

ПЛАТФОРМА ВИДЕОКОНФЕРЕНЦСВЯЗИ «ДИОН»

РУКОВОДСТВО ПО УСТАНОВКЕ И ЭКСПЛУАТАЦИИ

Правообладатель: ООО «ГК «Иннотех»

Место нахождения и адрес правообладателя:

125167, г. Москва, вн. тер. г. муниципальный округ

Аэропорт, пр-кт Ленинградский, д. 36, стр. 41, помещ. 23

СОДЕРЖАНИЕ

1	Введение	3
2	Термины и сокращения	4
3	Общие сведения	6
4	Подготовка к установке	7
4.1	Состав дистрибутива	7
4.2	Требования к программному обеспечению	7
5	Установка программы	9
5.1	Порядок установки	9
5.2	Дополнительные настройки	11
5.3	Проверка работоспособности	11
6	Установка Dion Rooms	12
6.1	Порядок установки	12
6.2	Дополнительные настройки	14
6.3	Проверка работоспособности	14
7	Эксплуатационные характеристики	15
7.1	Производительность	15
7.2	Доступность и надежность	15
7.3	Ролевая модель	15
7.4	Мониторинг	15
7.5	Логирование	15

1 Введение

В документе приводятся сведения для установки и эксплуатации программного обеспечения — программы для ЭВМ «Платформа видеоконференцсвязи “ДИОН”» (далее — программа).

2 Термины и сокращения

Термины и сокращения, используемые в контексте настоящего документа:

Термин/сокращение	Определение/расшифровка
Компонент	Отдельно выделенный микросервис, подсистема, подмодуль или компонент с открытым исходным кодом, входящий в состав модуля или программы для ЭВМ и применяемый для автоматизации определенного технологического или бизнес-процесса организации
Организация	Юридическое лицо, использующее программу для ЭВМ в своей деятельности
Программа для ЭВМ	Группа модулей / модулей и компонентов, целью которых является широкое покрытие автоматизацией ряда технологических или бизнес-процессов организации
deb-пакет	(англ. Debian) Бинарные пакеты для распространения и установки программного обеспечения в операционной системе проекта Debian и других, использующих систему управления пакетами dpkg
DLP	(англ. Data Loss Prevention) Набор процессов и технологий, направленных на защиту данных от их утечек, кражи или несанкционированного доступа
docker-образ	Контейнер, содержащий прикладное программное обеспечение вместе с окружением, включая ОС, и предназначенный для работы в ПО Docker
Push-уведомления	Всплывающие сообщения, которые приложения отправляют на устройства пользователей, даже когда приложение не активно. Они служат для информирования пользователей о различных событиях, акциях, обновлениях и другой важной информации
Simple Storage Service (S3)	Протокол передачи данных, разработанный компанией Amazon с использованием защищенного протокола транспортного уровня TLS/mTLS. Также это объектное хранилище. Его уникальность заключается в хранении огромного объема данных в исходном формате без иерархии и разбивки на отдельные каталоги

Session Initiation Protocol (SIP)	Протокол установления сеанса — протокол передачи данных, описывающий способ установления и завершения пользовательского сеанса связи, включающего обмен мультимедийным содержимым (IP-телефония, видео- и аудиоконференции, мгновенные сообщения, онлайн-игры). Протокол описывает, каким образом клиентское приложение (например, софтфон) может запросить начало соединения у другого, возможно, физически удалённого клиента, находящегося в той же сети, используя его уникальное имя. Протокол определяет способ создания канала связи и согласования протоколов обмена информации между клиентами (например, протокол RTP используется для обмена голосовыми данными). Допускается добавление или удаление таких каналов в течение установленного сеанса, а также подключение и отключение дополнительных клиентов (то есть предусмотрена конференцсвязь, когда допускается участие в обмене более двух сторон). SIP также определяет порядок завершения сеанса
Single Sign-On (SSO)	Технология, при использовании которой пользователь переходит из одного раздела портала в другой, либо из одной системы в другую, не связанную с первой системой, без повторной аутентификации

3 Общие сведения

Программа объединяет в себе платформу для видеоконференций, многофункциональный мессенджер, видеохостинг и инструменты для совместной работы над проектами, предназначенные для корпоративных коммуникаций.

