat**

Действия необходимо выполнять на серверах приложений.

1. Добавить пользователя и группу:

groupadd tomcat

useradd -s /bin/false -g tomcat -d /opt/tomcat tomcat

1. В директории /opt/ расположить архив с tomcat:

cd /opt

tar –xzvf apache-tomcat-7.0.54.tar.gz

mv apache-tomcat-7.0.54 /tomcat/

1. Установить права:

chown -hR tomcat:tomcat /opt/tomcat

1. Настроить запуск сервиса systemd:

vi /etc/systemd/system/tomcat.service

1. С содержимым:

[Unit]

Description=Apache Tomcat 7 Servlet Container

After=syslog.target network.target

[Service]

User=tomcat

Group=tomcat

Type=forking

Environment=CATALINA\_PID=/opt/tomcat/tomcat.pid

Environment=CATALINA\_HOME=/opt/tomcat

Environment=CATALINA\_BASE=/opt/tomcat

ExecStart=/opt/tomcat/bin/startup.sh

ExecStop=/opt/tomcat/bin/shutdown.sh

Restart=on-failure

[Install]

WantedBy=multi-user.target

1. Перезагрузить конфигурацию:

systemctl daemon-reload

1. Добавить сервис в автозагрузку:

systemctl enable tomcat

1. Запустить сервис:

systemctl start tomcat

1. Сервис должен запуститься без ошибок.

#### **Установка HAProxy**

Действия необходимо выполнить на прокси-серверах. Отказоустойчивая конфигурации HAProxy, состоит из двух нод. Ноды работают в режиме Active-Passive, проксирование запросов выполняется по алгоритму Round Robin на две ноды сервисов Интеграционной шины.

1. Установка приложений:

yum install –y haproxy keepalived

1. Добавить сервисы в автозагрузку

systemctl enable haproxy

systemctl enable keepalived

1. Запустить сервисы

systemctl start haproxy

systemctl start keepalived

Для работы по протоколу HTTPS необходим файл, содержащий публичный сертификат и приватный ключ. Файл сертификата необходимо расположить по следующему пути: /etc/haproxy/certificatename.pem.

#### **Установка КриптоПро JCP**

Действия выполняются на сервере приложения, на котором будет развернут модуль SMEV3-SENDER. Лицензии на право использования СКЗИ «КриптоПро JCP» на сервере предоставляются организацией.

1. Выполнить установку пакетов:

yum install unzip

unzip jcp-2.0.39014.zip

cd jcp-2.0.39014

chmod +x setup\_console.sh

.setup\_console.sh [путь\_к\_JRE]

На все вопросы мастера установки оставлются значения по умолчанию, далее необходимо нажимать Enter.

1. Для запуска контрольной панели необходимо выполнить:

ControlPanel.sh [путь\_к\_JRE]

1. Скопировать файлы из дистрибутива по пути [путь\_к\_JRE/lib/ext]:

commons-logging-1.2.jar

serializer-2.7.2.jar

slf4j-api-1.8.0-beta2.jar

xalan-2.7.2.jar

xmlsec-1.5.8.jar

logback-classic-1.2.3.jar,

logback-core-1.2.3.jar

javax.servlet-api-4.0.1.jar

Файл хранилища сертификата КриптоПро должен находиться в директории /var/opt/cprocsp. Ключи (директория с ключами) в /var/opt/cprocsp/key/tomcat.

1. У файлов сертификата и ключей необходимо установить владельцем пользователя tomcat. Для этого следует выполнить команды:

chown tomcat /var/opt/cprocsp/certstore

chown –R tomcat /var/opt/cprocsp/keys/tomcat/gknakmik.000

### Установка клиентского рабочего места

Для работы с Интеграционной шиной на клиентском рабочем месте должен быть установлен web-браузер:

Mozilla Firefox 64.0 и выше;

Opera 57.0 и выше;

Google Chrome 71.0 и выше.

### Определение пути доступа по сети к серверу

Для доступа к Интеграционной шине должен быть открыт порт 8080 на сервере приложения.

Веб-адреса модулей Интеграционной шины приведены в Таблице 2.

Таблица 2. Адреса для доступа к модулям Интеграционной шины

| **Веб-адрес** | **Описание** |
| --- | --- |
| http://[DNS\_NAME]:8080/operator/ | модуль мониторинга |
| http://[DNS\_NAME]:8080/admin/ | модуль администрирования |
| http://[DNS\_NAME]:8080/interaction | модуль взаимодействия |
| http://[DNS\_NAME]:8080/smev3-xmlsig/sign | модуль работы с ЭП |

### Установка программного обеспечения клиентского рабочего места

Действий не требуется.

### Загрузка необходимых компонентов системы

Необходимые компоненты и библиотеки поставляются в дистрибутиве, а также в данном документе описаны действия, которые необходимо выполнить для загрузки и установки актуальных версий компонентов, которые не входят в дистрибутив.

### Проверка функционирования программно-технического комплекса

После установки и настройки компонентов системы. Должны быть доступны web-интерфейсы Модуля мониторинга и Модуля администрирования Интеграционной шины. Для запуска Интеграционной шины требуется выполнить ввод в адресной строке запущенного web-браузера адреса модуля Интеграционной шины. Система работоспособна, если в результате действий пользователя, на экране монитора отобразилась форма авторизации в клиентском приложении без выдачи пользователю сообщений о сбое в работе.

### Настройка серверной части

#### **Настройка HAProxy**

Действия выполняются на прокси-серверах. Файл конфигурации расположен по пути /etc/haproxy/haproxy.cfg.

1. Необходимо изменить базовую часть для работы по HTTPS. Пример конфигурации для сервиса /interaction:

global

log 127.0.0.1 local2

chroot /var/lib/haproxy

pidfile /var/run/haproxy.pid

maxconn 4000

user haproxy

group haproxy

daemon

# turn on stats unix socket

stats socket /var/lib/haproxy/stats

#---------------------------------------------------------------------

# common defaults that all the 'listen' and 'backend' sections will

# use if not designated in their block

#---------------------------------------------------------------------

defaults

mode http

log global

option httplog

option dontlognull

option http-server-close

option forwardfor except 127.0.0.0/8

option redispatch

retries 3

timeout http-request 10s

timeout queue 1m

timeout connect 10s

timeout client 1m

timeout server 1m

timeout http-keep-alive 10s

timeout check 10s

maxconn 3000

#---------------------------------------------------------------------

# main frontend which proxys to the backends

#---------------------------------------------------------------------

frontend main \*:80

bind \*:443 ssl crt /etc/haproxy/certificatename.pem

stats uri /haproxy?stats

redirect scheme https if !{ ssl\_fc }

default\_backend rootapp

acl url\_int\_tag path\_beg /interaction

use\_backend app if url\_int\_tag

#---------------------------------------------------------------------

# static backend for serving up images, stylesheets and such

#---------------------------------------------------------------------

backend rootapp # this is your default backend

mode http

    balance     roundrobin

server node1 dns.name.node1:8080 check

server node2 dns.name.node2:8080 check

#---------------------------------------------------------------------

# round robin balancing between the various backends

#---------------------------------------------------------------------

backend app

mode http

balance roundrobin

server node1 dns.name.node1:8080 check

server node2 dns.name.node2:8080 check

1. Настроить демона Keepalived использующего в работе протокол VRRP (Virtual Redundancy Routing Protocol). Файл настроек располагается по пути /etc/keepalived/keepalived.conf. Общий IP адрес для кластера серверов определяем в [X.X.X.X]. Раздел проверяющий наличие рабочего процесса haproxy:

vrrp\_script check\_haproxy {

script "killall -0 haproxy"

interval 2

weight 2

}

vrrp\_instance LVS\_HAP {

#state MASTER|BACKUP

state MASTER

interface ens192

virtual\_router\_id 51

# 5 on master, 4 on backup

# Note that priority is set in the VRRP router and defines the master

priority 5

advert\_int 1

authentication {

#auth\_type PASS|AH

auth\_type PASS

auth\_pass changeme

}

virtual\_ipaddress {

X.X.X.X

}

track\_script {

check\_haproxy

}

}

#### **Настройка IBM WebSphere MQ**

Для настройки взаимодействия tomcat и WebSphere MQ необходимо обеспечить настроенный на WMQ Администратор очередей (имя администратора очереди и TCP/IP порт указывается при настройке контекста приложения Интеграционной шины). Администратор очередей должен содержать очереди, представленные в Таблица 3.

Таблица 3. Необходимые очереди сообщений

| **Название очереди** | **Описание** |
| --- | --- |
| QQ\_OUTBOUND | пример исходящей очереди для асинхронного абонента |
| INTERACTION\_Q | служебная очередь входящих сообщений для компонента взаимодействия по Http  В случае разворачивания системы в нескольких узлах, необходимо предусмотреть соответствующее количество очередей INTERACTION\_Qx, где x – порядковый номер очереди, соответствующий порядковому номеру узла |
| MQ\_INTERACTION\_Q | входящая очередь сообщений от асинхронных абонентов |
| MQ\_SENDER\_Q | служебная очередь для полученных сообщений от асинхронных абонентов MQ |
| MULTICAST\_Q | служебная очередь для сообщений, отправляемых по подписке |
| ROUTER\_IN | служебная очередь для отправляемых сообщений в маршрутизатор |
| SENDER\_Q | служебная очередь для исходящих сообщений по http |

Необходимо создать локальную учетную запись tomcat и предоставить права доступа для Администратора очередей. Необходимо настроить доступ к каналу Администратора очередей для соединения с WMQ.

