GS LABS
GS GROUP

Публичный - L0

Программный комплекс «Система условного доступа DREGUARD»

Руководство по установке

Индекс	CAS-DREGUARD-IG
Конфиденциальность	Публичный - L0
Ревизия	1.0
Статус	Согласован

Содержание

1. Аннотация

Данный документ содержит руководство по установке и первоначальной настройке Программного комплекса "Система условного доступа DREGUARD" (далее - CAS DREGUARD или Система), а также описание системных требований для компонентов.

Документ предназначен для сотрудников отдела мониторинга и инсталляции, а также для других технических специалистов, в обязанности которых входит установка и первоначальная настройка CAS DREGUARD.

Данное описание является публичным документом.

2. Термины и сокращения

Термин	Сокращение	Определение
Абонент	-	Физическое или юридическое лицо, с которым оператор ТВ заключает договор на оказание услуг.
Авторизация	-	Процесс предоставления абоненту прав на использование услуг телевизионного оператора (просмотр телевизионных каналов и услуги интерактивных телевизионных сервисов).
Антишаринг	-	Подход, используемый в разработке технологий по противодействию нелегальному доступу к каналам, закрытым CAS DREGUARD, при котором распространяются ключи (CW), полученные от одной авторизованной смарт-карты.
Биллинговая система (Business Support System)	BSS	Сторонний по отношению к CAS DREGUARD компонент, отвечающий за сбор информации об использовании услуг, выставление счетов абонентам, обработку платежей. На основании этой информации биллинговая система выдает CAS DREGUARD команды на добавление, удаление или изменение подписок, сообщений Инфокас, или иных данных, хранящихся в CAS DREGUARD.
Головное оборудование	-	Оборудование головной станции оператора. В данном документе под головным оборудованием подразумевается та его часть, которая непосредственно взаимодействует с Системой Условного Доступа согласно стандарту DVB-SimulCrypt.
Класс	-	Единица доступа в CAS DREGUARD. С точки зрения пользователя CAS DREGUARD (оператора ТВ), класс определяет пакет телевизионных каналов, предоставляемых абоненту в качестве единой услуги. На базе управления правами на класс реализовано управление доступом абонента к пакету каналов. При оформлении подписки на класс, абоненту предоставляется доступ ко всем телевизионным каналам, входящим в его состав.
Контрольное слово (Control word)	CW	Ключи, используемые для скремблирования/дескремблирования транспортного потока алгоритмом CSA.

ПАК "Криптокипер" (Криптокипер, Cryptokeeper)	СК	Специализированное шифрующее устройство.
Криптопериод		Период времени, в течение которого скремблером используется один и тот же ключ скремблирования (CW).
Мастер-ключ	MK	Ключ, необходимый для декодирования операционных ключей, получаемых из EMM сообщений. Мастер-ключ относится к самому верхнему уровню иерархии ключей и хранится в самой защищённой области энергонезависимой памяти смарт-карты. Этот ключ получается легальным пользователем вместе со смарт-картой и никогда не меняется.
Оператор ТВ (TV Provider)	-	Организация, предоставляющая услуги просмотра цифрового телевидения и использования дополнительных сервисов.
Операционный ключ	OPKEY	Ключ, используемый для шифрования и расшифровывания управляющих слов (CW). Операционные ключи передаются в зашифрованном виде в составе специальных команд в EMM сообщениях.
Пакет услуг	-	Данный термин используется в рамках функционала WHN. Совокупность прав на использование услуг оператора ТВ, предоставляемая абоненту при заключении договора. Подписка на пакет услуг определяет доступные для абонента типы услуг (Streaming, PVR и прочее), классы подключаемых устройств (например, планшеты GS), максимальное количество одновременно подключаемых устройств. Пакет услуг может иметь привязку к одному или нескольким каналам.
Подписка	-	Информация о правах доступа абонента к классам и услугам оператора ТВ (идентификатор класса, идентификатор пакета услуг и период, на который они предоставлены).
Приёмник (Set Top Box)	STB	Устройство абонента, принимающее и обрабатывающее сигнал цифрового телевидения и передающее его далее для воспроизведения (например, на телевизоре или планшете).
Оператор ТВ	-	Организация, предоставляющая услуги просмотра цифрового телевидения и использования дополнительных сервисов.