Для установки программы необходимо учесть требования к программному обеспечению и выполнить действия, приведенные ниже.

4 Подготовка к установке

4.1 Состав дистрибутива

Дистрибутив программы включает в себя:

- исполняемые сервисы в виде Docker-образов и deb-пакетов;
- Ansible Playbook;
- скрипты установки и конфигурации (configurator.sh, dion.sh, update.sh);
- универсальные контейнеры DION;
- уникальные контейнеры DION для конкретного домена;
- файлы конфигурации и шаблоны сертификатов;
- лицензионный файл.

4.2 Требования к программному обеспечению

Для установки и эксплуатации программы потребуются:

- операционная система семейства Linux (например, Ubuntu Server 22.04, Astra Linux версии 1.7.3 и выше (лицензия GNU General Public License от ООО «РусБИТехАстра») или «РЕД ОС» версии 7 и выше);
- прикладное программное обеспечение с открытым исходным кодом:

Название	Описание	Лицензия	Источник
Apache Kafka	Распределенная платформа для обработки потоков событий и передачи Push-уведомлений	Apache License 2.0	Официальный сайт
Grafana	Платформа для визуализации операционных метрик и технического мониторинга	Apache License 2.0	Официальный сайт
Janus / Mediasoup	WebRTC-серверы для обработки и микширования видео- и аудиопотоков	MIT / GPL	Официальный сайт
Keycloak	Система централизованного управления пользователями и реализации SSO (SAML, OIDC)	Apache License 2.0	Официальный сайт
Kubernetes	Платформа для оркестрации контейнеризированных модулей системы	Apache License 2.0	Официальный сайт
MinIO	Высокопроизводительное S3-совместимое хранилище для видеозаписей и файлов	GNU AGPLv3	Официальный сайт
Nginx	Высокопроизводительный HTTP-сервер и обратный прокси для маршрутизации трафика	2-clause BSD License	Официальный сайт

Название	Описание	Лицензия	Источник
PostgreSQL	Объектно-реляционная система управления базами данных для хранения профилей и метаданных	PostgreSQL License	Официальный сайт
Prometheus	Инструментарий для мониторинга состояния сервисов и сбора метрик в реальном времени	Apache License 2.0	Официальный сайт
RabbitMQ	Брокер сообщений для межмодульного взаимодействия компонентов	Apache License 2.0	Официальный сайт
Redis (open-source edition)	Хранилище данных в оперативной памяти для управления сессиями пользователей	AGPLv3	Официальный сайт

5 Установка программы

5.1 Порядок установки

Для установки программы выполните действия:

1. Смонтируйте образ операционной системы в CD-привод сервера или виртуальной машины.
2. Установите загрузку с CD-привода в настройках BIOS или в настройках конфигурации виртуальной машины.
3. Запустите сервер/виртуальную машину. Подготовьте сервер:
 - a. При первом запуске нажмите **Try or Install Ubuntu Server**.
 - b. Выберите язык операционной системы, язык раскладки клавиатуры и минимальный набор компонентов для установки.
 - c. Сконфигурируйте настройки сетевого адаптера.
 - d. Укажите адрес проху-сервера и адрес зеркала операционной системы.
 - e. Выберите способ конфигурации разделов диска.
 - f. Укажите имя сервера и учетные данные вашего профиля.
 - g. Добавьте опцию установки SSH-сервера.
 - h. Дождитесь окончания установки, размонтируйте образ из CD-привода и перезагрузите сервер.
4. Подключитесь к серверу с помощью SSH-клиента с указанными учетными данными при установке:

```
sudo adduser dion
```
5. Создайте пользователя `dion`:

```
sudo usermod -aG sudo dion
```
6. Добавьте пользователя `dion` в группу `sudo`:

```
sudo apt-get update -y
sudo apt-get install -y nano
```
7. Установите текстовый редактор `nano`:
 - a. Для корректной работы Ansible отредактируйте файл `/etc/sudoers`.

```
sudo visudo
```
 - b. Введите команду:

```
sudo cat /etc/sudoers
```
 - c. Найдите в редакторе строку `%sudo ALL=(ALL:ALL) ALL` и замените ее на `%sudo ALL=(ALL:ALL) NOPASSWD: ALL`.
 - d. Сохраните изменения и закройте редактор.