#### **Создать директорию для хранения файлов сообщений на сервере приложения**

Нужно создать директорию для хранений файлов сообщений на каждом сервере приложения и сделать так, чтобы ее владельцем был пользователь tomcat:

mkdir /opt/storage

chown –R tomcat /opt/storage

#### **Создание БД PostgreSQL**

Действия выполняются на серверах БД. Необходимо создать базу данных, скрипт для создания которой приведен ниже:

Строка пароля md5 формируется по правилу: "md5"+md5(password+login).

su - postgres

psql -U root template1

CREATE USER [имя пользователя] ENCRYPTED PASSWORD [пароль]

CREATE DATABASE [имя бд] WITH OWNER [имя пользователя];

GRANT ALL ON DATABASE [имя бд] TO [имя пользователя];

1. Для подключения с удаленной машины к PostgreSQL в файле /pgdata/data/postgresql.conf раскомментировать строку с параметром listen\_addresses, указав, что принимаются подключения с любых адресов:

listen\_addresses = '\*'

1. Также необходимо внести изменения в файл /pgdata/data/pg\_hba.conf, добавив строку:

host all all 0.0.0.0/0 md5

Данная строка означает, что принимаются любые подключения, прошедшие аутентификацию, для любых пользователей и любых баз данных.

#### **Настройка репликации баз данных**

Сначала нужно настроить ведущий сервер (master).

1. Для обеспечения работы потоковой репликации на MASTER-е редактируем файл /pgdata/data/postgresql.conf, добавляем следующие строки:

listen\_addresses=‘\*’  
wal\_level=hot\_standby  
wal\_log\_hints=on  
max\_wal\_senders=8  
wal\_keep\_segments=64  
hot\_standby = on

1. На MASTER-е создаем пользователя repluser под которым SLAVE будет подключаться к MASTER-у.

# sudo -u postgres psql

postgres=# CREATE ROLE repluser WITH REPLICATION PASSWORD [пароль]LOGIN;\q

1. На MASTER-е редактируем /pgdata/data/pg\_hba.conf, то есть, обеспечиваем, чтобы в этом файле были такие строчки (разрешаем SLAVE-у подключаться к MASTER-у под пользователем repluser для осуществления потоковой репликации):

host    all             all             <ip\_MASTER>/32        md5    
host    all             all             <ip\_SLAVE>/32         md5    
host    replication     repluser        <ip\_MASTER>/32     md5   
host    replication     repluser        <ip\_SLAVE>/32       md5

1. Перезапускаем СУБД:

# systemctl restart postgresql-10.6

Выполняем настройку SLAVE сервера:

1. Останавливаем СУБД:

# systemctl stop postgresql-10.6

1. Удаляем все файлы в директории data:

# rm -rf /pgdata/data/\*

1. Копируем с MASTER-а базу (внимание - запускаем pg\_basebackup под пользователем postgres, под которым работает база):

# su - postgres

pg\_basebackup --host=[ip\_MASTER] --username=repluser --pgdata=/pgdata/data --xlog-method=stream --write-recovery-conf

exit

1. Запускаем СУБД:

# systemctl start postgresql-10.6

#### **Миграция БД**

Действия выполняются на сервере БД Master.

1. Необходимо скачать flyway:

cd ~

wget https://bintray.com/artifact/download/business/maven/flyway-commandline-3.2.1-linux-x64.tar.gz

1. Распаковать архив и переместить в /usr/share/:

tar xf flyway-commandline-3.2.1-linux-x64.tar.gz

mv flyway-3.2.1 /usr/share/flyway

1. Скопировать SQL-файлы миграций проекта Интеграционной шины в /usr/share/flyway/sql.
2. Внести в файл конфигурации /usr/share/flyway/conf/flyway.conf следующие изменения:

flyway.url=jdbc:postgresql://localhost:5432/[имя бд]

flyway.user=[пользователь бд]

flyway.password=[пароль]

flyway.placeholders.role=[пользователь бд]

1. Запустить процесс накатывания миграций и дождаться окончания процесса (Рисунок 1):

/usr/share/flyway/flyway migrate

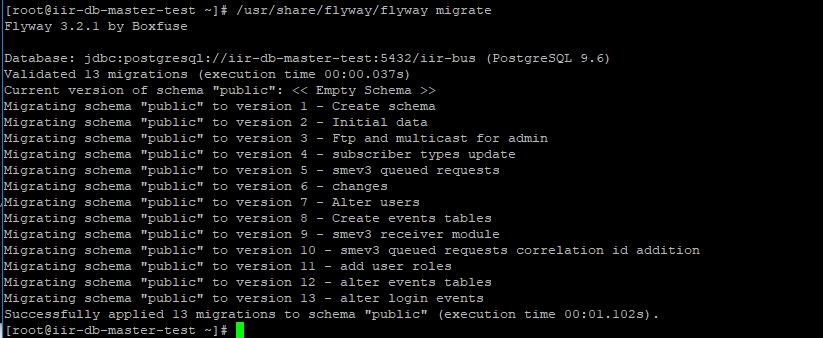


Рисунок 1 – Миграция БД

#### **Создание учетной записи первого администратора для Интеграционной шины**

Выполнить запросы, с указанием доменной учетной записи администратора:

insert into public.users (id,name,user\_name) values (3,'[admin\_login]', ‘[admin\_name]')

insert into public.user\_principals (user\_id,user\_role\_id) values (3,2)

#### **Конфигурирование контекста приложения Интеграционной шины**

Действия выполняются на сервере приложения.

1. Остановить сервис tomcat:

#systemctl stop tomcat

1. В файл /opt/tomcat/conf/context.xml добавить следующие строки:

<Environment name="spring.profiles.active" type="java.lang.String" value="tomcat,jndi,ldap" />

<Environment name="api.host" value="localhost:8080" type="java.lang.String" override="true" /> <ResourceLink name="jdbc/sv/ds" global="jdbc/sv/ds" type="javax.sql.DataSource"/>

<Environment name="conf/sv/hibernateDialect" type="java.lang.String" value="org.hibernate.dialect.PostgreSQLDialect" />

<Environment name="conf/ibssc/hibernateDialect" type="java.lang.String" value="org.hibernate.dialect.PostgreSQLDialect" />

<Environment name="jms/sender/dmqName" type="java.lang.String" value="PSEUDO\_DMQ" />

<Environment name="jms/sender/dmqBlockFlag" type="java.lang.Boolean" value="TRUE" />

<Environment name="conf/sv/sign.host" type="java.lang.String" value="localhost" />

<Environment name="conf/sv/sign.port" type="java.lang.String" value="8080" />

<ResourceLink global="jms/inter/cf" name="jms/inter/cf" type="javax.jms.ConnectionFactory"/>

<ResourceLink global="jms/inter/sendQueue" name="jms/inter/sendQueue" type="javax.jms.Queue"/>

<ResourceLink global="jms/inter/receiveQueue" name="jms/inter/receiveQueue" type="javax.jms.Queue"/>

<ResourceLink global="jms/router/cf" name="jms/router/cf" type="javax.jms.ConnectionFactory"/>

<ResourceLink global="jms/router/sendQueue" name="jms/router/sendQueue" type="javax.jms.Queue"/>

<ResourceLink global="jms/router/receiveQueue" name="jms/router/receiveQueue" type="javax.jms.Queue"/>

<ResourceLink global="jms/sender/cf" name="jms/sender/cf" type="javax.jms.ConnectionFactory"/>

<ResourceLink global="jms/sender/sendQueue" name="jms/sender/sendQueue" type="javax.jms.Queue"/>

<ResourceLink global="jms/sender/receiveQueue" name="jms/sender/receiveQueue" type="javax.jms.Queue"/>

<ResourceLink global="jms/multicast/cf" name="jms/multicast/cf" type="javax.jms.ConnectionFactory"/>

<ResourceLink global="jms/multicast/sendQueue" name="jms/multicast/sendQueue" type="javax.jms.Queue"/>

<ResourceLink global="jms/multicast/receiveQueue" name="jms/multicast/receiveQueue" type="javax.jms.Queue"/>

<ResourceLink global="jms/smevsender/cf" name="jms/smevsender/cf" type="javax.jms.ConnectionFactory"/>

<ResourceLink global="jms/smevsender/sendQueue" name="jms/smevsender/sendQueue" type="javax.jms.Queue"/>

<ResourceLink global="jms/smevsender/receiveQueue" name="jms/smevsender/receiveQueue" type="javax.jms.Queue"/>

<ResourceLink global="jms/smevinter/cf" name="jms/smevinter/cf" type="javax.jms.ConnectionFactory"/>

<ResourceLink global="jms/smevinter/sendQueue" name="jms/smevinter/sendQueue" type="javax.jms.Queue"/>

<ResourceLink global="jms/smevinter/receiveQueue" name="jms/smevinter/receiveQueue" type="javax.jms.Queue"/>

<ResourceLink global="jms/mqinter/cf" name="jms/mqinter/cf" type="javax.jms.ConnectionFactory"/>

<ResourceLink global="jms/mqinter/sendQueue" name="jms/mqinter/sendQueue" type="javax.jms.Queue"/>

<ResourceLink global="jms/mqinter/receiveQueue" name="jms/mqinter/receiveQueue" type="javax.jms.Queue"/>

