UNLIMITED PRODUCTION

eXpress
Система коммуникаций

Руководство администратора

Том 1. Установка

Сборка 3.42
23.06.2025

Почтовый адрес:	127030, г. Москва, ул. Новослободская, д. 24, стр. 1
Телефон:	+7 (499) 288-01-22
Email:	sales@express.ms
Web:	https://express.ms/

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Руководство предназначено для администраторов изделия «Система коммуникаций «Express» (далее – СК «Express», Express, система). Настоящий том 1 «Руководства администратора» содержит сведения, необходимые для установки и настройки системы.

Служба технической поддержки. Связаться со службой технической поддержки можно по электронной почте support@express.ms. Страница службы технической поддержки на сайте компании «Анлимитед продакшен» https://express.ms/faq/.

Сайт в интернете. Информацию о продукте компании «Анлимитед продакшен» представлена на сайте https://express.ms/.

Ведомость томов «Руководство администратора»:

- Том 1. Руководство администратора. Установка.
- Том 2. Руководство администратора. Эксплуатация сервера CTS.
- Том 3. Руководство администратора. Эксплуатация сервера ETS.
- Том 4. Руководство администратора. Установка и эксплуатация сервера RTS (поставляется по запросу).

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Термин	Определение
AD	Active Directory — служба каталогов корпорации Microsoft для операционных систем семейства Windows Server
API	Application programming interface — интерфейс для взаимодействия программ и приложений
APNS	Apple Push Notification Service — сервис push-уведомлений Apple
botX	Платформа для разработки чат-ботов
CTS	Corporate Transport Server — корпоративный сервер
ETS	Enterprise Transport Server — сервер предприятия
FCM	Firebase Cloud Messaging — служба, которая упрощает обмен сообщениями между мобильными приложениями и серверных приложений
JSON	Текстовый формат обмена данными, основанный на JavaScript
NTLM	Протокол сетевой аутентификации, разработанный фирмой Microsoft для Windows NT
RTS	Regional Transport Server — региональный сервер
SIEM	Security information and event management — управление информацией о безопасности и событиями безопасности
Single CTS	Единый корпоративный сервер
SIP	Session Initiation Protocol — протокол передачи данных, описывающий способ установки и завершения пользовательского интернет-сеанса, включающего обмен мультимедийным содержимым (IP-телефония, видео- и аудиоконференции, мгновенные сообщения)
SmartApp	Это веб-приложение, реализованное в виде надстройки, исполняемое внутри приложения, для доступа к корпоративным сервисам и системам
SMTP	Сетевой протокол, предназначенный для передачи электронной почты в сетях TCP/IP
SSL	Криптографический протокол для безопасной связи
STUN	Сетевой протокол для определения внешнего IP-адреса, используемый для установления соединения UDP между двумя хостами в случае, если они оба находятся за маршрутизатором NAT
TLS	Протокол защиты транспортного уровня
TTS	TTS — Transport transfer server, транспортный сервер. Сервер, предназначенный для передачи сообщений между корпоративными серверами вместо RTS, в том числе между CTS, у которых отсутствует трастовое соединение друг с другом (нетрастовыми CTS)
TURN	Протокол для получения входящих данных через TCP или UDP соединения
VAPID-ключи	Voluntary Application Server Identification — пара ключей: открытый и закрытый. Закрытый ключ сервер хранит в тайне, а открытый передает клиенту. Ключи позволяют сервису push-уведомлений знать о том, какой сервер приложения подписал пользователя, и быть уверенным в том, что это — тот же самый сервер, который отправляет уведомления конкретному пользователю
АТС	Автоматическая телефонная станция компании
Виджет	Конструктивный элемент панели, отвечающий за визуальный вывод части информации, собранной системой
ВКС	Видеоконференцсвязь
Кеш	Промежуточный буфер с быстрым доступом, содержащий информацию, которая может быть запрошена с наибольшей вероятностью
КСПД	Корпоративная сеть передачи данных
ПДС	Платформа доверенных сервисов
ПК	Персональный компьютер
Разделенный CTS	Разделенный корпоративный сервер: Front CTS и Back CTS
Роутинг	Сетевой сегмент, в котором существует чат (корпоративный, публичный, смешанный)
Траст	Сервис для передачи данных между CTS и RTS и другими сервисами, входящими в их сетевой сегмент

Глава 1

ОБЩИЕ СВЕДЕНИЯ

НАЗНАЧЕНИЕ СИСТЕМЫ

СК «Express» предназначена для предоставления качественной и непрерывной связи между сотрудниками компании и снижения рисков утечек информации за счет перемещения каналов обмена из сети Интернет в периметр локальных вычислительных сетей Компании.

ОСНОВНЫЕ ФУНКЦИИ

СК «Express» реализует следующие основные функции:

- быстрый обмен пользователей текстовыми сообщениями и файлами с помощью мобильных устройств и веб-клиента на ПК в рамках персональных и групповых чатов;
- обеспечение безопасного хранения и передачи конфиденциальных данных;
- создание копии данных для восстановления работоспособности подсистемы в случае ее повреждения или разрушения;
- оптимизация использования ресурсов;
- осуществление персональных и групповых аудио- и видеозвонков;
- запись звонков и видеоконференций.

ОСНОВНЫЕ КОМПОНЕНТЫ

СК «Express» предусматривает три сетевых сегмента взаимодействия пользователей (которые могут поставляться в трех исполнениях):

- публичный (внешний);
- предприятия (внутренний сетевой сегмент компании, объединяющий несколько внутренних серверов);
- корпоративный (внутренний).

Публичный (внешний) сетевой сегмент взаимодействия пользователей используется:

- для первичной регистрации пользователей;
- отправки push-уведомлений;
- обмена сообщениями и файлами с пользователями, не подключенными к какому-либо внутреннему сетевому сегменту;
- совершения звонков пользователями, не подключенными к какому-либо внутреннему сетевому сегменту;
- маршрутизации сообщений и файлов между внутренними сетевыми сегментами, не имеющими прямых доверенных подключений.

Сетевой сегмент предприятия (внутренний сетевой сегмент компании) используется:

- для регистрации пользователей;

- отправки push-уведомлений;
- маршрутизации сообщений и файлов между корпоративными сетевыми сегментами, не имеющими прямых доверенных подключений.

Корпоративный (внутренний) сетевой сегмент взаимодействия пользователей используется:

- для регистрации корпоративных пользователей;
- обмена сообщениями, файлами и совершения звонков с пользователями компании;
- предоставления корпоративной адресной книги;
- маршрутизации сообщений и файлов между корпоративным сетевым сегментом компании и корпоративными сетевыми сегментами партнеров, с которыми установлены доверенные подключения.

СК «Express» включает следующие отдельно устанавливаемые компоненты:

- региональный сервер Express (далее — RTS);
- сервер предприятия (далее — ETS);
- корпоративный сервер Express (далее — CTS);
- сервер Media;
- Bot Server;
- мобильное приложение;
- десктоп-приложение;
- веб-приложение.

Внимание! Для полноценной работы всех описанных функций версия приложения и серверной части должны совпадать.

RTS, ETS и CTS являются основными элементами в структуре системы.

RTS объединяют и обслуживают компьютерные сети внутри одного региона и отвечают за функционирование публичного сетевого сегмента взаимодействия.

ETS объединяют и обслуживают компьютерные сети и корпоративные серверы внутри одной большой компании и отвечают за функционирование сетевого сегмента предприятия.

Под ETS выпускается кастомизированное приложение, которое управляется компанией, использующей ETS. Пользователи CTS, подключенные к ETS, получают СМС и push-уведомления с этого ETS (подробнее см. в документе «Руководство администратора. Том 3. Эксплуатация сервера ETS»).

CTS объединяют и обслуживают клиентские устройства в пределах организации, подключаются к ETS или RTS и выполняют роль посредника между клиентским устройством и ETS/RTS. CTS отвечает за функционирование корпоративного сетевого сегмента. При установленном ETS информационный обмен между корпоративными серверами происходит внутри предприятия, данные с CTS передаются на ETS, ETS осуществляет информационный обмен с внешним сетевым сегментом (подробнее см. в документе «Руководство администратора. Том 2. Эксплуатация сервера CTS»).

Клиентское устройство может подключаться как к CTS, так и к ETS или RTS напрямую. Для каждого сервера пользователь регистрирует свой профиль. В зависимости от активного профиля пользователю доступны свои ресурсы в виде чатов, контактов и истории обмена сообщениями. Подключение клиента к CTS возможно после подключения к RTS или ETS. Все сообщения, переданные между

корпоративными пользователями, хранятся на CTS в зашифрованном виде и не доступны администраторам сервера.

Для обеспечения работы голосовых и видеовызовов используется отдельный сервер Media.

При количестве пользователей 100 и более из сервера Media в отдельный сервер выделяется сервер Transcoding.

Для развертывания чат-ботов и SmartApp используется отдельный сервер (Bot Server).

Для интеграции системы АТС используется модуль SIP-телефонии, который позволяет совершать и принимать голосовые вызовы, вести телефонную книгу и сопоставлять пользователей с номерами АТС («Определитель номера»).

Сопоставление функций и возможностей системы описаны в табл. 1:

табл. 1

Функции	Возможности
Исходящие вызовы	• Совершение голосовых вызовов на АТС с использованием мобильного устройства или ПК; • вызов абонента путем набора номера
Входящие вызовы	Прием голосовых вызовов, поступающих с АТС с использованием мобильного устройства или ПК
Ведение телефонной книги	Интеграция телефонной книги модуля телефонии: • с телефонной книгой устройства, на котором установлен СК «Express»; • записями, сохраненными в СК «Express»; • записями из AD
Определитель номера	Сопоставление номера вызывающего абонента с соответствующим пользователем СК «Express» при поступлении входящего вызова с АТС на устройство с установленным СК «Express». В результате вызываемый пользователь получает информацию о звонящем (имя, аватар и т. п.). При совершении исходящего вызова с устройства с установленным СК «Express» на АТС автоматически определяется вызываемый пользователь и отображается информация о нем

Для интеграции с системами предотвращения утечки данных, обеспечивающих проверку сообщений пользователей на наличие запрещенного контента, используется протокол ICAP (порт TCP/1344).

Управление системой осуществляется с помощью веб-интерфейса администратора, которыйя предоставляет возможности для настройки Express и контроля функционирования приложения.

ДОСТУПНЫЕ РОЛИ

Управление системой осуществляют сотрудники организации, обладающие правами администратора. Административные права системы назначаются иерархически.

Для безопасной и успешной эксплуатации Express определяются следующие роли (табл. 2):

табл. 2

Роль	Права	Тип учетной записи
Администратор	• назначение ролей; • просмотр журнала безопасности; • управление чатами; • управление учетными записями пользователей; • подключение чат-ботов; • управление настройками системы	Внутренний пользователь

Роль	Права	Тип учетной записи
Корпоративный пользователь	• отправка сообщений; • создание чата; • просмотр адресной книги сервера; • подключение к чат-ботам	Внутренний пользователь
Региональный пользователь	• отправка сообщений; • создание чата	Внешний пользователь
Администратор безопасности[1]	• просмотр сообщений в консоли DLP; • просмотр журналов в консоли DLP	Внутренний пользователь

Тип учетной записи зависит от положения сервера, на котором авторизован пользователь. Если в защитном сетевом сегменте находится RTS, то региональный пользователь становится внутренним.

СК «Express» предусматривает создание администраторов с ограниченными правами для решения конкретных задач.

Задачи администраторов:

- установка и управление обновлениями общесистемного и прикладного ПО;
- настройка, поддержка в работоспособном состоянии и мониторинг работы серверного оборудования;
- управление резервным копированием и восстановление данных;
- централизованная настройка мобильного приложения;
- управление учетными записями пользователей.

На сервере CTS в рамках ролевой модели для отдельных групп пользователей администратор может устанавливать ограничения для пользователей на операции с вложениями:

- запрет на отправку/пересылку вложений в чаты;
- запрет на загрузку/просмотр вложений в чатах;
- запрет возможности переслать/поделиться/сохранить вложения в память устройства.

Вначале администратор в разделе «Группы пользователей» создает группы пользователей, на которые будут распространятся ограничения, а затем в разделе «Ролевая модель» – правила, которым будут подчиняться ограничения.

Ограничения могут быть установлены для конкретных пользователей или определенных групп в зависимости от принадлежности к серверу (подробнее см. в документе «Руководство администратора. Том 2. Эксплуатация сервера CTS»).

[1] только для пользователей сервера CTS (подробнее см. в документе «Руководство администратора. Том 2. Эксплуатация сервера CTS»)

АРХИТЕКТУРА

Примечание. В данном документе рассматривается не отказоустойчивая конфигурация изделия. Для получения сведений о вариантах отказоустойчивой конфигурации обратитесь к разработчику.

СК «Express» состоит из внешнего сетевого сегмента и внутреннего сетевого сегмента. Связь между внешним и внутренним сетевым сегментом средства в локальной сети осуществляется с помощью специального сервиса — траста. Внешний сетевой сегмент состоит из регионального сервера (RTS), внутренний сетевой сегмент состоит из корпоративного сервера (CTS) или сервера предприятия (ETS) и CTS, которые к нему подключаются.

Серверная часть Express основана на микросервисной архитектуре с использованием контейнеризации на основе Docker. Данное решение позволяет максимально автоматизировать развертывание и обновление серверного ПО Express.

CTS поддерживает два вида развертывания:

- единый корпоративный сервер (Single CTS);
- разделенный корпоративный сервер (Front CTS и Back CTS).

ETS поддерживает два вида развертывания:

- единый сервер ETS и единый сервер Express (Single CTS);
- единый сервер ETS и разделенный сервер Express (Front CTS и Back CTS).

Сервер аудиовидеосвязи (Media) размещается в сети Интернет или в демилитаризованной сетевой зоне компании.

При количестве пользователей 100 и более из сервера Media в отдельный сервер выделяется сервер Transcoding. Сервер Transcoding размещается во внутренней сети компании.

Сервер чат-ботов (Bot Server) размещается во внутренней сети компании и предназначен для размещения чат-ботов и необходимых компонентов для их функционирования, например баз данных. Соединение с Bot-сервером выполняются с помощью docker-контейнера botx.

РЕГИОНАЛЬНЫЙ СЕРВЕР

Важно! Установка и настройка сервера RTS производится исключительно сотрудниками компании-разработчика. Информация о сервере RTS в настоящем документе носит ознакомительный характер.

Для всех вариантов развертывания системы региональный сервер (RTS) размещается в сети Интернет и содержит в себе следующие контейнеры:

- admin (интерфейс администратора);
- audit (сервис аудита подключений);
- authentication_service (отвечает за авторизацию на RTS);
- conference_bot (бот для уведомлений о предстоящих конференциях; отправляет ссылку на сохраненную запись при совершении личных звонков);
- email_notifications (отвечает за рассылку e-mail сообщений с кодом аутентификации);
- etcd (дополнение к settings, отвечает за хранение настроек сервисов);
- events (сервис информирования пользователей о событиях в чатах);

- file_service (сервис загрузки файлов);
- kafka (диспетчер сообщений между сервисами);
- kafka_exporter (отвечает за снятие метрик с kafka);
- kdc (хранилище ключей);
- messaging (сервис обмена сообщениями, отвечает за подключение клиентов через протокол websocket);
- nginx (веб-сервер, который отвечает за маршрутизацию внутренних подключений);
- notifications_bot (бот для отправки сообщений в глобальный чат);
- phonebook (адресная книга);
- postgres (основная база данных сервисов);
- postgres_exporter (отвечает за снятие метрик с postgres);
- preview_service (сервис предпросмотра страниц, на которые отправлены ссылки);
- prometheus (отвечает за снятие, обработку и хранение метрик сервисов);
- push_service (сервис отправки push-уведомлений);
- redis (KV-хранилище);
- redis_exporter (отвечает за снятие метрик с redis);
- routing_schema_service (сервис построения схем роутинга, визуализирует схему маршрутизации в чатах);
- settings (отвечает за хранение настроек сервисов);
- sms_service (сервис для отправки СМС-сообщений);
- stickers (сервис для управления стикерами);
- trusts (отвечает за взаимодействие с ETS и CTS);
- voex (сервис для совершения аудиовызовов);
- docker_socket_proxy (отвечает за просмотр логов контейнеров в интерфейсе администратора);
- traefik (отвечает за прием всех внешних подключений);
- botx (отвечает за интеграцию с ботами);
- metrics_service (сервис сбора индивидуальных показателей).

Состав проекта Media:

- coturn (сервер STUN/TURN);
- janus (сервис для групповых звонков).

Типовая схема развертывания Single CTS, Media и Transcoding изображена ниже (рис. 1).

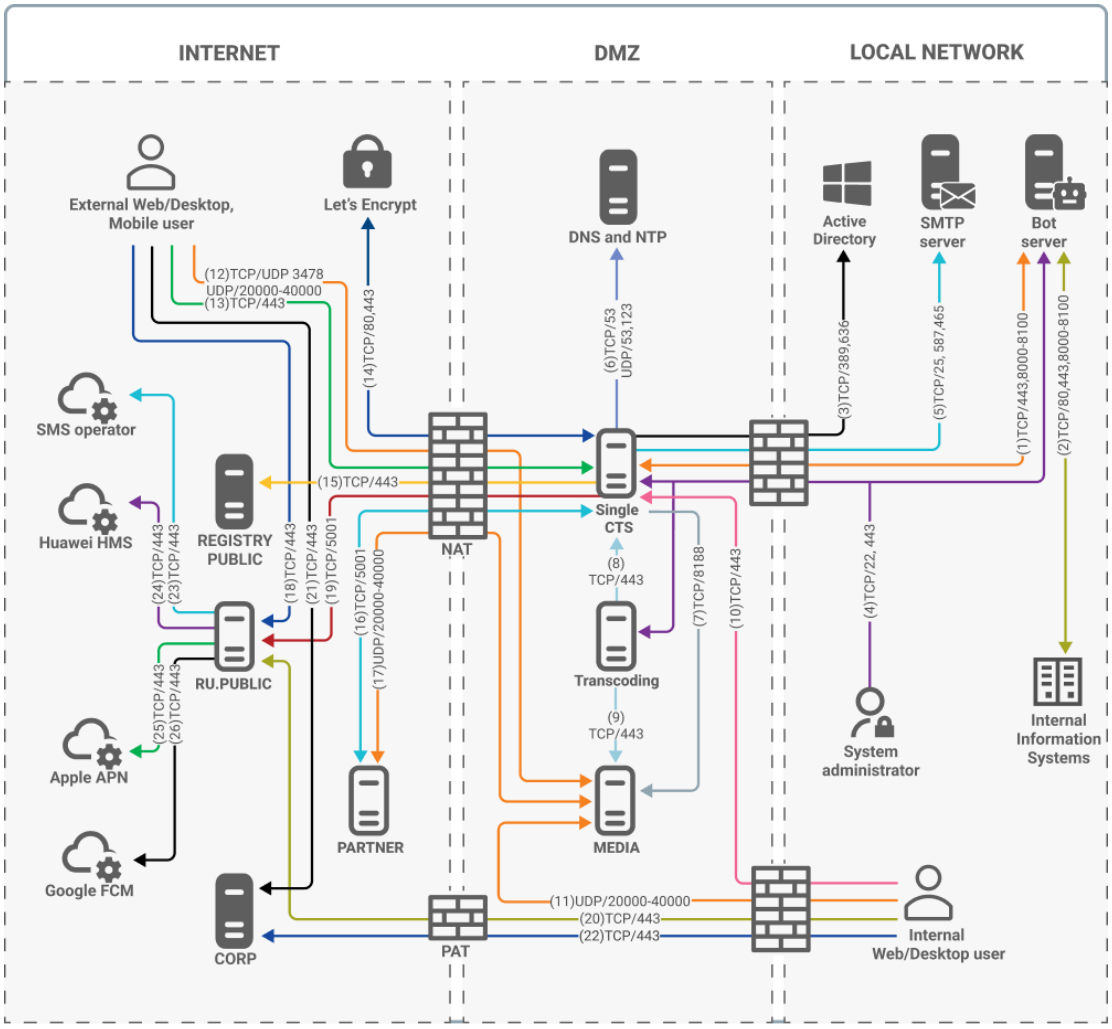

рис. 1. Типовая схема развертывания Single CTS и Media

Внимание! Partner – партнерский сервер CTS, с которым можно установить доверенное соединение. Он расположен в локальной сети другой организации или сети интернет. Пользователи такого сервера принимают участие в аудио- и видеозвонках с пользователями CTS сервера, поэтому для обмена медиаданными по протоколу SRTP необходимо открыть соответствующие порты.

Номера сетевых взаимодействий соответствуют номеру строки в Приложении 1.

Сетевая схема взаимодействия с АТС при развертывании Single CTS и сетевые взаимодействия для данной схемы развертывания представлены в Приложении 8.

Single CTS состоит из двух разных проектов: Media и CTS.

Single CTS размещается в демилитаризованной сетевой зоне компании и содержит в себе следующие контейнеры docker:

- ad_integration (интегрируется с Active Directory и другими LDAP-сервисами, отвечает за авторизацию клиента с помощью NTLM и AD);
- admin (интерфейс администратора);

- apigw (сервис информирования пользователей о событиях в чатах);
- audit (сервис аудита подключений);
- botx (отвечает за интеграцию с ботами);
- conference_bot (бот для уведомлений о предстоящих конференциях; отправляет ссылку на сохраненную запись при совершении личных звонков);
- corporate_directory (каталог открытых ботов и чатов);
- docker_socket_proxy (отвечает за ограничения доступа к сокету Docker);
- email_notifications (отвечает за рассылку e-mail сообщений с кодом аутентификации);
- etcd (дополнение к settings, отвечает за хранение настроек сервисов);
- events (сервис информирования пользователей о событиях в чатах);
- file_service (сервис загрузки файлов);
- kafka (диспетчер сообщений между сервисами);
- kafka_exporter (отвечает за снятие метрик с kafka);
- kdc (хранилище ключей);
- messaging (сервис обмена сообщениями, отвечает за подключение клиентов через протокол websocket);
- metrics_service (сервис сбора индивидуальных показателей ETS/CTS серверов);
- nginx (веб-сервер, который отвечает за маршрутизацию внутренних подключений);
- notifications_bot (бот для отправки сообщений в глобальный чат);
- phonebook (адресная книга);
- postgres (основная база данных сервисов);
- postgres_exporter (отвечает за снятие метрик с postgres);
- prometheus (отвечает за снятие, обработку и хранение метрик сервисов);
- redis (KV-хранилище)[1];
- redis_exporter (отвечает за снятие метрик с redis);
- routing_schema (сервис построения схем роутинга, визуализирует схему маршрутизации в чатах);
- settings (отвечает за хранение настроек сервисов);
- smartapp_proxy (отвечает за обмен файлами между SmartApp и сервером CTS);
- traefik (отвечает за получение сертификатов от LE и терминация TLS на входе);
- transcoding_manager (управляет процессом кодирования);
- trusts (отвечает за обмен событиями между RTS, ETS и CTS);
- preview_service (сервис предпросмотра страниц, на которые отправлены ссылки);

[1] При установке рекомендуется использовать отдельный системный Redis. Встроенные контейнер Redis предназначен для демонстраций возможностей изделия.

- homescreen (SmartApp, предоставляющий пользователю доступ к единому виртуальному пространству, в котором собраны корпоративные сервисы, реализованы новостная лента и анонсы предстоящих событий);
- stickers (сервис для управления стикерами);
- roles (ролевая модель);
- recordings_bot (бот, который посылает ссылку на файл записи после завершения кодирования);
- voex (сервис для совершения аудиовызовов).

Media размещается в демилитаризованной сетевой зоне компании и содержит в себе следующие контейнеры docker:

- coturn (STUN/TURN сервис);
- janus (сервис для групповых звонков).

Transcoding размещается в демилитаризованной сетевой зоне компании и содержит в себе контейнер transcoding (отвечает за перекодировку записи в выходной формат).

Отдельно поставляется DLPS-сервис, он состоит из контейнеров:

- dlps (DLP-система);
- nginx (веб-сервер, который отвечает за маршрутизацию внутренних подключений);
- traefik (отвечает за получение сертификатов от LE и терминация TLS на входе);
- prometheus (отвечает за снятие, обработку и хранение метрик сервисов).

Отдельно поставляется сервис ссылок, он состоит из контейнеров:

- link (отвечает за перенаправление пользователя в чат, канал, конференцию, звонок);
- traefik (отвечает за получение сертификатов от LE и терминацию TLS на входе).

РАЗДЕЛЕННЫЙ КОРПОРАТИВНЫЙ СЕРВЕР

Типовая схема развертывания Front CTS, Media, Transcoding и Back CTS изображена ниже (рис. 2).

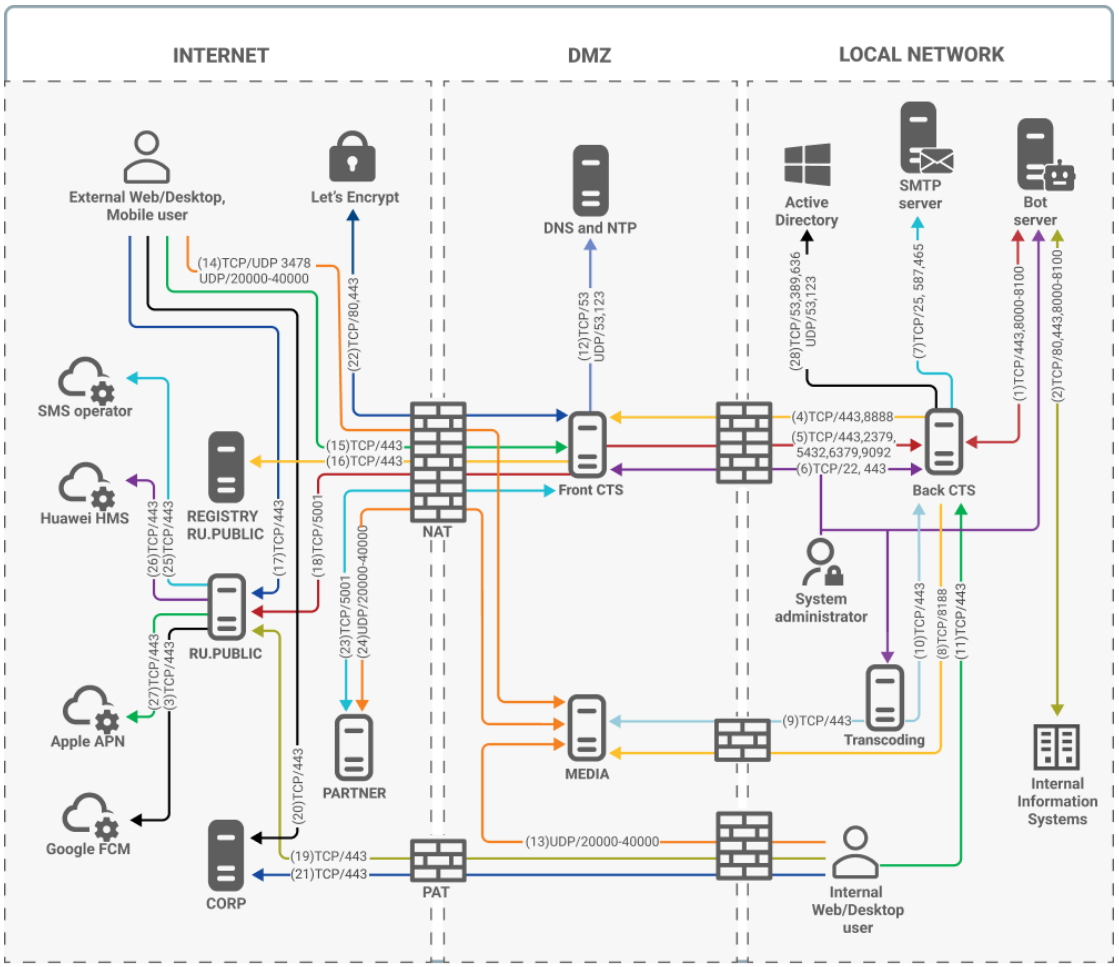

рис. 2. Типовая схема развертывания разделенного CTS (Front/Media/Back)

Внимание! Partner – партнерский сервер CTS, с которым можно установить доверенное соединение. Он расположен в локальной сети другой организации или сети интернет. Пользователи такого сервера принимают участие в аудио- и видеозвонках с пользователями CTS сервера, поэтому для обмена медиаданными по протоколу SRTP необходимо открыть соответствующие порты.

Номера сетевых взаимодействий соответствуют номеру строки в Приложении 2.

Разделенный сервер состоит из Front CTS и Back CTS серверов.

Сетевая схема взаимодействия с АТС при развертывании Front CTS + Media и Back CTS и сетевые взаимодействия для данной схемы развертывания представлены в Приложении 9.

Front CTS состоит из двух разных проектов: Media и CTS.

Front CTS-сервер размещается в демилитаризованной сетевой зоне компании и содержит в себе следующие контейнеры docker:

- nginx (веб-сервер, который отвечает за маршрутизацию внутренних подключений);
- prometheus (отвечает за снятие, обработку и хранение метрик сервисов);

- traefik (отвечает за получение сертификатов от LE и терминация TLS на входе);
- trusts (обеспечивает взаимодействие с сервером ETS/RTS и другими доверенными корпоративными CTS).

Back CTS-сервер размещается в локальной сети компании и содержит в себе следующие контейнеры docker:

- ad_integration (интегрируется с Active Directory и другими LDAP-сервисами, отвечает за авторизацию клиента с помощью NTLM и AD);
- admin (интерфейс администратора);
- audit (сервис аудита подключений);
- apigw (сервис информирования пользователей о событиях в чатах);
- botx (отвечает за интеграцию с ботами);
- conference_bot (бот для уведомлений о предстоящих конференциях; отправляет ссылку на сохраненную запись при совершении личных звонков);
- corporate_directory (каталог открытых ботов и чатов);
- docker_socket_proxy (отвечает за ограничения доступа к сокету Docker);
- email_notifications (отвечает за рассылку e-mail сообщений с кодом аутентификации);
- etcd (дополнение к settings, отвечает за хранение настроек сервисов);
- events (сервис информирования пользователей о событиях в чатах);
- file_service (сервис загрузки файлов);
- kafka (диспетчер сообщений между сервисами);
- kafka_exporter (отвечает за снятие метрик с kafka);
- kdc (хранилище ключей);
- messaging (сервис обмена сообщениями, отвечает за подключение клиентов через протокол websocket);
- metrics_service (сервис сбора индивидуальных показателей ETS/CTS серверов);
- nginx (веб-сервер, который отвечает за внутреннюю маршрутизацию подключений);
- notifications_bot (бот для отправки сообщений в глобальный чат);
- phonebook (адресная книга);
- postgres (основная база данных сервисов);
- postgres_exporter (отвечает за снятие метрик с postgres);
- prometheus (отвечает за снятие, обработку и хранение метрик сервисов);
- recordings_bot (бот, который посылает ссылку на файл записи после завершения кодирования);
- redis (KV-хранилище)[1];
- redis_exporter (отвечает за снятие метрик с redis);

[1] При установке рекомендуется использовать отдельный системный Redis. Встроенные контейнер Redis предназначен для демонстраций возможностей изделия.

- routing_schema (сервис построения схем роутинга, визуализирует схему маршрутизации в чатах);
- smartapp_proxy (отвечает за обмен файлами между SmartApp и сервером CTS);
- homescreen (SmartApp, предоставляющий пользователю доступ к единому виртуальному пространству, в котором собраны корпоративные сервисы, реализованы новостная лента и анонсы предстоящих событий);
- settings (отвечает за хранение настроек сервисов);
- traefik (отвечает за получение сертификатов от LE и терминацию TLS на входе);
- transcoding_manager (управляет процессом кодирования);
- preview_service (сервис предпросмотра страниц, на которые отправлены ссылки);
- stickers (сервис для управления стикерами);
- roles (ролевая модель);
- voex (сервис для совершения аудиовызовов).

Media размещается в демилитаризованной сетевой зоне компании и содержит в себе следующие контейнеры docker:

- coturn (STUN/TURN сервис);
- janus (сервис для групповых звонков).

Transcoding размещается в локальной сети компании и содержит в себе контейнер transcoding (отвечает за перекодировку записи в выходной формат).

Отдельно поставляется DLPS-сервис, он состоит из контейнеров:

- dlps (DLP-система);
- nginx (веб-сервер, который отвечает за маршрутизацию внутренних подключений);
- traefik (отвечает за получение сертификатов от LE и терминация TLS на входе);
- prometheus (отвечает за снятие, обработку и хранение метрик сервисов).

Отдельно поставляется сервис ссылок, он состоит из контейнеров:

- link (отвечает за перенаправление пользователя в чат, канал, конференцию, звонок);
- traefik (отвечает за получение сертификатов от LE и терминацию TLS на входе).

СЕРВЕР ПРЕДПРИЯТИЯ И ЕДИНЫЙ КОРПОРАТИВНЫЙ СЕРВЕР

Типовая схема развертывания ETS, Single CTS, Media, Transcoding и Web Client изображена ниже (рис. 3).

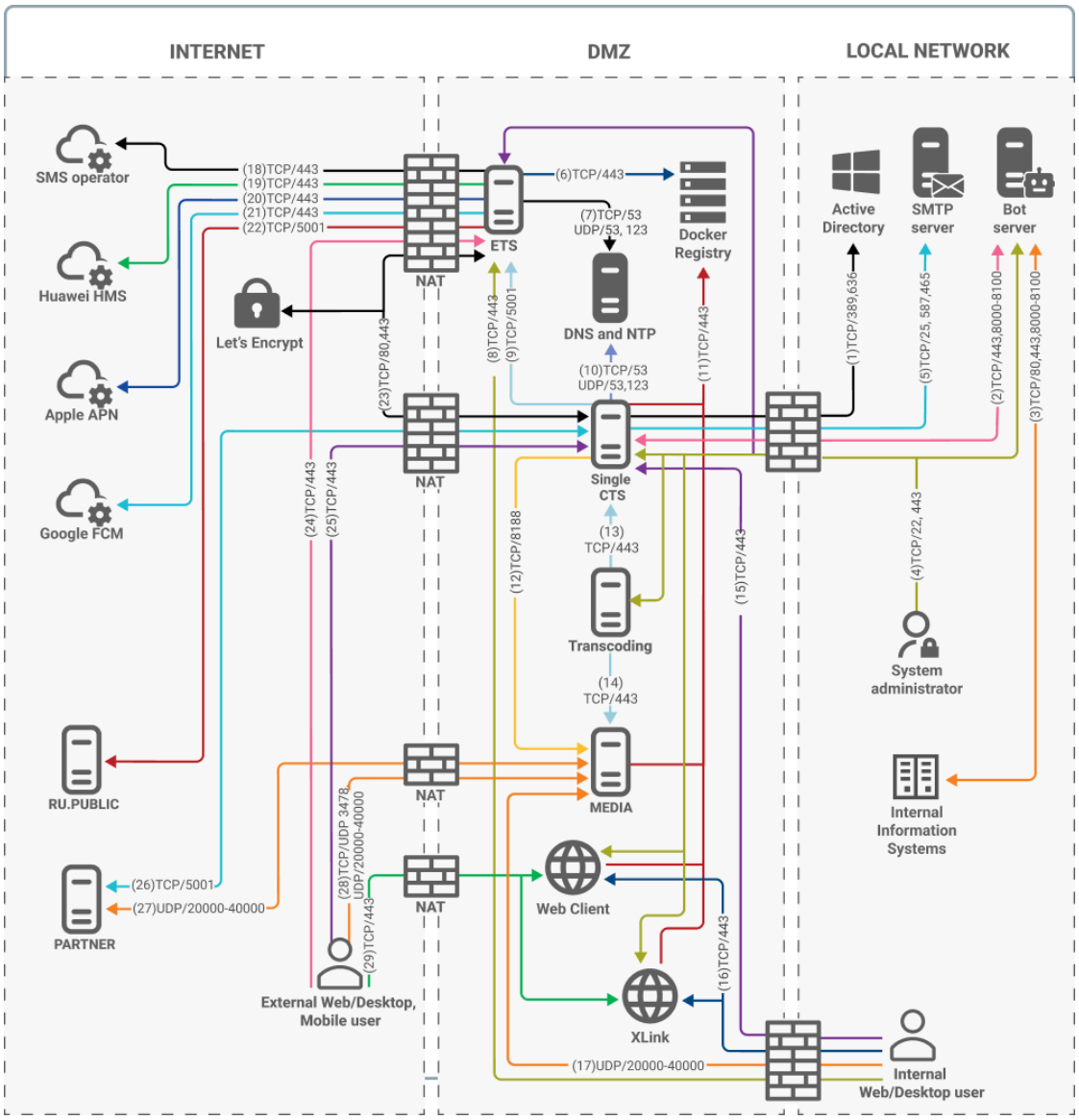

рис. 3. Типовая схема развертывания ETS, Single CTS, Media и Web Client

Внимание! Partner – партнерский сервер CTS, с которым можно установить доверенное соединение. Он расположен в локальной сети другой организации или сети интернет. Пользователи такого сервера принимают участие в аудио- и видеозвонках с пользователями CTS сервера, поэтому для обмена медиаданными по протоколу SRTP необходимо открыть соответствующие порты.

Номера сетевых взаимодействий соответствуют номеру строки в Приложении 3.

Сервер ETS размещается в демилитаризованной сетевой зоне компании и содержит в себе следующие контейнеры:

- audit (сервис аудита подключений);
- admin (интерфейс администратора);
- logstack (централизованная обработка логов);

- authentication_service (отвечает за авторизацию на ETS и RTS);
- botx (отвечает за интеграцию с ботами);
- email_notifications (отвечает за рассылку по электронной почте сообщений с кодом аутентификации);
- etcd (дополнение к settings, отвечает за хранение настроек сервисов);
- events (сервис информирования пользователей о событиях в чатах);
- file_service (сервис загрузки файлов);
- janus (сервис для групповых звонков);
- kafka (диспетчер сообщений между сервисами);
- kafka_exporter (отвечает за снятие метрик с kafka);
- kdc (хранилище ключей);
- messaging (сервис обмена сообщениями, отвечает за подключение клиентов через протокол websocket);
- metrics_service (сервис сбора индивидуальных показателей ETS/CTS серверов);
- nginx (веб-сервер, который отвечает за маршрутизацию внутренних подключений);
- notifications_bot (бот для отправки сообщений в глобальный чат);
- conference_bot (бот для уведомлений о предстоящих конференциях, отправляет ссылку на сохраненную запись при совершении личных звонков);
- phonebook (адресная книга);
- postgres (основная база данных сервисов);
- postgres_exporter (отвечает за снятие метрик с postgres);
- preview_service (сервис предпросмотра страниц, на которые отправлены ссылки);
- prometheus (отвечает за снятие, обработку и хранение метрик сервисов);
- push_service (сервис отправки push-сообщений);
- redis (KV-хранилище)[1];
- redis_exporter (за снятие метрик с redis);
- settings (отвечает за хранение настроек сервисов);
- sms_service (сервис для отправки СМС-сообщений);
- stickers (сервис для управления стикерами);
- traefik (отвечает за получение сертификатов от LE и терминация TLS на входе);
- trusts (отвечает за взаимодействие с RTS и CTS);
- docker_socket_proxy (отвечает за просмотр логов контейнеров в интерфейсе администратора);
- voex (сервис для совершения аудиовызовов).

[1] При установке рекомендуется использовать отдельный системный Redis. Встроенный контейнер Redis предназначен для демонстраций возможностей изделия.

Сервер Web Client размещается в демилитаризованной сетевой зоне компании и содержит в себе следующие контейнеры:

- web_client (сервис web client);
- link (сервис, обеспечивающий работу ссылок на конференции).

Список контейнеров Single CTS, Media и Transcoding представлен в подразделе «Единый корпоративный сервер».

СЕРВЕР ПРЕДПРИЯТИЯ И РАЗДЕЛЕННЫЙ КОРПОРАТИВНЫЙ СЕРВЕР

Типовая схема развертывания ETS, Front CTS, Back CTS, Media, Transcoding и Web Client изображена ниже (рис. 4).

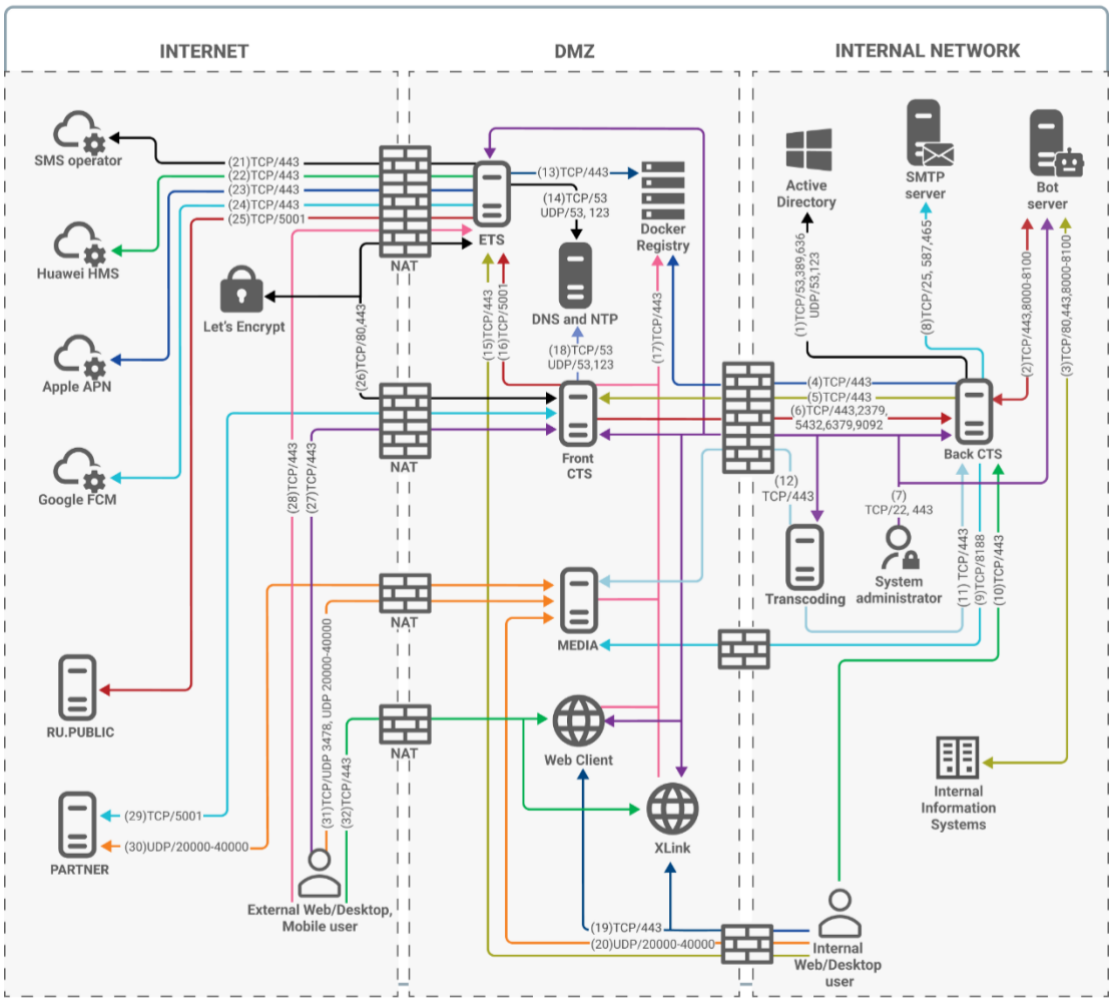

рис. 4. Типовая схема развертывания ETS, Front CTS, Back CTS, Media и Web Client

Внимание! Partner – партнерский сервер CTS, с которым можно установить доверенное соединение. Он расположен в локальной сети другой организации или сети интернет. Пользователи такого сервера принимают участие в аудио- и видеозвонках с пользователями CTS сервера, поэтому для обмена медиаданными по протоколу SRTP необходимо открыть соответствующие порты.

Номера сетевых взаимодействий соответствуют номеру строки в Приложении 4.

Сервер ETS размещается в демилитаризованной сетевой зоне компании и содержит в себе следующие контейнеры:

- audit (сервис аудита подключений);
- admin (интерфейс администратора);
- logstack (централизованная обработка логов);
- authentication_service (отвечает за авторизацию на ETS и RTS);
- botx (отвечает за интеграцию с ботами);
- email_notifications (отвечает за рассылку по электронной почте сообщений с кодом аутентификации);
- etcd (дополнение к settings, отвечает за хранение настроек сервисов);
- events (сервис информирования пользователей о событиях в чатах);
- file_service (сервис загрузки файлов);
- janus (сервис для групповых звонков);
- kafka (диспетчер сообщений между сервисами);
- kafka_exporter (отвечает за снятие метрик с kafka);
- kdc (хранилище ключей);
- messaging (сервис обмена сообщениями, отвечает за подключение клиентов через протокол websocket);
- metrics_service (сервис сбора индивидуальных показателей ETS/CTS серверов);
- nginx (веб-сервер, который отвечает за маршрутизацию внутренних подключений);
- notifications_bot (бот для отправки сообщений в глобальный чат);
- conference_bot (бот для уведомлений о предстоящих конференциях; отправляет ссылку на сохраненную запись при совершении личных звонков);
- phonebook (адресная книга);
- postgres (основная база данных сервисов);
- postgres_exporter (отвечает за снятие метрик с postgres);
- preview_service (сервис предпросмотра страниц, на которые отправлены ссылки);
- prometheus (отвечает за снятие, обработку и хранение метрик сервисов);
- push_service (сервис отправки push-сообщений);
- redis (KV-хранилище)[1];
- redis_exporter (за снятие метрик с redis);
- settings (отвечает за хранение настроек сервисов);
- sms_service (сервис для отправки СМС-сообщений);
- stickers (сервис для управления стикерами);
- traefik (отвечает за получение сертификатов от LE и терминация TLS на входе);

[1] При установке рекомендуется использовать отдельный системный Redis. Встроенные контейнер Redis предназначен для демонстраций возможностей изделия.

- trusts (отвечает за взаимодействие с RTS и CTS);
- docker_socket_proxy (отвечает за просмотр логов контейнеров в интерфейсе администратора);
- voex (сервис для совершения аудиовызовов).

Сервер Web Client размещается в демилитаризованной сетевой зоне компании и содержит в себе следующие контейнеры:

- web_client (сервис web client);
- link (сервис, обеспечивающий работу ссылок на конференции).

Список контейнеров разделенного CTS, Media и Transcoding представлен в подразделе «Разделенный корпоративный сервер».

ТИПЫ АУТЕНТИФИКАЦИИ

СК «Express» поддерживает несколько типов аутентификации:

- с помощью Active Directory;
- с помощью ADLDS;
- с помощью e-mail;
- с помощью Keycloak.

АУТЕНТИФИКАЦИЯ С ПОМОЩЬЮ ACTIVE DIRECTORY

К серверу CTS напрямую (либо через VPN-туннель) подключается контроллер домена Active Directory. Аутентификация пользователя выполняется парой логин/пароль из Active Directory

Поддерживается конфигурация с выгрузкой пользователей из AD. В этом случае аутентификацию нужно выполнить с помощью ПИН-кода, высланного на почту. Такая конфигурация позволяет оперативно влиять на поведение учетной записи в CTS с помощью изменений учетной записи в Active Directory. Например: отключение, просрочка, изменение пароля и исключение из группы выборки учетной записи в Active Directory.

Пример подключения рассматривается на базе типовой схемы развертывания разделенного корпоративного сервера (рис. 5).

Номера сетевых взаимодействий соответствуют номеру строки в Приложении 2.