Система управления подписками (Subscriber Management System)	SMS	Система, принимающая, обрабатывающая и хранящая информацию о подписках абонентов.
Скремблер	SCR	Устройство шифрования транспортного потока, входящее в состав головного оборудования. В терминологии стандарта DVB-Simulcrypt обозначает функциональный логический блок, ответственный за шифрование MPEG2 транспортного потока. Для выполнения данной функции должен обеспечивать прием CW от компонента SCS.
Смарт-карта	-	Версия внешней смарт-карты, реализованная на аппаратной платформе. Используется в CAS DREGUARD для идентификации пользователей, безопасного хранения приватных данных и защиты криптографических операций, необходимых для управления доступом.
Стриминг (Streaming)	-	Функция приёмника, позволяющая передавать контент с приёмника-сервера на устройство-клиент (приёмник, планшет). Различают следующие виды Streaming: • Mirror Streaming: на мобильное устройство транслируется контент, воспроизводимый на сервере; • Independent Streaming: на мобильное устройство транслируется контент по запросу клиента, независимо от контента, воспроизводимого на сервере.
Услуга	-	Дополнительная платная функциональность приёмного оборудования, доступ к которой ограничивается оператором цифрового телевидения в соответствии с разработанными им правилами использования данной функциональности (например, использование Streaming и т.д.).
Access criteria (Критерий доступа)	AC	Данные системы условного доступа, необходимые ECMG для формирования ECM сообщений. Состав и структура этих данных определяется разработчиком CAS DREGUARD и является закрытой информацией

Conditional access system (Система условного доступа)	CAS	Система условного доступа обеспечивает защиту контента, передаваемого по каналам вещания и распределения, от коммерческого пиратства.
CAS DREGUARD Library (далее по тексту - Library)	-	Система, представляющая собой промежуточное ПО, которое обеспечивает взаимодействие ПО приемника и эмулятора смарт-карты. Library управляет выделением служебных данных (например, ECM и EMM) из принятого транспортного потока, получением из них зашифрованных ключей и их передачу эмулятору смарт-карты для расшифровки.
DRE Account Manager (далее по тексту - Account Manager)	ACM	Сервис авторизации и распределения прав. CAS DREGUARD может обратиться к Account Manager (через свой фронтенд или API) для авторизации, передачи и проверки прав пользователя. Затем, при помощи WEB UI, пользователь CAS DREGUARD может создавать дополнительные учетные записи, назначать роли и создавать группы прав.
DRE Advanced Encryption Service	-	Программа, обеспечивает возможность дополнительной защиты контента при вещании в спутниковой и IP сетях.
DRE Config Manager (далее по тексту - ConfigManager)	CM	Сервис для хранения списка операторов и их конфигурационных данных. Сервис получает, агрегирует и выдает перечень операторов, которые используют DREAMPlatform, а также набор конфигурационных данных для каждого оператора. Таким образом, абонент, пользуясь одним клиентским приложением, может получать доступ к нескольким операторам.
DRE Messaging Service (далее по тексту - Hermes)	-	Система, реализующая функционал отправки уведомлений на оборудование абонентов.
DVB-Simulcrypt	-	DVB-стандарт архитектуры, позволяющей функционировать множеству Систем Условного Доступа в рамках единой головной станции. Этот стандарт определяет архитектуру головного оборудования и СУД, временные параметры взаимодействия компонентов, их интерфейсы и формат сообщений.

Electronic Program Guide, (электронный программный гид)	EPG	Продукт "Электронный телегид DREGUIDE".
Encoded Channel DRE	ECD	Дополнительная функция CAS DREGUARD, предназначенная для информирования абонента о причине ограничения доступа к телепередаче. Информирование производится через сообщения "Кодированный канал", которые содержат код статуса дескремблирования и краткую инструкцию по устранению проблемы.
Enhanced Common Scrambling Algorithm	ECSA	Технология аппаратного антишаринга, построенная на дополнительном шифровании CW до его шифрования алгоритмом смарт-карты. Требует аппаратной поддержки в процессоре STB, в который встраивается библиотека (CAS DREGUARD Library).
Entitlement Control Message	ECM	Сообщение CAS DREGUARD, содержащее в зашифрованном виде CW, дескремблирующие транслируемый поток.
Entitlement Management Message	EMM	Сообщение CAS DREGUARD, содержащее служебные данные, информацию о правах доступа и специальные команды (изменение подписки, обновление операционного ключа и другие).
InfoCAS	-	Дополнительная функция CAS DREGUARD, позволяющая оператору ТВ рассылать текстовые сообщения абонентам. Функция реализуется системой CAS DREGUARD или системой Сервисов. Сообщения принудительно отображаются на экране ТВ поверх основного изображения. Примеры использования сообщений - предупреждения об обновлении ПО, окончании подписки, оповещения населения и другие.
Lite mode	-	Режим работы ECMG. В данном режиме CW передаются в ECM в незашифрованном виде.
L-режим	-	Режим ограниченного просмотра, предназначенный для мотивации абонента продлить подписку. В данном режиме картинка телеканала пропорционально уменьшается, а в остальной области экрана выводится реклама.