<ResourceLink global="jms/mqsender/cf" name="jms/mqsender/cf" type="javax.jms.ConnectionFactory"/>

<ResourceLink global="jms/mqsender/sendQueue" name="jms/mqsender/sendQueue" type="javax.jms.Queue"/>

<ResourceLink global="jms/mqsender/receiveQueue" name="jms/mqsender/receiveQueue" type="javax.jms.Queue"/>

<ResourceLink global="jms/smev3sender/cf" name="jms/smev3sender/cf" type="javax.jms.ConnectionFactory"/>

<ResourceLink global="jms/smev3sender/sendQueue" name="jms/smev3sender/sendQueue" type="javax.jms.Queue"/>

<ResourceLink global="jms/smev3sender/receiveQueue" name="jms/smev3sender/receiveQueue" type="javax.jms.Queue"/>

<ResourceLink global="jms/smev3receiver/cf" name="jms/smev3receiver/cf" type="javax.jms.ConnectionFactory"/>

<ResourceLink global="jms/smev3receiver/sendQueue" name="jms/smev3receiver/sendQueue" type="javax.jms.Queue"/>

<ResourceLink global="jms/smev3receiver/receiveQueue" name="jms/smev3receiver/receiveQueue" type="javax.jms.Queue"/>

<Resource name="app/intersec/ldap"

auth="Container"

type="ru.kacit.sv.configuration.LdapConfig"

factory="org.apache.naming.factory.BeanFactory"

interceptUrl="/\*\*"

accessRole="isAuthenticated()"

ldapUrl="ldap://[AD-host]:389/"

managerDN="[managerDN]"

managerPWD="[managerPWD]"

userDnPattern="DC=[domain],DC=com"

groupDnPattern="DC=[domain],DC=com"

personFilter="[%filter%]"/>

1. Файл context.xml нужно скопировать на все сервера приложения Интеграционной шины.
2. В файл /opt/tomcat/conf/server.xml между тэгами GlobalNamingResources добавить (необходимо указать актуальные данные для подключений):

<Resource name="jdbc/sv/ds"

auth="Container"

type="com.mchange.v2.c3p0.ComboPooledDataSource"

user="[пользователь бд]"

password="[пароль]"

jdbcUrl=" jdbc:postgresql://[сервер\_бд]:5432/[имя\_бд]"

driverClass="org.postgresql.Driver"

maxPoolSize="120"

minPoolSize="0"

maxConnectionAge="5000"

acquireRetryAttempts="60"

acquireIncrement="1"

preferredTestQuery="SELECT 1"

description="c3p0 DB Connection"

factory="org.apache.naming.factory.BeanFactory"

testConnectionOnCheckout="false"/>

<Resource

name="jms/inter/cf"

auth="Container"

type="com.ibm.mq.jms.MQQueueConnectionFactory"

factory="com.ibm.mq.jms.MQQueueConnectionFactoryFactory"

description="JMS Queue Connection Factory for interaction messages"

HOST="[имя сервера wmq]"

PORT="[порт]"

CHAN="SYSTEM.DEF.SVRCONN"

TRAN="1"

QMGR="[имя\_администратора\_очереди]"/>

<Resource name="jms/smev3receiver/cf"

auth="Container"

type="com.ibm.mq.jms.MQQueueConnectionFactory"

factory="com.ibm.mq.jms.MQQueueConnectionFactoryFactory"

description="JMS Queue Connection Factory for smev3 receiver messages"

HOST="[имя сервера wmq]"

PORT=" [порт] "

CHAN="SYSTEM.DEF.SVRCONN"

TRAN="1"

QMGR="[имя\_администратора\_очереди]"/>

<Resource

name="jms/router/cf"

auth="Container"

type="com.ibm.mq.jms.MQQueueConnectionFactory"

factory="com.ibm.mq.jms.MQQueueConnectionFactoryFactory"

description="JMS Queue Connection Factory for router messages"

HOST="[имя сервера wmq]"

PORT="[порт]"

CHAN="SYSTEM.DEF.SVRCONN"

TRAN="1"

QMGR="[имя\_администратора\_очереди]"/>

<Resource

name="jms/sender/cf"

auth="Container"

type="com.ibm.mq.jms.MQQueueConnectionFactory"

factory="com.ibm.mq.jms.MQQueueConnectionFactoryFactory"

description="JMS Queue Connection Factory for sending messages"

HOST="[имя сервера wmq]"

PORT="[порт]"

CHAN="SYSTEM.DEF.SVRCONN"

TRAN="1"

QMGR="[имя\_администратора\_очереди]"/>

<Resource

name="jms/multicast/cf"

auth="Container"

type="com.ibm.mq.jms.MQQueueConnectionFactory"

factory="com.ibm.mq.jms.MQQueueConnectionFactoryFactory"

description="JMS Queue Connection Factory for multicast messages"

HOST="[имя сервера wmq]"

PORT="[порт]"

CHAN="SYSTEM.DEF.SVRCONN"

TRAN="1"

QMGR="[имя\_администратора\_очереди]"/>

<Resource

name="jms/smevsender/cf"

auth="Container"

type="com.ibm.mq.jms.MQQueueConnectionFactory"

factory="com.ibm.mq.jms.MQQueueConnectionFactoryFactory"

description="JMS Queue Connection Factory for smevsender messages"

HOST="[имя сервера wmq]"

PORT="[порт]"

CHAN="SYSTEM.DEF.SVRCONN"

TRAN="1"

QMGR="[имя\_администратора\_очереди]"/>

<Resource

name="jms/smev3sender/cf"

auth="Container"

type="com.ibm.mq.jms.MQQueueConnectionFactory"

factory="com.ibm.mq.jms.MQQueueConnectionFactoryFactory"

description="JMS Queue Connection Factory for smevsender messages"

HOST="[имя сервера wmq]"

PORT="[порт]"

CHAN="SYSTEM.DEF.SVRCONN"

TRAN="1"

QMGR="[имя\_администратора\_очереди]"/>

<Resource

name="jms/smevinter/cf"

auth="Container"

type="com.ibm.mq.jms.MQQueueConnectionFactory"

factory="com.ibm.mq.jms.MQQueueConnectionFactoryFactory"

description="JMS Queue Connection Factory for smevinter messages"

HOST="[имя сервера wmq]"

PORT="[порт]"

CHAN="SYSTEM.DEF.SVRCONN"

TRAN="1"

QMGR="[имя\_администратора\_очереди]"/>

<Resource

name="jms/mqinter/cf"

auth="Container"

type="com.ibm.mq.jms.MQQueueConnectionFactory"

factory="com.ibm.mq.jms.MQQueueConnectionFactoryFactory"

description="JMS Queue Connection Factory for mqinter messages"

HOST="[имя сервера wmq]"

PORT="[порт]"

CHAN="SYSTEM.DEF.SVRCONN"

TRAN="1"

QMGR="[имя\_администратора\_очереди]"/>

<Resource

name="jms/mqsender/cf"

auth="Container"

type="com.ibm.mq.jms.MQQueueConnectionFactory"

factory="com.ibm.mq.jms.MQQueueConnectionFactoryFactory"

description="JMS Queue Connection Factory for mqsender messages"

HOST="[имя сервера wmq]"

PORT="[порт]"

CHAN="SYSTEM.DEF.SVRCONN"

TRAN="1"

QMGR="[имя\_администратора\_очереди]"/>

<Resource name="jms/inter/receiveQueue"

auth="Container"

type="com.ibm.mq.jms.MQQueue"

factory="com.ibm.mq.jms.MQQueueFactory"

description="JMS Queue for receiving messages from Dialog"

QU="[название очереди для входящих сообщений компонента взаимодействия по http: в случае наличия только одного узла –INTERACTION\_Q, в случае нескольких – INTERACTION\_Qx, где x – порядковый номер, соответствующий порядковому номеру узла]"

version="1.1" />

<Resource name="jms/inter/sendQueue"

auth="Container"

type="com.ibm.mq.jms.MQQueue"

factory="com.ibm.mq.jms.MQQueueFactory"

QU="ROUTER\_IN"

version="1.1" />

<Resource name="jms/smev3receiver/receiveQueue"

auth="Container"

type="com.ibm.mq.jms.MQQueue"

factory="com.ibm.mq.jms.MQQueueFactory"

description="JMS Queue for receiving messages from Dialog"

QU="ROUTER\_IN"

version="1.1" />

<Resource name="jms/smev3receiver/sendQueue"

auth="Container"

type="com.ibm.mq.jms.MQQueue"

factory="com.ibm.mq.jms.MQQueueFactory"

description="JMS Queue for receiving messages from Dialog"

QU="ROUTER\_IN"

version="1.1" />

<Resource name="jms/router/receiveQueue"

auth="Container"

type="com.ibm.mq.jms.MQQueue"

factory="com.ibm.mq.jms.MQQueueFactory"

description="JMS Queue for receiving messages from Dialog"

QU="ROUTER\_IN"

version="1.1" />

<Resource name="jms/router/sendQueue"

auth="Container"

type="com.ibm.mq.jms.MQQueue"

factory="com.ibm.mq.jms.MQQueueFactory"

description="JMS Queue for receiving messages from Dialog"

QU="ROUTER\_IN"

version="1.1" />

<Resource name="jms/sender/receiveQueue"

auth="Container"

type="com.ibm.mq.jms.MQQueue"

factory="com.ibm.mq.jms.MQQueueFactory"

description="JMS Queue for receiving messages from Dialog"