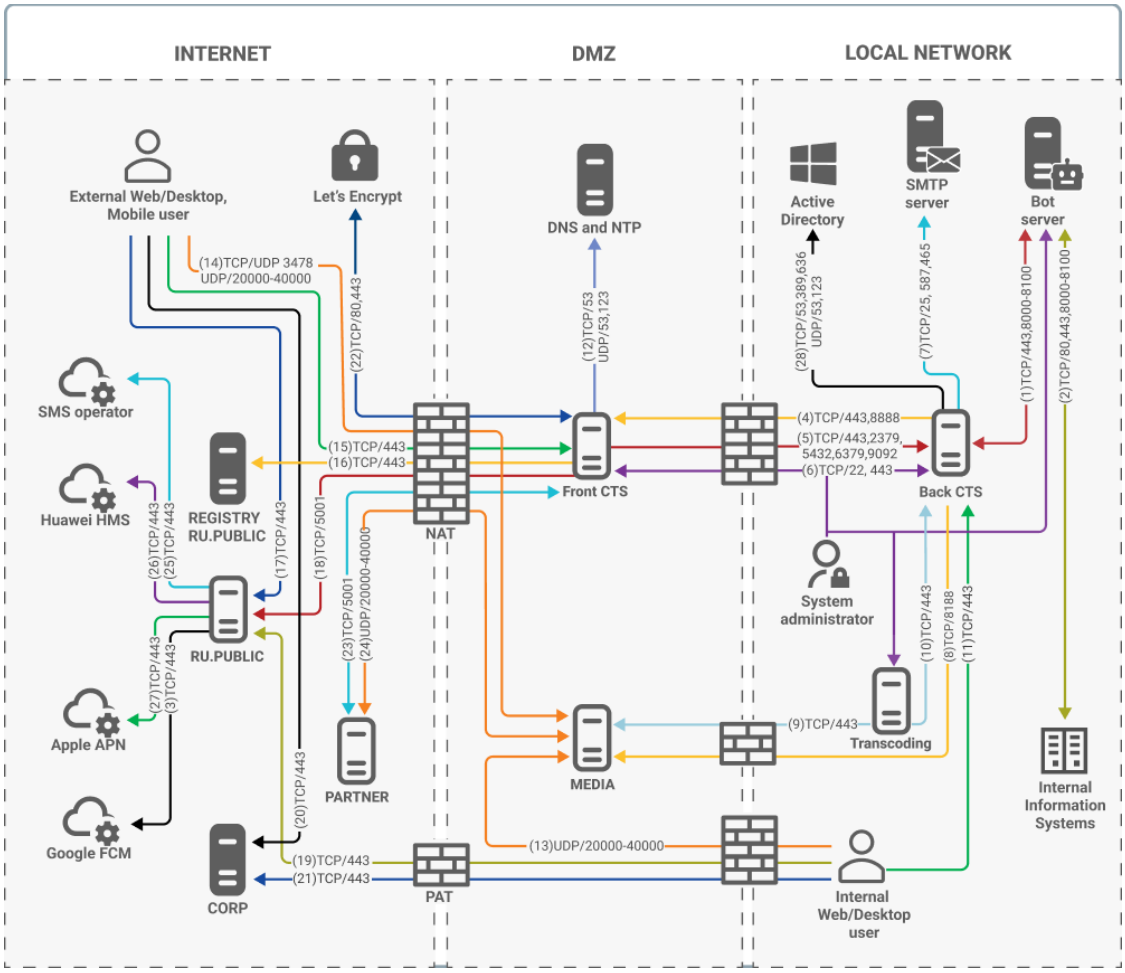

рис. 5

АУТЕНТИФИКАЦИЯ С ПОМОЩЬЮ ADLDS

К серверу CTS подключается сервер с ADLDS. Синхранизация пользователей из контроллера домена Active Directory производится с некоторой периодичностью с помощью специального скрипта. Скрипт предоставляется разработчиком на этапе внедрения.

Аутентификация пользователя выполняется только с помощью отправки ПИН-кода на почту пользователя, указанную в учетной записи в Active Directory. При заведении учетной записи пользователя поля формируются при помощи выгрузки атрибутов по аналогично прямому подключению к Active Directory.

Пример подключения рассматривается на базе типовой схемы развертывания разделенного корпоративного сервера (рис. 6).

Номера сетевых взаимодействий соответствуют номеру строки в Приложении 2.

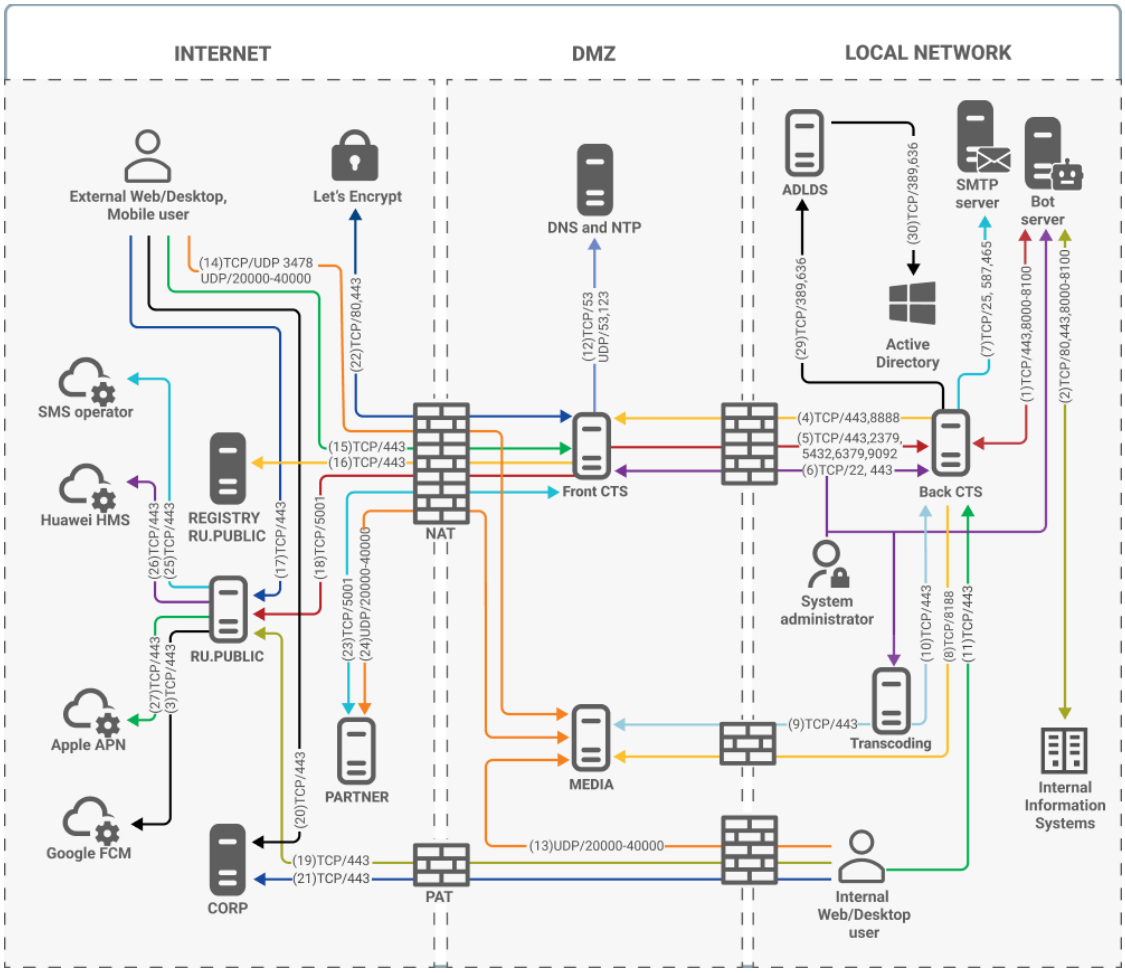

рис. 6

АУТЕНТИФИКАЦИЯ С ПОМОЩЬЮ E-MAIL

Учетные записи пользователей предварительно создаются на сервере CTS вручную администратором или администратор настраивает автоматическое создание пользователей по маске электронной почты.

Пример подключения рассматривается на базе типовой схемы развертывания разделенного корпоративного сервера (рис. 7).

Номера сетевых взаимодействий соответствуют номеру строки в Приложении 2.

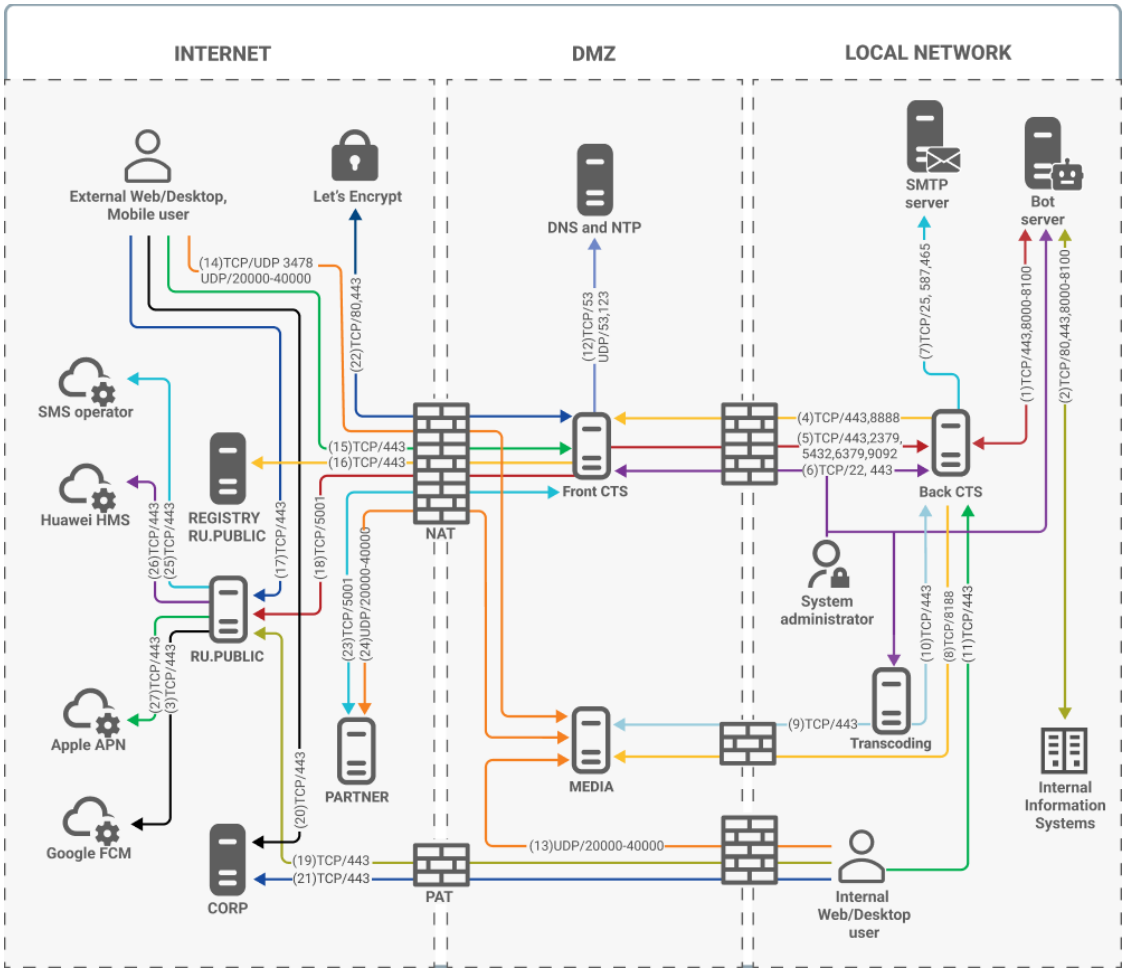

рис. 7

АУТЕНТИФИКАЦИЯ С ПОМОЩЬЮ KEYCLOAK

Данные пользователей заполняются согласно атрибутам учетной записи в Keycloak по аналогии с Active Directory (подробнее о Keycloak см. в Приложении 9).

Служба Keycloak может как подключаться к контроллеру Active Directory или другим источникам данных (например, HR-системы), так и содержать свою собственную базу пользователей.

Пример подключения рассматривается на базе типовой схемы развертывания разделенного корпоративного сервера (рис. 8).

Номера сетевых взаимодействий соответствуют номеру строки в Приложении 2.

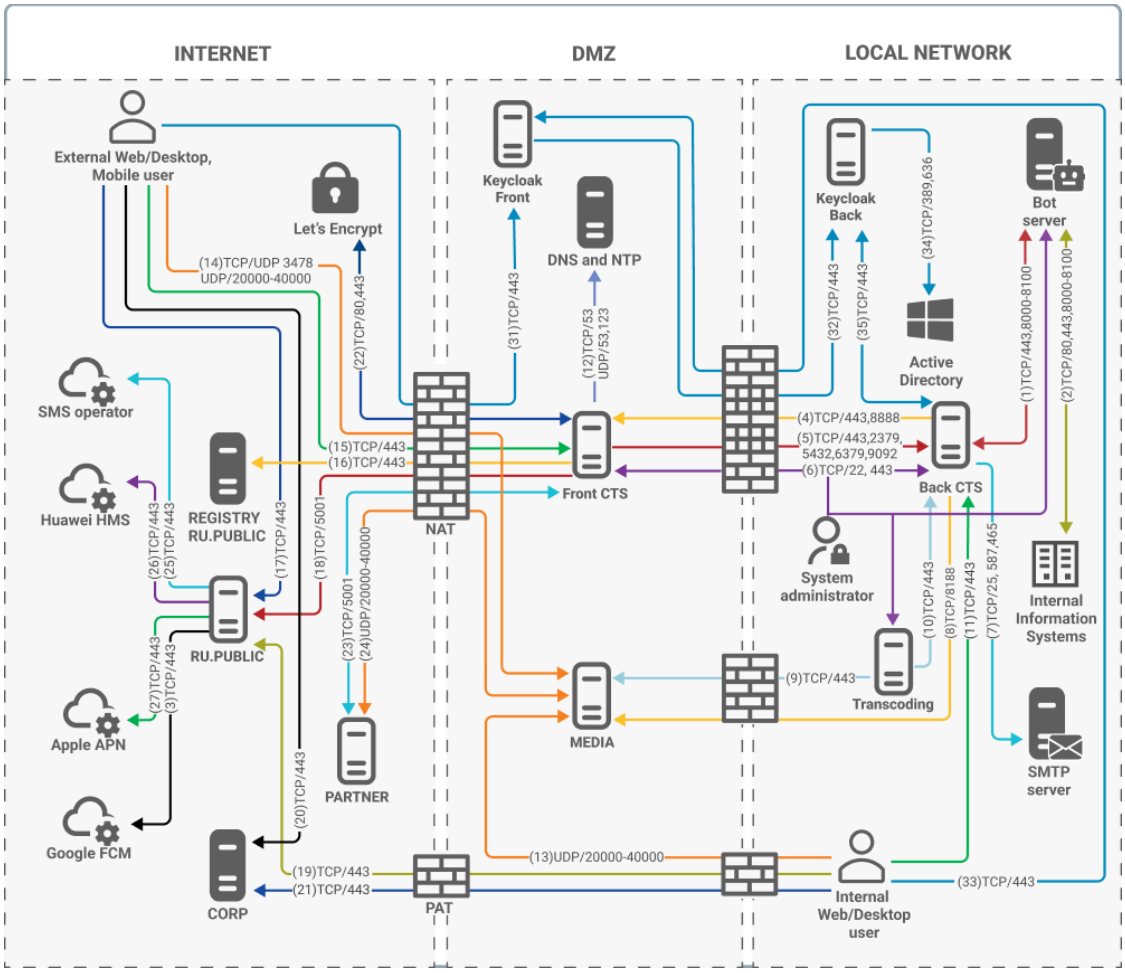

рис. 8

СИСТЕМНЫЕ ТРЕБОВАНИЯ

ТРЕБОВАНИЯ К ПЛАТФОРМЕ

Примечание. В данном подразделе рассматриваются требования к платформе неотказоустойчивой конфигурации из расчета количества пользователей менее 5000. Если предполагается большее количество пользователей, обратитесь за индивидуальным проектом к разработчику.

CTS может быть развернут на аппаратной платформе или в среде виртуализации.

У Front CTS и Media должен быть один сетевой интерфейс с поддержкой IPv6 (необходим для запуска сервисов, маршрутизация трафика IPv6 не требуется).

Расчет сервера Media выполнен из расчета 0.3 CPU на одного участника медиавызова, количество одновременных участников составляет 10% от количества пользователей системы. В случае увеличения количества одновременных участников медиавызовов следует увеличить количество CPU с округлением до целого в большую сторону.

Media содержит компонент обработки записей медиавызовов и конференций, для его работы требуется выделение дополнительных CPU. Количество выделенных CPU влияет на скорость обработки видеозаписей и может быть

увеличено в случае низкой скорости обработки записей. В требованиях ниже учтены необходимые ресурсы для сервиса обработки видеозаписей.

Если планируется более 80 одновременных участников во всех звонках и конференциях, то необходимо развертывать несколько серверов Media для уменьшения количества CPU на одном сервере.

Начиная от 100 пользователей и выше из сервера Media необходимо отдельно выделить сервер Transcoding.

Пропускная способность сети при проведении ВКС для входящего трафика рассчитывается как количество участников, умноженное на 1,5 Мбит/с. Исходящий трафик зависит от типа звонка и раскладки экрана у участников. Если у участников воспроизводится мультиэкран (мозаика), то на каждого участника приходится произведение количества ячеек в мозаике (максимально — 20) на 140 Кбит/с (низкое качество). Для звукового канала необходимо 16 Кбит/с. Демонстрация экрана зависит от характера картинки: для статичных презентаций 30—50 Кбит/с, для динамичных максимальные значения могут достигать 2 Мбит/с на каждого участника.

Важно! Для получения минимальных системных требований при установке сервера Single CTS требуется сложить соответствующие параметры для Front CTS и Back CTS.

табл. 3 – Количество пользователей:100

Роль сервера	vCPU/CPU Core	RAM Гб	SSD Гб	IOps
Front CTS	1	1	45	13
Media	3	2	45	13
Transcoding	2	4	65	13
Back CTS	4	8	211	33
Bot	1	2	65	7
Всего	**11**	**17**	**431**	**79**

табл. 4 – Количество пользователей:200

Роль сервера	vCPU/CPU Core	RAM Гб	SSD Гб	IOps
Front CTS	1	1	45	13
Media	6	4	45	13
Transcoding	2	4	65	13
Back CTS	4	10	358	43
Bot	2	4	85	9
Всего	**15**	**23**	**598**	**91**

табл. 5 – Количество пользователей:300

Роль сервера	vCPU/CPU Core	RAM Гб	SSD Гб	IOps
Front CTS	1	1	45	13
Media	9	4	45	13
Transcoding	3	4	65	13
Back CTS	6	12	504	53
Bot	3	5	105	11
Всего	**22**	**26**	**764**	**103**

табл. 6 – Количество пользователей:400

Роль сервера	vCPU/CPU Core	RAM Гб	SSD Гб	IOps
Front CTS	1	1	45	13
Media	14	8	45	13
Transcoding	4	4	65	13
Back CTS	6	14	651	63

Роль сервера	vCPU/CPU Core	RAM Гб	SSD Гб	IOps
Bot	3	6	100	13
Всего	**28**	**33**	**906**	**115**

табл. 7 – Количество пользователей:500

Роль сервера	vCPU/CPU Core	RAM Гб	SSD Гб	IOps
Front CTS	2	1	45	13
Media	19	10	45	13
Transcoding	4	4	65	13
Back CTS	8	16	797	73
Bot	4	7	145	15
Всего	**37**	**38**	**1097**	**127**

табл. 8 – Количество пользователей:600

Роль сервера	vCPU/CPU Core	RAM Гб	SSD Гб	IOps
Front CTS	2	1	45	13
Media	22	12	45	13
Transcoding	4	4	65	13
Back CTS	8	18	944	83
Bot	4	8	165	17
Всего	**40**	**43**	**1264**	**139**

табл. 9 – Количество пользователей:700

Роль сервера	vCPU/CPU Core	RAM Гб	SSD Гб	IOps
Front CTS	2	1	45	13
Media	25	12	45	13
Transcoding	5	4	65	13
Back CTS	10	18	1090	93
Bot	4	9	185	19
Всего	**46**	**44**	**1430**	**151**

табл. 10 – Количество пользователей:800

Роль сервера	vCPU/CPU Core	RAM Гб	SSD Гб	IOps
Front CTS	2	2	45	13
Media 1	14	8	45	13
Media 2	14	8	45	13
Transcoding	5	4	65	13
Back CTS	10	20	1237	103
Bot	5	10	205	21
Всего	**50**	**52**	**1642**	**176**

табл. 11 – Количество пользователей:900

Роль сервера	vCPU/CPU Core	RAM Гб	SSD Гб	IOps
Front CTS	2	2	45	13
Media 1	17	8	45	13
Media 2	17	8	45	13
Transcoding	6	4	65	13
Back CTS	12	22	1383	103
Bot	5	11	225	21
Всего	**59**	**55**	**1808**	**176**

табл. 12 – Количество пользователей:1000

Роль сервера	vCPU/CPU Core	RAM Гб	SSD Гб	IOps
Front CTS	2	2	45	13
Media 1	18	10	45	13
Media 2	18	10	45	13
Transcoding	6	4	65	13
Back CTS	12	24	1530	123
Bot	6	12	245	25
Всего	**62**	**62**	**1975**	**200**

табл. 13 – Количество пользователей:2000

Роль сервера	vCPU/CPU Core	RAM Гб	SSD Гб	IOps
Front CTS	4	2	45	13
Media 1	24	12	45	13
Media 2	24	12	45	13
Media 3	24	12	45	13
Transcoding	12	4	65	13
Back CTS	16	30	2995	223
Bot	7	14	445	45
Всего	**111**	**86**	**3685**	**333**

табл. 14 – Количество пользователей:3000

Роль сервера	vCPU/CPU Core	RAM Гб	SSD Гб	IOps
Front CTS	6	3	45	13
Media 1	22	12	45	13
Media 2	22	12	45	13
Media 3	22	12	45	13
Media 4	22	12	45	13
Media 5	22	12	45	13
Transcoding	20	4	65	13
Back CTS	20	36	4460	323
Bot	8	16	645	65
Всего	**164**	**119**	**5440**	**479**

табл. 15 – Количество пользователей:4000

Роль сервера	vCPU/CPU Core	RAM Гб	SSD Гб	IOps
Front CTS	8	4	45	13
Media 1	24	12	45	13
Media 2	24	12	45	13
Media 3	24	12	45	13
Media 4	24	12	45	13
Media 5	24	12	45	13
Media 6	24	12	45	13
Transcoding 1	14	4	65	13
Transcoding 2	14	4	65	13
Back CTS	24	42	5924	423
Bot	10	18	845	85
Всего	**214**	**144**	**7214**	**625**

табл. 16 – Количество пользователей:5000

Роль сервера	vCPU/CPU Core	RAM Гб	SSD Гб	IOps
Front CTS	10	5	45	13
Media 1	23	12	45	13

Роль сервера	vCPU/CPU Core	RAM Гб	SSD Гб	IOps
Media 2	23	12	45	13
Media 3	23	12	45	13
Media 4	23	12	45	13
Media 5	23	12	45	13
Media 6	23	12	45	13
Media 7	23	12	45	13
Media 8	23	12	45	13
Transcoding 1	18	4	65	13
Transcoding 2	18	4	65	13
Back CTS	28	48	7364	523
Bot	10	18	1020	105
Всего	**268**	**175**	**8919**	**771**

Примечание. Объем SSD взят из расчета глубины хранения журналов (1 Гб) и пользовательских данных (4 Гб) за 4 года. Данные по требуемому месту могут значительно отличаться от расчетных при более активном использовании изделия.

Для улучшения параметров производительности и совместимости, а также для упрощения обслуживания рекомендуется использовать актуальные на момент установки версии системного ПО.

Минимальные системные требования к серверу CTS для установки подсистем (без отказоустойчивости) (табл. 17):

табл. 17

Элемент	Параметры
Процессор	Количество ядер выбирается согласно табл. 3 — табл. 16, частота не менее 3.60 ГГц
Оперативная память	Количество памяти выбирается согласно табл. 3 — табл. 16
Операционная система	• Ubuntu 22.04 LTS и выше; • CentOS 7 и выше; • Centos Stream 8 и выше; • Debian 12.0 и выше; • RHEL 7.1 и выше; • РЕД ОС 7.2 и выше; • Astra Linux Special Edition 1.6 и выше
Жесткий диск	Не менее 500 Гб
Общесистемное ПО	• Docker-ce версии 20.10.23 и выше; • PostgreSQL версии 14 и выше; • etcd версии 3.5.x и выше; • Kafka версии 2.12 и выше; • Redis версии 7.2.4 и выше
Сетевой адаптер	1 Гб/с

Минимальные системные требования к серверу ETS для установки подсистем (без отказоустойчивости) (табл. 18):

табл. 18

Элемент	Параметры
Процессор	4 ядра, частота не менее 3.60 ГГц
Оперативная память	8 Гб
Операционная система	• Ubuntu 22.04 LTS и выше; • CentOS 7 и выше; • Centos Stream 8 и выше; • RHEL 7.1 и выше; • РЕД ОС 7.2 и выше; • Astra Linux Special Edition 1.6 и выше

Элемент	Параметры
Жесткий диск	Не менее 500 Гб
Общесистемное ПО	• Docker-ce версии 20.10.23 и выше; • PostgreSQL версии 14 и выше; • etcd версии 3.5.x и выше; • Kafka версии 2.12 и выше; • Redis версии 7.2.4 и выше
Сетевой адаптер	1 Гб/с

Минимальные системные требования к серверу RTS для установки подсистем (без отказоустойчивости) (табл. 19):

табл. 19

Элемент	Параметры
Процессор	4 ядра, частота не менее 3.60 ГГц
Оперативная память	16 Гб
Операционная система	• Ubuntu 22.04 LTS и выше; • CentOS 7 и выше; • Centos Stream 8 и выше; • RHEL 7.1 и выше; • РЕД ОС 7.2 и выше; • Astra Linux Special Edition 1.6 и выше
Жесткий диск	Не менее 500 Гб
Общесистемное ПО	• Docker-ce версии 20.10.23 и выше; • PostgreSQL версии 14 и выше; • etcd версии 3.5.x и выше; • Kafka версии 2.12 и выше; • Redis версии 7.2.4 и выше
Сетевой адаптер	1 Гб/с

В составе поставки ПО Express предоставляются компоненты в целях демонстрации функциональности. Их использование в продуктивной среде не рекомендуется. Перед установкой компонентов ПО Express рекомендуется разработать архитектурную схему инсталляций.

Примечание. Разработчик СК «Express» ответственности за использование демонстрационных компонентов в продуктивной среде не несет.

Требование к операционной системе: Серверы CTS, ETC, RTS поддерживают любую ОС семейства Linux, на который устанавливается Docker 20.10.23. Рекомендуется Ubuntu 20.04 LTS или Ubuntu 18.04 LTS.

Примечание. Серверы CTS, ETC, RTS поддерживают ОС Astra Linux 2.12.43 Common Edition «Орел».

Требование к ПО контейнеризации: Docker: 20.10.23 (настоятельно рекомендуется установка из репозитория docker[1]).

Требование к синхронизации времени: Необходим установленный и настроенный локальный сервер NTP с уровнем stratum не ниже 15.

[1] https://docs.docker.com/install/linux/docker-ce/ubuntu/

Для воспроизведения веб-интерфейса рекомендуется использовать браузеры, перечисленные в табл. 20.

табл. 20

Браузер	Версия
Google Chrome	118
Chromium	120
Yandex Browser	23
Firefox	120
Opera	100
Edge	118

ТРЕБОВАНИЯ К DNS

Для корректной работы СК «Express» используется технология Split DNS:

- требуется DNS-имя для сервера CTS, разрешаемое в сети Интернет и ссылающиеся на внешний IP-адрес публикации сервера Single CTS или Front CTS. Рекомендуется имя третьего уровня, например express.mydomain.tld;
- во внутренней сети компании DNS-имя должно разрешаться во внутренний IP-адрес сервера CTS. При использовании раздельной установки (Front + Back CTS) каждому серверу назначается внутреннее DNS-имя, отличное от имени CTS-сервера.

Важно! **Если нет возможности использовать Split DNS, допускается настройка средствами ОС linux (служба systemd-resolved) с преобразованием во внутренней сети компании имен во внутренний IP-адрес.**

Требования к DNS-имени сервера Media аналогичны требованиям к DNS-имени сервера CTS.

ТРЕБОВАНИЯ К СЕРТИФИКАТУ

Для работы изделия требуется оформить сертификат на внешнее имя сервиса Express (FQDN или wildcard), выпущенный публичным доверенным центром сертификации и удовлетворяющий следующим требованиям:

- версия 3 и не ниже TLS 1.2;
- длина ключа не меньше 2048 бит;
- алгоритм подписи SHA 256;
- версия синтаксиса X.509 3;
- незашифрованный закрытый ключ.

Файл должен содержать в себе сертификат сервера, сертификаты промежуточного центра сертификации и корневого центра сертификации. Формат сертификатов должен соответствовать кодировке Base64. Файл закрытого ключа должен содержать нешифрованный закрытый ключ кодировки Base64.

Примерная структура файла сертификата изображена на рисунке ниже (рис. 9).

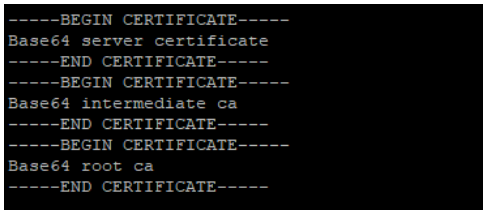

рис. 9

Поддерживается использование бесплатного сертификата от компании Let`s Encrypt.

ТРЕБОВАНИЯ К КОРПОРАТИВНОМУ КАТАЛОГУ LDAP

При интеграции Express с корпоративным каталогом на базе Microsoft Active Directory требуется создание учетной записи с правами «Domain Users» и контейнера «deleted objects»[1].

Стандартной практикой предоставления доступа пользователей к Express является создание группы пользователей Express в Active Directory. Тип группы — «Security», видимость группы — «Universal».

При интеграции Express с корпоративным каталогом на базе LDAP-совместимого сервера требуется создание учетной записи с правами чтения каталога.

При использовании каталога AD LDS авторизация пользователей осуществляется только по ПИН-коду на email.

ТРЕБОВАНИЯ К СЕРВЕРУ SMTP

Для возможности отправки ПИН-кодов аутентификации устройства пользователя требуется создание на почтовом сервер учетной записи, под которой будет производиться отправка электронной почты.

ТРЕБОВАНИЯ К СЕРВЕРУ MEDIA

Сервер Media может быть развернут на аппаратном сервере или в среде виртуализации. Для сервера Media требуется отдельный FQDN и внешний IP, отличные от CTS.

Минимальные системные требования к серверу Media представлены в табл. 21.

табл. 21

Элемент	Параметры
Процессор	Количество ядер выбирается согласно табл. 3 — табл. 16, частота не менее 3.60 ГГц
Оперативная память	Количество памяти выбирается согласно табл. 3 — табл. 16
Операционная система	• Ubuntu 22.04 LTS; • CentOS 7; • Centos Stream 8; • РЕД ОС 7.2 и 7.3; • Astra Linux Special Edition 1.6, 1.7 и 1.8.1
Жесткий диск	Не менее 50 Гб
Общесистемное ПО	Docker-ce версии 20.10.13 или 20.10.23, или 24.0
Сетевой адаптер	Ethernet

[1] https://docs.microsoft.com/ru-ru/troubleshoot/windows-server/identity/non-administrators-view-deleted-object-container

ТРЕБОВАНИЯ К СЕТЕВЫМ ВЗАИМОДЕЙСТВИЯМ

Требования к сетевым взаимодействиям описаны в Приложении 1, Приложении 2, Приложении 3 и Приложении 4.

ТРЕБОВАНИЯ К СЕРВЕРУ ВЕБ-КЛИЕНТ

Сервер Web Client может быть развернут на аппаратном сервере или в среде виртуализации. Минимальные системные требования к серверу Web Client представлены в табл. 22.

табл. 22

Элемент	Параметры
Процессор	2 ядра, частота не менее 3.60 ГГц
Оперативная память	4 Гб
Операционная система	• Ubuntu 22.04 LTS; • CentOS 7; • Centos Stream 8; • RHEL 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9 и 8.0, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8; • РЕД ОС 7.2 и 7.3; • Astra Linux Special Edition 1.6 и 1.7
Жесткий диск	Не менее 50 Гб
Общесистемное ПО	Docker-ce версии 20.10.23
Сетевой адаптер	Ethernet

ТРЕБОВАНИЯ К ХРАНЕНИЮ ФАЙЛОВ ЗАПИСЕЙ ВКС

В процессе записи конференции файлы создаются в максимально доступном качестве и затем сжимаются до расширения 1920x1080 пикселей.

Успешно созданные файлы хранятся на сервере CTS.

На сервере Media хранятся временные файлы, которые удаляются после завершения записи. Если запись не была завершена из-за сбоев или ошибок, файлы хранятся на сервере Media в течение 48 часов.

Для хранения файлов и стабильного процесса записи необходимо обеспечить соответствующий объем памяти на сервере Media и Single/Back CTS.

Приблизительный объем файлов в зависимости от режима записи представлен в табл. 23:

табл. 23

Длительность записи	Описание	Объем файла
10 минут	Аудиозапись. Запись звука с микрофонов участников	9.2 Мб
10 минут	Видеотрансляция. Запись видеотрансляции и звука с микрофонов участников	16.4 Мб
10 минут	Демонстрация экрана. Запись демонстрации экрана и звука с микрофонов участников	53.7 Мб

ТРЕБОВАНИЯ К DLPS

Для обеспечения работы DLPS необходим доступ к следующим объектам и функционалу:

- подсистеме kafka для получения событий «admin-events» и «system-events»;
- API подсистем kdc (БД ключей безопасности) и messaging (БД сообщений);
- базам данных messaging (БД сообщений) и DLP;
- LDAP-серверу при авторизации по LDAP;
- скачиванию файлов.

Требования к сетевой инфраструктуре входящих соединений (табл. 24):

табл. 24

Модуль/сервис	Протокол	Порт
Веб-клиент	TCP	80, 443

Требования к сетевой инфраструктуре исходящих соединений (табл. 25):

табл. 25

Модуль/сервис	Протокол	Порт
Kafka	TCP/UDP	9092/9093
Redis	TCP	6379
Postgresql	TCP	5432
CTS-app	TCP	80, 443

Требования к объему памяти (табл. 26):

табл. 26

Параметр	Значение
Процессор	8 ядер
Оперативная память	8 Гб
Жесткий диск	40 Гб
Пропускная способность сети	1 Гбит/с

Глава 2

УСТАНОВКА

Установка Express включает в себя следующие этапы:

- развертывание сервера ETS:
  1. Предварительная настройка.
  2. Установка сервера предприятия.
  3. Установка веб-клиента (опционально).
  4. Предварительная настройка Media.
  5. Установка сервера Media.
  6. Установка сервера Transcoding (опционально).
  7. Установка корпоративного сервера.
  8. Подключение сервера Media к корпоративному серверу.
  9. Настройка сервера Media.
  10. Установка сервиса ссылок (опционально).
  11. Установка DLPS (опционально).
  12. Установка компонентов записи звонков и конференций (опционально).
  13. Проверка сертификатов (опционально).
  14. Запуск сервера.
  15. Настройка сервера.
- развертывание сервера CTS:
  1. Предварительная настройка.
  2. Предварительная настройка Media.
  3. Установка сервера Media.
  4. Установка сервера Transcoding (опционально).
  5. Установка корпоративного сервера.
  6. Подключение сервера Media к корпоративному серверу.
  7. Настройка сервера Media.
  8. Установка сервиса ссылок (опционально).
  9. Установка DLPS (опционально).
  10. Установка компонентов записи звонков и конференций (опционально).
  11. Проверка сертификатов (опционально).
  12. Запуск сервера.
  13. Настройка сервера.

ПРЕДВАРИТЕЛЬНАЯ НАСТРОЙКА

Для корректной работы сервера выполните предварительную настройку.

Внимание! Установку Express должен осуществлять пользователь Linux с опытом администрирования.

Предварительная настройка зависит от ОС.

ОС UBUNTU/DEBIAN

Для предварительной настройки при использовании ОС Ubuntu/Debian:

1. Установите ОС Ubuntu 22.04 LTS или Ubuntu 20.04 LTS. Воспользуйтесь официальным источником для установки дистрибутива:

   https://ubuntu.com/download/server

   Внимание! Во время установки ОС выделите под рутовый «/» раздел 24 Гб, SWAP отключите, оставшееся место выделите под раздел «/var/lib/docker».

2. Удалите пакеты snapd и ufw с помощью команды:

   ```
   apt autoremove --purge snapd ufw
   ```

3. Установите программное обеспечение Docker. Для установки воспользуйтесь официальным источником:

   https://docs.docker.com/install/linux/docker-ce/ubuntu/

   Внимание! Если ПО Docker распаковано из пакета snapd, удалите его и выполните установку из официального источника.

   Пример кода для установки Docker:

   ```
   #Uninstall all conflicting packages
   for pkg in docker.io docker-doc docker-compose docker-compose-v2
   podman-docker containerd runc; do sudo apt-get remove $pkg; done

   # Add Docker's official GPG key:
   sudo apt-get update
   sudo apt-get install ca-certificates curl
   sudo install -m 0755 -d /etc/apt/keyrings
   sudo curl -fsSL https://download.docker.com/linux/ubuntu/gpg -o
   /etc/apt/keyrings/docker.asc
   sudo chmod a+r /etc/apt/keyrings/docker.asc

   # Add the repository to Apt sources:
   echo \
     "deb [arch=$(dpkg --print-architecture) signed-
   by=/etc/apt/keyrings/docker.asc]
   https://download.docker.com/linux/ubuntu \
     $(. /etc/os-release && echo "$VERSION_CODENAME") stable" | \
     sudo tee /etc/apt/sources.list.d/docker.list > /dev/null
   sudo apt-get update

   #Install the latest version
   sudo apt-get install docker-ce docker-ce-cli containerd.io docker-
   buildx-plugin docker-compose-plugin
   ```

4. Установите дополнительное ПО (см. ниже).

Для установки дополнительного ПО:

1. Выполните установку NTP-сервера с помощью команды:

   ```
   apt install chrony
   ```

   Если имеются источники точного времени внутри компании, в файл /etc/chrony/chrony.conf внесите серверы[1] NTP в виде:

   ```
   server ntp1.local
   server ntp2.local
   server ntp3.local
   ```

[1] Подразумеваются сервера заказчика, которые используют NTP-сервера.

Пример кода:

```
systemctl enable chrony
systemctl restart chrony
```

Для проверки подключения к NTP-серверам используйте следующую команду:

```
chronyc sources -v
```

2. Укажите параметры хранения журналов в Docker в каталоге /etc/docker/daemon.json:

```
{
"log-driver": "json-file",
 "log-opts": {
       "max-size": "100m"
 }
}
```

3. Выполните:

```
systemctl restart docker
```

4. Проверьте цепочку SSL-сертификатов и убедитесь в правильном порядке набора сертификатов (см. стр. 34).

5. Проверьте правильность настроек сервера[1] с помощью табл. 27:

табл. 27

Название настройки	Определение	Решаемая задача
Открытые порты CTS	22, TCP	Удаленное подключение к SSH для управления сервером
Открытые порты DNS сервера	53, UDP/TCP	DNS-запросы
Открытые порты NTP сервера	123, UDP	Синхронизация времени по протоколу NTP
Открытые порты AD сервера	389, TCP	Подключение к серверу AD для целей авторизации пользователей и получения их списка
Открытые порты AD сервера	636, TCP	TLS-подключение к серверу AD авторизации и получения списка пользователей
Открытые порты CTS	443, TCP	HTTPS-подключение мобильных клиентов к CTS
Открытые порты registry.public.express	443, TCP	Установка и обновление пакетов CTS
Открытый порт ru.public.express:5001	5001, TCP	Трастовое подключение к Российскому региональному серверу
Открытый порт Media-сервера	8188, TCP	Подключение к Janus на Media-сервере
DNS-имя	Рекомендуется иметь третий уровень DNS. Во внутренней сети компании DNS-имя должно разрешаться во внутренний IP сервера Single CTS либо Back CTS. Требования к DNS-имени сервера Media аналогичны требованиям к DNS-имени сервера CTS	

[1] Данные настройки подходят для установки всех компонентов на двух серверах. Подробные настройки сетевых взаимодействий для Single CTS и комбинации Front CTS и Back CTS см. стр. 45 «Приложение 2» и стр. 46 «Приложение 3» соответственно.

Название настройки	Определение	Решаемая задача
Сертификат для DNS-имени	SSL версии 3 и не ниже TLS 1.2. Длина ключа равна 2048 или больше. X.509 версия 3. Незашифрованный ключ для сертификата[1]	
Учетная запись Microsoft AD	Активная учетная запись с доступом к чтению выбранной группы и deleted objects	Получение списка пользователей

6. Запросите у разработчика следующие индивидуальные параметры для установки (параметры предоставляются по FQDN конкретного сервера) (табл. 28):

табл. 28

Параметр	Описание
cts_id	Идентификатор данного сервера;
rts_host	FQDN адрес сервера RTS, к которому будет подключен данный CTS;
rts_id	Идентификатор сервера RTS
rts_token	Токен для авторизации на сервере RTS. Имеет следующий формат <token_for_accept>:<token_for_connect>, где token_for_accept – токен для приема подключения от удаленного сервера, token_for_connect – токен для подключения к удаленному серверу

ОС CENTOS/RHEL

Для предварительной настройки при использовании ОС Centos/RHEL:

1. Установите ОС Centos/RHEL.

Внимание! Во время установки ОС выделите под рутовый «/» раздел 24 Гб, SWAP отключите, оставшееся место выделите под раздел «/var/lib/docker».

2. Удалите firewalld с помощью команды:

```
systemctl disable firewalld
```

или:

```
systemctl stop firewalld
```

3. Переведите SElinux в режим Permissive, отредактировав файл /etc/selinux/config.
4. Установите программное обеспечение Docker. Для установки воспользуйтесь официальным источником[2].
5. Установите NTP-сервер (см. ниже).

Для установки NTP-сервера:

1. Выполните установку NTP-сервера с помощью команды:

```
dnf install chrony
```

2. Если имеются источники точного времени внутри компании, в файл /etc/chrony.conf внесите серверы[3] NTP в виде:

```
server ntp1.local
server ntp2.local
```

[1] Могут быть предоставлены компанией-разработчиком.
[2] https://docs.docker.com/engine/install/centos/
[3] Подразумеваются сервера заказчика, которые используют NTP-сервера.

```
server ntp3.local
```

Пример кода:

```
systemctl enable chrony
systemctl start chrony
```

Для проверки подключения к NTP-серверам используйте следующую команду:

```
chronyc sources -v
```

3. Укажите параметры хранения журналов в Docker в каталоге /etc/docker/daemon.json:

```
{
"log-driver": "json-file",
 "log-opts": {
       "max-size": "100m"
 }
}
```

4. Выполните:

```
systemctl restart docker
```

5. Проверьте цепочку SSL-сертификатов и убедитесь в правильном порядке набора сертификатов (см. стр. 34).
6. Проверьте правильность настроек сервера[1] с помощью табл. 29:

табл. 29

Название настройки	Определение	Решаемая задача
Открытые порты CTS	22, TCP	Удаленное подключение к SSH для управления сервером
Открытые порты DNS сервера	53, UDP/TCP	DNS-запросы
Открытые порты NTP сервера	123, UDP	Синхронизация времени по протоколу NTP
Открытые порты AD сервера	389, TCP	Подключение к серверу AD для целей авторизации пользователей и получения их списка
Открытые порты AD сервера	636, TCP	TLS-подключение к серверу AD авторизации и получения списка пользователей
Открытые порты CTS	443, TCP	HTTPS-подключение мобильных клиентов к CTS
Открытые порты registry.public.express	443, TCP	Установка и обновление пакетов CTS
Открытый порт ru.public.express:5001	5001, TCP	Трастовое подключение к Российскому региональному серверу
Открытый порт Media-сервера	8188, TCP	Подключение к Janus на Media-сервере
DNS-имя	Рекомендуется иметь третий уровень DNS. Во внутренней сети компании DNS-имя должно разрешаться во внутренний IP сервера Single CTS либо Back CTS.	

[1] Данные настройки подходят для установки всех компонентов на двух серверах. Подробные настройки сетевых взаимодействий для Single CTS и комбинации Front CTS и Back CTS см. стр. 45 «Приложение 2» и стр. 46 «Приложение 3» соответственно.

Название настройки	Определение	Решаемая задача
	Требования к DNS-имени сервера Media аналогичны требованиям к DNS-имени сервера CTS	
Сертификат для DNS-имени	SSL версии 3 и не ниже TLS 1.2. Длина ключа равна 2048 или больше. X.509 версия 3. Незашифрованный ключ для сертификата[1]	
Учетная запись Microsoft AD	Активная учетная запись с доступом к чтению выбранной группы и deleted objects	Получение списка пользователей

7. Запросите у разработчика следующие индивидуальные параметры для установки (параметры предоставляются по FQDN конкретного сервера) (табл. 30):

табл. 30

Параметр	Описание
cts_id	Идентификатор данного сервера;
rts_host	FQDN адрес сервера RTS, к которому будет подключен данный CTS;
rts_id	Идентификатор сервера RTS
rts_token	Токен для авторизации на сервере RTS. Имеет следующий формат <token_for_accept>:<token_for_connect>, где token_for_accept – токен для приема подключения от удаленного сервера, token_for_connect – токен для подключения к удаленному серверу

ОС ASTRA LINUX ОРЕЛ

Для предварительной настройки при использовании ОС Astra Linux Орел:

1. Установите ОС Astra Linux Орел. Во время установки на шаге выбора «Выбор программного обеспечения» выделите «Базовые средства», «Средства удаленного доступа SSH».

Внимание! Во время установки ОС выделите под рутовый «/» раздел 24 Гб, SWAP отключите, оставшееся место выделите под раздел «/var/lib/docker».

2. Установите Docker помощью команды:

```
apt install docker.io
```

3. Установите дополнительное ПО (см. ниже).

Для установки дополнительного ПО:

1. Выполните установку NTP-сервера с помощью команды:

```
apt install chrony
```

Если имеются источники точного времени внутри компании, в файл /etc/chrony/chrony.conf внесите серверы[2] NTP.

Удалите или закомментируйте строку pool и укажите свои сервера.

Пример:

```
server ntp1.local
server ntp2.local
```

[1] Могут быть предоставлены компанией-разработчиком.
[2] Подразумеваются сервера заказчика, которые используют NTP-сервера.

```
server ntp3.local
```

2. Перезапустите службу для применения изменений:

```
systemctl restart chrony
```

Для проверки подключения к NTP-серверам используйте следующую команду:

```
chronyc sources -v
```

3. Получите права root с помощью команды:

```
sudo -s
```

4. Укажите параметры хранения журналов в Docker в каталоге /etc/docker/daemon.json:

```
{
"log-driver": "json-file",
 "log-opts": {
       "max-size": "100m"
 }
}
```

5. Выполните:

```
systemctl restart docker
```

6. Проверьте цепочку SSL-сертификатов и убедитесь в правильном порядке набора сертификатов (см. стр. 34).

7. Проверьте правильность настроек сервера[1] с помощью табл. 31:

табл. 31

Название настройки	Определение	Решаемая задача
Открытые порты CTS	22, TCP	Удаленное подключение к SSH для управления сервером
Открытые порты DNS сервера	53, UDP/TCP	DNS-запросы
Открытые порты NTP сервера	123, UDP	Синхронизация времени по протоколу NTP
Открытые порты AD сервера	389, TCP	Подключение к серверу AD для целей авторизации пользователей и получения их списка
Открытые порты AD сервера	636, TCP	TLS-подключение к серверу AD авторизации и получения списка пользователей
Открытые порты CTS	443, TCP	HTTPS-подключение мобильных клиентов к CTS
Открытые порты registry.public.express	443, TCP	Установка и обновление пакетов CTS
Открытый порт сервера Media	8188, TCP	Подключение к Janus на сервере Media

[1] Данные настройки подходят для установки всех компонентов на двух серверах. Подробные настройки сетевых взаимодействий для Single CTS и комбинации Front CTS и Back CTS см. стр. 45 «Приложение 2» и стр. 46 «Приложение 3» соответственно.