MUX Injector Server	MIS	Продукт, который обеспечивает вставку данных в MUX с определенным битрейтом. Используется для вставки в транспортный поток данных, получаемых из разных источников.
Pairing	-	Режим CAS DREGUARD, обеспечивающий работу смарт-карты только с одним конкретным приёмником.
Scrambling Control Group	SCG	Логическое объединение каналов, скремблируемых едиными CW, создаваемое на головном оборудовании Оператора ТВ.
Simulcrypt синхронизатор	SCS	Компонент головного оборудования, предназначенный для установления и поддержания соединения с ECMG, передачи ему CW и AC, получения сгенерированных ECM сообщений и перенаправление их в MUX.
Мультиплексор (Multiplexer)	MUX	Компонент головного оборудования, предназначенный для преобразования получаемой информации в TS с последующей передачей на спутник.
Common Scrambling Algorithm	CSA	Общий алгоритм скремблирования, используемый для защиты цифрового телевизионного потока от несанкционированного доступа
Transport Stream	TS	Формат медиаконтейнера, который инкапсулирует пакеты элементарных потоков и других данных.
TS Monitor	TSM	Набор программных средств, предназначенных для мониторинга транспортного потока.
Subscriber Management System	SMS	Компонент который позволяет управлять подписками/услугами /устройствами/каналами и т.д. Обеспечивает интеграцию с биллинг системами операторов.

3. Введение

3.1. Требования к квалификации установщика

Для установки системы сотрудник обязан:

- иметь базовые представления и практические навыки работы с системой оркестрации Kubernetes (https://kubernetes.io/docs/tutorials/kubernetes-basics/) и пакетным менеджером Helm.
- иметь навыки работы с ОС семейства Linux, а именно:
  - установка пакетов;
  - создание и настройка сетевых подключений;
  - запуск служб, настройка автозапуска служб;
  - установка и настройка PostgreSQL;
  - создание и работа с БД под управлением PostgreSQL.
- иметь знания о DNS.
- иметь базовые представления и практические навыки работы с Git.

3.2. Системные Требования

Для установки CAS DREGUARD желательно выделить отдельный сервер. Рекомендуется устанавливать сервер в локальной сети, защищенной от доступа извне.

3.2.1. Аппаратное Обеспечение

- Процессор — 4 ядра;
- Оперативная память — зависит от размера базы абонентов, с которой будет работать CAS DREGUARD. Минимум 8 GB;
- Жесткий диск — 2 × 150 GB (зависит от объема БД);
- Головное оборудование, соответствующее стандарту DVB-Simulcrypt ver. 2.

3.2.2. Программное Обеспечение

- Компоненты CAS DREGUARD поставляются в контейнерах, поэтому основное требование к ОС сервера - возможность установить Docker.
- Предполагается, что базы данных (OPKEY DB, CAS DB, Carousel DB и т.д.) будут развернуты на *nix системе.

3.2.3. Системные требования для развертывания компонентов Системы

Компоненты Системы разворачиваются в кластере Kubernetes. Для данных компонентов должна быть развернута одна нода кластера.

Для установки необходимо предварительно выполнить следующие требования:

- На отдельном сервере подготовлена Ansible node с поддержкой CI/CD. За информацией обращаться к разработчику платформы автоматизации CI/CD ООО "Цифра".
- Установлен и настроен кластер Kubernetes через K3s.
    - Так как развертывание производится в кластере k8s, то необходим config file для доступа к кластеру.
        1. Если пользователь выполнял развертывание Kubernetes самостоятельно, то он сам должен создать config file (см. документацию Kubernetes).
        2. Если Kubernetes был развернут сторонними людьми, то необходимо получить config file у администратора кластера.
- На машине администратора установлен kubectl (https://kubernetes.io/docs/tasks/tools/install-kubectl/).
- На машине администратора установлен helm.
- Развернут DNS-сервер, преобразование имен dns зоны настроено на мастера k8s (созданы A записи на зону dns). DNS устанавливается в сетевое окружение DMZ зоны, где будет развернут CAS DREGUARD.
- Для корректной работы системы CAS DREGUARD требуется развернуть кластер БД (ссылка и права доступа к инструкции по развертыванию кластера БД предоставляются по запросу заказчика)
- Для корректной работы системы CAS DREGUARD необходим доступ к следующим ресурсам:
    - chartmuseum (ссылка и права доступа предоставляются по запросу заказчика)
- Необходим доступ к репозиторию, содержащему helmfile для развертывания CAS DREGUARD. Helm файл содержит инструкции, с помощью которых осуществляются настройки устанавливаемых компонентов. Сами компоненты поставляются в виде образов (images), из которых разворачиваются Docker-контейнеры.

4. Состав компонентов для установки системы

4.1. Компоненты CAS DREGUARD

Развертывание компонентов CAS DREGUARD осуществляется из репозитория gitlab (с помощью CI/CD). Необходимые сборки, если не указано иное, лежат в gitlab.

Доступ к репозиторию, содержащему helmfile для развертывания CAS DREGUARD, предосталяется по запросу.

4.2. CAS scripts

Скрипты по работе с базами данных (в т.ч. базы CAROUSEL DB, входящей в состав MIS).

Поставляются в виде архива ***cas_scripts_X.X.X.zip***

5. Установка компонентов CAS DREGUARD

Установка MIS осуществляется совместно с CAS DREGUARD и выполняется следующим образом:

1. Настроить компоненты MIS в репозитории CAS DREGUARD, в файле production.yaml.
2. Указать/обновить тэг репозитория MIS в репозитории CAS DREGUARD.
3. Настроить и развернуть CAS DREGUARD из репозитория gitlab (с помощью CI/CD).
    a. При развертывании CAS DREGUARD будет автоматически подтянут и поднят MIS.

5.1. Процедура установки

Необходимо выполнить установку системы в соответствии с документом "Описание схемы CD", тэг 4.0 (ссылка и права доступа предоставляются по запросу заказчика).

5.2. Как создать новую среду

1. Создать отдельный проект в Gitlab
2. Настроить проект certification/rcas как подмодуль на основе инструкции (ссылка и права доступа предоставляются по запросу заказчика)
3. В проекте среды создать helmfile.yaml с содержимым:

```
---
helmfiles:
  - path: <путь до подмодуля>/helmfile.yaml
    values:
      - <путь до подмодуля>/default.yaml # Загружаем зачения по-умолчанию
      - production.yaml                  # Применяем собственную конфигурацию
      - versions.yaml                    # (опционально) Переопределяем версии некоторых компонентов
```

5.3. Пример .gitlab-ci.yml

```yaml
# здесь перечисляются необходимые шаги(stage) пайплайна
# в случае, если часть вышеописанного функционала
# не требуется, ненужные шаги можно удалить
# (например, оставить только init)
stages:
  - init
  - compose
  - grade

variables:
  # GIT_* переменные необходимы для правильной работы
  # репозитория с сабмодулем
  GIT_SUBMODULE_STRATEGY: recursive
  GIT_STRATEGY: clone
  # если namespace релиза не задаётся через values/шаблоны/helmfile,
  # то его можно задать через переменную NAMESPACE
  NAMESPACE: rcas-stand
  STAGED_PIPELINE: "true"

include:
  - project: 'automation/cd-templates'
    ref: "4.0"
    file: pipeline.yml
```

5.4. Настройка и развертывание CAS DREGUARD

5.4.1. CD для артефактов БД

При развертывании CAS DREGUARD происходит установка SCH и API для БД через механизм Kubernetes Jobs. В процессе установки сохраняется лог в контейнере.

```
sms_db_sch:
  enabled: true
  # You can optionally override database address and port here:
  #db:
  #  address: 127.0.0.1
  #  port: 5432

sms_db_api:
  enabled: true
```

Этот режим поддерживают все базы данных системы CAS DREGUARD.

5.4.2. Настройка переменных окружения

В системе развертывания CAS DREGUARD требуется указывать переменные окружения, которые используются непосредственно в самом процессе деплоя CAS DREGUARD в кластер.

Настройка переменных осуществляется в gitlab.