QU="SENDER\_Q"

version="1.1" />

<Resource name="jms/sender/sendQueue"

auth="Container"

type="com.ibm.mq.jms.MQQueue"

factory="com.ibm.mq.jms.MQQueueFactory"

description="JMS Queue for receiving messages from Dialog"

QU="ROUTER\_IN"

version="1.1" />

<Resource name="jms/multicast/receiveQueue"

auth="Container"

type="com.ibm.mq.jms.MQQueue"

factory="com.ibm.mq.jms.MQQueueFactory"

description="JMS Queue for receiving messages from Dialog"

QU="MULTICAST\_Q"

version="1.1" />

<Resource name="jms/multicast/sendQueue"

auth="Container"

type="com.ibm.mq.jms.MQQueue"

factory="com.ibm.mq.jms.MQQueueFactory"

description="JMS Queue for receiving messages from Dialog"

QU="ROUTER\_IN"

version="1.1" />

<Resource name="jms/smevsender/receiveQueue"

auth="Container"

type="com.ibm.mq.jms.MQQueue"

factory="com.ibm.mq.jms.MQQueueFactory"

description="JMS Queue for receiving messages from Dialog"

QU="SMEV\_Q"

version="1.1" />

<Resource name="jms/smev3sender/receiveQueue"

auth="Container"

type="com.ibm.mq.jms.MQQueue"

factory="com.ibm.mq.jms.MQQueueFactory"

description="JMS Queue for receiving messages from Dialog"

QU="SMEV3\_Q"

version="1.1" />

<Resource name="jms/smevsender/sendQueue"

auth="Container"

type="com.ibm.mq.jms.MQQueue"

factory="com.ibm.mq.jms.MQQueueFactory"

description="JMS Queue for receiving messages from Dialog"

QU="ROUTER\_IN"

version="1.1" />

<Resource name="jms/smev3sender/sendQueue"

auth="Container"

type="com.ibm.mq.jms.MQQueue"

factory="com.ibm.mq.jms.MQQueueFactory"

description="JMS Queue for receiving messages from Dialog"

QU="ROUTER\_IN"

version="1.1" />

<Resource name="jms/smevinter/receiveQueue"

auth="Container"

type="com.ibm.mq.jms.MQQueue"

factory="com.ibm.mq.jms.MQQueueFactory"

description="JMS Queue for receiving messages from Dialog"

QU="SMEV\_INTERACTION\_Q"

version="1.1" />

<Resource name="jms/smevinter/sendQueue"

auth="Container"

type="com.ibm.mq.jms.MQQueue"

factory="com.ibm.mq.jms.MQQueueFactory"

description="JMS Queue for receiving messages from Dialog"

QU="ROUTER\_IN"

version="1.1" />

<Resource name="jms/mqinter/receiveQueue"

auth="Container"

type="com.ibm.mq.jms.MQQueue"

factory="com.ibm.mq.jms.MQQueueFactory"

description="JMS Queue for receiving messages from Dialog"

QU="MQ\_INTERACTION\_Q"

version="1.1" />

<Resource name="jms/mqinter/sendQueue"

auth="Container"

type="com.ibm.mq.jms.MQQueue"

factory="com.ibm.mq.jms.MQQueueFactory"

description="JMS Queue for receiving messages from Dialog"

QU="ROUTER\_IN"

version="1.1" />

<Resource name="jms/mqsender/receiveQueue"

auth="Container"

type="com.ibm.mq.jms.MQQueue"

factory="com.ibm.mq.jms.MQQueueFactory"

description="JMS Queue for receiving messages from Dialog"

QU="MQ\_SENDER\_Q"

version="1.1" />

<Resource name="jms/mqsender/sendQueue"

auth="Container"

type="com.ibm.mq.jms.MQQueue"

factory="com.ibm.mq.jms.MQQueueFactory"

description="JMS Queue for receiving messages from Dialog"

QU="ROUTER\_IN"

version="1.1" />

<Environment name="jms/sender/dmqName"

type="java.lang.String"

value="PSEUDO\_DMQ" />

1. Файл server.xml необходимо скопировать на все сервера приложений.
2. Скопировать в каталог /opt/tomcat/lib следующие библиотеки (приложены к инструкции):

* postgresql-9.3-1100.jdbc41.jar
* spring-instrument-tomcat-4.0.5.RELEASE.jar
* jta-1.1.jar
* c3p0-0.9.1.1.jar
* javax.jms-api-2.0.1.jar
* com.ibm.mq.allclient-9.1.0.0.jar

1. Скопировать war-файлы Интеграционной шины на сервера приложений в соответствии со схемой стенда развертывания в директорию /opt/tomcat/webapps, указанные в Таблица 4.

Таблица 4. Соответствие war-файла и сервера приложения

| **Название War-файла** | **Название сервера приложения** |
| --- | --- |
| Тестовый контур | |
| admin.war  operator.war | пользовательские интерфейсы |
| interaction.war  sender.war  router.war  mq-Interaction.war  mq-Sender.war | внутренние сервисы |
| smev3-xmlsig.war | модуль работы с ЭП: |
| smev3-receiver.war  smev3-sender.war  smev3-requester.war | внешние сервисы |
| Продуктивный контур | |
| admin.war  operator.war | пользовательские интерфейсы |
| interaction.war  sender.war  router.war  mq-Interaction.war  mq-Sender.war | внутренние сервисы:  узел 1  узел 2 |
| smev3-xmlsig.war | модуль работы с ЭП:  узел 1  узел 2 |
| smev3-receiver.war  smev3-sender.war  smev3-requester.war | внешние сервисы:  узел 1  узел 2 |

1. После копирования war файлов нужно запустить сервисы на каждом из серверов приложений:

systemctl start tomcat

#### **Настройка модуля работы с ЭП**

Настройка модуля работы с ЭП осуществляется с помощью переменной окружения smev.security.config.file, в которой указан путь до файла с конфигурацией:

<Environment name="smev.security.config.file" type="java.lang.String" value="/root/smev\_security.xml"/>\n\

Файл конфигурации имеет следующую структуру:

<Keys>

<Key>

<CertStores>

<CertStore>

<Path>Путь до хранилища сертификатов, например, /var/opt/cprocsp/certstore</Path>

<Password>Пароль</Password>

<Certs>

<Cert>Наименование файла сертификата с расширением</Cert>

</Certs>

</CertStore>

</CertStores>

<Algorithm>

<SignatureMethod>urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr34102012-gostr34112012-256</SignatureMethod>

<DigestMethod>urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr34112012-256</DigestMethod>

</Algorithm>

</Key>

</Keys>

Элемент <Algorithm> настраивает алгоритм шифрования.

При загрузке модуль работы с ЭП считывает конфигурационный файл и загружает указанный в нем ключ, хранилище сертификатов ключей, сертификат в хранилище.

После считывания конфигурационного файла осуществляется соединение по HTTP-протоколу на путь:

/sign

Для настройки модулей, взаимодействующих с модулем работы с ЭП, необходимо указать в параметре smev.security.web.signer.host соответствующих модулей адрес модуля работы с ЭП, который прописан в параметре service.properties war-файла модуля работы с ЭП.

#### **Удаление устаревших данных из директории для хранения файлов сообщений на сервере приложения**

Действия необходимо выполнить на всех серверах приложениях, на которых создана директория /opt/storage/.

1. Необходимо скопировать из дистрибутива скрипт clear\_storage.sh в директорию /opt/.
2. Назначить права на скрипт:

chmod 755 /opt /clear\_storage.sh

Скрипт выполняет удаление файлов из /opt/storage/ и поддиректорий. Удаляются файлы старше 4 месяцев (120 дней) (параметр «-mtime» ,значение «+120», настраивается в скрипте clear\_storage.sh) и директории, которые не содержат файлов. Запуск происходит каждый день в 00:00.

1. Для запуска по расписанию используется crontab. Редактирование crontab вызывается командой:

crontab -e

1. Указать периодичность и путь до файла сценария:

SHELL=/bin/bash

PATH=/sbin:/bin:/usr/sbin:/usr/bin

MAILTO=root

HOME=/

0 0 \* \* \* \* sh /opt/clear\_storage.sh

1. Для проверки работы возможно использование команд, показывающих количество файлов и пустых папок в директории:

find /opt/storage/ -type f | wc -l

find /opt/storage/\* -type d -empty | wc -l

#### **Настройка параметров мониторинга работоспособности сервисов.**

Действия необходимо выполнить на всех серверах приложений:

Для конфигурирования компонентов мониторинга сервисов необходимо в файле context.xml добавить следующие строки.

<Environment name="delayTime" type="java.lang.String" value="180000"/>

где Value - Hастройка таймера опроса точек доступа.

<Environment name="moduleNames" type="java.lang.String" value="INTERACTION,SENDER,ROUTER,SMEV3\_REQUESTER,SMEV3\_SENDER,SMEV3\_RECEIVER,SMEV3\_XMLSIG,OPERATOR\_GUI,ADMIN\_GUI,MQ\_SENDER,MQ\_INTERACTION"/>

где Value - перечисление наименований сервисов на текущем узле.

Для каждого из moduleNames необходимо добавить строку:

<Environment name="healthcheck/%ИМЯ\_СЕРВИСА%" type="java.lang.String" value="http://%Имя\_узла%:8080/%имя\_сервиса%/healthcheck"/>

Где:

- %ИМЯ\_СЕРВИСА% - один из сервисов, перечисленных в Value элемента Environment с параметром name="moduleNames", который показан выше. Указывается в верхнем регистре.