Название настройки	Определение	Решаемая задача
Открытый порт ru.public.express:5001	5001, TCP	Трастовое подключение к Российскому региональному серверу
DNS-имя	Рекомендуется иметь третий уровень DNS. Во внутренней сети компании DNS-имя должно разрешаться во внутренний IP сервера Single CTS либо Back CTS. Требования к DNS-имени сервера Media аналогичны требованиям к DNS-имени сервера CTS	
Сертификат для DNS-имени	SSL версии 3 и не ниже TLS 1.2. Длина ключа равна 2048 или больше. X.509 версия 3. Незашифрованный ключ для сертификата[1]	
Учетная запись Microsoft AD	Активная учетная запись с доступом к чтению выбранной группы и deleted objects	Получение списка пользователей

8. Запросите у разработчика следующие индивидуальные параметры для установки (параметры предоставляются по FQDN конкретного сервера) (табл. 32):

табл. *32*

Параметр	Описание
cts_id	Идентификатор данного сервера;
rts_host	FQDN адрес сервера RTS, к которому будет подключен данный CTS;
rts_id	Идентификатор сервера RTS;
rts_token	Токен для авторизации на сервере RTS. Имеет следующий формат <token_for_accept>:<token_for_connect>, где token_for_accept – токен для приема подключения от удаленного сервера, token_for_connect – токен для подключения к удаленному серверу

УСТАНОВКА ETS

Следующий набор команд выполняется в командной строке сервера, на котором устанавливается ETS.

Для установки ETS:

1. Запустите командную строку.
2. Подключитесь к репозиторию разработчика в Docker для скачивания контейнеров:

```
docker login -u Login -p Password registry.public.express
```

Примечание. В качестве логина и пароля используются Login и Password, которые выдаются разработчиком.

3. Скачайте контейнер-инсталлятор:

```
docker run --rm registry.public.express/dpl:ets-release dpl-install | bash
```

[1] Могут быть предоставлены компанией-разработчиком.

Из репозитория на сервер скачается файл в формате YAML с контейнерами и инсталлятор.

4. Создайте рабочий каталог ETS:

```
mkdir -p /opt/express
cd /opt/express
echo DPL_IMAGE_TAG=ets-release > dpl.env
dpl --init
```

После выполнения команды dpl --init создается файл settings.yaml.

5. Установите цепочки сертификатов и ключа SSL:
   - при использовании собственного сертификата создайте директорию для сертификатов.

     Внимание! Имя файла сертификата и имя ключа должны соответствовать примеру ниже:

     ```
     mkdir -p certs
     cp /somewhere/my-certificate-chain.crt certs/express.crt
     cp /somewhere/my-unencrypted-key.key certs/express.key
     ```

     Конструкции /somewhere/my-certificate-chain.crt и /somewhere/my-unencrypted-key.key индивидуальны для каждого конкретного случая.

     Конструкции certs/express.crt и certs/express.key являются обязательными.

     Требования к сертификатам изложены на стр. 34;
   - при использовании сертификата от Let's Encrypt в файл settings.yaml добавьте параметр le_email: admin@company-mail.ru

   Проверка подключения сертификатов после инсталляции описана на стр. 71.
6. Выполните настройку DLPS для доступа администраторов безопасности к содержимому сообщений (параметры настройки см. стр. 69).
7. Установите cAdvisor (установка выполняется из каталога /opt/express):

```
dpl cadvinstall
ps ax|grep cadvisor | grep -v grep
```

Вывод команды:

```
17605 ? Ssl 44:20 /usr/bin/cadvisor -listen_ip 172.17.0.1 -port
9100
```

8. Установите Prometheus node exporter из каталога /opt/express с помощью команды:

```
dpl nxinstall
ps ax|grep node_exporter | grep -v grep
```

Вывод команды:

```
17802 ?        Ssl  322:51 /usr/bin/node_exporter --web.listen-
address=172.17.0.1:9200
```

По завершении установки ETS и вспомогательного ПО создается файл конфигурации, в котором необходимо задать параметры для подключения к RTS, получения push-уведомлений, SMS-сообщений и других функций.

Созданный по умолчанию файл конфигурации имеет следующий вид и требует редактирования:

```
api_internal_token:
ccs_host: cts_name.somedomain.sometld
ets_id: 'dddd-cccc-dddd-cccc'
phoenix_secret_key_base:
postgres_password:
prometheus_users:
```

```
  prometheus:
rts_host: 'rts_name.somedomain.sometld'
rts_id: 'aaaa-bbbb-cccc-dddd'
rts_token: 'verystrongpassword'
```

Для изменения файла конфигурации воспользуйтесь любым текстовым редактором и внесите исправления в файл. Перечень всех настроек в файле конфигурации представлен в табл. 33.

табл. 33

Название настройки	Значение
Обязательные настройки	
ccs_host	Полное имя домена данного сервера, прописанное в DNS и соответствующее имени, на которое приобретался сертификат
ets_id	Идентификатор установленного сервера, предоставляется разработчиком
prometheus_users	Список пользователей с паролями, генерируемыми утилитой htpasswd, для доступа к интегрированному в систему стеку Prometheus
rts_host	Полное имя домена сервера RTS, к которому будет подключен установленный CTS (предоставляется разработчиком)
rts_id	Идентификатор сервера RTS (предоставляется разработчиком)
rts_token	Токен для авторизации на сервере RTS (предоставляется разработчиком)
le_email	Параметр устанавливается при использовании сертификата от компании Let`s Encrypt. Значение параметра должно соответствовать e-mail, на который будут приходить оповещения от Let`s Encrypt
admin_url	Параметр указывается для переопределения стандартного пути (/admin) к веб интерфейсу администратора: например, /not-admin
Необязательные настройки	
Доступ к веб-интерфейсу администратора и консоли администратора DLPS	admin_allow: - 10.0.0.0/8 - 172.16.1.0/24
Доступ к Prometheus	prometheus_allow: - 10.0.0.0/8 - 172.16.1.0/24
Изменение пути к интерфейсу администратора	admin_url: /express-admin-ui
Изменение пути к интерфейсу администратора DLPS	dlps_url: /dlps-admin-ui

Для корректного функционирования сервера рекомендуется исправлять параметры ets_id, rts_host, rts_id и rts_token; в примере выше они выделены красным цветом.

Примечание: Значения параметров ets_id, rts_host, rts_id и rts_token должны находиться внутри кавычек ('value'). На другие параметры данное требование не распространяется. Для предотвращения ошибок рекомендуется заменить параметры сгенерированного файла параметрами, выданными разработчиками. В случае ручного ввода значений символ кавычки не вводится.

Для данного типа архитектуры установите веб-клиент.

УСТАНОВКА ВЕБ-КЛИЕНТА

Внимание! Веб-клиент устанавливается на сервер после установки docker-ce и docker-compose.

Веб-клиент подключается к ETS и к CTS. Установка веб-клиента может быть произведена в любой момент, но вход осуществится только после установки CTS.

Для установки веб-клиента:

1. Запустите командную строку.
2. Подключитесь к репозиторию разработчика в Docker для скачивания контейнеров:

```
docker run --rm registry.public.express/dpl:web-release dpl-install | bash
docker login -u Login -p Password registry.public.express
```

Примечание. В качестве логина и пароля используются Login и Password, которые выдаются разработчиком.

3. Создайте рабочий каталог веб-клиента:

```
mkdir -p /opt/web_client
cd /opt/web_client
echo DPL_IMAGE_TAG=web-release > dpl.env
dpl --init
```

4. После выполнения команды dpl --init создается файл settings.yaml.
5. Установите цепочки сертификатов и ключа SSL:
   - при использовании собственного сертификата создайте директорию для сертификатов.

     Важно! Имя файла сертификата и имя ключа должны соответствовать примеру ниже:

     ```
     mkdir -p certs
     cp /somewhere/my-certificate-chain.crt certs/express.crt
     cp /somewhere/my-unencrypted-key.key certs/express.key
     ```

     Конструкции /somewhere/my-certificate-chain.crt и /somewhere/my-unencrypted-key.key индивидуальны для каждого конкретного случая.

     Конструкции certs/express.crt и certs/express.key являются обязательными.

     Требования к сертификатам изложены на стр. 34:
   - при использовании сертификата от Let's Encrypt в файл settings.yaml добавьте параметр le_email: admin@company-mail.ru.

     Проверка подключения сертификатов после инсталляции описана на стр. 71.
6. Созданный по умолчанию файл конфигурации имеет следующий вид и требует редактирования:

```
ccs_host: somehost.somedomain.sometld
web_client_config: ''
```

7. Пример заполнения конфигурации:

```
ccs_host:  example.com
le_email: test@example.com
web_client_enabled: true
web_client_config:
  regions:
    ru:
```

```
      host:  rts1dev.server.ru
      prefix:  7
    ae:
      host:  rts2dev.server.ru
      prefix:  971
  sentryDSN: https://sentryToken@sentry.server.ru/58
  ccsHost: corp.express
  ctsWeb: false
  locales: ["en","ru","de","fr","es"]
  platformPackageId: ru.unlimitedtech.express
  gcmSenderId: senderId
  landingUrl: https://express.ms/mobile-corp-express
  allowCtsLogin: true
  allowDebugInfo: true
  ets: true
  gmapsApiKey: apiKeyapiKeyapiKey
  actionTaskFeature: true
  changelogUrl: https://dl.express.ms/changelog/changelog-{}.md
images:
  web_client: registry.public.express/web_client:develop
```

8. В каталоге /opt/express/web_client выполните команду:

```
dpl -d
```

УСТАНОВКА СЕРВЕРА MEDIA

Сервер Media предназначен для организации видео- и аудиосвязи между пользователями. Видео использует по умолчанию кодек VP8, битрейт 120 kbps, 360 kbps, 1080 kbps на участника (в зависимости от выбранного качества на стороне клиента). Аудио использует по умолчанию кодек OPUS, битрейт 16 kbps на участника. Суммарная полоса пропускания, которую может использовать клиент, не превышает 2500 kbps.

Установка сервера Media проходит в следующем порядке:

- предварительная настройка;
- установка сервера Media;
- установка корпоративного сервера (Single CTS или серверы Front CTS и Back CTS);
- подключение сервера Media к CTS-серверу;
- настройка сервера Media.

ПРЕДВАРИТЕЛЬНАЯ НАСТРОЙКА

Для корректной работы сервера выполните предварительную настройку.

Примечание. Задержки при передаче голосовой информации в режиме TURN зависят от удаленности конечного пользователя от TURN-сервера.

Перед установкой сервера Media:

1. Определите доступный для обращений из интернета глобальный IP-адрес для сервера Media.
2. Проверьте правильность выставленных настроек сервера с помощью табл. 34:

табл. 34

Направление	Источник	Приемник	Порт	Протокол	Предназначение порта
Входящий	Admin IP	Media	22	TCP	SSH

Направление	Источник	Приемник	Порт	Протокол	Предназначение порта
Входящий	CTS	Media	8188	TCP	Management conference
Входящий	Любой	Media	3478	TCP/UDP	TURN
Входящий	Любой	Media	20000–40000	UDP	SRTP media
Исходящий	Media	Любой	Любой	UDP	SRTP media
Исходящий	Media	DNS	53	TCP/UDP	DNS
Исходящий	Media	NTP	123	UDP	NTP
Исходящий	Media	registry.public.express	443	TCP	Docker registry

3. Присвойте доменное имя серверу Media.
4. Подготовьте цепочку сертификатов SSL в формате PEM и нешифрованный приватный ключ.

УСТАНОВКА СЕРВЕРА MEDIA

Следующий набор команд выполняется в командной строке сервера, на котором устанавливается Media.

Для установки сервера Media:

1. Подключитесь к Media серверу через SSH.
2. Запустите командную строку.
3. Выполните установку NTP-сервера с помощью команды:

```
apt install chrony
```

Если имеются источники точного времени внутри компании, в файл /etc/chrony/chrony.conf внесите серверы NTP в виде:

```
server ntp1.local
server ntp2.local
server ntp3.local
```

Пример кода:

```
systemctl enable chrony
systemctl restart chrony
```

Для проверки подключения к NTP-серверам используйте следующую команду:

```
chronyc sources -v
```

4. Подключитесь к репозиторию разработчика в Docker для скачивания контейнеров:

```
docker login -u Login -p Password registry.public.express
```

Примечание. В качестве логина и пароля используются Login и Password, которые выдаются разработчиком.

5. Скачайте контейнер-инсталлятор:

```
docker run --rm registry.public.express/dpl:voex-release dpl-install | bash
```

Из репозитория на сервер скачается файл в формате YAML с контейнерами и инсталлятор.

6. Создайте рабочий каталог проекта:

```
mkdir -p /opt/express-voice
cd /opt/express-voice
```

```
echo DPL_IMAGE_TAG=voex-release > dpl.env
dpl --init
```

7. Установите цепочку сертификатов и ключа SSL для TURN и STUN серверов:

```
mkdir -p certs
cp /somewhere/my-certificate-chain.crt certs/express.crt
cp /somewhere/my-unencrypted-key.key certs/express.key
```

8. Создайте DH (Diffie Hellman) ключ:

```
openssl dhparam -out certs/dhparam.pem 2048
```

9. Откройте файл /opt/express-voice/settings.yaml для редактирования:

```
external_interface: eth0
janus_ws_enable: true
janus_ws_ip: 127.0.0.1
janus_wss_enable: false
janus_wss_ip: 127.0.0.1
  - ''
ccs_host: somehost.somedomain.sometld
phoenix_secret_key_base: **********
turnserver_server_name: localhost
turnserver_listening_ip: 127.0.0.1
api_internal_token: token
```

Настройки по умолчанию описаны в табл. 35:

табл. 35

Название настройки	Значение
external_interface	Наименование интерфейса с внешним IP-адресом
janus_keep_private_host	Включение согласования подключения на все локальные ip-адреса сервера
ccs_host	FQDN имя Media-сервера
api_internal_token	Токен для запросов к API
janus_ws_acl	Адреса или сети серверов, на которых расположен контейнер messaging (например, 172.18.0.)
janus_ws_ip - ip	Интерфейс, который использует janus websocket для управления конференциями сервисом messaging
janus_wss_enable janus secure websocket	Включение janus secure websocket
janus_wss_ip	Интерфейс, который использует janus secure websocket
nat_1_1_mapping keep_private_host	При использовании NAT 1:1 указывается внешний IP-адрес и включается режим сохранения приватного IP-адреса
keep_private_host	Список разрешенных IP-адресов: • для одного CTS-сервера – его адрес: [1.2.3.4]; • если CTS и Media-сервер находятся на одном сервере – пустой список: []
phoenix_secret_key_base	Серверный ключ (оставить без изменения)
turnserver_shared_key	Ключ для подключения Media к CTS (скопировать и сохранить сгенерированное значение ключа)
turnserver_allowed_peer_ip	Параметр, фильтрующий трафик IP адресов всех медиа серверов до NAT адреса
janus_ice_enforce_list	Параметр, фильтрующий согласование точек подключения с пользователями через указанную сетевую карту медиа сервера
turnserver_external_ip	Внешний IP-адрес
turnserver_listening_ip	Внешний или внутренний IP-адрес интерфейса для TURN и STUN серверов
transcoding_storage_enabled	Включение сервиса временного хранения записей, по умолчанию выключен

10. Внесите изменения в настройки по умолчанию и добавьте следующий параметр:

```
turnserver_external_ip:
  - 1.2.3.4
```

11. С помощью команды ниже сгенерируйте значение ключа turnserver_shared_key:

```
cat /proc/sys/kernel/random/uuid | tr -d '-' | base64 | cut -b 1-22
```

12. Скопируйте и сохраните сгенерированное значение ключа (для примера используется YmNjY2VmNDk0ZTEwNDgzNj) для дальнейшего подключения сервера Media к CTS-серверу.
13. Добавьте этот параметр в конфигурацию:

```
turnserver_shared_key: YmNjY2VmNDk0ZTEwNDgzNj
```

14. Добавьте следующий параметр turnserver_allowed_peer_ip, указав локальные IP адреса всех медиа серверов (если их несколько) или локальный IP адрес единственного медиа сервера для фильтрации трафика до NAT адреса:

```
turnserver_allowed_peer_ip:
- 172.20.56.15
- 172.20.56.16
```

Примечание. Если на медиа сервере используется внешний (белый) ip адрес - данный фильтр указывать не требуется

15. Добавьте этот параметр в конфигурацию:

```
janus_ice_enforce_list: eth0
```

16. Если будет использоваться запись звонков, добавьте параметр:

```
transcoding_storage_enabled: true
```

17. Добавьте следующие параметры и установите параметр «janus_nat_1_1_mapping» равным значению внешнего IP-адреса в сети Интернет, с которого производится переброс портов:

```
janus_keep_private_host: true
janus_ws_ip: 172.17.0.1
janus_ws_acl: 172.19.0.
janus_nat_1_1_mapping: 1.2.3.4
```

18. Выполните команду предварительного генерирования файлов конфигураций:

```
dpl -p
```

19. Выполните команду:

```
dpl -d
```

Если архитектурное решение предполагает раздельную установку сервиса записи конференций (Recording-бот) и сервиса конференций (Media), обратитесь к компании-разработчику.

УСТАНОВКА СЕРВЕРА TRANSCODING

Для установки и настройки сервера Transcoding:

1. Подключитесь к выделенному серверу через SSH.
2. Создайте папку для работы транскодирования:

```
mkdir -p /opt/transcoding
```

3. Установите сервис Docker:

```
curl -fsSL http://get.docker.com -o get-docker.sh && sh get-docker.sh
```

4. Укажите параметры хранения журналов в Docker в каталоге /etc/docker/daemon.json:

```
{
"log-driver": "json-file",
 "log-opts": {
       "max-size": "100m"
 }
}
```

5. Перезагрузите сервис Docker:

```
systemctl restart docker
```

6. Перейдите в директорию /opt/transcoding:

```
cd /opt/transcoding
```

7. Создайте переменную проекта:

```
echo "DPL_IMAGE_TAG=voex-release" > dpl.env
```

8. Создайте и запустите контейнер Docker:

```
docker run --rm registry.public.express/dpl:voex-release dpl-
install | bash
```

9. Инициализируйте проект VoEx:

```
dpl --init
```

10. Откройте файл /opt/transcoding/settings.yaml в любом текстовом редакторе (например, nano):

```
nano /opt/transcoding/settings.yaml
```

11. Отключите сервисы redis, coturn и janus, установив значение «false»:

```
coturn_enabled: false
janus_enabled: false
redis_enabled: false
transcoding_storage_enabled: false
```

12. Добавьте хосты для работы транскодирования. Параметры для работы транскодирования описаны в табл. 36. Значения можно скопировать с Media-сервера, с которого переносится контейнер.

Важно! Значения api_internal_token скопируйте из файлов /opt/express/settings.yaml, расположенных на соответствующих серверах ccs_hosts. Значения token скопируйте из файлов /opt/express-voice/settings.yaml (значение api_internal_token), расположенных на соответствующих серверах Media.

Пример настроек хостов транскодирования:

- для одного сервера CTS:

```
transcoding_hosts:
  cts:
    ccs_host: fqdn_cts
    api_internal_token: $api_internal_token_cts
    storages_tokens_mapping:
      fqdn_media1:
        token: $api_internal_token_media
        ssl_envs_prefix: "TSS"
# не обязательные параметры
# если не публичные сертификаты, то отключаем проверку
сертификата:
tc-cts_env_override:
  TSS_SSL_ENABLED: true
  TSS_SSL_VERIFY: verify_none
```

- для нескольких CTS-серверов:

```
transcoding_hosts:
  cts1:
    ccs_host: fqdn_cts1
    api_internal_token: $api_internal_token_cts1
    storages_tokens_mapping:
      fqdn_media1:
        token: $api_internal_token_media1
        ssl_envs_prefix: "TSS"
  cts2:
    ccs_host: fqdn_cts2
    api_internal_token: $api_internal_token_cts2
    storages_tokens_mapping:
      fqdn_media2:
        token: $api_internal_token_media2
        ssl_envs_prefix: "TSS"
```

табл. 36

Название настройки	Значение
transcoding_hosts	Список объектов hosts (CTS), состоит из параметров: • cts (cts1, cts2) — уникальное название, можно использовать fqdn_cts; • ccs_host — FQDN CTS-сервера; • api_internal_token — токен для запросов к API (скопируйте из файлов /opt/express/settings.yaml, расположенных на соответствующих серверах ccs_hosts). Может содержать несколько блоков cts, если у вас один сервер транскодинга для нескольких CTS серверов
storages_tokens_mapping	Список объектов hosts, состоит из параметров: • fqdn_media — fqdn Media сервера, должно быть уникальным; • token — api_internal_token Media сервера; • ssl_envs_prefix — префикс сертификата. Может содержать несколько блоков fqdn_media, если у CTS сервера больше одного Janus(janus_ws_url)
tc-ct_env_override	Дополнительные параметры для transcoding
TSS_SSL_ENABLE	Включение/отключение дополнительных настроек transcoding
TSS_SSL_VERIFY	Проверка сертификата для transcoding

13. Запустите сервис командой:

```
dpl -d
```

14. Проверьте статус контейнеров:

```
docker ps -a
```

В результате выполнения команды должны появиться контейнеры transcoding в соответствии со значением, указанным в переменной transcoding_hosts, например:

```
root@yc-msg-ext-voex-transcoding01:~# docker ps -a
CONTAINER ID   IMAGE
COMMAND                  CREATED         STATUS         PORTS
NAMES
dd5ca4e7bdee   registry.public.express/transcoding:3.24.0
"/bin/sh -c 'export …"   45 hours ago    Up 22 hours    4000/tcp
voex-tc-cts-1
```

15. Проверьте доступность Media-сервера используя команду:

```
curl https://fqdn-media/testtest
```

16. Выполните команду для получения логов контейнера Docker на сервере Media:

```
docker logs voex-nginx-1 | grep testtest
```

В ответе должен содержатся запрос (запросы):

```
voice.test.corp.express 172.18.0.2 - - [02/Oct/2024:08:50:34
+0000] "GET /testtest HTTP/1.1" 204 0 "-" "curl/8.5.0"
"51.250.102.111"
```

УСТАНОВКА КОРПОРАТИВНОГО СЕРВЕРА

Важно! Перед началом процедуры установки необходимо установить Media (см. стр. 45).

УСТАНОВКА SINGLE CTS

Следующий набор команд выполняется в командной строке сервера, на котором устанавливается CTS.

Для установки CTS:

1. Запустите командную строку.
2. Подключитесь к репозиторию разработчика в Docker для скачивания контейнеров:

   ```
   docker login -u Login -p Password registry.public.express
   ```

   Примечание. В качестве логина и пароля используются Login и Password, которые выдаются разработчиком.

3. Скачайте контейнер-инсталлятор:

   ```
   docker run --rm registry.public.express/dpl:cts-release dpl-
   install | bash
   ```

   Из репозитория на сервер скачается файл в формате YAML с контейнерами и инсталлятор.

4. Создайте рабочий каталог CTS:

   ```
   mkdir -p /opt/express
   cd /opt/express
   echo DPL_IMAGE_TAG=cts-release > dpl.env
   dpl --init
   ```

   После выполнения команды dpl --init создается файл settings.yaml.

5. Установите цепочки сертификатов и ключа SSL:

   - при использовании собственного сертификата создайте директорию для сертификатов.

     Внимание! Имя файла сертификата и имя ключа должны соответствовать примеру ниже:

     ```
     mkdir -p certs
     cp /somewhere/my-certificate-chain.crt certs/express.crt
     cp /somewhere/my-unencrypted-key.key certs/express.key
     ```

     Конструкции /somewhere/my-certificate-chain.crt и /somewhere/my-unencrypted-key.key индивидуальны для каждого конкретного случая.

     Конструкции certs/express.crt и certs/express.key являются обязательными.

     Требования к сертификатам изложены на стр. 34;

   - при использовании сертификата от Let's Encrypt в файл settings.yaml добавьте параметр le_email: admin@company-mail.ru

   Проверка подключения сертификатов после инсталляции описана на стр. 71.

6. Выполните настройку DLPS для доступа администраторов безопасности к содержимому сообщений (параметры настройки см. стр. 69).
7. Установите cAdvisor (установка выполняется из каталога /opt/express):

```
dpl cadvinstall
ps ax|grep cadvisor | grep -v grep
```

Вывод команды:

```
17605 ? Ssl 44:20 /usr/bin/cadvisor -listen_ip 172.17.0.1 -port
9100
```

8. Установите Prometheus node exporter из каталога /opt/express с помощью команды:

```
dpl nxinstall
ps ax|grep node_exporter | grep -v grep
```

Вывод команды:

```
17802 ?        Ssl  322:51 /usr/bin/node_exporter --web.listen-
address=172.17.0.1:9200
```

По завершении установки CTS и вспомогательного ПО создается файл конфигурации, в котором необходимо задать параметры для подключения к RTS, получения push-уведомлений, SMS-сообщений и других функций.

Созданный по умолчанию файл конфигурации имеет следующий вид и требует редактирования:

```
api_internal_token: verystrongpassword
ccs_host: cts_name.somedomain.sometld
cts_id: 'aaaa-bbbb-cccc-dddd'
phoenix_secret_key_base: verystrongpassword
postgres_password: verystrongpassword
prometheus_users:
    prometheus:  verystrongpassword
rts_host: 'rts_name.somedomain.sometld'
rts_id: 'aaaa-bbbb-cccc-dddd'
rts_token: 'verystrongpassword'
```

Для изменения файла конфигурации воспользуйтесь любым текстовым редактором и внесите исправления в файл. Перечень всех настроек в файле конфигурации представлен в табл. 37.

табл. 37

Название настройки	Значение
Обязательные настройки	
ccs_host	Полное имя домена данного сервера, прописанное в DNS и соответствующее имени, на которое приобретался сертификат
cts_id	Идентификатор установленного сервера, предоставляется разработчиком
prometheus_users	Список пользователей с паролями, генерируемыми утилитой htpasswd, для доступа к интегрированному в систему стеку Prometheus
rts_host	Полное имя домена сервера RTS, к которому будет подключен установленный CTS (предоставляется разработчиком)
rts_id	Идентификатор сервера RTS (предоставляется разработчиком)
rts_token	Токен для авторизации на сервере RTS (предоставляется разработчиком)
le_email	Параметр устанавливается при использовании сертификата от компании Let`s Encrypt. Значение параметра должно соответствовать e-mail, на который будут приходить оповещения от Let`s Encrypt
janus_enabled	Установите значение «true»

Название настройки	Значение
turnserver_shared_key	Ключ для подключения Media к CTS (формируется на этапе установки сервера Media)
admin_url	Параметр указывается для переопределения стандартного пути (/admin) к веб интерфейсу администратора: например, /not-admin

sip_trunk_enable: true	Параметр устанавливается для использования вызовов через SIP-телефонию. После добавления параметра выполните в каталоге /opt/express команду
	`- dpl -d messaging`
	`ss -stuln | grep 5060`

Необязательные настройки	
Доступ к веб-интерфейсу администратора и консоли администратора DLPS	admin_allow: - 10.0.0.0/8 - 172.16.1.0/24
Доступ к Prometheus	prometheus_allow: - 10.0.0.0/8 - 172.16.1.0/24
Изменение пути к интерфейсу администратора	admin_url: /express-admin-ui
Изменение пути к интерфейсу администратора DLPS	dlps_url: /dlps-admin-ui
Экспорт корневых сертификатов с хоста в контейнер Docker	Установите значение «true» для параметра host_ca_enabled. Для дистрибутивов, отличных от Ubuntu, добавьте параметр host_ca: /somwhere/my-ca-certificates.crt Путь к файлу сертификатов индивидуален для каждого дистрибутива: - /etc/pki/ca-trust/extracted/openssl/ca-bundle.trust.crt (CentOS/CentOS Stream); - /etc/ssl/certs/ca-certificates.crt (Debian/AstraLinux); - /etc/pki/tls/certs/ca-bundle.crt (RHEL); - /etc/pki/ca-trust/extracted/pem/tls-ca-bundle.pem (ALT Linux)

Действия по подключению сервера Media к CTS описаны в разделе «Подключение сервера Media к CTS-серверу».

Для корректного функционирования сервера рекомендуется исправлять параметры cts_id, rts_host, rts_id и rts_token; в примере выше они выделены красным цветом.

Примечание: Значения параметров cts_id, rts_host, rts_id и rts_token должны находиться внутри кавычек ('value'). На другие параметры данное требование не распространяется. Для предотвращения ошибок рекомендуется заменить параметры сгенерированного файла параметрами, выданными разработчиками. В случае ручного ввода значений символ кавычки не вводится.

УСТАНОВКА СЕРВЕРОВ FRONT CTS И BACK CTS

Установка комбинации серверов Front CTS и Back CTS осуществляется в определенном порядке.

Для установки Front CTS:

1. Запустите командную строку.
2. Подключитесь к репозиторию разработчика в Docker для скачивания контейнеров:

```
docker login -u Login -p Password registry.public.express
```

Примечание. В качестве логина и пароля используются Login и Password, которые выдаются разработчиком.

3. Скачайте контейнер-инсталлятор:

```
docker run --rm registry.public.express/dpl:cts-release dpl-
install | bash
```

4. Из репозитория на сервер скачается файл в формате YAML с контейнерами и инсталлятор.
5. Создайте рабочий каталог Front CTS:

```
mkdir -p /opt/express
cd /opt/express
echo DPL_IMAGE_TAG=cts-release > dpl.env
dpl --init
```

6. Установите цепочки сертификатов и ключа SSL:
   - при использовании собственного сертификата создайте директорию для сертификатов.

     Внимание! Имя файла сертификата и имя ключа должны соответствовать примеру ниже:

     ```
     mkdir -p certs
     cp /somewhere/my-certificate-chain.crt certs/express.crt
     cp /somewhere/my-unencrypted-key.key certs/express.key
     ```

     Конструкции /somewhere/my-certificate-chain.crt и /somewhere/my-unencrypted-key.key индивидуальны для каждого конкретного случая.

     Конструкции certs/express.crt и certs/express.key являются обязательными.

     Требования к сертификатам изложены на стр. 34;
   - при использовании сертификата от Let's Encrypt в файл settings.yaml добавьте параметр le_email: admin@company-mail.ru.

   Проверка подключения сертификатов после инсталляции описана на стр. 71.
7. Откройте для редактирования конфигурационный файл settings.yaml, добавив добавьте следующие параметры:

```
api_internal_token: verystrongpassword
ccs_host: cts_name.somedomain.sometld
cts_id: 'aaaa-bbbb-cccc-dddd'
phoenix_secret_key_base: verystrongpassword
postgres_password: verystrongpassword
prometheus_users:
  prometheus: verystrongpassword
rts_host: 'rts_name.somedomain.sometld'
rts_id: 'aaaa-bbbb-cccc-dddd'
rts_token: 'verystrongpassword'
```

   Для корректного функционирования сервера рекомендуется исправлять параметры cts_id, rts_host, rts_id и rts_token; в примере выше они выделены красным цветом.

   Примечание: Значения параметров cts_id, rts_host, rts_id и rts_token должны находиться внутри кавычек ('value'). На другие параметры данное требование не распространяется. В случае ручного ввода значений символ кавычки не вводится.
8. Отредактируйте конфигурационный файл settings.yaml, добавив следующие параметры:

```
cts_frontend: true
kafka_host: backend_name.somedomain.sometld
postgres_host: backend_name.somedomain.sometld
frontend_host: frontend_name.somedomain.sometld
backend_host: backend_name.somedomain.sometld
```

Для установки Back CTS:

1. Запустите командную строку.
2. Подключитесь к репозиторию разработчика в Docker для скачивания контейнеров:

```
docker login -u Login -p Password registry.public.express
```

Примечание. В качестве логина и пароля используются Login и Password, которые выдаются разработчиком.

3. Скачайте контейнер-инсталлятор:

```
docker run --rm registry.public.express/dpl:cts-release dpl-
install | bash
```

Из репозитория на сервер скачается файл в формате YAML с контейнерами и инсталлятор.

4. Создайте рабочий каталог Back CTS:

```
mkdir -p /opt/express
cd /opt/express
```

5. Установите цепочки сертификатов и ключа SSL:
   - при использовании собственного сертификата создайте директорию для сертификатов.

     Внимание! Имя файла сертификата и имя ключа должны соответствовать примеру ниже:

     ```
     mkdir -p certs
     cp /somewhere/my-certificate-chain.crt certs/express.crt
     cp /somewhere/my-unencrypted-key.key certs/express.key
     ```

     Конструкции /somewhere/my-certificate-chain.crt и /somewhere/my-unencrypted-key.key индивидуальны для каждого конкретного случая.

     Конструкции certs/express.crt и certs/express.key являются обязательными.

     Требования к сертификатам изложены на стр. 34;
   - при использовании сертификата от Let's Encrypt в файл settings.yaml добавьте параметр le_email: admin@company-mail.ru.

   Проверка подключения сертификатов после инсталляции описана на стр. 71.
6. Скопируйте файл конфигурации с Front CTS (/opt/express/settings.yaml) на сервер Back CTS и разместите его в папке /opt/express.
7. Откройте для редактирования конфигурационный файл settings.yaml (файл использует язык разметки YAML):

```
api_internal_token: verystrongpassword
ccs_host: cts_name.somedomain.sometld
cts_id: 'aaaa-bbbb-cccc-dddd'
phoenix_secret_key_base: verystrongpassword
postgres_password: verystrongpassword
prometheus_users:
  prometheus: verystrongpassword
rts_host: 'rts_name.somedomain.sometld'
rts_id: 'aaaa-bbbb-cccc-dddd'
rts_token: 'verystrongpassword'
cts_frontend: true
kafka_host: backend_name.somedomain.sometld
postgres_host: backend_name.somedomain.sometld
frontend_host: frontend_name.somedomain.sometld
backend_host: backend_name.somedomain.sometld
```

Примечание: Значения параметров cts_id, rts_host, rts_id и rts_token должны находиться внутри кавычек ('value'). На другие параметры данное требование не распространяется. В случае ручного ввода значений символ кавычки не вводится.

Перечень всех настроек в файле конфигурации представлен в табл. 38.

табл. 38

Название настройки	Значение
Обязательные настройки	
ccs_host	Полное имя домена данного сервера, прописанное в DNS и соответствующее имени, на которое приобретался сертификат
cts_id	Идентификатор установленного сервера, предоставляется разработчиком
prometheus_users	Список пользователей с паролями, генерируемыми утилитой htpasswd, для доступа к интегрированному в систему стеку Prometheus
rts_host	Полное имя домена сервера RTS, к которому будет подключен установленный CTS (предоставляется разработчиком)
rts_id	Идентификатор сервера RTS (предоставляется разработчиком)
rts_token	Токен для авторизации на сервере RTS (предоставляется разработчиком)
le_email	Параметр устанавливается при использовании сертификата от компании Let`s Encrypt. Значение параметра должно соответствовать e-mail, на который будут приходить оповещения от Let`s Encrypt
janus_enabled	Установите значение «true»
turnserver_shared_key	Ключ для подключения Media к CTS (формируется на этапе установки сервера Media)
admin_url	Параметр указывается для переопределения стандартного пути (/admin) к веб интерфейсу администратора: например, /not-admin

sip_trunk_enable: true	Параметр устанавливается для использования вызовов через SIP-телефонию. После добавления параметра выполните в каталоге /opt/express команду
	`- dpl -d messaging`
	`ss -stuln | grep 5060`

Необязательные настройки	
Доступ к веб-интерфейсу администратора и веб-интерфейсу DLPS	admin_allow: - 10.0.0.0/8 - 172.16.1.0/24
Доступ к Prometheus	prometheus_allow: - 10.0.0.0/8 - 172.16.1.0/24
Изменение пути к интерфейсу администратора	admin_url: /express-admin-ui
Изменение пути к интерфейсу администратора DLPS	dlps_url: /dlps-admin-ui

Для изменения файла конфигурации воспользуйтесь любым текстовым редактором и внесите исправления в файл.

8. При редактировании файла конфигурации удалите дополнительные настройки:

```
cts_frontend: true
kafka_host: backend_name.somedomain.sometld
postgres_host: backend_name.somedomain.sometld
```

добавьте следующий параметр:

```
cts_backend: true
set_real_ip_from:
```

```
  - ip_frontend
```

где ip_frontend – это IP-адрес Front-сервера.

Отредактируйте параметры, подставив соответствующие значения:

- frontend_name.somedomain.sometld;
- backend_name.somedomain.sometld:

```
kafka_advertised_host_name: backend_name.somedomain.sometld
```

9. Установите Prometheus node exporter из каталога /opt/express с помощью команды:

```
dpl nxinstall
ps ax|grep node_exporter | grep -v grep
```

Действия по подключению сервера Media к CTS описаны в разделе «Подключение сервера Media к CTS-серверу».

Внимание! Если по требованиям информационной безопасности выход в Интернет с Back CTS должен быть ограничен, предусмотрено использование TinyProxy. При необходимости использовать proxy, рекомендуем ознакомиться с настройкой proxy для службы Docker по ссылке https://docs.docker.com/config/daemon/systemd/.

Для установки TinyProxy:

1. В каталоге, в котором установлена ОС, запустите команду:

```
Ubuntu\Debian - apt-get install -y tinyproxy
RHEL\CentOS - yum install -y epel-release
RHEL\CentOS - yum install -y tinyproxy
```

2. Создайте файл /etc/tinyproxy/filter, в котором перечисляются хосты для доступа через прокси:

```
registry.public.express
registry-auth.public.express
```

Автоматически будет создан файл конфигурации для tinyproxy: /etc/tinyproxy/tinyproxy.conf.

3. В файл /etc/tinyproxy/tinyproxy.conf внесите настройки:

```
User tinyproxy
Group tinyproxy
Port 8888
Timeout 600
DefaultErrorFile "/usr/share/tinyproxy/default.html"
StatFile "/usr/share/tinyproxy/stats.html"
LogFile "/var/log/tinyproxy/tinyproxy.log"
LogLevel Info
PidFile "/var/run/tinyproxy/tinyproxy.pid"
MaxClients 300
MinSpareServers 5
MaxSpareServers 10
StartServers 3
MaxRequestsPerChild 0
#BackIP
Allow 192.168.80.22
ViaProxyName "tinyproxy"
Filter "/etc/tinyproxy/filter"
FilterDefaultDeny Yes
ConnectPort 443
ConnectPort 563
```

4. Перезапустите сервис tinyproxy с помощью команды:

```
systemctl restart tinyproxy
```

ПОДКЛЮЧЕНИЕ СЕРВЕРА MEDIA К CTS-СЕРВЕРУ

Для настройки подключения Media сервера к CTS:

1. Подключитесь к CTS (Single/Back) серверу через SSH.
2. Укажите значение turnserver_shared_key в /opt/express/settings.yaml (ключ формируется на этапе установки сервера Media, для примера используется YmNjY2VmNDk0ZTEwNDgzNj):

```
turnserver_shared_key: YmNjY2VmNDk0ZTEwNDgzNj
```

3. Удалите конфигурационные файлы сервиса групповых звонков (janus), выполнив команды:

```
cd /opt/express-voice && dpl --dc down
cd ~ && rm -rf /opt/express-voice
```

НАСТРОЙКА СЕРВЕРА MEDIA

Настройка сервера Media включает:

- настройку серверов JANUS, STUN и TURN (обязательная настройка);
- настройку IP-телефонии (опциональная настройка).

НАСТРОЙКА СЕРВЕРОВ JANUS, STUN И TURN

Для настройки серверов JANUS, STUN и TURN:

1. Перейдите в директорию /opt/express-voice/:

```
cd /opt/express-voice
```

2. Запустите сервер Media в командной строке командой:

```
dpl -d
```

3. Откройте веб-интерфейс администратора.
4. В разделе «VoEx» для включения функции аудио- и видеовызовов в разделе «Janus-инстансы» (рис. 10) добавьте имена Media в формате ws://internal_fqdn_media_cts:8188 для каждого сервера отдельно. В разделе «Внешний хост Janus» введите публичный IP медиасервера.

рис. 10

5. Отключите настройки старого Janus-сервера.
6. В поле «TURN Server (через запятую)» введите внешний FQDN вашего сервера и через двоеточие номер порта, например, «express.firma.ru:3478»;
7. В поле «STUN Server (через запятую)» введите внешний FQDN вашего сервера и через двоеточие номер порта, например, «express.firma.ru:3478».
8. В поле «Локальная сеть voex» укажите маску локальной сети (рис. 11).

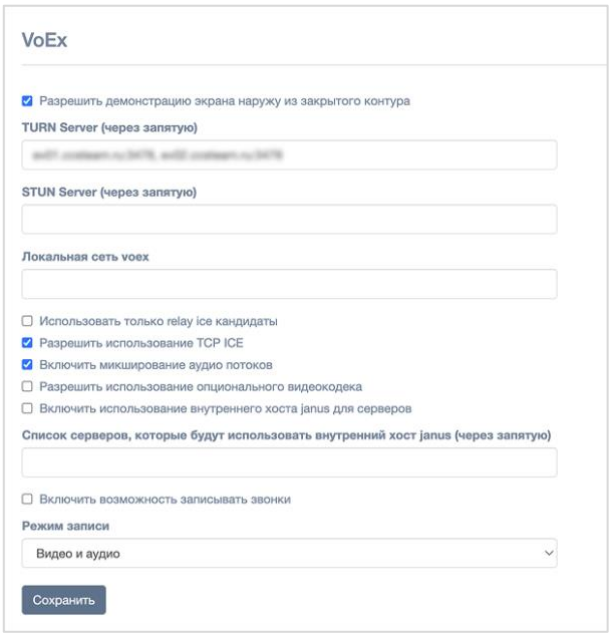

рис. 11

9. Поставьте следующие отметки, если это необходимо. Описание настроек представлено в табл. 39:

табл. 39

Настройка	Описание
Разрешить демонстрацию экрана наружу из закрытого контура	Позволяет пользователям демонстрировать экран своих устройств другим пользователям, находящимся за пределами КСПД (RTS-пользователям, пользователям трастовых серверов, пользователям, покинувшим зону КСПД)
Использовать только relay ice кандидаты	Принудительное использование TURN-сервера
Разрешить использование TCP ICE	Отметка установлена - подключение TCP в TURN-сервере разрешено. Отметка не установлена - подключение TCP в TURN-сервере запрещено
Включить микширование аудиопотоков	Объединяет аудиопотоки звонков, направленные от пользователей к серверу, в один поток
Разрешить использование опционального видеокодека	Пункт находится в разработке
Включить использование внутреннего хоста janus для серверов	Использование внутреннего хоста Janus для серверов, указанных в поле ниже (см. п. 10)
Включить возможность записывать звонки	Позволяет пользователям записывать индивидуальные и групповые звонки

Примечание. Рекомендуется поставить отметки «Разрешить демонстрацию экрана наружу из закрытого контура» и «Включить микширование аудио потоков».

10. В поле «Список серверов, которые будут использовать внутренний хост janus (через запятую)», введите список CTS ID серверов, с которыми будет происходить взаимодействие через внутренний хост.
11. Выберите из выпадающего списка режим записи.
12. Нажмите «Сохранить».

Для запуска сервера Media выполните команды, аналогичные командам запуска сервера CTS на стр. 71. Команды установки сервера Media выполняются из директории /opt/express-voice/.

Для настройки IP-телефонии:

1. В секции «SIP» установите флаг «SIP включен» (рис. 12).

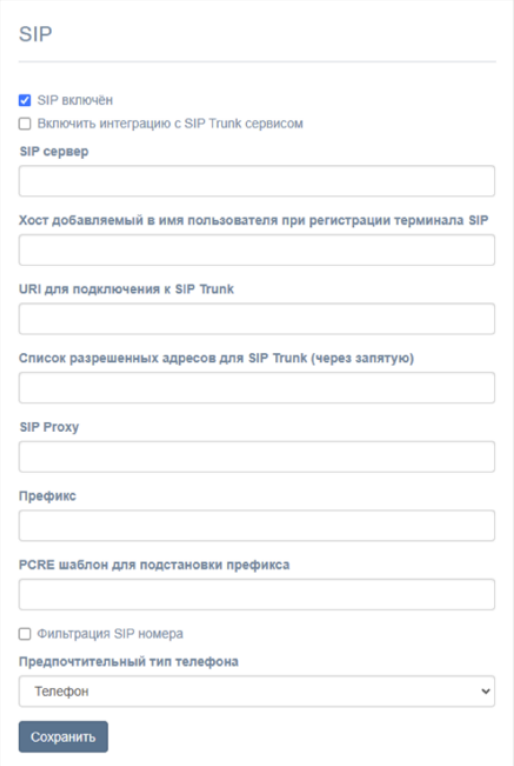

рис. 12

2. Заполните поля. Описание полей представлено в табл. 40:

табл. 40

Поле	Назначение
SIP-сервер	Доменное имя или IP-адрес АТС (SIP-транк). Если порт отличается от UDP/5060, укажите его через двоеточие
Хост, добавляемый в имя пользователя при регистрации терминала SIP	Поле, которое передается в invite-сообщении в сторону АТС. По умолчанию добавляется значение ccs_host. Если необходимо, укажите адрес хоста из конфигурационного файла
URI для подключения к SIP Trunk	Адрес Back CTS, на котором установлен контейнер messaging. Заполняется для развертывания Media и Back CTS. Формат записи: sip:<IP или DNS-имя>:<port>
Список разрешенных адресов SIP Trunk	IP-адреса, с которых будут приниматься вызовы SIP-транком СК «Express». Укажите минимум два IP-адреса: • IP-адрес АТС; • адрес, на котором установлен контейнер janus (SIP-шлюз устанавливаемый вместе с СК «Express»). Все IP или сети указываются с маской, например – 10.10.10.1/32 для одиночного IP, 192.168.12.0/24 для сети. Для развертывания Single CTS укажите IP-адрес самого сервера СК «Express» (10.10.10.1/32) и внутренний IP интерфейса docker сети (172.18.0.1/32) и АТС. Для развертывания Media и Back CTS укажите IP Media и АТС
SIP Proxy	Адрес прокси-сервера SIP-телефонии или адрес АТС. Формат записи SIP: <IP или DNS-имя >:<port>. Не обязательно указывать порт, если он не отличается от стандартного UDP/5060

Поле	Назначение
Префикс	Строка, подставляемая к началу набираемого номера при передаче номера на АТС и номера, принимаемого с АТС, в случае, если АТС отправляет номер без префикса
PCRE-шаблон для подстановки префикса	Регулярное выражение по совпадению структуры номера, к которому при исходящем вызове с СК «Express» будет подставляться префикс. Для того чтобы префикс не подставлялся к номерам, введите выражение - ^[0-9](1)
Предпочтительный тип телефона	Тип телефона, с которого будут осуществляться звонки. Возможные варианты: • телефон; • IP-телефон; • телефон (другой); • IP-телефон (другой). Сопоставление параметров объекта пользователя с данными типами телефонов настраивается в разделе Active Directory веб-интерфейса администратора. Выбранный тип телефона будет скрыт в профилях пользователей сервера, когда интеграция SIP выключена.

3. Нажмите «Сохранить».

Далее выполняется настройки клиентского АТС SIP-транка.

Внимание! Для всех схем развертывания, обязательным условием является отключение проверки состояния SIP-транка.

Для корректной работы при схеме развертывания Single CTS [1] настройте в АТС 2 SIP-транк:

1. Для вызовов с АТС в Систему укажите IP назначения Single CTS.
2. Для вызовов с Системы в АТС укажите IP назначения Media.

Для корректной работы при схеме развертывания Front CTS и Back[2] настройте в АТС 2 SIP-транк:

1. Для вызовов с АТС в Систему укажите IP назначения Back CTS.
2. Для вызовов с Системы в АТС укажите IP назначения Media.

УСТАНОВКА СЕРВИСА ССЫЛОК

Для установки сервиса ссылок:

1. Запустите командную строку.
2. Подключитесь к репозиторию разработчика в Docker для скачивания контейнеров:

```
docker login -u Login -p Password registry.public.express
```

Примечание. В качестве логина и пароля используются Login и Password, которые выдаются разработчиком.

[1] Сетевая схема взаимодействия с АТС при развертывании Single CTS и сетевые взаимодействия для данной схемы развертывания представлены в Приложении 8.

[2] Сетевая схема взаимодействия с АТС при развертывании Front CTS +Media и Back CTS и сетевые взаимодействия для данной схемы развертывания представлены в Приложении 9.