В боковом меню выбрать **Settings** (на панели слева) -> **CI/CD** -> **Environment variables**. Отредактировать переменные.

Список используемых переменных Gitlab предоставляется по запросу заказчика.

> **ВАЖНО!** Environment variables имеют более высокий приоритет, чем переменные, заданные в файлах.

5.4.3. Настройка additional

Папка ***additional*** содержит файлы, с помощью которых настраиваются dns, ingress, probes, statsd. Указанные параметры применяются ко всем сервисам и службам в данном репозитории. **Рекомендуется не менять эти настройки**.

5.4.4. Состав репозитория

Репозиторий имеет следующий состав:

- helmfile.yaml - главный конфигурационный файл утилиты helmfile.
- default.yaml - файл с values окружения утилиты helmfile.
- values - папка с values для каждого чарта; они являются шаблонными и забирают значения из values окружения (файла default.yaml).
- versions.yaml - файл с версиями компонентов; если в версии установлена пустая строка, то берется последняя версия (в соответствии с semver2).
- limitation - папка с values ресурсов подов. С помощью этих файлов настраиваются компоненты CAS DREGUARD, в том числе многочисленные базы данных.

5.4.5. Выбор компонентов CAS DREGUARD для установки

По умолчанию разворачиваются все компоненты CAS DREGUARD, однако при необходимости можно отключать ненужные: для этого в production.yaml, в корне секции соответствующего компонента нужно выставить *enabled: false*.

5.4.6. Динамические параметры в конфигурационных файлах

В конфигурационных файлах *_server.cfg параметры разделены на две группы:

1. Все параметры, лежащие вне секции "system". Эти параметры можно менять динамически, т.е. без перезапуска соответствующей службы. При изменении значений этих параметров в конфигурационном файле, по прошествии некоторого времени, новые значения будут автоматически применены к службе.

   > ⚠ **Обратите внимание!** Параметры, изменяемые динамически, нельзя задать через переменные окружения (см. выше), они меняются только в конфигурационном файле.

2. Параметры в секции "system". Эти параметры нельзя изменить динамически: чтобы изменения этих параметров вступили в силу, соответствующая служба должна быть перезапущена.

Некоторые из динамически изменяемых параметров (например, xxx.host в *.cfg) нельзя применять со значениями "по умолчанию", они должны быть настроены на production.

5.5. Развертывание системы (основные этапы)

Этапы развёртывания:

1. Подготовка данных в git (см. гл. "Установка компонентов CAS DREGUARD"):
   a. Изучить документ "Описание схемы CD" (ссылка и права доступа предоставляются по запросу заказчика). Выполнить описанные процедуры.
   b. Настроить двухступенчатый деплой.
   c. Настроить environment variables (см. "Настройка переменных окружения").
   d. Настроить yml-файлы, которые определяют состав и настройки разворачиваемых сервисов и баз данных, см. "Настройка additional", "Состав репозитория".
   e. В конфигурационных файлах настроить параметры, которые нельзя оставлять "по умолчанию" и /или нельзя изменить динамически, см. "Динамические параметры в конфигурационных файлах ".
2. Установка баз данных, входящих в состав Системы, в git (с помощью CI/CD). См. "Установка Баз Данных ".

   > ⚠ Развертывание CAS DREGUARD происходит в два этапа: сначала производится установка баз данных, затем (после их наполнения) - сервисов CAS DREGUARD.
   >
   > Этапы (stages) настраиваются в gitlab-ci.yaml.

   a. Перед установкой требуется создать и соответствующим образом настроить production.yaml (см. CD для артефактов БД).
3. Наполнение баз данных (с помощью скриптов). См. "Установка Баз Данных".
4. Установка служб/сервисов, входящих в состав Системы, в git (с помощью CI/CD).

a. Перед установкой требуется создать и соответствующим образом настроить production.yaml.
b. Делается несколько инстансов CAS DREGUARD:
    i. один - для sms_postgres
    ii. по одному инстансу CAS DREGUARD - для каждого провайдера (provider_id)

5. **(Обязательно) удалить jobs**, созданные при развертывании баз данных, иначе в дальнейшем нельзя будет накатить новые DB_API и DB_SCH.

> ⚠ **ВНИМАНИЕ!** При установке в production базы (XXX DB) её старые схемы XXX_DB_API, соответствующие более ранним релизам, автоматически не удаляются. Т.е. старые схемы XXX_DB_API нужно удалять вручную.

5.6. Редактирование production.yaml (для сервисов CAS DREGUARD)

Файл production.yaml создается на основе default.yaml (ссылка предоставляется по запросу заказчика), содержащего основные настройки Системы. Настройки, заданные в default.yaml, кроме (опционально) параметров подключения, являются достаточными для эксплуатации Системы.

Особенности:

- Значения параметров, заданные в production.yaml, имеют более высокий приоритет, чем значения, заданные в default.yaml.
- Если параметр не задан в production.yaml, то будет использовано значение, заданное в default.yaml.
- Если параметр не задан ни в production.yaml, ни в default.yaml, то будет использовано значение, заданное в конфигурационном файле данного компонента.

6. Предварительные действия

6.1. Установка ОС

1. Установите на сервере желаемую ОС. Следуйте стандартный инструкциям по настройке данной ОС. Предполагается, что сервер будет функционировать под управлением ОС *nix.
2. Установите Docker на данной ОС.

6.2. Настройка локализации

Проверьте, что у вас активна локаль **ru_RU.UTF-8**. Например, в Debian это можно сделать так:

1. Выполните команду:

```
sudo dpkg-reconfigure -plow locales
```

2. Убедитесь, что в списке локализаций отмечена **ru_RU.UTF-8**. Если это не так, выберите её в добавок к уже имеющимся и нажмите *Ok*.
3. Проверьте, что вывод имеет вид:

```
Generating locales (this might take a while)...
   en_US.UTF-8... done
   ru_RU.UTF-8... done
Generation complete.
```

6.3. Установка PostgreSQL

По умолчанию требуется развернуть кластер БД (ссылка и права доступа к инструкции по развертыванию кластера БД предоставляются по запросу заказчика)

Данный раздел следует использовать только в случае установки БД в режиме Standalone.

Для работы системы CAS DREGUARD требуется PostgreSQL версии 14 или выше.

Установки PostgreSQL на сервер (без развертывания и настройки кластера БД) выполняется стандартным образом.

6.4. Настройка PostgreSQL

По умолчанию требуется развернуть кластер БД (ссылка и права доступа к инструкции по развертыванию кластера БД предоставляются по запросу заказчика).

Настройку PostgreSQL следует использовать только в случае установки БД в режиме Standalone.

Настройка осуществляется стандартным образом (редактируются файлы ***postgresql.conf*** и ***pg_hba.conf***, после внесения изменений перезапускается PostgreSQL).

6.5. Установка необходимых библиотек (для PostgreSQL)

Перед запуском скриптов для создания SMS_CAS_DB необходимо выполнить следующее:

1. Установить citus и pg_cron.
   Пример (для postgresql версии 14):

   ```
   sudo apt-get -y install postgresql-14-citus postgresql-14-cron
   ```

2. Открыть файл ***postgresql.conf*** для редактирования. Файл находится здесь:

   ```
   /etc/postgresql/14/main/postgresql.conf
   ```

3. Добавить установленные библиотеки в файл:

   ```
   shared_preload_libraries = 'citus, pg_cron' # (change requires restart)
   ```

4. Добавить в файл название БД для pg_cron:

   ```
   cron.database_name = 'smscas'
   ```

5. Убедиться, что в ***postgresql.conf*** следующее значение параметра *timezone*:

   ```
   timezone = 'UTC'
   ```

6. Перезапустить PostgreSQL:

   ```
   sudo /etc/init.d/postgresql restart
   ```

7. Установка Баз Данных

⚠ **ВНИМАНИЕ!** При развёртывании / обновлении схем баз данных CAS DREGUARD для них автоматически устанавливается 'UTC' timezone, вне зависимости от настройки PostgreSQL.

По умолчанию, БД будут созданы в табличном пространстве *pg_default* (табличное пространство по умолчанию для PostgreSQL).

7.1. Подготовка к установке

Порядок действий:

1. Распаковать архив ***cas_scripts_X.X.X.zip*** , входящий в комплект поставки, в желаемую папку на разделе диска (например, */home*).
2. Предоставить пользователям права на чтение, изменение и запуск содержимого папки, созданной на предыдущем шаге:

```
sudo chmod -R +x /home/cas_scripts
```

3. Сменить владельца данной папки на *postgres*:

```
sudo chown -R postgres /home/cas_scripts
```

7.2. Установка БД

Развертывание всех баз данных, входящий в состав системы CAS DREGUARD, осуществляется из репозитория gitlab (с помощью CI/CD). См. Установка компонентов CAS DREGUARD.

⚠ **Обратите внимание!** При установке и развертывании баз данных с помощью CI/CD **названия баз данных не должны содержать "-" и "_" (дефисы и нижние подчеркивания)**. Поэтому здесь и далее соблюдайте это ограничение для всех разворачиваемых баз данных.

7.3. Наполнение CAS_DB

Получите данные, необходимые для наполнения CAS_DB и других баз, от поставщика ключей (Key Owner). Загрузите эти данные в базы CAS DREGUARD.

Описание этой процедуры выходит за рамки данного документа и приведено в отдельном документе (доступ строго ограничен).

7.4. Наполнение Schedule DB

Компонент schedule_db_init отвечает за начальное наполнение расписания задач в SCHEDULE DB.

В параметрах компонента есть стандартный *enabled: false/true* (по умолчанию false) и *cas_versions*, обозначающий версию команд, для которой нужно загрузить начальное наполнение.

7.5. Наполнение остальных БД

При установке в БД заносится начальное наполнение, с которым можно проводить тестовые запуски системы.

Однако при развёртывании боевой системы наполнение данной БД необходимо менять в соответствии с нуждами заказчика.

Общие принципы настройки БД описаны в соответствующем разделе документа "Руководстве администратора" (предоставляется по запросу заказчика).

7.6. Настройка взаимодействия CAS DREGUARD и DRE Account Manager

Для корректного взаимодействия систем CAS DREGUARD и DRE Account Manager (далее - ACM) должны быть настроены и использоваться permissions по работе с разными разделами web-интерфейса CAS DREGUARD.

Процедура выполняется в следующих случаях:

- при установке системы CAS DREGUARD "с нуля";
- в случае обновления/добавления/удаления прав (permissions).

Данную процедуру можно выполнять только после установки обновленной SMS DB (одна из обновленных баз данных CAS DREGUARD).

Последовательность действий:

1. В ACM добавить сервис "rcassms".

   ⚠ См. Руководство пользователя DRE Account Manager.

2. В ACM добавить сервис "dre_platformui".
3. Обновить конфигурационные файлы репозитория CAS DREGUARD:

a. В production.yaml, в секции **account_manager**, необходимо проверить, что параметр service_name равен "rcassms".
b. Проверить, что в production.yaml, в секции **routing_server**, включен и имеются блок *configEnabled: true* и *config*.
c. В production.yaml, в секции **routing_init**, выставить параметр *enabled: true*.

4. Выполнить деплой CAS DREGUARD.
5. В ACM добавить в роль "MDS" (или любую другую роль для пользователей CAS DREGUARD) права из сервисов "rcassms" и "dre_platformui".
6. Если web-интерфейс CAS DREGUARD уже запущен, то сбросить кеш страницы (в браузере) и выполнить переавторизацию в CAS DREGUARD web.

7.7. Интеграция CAS DREGUARD с DRE Config Manager

⚠ Для оператора с кодом решения aptb-dvb должны быть добавлены параметры согласно реестру DRE Config Manager.

Особенности интеграции CAS DREGUARD с DRE Config Manager (далее по тексту - CM):

1. При необходимости интеграции в production.yaml, в секции *config_manager*, задается параметр *enabled: true*, если взаимодействие с CM не требуется - *enabled:false*.
2. При включении интеграции с CM необходимо, чтобы в CM был задан полный набор необходимых параметров. Если каких-то параметров будет недоставать, то сервис (rcas_ecmg/rcas_emmg) не запустится и будет выведена соответствующая ошибка. Список параметров приведен в документе "Техническое описание", раздел "Список шаблонов параметров конфигурации для подключения к головному оборудованию" (доступ к документу предоставляется по запросу).
3. Название параметров muxs_bitrate и muxs_settings, получаемых от CM, привязаны к версии команд и списку провайдеров и имеют вид – muxs_bitrate_v[версия команд]*prov*[провайдер1_..._провайдерN] Таким образом, при включении интеграции с CM, требуется:
   a. Обязательно выставить в конфигурации rcas_emmg список провайдеров, используемых на стенде, чтобы подтянулся нужный параметр с CM.
   b. Если требуемого шаблона нет в CM, под необходимую конфигурацию провайдеров, то требуется создать её вручную.