- %Имя\_узла% - имя узла, где находится сервис %ИМЯ\_СЕРВИСА%.

- %имя\_сервиса% - %ИМЯ\_СЕРВИСА% в нижнем регистре.

#### **Настройка параметров логирования**

Действия необходимо выполнить на всех серверах приложений.

1. Необходимо скопировать из дистрибутива файлы конфигурации логов “logback-<serviceName>.xml” в директорию /opt/tomcat/libs/.
2. В файлах конфигурации задаются следующие параметры логирования:

Размер каждого из файлов логирования(например 50 MB) указывается в

 <property name="LOG\_\_FILE\_\_SIZE" value="50MB"/>

Уровень логирования(INFO, DEBUG, TRACE)

<property name="LOG\_\_LEVEL" value="TRACE"/>

Максимальное количество файлов:

<maxIndex>50</maxIndex>

Указывается отдельно для каждого журнала логирования.

Таким образом объем журнала не превысит заданных параметров.

#### **Удаление устаревших оперативных данных в БД Интеграционной шины**

Действия необходимо выполнить на сервере БД master.

1. Необходимо скопировать из дистрибутива скрипт tracks\_cleanup.sh в директорию /root/.
2. Назначить права доступа на скрипт:

chmod 755 /root/tracks\_cleanup.sh

Необходимо выполнить настройку файла tracks\_cleanup.sh:

1. Указать для каждого подключения в скрипте актуальные данные. Пример одной из команд в скрипте:

psql -h [ip адрес сервера бд mater] -d [имя бд] -U [пользователь бд] -p [порт сервера] -c "SELECT public.tracks\_cleanup($1);" >>tracks\_cleanup.txt 2>&1

1. Необходимо создать или дополнить файл .pgpass в домашней директории root, добавить строку, заполнив необходимыми параметрами:

Ip\_address:port:database:username:password

1. Изменить права доступа к файлу .pgpass, выполнив команду:

chmod 0600 .pgpass

1. Для запуска по расписанию используется crontab. Редактирование crontab вызывается командой:

crontab -e

1. Добавить в конец текста cron-настроек строку, Где 540 - количество дней, старше которых данные должны быть удалены. По умолчанию значение 18 месяцев (540 дней). Запуск происходит каждый день в 00:00.

0 0 \* \* \* \* sh /root/tracks\_cleanup.sh 540

### Настройка клиентской части

Настройка клиентской части системы не требуется.

## Проверка работоспособности сервисов Интеграционной шины

Мониторинг работоспособности сервисов Интеграционной шины осуществляется средствами встроенного в Модуль администрирования Интеграционной шины сервиса мониторинга.

Для проверки работоспособности сервиса Интеграционной шины необходимо:

1. Выполнить запрос по адресу – http://[DNS\_NAME]:8080/[SERVICE\_NAME]/healthcheck, где

[DNS\_NAME] – имя узла

[SERVICE\_NAME] – имя сервиса в tomcat

В продуктивном полигоне сервисы Интеграционной шины располагаются на разных серверах, адреса для опроса точек доступа сервисов показаны в таблице ниже:

Таблица 5. Адреса сервисов Интеграционной шины для проведения мониторинга

| **№ п/п** | **Сервисы Интеграционной шины** | **Адреса сервисов** |
| --- | --- | --- |
| 1 | Модуль администрирования | http://[DNS\_NAME]:8080/admin/healthcheck |
| 2 | Модуль мониторинга | http://[DNS\_NAME]:8080/operator/healthcheck |
| 3 | Внутренние сервисы (узел 1) | http://[DNS\_NAME1]:8080/interaction/healthcheck  http://[DNS\_NAME1]:8080/sender/healthcheck  http://[DNS\_NAME1]:8080/router/healthcheck  http://[DNS\_NAME1]:8080/mq-interaction/healthcheck  http://[DNS\_NAME1]:8080/mq-sender/healthcheck |
| 4 | Внутренние сервисы (узел 2) | http://[DNS\_NAME2]:8080/interaction/healthcheck  http://[DNS\_NAME2]:8080/sender/healthcheck  http://[DNS\_NAME2]:8080/router/healthcheck  http://[DNS\_NAME2]:8080/mq-interaction/healthcheck  http://[DNS\_NAME2]:8080/mq-sender/healthcheck |
| 5 | Внешние сервисы (узел 1) | http://[DNS\_NAME3]:8080/smev3-sender/healthcheck  http://[DNS\_NAME3]:8080/smev3-receiver/healthcheck  http://[DNS\_NAME3]:8080/smev3-requester/healthcheck  http://[DNS\_NAME3]:8080/smev3-xmlsig/healthcheck |
| 6 | Внешние сервисы (узел 2) | http://[DNS\_NAME4]:8080/smev3-sender/healthcheck  http://[DNS\_NAME4]:8080/smev3-receiver/healthcheck  http://[DNS\_NAME4]:8080/smev3-requester/healthcheck  http://[DNS\_NAME4]:8080/smev3-xmlsig/healthcheck |

1. Получить объект JSON, содержащий информацию о:

* Успешной работоспособности.
* Версии ПО сервиса.

Пример такого объекта показан на рисунке ниже



Рисунок 2 – Сведения о мониторинге сервиса

Для проверки работоспособности всех сервисов Интеграционной шины необходимо:

Сделать запрос к точке доступа модуля администрирования по следующему адресу: http://[DNS\_NAME]:8080/admin/health/

Получить объект JSON, содержащий информацию об:

* Имени сервиса;
* Узле, где развернут сервис;
* Типе проверки(app, jms, ldap, db, smev);
* Состоянии работоспособности;
* Времени проверки;
* Версии ПО;

Пример объекта JSON приведен на Рисунке 3ниже:

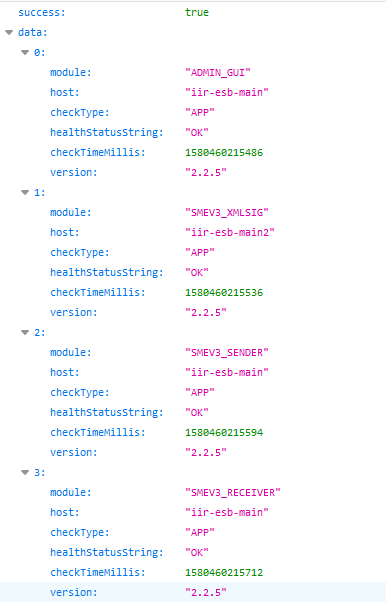


Рисунок 3 – Сведения о мониторинге сервисов.

## Функции администрирования при эксплуатации системы

При эксплуатации Интеграционной шины должны выполняться следующие функции администрирования:

1. управление правами доступа обслуживающего персонала к функциям Модуля администрирования и Модуля мониторинга Интеграционной шины;
2. управление прикладными системами, взаимодействующими между собой, а также с ФОИВ посредством Интеграционной шины;
3. ведение перечня ФОИВ, взаимодействующих с прикладными системами;
4. протоколирование действий обслуживающего персонала при работе с Модулем администрирования и Модулем мониторинга Интеграционной шины;
5. мониторинг работоспособности сервисов Интеграционной шины.

### Управление правами доступа

Управление правами доступа пользователей к Интеграционной шине осуществляется средствами Модуля администрирования пользователей Интеграционной шины.

Модуль администрирования пользователей обеспечивает следующие функции:

1. добавление пользователей технического и технологического сопровождения (администраторов), имеющих доступ к функциям Модуля администрирования и Модуля мониторинга Интеграционной шины.
2. назначение прав доступа пользователям технического и технологического сопровождения (администраторам) к функциям Модуля администрирования и Модуля мониторинга Интеграционной шины;
3. просмотр списка добавленных пользователей с возможностью изменения прав доступа, удаления и блокировки пользователей Модуля администрирования и Модуля мониторинга Интеграционной шины.

#### **Ролевая модель**

В Интеграционной шине предусмотрены следующие пользовательские роли:

* Главный (системный) администратор (Administrator);
* Администратор безопасности (SecurityAdministrator);
* Администратор пользователей (UserAdministrator);
* Оператор (Operator).

Роль оператора предназначена для доступа к Модулю мониторинга Интеграционной шины.

Роли администраторов предназначены для разграничения прав доступа к следующим объектам Модуля администрирования Интеграционной шины:

* раздел «Абоненты»;
* раздел «Организации и информационные системы»;
* раздел «Данные аутентификации»;
* раздел «Отчеты»;
* раздел «Виды сведений».

При присвоении нескольких ролей пользователю одна роль не уменьшает количество разрешений другой роли, т.е. в итоге пользователь обладает суммой всех разрешений присвоенных ему ролей (Таблица 6).

Таблица 6. Пересечение ролей

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Объект системы | Главный администратор  Администратор безопасности | Главный администратор  Администратор пользователей | Администратор пользователей  Администратор безопасности | Главный администратор  Администратор безопасности  Администратор пользователей |
| Раздел «Абоненты» | модификация | модификация | просмотр | модификация |
| Раздел «Организации» | модификация | модификация | просмотр | модификация |
| Раздел «Данные аутентификации» | модификация | модификация | модификация | модификация |
| Раздел «Отчеты» | модификация | нет прав | модификация | модификация |
| Раздел «Виды сведений» | модификация | модификация | нет прав | модификация |

#### **Порядок назначения прав пользователям**

Пользователями с правами Главный администратор и Администратор пользователей имеют права на создание, модификацию и удаление прав доступа учетных записей пользователей к объектам системы.