3. Создайте рабочий каталог веб-клиента:

```
mkdir -p /opt/xlnk
cd /opt/xlnk
echo DPL_IMAGE_TAG=xlnk-release > dpl.env
dpl --init
```

4. После выполнения команды dpl --init создается файл settings.yaml.
5. Установите цепочки сертификатов и ключа SSL:
   - при использовании собственного сертификата создайте директорию для сертификатов:

     Важно! Имя файла сертификата и имя ключа должны соответствовать примеру ниже:

     ```
     mkdir -p certs
     cp /somewhere/my-certificate-chain.crt certs/express.crt
     cp /somewhere/my-unencrypted-key.key certs/express.key
     ```

     Конструкции /somewhere/my-certificate-chain.crt и /somewhere/my-unencrypted-key.key индивидуальны для каждого конкретного случая.

     Конструкции certs/express.crt и certs/express.key являются обязательными.

     Требования к сертификатам изложены на стр. 34;
   - при использовании сертификата от Let's Encrypt в файл settings.yaml добавьте параметр le_email: admin@company-mail.ru.

     Проверка подключения сертификатов после инсталляции описана на стр. 71.

   Созданный по умолчанию файл конфигурации имеет следующий вид и требует редактирования:

   ```
   ccs_host: somehost.somedomain.sometld
   ```

   Пример заполнения конфигурации:

   ```
   ccs_host: xlnk.example.com
   le_email: test@example.com
   home_address: www.example.com
   android_app_link:
   'https://play.google.com/store/apps/details?id=ru.unlimitedtech.express'
   ios_app_link: 'https://apps.apple.com/ru/app/express-enterprise-messaging/id1225251588?l=en'ets_id: 00000000-0000-000-000-000000000000
   api_gw_url: 'http://link:4000'
   web_host_default: 'web.example.com'
   ```

   Перечень настроек с описанием представлен в табл. 41.
6. В каталоге /opt/express/xlnk выполните команду

   ```
   dpl -d
   ```

Для изменения файла конфигурации воспользуйтесь любым текстовым редактором и внесите исправления в файл (табл. 41):

табл. 41

Название настройки	Значение
ccs_host	Полное имя домена данного сервера, прописанное в DNS и соответствующее имени, на которое приобретался сертификат
le_email	Параметр устанавливается при использовании сертификата от компании Let`s Encrypt. Значение параметра должно соответствовать e-mail, на который будут приходить оповещения от Let`s Encrypt

Название настройки	Значение
home_address	Полное имя домена основного сайта компании, на который будут перенаправляться пользователи при обращении без ссылки на чат/конференцию
ets_id	Идентификатор сервера ETS, необходимый для определения ссылок, созданных на серверах предприятия. Включает отображение ссылок на мобильные приложения компании
android_app_link ios_app_link	Ссылки на мобильные приложения в магазинах приложений Apple, Play Market
android_app_name ios_app_name	Название ссылки на мобильные приложения, по умолчанию имеют значение Android Custom App, iOS Custom App. Отображается при переходе с мобильных устройств по ссылке
api_gw_url	Путь до сервиса xlink для доступа
web_host_default	Полное имя домена сервера web-клиента для чата/конференции

УСТАНОВКА DLPS

УСТАНОВКА DLPS НА ВЫДЕЛЕННОМ СЕРВЕРЕ

Для формирования ключа DLPS и добавления его во все чаты:

Внимание! В данном примере DLPS устанавливается на сервере, отделенном от CTS.

На сервере CTS укажите внешний DLPS.

Для инсталляции Docker, на Back-сервере, в файле /opt/express/settings.yaml допишите:

```
dlps_external: true
dlps_host: fqdn_dlps
```

После внесения изменений на этом же сервере выполните:

```
cd /opt/express/ && DPL_PULL_POLICY=never dpl -p && DPL_PULL_POLICY=never dpl --dc exec nginx nginx -s reload
```

Для инсталляции в k8s, в чарте в values.yaml заполните параметр:

```
dlps_host: fqdn_dlps
```

1. Запустите командную строку.
2. Подключитесь к репозиторию разработчика в Docker для скачивания контейнеров:

   ```
   docker login -u Login -p Password registry.public.express
   ```

   Примечание. В качестве логина и пароля используются Login и Password, которые выдаются разработчиком.
3. Скачайте контейнер-инсталлятор:

   ```
   docker run --rm registry.public.express/dpl:dlps-release dpl-install | bash
   ```
4. Создайте рабочий каталог веб-клиента:

   ```
   mkdir -p /opt/express
   cd /opt/express
   echo DPL_IMAGE_TAG=dlps -release > dpl.env
   dpl --init
   ```

   После выполнения команды dpl --init создается файл settings.yaml.
5. Установите цепочки сертификатов и ключа SSL.
   - при использовании собственного сертификата создайте директорию для сертификатов.

Важно! Имя файла сертификата и имя ключа должны соответствовать примеру ниже:

```
mkdir -p certs
cp /somewhere/my-certificate-chain.crt certs/express.crt
cp /somewhere/my-unencrypted-key.key certs/express.key
```

Конструкции /somewhere/my-certificate-chain.crt и /somewhere/my-unencrypted-key.key индивидуальны для каждого конкретного случая.

Конструкции certs/express.crt и certs/express.key являются обязательными.

Требования к сертификатам изложены на стр. 34.

- при использовании сертификата от Let's Encrypt в файл settings.yaml добавьте параметр le_email: admin@company-mail.ru.

  Проверка подключения сертификатов после инсталляции описана на стр. 71.

6. Выполните команду:

```
mkdir -p dlps_keys/storage && chown -R 888:888 dlps_keys
```

Созданный по умолчанию файл конфигурации имеет следующий вид и требует редактирования:

```
api_internal_token: token
ccs_host: somehost.somedomain.sometld
cts_id: ''
dlps_host: ''
dlps_icap_client_host: ''
dlps_icap_additional_headers: {}
etcd_endpoints: http://etcd:2379
kafka_host: kafka
phoenix_secret_key_base: token
postgres_endpoints: ''
postgres_user: ''
postgres_password: ''
redis_connection_string: ''
rts_id: ''dlps_enabled: true
```

Перечень настроек с описанием представлен в табл. 42.

7. Выполните команду (находясь в папке /opt/express):

```
dpl -d
```

После выполнения данной команды будет сгенерирован ключ, который будет добавляться во все чаты.

Для изменения файла конфигурации воспользуйтесь любым текстовым редактором и внесите исправления в файл.

табл. 42

Название настройки	Значение
Обязательные настройки	
ccs_host	Полное имя домена сервера CTS, прописанное в DNS и соответствующее имени, на которое приобретался сертификат
le_email	Параметр устанавливается при использовании сертификата от компании Let`s Encrypt. Значение параметра должно соответствовать e-mail, на который будут приходить оповещения от Let`s Encrypt
cts_id	Идентификатор установленного сервера
rts_id	Идентификатор сервера RTS (предоставляется разработчиком)
etcd_endpoints	Адрес подключения к ETCD-серверу
kafka_host	Адрес подключения к Kafka-серверу
redis_connection_string	Параметры подключения к базе данных REDIS

Название настройки	Значение
postgres_endpoints postgres_user postgres_password	Параметры подключения к базе данных PostgreSQL
dlps_postgres_endpoints dlps_postgres_user dlps_postgres_password	В случае использования отдельной базы для dlps-модуля указывается дополнительно
Необязательные настройки	
Доступ к веб-интерфейсу DLPS	admin_allow: - 10.0.0.0/8 - 172.16.1.0/24
Изменение пути к интерфейсу администратора DLPS	dlps_url: /dlps-admin-ui

УСТАНОВКА DLPS НА SINGLE CTS

Для формирования ключа DLPS и добавления его во все чаты:

Внимание! В данном примере DLPS устанавливается на Single CTS. Схемы установки для другого расположения DLPS запрашивайте у разработчиков.

1. Выполните команду:

```
mkdir -p dlps_keys/storage && chown -R 888:888 dlps_keys
```

2. Пропишите в файле конфигурации параметр dlps_enabled: true:

```
api_internal_token: S0L2U6zD0s2iQmdQ
ccs_host: cts_name.somedomain.sometld
cts_id: 'aaaa-bbbb-cccc-dddd'
phoenix_secret_key_base: verystrongpassword
prometheus_users: verystrongpassword
prometheus: verystrongpassword
rts_host: 'rts_name.somedomain.sometld'
rts_id: 'aaaa-bbbb-cccc-dddd'
rts_token: 'verystrongpassword'
dlps_enabled: true
```

3. Выполните команду (находясь в папке /opt/express):

```
dpl -d && dpl --dc restart nginx
```

4. После выполнения данной команды будет сгенерирован ключ, который будет добавляться во все чаты.
5. Консоль администратора будет доступа по URL https://express.mydomain.tld/dlps/. Стандартная учетная запись admin/admin.
6. В консоли администратора включите настройку DLPS нажатием кнопки «Enable DLPS» (рис. 13):

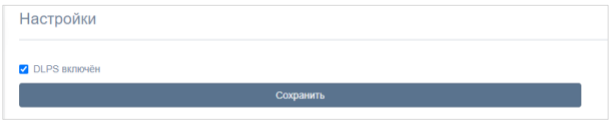

рис. 13

УСТАНОВКА DLPS НА SINGLE CTS С ХРАНЕНИЕМ КЛЮЧЕЙ НА ВНЕШНЕМ НОСИТЕЛЕ

Для настройки DLPS на внешнем носителе:

1. Вставьте USB-флеш-накопитель стандарта RW в компьютер и смонтируйте диск в нужную директорию. Директория по умолчанию — /opt/express-dlps/dlps_keys/. Файловая система на флеш-накопителе должна быть совместима с ОС RHEL.
2. Пропишите в файле конфигурации настройку dlps_keys_mount_path: /PATH_TO_DIRECTORY, где PATH_TO_DIRECTORY — путь к директории, куда записываются ключи.

   Например:

```
api_internal_token: TOKEN
ccs_host: cts_name.somedomain.sometld
cts_id: 'aaaa-bbbb-cccc-dddd'
dlps_icap_client_host: IP_ADDRESS
dlps_icap_client_port: PORT
dlps_icap_additional_headers: verystrongpassword
network_segment: CTS
application: PROD
client_ip: 127.0.0.1
server_ip: 127.0.0.1
kafka_host: etcd01.ru,etcd02.ru,etcd03.ru
phoenix_secret_key_base: PHOENIX_SECRET_KEY_BASE
etcd_endpoints:
http://etcd01.ru:2379,http://etcd02.ru:2379,http://etcd03.ru:2379
postgres_host: CTS.CTS.RU
postgres_user: POSTGRES_USER
postgres_password: POSTGRES_PASSWORD
dlps_keys_mount_path: /MOUNT_POINT
prometheus_users: verystrongpassword
prometheus: verystrongpassword
rts_id: 'aaaa-bbbb-cccc-dddd'
pacemaker_generate: true
pacemaker_virtual_ip: 10.0.0.1
```

3. Выполните команду:

```
mkdir -p dlps_keys/storage && chown -R 888:888 dlps_keys
```

4. Запустите DLPS (если DLPS уже запущен, то остановите и перезапустите):

```
dpl -d
```

5. Для проверки правильности установки убедитесь, что в файле /opt/express-dlps/dlps/docker-compose.yml, прописано верное значение volumes: «/PATH_TO_DIRECTORY:/app/keys».

УСТАНОВКА КОМПОНЕНТОВ ЗАПИСИ ЗВОНКОВ И КОНФЕРЕНЦИЙ

Примечания:

- перед установкой необходимо обновить версию сервера CTS до версии 3.10 и выше[1];
- перед установкой компонентов рекомендуется ознакомиться с архитектурой;
- необходимо открыть сетевой доступ с сервера Media к CTS Back по порту 443.

[1] Настройка записи звонков и конференций описана в одноименном разделе в документе «Руководство администратора. Т.2. Эксплуатация сервера CTS».

Для установки компонентов:

1. На Back CTS или Single CTS добавьте в /opt/express/settings.yaml:

```
transcoding_enabled: true
```

2. На сервере Back CTS или Single CTS выполните команду:

```
cd /opt/express/ && dpl -p && dpl -d transcoding_manager
recordings_bot admin && dpl --dc restart nginx
```

3. На сервере Media добавьте в /opt/express-voice/settings.yaml:

Примечание. Значения ccs_host, api_internal_token скопируйте из /opt/express/settings.yaml, расположенного на Back CTS или Single CTS.

```
transcoding_hosts:
  cts:
    ccs_host: cts.corp.express
    api_internal_token: token-cts
```

Если сервер записи и janus используется несколькими CTS, перечислить несколько хостов:

```
transcoding_hosts:
 cts1:
  ccs_host:
  cts1.corp.express
  api_internal_token: token-cts1
 cts2:
  ccs_host: cts2.corp.express
  api_internal_token: token-cts2
```

4. На сервере Media выполните команду:

```
cd /opt/express-voice/ && dpl -p && dpl -d
```

ПРОВЕРКА СЕРТИФИКАТОВ

Для тестирования корректности сертификата после инсталляции изделия выполните команду:

```
openssl s_client -connect fqnd-cts:443
```

Сообщение следующего вида сигнализирует об ошибке:

```
depth=0 CN = *.domain.ru
verify error:num=20:unable to get local issuer certificate
verify return:1
depth=0 CN = *.domain.ru
verify error:num=21:unable to verify the first certificate
verify return:1
```

ЗАПУСК СЕРВЕРА

Для запуска сервера:

Примечание. Команды для запуска сервера выполняются из каталога установки /opt/express.

1. Выполните команду:

Примечание. В случае использования разделенной установки, данная команда выполняется сначала на сервере Back CTS, затем—на сервере Front CTS.

```
dpl -d
```

2. Проверьте, запустились ли все контейнеры, с помощью команды:

```
docker ps -a
```

Если контейнеры не запустились, для просмотра журнала событий выполните команду:

```
dpl --dc logs --tail=200  <не_запускаемый_контейнер>
```

Если процедура установки сервера выполнена правильно, в течение пяти минут будет установлен и доступен веб-интерфейс администратора: https://ccs_host/admin.

Примечание. Для корректной работы веб-интерфейса администратора **не рекомендуется** использовать Internet Explorer.

3. Создайте учетную запись администратора. Команда должна производиться на Back CTS:

```
dpl --dc exec admin bin/admin add_admin -u admin -p
'veryinsecurepassword123'
```

Примечание. Требования к паролю администратора:

- минимальная длина пароля – 8 символов;
- пароль должен содержать как минимум один специальный символ #!?&@$%^&*(), одну строчную и одну прописную букву.

Если веб-интерфейс администратора не установился, то произошла ошибка несовпадения по политике паролей. В этом случае, а также в случае возникновения других ошибок выполните проверку.

Для проверки на наличие ошибок в появившихся логах найдите наиболее частое упоминание с ошибками и перезапустите контейнер, выдающий ошибку, с помощью команды:

```
dpl --dc restart {имя_контейнера}
```

Например:

```
dpl --dc restart nginx
```

Примечание. Все имена контейнеров, соответствующих конкретной архитектуре, перечислены в разделе «Архитектура».

Если операция не поможет, свяжитесь с технической поддержкой компании разработчика.

Глава 3

НАСТРОЙКА СЕРВЕРА

Для нормального функционирования системы необходимо выполнить предварительную настройку сервера в веб-интерфейсе администратора. Процедура настройки зависит от типа сервера и описывается в соответствующих разделах ниже:

- ETS;
- CTS.

Для авторизации в веб-интерфейсе администратора:

1. В адресной строке браузера укажите адрес веб-интерфейса администратора.

   Важно! Для ETS вход выполняется в веб-интерфейсе администратора https://ets_host/admin, для CTS — https://cts_host/admin. Без https веб-интерфейс администратора недоступен.

   Откроется окно авторизации (рис. 14):

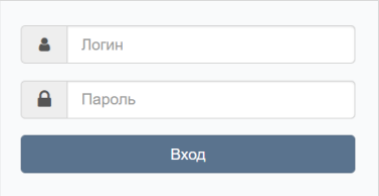

рис. 14

2. Введите имя учетной записи и пароль в соответствующие поля.
3. Нажмите «Вход».

   Откроется главное окно веб-интерфейса администратора.

Для выхода из веб-интерфейса администратора нажмите в верхней левой части окна.

НАСТРОЙКА ETS

Настройка ETS включает в себя следующие процедуры:

- подключение TLS-сертификата (если это не было выполнено в процессе установки ETS);
- настройка видео- и голосовой связи;
- подключение SMTP-сервера;
- настройка push-уведомлений;
- настройка CMC-сервера;
- подключение администраторов данного ETS из AD;
- настройка подключений CTS.

ПОДКЛЮЧЕНИЕ TLS-СЕРТИФИКАТА

Для настройки TLS-сертификата в веб-интерфейсе администратора выберите пункт меню «Сервер». Откроется окно с информацией о данном ETS-сервере (рис. 15).

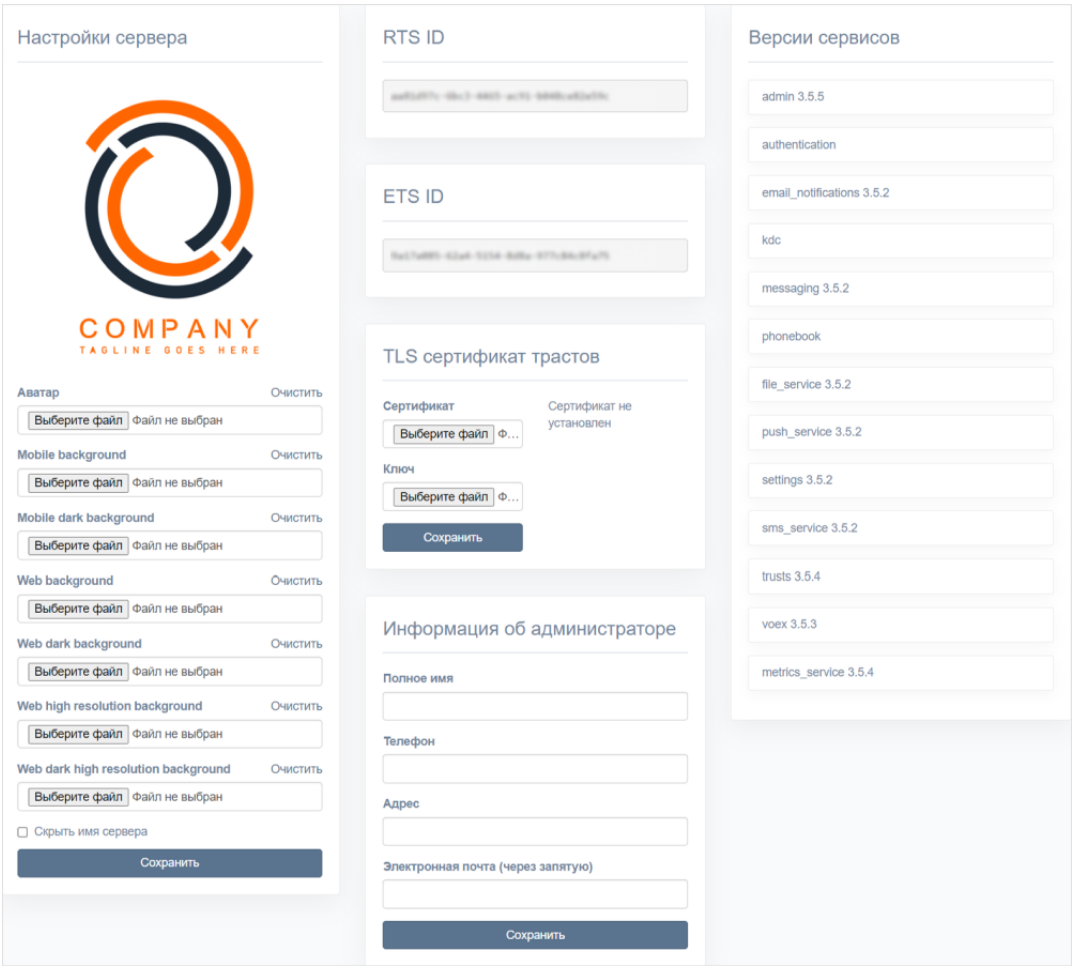

рис. 15

Для применения TLS-протокола в трастовых соединениях:

1. Внесите данные о сертификате и ключе в соответствующие поля области «TLS-сертификат трастов».
2. Нажмите «Сохранить».

Примечание. Допускается применение TLS-сертификата, использованного на этапе установки CTS.

НАСТРОЙКА ВИДЕО- И ГОЛОСОВОЙ СВЯЗИ

Настройка видео- и голосовой связи выполняется после установки сервера Media и описана на стр. 62.

ПОДКЛЮЧЕНИЕ SMTP-СЕРВЕРА

Для подключения SMTP-сервера:

1. В меню выберите пункт «E-mail».
   Откроется окно «Настройки e-mail» для ввода параметров (рис. 16).

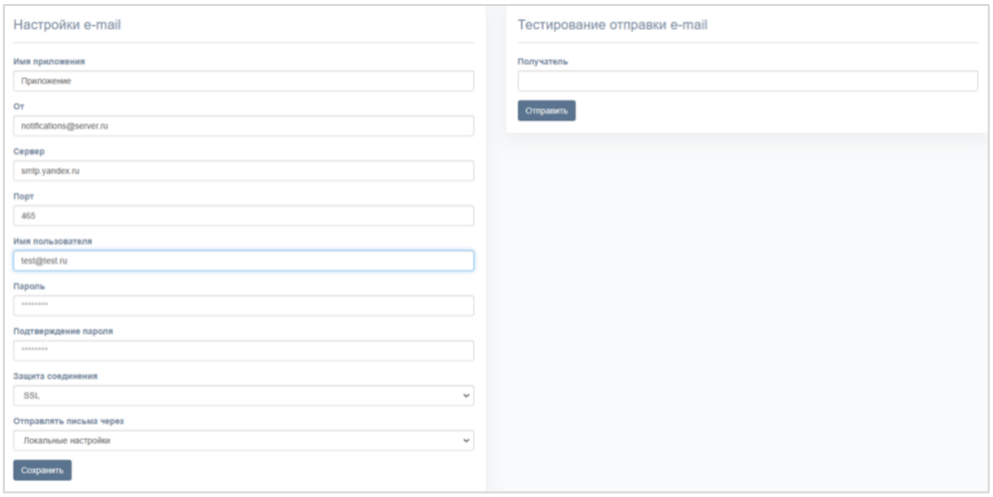

рис. 16

2. В области «Настройки e-mail» заполните поля формы. Описание полей представлено в табл. 43:

табл. 43

Поле	Описание
Имя приложения	Название приложения, от которого будут отправляться письма
От	Обратный адрес
Сервер	FQDN или IP-адрес почтового сервера
Порт	Номер порта для ретрансляции исходящей почты: 25, 587 или 465. Номер порта зависит от типа соединения
Имя пользователя	Адрес электронной почты
Пароль	Данные для авторизации на SMTP-сервере. Если не используется аутентификация на почтовом сервере, то данные поля оставьте пустыми
Подтверждение пароля	Данные для авторизации на SMTP-сервере. Если не используется аутентификация на почтовом сервере, то данные поля оставьте пустыми
Защита соединения	Тип защищенного соединения (выпадающий список: SSL, Start/TLS или пустое значение)
Отправлять письма через	Выпадающий список выбора сервера, с которого будут отправляться письма (при выборе «Локальные настройки» в выпадающем списке письма будут отправляться через сервер, настроенный в данном окне, при выборе «RTS» — через RTS)

3. Нажмите «Сохранить».

Для проверки настроек подключения воспользуйтесь областью «Тестирование отправки e-mail». Впишите в пустое поле адрес получателя и нажмите «Отправить».

НАСТРОЙКА PUSH-УВЕДОМЛЕНИЙ

Для подключения и настройки push-уведомлений перейдите в раздел «Push Service».

Интерфейс предназначен для подключения push-уведомлений (рис. 17).

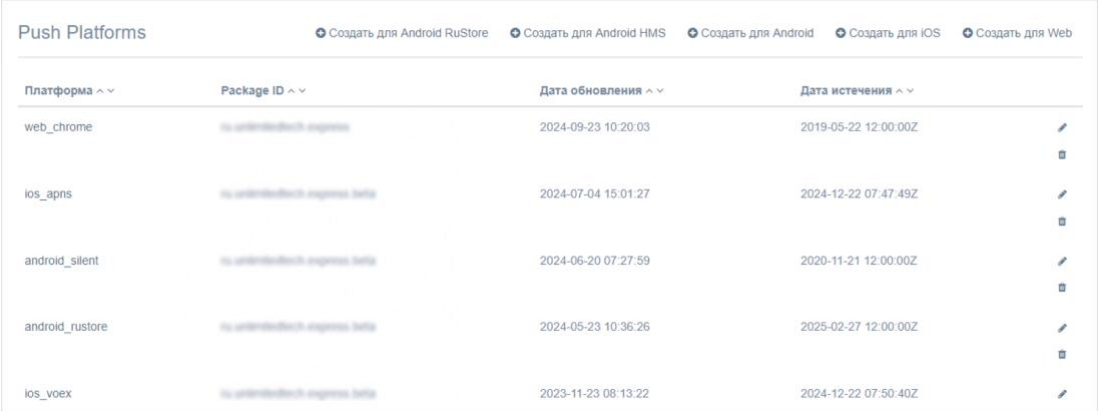

рис. 17

Описание интерфейса представлено в табл. 44:

табл. 44

Название столбца	Информация
Платформа	Платформа, на которой подключены push-уведомления
Package ID	Наименование пакета сборки приложения Express
Дата обновления	Дата последнего изменения настройки push-уведомлений
Дата истечения	Дата истечения поступления push-уведомлений

Для редактирования подключения нажмите и внесите изменения в открывшемся окне.

Для удаления подключения нажмите .

Механизм подключения push-уведомлений отличается в зависимости от платформы. Push-уведомления подключаются:

- для Android RuStore – через RuStore;
- Android — через FCM;
- Huawei — через Push Kit;
- iOS — через APNS;
- веб-приложения — через FCM.

Примечание. Для корректной работы необходим доступ к APN Push-сервисам:

- Apple APN — api.push.apple.com;
- Google FCM — fcm.googleapis.com; www.googleapis.com;
- Huawei HMS — push-api.cloud.huawei.com, oauth-login.cloud.huawei.com;
- RuStore — vkpns.rustore.ru.

При взаимодействии с внешними системами (Huawei HCM, Apple APN, Google FCM) push-уведомление может содержать следующие данные (табл. 45):

табл. 45

Название	Информация
group_chat_id	ID чата, где произошло событие
chat_type	Тип чата (chat(group_chat|botx))
push_opts	Дополнительные опции (silent – обработка не должна вызывать появления уведомления, dnd – уведомление должно отображаться, даже если на чате установлен режим «беззвучный», например, если в сообщении было упоминание текущего пользователя)

Название	Информация
sync_id	ID сообщения в чате
event_type	Тип сообщения (message_new|bot_command|app_event)
event_version	Версия сообщения (по умолчанию 1)
server_id	ID сервера – отправителя сообщения (кроме Android)
sender	ID пользователя – отправителя сообщения
push_tag_id	ID тега (кроме Android)
cleaned_at	Дата очистки сообщения, заполняется при удалении сообщения
unread_messages_count	Счетчик непрочитанных сообщений, отображаемый на иконке приложения (кроме Android)
missed_calls_count	Счетчик неотвеченных звонков (кроме Android)
parent_group_chat_id	ID родительского чата, где произошло событие (UID) (для звонков)
inserted_at	Время начала звонка (для звонков)
body	Текст нотификации (для SmartApp) (если пусто, то «Новое событие в SmartApp»)
meta	Метаданные нотификации (для SmartApp)
name	Название конференции
startAt	Время начала конференции

Для создания подключения на Android RuStore:

1. Войдите в консоль RuStore.
2. Создайте новое приложение (если еще не создано), нажав + Добавить приложение в правом верхнем углу страницы.
3. Войдите в созданное приложение и создайте новый проект в разделе «Push-уведомления -> Проекты», нажав «Добавить проект» (рис. 18).

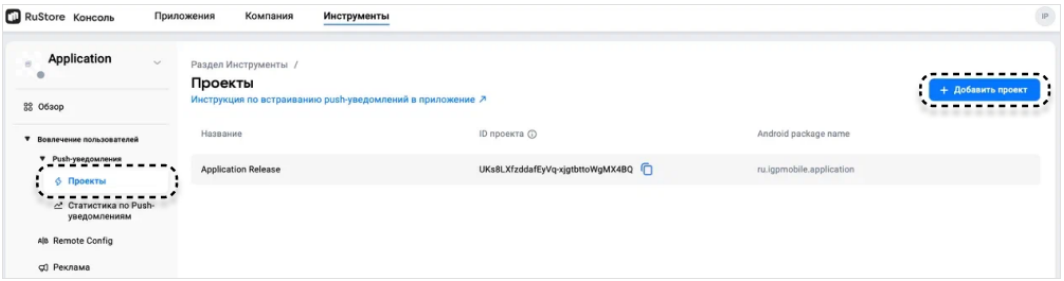

рис. 18

4. Заполните поля нового проекта (рис. 19) и нажмите «Создать».
   Описание параметров представлено в табл. 46.

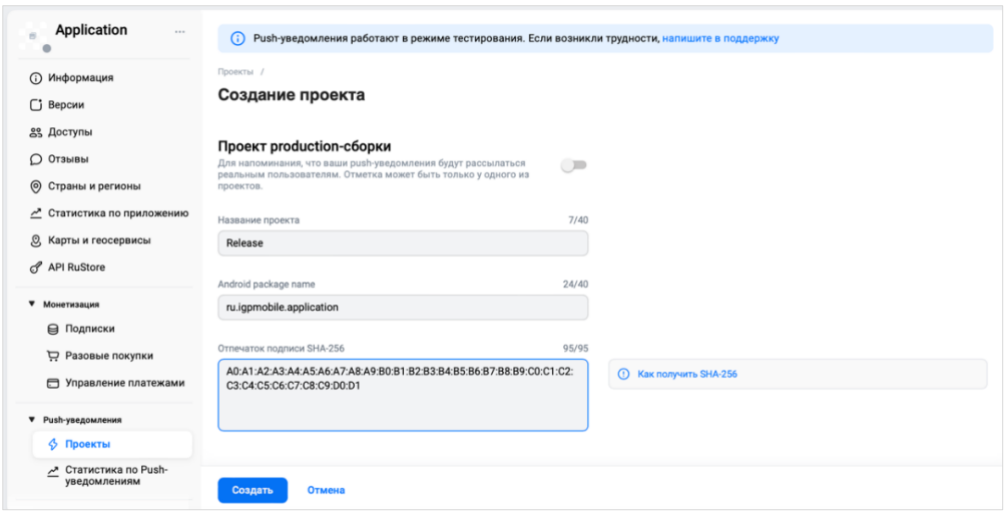

рис. 19

табл. 46

Параметр	Описание	Значение
Название проекта	Название проекта. Может быть произвольным.	Например: Release
Android Package Name	Это корректное наименование пакета вашего приложения	Например: com.app.packageid
Отпечаток подписи SHA-256	Для получения отпечатка подписи SHA-256 воспользуйтесь инструкцией по ссылке на странице	

5. Создайте сервисный токен (рис. 20):

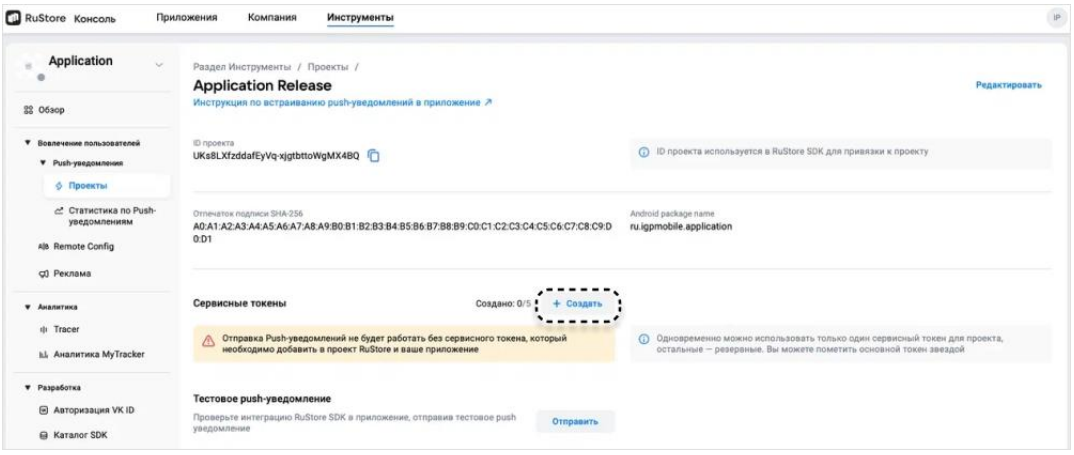

рис. 20

6. В веб-интерфейсе администратора СК Express в разделе Push Service нажмите «Создать для Android RuStore».

   Откроется окно создания подключения для платформы RuStore (рис. 21).

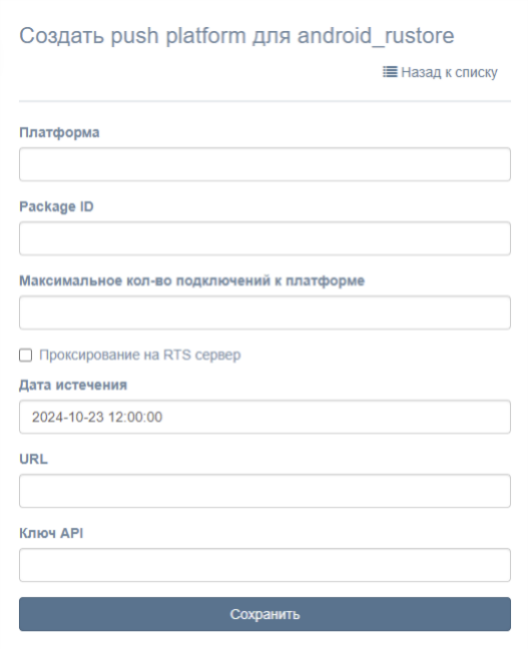

рис. 21

7. Заполните поля формы в соответствии с табл. 47:

табл. 47

Параметр	Описание	Значение
Платформа	Платформа, на которой подключены push-уведомления	android_rustore
Package ID	Наименование пакета сборки приложения Express	com.app.packageid
Максимальное количество подключений к платформе	Размер пула подключений к push-платформе	Если оставить поле пустым, то размер пула по умолчанию будет равен 10
Дата истечения	Дата истечения поступления push-уведомлений	
URL	Адрес проекта в RuStore (https://vkpns.rustore.ru/v1/projects/<project_id>/messages:send, где /<project_id> – это id проекта)	Например: https://vkpns.rustore.ru/v1/projects UKs8LXfzddafEyVq-xjgtbttoWgMX4BQ /messages:send
API Key	Ключ API, выдаваемый в консоли администратора RuStore	

8. Для включения проксирования на RTS-сервер поставьте отметку в соответствующем поле.
9. Нажмите «Сохранить».

Для создания подключения на Android:

1. Откройте консоль Firebase.
2. В проекте (меню «Project Overview»), где сконфигурированы ключи для Android, выберите пункт «Project settings».
3. В веб-интерфейсе администратора Express в разделе «Push Service» нажмите «Создать для Android» в верхнем правом углу.

   Откроется окно создания подключения для платформы Android (рис. 22).

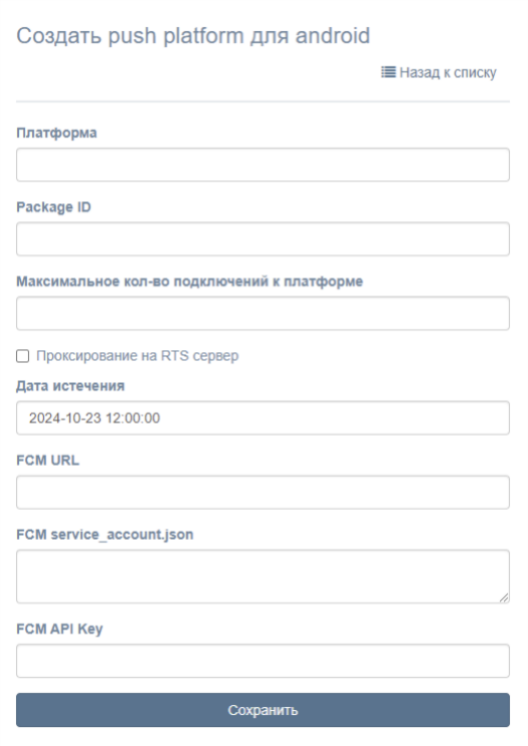

рис. 22

4. Заполните поля формы согласно табл. 48:

табл. 48

Параметр	Описание	Значение
Платформа	Платформа, на которой подключены push-уведомления	android_silent
Package ID	Наименование пакета сборки приложения Express	
Максимальное количество подключений к платформе	Размер пула подключений к push-платформе	Если оставить поле пустым, то размер пула по умолчанию будет равен 10
Дата истечения	Дата истечения поступления push-уведомлений	
FCM URL	Адрес сервера Firebase Cloud Messaging	https://fcm.googleapis.com/v1/projects/{fcmProjectID}/messages:send Значение ProjectID берется из консоли Firebase (Настройки проекта → General)
FCM service_account.json	JSON-файл сервисного аккаунта	Файл можно загрузить из консоли Firebase (Настройки проекта → Service Account)
FCM API Key	Ключ не предоставляется и не требуется на последней версии Firebase Cloud Messaging API (HTTP v1)	

5. Нажмите «Сохранить».

Для создания подключения на HMS Android:

1. Нажмите «Создать для HMS Android».

   Откроется окно создания подключения для платформы Huawei (рис. 23).

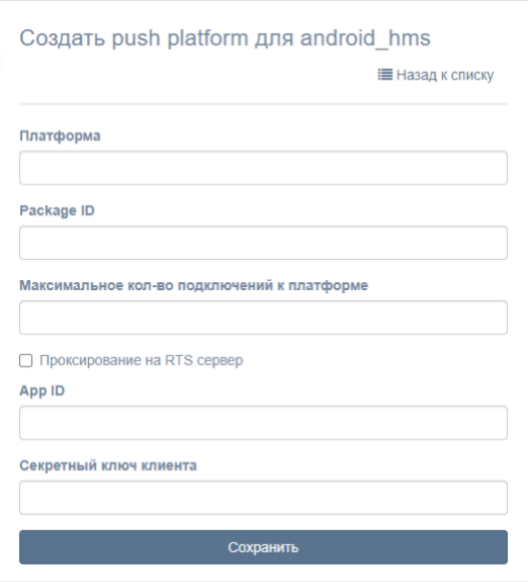

рис. 23

2. Заполните поля формы (табл. 49):

табл. 49

Параметр	Описание	Значение
Платформа	Платформа, на которой подключены push-уведомления	android_hms
Package ID	Наименование пакета сборки приложения Express	
Максимальное количество подключений к платформе	Размер пула подключений к push-платформе	Если оставить поле пустым, то размер пула по умолчанию будет равен 10
App ID	ID приложения в консоли Push Kit	
Секретный ключ клиента	Ключ в консоли Push Kit	

3. Нажмите «Сохранить».

Для создания подключения на iOS:

1. Нажмите «Создать для iOS» в верхнем правом углу.

   Откроется окно создания подключения для платформы iOS (рис. 24).

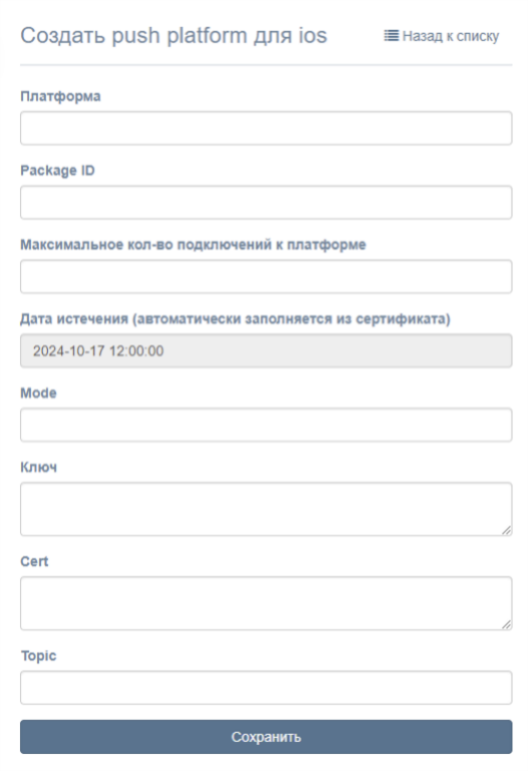

рис. 24

2. Заполните поля формы согласно табл. 50:

табл. 50

Параметр	Описание	Значение
Платформа	Платформа, на которой подключены push-уведомления	• ios_apns (для alert push с сертификатом apns); • ios_voex (для push-уведомлений звонков с сертификатом voip)
Package ID	Наименование пакета сборки приложения Express	
Максимальное количество подключений к платформе	Размер пула подключений к push-платформе	Если оставить поле пустым, то размер пула по умолчанию будет равен 10
Дата истечения	Дата истечения поступления push-уведомлений	
Mode	Режим работы push-уведомлений. Возможные значения prod/dev	• dev (для сборки beta); • prod (для релиза/пререлиза)
Ключ	Приватный ключ	
Cert	Сертификат	
Topic	Название сборки приложения Express	Package ID (для ios_apns); пустое значение (для ios_voex)

3. Нажмите «Сохранить».

Для создания подключения в веб-приложении:

1. Откройте консоль Firebase.
2. В консоли Firebase создайте проект для веб-приложения.
3. В открывшемся окне нажмите «Generate key pair».
4. В веб-интерфейсе администратора в разделе «Push Service» нажмите «Создать для Web» в верхнем правом углу.

Откроется окно создания подключения для веб-приложения (рис. 25).

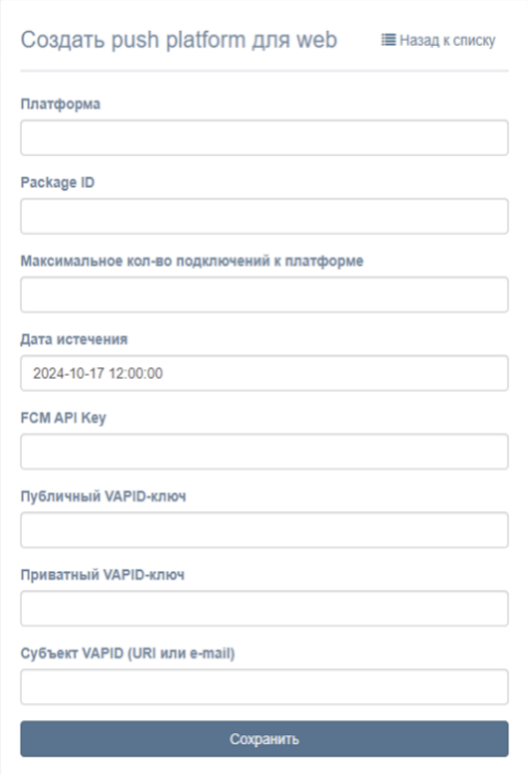

рис. 25

5. Заполните поля формы (табл. 51):

Примечание. В поле «Платформа» укажите значение «web».

табл. 51

Параметр	Описание	Значение
Платформа	Платформа, на которой подключены push-уведомления	• web; • web_chrome; • web_firefox; • web_edge
Package ID	Наименование пакета сборки приложения Express	
Максимальное количество подключений к платформе	Размер пула подключений к push-платформе	Если оставить поле пустым, то размер пула по умолчанию будет равен 10
Дата истечения	Дата истечения поступления push-уведомлений	
FCM API Key	Ключ API, выдаваемый в консоли администратора Firebase	
Публичный VAPID-ключ	Публичный ключ API, сгенерированный в консоли администратора Firebase	
Приватный VAPID-ключ	Приватный ключ API, сгенерированный в консоли администратора Firebase	
Субъект VAPID (URI или e-mail)	Адрес электронной почты пользователя в Firebase	mailto:<email аккаунта Firebase>

6. Нажмите «Сохранить».
7. Повторите действия 1–6 для Chrome, указав в поле «Платформа» значение «web_chrome».

   В разделе «Push Service» появятся две записи (для двух браузеров).

8. В конфигурационном файле docker-образа веб-приложения (WEB_CLIENT_CONFIG) измените параметр gcmSenderId на значение из Firebase.

НАСТРОЙКА СМС-СЕРВИСА

В разделе «SMS» администратор может настраивать текст отправляемого сообщения, интеграцию с провайдером, который будет отправлять пользователям СМС-сообщения с кодом авторизации, и параметры безопасности.

НАСТРОЙКА ТЕКСТА СМС-СООБЩЕНИЯ

Для настройки текста СМС-сообщения:

1. Выберите в меню раздел «SMS».

   Откроется окно «Настройки SMS».
2. В поле «Провайдер» выберите провайдера. Например, Beeline.
3. В поле «Текст SMS сообщения» введите текст, который будет отправляться вместе с кодом авторизации, и нажмите «Сохранить» (рис. 26).

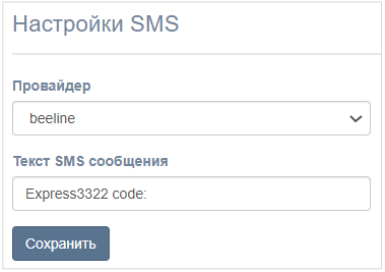

рис. 26

НАСТРОЙКА ИНТЕГРАЦИИ С ПРОВАЙДЕРОМ

Для настройки интеграции с провайдером:

1. Перейдите в подраздел «Адаптеры».
2. Установите параметры выбранного провайдера в соответствующей секции, и нажмите «Сохранить» (рис. 27).

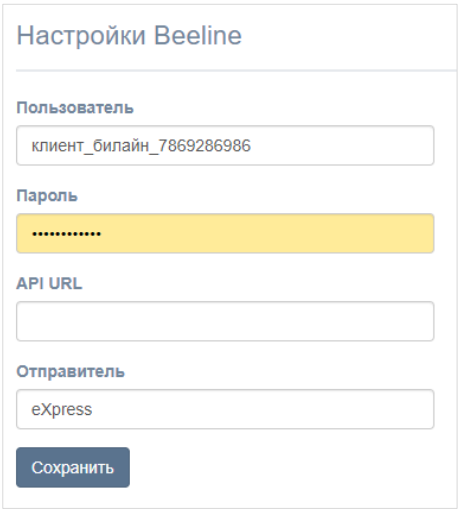

рис. 27

Настраиваемые параметры зависят от провайдера. Примеры настроек для провайдеров представлены в табл. 52:

табл. 52

Параметр	Назначение	Провайдер
Ключ API	Ключ для отправки СМС-сообщений. Предоставляется провайдером	Clickatell
API URL	Адрес API СМС-сервиса	Clickatell, QTelecom, Beeline, SMSTraffic
Пользователь	Имя пользователя СМС-сервиса провайдера	QTelecom, Beeline, SMSTraffic, Stream Telecom
Логин	Логин пользователя СМС-сервиса провайдера	SMSC, Tele2
Пароль	Пароль пользователя СМС-сервиса провайдера	QTelecom, Beeline, SMSC, Tele2, SMSTraffic, Stream Telecom
Отправитель	Имя отправителя СМС (например, eXpress)	QTelecom, Beeline, SMSC, SMSTraffic
Отправитель для MTS	Имя отправителя СМС (например, eXpress)	QTelecom
Shortcode	Предоставляется провайдером	Tele2
SID	Предоставляется провайдером	Twilio
Токен	Предоставляется провайдером	Twilio
От	Имя отправителя СМС-сообщения	Stream Telecom
Validity	Время жизни сообщения	Stream Telecom
Callback URL	Адрес скрипта, на который возвращаются POST данные о статусе доставки СМС	Stream Telecom
Пользователь	Цифровой идентификатор клиента, который возвращается на адрес, указанный в параметре Callback_url	Stream Telecom
Name deliver	Название рассылки, присваиваемое для удобства поиска в статистике	Stream Telecom

НАСТРОЙКА ПАРАМЕТРОВ БЕЗОПАСНОСТИ

В Express предусмотрены следующие параметры безопасности:

- ограничение количества запросов для определенного IP-адреса;
- фильтр по User-Agent;
- фильтр по DEF-коду;
- фильтр по номеру телефона;
- ограничение количества запросов на определенный телефонный номер.

Для настройки параметров безопасности:

1. Перейдите в подраздел «Безопасность».
2. Введите значения в соответствующие поля и нажмите «Сохранить» (рис. 28).

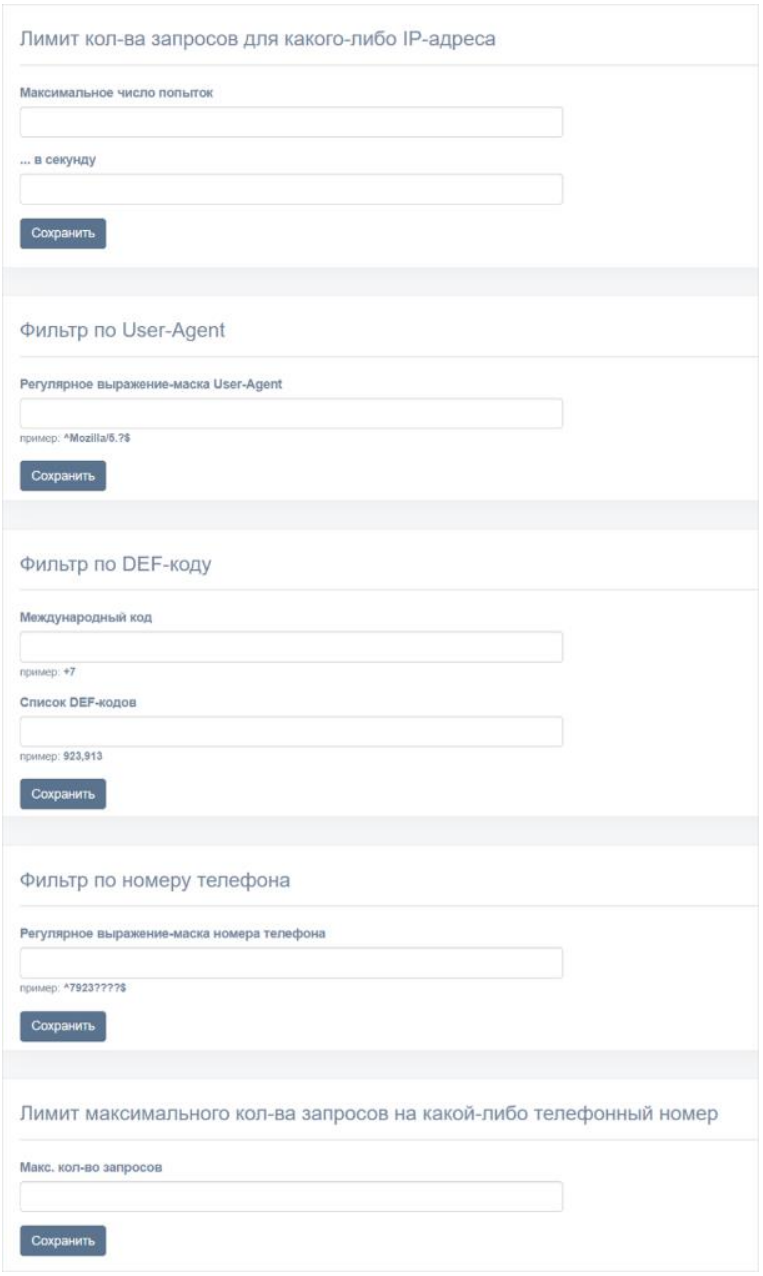
Лимит кол-ва запросов для какого-либо IP-адреса
Максимальное число попыток
... в секунду
Сохранить
Фильтр по User-Agent
Регулярное выражение-маска User-Agent
пример: ^Mozilla/5.?$
Сохранить
Фильтр по DEF-коду
Международный код
пример: +7
Список DEF-кодов
пример: 923,913
Сохранить
Фильтр по номеру телефона
Регулярное выражение-маска номера телефона
пример: ^7923????$
Сохранить
Лимит максимального кол-ва запросов на какой-либо телефонный номер
Макс. кол-во запросов
Сохранить

рис. 28

Для настройки загрузки учетных записей администратора из AD:

1. Перейдите в раздел «Аутентификация администраторов».
   Откроется окно (рис. 29):

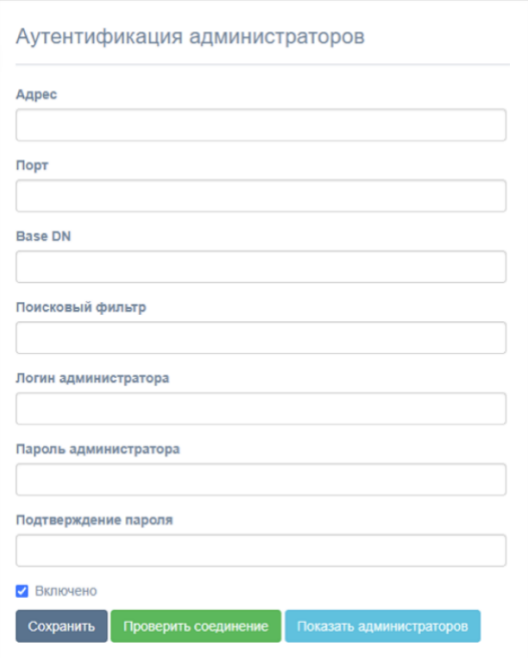

рис. 29

2. Настройте параметры, представленные в табл. 53.
   Значения параметров предоставляет администратор Active Directory.

табл. 53

Параметр	Описание
Адрес	Адрес Active Directory
Порт	Порт подключения к AD
Base DN	Объект каталога, начиная с которого производится поиск
Поисковый фильтр	Фильтр для поиска LDAP. Должен обеспечивать фильтрацию активных пользователей, которым разрешено подключение к данному серверу. Рекомендуемая конструкция запроса: «**(&(objectClass=person)(objectClass=user)(memberOf:1.2.840.113556.1.4.1941:=cn= express,ou=Groups,dc=firma,dc=local))**», где «**cn= express,ou=Groups,dc=firma,dc=local**» DN группы, члены которой будут пользователями Express. При использовании кроссдоменных структур укажите домен **DC=ru** в параметрах подключения. Пример настройки синхронизации административных пользователей с фильтром: **(|(memberOf=adm,OU=Groups,DC=example,DC=local)(memberOf=CN=adm_bot,OU=Groups,DC=example,DC=local)(memberOf=adm_ib,OU=Groups,DC=example,DC=local))**
Логин администратора	Логин пользователя, имеющего доступ к чтению списка пользователей по указанному DN
Пароль администратора	Пароль пользователя, имеющего доступ к чтению списка пользователей по указанному DN
Подтверждение пароля	Подтверждение пароля пользователя, имеющего доступ к чтению списка пользователей по указанному DN

Для включения/отключения аутентификации администраторов Active Directory установите/снимите флаг «Включено».

Для проверки соединения с Active Directory нажмите «Проверить соединение».

После нажатия кнопки «Показать администраторов» выводится список администраторов Active Directory.

НАСТРОЙКА ПОДКЛЮЧЕНИЙ КОРПОРАТИВНЫХ СЕРВЕРОВ

В разделе «Серверы» представлена информация об RTS-сервере, к которому подключен данный ETS-сервер (рис. 30), и о CTS-серверах, подключенных к данному ETS-серверу (рис. 31).

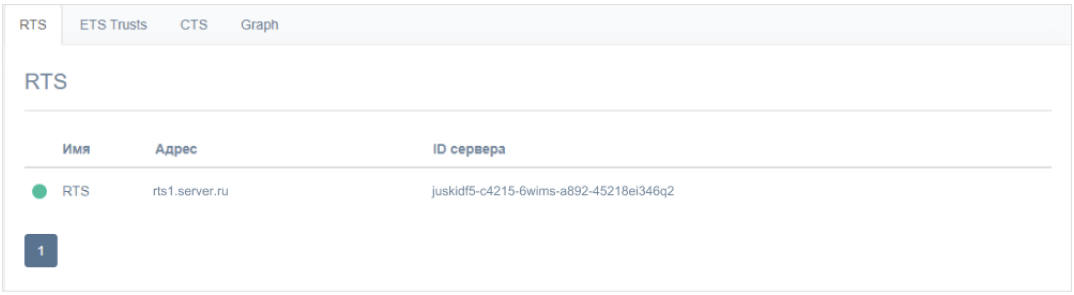

рис. 30

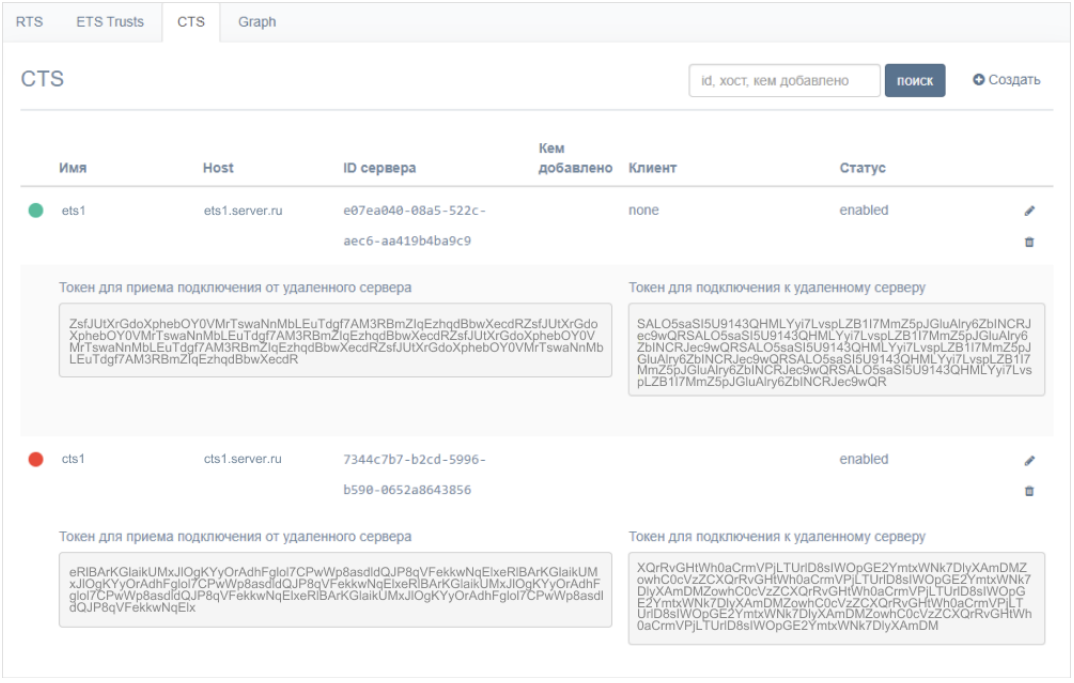

рис. 31

Статус подключения серверов RTS и CTS обозначается с помощью цветовых маркеров рядом с именами серверов.

- зеленый — сервер подключен и есть связь;
- фиолетовый — сервер заблокирован;
- красный — сервер подключен и нет связи;
- пустое место — сервер подключен к другому RTS.

Раздел «Серверы» позволяет:

- просматривать информацию о графической схеме маршрутизации подключений;
- просматривать информацию о подключении к отдельному серверу на графической схеме маршрутизации подключений.

Для просмотра графической схемы маршрутизации подключений откройте вкладку «Graph» (рис. 32).

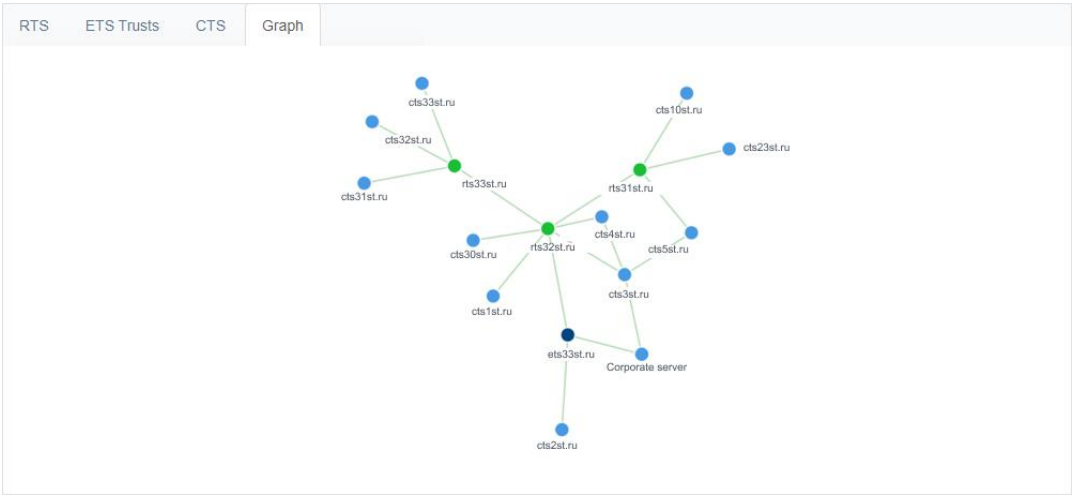

рис. 32

Серверы обозначены на схеме цветными кругами в зависимости от типа:

- RTS — зеленым;
- ETS — фиолетовым;
- CTS — синими.

Для удобства просмотра элементы схемы можно перетаскивать с помощью мыши.

Для просмотра информации о подключении к серверу на схеме:

1. На вкладке «Graph» нажмите на круг, которым обозначен данный сервер.

   В правом верхнем углу экрана отобразится адрес выбранного сервера и количество чатов, созданных на нем (рис. 33).

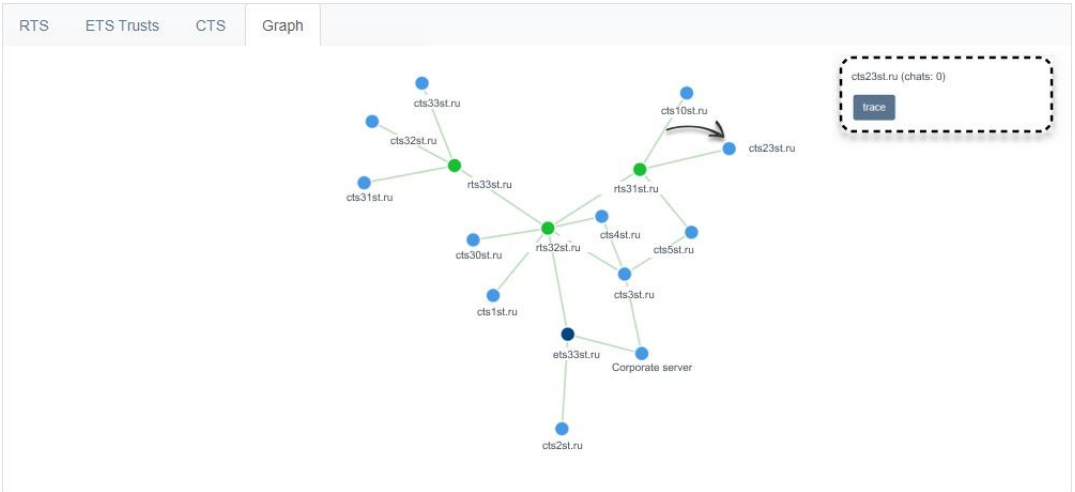

рис. 33

2. Нажмите на название сервера в правом верхнем углу экрана.

   Откроется окно с информацией об RTS/ETS/TTS, через который происходит обмен данными с текущим сервером (рис. 34).

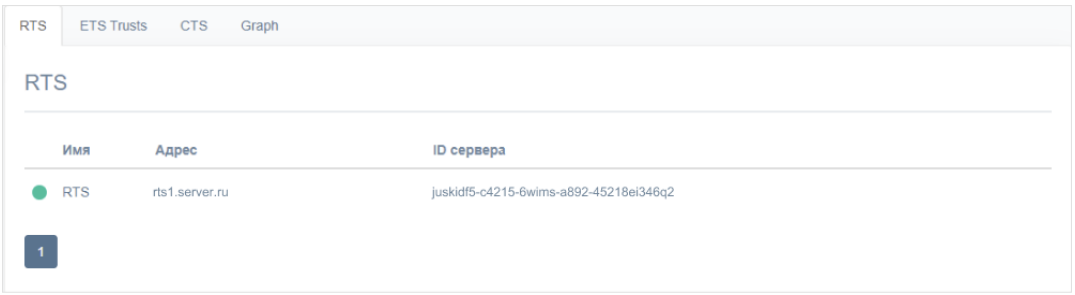

рис. 34

НАСТРОЙКА CTS

Настройка CTS включает в себя следующие процедуры:

- подключение TLS-сертификата (если это не было выполнено в процессе установки ETS);
- подключение Botx SSL-сертификата;
- настройка видео- и голосовой связи;
- подключение SMTP-сервера;
- подключение администраторов данного CTS из AD;
- настройка интеграции с Active Directory;
- настройка доверительных подключений.

ПОДКЛЮЧЕНИЕ TLS-СЕРТИФИКАТА И BOTX SSL-СЕРТИФИКАТА

Для применения TLS-протокола в трастовых соединениях:

1. Выберите пункт меню «Сервер».

   Откроется окно с информацией о данном CTS (рис. 35).

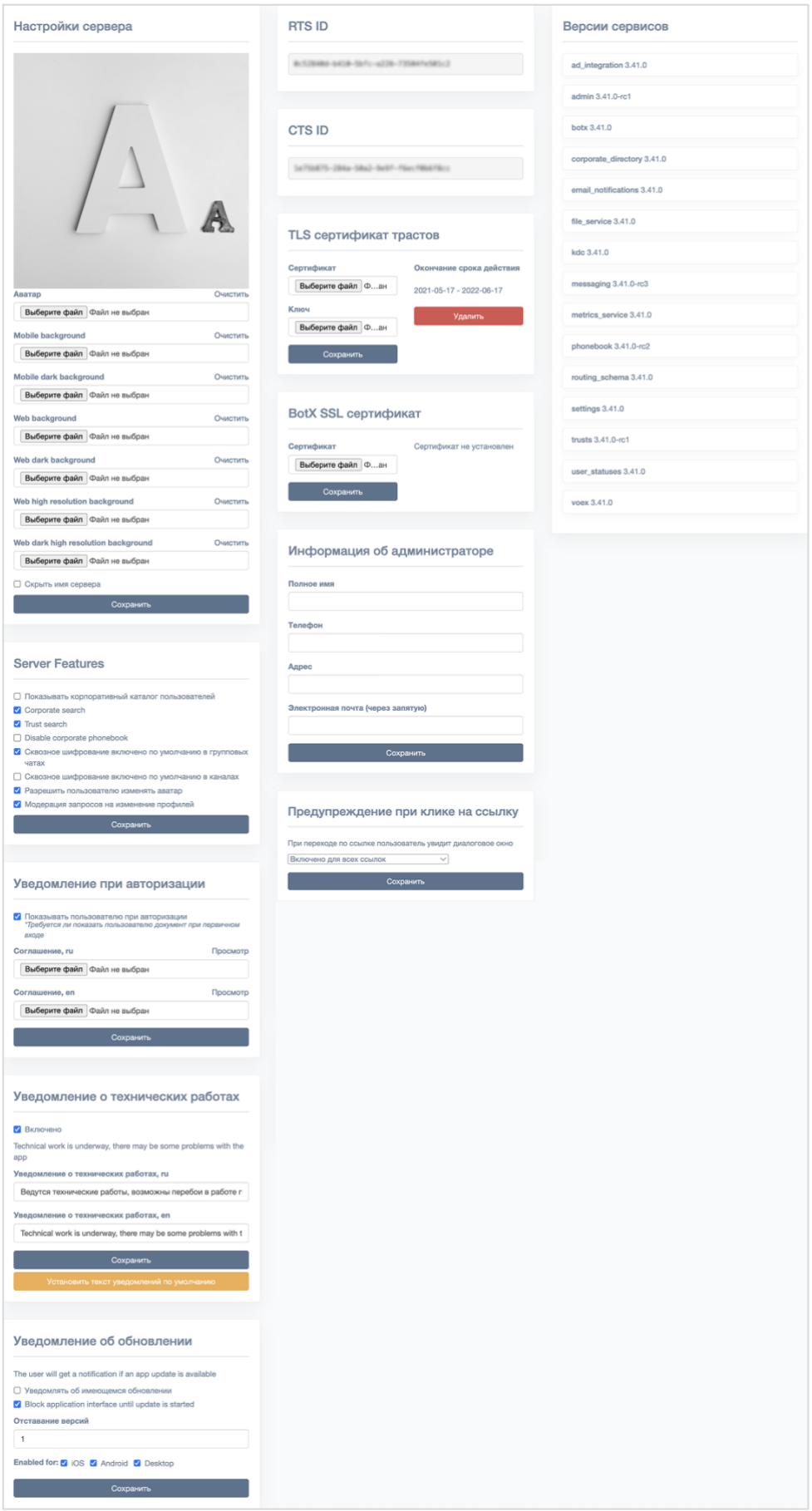
Настройки сервера
Аватар
Очистить
Выберите файл
Файл не выбран
Mobile background
Mobile dark background
Web background
Web dark background
Web high resolution background
Web dark high resolution background
Скрыть имя сервера
Сохранить
Server Features
Показывать корпоративный каталог пользователей
Corporate search
Trust search
Disable corporate phonebook
Сквозное шифрование включено по умолчанию в групповых чатах
Сквозное шифрование включено по умолчанию в каналах
Разрешить пользователю изменять аватар
Модерация запросов на изменение профилей
Уведомление при авторизации
Показывать пользователю при авторизации
Соглашение, ru
Просмотр
Соглашение, en
Уведомление о технических работах
Включено
Technical work is underway, there may be some problems with the app
Уведомление о технических работах, ru
Ведутся технические работы, возможны перебои в работе г
Уведомление о технических работах, en
Technical work is underway, there may be some problems with t
Установить текст уведомлений по умолчанию
Уведомление об обновлении
The user will get a notification if an app update is available
Уведомлять об имеющемся обновлении
Block application interface until update is started
Отставание версий
Enabled for: iOS Android Desktop
RTS ID
CTS ID
TLS сертификат трастов
Сертификат
Окончание срока действия
2021-05-17 - 2022-06-17
Ключ
Удалить
BotX SSL сертификат
Сертификат не установлен
Информация об администраторе
Полное имя
Телефон
Адрес
Электронная почта (через запятую)
Предупреждение при клике на ссылку
При переходе по ссылке пользователь увидит диалоговое окно
Включено для всех ссылок
Версии сервисов
ad_integration 3.41.0
admin 3.41.0-rc1
botx 3.41.0
corporate_directory 3.41.0
email_notifications 3.41.0
file_service 3.41.0
kdc 3.41.0
messaging 3.41.0-rc3
metrics_service 3.41.0
phonebook 3.41.0-rc2
routing_schema 3.41.0
settings 3.41.0
trusts 3.41.0-rc1
user_statuses 3.41.0
voex 3.41.0

рис. 35

2. Внесите данные о сертификате и ключе в соответствующие поля области «TLS-сертификат трастов» (рис. 36).

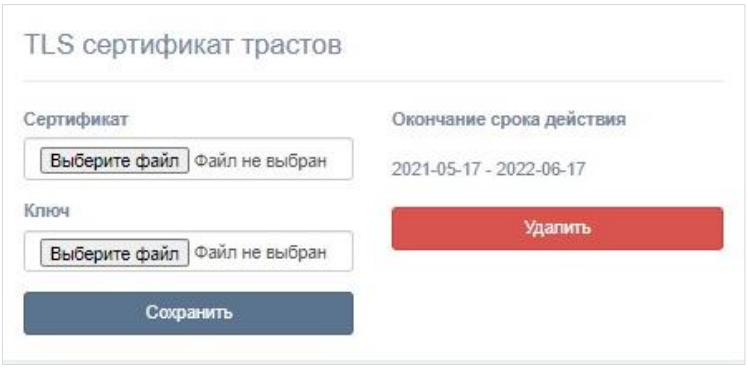

рис. 36

3. Нажмите «Сохранить».

Примечание. Допускается применение TLS-сертификата, использованного на этапе установки CTS.

Для подключения сертификата чат-бота в области «BotX SSL сертификат» введите данные о сертификате и нажмите «Сохранить» (рис. 37).

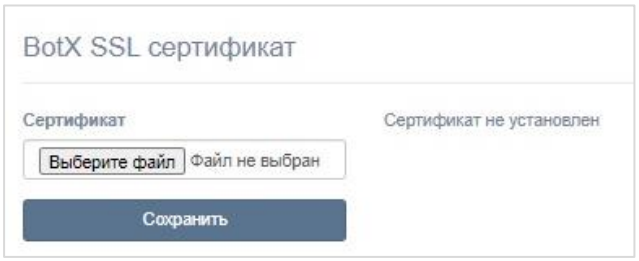

рис. 37

НАСТРОЙКА ВИДЕО- И ГОЛОСОВОЙ СВЯЗИ

Настройка видео- и голосовой связи выполняется после установки сервера Media и описана на стр. 62.

ПОДКЛЮЧЕНИЕ SMTP-СЕРВЕРА

Для подключения SMTP-сервера:

1. В меню выберите пункт «E-mail».

   Откроется окно «Настройки e-mail» для ввода параметров (рис. 38):

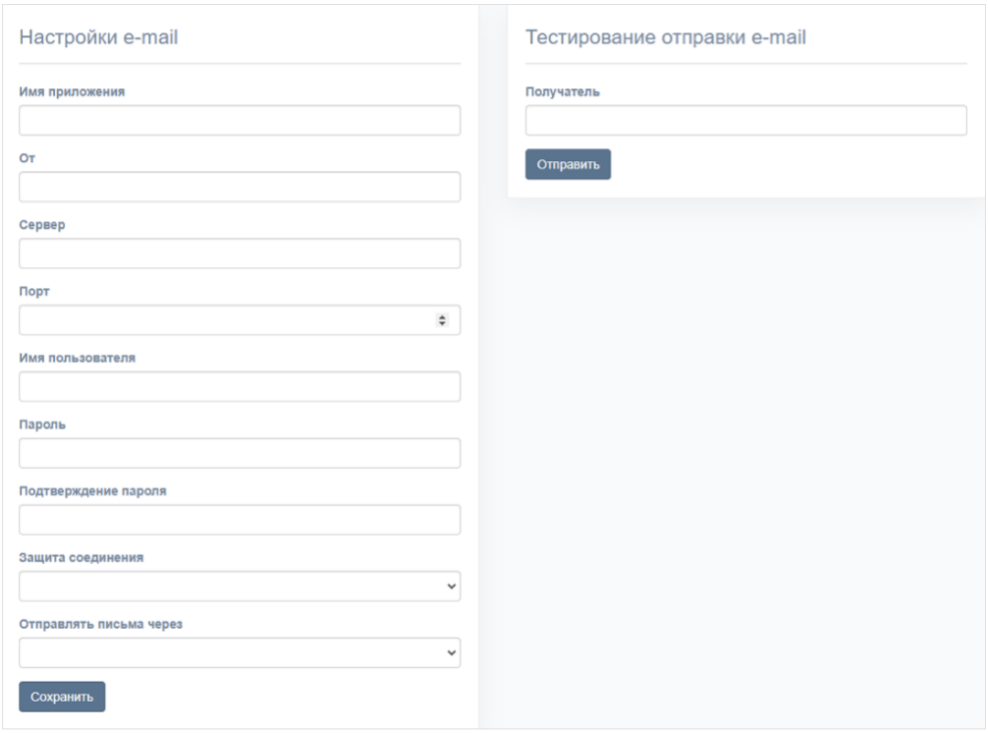

рис. 38

2. В окне «Настройки e-mail» заполните поля (табл. 54):

табл. 54

Поле	Описание
Имя приложения	Название приложения, от которого будут отправляться письма
От	Обратный адрес
Сервер	FQDN или IP-адрес почтового сервера
Порт	Номер порта для ретрансляции исходящей почты: 25, 587 или 465. Номер порта зависит от типа соединения
Имя пользователя	Адрес электронной почты
Пароль	Данные для авторизации на SMTP-сервере. Если не используется аутентификация на почтовом сервере, то данные поля оставьте пустыми
Подтверждение пароля	Данные для авторизации на SMTP-сервере. Если не используется аутентификация на почтовом сервере, то данные поля оставьте пустыми
Защита соединения	Тип защищенного соединения (выпадающий список: SSL, Start/TLS или пустое значение)
Отправлять письма через	Выпадающий список выбора сервера, с которого будут отправляться письма (при выборе «Локальные настройки» в выпадающем списке письма будут отправляться через сервер, настроенный в данном окне, при выборе «RTS» — через RTS)

3. Нажмите «Сохранить».

Для проверки настроек подключения воспользуйтесь областью «Тестирование отправки e-mail». Впишите в пустое поле адрес получателя и нажмите «Отправить».

НАСТРОЙКА АУТЕНТИФИКАЦИИ АДМИНИСТРАТОРОВ

Раздел предназначен для подключения администраторов с помощью AD.

Для настройки загрузки учетных записей администратора из AD:

1. Перейдите в раздел «Аутентификация администраторов» (рис. 39).

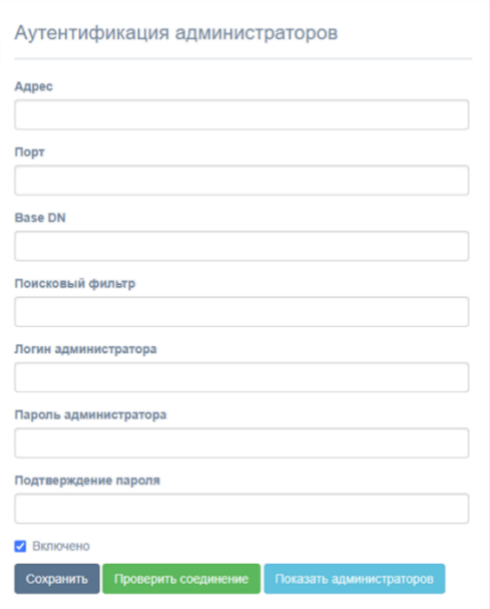

рис. 39

2. Настройте параметры, представленные в табл. 55.

   Значения параметров предоставляет администратор Active Directory.

табл. 55

Параметр	Описание
Адрес	Адрес Active Directory
Порт	Порт подключения к AD
Base DN	Объект каталога, начиная с которого производится поиск
Поисковый фильтр	Фильтр для поиска LDAP. Должен обеспечивать фильтрацию активных пользователей, которым разрешено подключение к данному серверу. Рекомендуемая конструкция запроса: «**(&(objectClass=person)(objectClass=user)(memberOf:1.2.840.113556.1.4.1941:=cn= express,ou=Groups,dc=firma,dc=local))**», где «**cn= express,ou=Groups,dc=firma,dc=local**» DN группы, члены которой будут пользователями Express. При использовании кроссдоменных структур укажите домен **DC=ru** в параметрах подключения. Пример настройки синхронизации административных пользователей с фильтром: **(|(memberOf=adm,OU=Groups,DC=example,DC=local)(memberOf=CN=adm_bot,OU=Groups,DC=example,DC=local)(memberOf=adm_ib,OU=Groups,DC=example,DC=local))**
Логин администратора	Логин пользователя, имеющего доступ к чтению списка пользователей по указанному DN
Пароль администратора	Пароль пользователя, имеющего доступ к чтению списка пользователей по указанному DN
Подтверждение пароля	Подтверждение пароля пользователя, имеющего доступ к чтению списка пользователей по указанному DN

Для включения/отключения аутентификации администраторов Active Directory установите/снимите флаг «Включено».

Для проверки соединения с Active Directory нажмите «Проверить соединение».

После нажатия кнопки «Показать администраторов» выводится список администраторов Active Directory.

НАСТРОЙКА РЕГИСТРАЦИИ

Важно! Неудачное сочетание кастомизации первого экрана входа в приложение, включения и отключения регистрации без номера и возможность задавать права пользователю на выполнение ряда операций со своим номером телефона может привести к неудачному сочетанию, которое вызовет потерю доступа к приложению! Ряд распространенных ошибок, вызванных неправильной настройкой сервера, представлен в разделе «Устранение типовых ошибок».

Администратору доступны следующие способы для настройки регистрации/авторизации пользователей в системе:

- Active Directory (NTLM);
- E-mail;
- OpenID;
- Регистрация без номера телефона.

Для выбора способа регистрации:

1. Перейдите в раздел «Настройка регистрации» (рис. 40).
2. Выберите метод регистрации.
3. Выберите источник синхронизации.
4. Задайте расписание синхронизации (в формате cron).

Внимание! Для запуска задачи, обеспечивающей выбранный метод регистрации, данный шаг является обязательным.

5. Нажмите «Сохранить».

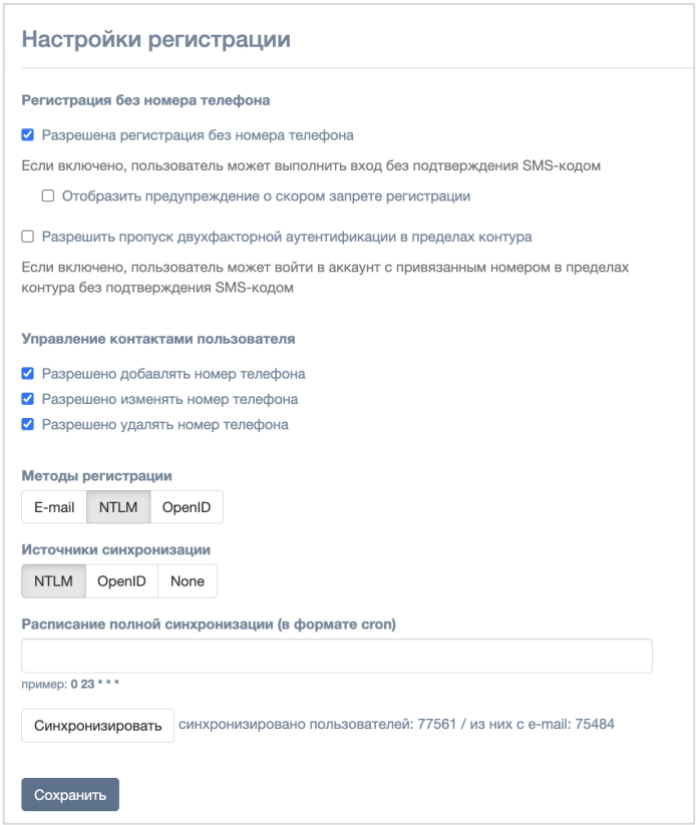

рис. 40

Выбранный метод регистрации будет сохранен. В верхней части экрана появится соответствующее системное сообщение.

Для завершения настройки задайте параметры для указанного способа в соответствующей вкладке: E-mail, NTML или OpenID.

НАСТРОЙКА ИНТЕГРАЦИИ С ACTIVE DIRECTORY

Для интеграции с AD подключитесь к AD и загрузите контакты на сервер.

При интеграции Express с корпоративным каталогом на базе Microsoft Active Directory создайте учетную запись с правами «Domain Users» и чтение контейнера «deleted objects» (https://support.microsoft.com/en-us/help/892806/how-to-let-non-administrators-view-the-active-directory-deleted-object).

Для подключения к Active Directory:

Примечание. Для корректной настройки системы под домен заказчика рекомендуется привлечь администратора Active Directory.

1. Перейдите в раздел «Active Directory».

   Откроется окно настройки параметров регистрации через Active Directory (рис. 41).

2. В левой колонке в текстовых полях задайте значения параметров для синхронизации пользователей LDAP (рис. 41, табл. 56).

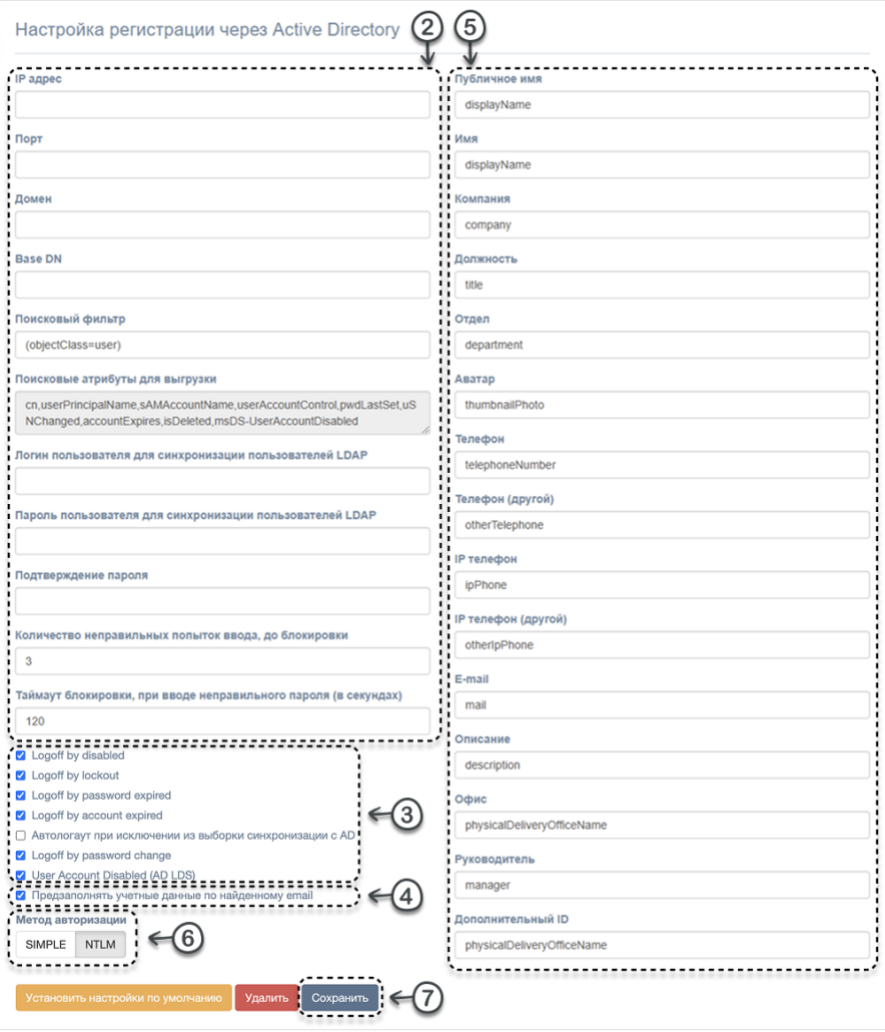

рис. 41

табл. 56

Параметр	Назначение
IP-адрес	IP-адрес LDAP. Если требуется подключение по протоколу LDAPS, то перед именем домена или IP-адреса введите «ldaps://», например «ldaps://firma.local»
Порт	Порт подключения к AD. Для протокола LDAP введите значение «389», для протокола LDAPS — значение «636»
Домен	Домен сервера, на который выгружаются учетные записи
Base DN	Объект каталога, начиная с которого производится поиск
Поисковый фильтр	Фильтр для поиска в Active Directory
Поисковые атрибуты для выгрузки	Выгружаемые атрибуты учетных записей
Логин пользователя для синхронизации пользователей LDAP	Логин для подключения к AD для синхронизации
Пароль пользователя для синхронизации пользователей LDAP	Пароль для подключения к AD для синхронизации
Подтверждение пароля	Подтверждение пароля для подключения к AD для синхронизации
Количество неправильных попыток ввода, до блокировки	Максимальное количество попыток ввода пароля, после которого учетная запись блокируется
Таймаут блокировки, при вводе неправильного пароля (в секундах)	Время в секундах, на которое блокируется приложение при вводе неверного пароля

3. Укажите события в Active Directory, при которых у пользователя Express будет повторно запрашиваться аутентификация на корпоративном сервере Express (табл. 57):

табл. 57

Параметр	Назначение
Logoff by disabled	После отключения учетной записи пользователя создает запрос на отключение пользователя от CTS. Данный запрос требует подтверждения в разделе «Запросы на логаут», после подтверждения пользователь будет автоматически отключен от CTS
Logoff by lockout	после временной блокировки учетной записи пользователя в AD создается запрос на отключение пользователя от CTS. Все активные сессии пользователя будут закрыты. Данный запрос требует подтверждения в разделе «Запросы на логаут», после подтверждения пользователь будет автоматически отключен от CTS
Logoff by password expired	Если срок действия пароля пользователя в AD истек, создается запрос на отключение пользователя от CTS. Все активные сессии пользователя будут закрыты. Данный запрос требует подтверждения в разделе «Запросы на логаут», после подтверждения пользователь будет автоматически отключен от CTS
Logoff by account expired	Если срок действия учетной записи пользователя в AD истек, создается запрос на отключение пользователя от CTS. Все активные сессии пользователя будут закрыты. Данный запрос требует подтверждения в разделе «Запросы на логаут», после подтверждения пользователь будет автоматически отключен от CTS
Автологаут при исключении из выборки синхронизации с AD	Если учетная запись пользователя исключена из группы, создается запрос на отключение пользователя от CTS. Все активные сессии пользователя будут закрыты. Данный запрос требует подтверждения в разделе «Запросы на логаут», после подтверждения пользователь будет автоматически отключен от CTS
Logoff by password change	Если пароль от учетной записи пользователя в AD изменен, создается запрос на отключение пользователя от CTS. Все активные сессии пользователя будут закрыты. Данный запрос требует подтверждения в разделе «Запросы на логаут», после подтверждения пользователь будет автоматически отключен от CTS
User Account Disabled (AD LDS)	Если учетная запись пользователя заблокирована, создается запрос на отключение пользователя от CTS. Все активные сессии пользователя будут закрыты. Данный запрос требует подтверждения в разделе «Запросы на логаут», после подтверждения пользователь будет автоматически отключен от CTS

4. Активируйте настройку «Предзаполнять учетные данные по найденному email» для упрощенной авторизации пользователей. При активированной настройке, когда нашлось сопоставление упрощенной аутентификации, данные о логине и домене будут предзаполнены.
5. В правой колонке укажите атрибуты, которые будут отображаться в карточке пользователя. Подробнее данная настройка описана ниже.
6. Выберите метод авторизации: упрощенная или через NTLM, нажав на кнопку «Simple» или «NTLM».
7. Нажмите «Сохранить» для сохранения изменений.

   Если все настройки указаны правильно, в течение трех часов список пользователей появится в разделе «Пользователи».

Для выполнения синхронизации с LDAP нажмите «Синхронизировать».

Для удаления изменений нажмите «Удалить».

В случае возникновения проблем при синхронизации проверьте корректность полученных данных из AD с помощью команды ldapsearch (красным цветом выделены параметры, которые требуется заменить в соответствии с настройками подключения к AD):

```
$ ldapsearch -v -h myhost.mydomain.mytld -p 389 -D 'mydomain\myuser'
-W -b "cn=Users,dc=mydomain,dc=mytld" -s sub
"(&(objectCategory=person)(objectClass=user)(memberOf:1.2.840.113556.
1.4.1941:=CN=ExpressUsers,CN=Users,DC=mydomain,DC=mytld))" -x
```

Примечание. Для OS Ubuntu версии 19 и выше, а также при возникновении ошибки на других OS, выполните следующую команду:

```
$ ldapsearch -v -H myhost.mydomain.mytld -p 389 -D 'mydomain\myuser' -W -b
"cn=Users,dc=mydomain,dc=mytld" -s sub
"(&(objectCategory=person)(objectClass=user)(memberOf:1.2.840.113556.1.4.1941
:=CN=ExpressUsers,CN=Users,DC=mydomain,DC=mytld))" -x
```

Для предоставления доступа пользователей к Express создайте группы пользователей Express в Active Directory. Тип группы — «Security», видимость группы — «Universal».

При интеграции Express с корпоративным каталогом на базе LDAP-совместимого сервера создайте учетную запись с правами чтения каталога.

Для настройки видимости полей профиля:

1. Перейдите в раздел «Настройки видимости полей».

   Откроется окно «Видимость полей профиля» (рис. 42):

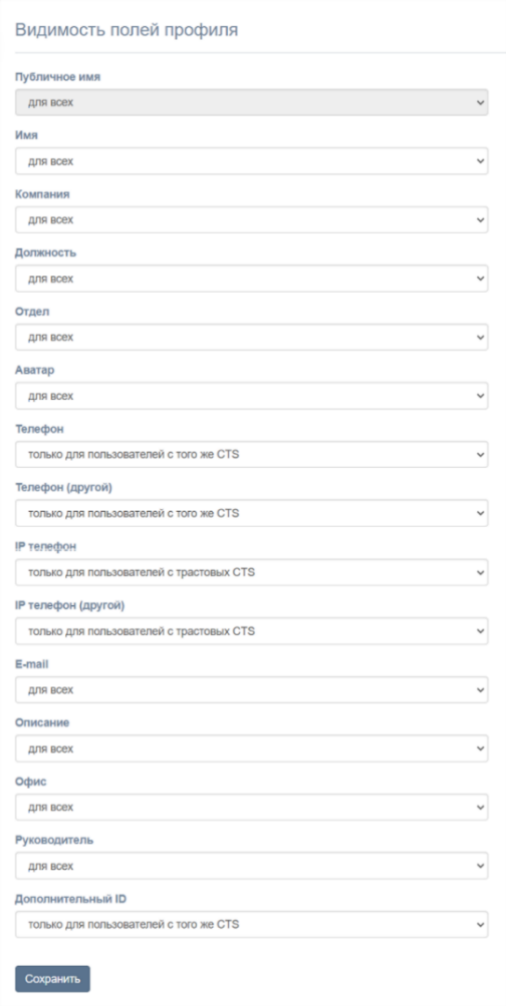

рис. 42

2. Установите значения корпоративных переменных профиля в полях доступа.

   Корпоративные переменные профиля автоматически заполняются значениями из базы AD и доступны для просмотра в приложении в карточке чата. Описание уровня доступа к данным представлено в табл. 58:

   табл. 58

Название поля	Комментарий
Никому	Значение данного поля недоступно для просмотра в приложении
Только для пользователей с того же CTS	Значение данного поля доступно для просмотра в приложении только пользователям, зарегистрированным на данном корпоративном сервере
Только для пользователей с трастовых CTS	Значение данного поля доступно для просмотра в приложении только пользователям, зарегистрированным: • на данном корпоративном сервере; • серверах, с которыми установлено трастовое соединение
Только для корпоративных пользователей	Значение данного поля доступно для просмотра в приложении всем пользователям, зарегистрированным в корпоративном сетевом сегменте
Для всех	Значение данного поля доступно для просмотра в приложении всем пользователям

3. Нажмите «Сохранить».

   Настроенные поля станут доступны для указанных пользователей. В верхней части экрана появится системное сообщение «Настройки видимости полей профиля сохранены».

НАСТРОЙКА E-MAIL

Для настройки регистрации по маске e-mail:

1. Перейдите на вкладку «Настройки регистрации» → «E-mail».

   Откроется окно «Настройки e-mail» (рис. 43).

2. Введите маску e-mail в поле, используя регулярное выражение (например, ^.*?@corporate.local).

3. Задайте максимальное количество попыток ввода пароля и максимальное количество попыток отправки кода на e-mail до блокировки.

   По умолчанию значение в поле «Максимальное количество попыток отправки кода до блокировки» блокировки равно 3. Значение в поле не может быть пустым или равным 0.

4. Нажмите «Сохранить».

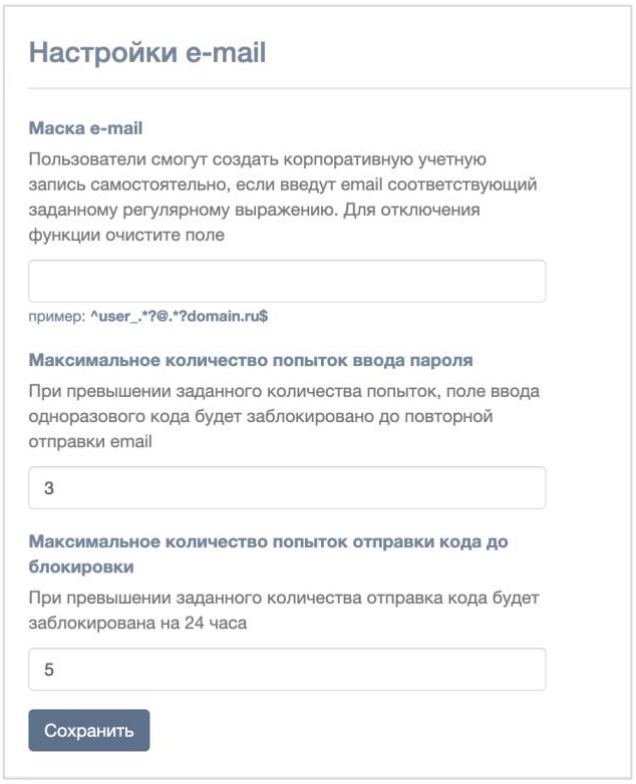

рис. 43

После успешного сохранения изменений в верхней части экрана появится системное сообщение «Настройки регистрации по маске e-mail сохранены».