8. Подключитесь к серверу с помощью SSH-клиента с указанными учетными данными пользователя dion:

```
ssh-keygen -t rsa
```

9. Создайте новую пару SSH-ключей и скопируйте открытый SSH-ключ на этот же сервер:

```
ssh-copy-id dion@localhost  
  
ssh dion@localhost  
exit
```

10. Установите Docker и добавьте пользователя dion в группу docker.

11. Завершите сеанс пользователя dion и подключитесь заново для применения настроек.

12. Загрузите и распакуйте Ansible Playbook:

```
cd /home/dion  
  
wget --user=имя_пользователя --password=пароль  
https://registry.onprem.dion.vc/архив\_playbook.gz  
  
tar -xf on_dion-2024.01-архив_playbook.gz
```

13. Запустите скрипт конфигурации и ответьте на его вопросы:

```
cd /home/dion/on_dion  
  
./configurator.sh
```

14. Настройте DNS-записи (A-записи на DNS-сервере внутренней зоны:

```
cd /home/dion/on_dion/scripts/  
  
./dns_check_defis.sh dion.your_domain.com
```

15. Установите SSL-сертификаты в директорию certs в формате:

- chain.pem — корневой сертификат или цепочка сертификатов выпускающего центра;
- fullchain.pem — сертификат сервера, а также полная цепочка сертификатов выпускающего центра;
- privkey.pem — приватный ключ сертификата;
- cert.pem — только сертификат сервера, без цепочки.

Пример:

```
mkdir /home/dion/certs  
  
cd /home/dion/on_dion/files/dion.<YourDomain>.com/certs/  
  
cp /home/dion/certs/chain.pem web/rootCA.crt  
cp /home/dion/certs/chain.pem service/rootCA.crt  
  
cp /home/dion/certs/fullchain.pem web/server.crt  
cp /home/dion/certs/fullchain.pem service/server.crt  
cp /home/dion/certs/cert.pem          ad/sso.crt
```

```
cp /home/dion/certs/privkey.pem web/server.key
cp /home/dion/certs/privkey.pem service/server.key
cp /home/dion/certs/privkey.pem ad/sso.key

sed -n 'p' /home/dion/certs/fullchain.pem
/home/dion/certs/privkey.pem > web/haproxy.pem
```

16. Запустите установку компонентов командой:

```
cd /home/dion/on_dion

./dion.sh
```

17. Дождитесь окончания установки.

5.2 Дополнительные настройки

Для дополнительных настроек:

1. Получите доступ в Панель администрирования: для облачной и гибридной версии запросите его в поддержке DION; для версии on-prem разверните Панель администрирования.
2. Настройте организацию в Панели администрирования: добавьте почтовые домены, провайдеры аутентификации (SSO/Логин-пароль).
3. При необходимости выполните настройку интеграции: Active Directory, почтовые серверы, SIP-устройства, DLP-системы, Push-сервисы.
4. Настройте политики безопасности: правила доступа, парольные политики, ограничения на загрузку файлов.

5.3 Проверка работоспособности

Для проверки работоспособности программы используйте, например, команду:

```
helm status --namespace $K8S_NAMESPACE $HELM_RELEASE
```

где:

- `$K8S_NAMESPACE` – название пространства имен в Kubernetes, в котором выполнена установка;
- `$HELM_RELEASE` – название релиза в Kubernetes.

При положительном результате проверки вывод команды содержит:

```
STATUS: deployed
```

6 Установка Dion Rooms

6.1 Порядок установки

Для установки модуля Dion Rooms выполните действия:

1. Подготовьте и установите сервер DION Rooms (сервисы drcs и ews/caldav connector):

- a. На машине, где будут развернуты сервисы DRCS и ews/caldav connector, выполните команды:

```
sudo apt update
sudo apt upgrade
```