На вкладке «Данные аутентификации» отображается весь перечень пользователей и абонентов Интеграционной шины (Рисунок 4).

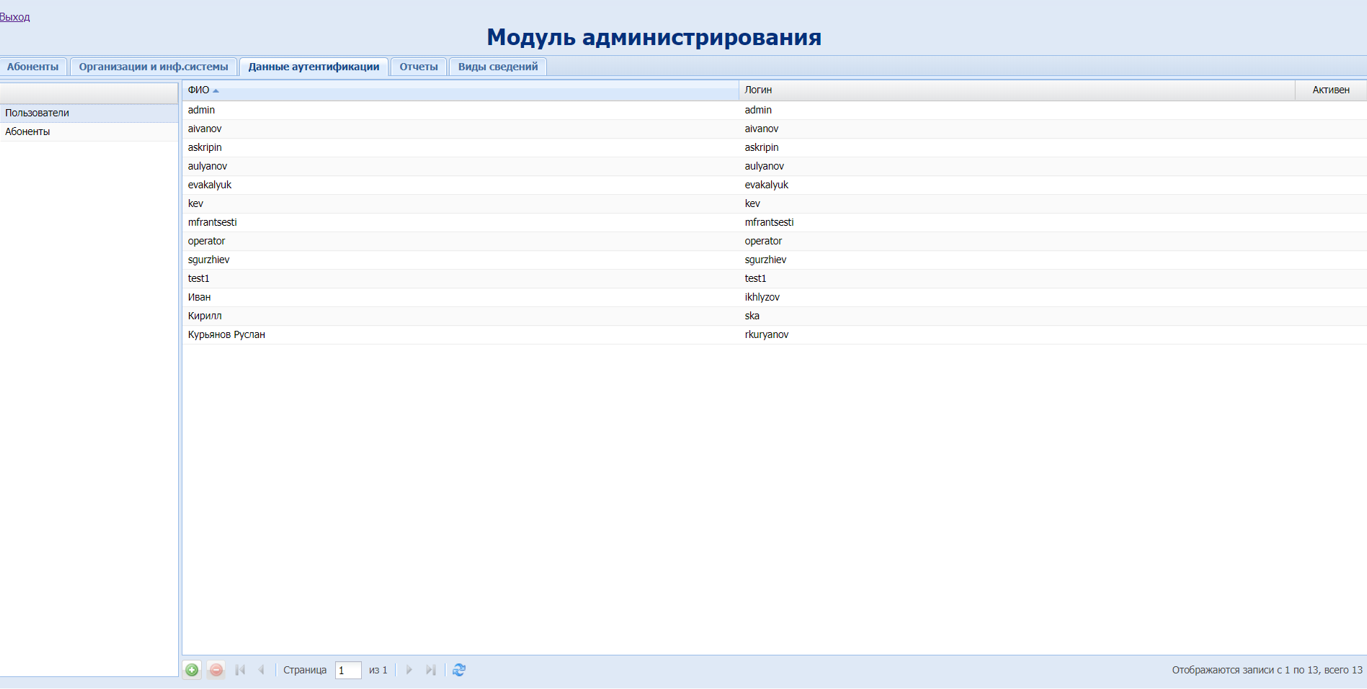


Рисунок 4 – Вкладка «Данные аутентификации»

Для добавления нового пользователя необходимо воспользоваться пиктограммой  «Добавить», а для удаления  «Удалить».

Для переключения между страницами используются пиктограммы кнопок вперед/назад  и . Для прокрутки в начало и конец списка используются пиктограммы  и .

Для обновления списка используется пиктограмма кнопки «Обновить» .

При добавлении нового пользователя открывается форма «Пользователь» (Рисунок 5). Обязательными для заполнения полями являются: «ФИО», «Логин» и «Роль».

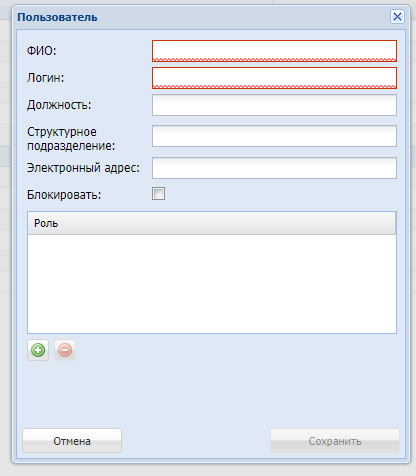


Рисунок 5 – Форма «Пользователь»

Для добавления роли пользователи на форме необходимо выбрать одну из нескольких ролей, существующих в Интеграционной шине (Рисунок 6).

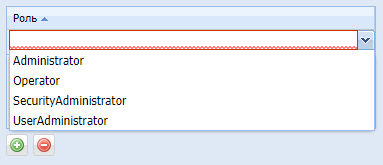


Рисунок 6 – Роли

### Управление прикладными системами, взаимодействующими между собой и с системами ФОИВ посредством Интеграционной шины

Управление прикладными системами, взаимодействующими между собой и с системами ФОИВ посредством Интеграционной шины, осуществляется средствами Модуля администрирования Интеграционной шины.

Прикладные системы, взаимодействующие между собой и с системами ФОИВ посредством Интеграционной шины, являются абонентами Интеграционной шины.

Пользователь с ролью Главный администратор имеет права на создание, модификацию и удаление абонентов системы.

При входе в интерфейс администратора по умолчанию открывается экранная форма «Модуль администрирования» на вкладке «Абоненты» (Рисунок 7).



Рисунок 7 – «Модуль администрирования»

В Интеграционной шине существует два типа абонентов:

1. синхронный;
2. абонент MQ.

При создании синхронного абонента обязательными для заполнения являются поля: «Наименование», «Логический адрес» и «Аутентификация».

Главному администратору доступны кнопки «Сохранить» и «Отмена», предусмотрена возможность вносить изменения в текстовые поля.

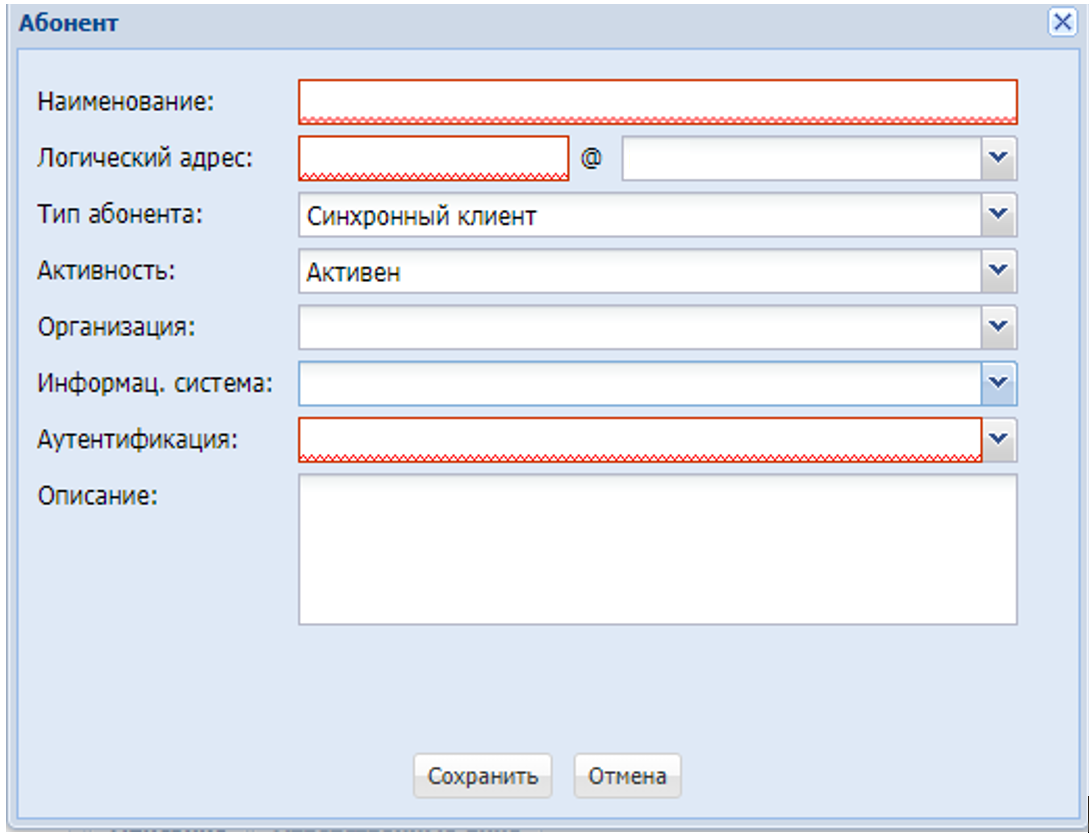


Рисунок 8 – Синхронный абонент

При создании абонента MQ обязательными для заполнения полями являются: «Наименование», «Логический адрес», «Физический адрес», «Аутентификация» (Рисунок 9).