НАСТРОЙКА OPENID

Примечание. Перед настройкой OpenID необходимо настроить интеграцию CTS и Keycloak. См. «Интеграция CTS и Keycloak».

Для настройки OpenID:

1. Перейдите в раздел «Настройка регистрации» → «OpenID».

   Откроется окно настройки параметров регистрации через OpenID (рис. 44).

2. Заполните поля (табл. 59):

табл. 59

Поле	Описание
OpenID провайдер	Переключатель автоподстановки префикса /auth в запросы к кейклок. Для версий ниже 17 добавляется префикс
Хост OpenID	URL по которому доступен Keylcloak (включает в себя обязательный протокол), например — https://openid.provider.com
Порт OpenID	Порт, на котором Keycloak принимает запросы, например — 8443
ID Realm OpenID	Имя реалма в который будет подключен CTS, например — Express
ID клиента OpenID	ID клиента, к которому будет обращатся CTS, например — cts-adintegration
Secret клиента OpenID	Секретный ключ клиента, указанный в меню credentials Keycloak, например — aNicQoU5k8UK7BZsUJYaegT493e8pYaX
Редирект URI OpenID	URI CTS, на который браузер будет перенаправлять пользователей после успешного входа в систему, например — https://cts.express/api/v1/ad_integration/openid/success
Возможные редирект URIs OpenID	Перечень URL адресов WEB-клиентов, с которых разрешено перенаправление (через запятую). Используется только в случае отключения iframe окна в клиентских приложениях web/desktop. Например — https://web-beta.express,https://web.express
Тип ответа OpenID	Значение параметра response_type OpenID Connect. Значение всегда указывается «code»
OpenID scope	Список разделенных пробелами областей, которые запрашиваются с помощью параметра scope, например openid express-scopes email offline_access roles
Требуемая роль OpenID	Указывается имя роли пользователей, разрешенное к входу в CTS, например user_cts01
Путь до списка ролей. Использовать точку для вложенных путей, напр. "path.role"	Путь, по которому находится список ролей, например realm_access.roles
Время ожидания ответа при асинхронном обновлении (в миллисекундах)	Время ожидания ответа от Keycloak, например 5000
Предзаполнение логина OpenID	Выбор режима заполнения поля логин в форме входа Keycloak
Метод авторизации устройства	Тип авторизации клиентских приложений по QR-коду, например CIBA

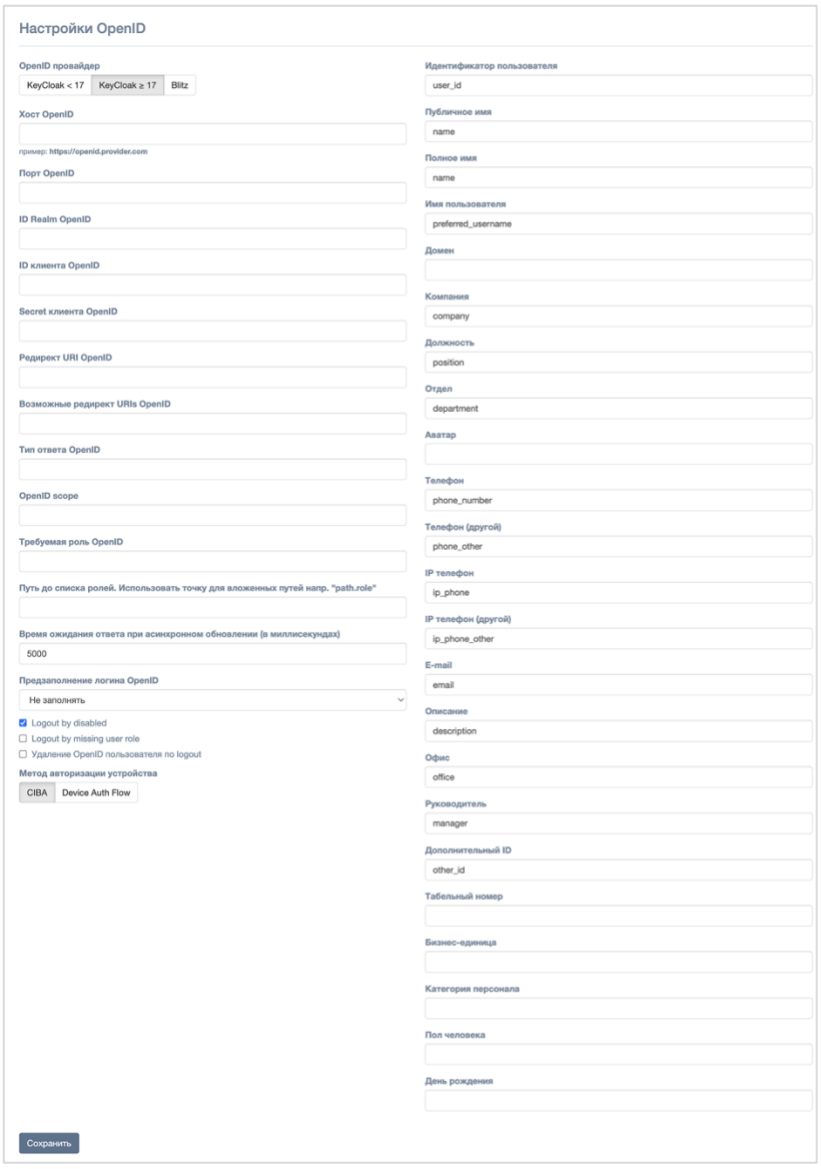

рис. 44

Примечание. В поле «OpenID scope» рекомендуется указать значение из строки «scope» консоли администратора Keycloak. Это необходимо для получения списка передаваемого «scope».

Для этого откройте консоль администратора Keycloak, перейдите в раздел «Clients» →Client scopes→Client ID→Evaluate→Generated access token→строка «scope» и скопируйте значение (рис. 45).

3. В полях правой колонки укажите атрибуты, которые будут отображаться в карточке пользователя.
4. Поставьте отметку «Удаление OpenID пользователя по logout» для автоматического удаления OpenID пользователя при подтверждении запроса на выход с корпоративного сервера в разделе «Запросы на логаут» (подробнее о разделе «Запросы на логаут» см. в документе «Руководство администратора. Том 2. Эксплуатация сервера CTS»).

Примечание. Пункты «Logout by disabled» и «Logout by missing user role» находятся в разработке.

5. Нажмите «Сохранить».

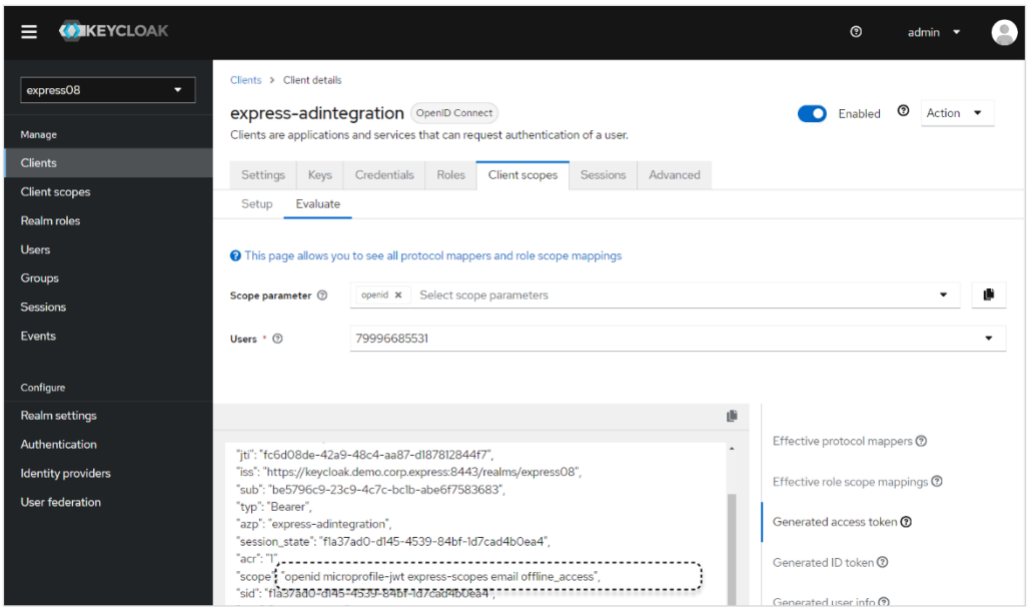

рис. 45

РЕГИСТРАЦИЯ БЕЗ НОМЕРА ТЕЛЕФОНА

Для настройки регистрации без номера телефона:

1. Перейдите в раздел «Настройка регистрации».
2. Установите/снимите отметку в поле «Разрешена регистрация без номера телефона» (по умолчанию настройка включена).
3. Установите/снимите отметку в поле «Отобразить предупреждение о скором отключении» (доступно для изменения только при разрешенной регистрации без номера телефона).
4. Установите/снимите отметку в поле «Разрешить пропуск двухфакторной аутентификации в пределах контура» (по умолчанию настройка выключена).
5. Установите разрешения пользователю на операции с номером телефона (по умолчанию все разрешения предоставлены).
6. Нажмите «Сохранить».

НАСТРОЙКА ДОВЕРИТЕЛЬНЫХ ПОДКЛЮЧЕНИЙ

Для создания доверительного подключения (траста):

1. Откройте пункт меню «Серверы».
2. Выберите вкладку «Trusts» (рис. 46).

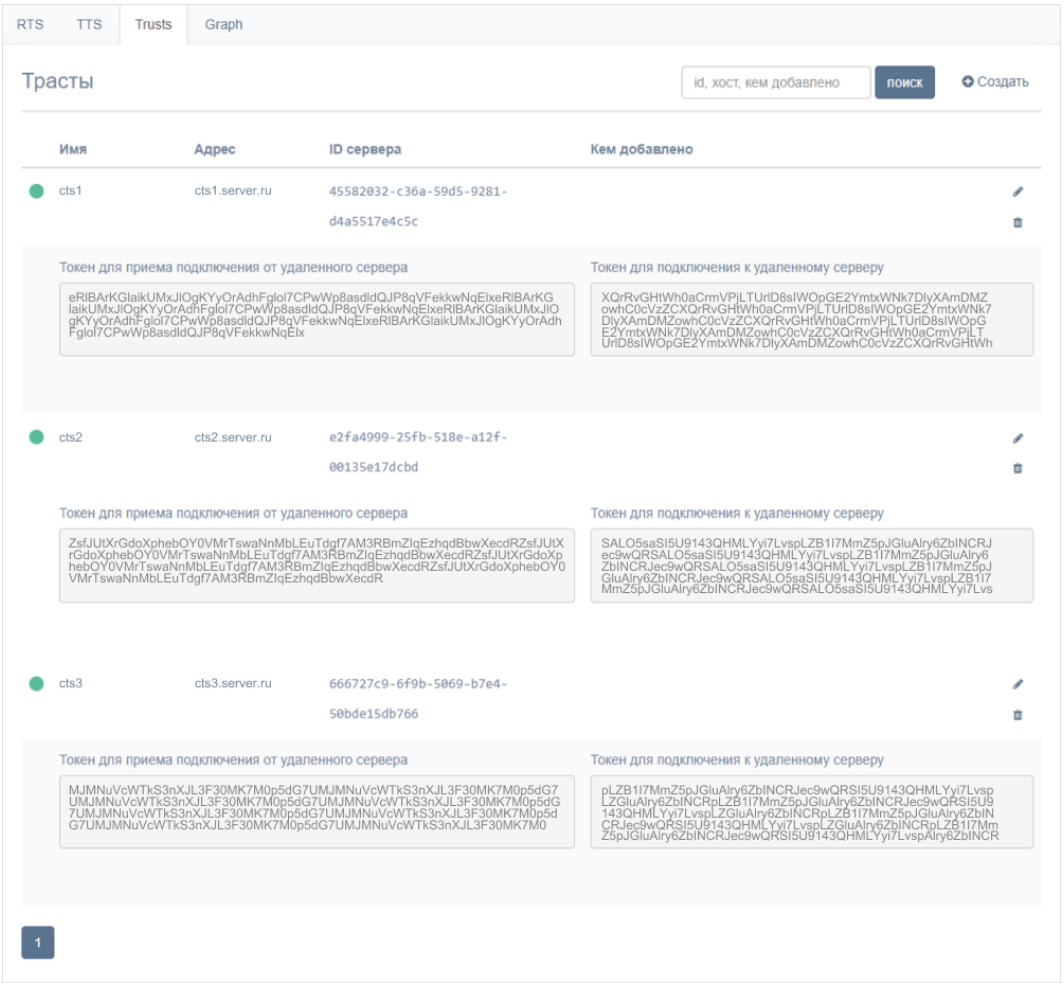

рис. 46

3. Нажмите «Создать» в правом верхнем углу.
   Откроется окно (рис. 47):

рис. 47

4. Заполните поля (табл. 60):

табл. 60

Поле	Описание
CTS ID	Идентификатор сервера CTS, с которым будет установлено соединение. Идентификатор CTS сервера находится в пункте меню «Сервер» веб-интерфейса администратора этого сервера
Имя	Краткое обозначение для создаваемого траста

Поле	Описание
Токен для приема подключения от удаленного сервера	Название токена
Токен для подключения к удаленному серверу	Название токена
Endpoint	Адрес подключения к серверу. В таблице с перечнем токенов данные из этого поля отображаются в столбце «Адрес»
Разрешить трастовый поиск	Разрешает доступ другому серверу к корпоративной книге контактов сервера, на котором создается траст. Трастовый поиск доступен в том случае, если в настройках сервера разрешен корпоративный поиск — Corporate search

Пример. Требуется создать траст между двумя серверами: CTS1 и CTS2. Для решения этой задачи администратор на каждом из серверов создает траст, в настройках указывая токены таким образом, чтобы токен для подключения на сервере CTS1 совпадал с токеном для приема подключения на CTS2, и наоборот.

5. Нажмите «Сохранить».

Далее зайдите в веб-интерфейс администратора корпоративного сервера (в примере, приведенном на шаге 2, CTS2), с которым устанавливается соединение, и создайте траст с текущим сервером (CTS1).

Глава 4

ПРОЦЕДУРА ОБНОВЛЕНИЯ

Полностью процедура обновления системы, ее компонентов и дополнительного ПО описана в документе «Руководство администратора. Обновление».

Процедура обновления системы включает:

- обновление ОС;
- ручное обновление серверов;
- обновление серверов с использованием Ansible-сценариев;
- обновление отказоустойчивой конфигурации;
- обновление сервера Media.

Процедура обновления дополнительных компонентов системы и интеграционного ПО включает:

- обновление десктоп-версии;
- обновление сертификата;
- обновление PostgreSQL.

Документ «Руководство администратора. Обновление» содержит описание процедуры обновления СК «Express» до версии 3.27, с изменением архитектуры приложения, и процесса миграции больших баз данных.

Также в документе приведено описание возможных аварийных ситуаций при обновлении из локального репозитория Registery.

Глава 5

УСТРАНЕНИЕ ТИПОВЫХ ОШИБОК

Примечание. Все работы на серверах должны проводиться от имени суперпользователя.

В СК «Express» предусмотрены следующие типы сообщений (табл. 61):

табл. 61

Сообщение об ошибке	Значение
403 Forbidden — You don't have access to view this page	У администратора нет прав на доступ
404 Page Not Found	Страница отсутствует
413 Request is too large	Возникает, если администратор пытается загрузить слишком большой файл, например, аватар
500 Internal Server Error	Исключительная ошибка

Для получения прав суперпользователя выполните команду:

```
sudo -s
```

СК «Express» построен на базе микросервисной архитектуры с использованием контейнеризации на основе ПО Docker. Все операции обслуживания СК «Express» и устранения неполадок производятся с контейнерами Docker.

В случае неполадок в работе СК «Express» в первую очередь требуется проверить статус работы контейнеров.

Для проверки статуса контейнеров (запущен или остановлен) используйте команду:

```
docker ps -a --format "{{.Names}}: {{.Status}}"
```

Нормальное состояние контейнеров — «UP».

Если контейнеру присвоен статус «Exited», запустите его командой:

```
docker start <имя контейнера вида cts-containername_1>
```

Если проблема не решена, соберите логи системы.

Для сбора логов выполните команду:

```
cd /opt/express
dpl --dc logs --tail=1000 > logs.txt
```

Отправьте собранные логи администраторам, ответственным за СК «Express».

Если пользователь не может войти на сервер, соберите логи командой:

```
cd /opt/express
dpl --dc logs --tail=1000 ad_integration > logs.txt
```

Для перезагрузки всех контейнеров выполните команду:

```
cd /opt/express
dpl --dc restart
```

Если у пользователей нарушился порядок отображения сообщений в беседах, то проверьте время на сервере командой:

```
date
```

Если время некорректное, проверьте статус сервиса точного времени chronyd.

Для проверки статуса сервиса точного времени выполните команду:

```
systemctl status chronyd
```

Если статус «active» имеет значение «inactive», запустите сервис командой:

```
systemctl start chronyd
```

Ошибка авторизации

Данная ошибка может появиться в том случае, если аккаунт пользователя появился в системе после синхронизации с AD (рис. 48):

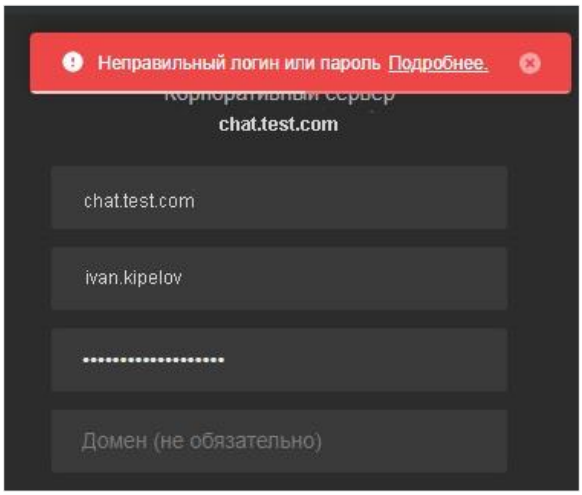

рис. 48

Возникновение данной ошибки происходит в том случае, если в AD зарегистрированы пользователи с разными User logon name и в настройках AD указан другой домен.

Для решения проблемы при авторизации пользователь должен дополнить свой логин доменом через @, например user9@it-company.local.

В табл. 62 представлены возможные ошибки, которые могут возникнуть в случае неверного сочетания настроек регистрации пользователей:

табл. 62

№	Описание сочетания настроек	Описание последствий
1.	В сборке отключена кнопка «телефон и учетные данные», в веб-интерфейсе администратора отключена опция «регистрация без номера разрешена»	Так запрещены оба способа регистрации. В приложение попадут только пользователи, ранее добавившие вапрофиле номер через редирект на ввод смс
2.	В сборке отключены все кнопки, кроме «телефон и учетные данные», в веб-интерфейсе администратора отключена возможность добавлять номер	Пользователи, не добавившие в профиле номер, не смогут зайти в приложение
3.	В веб-интерфейсе администратора отключена регистрация без номера без предварительного уведомления пользователям о необходимости его добавить	Пользователи, не добавившие в профиль номер телефона, не смогут зайти в приложение
4.	Первично пользователи зарегистрированы на публичном сервере, после чего им было предложено войти под учетными данными через «корпоративный email» или «адрес корпоративного сервера»	В этом случае у пользователя создается два аккаунта: публичный с номером и корпоративный без номера. Объединить их в один технически невозможно. Единственный выход из данной ситуации - добавить этот же номер к корпоративной учетной записи и удалить публичный аккаунт, потеряв всю переписку.

№	Описание сочетания настроек	Описание последствий
5.	На брендированной сборке отключены все кнопки, кроме «Телефон и учетные данные», в веб-интерфейсе администратора оставлено разрешение пользователю удалять номер телефона	Пользователь, удаливший номер телефона, не сможет войти в приложение
6.	В веб-интерфейсе администратора регистрация без номера запрещена, при этом оставлено разрешение пользователю удалять номер	Пользователь, удаливший номер, не сможет войти в приложение

Глава 6

УСТРАНЕНИЕ УЯЗВИМОСТЕЙ

Для устранения уязвимости log4j (CVE-2021-44228), CVE-2021-45046:

Примечание. Если версия менее 2.16, но не 1.x, то требуется обновление до самой последней версии. Для версии 1.x данная уязвимость отсутствует.

1. Проверьте версию log4j с помощью команды:

```
find / -name 'log4j*.jar'
```

или найдите через вывод CLASSPATH используемой установки java:

```
echo $CLASSPATH
```

2. В настройках Java Virtual Machine (JVM) для пакетов log4j версий 2.0-2.15 добавьте флаг для приложения:

- Dlog4j2.formatMsgNoLookups=true;

Важно! Поставьте последний пакет обновлений Log4j 2.16.0, исправляющий пакет обновлений, который был сделан для CVE-2021-45046 Log4j 2.15.0. Установка последнего пакета не отличается от предыдущей установки, и не требуется, если не используется дополнительная программа APM с настройкой журналирования в режиме «tracing».

В ином случае настоятельно рекомендуется обновить текущую версию Elasticsearch до 7.16.1 (или до 6.8.21) и выполнить последовательный перезапуск нод.

- для elasticsearch — /etc/elasticsearch/jvm.options;
- для logstash — /etc/logstash/jvm.options.

Примечание. Путь может отличаться и зависит от способа установки.

3. Перезапустите приложение командой:

```
systemctl restart elasticsearch
```

4. Проверьте, что настройка jvm активна:

```
ps axw | grep formatMsgNoLookups
```

Флаг должен быть виден в строке запуска приложения.

Пример обновления log4j для elasticsearch:

```
wget https://dlcdn.apache.org/logging/log4j/2.16.0/apache-
log4j2.16.0-bin.tar.gz
tar zxvf apache-log4j-2.16.0-bin.tar.gz
cd apache-log4j-2.16.0-bin/
ls /usr/share/elasticsearch/lib/log4*
cp log4j-api-2.16.0.jar /usr/share/elasticsearch/lib/
cp log4j-core-2.16.0.jar /usr/share/elasticsearch/lib/
rm -f /usr/share/elasticsearch/lib/log4j-api-2.11.1.jar
rm -f /usr/share/elasticsearch/lib/log4j-core-2.11.1.jar
```

Для Logstash версий ниже 6.8.21 и 7.16.0 выполните:

```
zip -q -d <LOGSTASH_HOME>/logstash-core/**/*/log4j-core-2.*
org/apache/logging/log4j/core/lookup/JndiLookup.class
```

или

```
wget https://dlcdn.apache.org/logging/log4j/2.16.0/apache-log4j-
2.16.0-bin.tar.gz
tar zxvf apache-log4j-2.16.0-bin.tar.gz
cd apache-log4j-2.16.0-bin/
ls /usr/share/logstash/lib/log4*
cp log4j-api-2.16.0.jar /usr/share/logstash/lib/
```

```
cp log4j-core-2.16.0.jar /usr/share/logstash/lib/
rm -f /usr/share/logstash/lib/log4j-api-2.11.1.jar
rm -f /usr/share/logstash/lib/log4j-core-2.11.1.jar
```

Приложение 1

СЕТЕВЫЕ ВЗАИМОДЕЙСТВИЯ SINGLE CTS

№	Источник	Получатель	Порт и протокол	Описание
1	Сервер Single CTS	Bot-сервер	TCP/8000-8100 TCP/443	Взаимодействие Single CTS с Bot-сервером, взаимодействие Bot-сервера с Single CTS по протоколу HTTP/HTTPS
	Bot-сервер	Сервер Single CTS		
2	Внутренние ИС	Bot-сервер	TCP/80 TCP/443 TCP/8000-8100	Взаимодействие внутренних информационных систем с Bot-сервером, взаимодействие Bot-сервера с внутренними информационными системами по протоколу HTTP/HTTPS
	Bot-сервер	Внутренние ИС		
3	Сервер Single CTS	Сервер LDAP	TCP/389, 636	Обеспечение работы LDAP/LDAPS
4	Администратор	Сервер Single CTS и Media	TCP/22	Администрирование серверов по протоколу SSH
			TCP/443	Администрирование Express через веб-интерфейс по протоколу HTTPS
5	Сервер Single CTS	Сервер SMTP	TCP/25 TCP/587 TCP/465	Обеспечение отправки писем с ПИН-кодом аутентификации по протоколу SMTP
6	Сервер Single CTS	Сервер DNS и NTP	TCP/53 UDP/53	Обеспечивание работы разрешения имен DNS
			UDP/123	Обеспечение работы службы точного времени NTP
7	Сервер Single CTS	Сервер Media	TCP/8188	Обеспечение аутентификации и шифрования голосовых вызовов
8	Transcoding	Сервер Single CTS	TCP/443	Передача транскодированных записей в файловое хранилище
9	Transcoding	Сервер Media	TCP/443	Обеспечение передачи файлов записи звонков по протоколу HTTPS для последующей обработки сервером Transcoding
10	Внутренний пользователь	Сервер Single CTS	TCP/443	Клиентский доступ к корпоративному сетевому сегменту Express с использованием протокола HTTPS
11	Внутренний пользователь	Сервер Media	UDP/20000-40000	Обеспечение передачи медиаданных по протоколу SRTP конференцсвязи
12	Внешний пользователь	Сервер Media (Внешний IP NAT)	TCP/3478 UDP/3478	Обеспечение работы протоколов STUN/TURN
			UDP/20000-40000	Обеспечение передачи медиаданных по протоколу SRTP конференцсвязи
13	Внешний пользователь	Сервер Single CTS	TCP/443	Клиентский доступ к корпоративному сетевому сегменту Express с использованием протокола HTTPS
14	Сервер Single CTS	Сервера Let`s Encrypt (ANY)	TCP/80 TCP/443	При использовании бесплатного сертификата от компании Let`s Encrypt
	Сервера Let`s Encrypt (ANY)	Сервер Single CTS		

№	Источник	Получатель	Порт и протокол	Описание
15	Сервер Single CTS	Сервер установки и обновлений Registry.public.express	TCP/443	Доступ к репозиторию образов Docker для установки и обновления ПО Express
16	Сервер Single CTS	Партнерский сервер Express CTS	TCP/5001	Обеспечение прямой передачи сообщений между корпоративными серверами минуя публичный сетевой сегмент
	Партнерский сервер Express CTS	Сервер Single CTS		
17	Сервер Media	Партнерский сервер Express CTS	UDP/20000-40000	Обеспечение передачи медиаданных по протоколу SRTP
	Партнерский сервер Express CTS	Сервер Media		
18	Внешний пользователь	RTS ru.public.express	TCP/443	Обеспечение взаимодействия внешнего пользователя с RTS
19	Сервер Single CTS	RTS ru.public.express	TCP/5001	Обеспечение взаимодействия корпоративного сервера Express и RTS
20	Внутренний пользователь	RTS ru.public.express	TCP/443	Клиентский доступ к публичному сетевому сегменту Express с использованием протокола HTTPS
21	Внешний пользователь	Сервер веб-клиента corp.express	TCP/443	Клиентский доступ к серверу веб-клиента в публичном доступе
22	Внутренний пользователь	Сервер веб-клиента corp.express	TCP/443	Клиентский доступ к серверу веб-клиента в публичном доступе
23	RTS ru.public.express	SMS-оператор	TCP/443	Отправка SMS-сообщений пользователям
24	RTS ru.public.express	Служба push-уведомлений Huawei	TCP/443	Отправка push-уведомлений пользователям Huawei
25	RTS ru.public.express	Служба push-уведомлений Apple	TCP/443	Отправка push-уведомлений пользователям iOS
26	RTS ru.public.express	Служба push-уведомлений Google	TCP/80	Отправка push-уведомлений пользователям Android

Для сервера Single CTS должен быть настроен NAT IP-to-IP и выполнена трансляция следующих портов и протоколов:

- TCP/443 (в том числе для сервера Media);
- TCP/5001;
- TCP/3478 (только для сервера Media);
- UDP/3478 (только для сервера Media);
- UDP/20000-40000 (только для сервера Media).

Порт TCP/80 добавляется при использовании Let's Encrypt.

Приложение 2

СЕТЕВЫЕ ВЗАИМОДЕЙСТВИЯ FRONT CTS, MEDIA И BACK CTS

№	Источник	Получатель	Порт и протокол	Описание
Основные сетевые взаимодействия				
1	Сервер Back CTS	Bot-сервер	TCP/8000-8100 TCP/443	Взаимодействие Back CTS с Bot-сервером, взаимодействие Bot-сервера с сервером Back CTS по протоколу HTTP либо HTTPS
	Bot-сервер	Сервер Back CTS		
2	Внутренние ИС	Bot-сервер	TCP/8000-8100 TCP/80 TCP/443	Взаимодействие внутренних информационных систем с Bot-сервером, взаимодействие Bot-сервера с внутренними информационными системами по протоколу HTTP либо HTTPS
	Bot-сервер	Внутренние ИС		
3	RTS ru.public.express	Служба push-уведомлений Google	TCP/443	Отправка push-уведомлений пользователям Android
4	Сервер Back CTS	Сервер Front CTS	TCP/8888	Tinyproxy – локальный прокси-сервер для подключения Back CTS к репозиторию образов Docker, используемых для установки и обновления изделия
			TCP/443	Мониторинг работы контейнера trusts
5	Сервер Front CTS	Сервер Back CTS	TCP/443	Передача зашифрованных пользовательских данных в транспортной обертке TLS
			TCP/2379	Подключение к хранилищу конфигураций для получения различных настроек сервисов
			TCP/5432	Подключение контейнера trusts к базе данных для хранения информации, необходимой для работы
			TCP/9092	Подключение к программному брокеру сообщений Kafka для обмена событиями между сервисами
			TCP/6379	Подключение к Redis для работы функции кеширования
6	Администратор	Сервер Front CTS, Back CTS и Media	TCP/22	Администрирование серверов по протоколу SSH
			TCP/443	Администрирование Express через веб-интерфейс по протоколу HTTPS
7	Сервер Back CTS	Сервер SMTP	TCP/25 TCP/587 TCP/465	Обеспечение отправки писем с ПИН-кодом аутентификации по протоколу SMTP
8	Сервер Back CTS	Сервер Media	TCP/8188	Обеспечение аутентификации и шифрования голосовых вызовов
9	Transcoding	Сервер Media	TCP/443	Обеспечение передачи файлов записи звонков по протоколу HTTPS для последующей обработки сервером Transcoding
10	Transcoding	Сервер Back CTS	TCP/443	Передача транскодированных записей в файловое хранилище
11	Внутренний пользователь	Сервер Back CTS	TCP/443	Клиентский доступ к корпоративному сетевому сегменту Express с использованием протокола HTTPS
12	Сервер Front CTS	Сервер DNS и NTP	TCP/53 UDP/53	Обеспечение работы разрешения имен DNS
			UDP/123	Обеспечение работы службы точного времени NTP

№	Источник	Получатель	Порт и протокол	Описание
13	Внутренний пользователь	Сервер Media	UDP/20000-40000	Обеспечение передачи медиаданных по протоколу SRTP конференцсвязи
14	Внешний пользователь	Сервер Media (Внешний IP NAT)	TCP/3478 UDP/3478	Обеспечение работы протоколов STUN/TURN
			UDP/20000-40000	Обеспечение передачи медиаданных по протоколу SRTP
15	Внешний пользователь	Сервер Front CTS (Внешний IP NAT)	TCP/443	Клиентский доступ к корпоративному сетевому сегменту Express с использованием протокола HTTPS
16	Сервер Front CTS	Сервер установки и обновлений registry.public.express	TCP/443	Доступ к репозиторию образов Docker для установки и обновления ПО Express
17	Внешний пользователь	RTS ru.public.express	TCP/443	Обеспечение взаимодействия внешнего пользователя с RTS
18	Сервер Front CTS	RTS ru.public.express	TCP/5001	Обеспечение взаимодействия корпоративного сервера Express с RTS
19	Внутренний пользователь	RTS ru.public.express	TCP/443	Клиентский доступ к публичному сетевому сегменту Express с использованием протокола HTTPS
20	Внешний пользователь	Сервер веб-клиента corp.express	TCP/443	Клиентский доступ к серверу веб-клиента в публичном сетевом сегменте
21	Внутренний пользователь	Сервер веб-клиента corp.express	TCP/443	Клиентский доступ к серверу голосовых коммуникаций в публичном сетевом сегменте
22	Сервер Front CTS	Сервера Let`s Encrypt (ANY)	TCP/443 TCP/80	При использовании бесплатного сертификата от компании Let`s Encrypt
	Сервера Let`s Encrypt (ANY)	Сервер Front CTS		
23	Сервер Front CTS	Партнерский сервер Express CTS	TCP/5001	Обеспечение прямой передачи сообщений между корпоративными серверами минуя публичный сетевой сегмент
	Партнерский сервер Express CTS	Сервер Front CTS		
24	Сервер Media	Партнерский сервер Express CTS	UDP/20000-40000	Обеспечение передачи медиаданных по протоколу SRTP
	Партнерский сервер Express CTS	Сервер Media		
25	RTS ru.public.express	SMS оператор	TCP/443	Отправка SMS-сообщений пользователям
26	RTS ru.public.express	Служба push-уведомлений Huawei	TCP/443	Отправка push-уведомлений пользователям Huawei
27	RTS ru.public.express	Служба push-уведомлений Apple	TCP/443	Отправка push-уведомлений пользователям iOS
Аутентификация с помощью AD				
28	Сервер Back CTS	Сервер LDAP	TCP/53 UDP/53	Обеспечение работы разрешения имен DNS
			UDP/123	Обеспечение работы службы точного времени NTP
			TCP/389 TCP/636	Обеспечение работы LDAP или LDAPS
Аутентификация с помощью ADLDS				
29	Сервер Back CTS	Сервер ADLDS	TCP/389	Обеспечение работы LDAP или LDAPS

№	Источник	Получатель	Порт и протокол	Описание
			TCP/636	
30	Сервер ADLDS	Сервер LDAP	TCP/389 TCP/636	Импорт пользователей LDAP или LDAPS
Аутентификация с помощью e-mail				
Подключение к серверу SMTP описано выше (п. 7), дополнительных подключений не требуется				
Аутентификация с помощью Keycloak				
31	Внешний пользователь	Сервер Keycloak Front	TCP/443	Аутентификация пользователей
32	Сервер Keycloak Front	Сервер Keycloak Back	TCP/443	Проксирование запросов пользователей
33	Внутренний пользователь	Сервер Keycloak Front	TCP/443	Аутентификация пользователей
34	Сервер Keycloak Back	Сервер LDAP	TCP/389 TCP/636	Импорт пользователей LDAP или LDAPS
35	Сервер Back CTS	Сервер Keycloak Back	TCP/443	Обеспечение работы OpenID
	Сервер Keycloak Back	Сервер Back CTS		

Приложение 3

СЕТЕВЫЕ ВЗАИМОДЕЙСТВИЯ ETS, MEDIA И SINGLE CTS

№	Источник	Получатель	Порт и протокол	Описание
1	Сервер Single CTS	Сервер LDAP	TCP/389, 636	Обеспечение работы LDAP либо LDAPS
2	Сервер Single CTS Bot-сервер	Bot-сервер Сервер Single CTS	TCP/8000–8100 TCP/443	Взаимодействие Single CTS с Bot-сервером, взаимодействие Bot-сервера с Single CTS по протоколу HTTP/HTTPS
3	Внутренние ИС Bot-сервер	Bot сервер Внутренние ИС	TCP/8000–8100 TCP/80 TCP/443	Взаимодействие внутренних информационных систем с Bot-сервером, взаимодействие Bot-сервера с внутренними информационными системами по протоколу HTTP/HTTPS
4	Администратор	Сервер Single CTS, ETS, Media, Web Client, XLink	TCP/22	Администрирование серверов по протоколу SSH
			TCP/443	Администрирование Express через веб-интерфейс по протоколу HTTPS
5	Сервер Single CTS	Сервер SMTP	TCP/25 TCP/587 TCP/465	Обеспечение отправки писем с ПИН-кодом аутентификации по протоколу SMTP
6	Сервер ETS	Docker registry	TCP/443	Доступ к репозиторию образов Docker для установки и обновления ПО Express
7	Сервер ETS	Сервер DNS и NTP	TCP/53 UDP/53	Обеспечение работы разрешения имен DNS
			UDP/123	Обеспечение работы службы точного времени NTP
8	Внутренний пользователь	Сервер ETS	TCP/443	Клиентский доступ к корпоративному сетевому сегменту Express с использованием протокола HTTPS
9	Сервер Single CTS	Сервер ETS	TCP/5001	Обеспечение взаимодействия корпоративного сервера Express с сервером предприятия ETS
10	Сервер Single CTS	Сервер DNS и NTP	TCP/53 UDP/53	Обеспечение работы разрешения имен DNS
			UDP/123	Обеспечение работы службы точного времени NTP
11	Сервер Single CTS, Media, Web Client, Сервер XLink	Docker registry	TCP/443	Доступ к репозиторию образов Docker для установки и обновления ПО Express
12	Single CTS	Media	TCP/8188	Управление звонками конференцсвязи
13	Transcoding	Сервер Single CTS	TCP/443	Передача транскодированных записей в файловое хранилище
14	Transcoding	Сервер Media	TCP/443	Обеспечение передачи файлов записи звонков по протоколу HTTPS для последующей обработки сервером Transcoding
15	Внутренний пользователь	Сервер Single CTS	TCP/443	Клиентский доступ к корпоративному сетевому сегменту Express с использованием протокола HTTPS
16	Внутренний пользователь	Сервер Web Client	TCP/443	Подключение внутренних пользователей к веб-клиенту

№	Источник	Получатель	Порт и протокол	Описание
		Сервер XLink	TCP/443	Подключение внутренних пользователей к XLink
17	Внутренний пользователь	Сервер Media	UDP/20000-40000	Обеспечение передачи медиаданных по протоколу SRTP конференцсвязи
18	Сервер ETS	SMS оператор	TCP/443	Отправка SMS-сообщений пользователям
19	Сервер ETS	Служба push-уведомлений Huawei	TCP/443	Отправка push-уведомлений пользователям Huawei
20	Сервер ETS	Служба push-уведомлений Apple	TCP/443	Отправка push-уведомлений пользователям iOS
21	Сервер ETS	Служба push-уведомлений Google	TCP/443	Отправка push-уведомлений пользователям Android
22	Сервер ETS	RTS ru.public.express	TCP/5001	Обеспечение взаимодействия ETS с RTS
23	Сервера Let`s Encrypt	Сервер ETS	TCP/80	Проверка домена, на который запрашивается сертификат от компании Let`s Encrypt
		Сервер Single CTS		
	Сервер ETS	Сервера Let`s Encrypt	TCP/443	Запрос бесплатного сертификата от компании Let`s Encrypt
	Сервер Single CTS	Сервера Let`s Encrypt	TCP/443	
24	Внешний пользователь	Сервер ETS	TCP/443	Клиентский доступ к корпоративному сетевому сегменту Express с использованием протокола HTTPS
25	Внешний пользователь	Сервер Single CTS (Внешний IP NAT)	TCP/443	Клиентский доступ к корпоративному сетевому сегменту Express с использованием протокола HTTPS
26	Сервер Single CTS	Партнерский сервер CTS	TCP/5001	Обеспечение прямой передачи сообщений между корпоративными серверами минуя публичный сетевой сегмент
	Партнерский сервер CTS	Сервер Single CTS (Внешний IP NAT)		
27	Сервер Media	Партнерский сервер CTS	UDP/20000-40000	Обеспечение передачи медиаданных по протоколу SRTP
	Партнерский сервер CTS	Сервер Media (Внешний IP NAT)		
28	Внешний пользователь	Сервер Media (Внешний IP NAT)	TCP/3478	Обеспечение работы протоколов STUN/TURN
			UDP/3478	
		Сервер Media	UDP/20000-40000	Обеспечение передачи медиаданных по протоколу SRTP
29	Внешний пользователь	Сервер Web Client	TCP/443	Клиентский доступ к веб-клиенту с использованием протокола HTTPS
		Сервер XLink	TCP/443	Клиентский доступ к XLink

Приложение 4

СЕТЕВЫЕ ВЗАИМОДЕЙСТВИЯ ETS, MEDIA, FRONT CTS И BACK CTS

№	Источник	Получатель	Порт и протокол	Описание
1	Сервер Back CTS	Сервер LDAP	TCP/53	Обеспечение работы разрешения имен DNS
			UDP/53	
			UDP/123	Обеспечение работы службы точного времени NTP
			TCP/389	Обеспечение работы LDAP/LDAPS
			TCP/636	
2	Сервер Back CTS	Bot-сервер	TCP/8000–8100	Взаимодействие Back CTS с Bot-сервером по протоколу HTTP/HTTPS
			TCP/443	
	Bot-сервер	Сервер Back CTS	TCP/443	Взаимодействие Bot-сервера с Back CTS по протоколу HTTP/HTTPS
3	Внутренние ИС	Bot-сервер	TCP/443	Взаимодействие внутренних информационных систем с сервером Bot по протоколу HTTP/HTTPS
			TCP/8000–8100	
	Bot-сервер	Внутренние ИС	TCP/80	Взаимодействие Bot-сервера с внутренними информационными системами по протоколу HTTP /HTTPS
			TCP443	
4	Сервер Back CTS	Docker registry	TCP/443	Доступ к репозиторию образов Docker для установки и обновления ПО Express
5	Сервер Back CTS	Сервер Front CTS	TCP/443	Мониторинг работы контейнера trusts и взаимодействие с его API
6	Сервер Front CTS	Сервер Back CTS	TCP/443	Передача зашифрованных пользовательских данных с транспортной оберткой TLS
			TCP/2379	Подключение к хранилищу конфигураций для получения различных настроек сервисов
			TCP/5432	Подключение контейнера trusts к базе данных для хранения информации, необходимой для работы
			TCP/6379	Подключение к Redis
			TCP/9092	Подключение к программному брокеру сообщений Kafka для обмена событиями между сервисами
7	Администратор	Сервер ETS, Front CTS, Back CTS, Media, Web Client, XLink	TCP/22	Администрирование серверов по протоколу SSH
			TCP/443	Администрирование Express через веб-интерфейс по протоколу HTTPS
8	Сервер Back CTS	Сервер SMTP	TCP/25 TCP/587 TCP/465	Обеспечение отправки писем с ПИН-кодом аутентификации по протоколу SMTP
9	Сервер Back CTS	Сервер Media	TCP/8188	Управление звонками конференцсвязи
10	Внутренний пользователь	Сервер Back CTS	TCP/443	Клиентский доступ к корпоративному сетевому сегменту Express с спользованием протокола HTTPS

№	Источник	Получатель	Порт и протокол	Описание
11	Transcoding	Сервер Back CTS	TCP/443	Передача транскодированных записей в файловое хранилище
12	Transcoding	Сервер Media	TCP/443	Обеспечение передачи файлов записи звонков по протоколу HTTPS для последующей обработки сервером Transcoding
13	Сервер ETS	Docker-реестр	TCP/443	Доступ к репозиторию образов Docker для установки и обновления ПО Express
14	Сервер ETS	Сервер DNS и NTP	TCP/53	Обеспечение работы разрешения имен DNS
			UDP/53	
			UDP/123	Обеспечение работы службы точного времени NTP
15	Внутренний пользователь	Сервер ETS	TCP/443	Клиентский доступ к корпоративному сетевому сегменту Express с использованием протокола HTTPS
16	Сервер Front CTS	Сервер ETS	TCP/5001	Обеспечение взаимодействия корпоративного сервера Express с ETS
17	Сервер Front CTS, Media, Web Client	Docker registry	TCP/443	Доступ к репозиторию образов Docker для установки и обновления ПО Express
	Сервер XLink			
18	Сервер Front CTS	Сервер DNS и NTP	TCP/53	Обеспечение работы разрешения имен DNS
			UDP/53	
			UDP/123	Обеспечение работы службы точного времени NTP
19	Внутренний пользователь	Сервер Web Client	TCP/443	Подключение внутренних пользователей к веб-клиенту
		Сервер XLink	TCP/443	Подключение внутренних пользователей к XLink
20	Внутренний пользователь	Сервер Media	UDP/20000-40000	Обеспечение передачи медиаданных по протоколу SRTP конференцсвязи
21	Сервер ETS	SMS оператор	TCP/443	Отправка SMS-сообщений пользователям
22	Сервер ETS	Служба push-уведомлений Huawei	TCP/443	Отправка push-уведомлений пользователям Huawei
23	Сервер ETS	Служба push-уведомлений Apple	TCP/443	Отправка push-уведомлений пользователям iOS
24	Сервер ETS	Служба push-уведомлений Google	TCP/443	Отправка push-уведомлений пользователям Android
25	Сервер ETS	RTS ru.public.express	TCP/5001	Обеспечение взаимодействия ETS с RTS
26	Сервер Let`s Encrypt	Сервер ETS	TCP/80	Проверка домена, на который запрашивается сертификат от компании Let`s Encrypt
		Сервер Front CTS		
	Сервер ETS	Сервер Let`s Encrypt	TCP/443	Запрос бесплатного сертификата от компании Let`s Encrypt
	Сервер Front CTS	Сервер Let`s Encrypt	TCP/443	
27	Внешний пользователь	Сервер Front CTS	TCP/443	Клиентский доступ к корпоративному сетевому сегменту Express с использованием протокола HTTPS

№	Источник	Получатель	Порт и протокол	Описание
28	Внешний пользователь	Сервер ETS	TCP/443	Клиентский доступ к корпоративному сетевому сегменту Express с использованием протокола HTTPS
29	Партнерский сервер CTS	Сервер Front CTS (Внешний IP NAT)	TCP/5001	Обеспечение прямой передачи сообщений между корпоративными серверами минуя публичный сетевой сегмент
	Сервер Front CTS	Партнерский сервер CTS		
30	Партнерский сервер CTS	Сервер Media (Внешний IP NAT)	UDP/20000-40000	Обеспечение передачи медиаданных по протоколу SRTP конференцсвязи
	Сервер Media	Партнерский сервер CTS		
31	Внешний пользователь	Сервер Media (Внешний IP NAT)	TCP/3478	Обеспечение работы протоколов STUN/TURN
			UDP/3478	
			UDP/20000-40000	Обеспечение передачи медиаданных по протоколу SRTP конференцсвязи
32	Внешний пользователь	Сервер Web Client	TCP/443	Клиентский доступ к веб-клиенту с использованием протокола HTTPS
		Сервер XLink	TCP/443	Клиентский доступ к XLink

Приложение 5

МОНИТОРИНГ EXPRESS

В состав СК «Express» входит стороннее ПО, отвечающее за мониторинг работы системы:

- Prometheus;
- Grafana;
- Алерты.

PROMETHEUS

СК «Express» содержит служебный модуль (docker-контейнер) с ПО мониторинга Prometheus, который собирает метрики с остальных модулей.

Метрики формируются разными модулями: node_exporter, cadvisor, redis_exporter и программными средствами внутри модулей СК «Express».

Prometheus доступен по пути /system/prometheus/. Схема авторизации — basic (поддерживается зашифрованный формат openssl passwd). Логин и пароль можно найти на сервере Single/Back в /opt/express/settings.yaml.

node_exporter

Node_exporter предоставляет аппаратные и системные метрики на уровне ОС, предоставляемые ядрами *NIX через сборщики метрик. Node_exporter измеряет несколько метрик, таких как: память, диск, CPU, сеть.

Если сервера CTS/ETS разворачивали с помощью утилиты dpl, то node_exporter должен быть установлен автоматически.

Внимание! Если модуль устанавливается на распределенном сервере (Front + Back), процедуру установки выполняют на каждом сервере отдельно.

Для установки на распределенном сервере:

1. Зайдите в каталог:

```
/opt/express
```

2. Выполните команду:

```
dpl nxinstall
ps ax|grep node_exporter | grep -v grep
17802 ? Ssl 322:51 /usr/bin/node_exporter --web.listen-
address=172.17.0.1:9200
```

cAdvisor

cAdvisor — это запущенный демон, который собирает, агрегирует, обрабатывает и экспортирует информацию о запущенных контейнерах. В частности, для каждого контейнера он хранит параметры изоляции ресурсов, историческое использование ресурсов, гистограммы полного исторического использования ресурсов и сетевую статистику.

Если сервера CTS/ETS разворачивали с помощью утилиты dpl, то cAdvisor должен быть установлен автоматически.

Если модуль устанавливается на распределенном сервере (Front + Back), процедуру установки выполняют на каждом сервере отдельно.

Для установки на распределенном сервере:

1. Зайдите в каталог:

```
/opt/express
```

2. Выполните команду:

```
dpl cadvinstall
ps ax|grep cadvisor | grep -v grep
17605 ? Ssl 44:20 /usr/bin/cadvisor -listen_ip 172.17.0.1 -port
9100
```

Federation Prometheus

Если в состав СК «Express» входит несколько дополнительных отдельных серверов: bot-сервер, отдельный сервер Media или несколько серверов СК «Express», для единой системы мониторинга нужно развернуть федерацию Prometheus, которая объединит все метрики в одном месте. Рекомендуемый способ централизованного сбора и хранения метрик со всех компонентов СК «Express»:

```
mkdir /opt/prometheus
cd /opt/prometheus
mkdir conf
```

docker-compose.yaml

Исходный код:

```
services:
  prometheus:
    image: "prom/prometheus"
    container_name: prometheus
    volumes:
      - "./conf/prometheus.yaml:/etc/prometheus/prometheus.yaml:ro"
      - "prometheus:/prometheus"
    command:
      - '--config.file=/etc/prometheus/prometheus.yaml'
      - '--storage.tsdb.path=/prometheus'
      - '--web.console.libraries=/etc/prometheus/console_libraries'
      - '--web.console.templates=/etc/prometheus/consoles'
      - '--web.route-prefix=/prom/'
      - '--storage.tsdb.retention.time=30d'
    restart: "always"
    security_opt:
      - no-new-privileges

    ports:
      - "8002:9090"

volumes:
  prometheus:
    driver: local
```

Укажите нужные параметры (табл. 63):

табл. 63

Параметр	Описание
job_name	Произвольное уникальное название (например, job_name: cts)
basic_auth	Аутентификация по логину/паролю (например, basic_auth: • username: Prometheus; • password: pass)
fqnd	доменное имя вашего CTS\ETS-сервера (например, static_configs: - targets: - 'fqnd:443')

conf/prometheus.yaml

Выполните команду:

```
docker compose up -d
```

Пример кода:

```
scrape_configs:
  - job_name: 'cts' # изменить, уникальное поле
    scheme: https
    scrape_timeout: 1m
    tls_config:
      insecure_skip_verify: true
    relabel_configs:
      - source_labels: [__address__]
        target_label: federate_host
    basic_auth:
      username: prometheus # изменить
      password: pass       # изменить

    honor_labels: true
    metrics_path: '/system/prometheus/federate'

    params:
      'match[]':
        - '{job=~".+"}'

    static_configs:
        - targets:
          - 'fqnd:443' # изменить fqdn cts
```

Метрики во встроенном Prometheus хранятся 15 дней, но при необходимости метрики можно передать для длительного хранения в централизованное хранилище, совместимое с Prometheus (например, централизованный сервер Prometheus, работающий в режиме «федерации»).

Метрики условно можно разделить на группы:

- метрики состояния модулей («включен–выключен», «uptime», «время запуска» и т.п.);
- метрики производительности (cpu usage, memory usage и т. д.);
- метрики доступности и т. п.

Метрики состояния модулей представлены в табл. 64.

табл. 64

Компоненты	Модуль	Метрика
Статус контейнеров в docker	Prometheus	up
Статус базы данных Posrgres	Prometheus	pg_up
Статус базы данных Redis	Prometheus	redis_up

Метрики производительности представлены в табл. 65.

табл. 65

Компоненты	Модуль	Метрика
CPU usage	Zabbix Agent	CPU usage
Memory	Zabbix Agent	Memory usage
Networking	Zabbix Agent	rx/tx rate

SSD	Zabbix Agent	Free space
container: CPU Usage	Prometheus	container_cpu_user_seconds_total
container: Memory Usage	Prometheus	container_memory_usage_bytes
container: SSD	Prometheus	container_fs_writes_bytes_total container_fs_reads_bytes_total
container: Networking	Prometheus	container_network_transmit_bytes_total container_network_receive_bytes_total

Метрики доступности сетевых сервисов представлены в табл. 66.

табл. 66

Компоненты	Модуль	Метрика
Front	Zabbix Server	TCP/80, 443, 3478, 6379, 8188
Front	Zabbix Server	TCP 5001
Back	Zabbix Server	TCP/80, 443, 5432, 9092

Статистическая информация о системе представлена в табл. 67.

табл. 67

Параметр	Модуль	Метрика
Зарегистрированные пользователи	Prometheus	active_users
Подключенные пользователи к серверу в данный момент	Prometheus	online_users
Общее количество работающих Android-клиентов	Prometheus	android_users
Общее количество пользователей	Prometheus	total_users
Количество зарегистрированных пользователей с сортировкой по названию компании	Prometheus	users_count
Общее количество работающих веб-клиентов	Prometheus	web_users
Общее количество переданных сообщений	Prometheus	messages_count
Общее количество работающих iOS-клиентов	Prometheus	ios_users
Общее количество работающих десктоп-клиентов	Prometheus	desktop_users
Версии контейнеров Express	Prometheus	express_version
Количество пользователей, находящихся в данный момент в звонке	Prometheus	users_in_calls_count
Размер баз данных Postgres	Prometheus	pg_database_size
Статус федеративных подключений	Prometheus	connection_status

Администратор может управлять Janus-серверами из веб-интерфейса администратора, масштабировать сервис, а также мониторить его метрики. метрики Janus-сервера представлены в табл. 68.

табл. 68

Параметр	Модуль	Метрика
Количество отчетов по звонкам, оцененным пользователями как неуспешные	Prometheus	call_reports_bad_count
Количество отчетов по звонкам, оцененным пользователями как успешные	Prometheus	call_reports_good_count
Количество отчетов «я никого не слышу»	Prometheus	call_reports_input_issue_count

Параметр	Модуль	Метрика
Количество отчетов «другое»	Prometheus	call_reports_other_issue_count
Количество отчетов «меня никто не слышит»	Prometheus	call_reports_output_issue_count
Количество отчетов с проблемами с подключением	Prometheus	call_reports_poor_connection_count
Количество отчетов с проблемами с демонстрацией экрана	Prometheus	call_reports_poor_sharing_count
Количество отчетов с проблемами со звуком	Prometheus	call_reports_poor_sound_count
Количество отчетов с проблемами с видео	Prometheus	call_reports_poor_video_count
Количество автоматических отчетов в связи с недоступностью	Prometheus	call_reports_session_issue_count
Количество отчетов «выкинуло из звонка»	Prometheus	call_reports_user_disconnected_count
Количество автоматических отчетов в связи с разрывом сети	Prometheus	call_reports_webrtc_issue_count
Количество аудио	Prometheus	janus_audio_count
Количество пользователей, получающих медиаданные	Prometheus	janus_participants_count
Количество участников	Prometheus	janus_publishers_count
Количество записей	Prometheus	janus_recording_count
Количество комнат	Prometheus	janus_rooms_count
Количество демонстраций экрана	Prometheus	janus_screen_count
Количество видео	Prometheus	janus_video_count
Количество автоматических отчетов в связи с ошибками бизнес-логики звонков	Prometheus	redis call_reports_domain_issue_count
Количество звонков за период	Prometheus	voex_call_started_count
Количество конференций за период	Prometheus	voex_conference_started_count
Количество пользователей, принявших участие в звонках/конференциях за период	Prometheus	voex_publisher_joined_count

Для настройки добавьте в файл settings.yaml параметры:

Примечание. В случае использования раздельной установки параметры добавляются на Back CTS.

```
prometheus_options:
  command:
    - --config.file=/etc/prometheus/prometheus.yml
    - --storage.tsdb.path=/prometheus
    - --storage.tsdb.retention.time=90d
    - --web.console.libraries=/etc/prometheus/console_libraries
    - --web.console.templates=/etc/prometheus/consoles
    - --web.external-url=/system/prometheus
    - --web.route-prefix=/
```

Интерфейс для доступа к Prometheus:

- url – задается в файле settings.yaml;
- username: prometheus;
- password: генерируется в файле settings.yaml при инициализации.

GRAFANA

Grafana — это платформа с открытым исходным кодом для визуализации, мониторинга и анализа данных. Grafana позволяет пользователям создавать дашборды с панелями, каждая из которых отображает определенные показатели в течение установленного периода времени. Каждый дашборд универсален, поэтому его можно настроить для конкретного проекта или с учетом любых потребностей разработки и/или бизнеса.

Публичный дашборд для сервера Single: https://grafana.com/grafana/dashboards/21386-express-single-cts/

Для установки Grafana с отдельным обратным прокси-сервисом:

1. На отдельном хосте создайте директорию:

```
mkdir /opt/grafana && cd /opt/grafana
```

2. В этой директории создайте файл docker-compose.yaml с содержанием

```
services:
  grafana:
    image: grafana/grafana-enterprise
    container_name: grafana
    environment:
      TZ: Europe/Moscow
    restart: unless-stopped
    volumes:
      - "grafana:/var/lib/grafana"
    ports:
     - "8001:3000"

volumes:
  grafana:
    driver: local
```

3. Запустите команду:

```
docker compose up -d
```

После того как контейнер будет развернут, зайдите через браузер по адресу http://ip:8001/, введите логин/пароль admin/admin и измените пароль.

Для настройки работы Grafana:

1. Добавьте источник данных. Например, Prometheus. Если серверов несколько рекомендуется федерация Prometheus.
2. В меню grafana перейдите в Connections > Data sources > Add data source и нажмите «Add data source».
3. Выберите Prometheus и заполните поля формы (табл. 69):

табл. 69

Параметр	Описание
Prometheus server URL	Подключаете к серверам CTS\ETS напрямую https://fqdn/system/prometheus/. Если это федерация – http(s)://ip/. Если развернули федерацию по нашей инструкции, и они находятся в одной докер-сети — http://prometheus:9090/prom/
Authentication methods	Аутентификация по логину/паролю (например, authorization (находится на сервере в /opt/express/settings.yaml)
Prometheus type	Укажите Prometheus
Prometheus version	Укажите используемую версию Prometheus

4. Перейдите в меню Dashboards и выберите «Create dashboard».
5. Выберите «import dashboard».

6. В поле «Find and import dashboards for common applications at grafana.com/dashboards» укажите 21386 и нажмите Load.
7. В поле CTS-DEMO выберите Prometheus (ранее добавленный data-sources) и нажмите «import».

АЛЕРТЫ

Алерты — это уведомления сервиса. Они появляются, когда показатели системы приближаются к пороговому значению или пытаются выйти за его пределы. СК «Express» отслеживает следующие показатели:

- Система:
  - CPU;
  - оперативная память;
  - диск;
  - диск I/O Utilization.
- Взаимодействие компонентов:
  - ошибки 5xx;
  - ошибки 4xx;
  - длительность http-ответов по сервисам.
- Kafka:
  - задержки Kafka.
- Docker:
  - доступность модулей;
  - доступность trusts;
  - доступность хоста;
  - проблемы подключения trust-сервиса.
- Postgres:
  - различия в репликации postgres превысили 1 Гб;
  - изменение количествава нод репликации Postgres.

СИСТЕМА

CPU

Уровень: ***предупреждение***

Рекомендуемое значение срабатывания триггера: ***> 80%***

Продолжительность теста: ***5 минут***

Использование процессора в процентах:

```
100 * sum(
    avg(
        rate(node_cpu_seconds_total{mode!="idle"}[10m])
    ) without(cpu)
) without(mode)
```

Оперативная память

Уровень: ***предупреждение***

Рекомендуемое значение срабатывания триггера: ***> 80%***

Продолжительность теста: ***5 минут***

Занято оперативной памяти в процентах:

```
(1 - (
    avg_over_time(node_memory_MemAvailable_bytes[10m])
      /
    avg_over_time(node_memory_MemTotal_bytes[10m])
    )
) * 100
```

Диск

Уровень: ***предупреждение***

Рекомендуемое значение срабатывания триггера: ***> 80%***

Продолжительность теста: ***5 минут***

Занято место на дисках в процентах:

```
(1 - (node_filesystem_avail_bytes{device!~'tmpfs'} /
node_filesystem_size_bytes)) * 100
```

Диск I/O Utilization

Уровень: ***предупреждение***

Рекомендуемое значение срабатывания триггера: ***> 30%***

Продолжительность теста: ***5 минут***

Утилизация дисков в процентах:

```
irate(node_disk_io_time_seconds_total{device!~'dm.*'}[5m])
```

ВЗАИМОДЕЙСТВИЕ КОМПОНЕНТОВ

Ошибки 5xx

Это общее количество 5xx ошибок при обращениях к nginx, грубая оценка наличия проблем (неполадок — в случае 4xx ошибок) взаимодействия компонентов.

Уровень: ***предупреждение***

Рекомендуемое значение срабатывания триггера: ***> 20%***

Продолжительность теста: ***15 минут***

Процент 5xx ошибок от общего числа запросов:

```
(
    sum by (express_host)( avg_over_time(
        rate(http_requests_total{status=~"5.."}[5m])
        [1h:]
    ))
    /
    sum by (express_host)( avg_over_time(
        rate(http_requests_total[5m])
        [1h:]
    ))
) * 100
```

Ошибки 4xx

Уровень: ***предупреждение***

Рекомендуемое значение срабатывания триггера: ***> 20%***

Продолжительность теста: ***15 минут***

Процент 4xx ошибок от общего числа запросов:

```
(
    sum by (express_host)( avg_over_time(
        rate(http_requests_total{status=~"4.."}[5m])
```

```
        [1h:]
    ))
    /
    sum by (express_host)( avg_over_time(
        rate(http_requests_total[5m])
        [1h:]
    ))
) * 100
```

Длительность http-ответов по сервисам

Уровень: ***предупреждение***

Рекомендуемое значение срабатывания триггера: ***> 10 секунд***

Продолжительность теста: ***15 минут***

Средняя длительность http-ответов по сервисам:

```
increase(http_request_duration_seconds_sum{app!~'.*_socket'}[5m])
/
increase(http_request_duration_seconds_count[5m])
```

KAFKA

Задержки Kafka

Отслеживает скорость работы компонентов с данными (есть проблемы или нет).

Уровень: ***предупреждение, катастрофа***

Рекомендуемое значение срабатывания триггера: ***> 100***

Продолжительность теста: ***10 минут***

Задержки Kafka по топикам:

```
sum(kafka_consumergroup_lag) by (topic)
```

DOCKER

Доступность модулей

Метрика собирает данные доступности модулей в системе (1 — доступен, 0 — не доступен).

Уровень: ***предупреждение, катастрофа***
Рекомендуемое значение срабатывания триггера: ***=0***
Продолжительность теста: ***10 минут***

Доступность модулей:

```
up
```

Доступность trusts

Состояние сервиса trust (для неизолированных сетевых сегментов или для схем с ETS).

Метрика требуется для обзора состояния сервиса, отвечающего за маршрутизацию cj внешними сетевыми сегментами. Значения: 1 — штатное состояние, 0 — модуль недоступен, 2+ — ошибка в работе отказоустойчивости (при наличии).

Уровень: ***предупреждение, катастрофа***

Рекомендуемое значение срабатывания триггера: ***=0***

Продолжительность теста: ***5 минут***

Доступность trusts:

```
up{job="trusts"}
```

Доступность хоста

Метрика показывает доступность CTS на основе доступности HTTP-ответов.

Уровень: ***предупреждение, катастрофа***

Рекомендуемое значение срабатывания триггера: ***< 1***

Продолжительность теста: ***5 минут***

Количество подключений http:

```
sum by(express_host)  (http_connections)
```

Проблемы подключения trust-сервиса

Метрика указывает на неполадки с маршрутизацией между CTS/eCTS/ETS/RTS.

Уровень: ***предупреждение, катастрофа***

Рекомендуемое значение срабатывания триггера: ***> 0***

Продолжительность теста: ***5 минут***

Трастовые подключения:

```
connection_status{status="red"}
```

POSTGRES

Метрики для систем с отказоустойчивыми кластерами postgres.

Различия в репликации Postgres превысили 1 Gb

Метрика указывает на проблемы в репликации данных внутри кластера.

Уровень: ***предупреждение, катастрофа***

Рекомендуемое значение срабатывания триггера: ***> 1***

Продолжительность теста: ***10 минут***

Выполните команду:

```
sum by(slot_name) (pg_replication_slots_pg_wal_lsn_diff) / 1073741824
```

Изменение количества нод репликации Postgres

Метрика указывает на изменения в поведении кластера.

Уровень: ***предупреждение, катастрофа***

Рекомендуемое значение срабатывания триггера: ***!= <количество реплик>***

Продолжительность теста: ***10 минут***

Выполните команду:

```
count(pg_replication_slot_slot_is_active)
```

Приложение 6

НАСТРОЙКА ХОСТОВ SMARTAPPPROXY

Если файл из КСПД должен стать частью веб-страницы SmartApp Frontend (например, видео в плеере), передача файлов через сервис «File Service» не работает, так как SmartApp Frontend является отдельным компонентом.

Для этой задачи существует вариант передачи файлов через smartapp_proxy, который могут использовать разработчики SmartApp.

Примечание:

- данный функционал доступен только в SmartApp без кеширования и с проксированием;
- данная инструкция актуальна для сборки сервера CTS 3.4 или выше.

Для настройки хостов SmartAppProxy на Single CTS:

1. Добавьте в файл settings.yaml сервера CTS:

```
smartapp_proxy_enabled: true
smartapp_proxy_env_override:
COOKIE_KEY: _file_service_key
COOKIE_SIGNING_SALT: <salt из file_service или vm5ponDZ вшитый дефолт>
```

2. Выполните деплой:

```
dpl -p
dpl -d smartapp_proxy admin
```

3. В разделе «SmartApp» веб-интерфейса администратора CTS в блоке «Настройки хостов SmartAppProxy»:
   - в поле «Host ID» введите произвольный набор из латинских букв и цифр. Этот ID является элементом URL к проксируемому файлу;
   - в поле «Host» введите URL ресурса, с которого будут запрашиваться файлы.

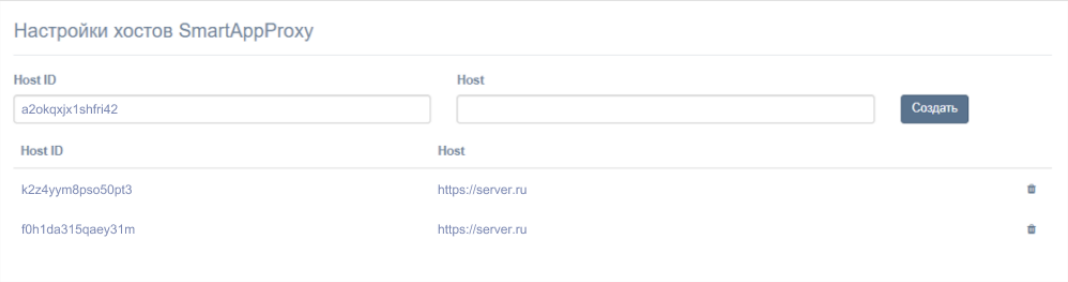

рис. 49

4. Нажмите «Создать».

Для настройки хостов SmartAppProxy на разделенном корпоративном сервере (Front CTS+Back CTS):

1. Добавьте в файл settings.yaml сервера Back CTS:

```
smartapp_proxy_enabled: true
smartapp_proxy_env_override:
COOKIE_KEY: _file_service_key
COOKIE_SIGNING_SALT: <salt из file_service или vm5ponDZ вшитый дефолт>
```

2. Выполнить деплой:

```
dpl -p
dpl -d smartapp_proxy admin
```

3. В разделе «SmartApp» веб-интерфейса администратора CTS в блоке «Настройки хостов SmartAppProxy»:
   - в поле «Host ID» введите произвольный набор из латинских букв и цифр. Этот ID является элементом URL к проксируемому файлу;
   - в поле «Host» введите URL ресурса, с которого будут запрашиваться файлы.

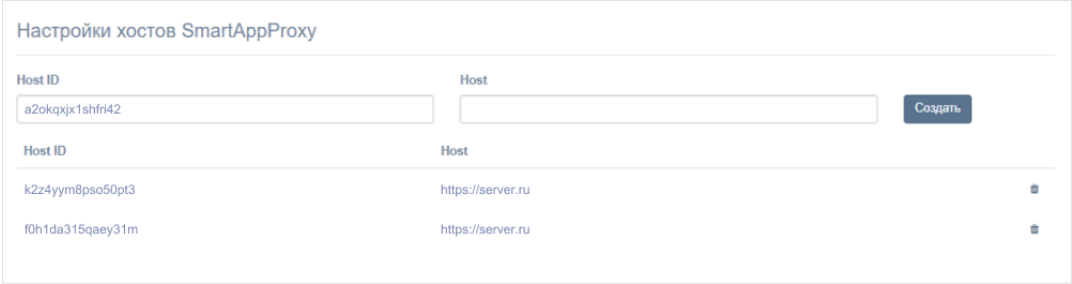

рис. 50

4. Нажмите «Создать».

Приложение 7

СЕТЕВАЯ СХЕМА ВЗАИМОДЕЙСТВИЯ С АТС ДЛЯ SINGLE CTS

Сетевая схема взаимодействия с АТС при развертывании Single CTS представлена на рисунке ниже (рис. 51).

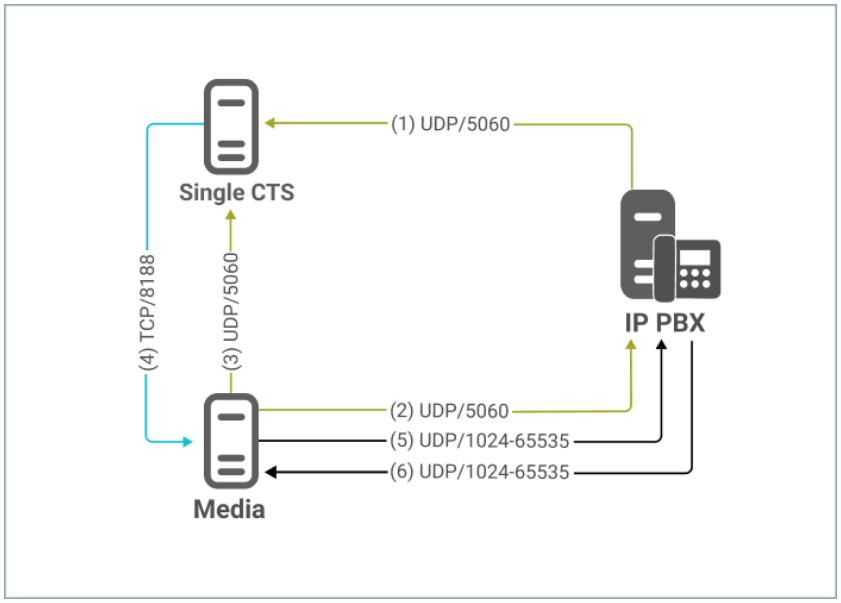

рис. 51. Сетевая схема взаимодействия с АТС при развертывании Single CTS

Сетевые взаимодействия для схемы развертывания Single представлены в табл. 70 (номера соединений в таблице соответствуют номерам соединений на рисунке выше — рис. 51).

табл. 70

№	IP источника	Порт источника	IP назначения	Порт назначения	Протокол	Описание
1	IP PBX	1024–65535	IP Single CTS	5060	UDP	SIP-сигнализация вызова от IP АТС
2	IP Media	1024–65535	IP PBX	5060	UDP	SIP-сигнализация вызова к IP АТС
3	IP Media	1024–65535	IP Single CTS	5060	UDP	SIP-сигнализация вызова к Single CTS
4	IP Single CTS	1024–65535	IP Media	8188	TCP	Управление работой сервера конференций
5	IP Media	1024–65535	IP PBX	1024-65535	UDP	Медиаданные вызова к IP АТС
6	IP PBX	1024–65535	IP Media	1024-65535	UDP	Медиаданные вызова к приложению

Приложение 8

СЕТЕВАЯ СХЕМА ВЗАИМОДЕЙСТВИЯ С АТС ПРИ РАЗВЕРТЫВАНИИ FRONT CTS И BACK CTS

Сетевая схема взаимодействия с АТС при развертывании Front CTS + Media и Back CTS представлена на рисунке ниже (рис. 52).

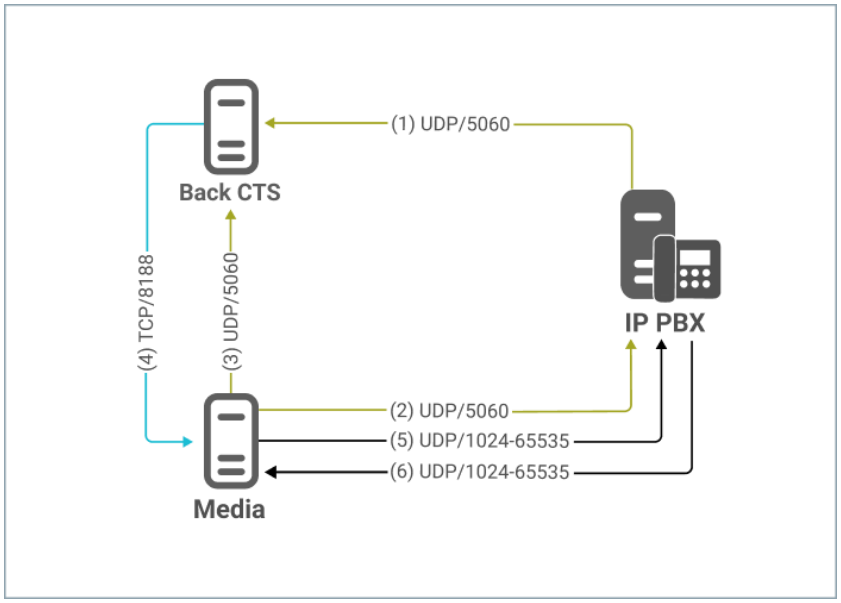

рис. 52. Сетевая схема взаимодействия с АТС при развертывании Front CTS + Media и Back CTS

Сетевые взаимодействия для схемы развертывания Front CTS + Media и Back CTS представлены в табл. 71 (номера соединений соответствуют номерам на рисунке выше — рис. 52).

табл. 71

№	IP источника	Порт источника	IP назначения	Порт назначения	Протокол	Описание
1	IP PBX	1024-65535	IP Single CTS	5060	UDP	SIP-сигнализация вызова от IP АТС
2	IP Media	1024-65535	IP PBX	5060	UDP	SIP-сигнализация вызова к IP АТС
3	IP Media	1024-65535	IP Single CTS	5060	UDP	SIP-сигнализация вызова к Single CTS
4	IP Single CTS	1024-65535	IP Media	8188	TCP	Управление работой сервера конференций
5	IP Media	1024-65535	IP PBX	1024-65535	UDP	Медиаданные вызова к IP АТС
6	IP PBX	1024-65535	IP Media	1024-65535	UDP	Медиаданные вызова к приложению

Приложение 9

ИНТЕГРАЦИЯ CTS И KEYCLOAK

Keycloak — это продукт с открытым исходным кодом для реализации единого входа. Данное программное обеспечение позволяет управлять идентификацией и доступом к сервисам и приложениям. Лицензия ПО — Apache License 2.0, разработано RedHat, Inc.

Основные функции Keycloak:

- управление пользователями, группами и ролями;
- аутентификация клиентских приложений по протоколам OpenID Connect и SAML;
- единый вход (single sign-on);
- поддержка как реляционных СУБД, так и NoSQL (MongoDB);
- кластеризация;
- ограниченная поддержка аутентификации по OTP (с помощью Google Authenticator);
- интеграция с внешними директориями LDAP и Active Directory;
- интеграция с социальными сервисами (Facebook, Twitter, GitHub, StackExchange etc.);
- расширение функциональности через разработку собственных SPI.

ТРЕБОВАНИЯ К KEYCLOAK

Рекомендуется версия Keycloak 21.1.2 и выше.

При установке необходимо выполнить следующие условия:

- настроена конфигурация HTTPS;
- указано публичное имя хоста Keycloak (FQDN) в соответствии с выпущенным SSL сертификатом;
- используется база данных PostgreSQL.

В настройках области (Realm) указаны следующие значения (табл. 72):

табл. 72

Параметр	Значение	Комментарий
Tokens -> Access Token Lifespan	8 Hours	Продолжительность жизни токена доступа
Sessions -> SSO Session Idle	8 Hours	Таймаут сессии SSO
Sessions -> SSO Session	9 Hours	Ограничение сессии SSO

Указанные интервалы необходимы для минимизации возможных негативных последствий при операциях обновлений токена и сокращение нагрузки компонентов CTS и Keycloak.

Требования к параметрам федерации LDAP (при наличии) (табл. 73):

табл. 73

Параметр	Значение	Комментарий
User federation -> LDAP -> Settings -> Import users	ON	Включение импорта пользователей
User federation -> LDAP -> Settings -> Sync Registrations	ON	Новые пользователи, созданные Keycloak, будут добавляться в LDAP

Параметр	Значение	Комментарий
User federation -> LDAP -> Settings -> Periodic full sync	ON	Периодическая полная синхронизация
User federation -> LDAP -> Settings -> Full sync period	3600	Период полной синхронизации. Значение не должно быть больше настроенного интервала в интерфейсе администратора CTS
User federation -> LDAP -> Settings -> Periodic changed users sync	ON	Периодическая синхронизация изменений пользователей
User federation -> LDAP -> Settings -> Changed users sync period	300	Период синхронизации измененных пользователей

Требования к передаче ролей (для реализации правил ролевой модели): необходимо включить в передачу id_token и userinfo список ролей доступных пользователю Keycloak.

ЭТАПЫ РЕГИСТРАЦИИ/АВТОРИЗАЦИИ

Основные этапы регистрации/авторизации пользователя на CTS с помощью Keycloak показаны на схеме ниже (рис. 53):

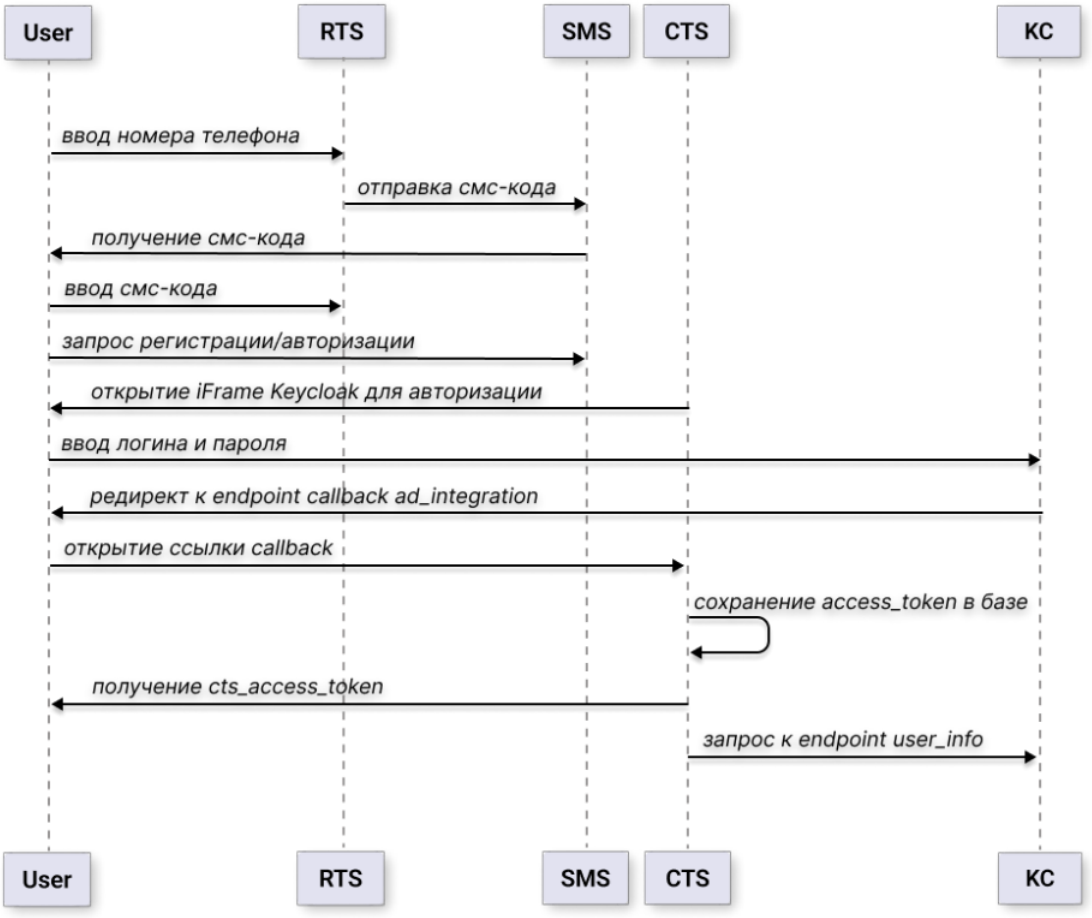

рис. 53. Основные этапы регистрации/авторизации пользователя на CTS с помощью Keycloak

СЕТЕВЫЕ ВЗАИМОДЕЙСТВИЯ

Существуют два варианта сетевых взаимодействий.

Схема пользовательского доступа к интерфейсу Keycloak показана на рисунке ниже (рис. 54):

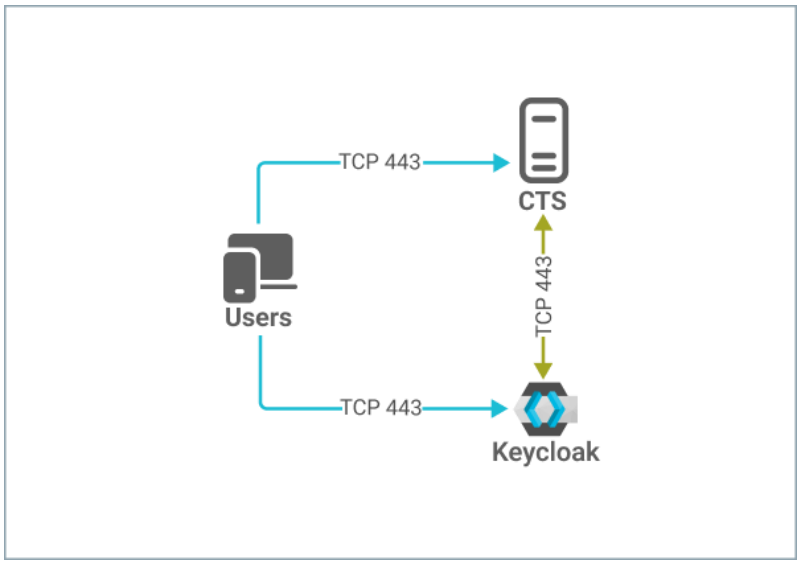

рис. 54. Пользовательский доступ к интерфейсу Keycloak

Схема пользовательского доступа к интерфейсу Keycloak через reverse proxy показана на рисунке ниже (рис. 55):

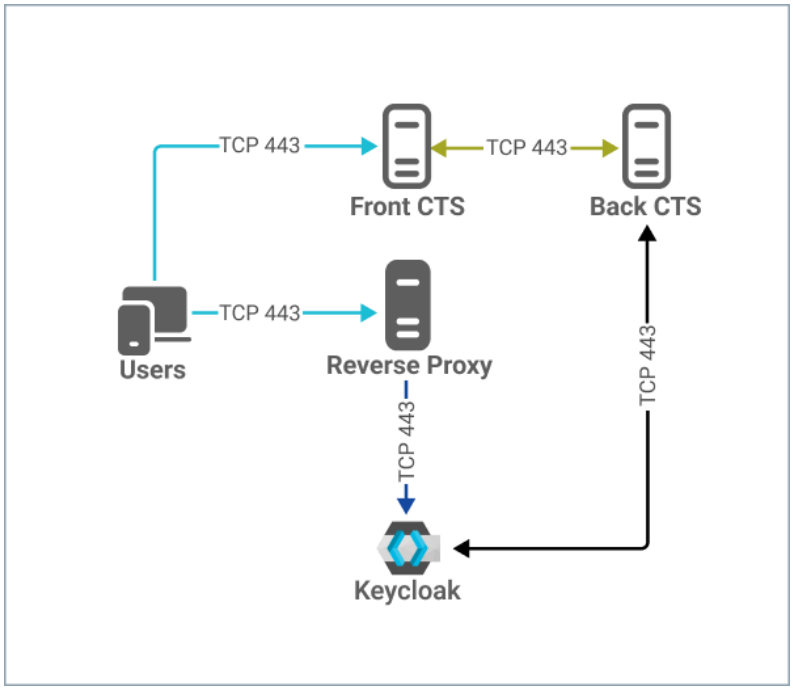

рис. 55. Пользовательский доступ к интерфейсу Keycloak через reverse proxy

НАСТРОЙКА ИНТЕГРАЦИИ

Примечание. Данное описание настройки интеграции составлено на примере интерфейса консоли администратора Keycloak версии 21.1.2.

Настройка интеграции CTS и Keycloak включает в себя следующие процедуры:

- создание client scope;
- настройка маппинга полей;
- создание client;
- настройка отображение формы авторизации Keycloak;
- настройка авторизацию по QR-коду.

СОЗДАНИЕ CLIENT SCOPE

Для интеграции CTS и Keycloak, необходимо сначала создать client scope и настроить маппинг полей:

- username — обязательный параметр (в веб-интерфейсе администратора CTS указать соответствие «Имя пользователя» — «preferred_username»);
- user ID — обязательный параметр;
- domain — обязательный параметр (в веб-интерфейсе администратора CTS указать соответствие «Домен» — «domain»);
- name — необязательный параметр;
- public name — необязательный параметр;
- company — необязательный параметр.

Дополнительные мапперы создаются опционально с типом «User Attribute» и привязываются к конечной точке «user-info».

Для создания client scope:

1. В консоли администратора Keycloak перейдите в раздел «Client scopes».
2. Нажмите «Create client scope» и задайте следующие значения (рис. 56 и табл. 74):

табл. 74

Параметр	Значение
Name	Название client scope. Например, **express-scopes**
Description	Оставить незаполненным
Type	None
Display on consent screen	On
Consent screen text	Оставить незаполненным
Include in token scope	On
Display Order	Оставить незаполненным

3. Нажмите «Save».

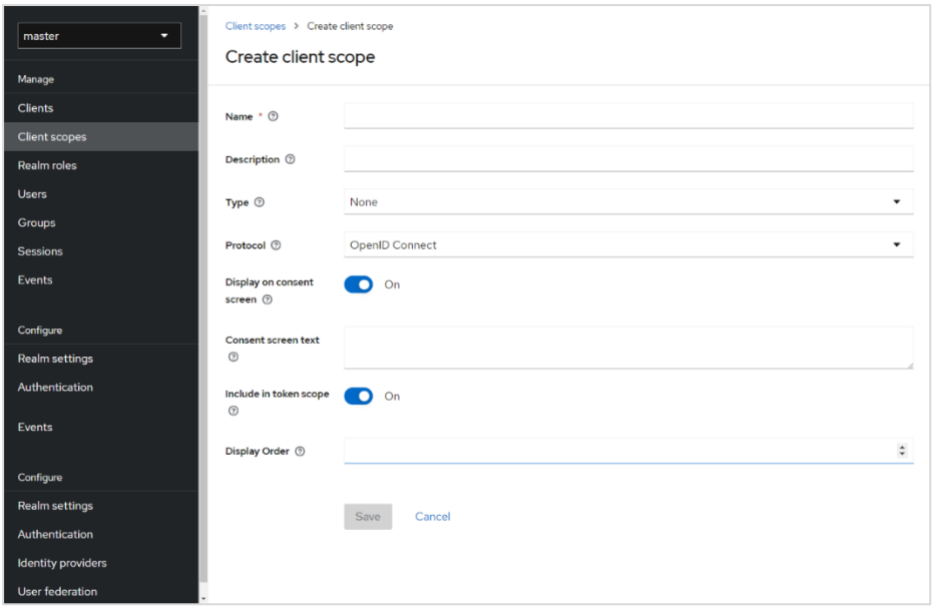

рис. 56

НАСТРОЙКА МАППИНГА ПОЛЕЙ

Для добавления маппинга полей типа «User property»:

1. В созданном client scope «express-scopes» выберите вкладку «Mappers».
2. Нажмите «Configure a new mapper» (рис. 57).

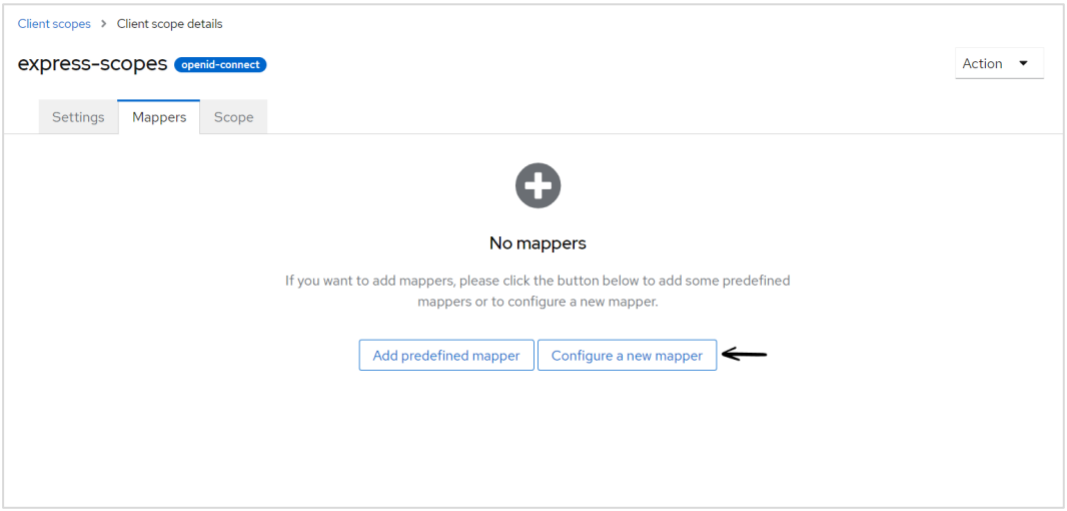

рис. 57

3. В окне «Configure a new mapper» выберите «User Property».
4. В отобразившемся окне задайте следующие значения (рис. 58).
   - для атрибута «Username» согласно табл. 75:

табл. 75

Поле/переключатель	Значение
Mapper type	User Property
Name	username
Property	username
Token Claim Name	preferred_username
Claim JSON Type	String

Поле/переключатель	Значение
Add to ID token	On
Add to access token	On
Add to userinfo	On

- для атрибута «User ID» согласно табл. 76:

табл. 76

Поле/переключатель	Значение
Mapper type	User Property
Name	User ID
Property	id
Token Claim Name	user_id
Claim JSON Type	String
Add to ID token	On
Add to access token	On
Add to userinfo	On

5. Нажмите «Save».

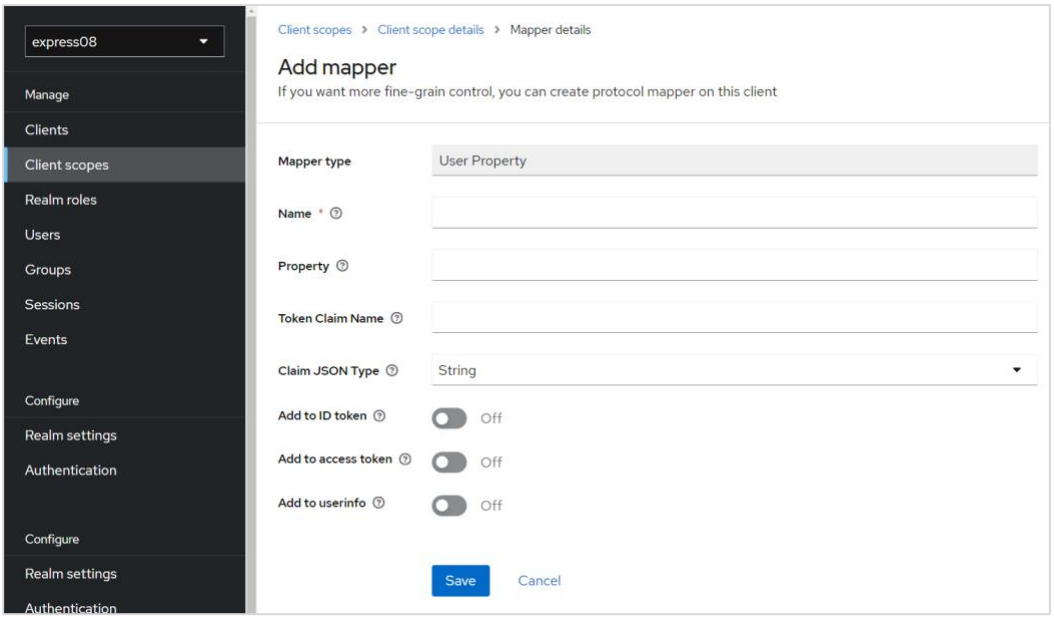

рис. 58

Для добавления маппинга полей типа «User attribute»:

1. В созданном client scope «express-scopes» выберите вкладку «Mappers».
2. Нажмите «Configure a new mapper» (рис. 57).
3. В окне «Configure a new mapper» выберите пункт «User Attribute».
4. В отобразившемся окне задайте следующие значения (рис. 59):
   - для атрибута «Domain» (обязательный атрибут) согласно табл. 77:

табл. 77

Поле/переключатель	Значение
Mapper type	User Attribute
Name	Domain
User Attribute	domain
Token Claim Name	domain
Claim JSON Type	String

Поле/переключатель	Значение
Add to ID token	On
Add to access token	Off
Add to userinfo	On
Multivalued	Off
Aggregate attribute values	Off

- для атрибута «Name» (опциональный атрибут) согласно табл. 78:

табл. 78

Поле/переключатель	Значение
Mapper type	User Attribute
Name	Name
User Attribute:	name
Token Claim Name	name
Claim JSON Type	String
Add to ID token	Off
Add to access token	Off
Add to userinfo	On
Multivalued	Off
Aggregate attribute values	Off

- для атрибута «Public name» (опциональный атрибут) согласно табл. 79:

табл. 79

Поле/переключатель	Значение
Mapper type	User Attribute
Name	Public name
User Attribute:	public_name
Token Claim Name	public_name
Claim JSON Type	String
Add to ID token	Off
Add to access token	Off
Add to userinfo	On
Multivalued	Off
Aggregate attribute values	Off

- для атрибута «Company» (опциональный атрибут) согласно табл. 80:

табл. 80

Поле/переключатель	Значение
Mapper type	User Attribute
Name	Company
User Attribute:	company
Token Claim Name	company
Claim JSON Type	String
Add to ID token	Off
Add to access token	Off
Add to userinfo	On
Multivalued	Off
Aggregate attribute values	Off

5. Нажмите «Save».

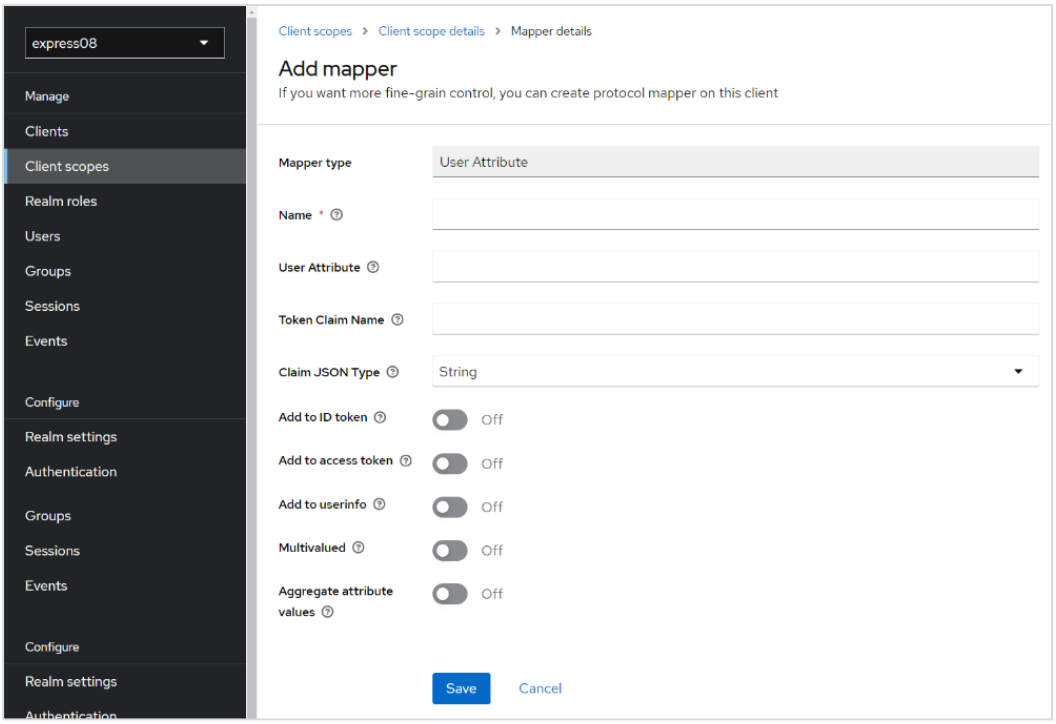

рис. 59

СОЗДАНИЕ CLIENT

Для создания Client:

1. В консоли администратора Keycloak перейдите в раздел «Clients».
2. Нажмите «Create client».
3. В открывшемся окне задайте следующие значения (рис. 60) в соответствии с табл. 81:

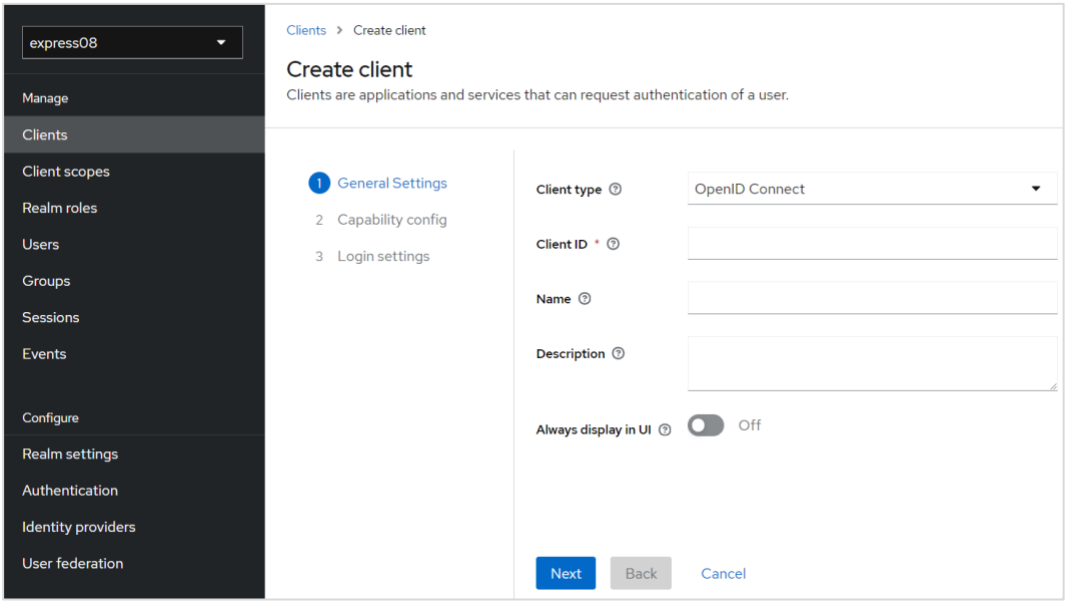

рис. 60

табл. 81

Параметр	Значение
Client type	OpenID Connect
Client ID	Идентификационный номер клиента, например **«express-adintegration»**
Name	CTS integration
Description	Оставить незаполненым
Always display in UI	Off

4. Нажмите «Next».
5. В открывшемся окне задайте следующие значения в соответствии с табл. 82:

табл. 82

Параметр	Значение
Client authentication	On
Authorization	Оставить незаполненым
Authentication flow	Установите флаги: • «Standard flow»; • «Direct access grants»; • «Service accounts roles»; • «OIDC CIBA Grant»

6. Нажмите «Next» и задайте следующие значения в соответствии с табл. 83:

табл. 83

Параметр	Значение
Root URL	Оставить незаполненым
Home URL	Оставить незаполненым
Valid redirect URIs	https://cts.company.local/api/v1/ad_integration/openid/success* (адрес cts.company.local необходимо заменить на адрес своего CTS/CTS BACK)
Valid post logout redirect URIs	+
Web origins	*

7. Нажмите «Save».
8. В созданном Client перейдите в раздел «Client scopes».
9. Нажмите «Add client scope».
10. Выберите созданный ранее client scope «express-scopes».
11. Нажмите на меню «Add» и выберите «Default».
12. Далее в окне «Client details» для scope «offline_access» установите значение «Default».

НАСТРОЙКА ОТОБРАЖЕНИЯ ФОРМЫ АВТОРИЗАЦИИ KEYCLOAK

Для отображения формы авторизации Keycloak:

1. В консоли администратора Keycloak перейдите в раздел «Realm settings».
2. Выберите вкладку «Security defenses».
3. В поле «Content-Security-Policy» укажите:

```
frame-src 'self'; frame-ancestors 'self' https://web.company.local
file:; object-src 'none';
```

Примечание. Красным цветом выделен пример адреса веб-клиента:

- для CTS-сервера укажите https://corp.express;
- для ETS-сервера укажите адрес его веб-клиента (например, https://web.ets.local).

4. Нажмите «Save».

НАСТРОЙКА АВТОРИЗАЦИИ ПО QR-КОДУ

Для включения авторизации на CTS-сервере по QR-коду в командной строке в строке запуска сервера Keycloak добавить:

```
--spi-ciba-auth-channel-ciba-http-auth-channel-http-authentication-channel-uri=https://ru.public.express
/api/v1/authentication/openid/ciba/callback
```

Для включения авторизации на ETS-сервер по QR-коду в командной строке запуска в строке сервера Keycloak добавить:

```
--spi-ciba-auth-channel-ciba-http-auth-channel-http-authentication-channel-uri=https://ets.corp.lan
/api/v1/authentication/openid/ciba/callback
```

РОЛЕВАЯ МОДЕЛЬ

В рамках ролевой модели для отдельных групп пользователей администратор может устанавливать ограничения для пользователей на операции с вложениями:

- запрет на отправку/пересылку вложений в чаты;
- запрет на загрузки/просмотра вложений в чатах;
- запрет возможности переслать/поделиться/сохранить вложения в память устройства.

Ограничения могут распространяться:

- на тип вложений (изображение, видео, документ);
- формат документов (например, PDF, DOCX, TXT и т. д.);
- размер вложений (например, 300 Мб);
- определенные чаты/каналы;
- обсуждения и чаты звонков/конференций;
- пользователей.

Вначале администратор в разделе «Группы пользователей» создает группы пользователей, на которые будут распространятся ограничения, а затем в разделе «Ролевая модель» – правила, которым будут подчиняться ограничения.

Ограничения могут быть установлены для конкретных пользователей или определенных групп в зависимости от принадлежности к серверу (подробнее см. в документе «Руководство администратора. Том 2. Эксплуатация сервера CTS»).

При создании группы администратор может указать OpenID пользователя (рис. 61).

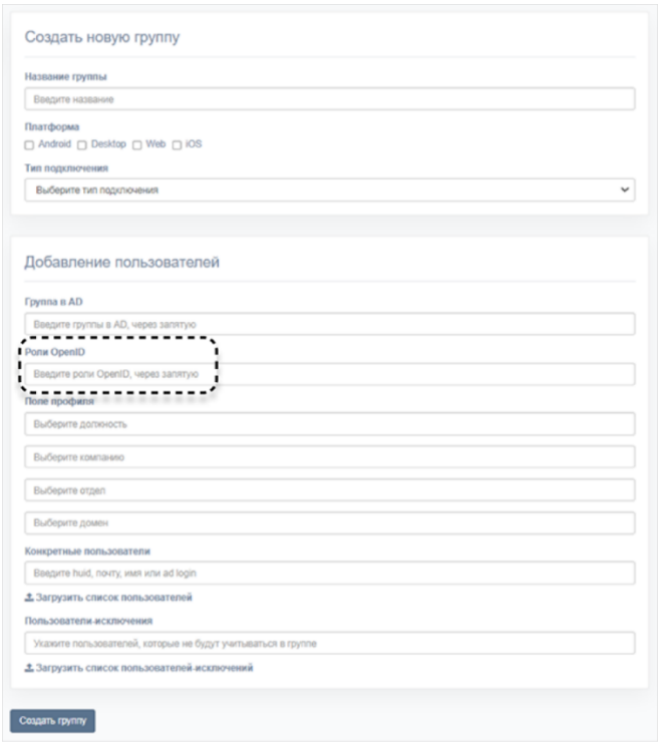

рис. 61

Для корректной работы ролевой модели предварительно нужно настроить роль пользователя в Keycloak.

Для настройки роли пользователя в Keycloak:

1. В интерфейсе администратора в Keycloak в настройках Client scopes выберите «roles» (рис. 62).

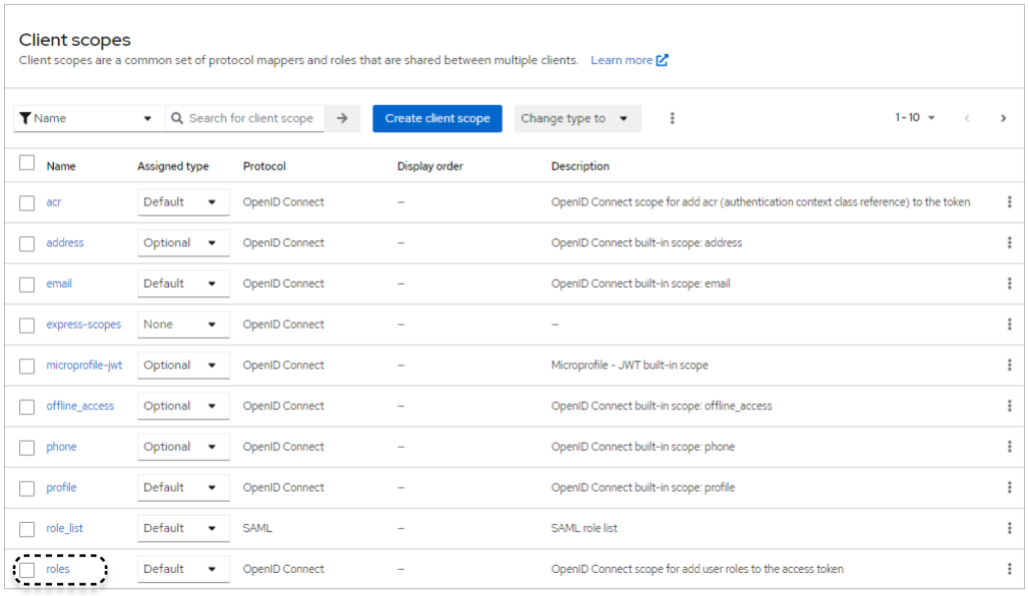

рис. 62

2. В открывшемся окне перейдите на вкладку «Mappes» и выберите «realm roles» (рис. 63).

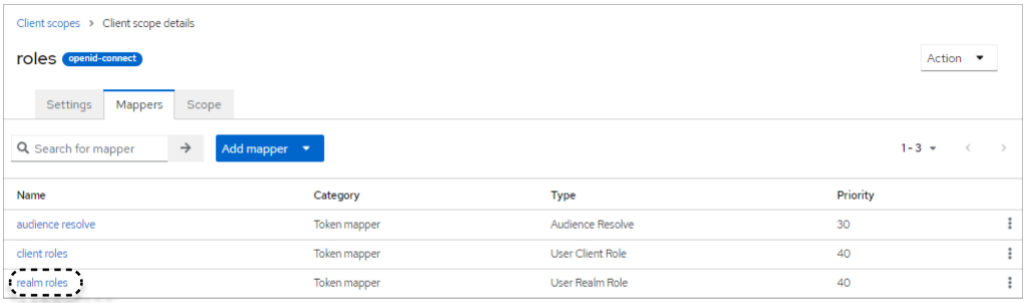

рис. 63

3. В открывшемся окне активируйте опции «Add to ID token» и «Add to userinfo», передвинув выключатель вправо (рис. 64).

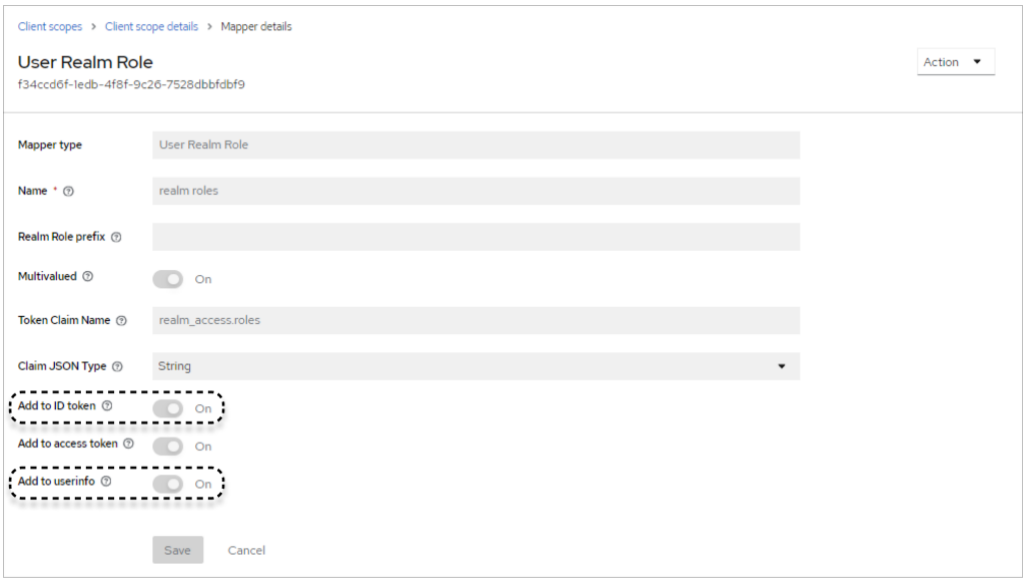

рис. 64

4. Проверьте корректность настроек в информации о пользователе (рис. 65).

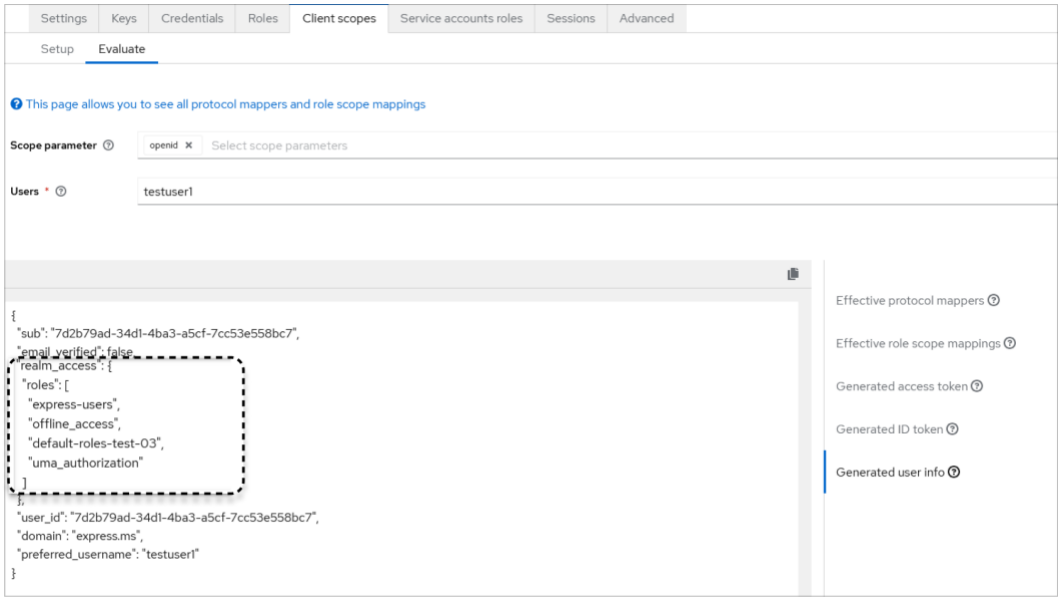

рис. 65

5. Перейдите в настройки OpenID в веб-интерфейсе администратора Express (рис. 66).

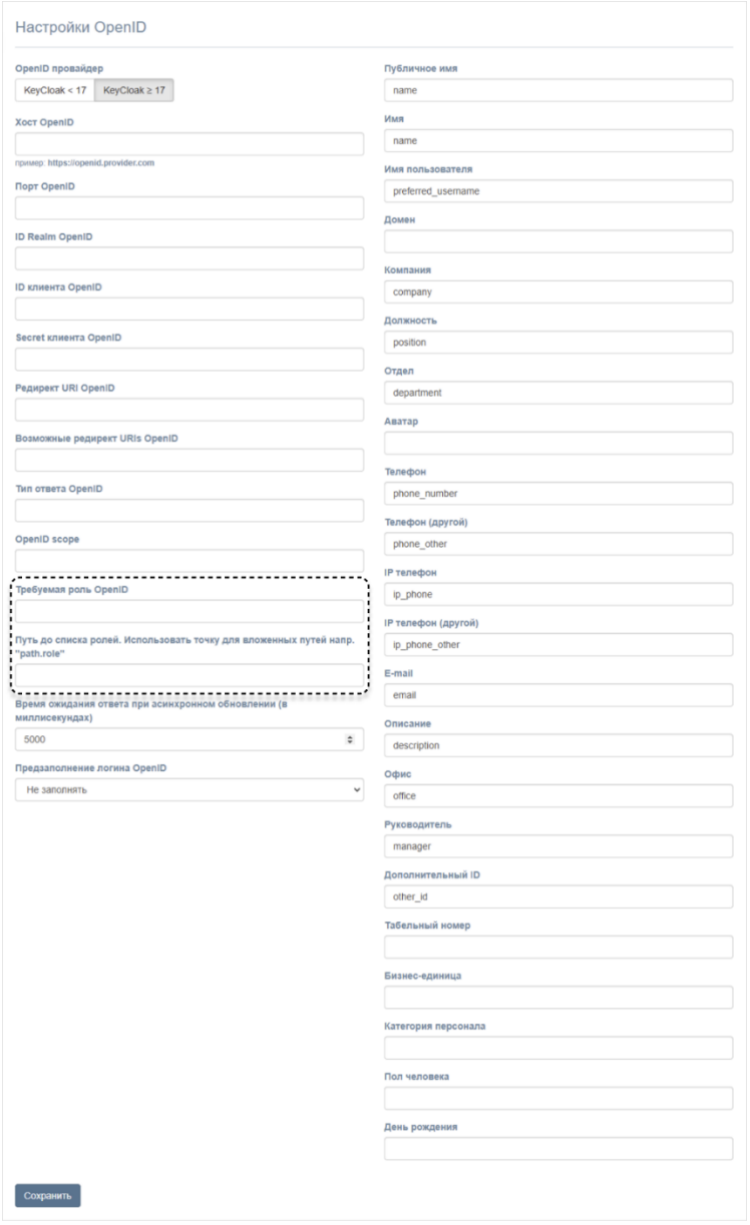

рис. 66

6. Укажите требуемую роль OpenID – realm-management query-groups.
7. Проверьте путь до ролей. Стандартный путь – realm_access.roles. Если он отличается, введите стандартное значение.
8. Нажмите «Сохранить».

ИСТОРИЯ ИЗМЕНЕНИЙ

Раздел «История изменений» содержит список изменений в документе, связанных с изменениями/доработками СК «Express».

Сборка 2.5.7

№	Раздел	Изменение	Сервер	Ссылка
1.	Настройка интеграции с Active Directory	Дополнены требования к аватарам пользователей		стр. 95
2.	Установка корпоративного сервера eXpress	Исправлено примечание		стр. 52
3.	Настройка push-уведомлений	Добавлено примечание с указанием APN Push сервисов	ETS	стр. 75
4.	Приложение 6	Добавлено		стр. 122
5.	Настройка сервера VoEx	Актуализированы рисунки	CTS	стр. 62
6.	Подключение SMTP-сервера	Дополнена информация в списке «Настройки e-mail»	CTS	стр. 92
7.	Настройка аутентификации администраторов	В тексте переименован пункт меню	CTS	стр. 93
8.	Термины и определения	Добавлены АТС и SIP	CTS	стр. 7
9.	Основные компоненты	Добавлена информация о SIP	CTS	стр. 8
10.	Единый корпоративный сервер	Добавлена информация о SIP	CTS	стр. 14
11.	Разделенный корпоративный сервер	Добавлена информация о SIP	CTS	стр. 17
12.	Установка Single CTS	Добавлен параметр SIP	CTS	стр. 55
13.	Настройка сервера VoEx	Добавлено	CTS	стр. 62
14.	Настройки АТС SIP-транк	Добавлено	CTS	стр. 64
15.	Приложение 7	Добавлено	CTS	стр. 134
16.	Приложение 8	Добавлено	CTS	стр. 134
17.	Приложение 9	Добавлено	CTS	стр. 135

Сборка 2.6.0

№	Раздел	Изменение	Сервер	Ссылка
1.	Основные компоненты	Добавлена информация о модуле SIP		стр. 8
2.	Архитектура. Единый корпоративный сервер	Добавлена информация о подключении АТС, архитектурные схемы, сетевые схемы взаимодействия, убрали компонент ZooKeeper		стр. 14
3.	Архитектура. Разделенный корпоративный сервер			стр. 17
4.	Приложение 7			стр. 134
5.	Приложение 8			стр. 134

№	Раздел	Изменение	Сервер	Ссылка
	Архитектура. Сервер предприятия и единый корпоративный сервер	Убрали компонент ZooKeeper		стр. 20
6.	Архитектура. Сервер предприятия и разделенный корпоративный сервер	Убрали компонент ZooKeeper		стр. 22
7.	Установка Single CTS	В таблицу с доступными параметрами конфигурации добавлен параметр для подключения SIP		стр. 57
8.	Настройка сервера VoEx	Добавлены изменения в настройку сервера VoEx и SIP	CTS, ETS	стр. 62
9.	Настройка АТС SIP-транк	Добавлен раздел о настройке SIP-транк в зависимости от архитектуры развертывания		стр. 64

Сборка 2.7.0

№	Раздел	Изменение	Сервер	Ссылка
1.	Архитектура	Добавление поясняющие примечания об особенностях конфигурации, добавлено описание Bot-сервера		стр. 12
2.	Системные требования	Актуализированы системные требования к платформе		стр. 28
3.	Единый корпоративный сервер	Актуализирована типовая схема развертывания	CTS	стр. 14
4.	Разделенный корпоративный сервер	Актуализирована типовая схема развертывания	CTS	стр. 17
5.	Сервер предприятия и единый корпоративный сервер	Актуализирована типовая схема развертывания	ETS, CTS	стр. 20
6.	Сервер предприятия и разделенный корпоративный сервер	Актуализирована типовая схема развертывания	ETS, CTS	стр. 22
7.	Приложение 1	Актуализирована таблица сетевых взаимодействий	CTS	стр. 112
8.	Приложение 2	Актуализирована таблица сетевых взаимодействий	CTS	стр. 114
9.	Приложение 3	Актуализирована таблица сетевых взаимодействий	ETS, CTS	стр. 117
10.	Приложение 4	Актуализирована таблица сетевых взаимодействий	ETS, CTS	стр. 119

Сборка 2.9.0

№	Раздел	Изменение	Сервер	Ссылка
1.	Настройка подключений корпоративных серверов	Актуализирована информация о заполнении поля «Имя»	ETS	стр. 88

№	Раздел	Изменение	Сервер	Ссылка
2.	Установка Веб-клиента	Перенесен раздел	ETS	стр. 48
3.	Настройка сервера VoEx	Изменена структура раздела		стр. 62
4.	Настройка интеграции с Active Directory	Актуализирован пункт о настройке видимости полей профиля	CTS	стр. 95
5.	Настройка СМС-сервиса	Добавлено	ETS	стр. 84

Сборка 2.10.0

№	Раздел	Изменение	Сервер	Ссылка
1.	Требования к DNS	Добавлена информация об использовании технологии Split DNS, описаны особенности ее применения	CTS	стр. 34

Сборка 2.11.0

№	Раздел	Изменение	Сервер	Ссылка
1.	Запуск сервера	Добавлено примечание о создании учетной записи администратора сервера на Back CTS	CTS	стр. 71

Сборка 2.12.0

№	Раздел	Изменение	Сервер	Ссылка
1.	Архитектура	Добавлено примечание о Partner Express		стр. 12

Сборка 3.0.0

№	Раздел	Изменение	Сервер	Ссылка
1.	Архитектура	Из списка контейнеров удалены контейнеры «logstash» и «elasticsearch»		стр. 14 стр. 17
2.	Архитектура	В список контейнеров добавлен контейнер «metrics_service»		стр. 14 стр. 17 стр. 20 стр. 22
3.	Устранение уязвимостей	Добавлен пункт в примечание		
5.	Настройка IP-телефонии	Добавлены ссылки на Приложения 7 и 8		стр. 64
6.	Процедура обновления	Добавлен подраздел «Обновление ОС»		стр. 106
7.	Процедура установки	Актуализирована процедура установки корпоративных серверов	CTS	стр. 52
8.	Требования к DLP	Актуализированы требования к DLP		стр. 36
9.	Требования к платформе	Актуализированы требования к платформе		стр. 28
10	Обновление Deployka	По всему документу исправлена операция DEPLOYKA_SKIP_UPDATE=true на DPL_PULL_POLICY=never		
11	Актуализированы сетевые взаимодействия	Актуализированы сетевые взаимодействия в приложениях	CTS ETS	стр. 112 стр. 114 стр. 117 стр. 119

Сборка 3.1.0

№	Раздел	Изменение	Сервер	Ссылка
1.	Требования к платформе	Добавлена версия ОС 22.04 LTS		стр. 28

Сборка 3.3.0

№	Раздел	Изменение	Сервер	Ссылка
1.	Установка сервера VoEx	Обновлен		стр. 45
2.	Настройка регистрации	Добавлен	CTS	стр. 95

Сборка 3.4

№	Раздел	Изменение	Сервер	Ссылка
1.	Системные требования	Обновлены в части использования SSD вместо HDD		стр. 28

Сборка 3.5

№	Раздел	Изменение	Сервер	Ссылка
1.	Архитектура	Обновлен		стр. 12

Сборка 3.6

№	Раздел	Изменение	Сервер	Ссылка
1.	Архитектура	Добавлен контейнер «smartapp_proxy»		стр. 12
2.	Настройка хостов SmartAppProxy	Добавлен раздел		стр. 132
4	Глава 6. Устранение уязвимостей	Удалено		
6.	Настройка DLP	Обновлена команда в шаге 3		стр. 69
7.	Установка сервера VoeX	Адрес в шаге 11 изменен		стр. 45

Сборка 3.7

№	Раздел	Изменение	Сервер	Ссылка
1.	Установка web-клиента	Актуализирован порядок установки и примеры	ETS	стр. 48
2.	Настройка интеграции с Active Directory	Дополнено описание событий в Active Directory, при которых у пользователя Express будет повторно запрашиваться аутентификация на корпоративном сервере Express	CTS	стр. 96
3.	Настройка push-уведомлений	Добавлено описание подключения к Android RuStore	ETS	стр. 75

Сборка 3.8

№	Раздел	Изменение	Сервер	Ссылка
1.	Настройка OpenID	Актуализирован	CTS	стр. 100

№	Раздел	Изменение	Сервер	Ссылка
2.	Интеграция CTS и Keycloak	Создан		стр. 136
4.	Требования к платформе	Добавлена таблица «Количество пользователей: 5000»		стр. 28
5.	Основные компоненты	Добавлено «Для интеграции с системами предотвращения утечки данных, обеспечивающих проверку сообщений пользователей на наличие запрещенного контента, используется протокол ICAP (порт TCP/1344)»		стр. 8
6.	Настройка сервера VoEx (STUN и TURN)	Актуализирован		стр. 62

Сборка 3.9

№	Раздел	Изменение	Сервер	Ссылка
1.	Разделенный корпоративный сервер	Добавлен контейнер prometheus в перечень компонентов сервера Front CTS	CTS	стр. 17
2.	Запуск сервера	Добавлены требования к паролю администратора. Вынесена отдельной операцией проверка на наличие ошибок	CTS	стр. 71
3.	Настройка интеграции с Active Directory	Добавлена команда для OS Ubuntu версии 19 и выше и других систем в случае ошибки	CTS	стр. 96

Сборка 3.10

№	Раздел	Изменение	Сервер	Ссылка
1.	Требования к хранению файлов записей ВКС	Добавлена информация о требованиях к хранению файлов записей ВКС	CTS	стр. 36
2.	Установка компонентов записи звонков и конференций	Добавлен	CTS	стр. 67
3.	Настройка маппинга полей	Добавлен рисунок, дополнено описание шагов		стр. 140
4.	Процедура обновления	В разделе перечислены необходимые обновления, убраны подразделы, дана ссылка на отдельный документ по процедуре обновления.		стр. 106

Сборка 3.11

№	Раздел	Изменение	Сервер	Ссылка
1.	Требования к платформе	Удалены требования к ОС персональных компьютеров пользователей		стр. 28
2.	Установка компонентов записи звонков и конференций	Добавлено требование об обновлении версии сервера CTS перед установкой компонентов, актуализирован шаг два	CTS	стр. 67

Сборка 3.12

№	Раздел	Изменение	Сервер	Ссылка
1.	Единый корпоративный сервер	Исправлено имя докер-контейнера docker_socket_proxy в перечне докер-контейнеров Single CTS-сервера	CTS	стр. 14
2.	Разделенный корпоративный сервер	Исправлено имя докер-контейнера docker_socket_proxy в перечне докер-контейнеров Back CTS-сервера	CTS	стр. 17
3.	Разделенный корпоративный сервер	Из перечня докер-контейнеров Back CTS-сервера удален janus	CTS	стр. 17
4.	Устранение типовых ошибок	Исправлены имена докер-контейнеров: cts-containername_1; --tail		стр. 107
5.	Приложение 1	Актуализирована таблица «Сетевые взаимодействия Single CTS». Пункты 13–19	CTS	стр. 112
6.	Единый корпоративный сервер	Добавлены контейнеры transcoding, transcoding_manager и recordings_bot в перечень компонентов сервера CTS	CTS	стр. 14
7.	Разделенный корпоративный сервер	Добавлен контейнер transcoding в перечень компонентов сервера Front CTS	CTS	стр. 17
8.	Разделенный корпоративный сервер	Добавлены контейнеры transcoding_manager и recordings_bot в перечень компонентов сервера Back CTS	CTS	стр. 17

Сборка 3.13

№	Раздел	Изменение	Сервер	Ссылка
1.	Установка Front CTS- и Back CTS-серверов	Актуализирован порядок установки Front CTS-сервера (пп. 6; 7) и Back CTS-сервера (пп. 7; 8)	CTS	стр. 57
2.	Установка сервера ссылок	Добавлен раздел, описывающий установку сервера ссылок	CTS	стр. 65
3.	Установка веб-клиента	Раздел перенесен в главу 2 «Установка Express»	Для всех серверов	стр. 48
4.	Установка DLP	Добавлен отдельный раздел, описывающий установку DLP. Ранее содержавшаяся информация по установке DLP перенесена в данный раздел	CTS	стр. 67

Сборка 3.14

№	Раздел	Изменение	Сервер	Ссылка
1.	Установка Front CTS- и Back CTS-серверов	Актуализированы команды шагов 8 и 9 установки Back CTS	CTS	стр. 57
2.	Установка сервера VoEx. Предварительная настройка	Актуализирован	CTS	стр. 49
3.	Установка DLP на выделенном сервере	Добавлен шаг 3 установки выделенного DLP-сервера	CTS	стр. 67
4.	Установка сервера VoEx	Актуализировано название шага 3	CTS	стр. 50
5.	Установка сервера VoEx	Актуализирован	CTS	стр. 50
6.	Установка Single CTS	Актуализировано название шага 3	CTS	стр. 55

№	Раздел	Изменение	Сервер	Ссылка
7.	Установка Front CTS- и Back CTS-серверов	Актуализировано название шага 3	CTS	стр. 57 стр. 59

Сборка 3.16

№	Раздел	Изменение	Сервер	Ссылка
1.	Изменение названия	Произведено разделение на тома. Теперь название документа «Том 1. Установка»		
2.	Настройка интеграции с Active Directory	Актуализирован п.3 процедуры настройки интеграции с AD	CTS	стр. 96
3.	Требования к платформе	Обновлены технические требования к платформе неотказоустойчивой конфигурации	CTS	стр. 28
4.	Приложение 5. Мониторинг Express CTS	Добавлена таблица о передаче метрик Janus в Prometheus	CTS	стр. 122
5.	Приложение 1. Сетевые взаимодействия Single CTS	Актуализировано приложение	CTS	стр. 112

Сборка 3.17

№	Раздел	Изменение	Сервер	Ссылка
1.	Архитектура	Обновлены архитектурные схемы. Актуализирован список doker-контейнеров	Для всех серверов	стр. 12
2.	Мониторинг express cts	Актуализирована таблица		стр. 122

Сборка 3.18

№	Раздел	Изменение	Сервер	Ссылка
1.	Требования к DLPS	Скорректировано название	CTS	стр. 37
2.	Установка DLPS	Скорректировано название	CTS	стр. 67

Сборка 3.19

№	Раздел	Изменение	Сервер	Ссылка
1.	Установка сервера VoEx	Скорректировано значение параметра janus_ws_ac в п. 9 процедуры установки сервера VoEx	CTS	стр. 50
2.	Установка Front CTS- и Back CTS-серверов	Добавлен параметр set_real_ip_from в п. 8 процедуры установки Back CTS	CTS	стр. 59
3.	Приложение 5. Мониторинг Express CTS	Добавлен параметр «Количество пользователей, получающих медиаданные» в таблицу о передаче метрик Janus в Prometheus	CTS	стр. 122
4.	Настройка push-уведомлений	Добавлен адрес Google FCM в примечании о необходимости доступа к APN Push-сервисам	ETS	стр. 75

Сборка 3.21

№	Раздел	Изменение	Сервер	Ссылка
1.	Основные компоненты	Добавлено примечание о справочном характере информации об RTS-сервере в документе	RTS	стр. 8
2.	Региональный сервер	Добавлено примечание о справочном характере информации об RTS-сервере в документе	RTS	стр. 12
3.	По всему документу	Удалена информация об установке и настройке сервера RTS	RTS	

Сборка 3.22

№	Раздел	Изменение	Сервер	Ссылка
1.	По всему документу	В связи с архитектурными изменениями вместо сервера VoEx для обеспечения видео- и голосовой связи используется сервер Media	CTS	
2.	Архитектура	Актуализировано описание не отказоустойчивой конфигурации СК «Express» для CTS- и ETS-серверов	CTS, ETS	стр. 12
3.	Требования к платформе	Обновлены требования к платформе	CTS	стр. 28
4.	Требования к DNS	Обновлены требования к DNS	CTS	стр. 34
5.	Требования к серверу Web client	Добавлен раздел	CTS	стр. 36
6.	Требования хранению файлов записей ВКС	Информация актуализирована	CTS	стр. 36
7.	ОС Ubuntu/Debian	Раздел обновлен	CTS	стр. 39
8.	ОС Astra Linux Орел	Раздел обновлен	CTS	стр. 42
9.	Установка сервера Media	Раздел переработан, обновлены параметры установки	CTS	стр. 45
10.	Установка Single CTS	Раздел актуализирован, обновлены параметры установки	CTS	стр. 55
11.	Установка Front CTS- и Back CTS-серверов	Раздел актуализирован, обновлены параметры установки	CTS	стр. 57
12.	Настройка сервера Media	Раздел актуализирован, обновлены параметры установки	CTS	стр. 62
13.	Установка компонентов записи звонков и конференций	Раздел актуализирован, обновлены параметры установки	CTS	стр. 70
14.	Приложение 2. Сетевые взаимодействия Front CTS, Media и Back CTS	Информация актуализирована	CTS	стр. 114
15.	Приложение 3. Сетевые взаимодействия ETS и Single CTS	Информация актуализирована	CTS, ETS	стр. 117
16.	Приложение 4.	Информация актуализирована	CTS, ETS	стр. 119

№	Раздел	Изменение	Сервер	Ссылка
	Сетевые взаимодействия ETS, Front CTS и Back CTS			
17.	Приложение 8. Сетевая схема взаимодействия с АТС для Single CTS	Информация актуализирована	CTS	стр. 134
18.	Приложение 9. Сетевая схема взаимодействия с АТС при развертывании Front CTS и Back CTS	Информация актуализирована	CTS	стр. 135

Сборка 3.23

№	Раздел	Изменение	Сервер	Ссылка
1.	Установка Single CTS	Актуализирован пример файла конфигурации	CTS	стр. 56
2.	Настройка регистрации	Обновлена процедура выбора регистрации, заменен рисунок	CTS	стр. 95
3.	Настройка e-mail	Заменен рисунок	CTS	стр. 100
4.	Настройка Open ID	Заменен рисунок	CTS	стр. 100
5.	Сетевая схема взаимодействия с АТС для Single CTS	Заменен рисунок	CTS	стр. 134
6.	Сетевая схема взаимодействия с АТС при развертывании Front CTS и Back CTS	Заменен рисунок	CTS	стр. 135
7.	Настройка push-уведомлений	Добавлена таблица с описанием параметров push-уведомлений	ETS	табл. 45
8.	По всему документу	Название партнерского сервера Partner Express заменено на Partner	CTS, ETS	

Сборка 3.24

№	Раздел	Изменение	Сервер	Ссылка
1.	Требования к платформе	Обновлены технические требования к платформе. Добавлено примечание о необходимости проверки актуальности версий устанавливаемого дополнительного ПО	CTS	стр. 32
			ETS	стр. 32
			RTS	стр. 32
2.	Настройка регистрации	Актуализирован первый абзац	CTS	стр. 95
3.	Приложение 1	Обновлена таблица сетевых взаимодействий Single CTS	CTS	стр. 112
4.	Приложение 2	Обновлена таблица сетевых взаимодействий Front CTS, Media и Back CTS	CTS	стр. 114
5.	Приложение 3	Обновлена таблица сетевых взаимодействий ETS, Media и Single CTS	CTS	стр. 117

№	Раздел	Изменение	Сервер	Ссылка
6.	Приложение 4	Обновлена таблица сетевых взаимодействий ETS, Media, Front CTS и Back CTS	CTS	стр. 119

Сборка 3.26

№	Раздел	Изменение	Сервер	Ссылка
1.	Аннотация	Раздел актуализирован		
2.	По всему документу	«Предустановленное ПО» заменено на «Общесистемное ПО»		
3.	Требования к платформе	Добавлена информация о демонстрационном характере компонентов ПО и примечание об отсутствии ответственности разработчика за использование демонстрационных компонентов в продуктивной среде		стр. 33
		«Recordings» заменено на «Transcoding». «AV» заменено на «Media»		табл. 3 – табл. 16
4.	Установка Single CTS Установка серверов Front CTS и Back CTS Установка DLPS на выделенном сервере	Добавлены параметры в таблицу конфигурационного файла	CTS	стр. 55 стр. 57 стр. 67
5.	Установка веб-клиента	Актуализирована процедура установки веб-клиента		стр. 48
6.	Настройка CTS	Добавлен подраздел «Настройка регистрации»	CTS	стр. 95
7.	Процедура обновления	Раздел актуализирован		стр. 106
8.	Устранение уязвимостей	Добавлен раздел		стр. 110
9.	Дополнительные возможности	Добавлен раздел		стр. 122
10.	Настройка хостов SmartAppProxy	Актуализирована процедура настройки хостов		стр. 132
11.	Настройка отображения формы авторизации Keycloak	Добавлено примечание об адресе веб-сервера	CTS	стр. 144
12.	По всему документу	Актуализированы рисунки		

Сборка 3.27

№	Раздел	Изменение	Сервер	Ссылка
1.	По всему документу	Актуализированы рисунки		По всему документу
2.	Основные компоненты	Добавлено описание сервера Transcoding		стр. 8
3.	Архитектура	Раздел актуализирован. Заменены схемы, добавлено описание сервера Transcoding		стр. 12
4.	Установка сервера Media	Обновлена процедура установки		стр. 50, табл. 35

№	Раздел	Изменение	Сервер	Ссылка
5.	Настройка подключения сервера Media к CTS			стр. 62
6.	Установка сервера Transcoding			стр. 52
7.	Настройка серверов JANUS, STUN и TURN	Обновлена процедура установки		стр. 62
8.	Настройка push-уведомлений	Обновлены рисунки, актуализированs таблицы	ETS	стр. 75, табл. 47, табл. 51
9.	Настройка OpenID	Обновлен рисунок	CTS	стр. 100
10.	Приложение 1	Обновлена таблица сетевых взаимодействий Single CTS	CTS	стр. 112
11.	Приложение 2	Обновлена таблица сетевых взаимодействий Front CTS, Media и Back CTS	CTS	стр. 114
12.	Приложение 3	Обновлена таблица сетевых взаимодействий ETS, Media и Single CTS	CTS	стр. 117
13.	Приложение 4	Обновлена таблица сетевых взаимодействий ETS, Media, Front CTS и Back CTS	CTS	стр. 119
14.	Приложение 10	Актуализированы рисунки. Добавлено описание ролевой модели	CTS	стр. 136

Сборка 3.28

№	Раздел	Изменение	Сервер	Ссылка
1.	Разделенный корпоративный сервер	Обновлен рисунок	CTS	стр. 17
2.	Требования к серверу Media	Добавлен подраздел		стр. 35
3.	Настройка IP-телефонии	Раздел актуализирован	CTS	стр. 64
4.	Подключение SMTP-сервера	Раздел актуализирован	ETS	стр. 74
5.	Настройка подключений корпоративных серверов	Раздел актуализирован	ETS	стр. 88
6.	Регистрация без номера телефона	Раздел актуализирован	CTS	стр. 103
7.	Настройка доверительных подключений	Раздел актуализирован	CTS	стр. 103
8.	Приложение 5	Приложение актуализировано		стр. 122

Сборка 3.30

№	Раздел	Изменение	Сервер	Ссылка
1.	Установка сервера Media	Добавлен параметр transcoding_storage_enabled		стр. 50
2.	Настройка хостов SmartAppProxy	Добавлена информация о настройке		стр. 132
3.	Требования к Keycloak	Добавлен раздел		стр. 136

Сборка 3.31

№	Раздел	Изменение	Сервер	Ссылка
1.	Настройка серверов JANUS, STUN и TURN	Актуализирована информация и рисунок		стр. 62

Сборка 3.32

№	Раздел	Изменение	Сервер	Ссылка
1.	Требования к платформе	Добавлена информация о пропускной способности сети при проведении ВКС		стр. 28
2.	Требования к серверу Media	Актуализированы требования		стр. 35
3.	Установка сервера Media	Актуализирована информация		стр. 50
4.	Настройка OpenID	Добавлена таблица описания полей, актуализирован рисунок	CTS	стр. 100
5.	Prometheus	Добавлен пример кода в блоке conf/prometheus.yaml		стр. 122
6.	Подключение TLS-сертификата и Botx SSL-сертификата	Актуализирован рисунок	CTS	стр. 90

Сборка 3.33

№	Раздел	Изменение	Сервер	Ссылка
1.	Настройка серверов JANUS, STUN и TURN	Актуализирован рисунок		стр. 62
2.	Установка DLPS на выделенном сервере	Актуализировано примечание		стр. 67
3.	Архитектура	Актуализированы рисунки (схемы)		стр. 12
4.	Типы аутентификации	Добавлен раздел		стр. 24
5.	Приложение 1, Приложение 2, Приложение 3, Приложение 4	Актуализированы таблицы		стр. 112, 114, 117, 119
6.	Настройка интеграции с Active Directory	Актуализирована таблица		стр. 96

Сборка 3.34

№	Раздел	Изменение	Сервер	Ссылка
1.	Настройка серверов JANUS, STUN и TURN	Актуализирован рисунок, добавлена информация о настройках		стр. 62
2.	Архитектура	Актуализированы рисунки (схемы), удалена информация о redis на сервере Media		стр. 12
3.	Типы аутентификации	Актуализированы рисунки (схемы)		стр. 24
4.	Установка сервера Media	Актуализирована информация (redis заменен на turnserver_shared_key)		стр. 45
5.	Установка Single CTS			стр. 55
6.	Установка серверов Front CTS и Back CTS			стр. 57
7.	Подключение сервера Media к CTS-серверу			стр. 62
8.	Приложение 1, Приложение 2, Приложение 3, Приложение 4	Актуализированы таблицы		стр. 112, 114, 117, 119
9.	Установка	Актуализированы этапы развертывания серверов		стр. 38
10.	Установка ETS	Актуализирована информация		стр. 45
11.	Установка веб-клиента	Актуализирована информация		стр. 48
12.	Настройка IP-телефонии	Дополнена информация в таблице		стр. 64

Сборка 3.35

№	Раздел	Изменение	Сервер	Ссылка
1.	Архитектура	Актуализированы рисунки (схемы)		стр. 12
2.	Приложение 3, Приложение 4	Актуализированы таблицы		стр. 117, 119

Сборка 3.36

№	Раздел	Изменение	Сервер	Ссылка
1.	Настройка серверов JANUS, STUN и TURN	Актуализирована информация		стр. 62
2.	Настройка интеграции с Active Directory	Актуализирована информация		стр. 96
3.	Настройка OpenID	Удален блок о настройке уровней доступа к атрибутам		стр. 100

Сборка 3.37

№	Раздел	Изменение	Сервер	Ссылка
1.	Настройка серверов JANUS, STUN и TURN	Обновлен рисунок, актуализирована таблица		стр. 62

Сборка 3.38

№	Раздел	Изменение	Сервер	Ссылка
1.	По всему документу	Слово «контур» заменено на «сетевой сегмент»		По всему документу
2.	Установка Single CTS	В таблицу добавлена новая настройка	CTS	стр. 55

Сборка 3.39

№	Раздел	Изменение	Сервер	Ссылка
1.	Настройка регистрации	Актуализирован рисунок		стр. 95
2.	Настройка e-mail	Актуализирован рисунок и информация о заполнении полей	CTS	стр. 100
3.	Регистрация без номера телефона	Актуализировано название поля		стр. 103
4.	Настройка интеграции с Active Directory	Актуализирован рисунок и информация о заполнении полей	CTS	стр. 96

Сборка 3.40

№	Раздел	Изменение	Сервер	Ссылка
1.	Установка сервера Media	Добавлены новые параметры		стр. 49
2.	Настройка серверов JANUS, STUN и TURN	Актуализирован рисунок		стр. 62
3.	Подключение TLS-сертификата и BotX SSL-сертификата	Актуализирован рисунок	CTS	стр. 90
4.	Настройка регистрации	Добавлено примечание	CTS	стр. 95
5.	Настройка интеграции с Active Directory	Актуализирована информация о заполнении полей	CTS	стр. 96
6.	Настройка OpenID	Актуализирован рисунок и информация	CTS	стр. 100
7.	Создание Client	Актуализирована информация		стр. 143

Сборка 3.41

№	Раздел	Изменение	Сервер	Ссылка
1.	Подключение TLS-сертификата и BotX SSL-сертификата	Актуализирован рисунок	CTS	стр. 90

Сборка 3.42

№	Раздел	Изменение	Сервер	Ссылка
1.	Предварительная настройка. ОС Centos/RHEL	Унифицирована процедура установки	CTS	стр. 41
2.	Предварительная настройка. ОС Astra Linux Орел	Добавлено примечание. Унифицирована процедура установки	CTS	стр. 43
3.	Grafana	Актуализирована табл. 69	CTS	стр. 127