- b. Установите на машину docker и docker compose.
- c. Перенесите на машину содержимое архива с дистрибутивами для Сервера DION ROOMS.
- d. Перенесите на машину сертификаты и ключ, полученные от команды DION. Рекомендуется сложить их в отдельную папку, например /opt/dion-rooms/certs.
- e. Перенесите на машину сертификат, выпущенный на DNS-имя, по которому к серверу будут обращаться устройства в переговорной. Файлы с расширениями .crt и .key необходимо переименовать в **server.crt** и **server.key** соответственно. Файл server.crt должен включать полную цепочку – Root, Intermediate, Server. Рекомендуется сложить эти файлы в отдельную папку. В этой же папке создайте файл **server.pass** и добавьте в него пароль от ключа сертификата если таковой имеется. Если нет, то файл нужно оставить пустым.
- f. Убедитесь, что на машине присутствуют файлы в составе:
- docker-compose-ews.yml или docker-compose-cda.yml в зависимости от типа используемого дистрибутива - EWS или CalDav;
 - ews.env или cda.env в зависимости от типа используемого дистрибутива - EWS или CalDav;
 - install.sh;
 - папка tarballs;
 - сертификат dion в формате .crt;
 - ключ dion в формате .key;
 - сертификат из пункта 5 в формате .crt;
 - ключ сертификата из пункта 5 в формате .key.

```
ls -aslh< путь до папки, куда распаковали архив, либо перенесли файлы>
```

- g. Перейдите в эту папку:

```
cd< путь до папки, куда распаковали архив, либо перенесли файлы>
```

- h. Запустите скрипт-установщик от имени суперпользователя и дождитесь сообщения об успешном выполнении:

```
sudo ./install.sh
```

2. Отредактируйте конфигурационные файлы:

Для редактирования конфигурационных файлов и перезапуска сервисов вам потребуются root-права:

- a. Откройте на редактирование конфигурационный файл .env. Можно использовать любой удобный текстовый редактор, например nano.

- b. Заполните конфигурационный файл в соответствии с подсказками в самом файле и ниже. Вносите изменения только в те переменные, которые указаны в инструкции.

Если сервер уже запущен, и вы хотите внести изменения в значения переменных, нужно полностью перезапускать сервер командами `docker compose down` и `docker compose up -d` (или `docker-compose down` и `docker-compose up -d`, соответственно). Только так новые значения будут применены.

Общие для всех установок переменные:

- Укажите путь до директории, в которой находится сертификат, выданный командой DION:
`GRPC_DIR=`
- Укажите имя файла сертификата `.crt`, выданного командой DION:
`DION_GRPC_SERVICE_CERTIFICATE_CHAIN=`
- Укажите имя файла ключа `.key`, выданного командой DION:
`DION_GRPC_SERVICE_PRIVATE_KEY=`
- Введите произвольный код-пароль, который будет использоваться для авторизации устройств в вашей системе DION ROOMS:
`SECURITY_TOKEN=`
- Впишите путь до папки, в которой содержится сертификат для сервера:
`CERTS_PATH=`
- Установите часовой пояс:
`TZ=`
- Идентификатор сервера для сбора метрик:
`METRICS_EXPORTER_CONNECTOR_ID=`
- Почта, на которую зарегистрирована УЗ DION для доступа в DION API:
`DION_API_EMAIL=`
- Пароль от УЗ DION для доступа в DION API:
`DION_API_PASSWORD=`

Переменные, зависящие от типа дистрибутива:

EWS

- ASMX URL вашего сервера Exchange. Впишите DNS-имя вашего сервера Exchange вместо `x-x-x` в формате: `https://x-x-x/EWS/Exchange.asmx`:
`EXCHANGE_URL=`
Ваш почтовый домен без собаки и без слеша:
`EXCHANGE_DOMAIN=`
- Имя пользователя служебной учетной записи Exchange, созданной на этапе подготовки. Необходимо указать без собаки и почтового домена:
`EXCHANGE_USERNAME=`
- Пароль от служебной учетной записи Exchange:
`EXCHANGE_PASSWORD=`

CalDav

- URL, по которому доступен протокол CalDav вашего почтового сервера:
CDA_URL=
- Ваш почтовый домен:
CDA_DOMAIN=
- Имя пользователя почтовой служебной учётной записи:
CDA_USERNAME=
- Пароль почтовой служебной учётной записи:
CDA_PASSWORD=

6.2 Дополнительные настройки

Для дополнительных настроек:

1. Выполните настройку дополнительных компонентов для мониторинга работы системы. Настройте подключение к внешнему сервису, через который будут отправляться оповещения о состоянии устройств, например: корпоративная почта.
2. Настройте устройства, подключенные к переговорным комнатам, в Панели администрирования. Выполните настройку переговорных комнат.
3. Выполните настройку устройств:
 - a. Настройте планшет Панель Управления.
 - b. Установите дополнительное ПО: Android SDK Platform, ПО Controller на планшет Панель Управления, ПО Scheduler (TSA) на планшет Панель Бронирования.
 - c. Установите APK на планшеты Панель управления и Панель Бронирования:

```
.\adb install -t "путь к apk файлу"
```

```
.\adb shell dpm set-device-owner com.inno.tech.dion.roomsTSA/.MyAdmin
```
4. При необходимости выполните настройку киоска и настройку главного экрана приложения.

6.3 Проверка работоспособности

Для проверки работоспособности Dion Rooms:

1. Запустите сервисы:

```
docker compose up -d
```

или

```
docker-compose up -d
```

2. Удостоверьтесь что сервисы запустились корректно:

```
docker ps
```

Должно быть запущено 3 контейнера: их имена (колонок NAMES) должны содержать слова проху, rooms-service, ews-connector (caldav-connector вместо ews-connector для CalDavy-становок). У всех контейнеров из перечисленных должен быть статус Up.

7 Эксплуатационные характеристики

7.1 Производительность

Показатели производительности программы:

- Поддержка до 10 000 активных участников в конференциях;
- Пропускная способность от 500 Kbit/s до 3 Mbit/s на пользователя;
- Одна активная запись конференции утилизирует 2 ядра процессора.

7.2 Доступность и надежность

Текущий класс критичности системы – Business Critical.

Система доступна в режиме 24/7; показатель доступности – не менее 99,9%.

Показатели RTO и RPO – согласно уровню критичности Mission Critical.

Отказоустойчивость обеспечивается за счет технологий: Patroni (PostgreSQL), Redis/Valkey Sentinel, репликация данных в Kafka, ClickHouse, S3. Для архитектуры All-In-One отказоустойчивость не предусмотрена.

7.3 Ролевая модель

Для контроля доступа к операциям в программе и управления правами на проведение конференций реализована ролевая модель. Пользователям предоставляются полномочия, минимально необходимые для выполнения их обязанностей, включая разделение прав между администраторами системы, организаторами встреч и участниками.

Функциональность компонентов, включая управление оборудованием Переговорных комнат (Dion Rooms) и доступ к записям встреч, доступна только после успешной авторизации через SSO (Keycloak/ADFS) в соответствии с назначенной ролью.

7.4 Мониторинг

Метрики мониторинга предоставляются в формате Prometheus text-based exposition format v0.0.4 по модели Pull.

Предоставление системных метрик осуществляет node_exporter, также предоставляются метрики работы docker с помощью cadvisor. Для этих метрик поставляются готовые витрины Grafana.

7.5 Логирование

Система логирования включена в поставку. Построена на базе свободно-распространяемого ПО OpenSearch.

Backend приложения осуществляют логирование локально в файлы, затем сборщиками выполняется доставка журналов из локальных файлов в централизованное хранилище.

Данные аудита (действия пользователей, события безопасности) хранятся в отдельном хранилище и защищены от модификации для всех пользователей. Доступ к данным аудита предоставляется через Панель администрирования для пользователей со следующими ролями:

- «Аудитор»;
- «Администратор организации»;
- «Администратор DION»;
- «Специалист поддержки организации»;

- «Специалист поддержки DION».

Для каждого регистрируемого события информационной безопасности аудита могут быть указаны:

- тип события;
- идентификационные данные пользователя, инициировавшего регистрируемое событие (учетная запись пользователя, ФИО);
- данные об успешности выполнения действия;
- дата и время события;
- IP-адрес;
- предыдущее и текущие значения полей, содержащие изменение сущности;
- другие данные, достаточные для однозначной интерпретации события.