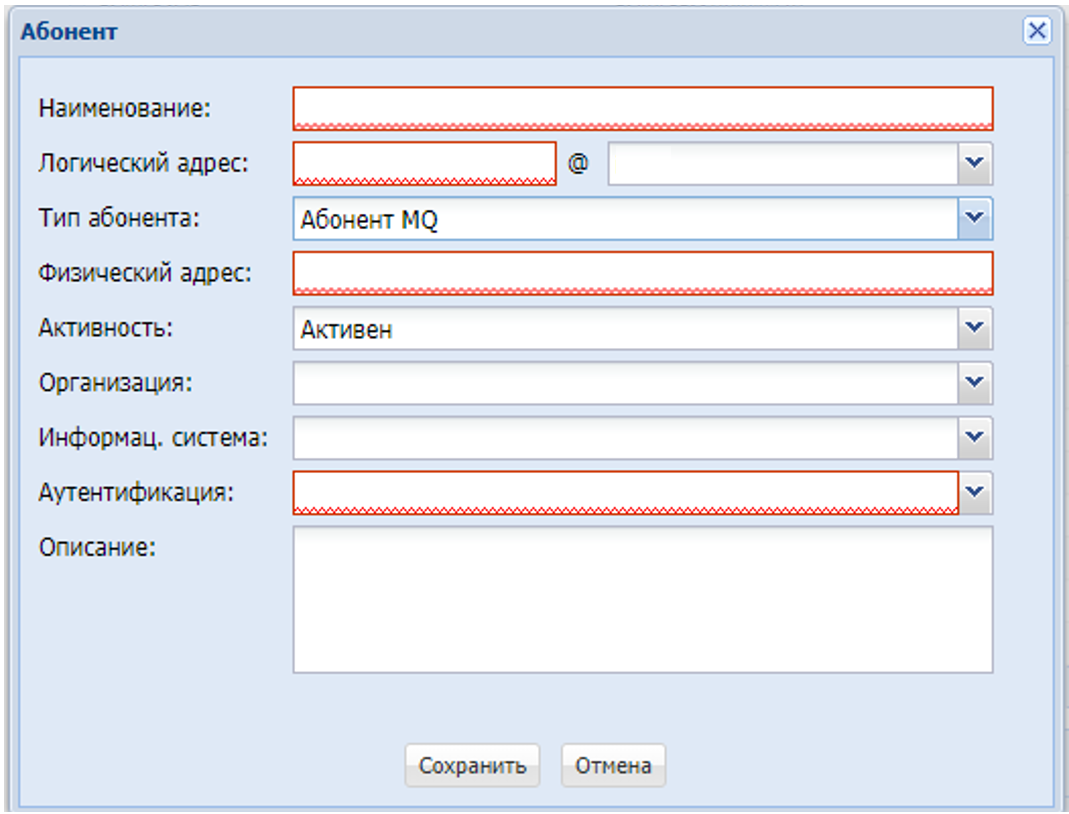


Рисунок 9 – Абонент MQ

При выделении абонента в общем списке абонентов двойным щелчком мыши доступна возможность редактирования полей абонента (Рисунок 10).

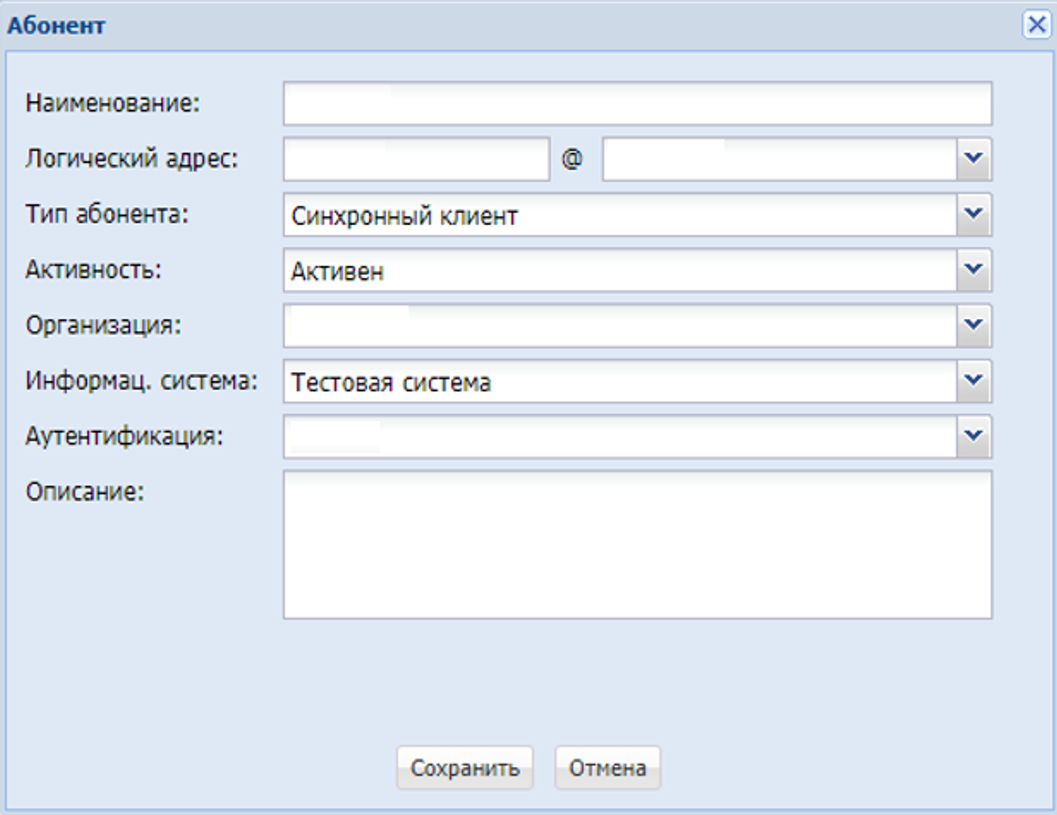


Рисунок 10 – Редактирование карточки абонента

### Введение перечня ФОИВ и информационных систем

Управление перечнем ФОИВ и информационными системами осуществляется средствами Модуля администрирования Интеграционной шины.

Пользователь с ролью Главный администратор имеет права на создание, модификацию и удаление организаций и информационных систем.

На вкладке «Организации и инф. системы» представлены системы, участвующие в межведомственном взаимодействии (Рисунок 11).

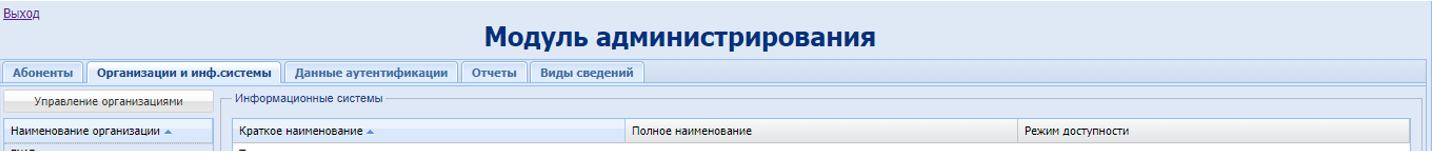


Рисунок 11 – Вкладка «Организации и инф. системы»

При добавлении новой системы открывается форма «Информационная система» (Рисунок 12). Обязательным для заполнения полем является «Краткое наименование» и «Организация».

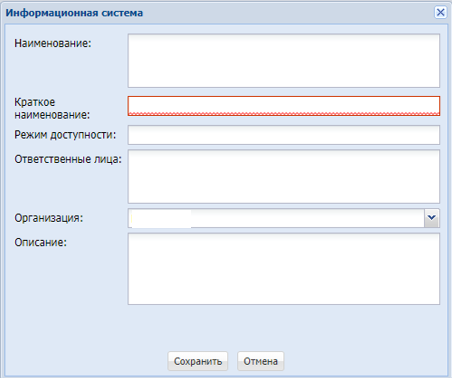


Рисунок 12 – Вкладка «Информационная система»

Для взаимодействия прикладных систем с информационными системами ФОИВ посредством СМЭВ используются электронные сообщения, в которых указывается вид сведений.

На вкладке «Виды сведений» реализована возможность добавления, редактирования и удаления вида сведений для каждой организации (Рисунок 13).

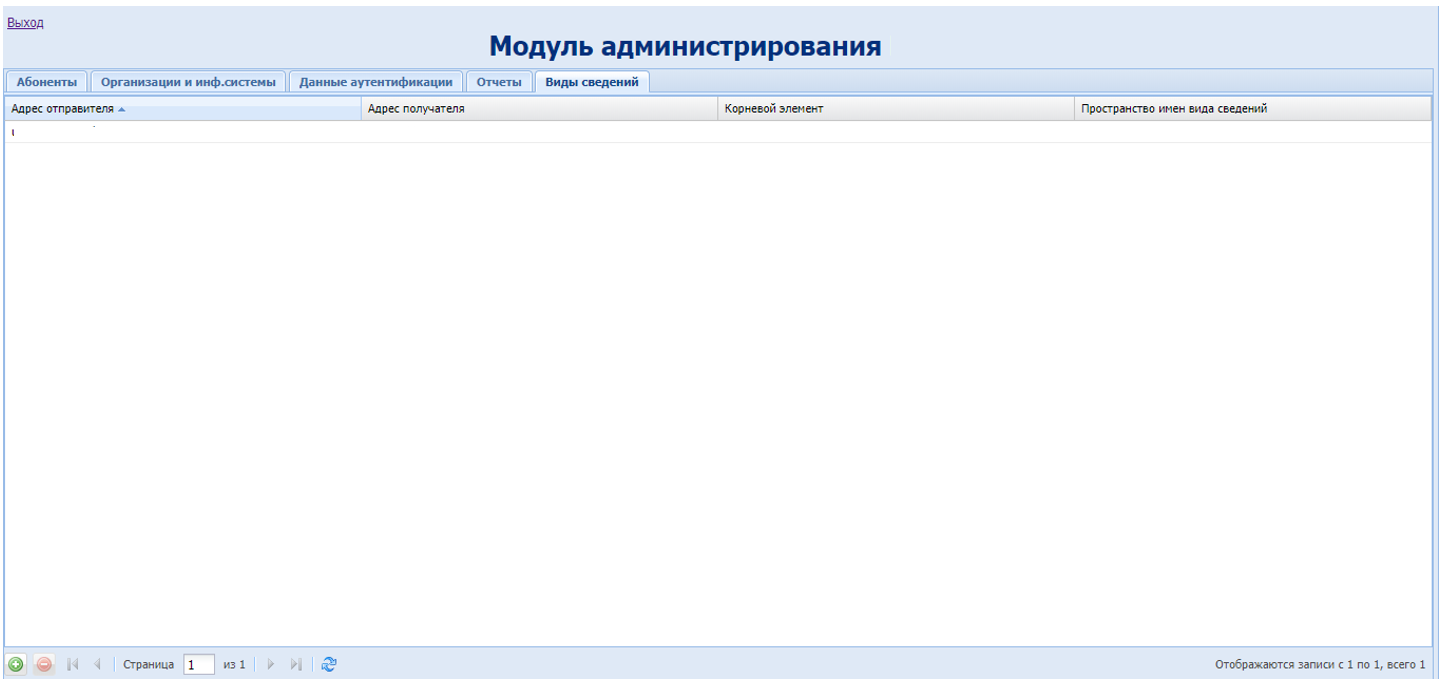


Рисунок 13 – Вкладка «Виды сведений»

Для добавления нового вида сведений используется форма «Вид сведений» (Рисунок 14). Обязательными для заполнения являются поля: «Адрес отправителя» и «Адрес получателя».

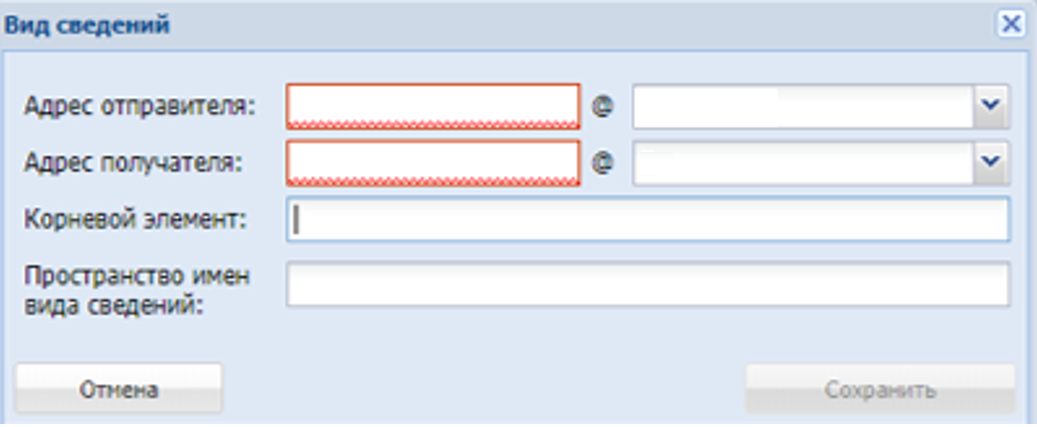


Рисунок 14 – Форма создания «Вид сведений»

### Протоколирование действий пользователей

Протоколирование действий пользователей осуществляется Модулем администрирования и Модулем мониторинга Интеграционной шины.

Просмотр протоколов действий пользователей осуществляется в Модуле администрирования Интеграционной шины. Права на просмотр действий пользователей доступны пользователю с ролью Администратор безопасности.

В интерфейсе Администратора безопасности предусмотрена вкладка «Отчеты». В указанном разделе предусмотрено формирование отчетов по нескольким видам с возможностью выбора периода формирования отчета и выгрузки в формате EXCEL (Рисунок 15).

В разделе предусмотрены следующие виды отчетов:

1. Отчет о работе пользователей.
2. Отчет по объектам доступа.
3. Отчет активности работы пользователей.
4. Отчет по списку пользователей.
5. Отчет о доступе пользователей.
6. Отчет о назначенных правах учетной записи.
7. Отчет о работе структурных подразделений.

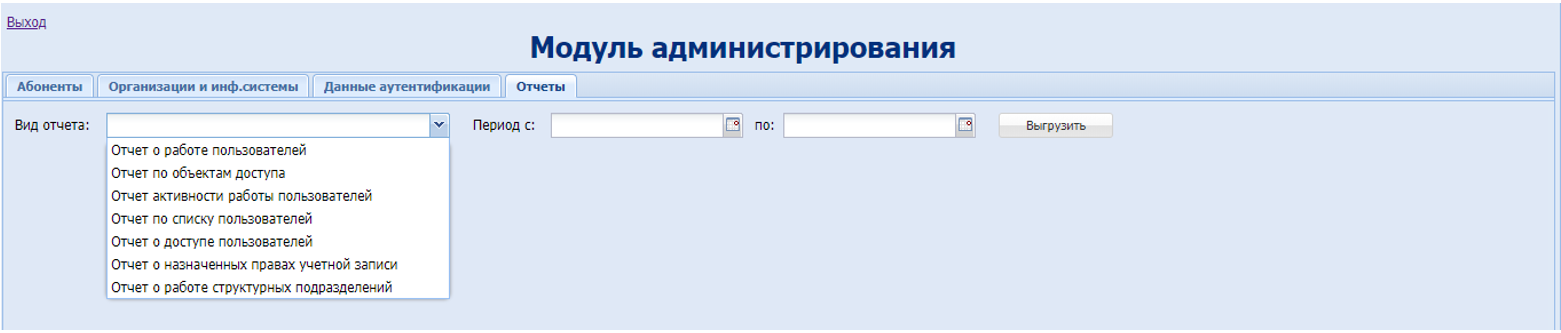


Рисунок 15 – Вкладка «Отчеты»

### Мониторинг работоспособности сервисов Интеграционной шины

Мониторинг работоспособности сервисов Интеграционной шины осуществляется средствами встроенного в Модуль администрирования Интеграционной шины сервиса мониторинга, описание работы с которым содержится в разделе 4.2.

### Работа с сервером приложений Tomcat

Основные директории сервера приложений Apache Tomcat расположены на узлах Интеграционной шины в корневой папке Tomcat ***/opt/tomcat:***

***bin***– файлы и скрипты для запуска, остановки tomcat;

***conf*** – конфигурационные файлы, главный их которых server.xml;

***lib***– используемые библиотеки;

***logs***– директория для хранения всех логов сервера и работы запущенных приложений;

***webapps***– папка для веб-приложений. По умолчанию Tomcat устанавливает свои приложения с примерами и веб-консоль для настройки

Для изменения порта, на котором запускается Tomcat, необходимо открыть на редактирование файл server.xml в папке conf:

$ nano /opt/tomcat/conf/server.xml

Далее следует найти запись:

<Connector port="8080" protocol="HTTP/1.1"

connectionTimeout="20000"

redirectPort="8443" />

Далее – изменить порт 8080 на желаемый, а затем перезапускаем Tomcat:

$ service tomcat restart

Если Tomcat не доступен на запускаемом порту извне, то необходимо проверить настройки фаервола и открыть порт.

В файле server.xml можно также настроить поддержку SSL/TLS. Для этого необходимо раскомментировать следующие строки:

<Connector port="8443" protocol="org.apache.coyote.http11.Http11AprProtocol"

maxThreads="150" SSLEnabled="true" >

<UpgradeProtocol className="org.apache.coyote.http2.Http2Protocol" />

<SSLHostConfig>

<Certificate certificateKeyFile="conf/localhost-rsa-key.pem"

certificateFile="conf/localhost-rsa-cert.pem"

certificateChainFile="conf/localhost-rsa-chain.pem"

type="RSA" />

</SSLHostConfig>

</Connector>

Более подробно о всех поддерживаемых форматах и параметрах можно найти информацию на официальной странице Tomcat по следующей ссылке:

http://tomcat.apache.org/tomcat-7.0-doc/.

При необходимости настроить права доступа для работы с сервером Tomcat, следует сделать в файле tomcat-users.xml, который находится в папке conf. После внесения изменений следует перезагрузить сервер.

В конфигурационном файле context.xml, расположенном в папке /opt/tomcat/conf/, содержатся логин учетной записи и пароль пользователя LDAP в Active Directory (значение параметра managerPWD тега Resource name = «app/intersec/ldap»). Смена пароля пользователя LDAP должна производиться в соответствии требованиям политики безопасности.

# АВАРИЙНЫЕ СИТУАЦИИ

В случае возникновения аварийной или нештатной ситуации при несоблюдении условий выполнения технологического процесса действия по восстановлению работоспособности и при необходимости восстановлению данных могут производить только администраторы системы Интеграционной шины.

Восстановление Интеграционной шины производится путем повторной установки компонент программного обеспечения и восстановления баз данных из резервных копий в соответствии с разделом 4.1.

ЛИСТ СОГЛАСОВАНИЯ

|  |  |  |
| --- | --- | --- |
| **Должность** | **Подпись** | **Расшифровка** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |