Общество с ограниченной ответственностью «СКАД тех Цифровые Решения»

Программное обеспечение

«МАТЕРИК»

РУКОВОДСТВО АДМИНИСТРАТОРА

Установка, настройка и эксплуатация

Версия ПО 2.1

МАТЕРИК-РА-2.1

г. Тольятти

Содержание

1 Общие сведения 3
1.1 Состав дистрибутива 3
1.2 Роли и ответственность 3
2 Требования 3
2.1 Аппаратные требования 4
3 Установка 5
3.1 Порядок установки 5
3.2 База данных 6
3.3 Keycloak 6
3.4 PostgREST 6
3.5 Веб-клиент и nginx 7
3.6 Установка варианта с репликой 7
4 Подключение компонентов расширенного профиля 7
5 Проверка после установки 8
6 Эксплуатация 8
6.1 Резервное копирование и восстановление 8
6.2 Обновление 8
6.3 Журналы и мониторинг 9
6.4 Типовые неисправности 9
7 Лицензия 9
8 Вывод из эксплуатации 9

1 Общие сведения

Документ содержит сведения, необходимые для установки, настройки и эксплуатации ПО «МАТЕРИК» версии 2.1. Установку выполняет администратор, владеющий администрированием Linux, PostgreSQL и веб-сервера nginx.

1.1 Состав дистрибутива

Таблица 1 — Состав дистрибутива

Каталог или файл	Содержание
source/materik-web	Исходные тексты веб-клиента, package-lock.json, собранные файлы в dist
db/001_materik_core.sql	Модель данных: схема materik_core, роли, таблицы, функции, триггеры, политики RLS, права
db/002_materik_seed.sql	Начальные настройки (можно применять повторно)
db/003_materik_api.sql	Функции проверки доступа для nginx (auth_check, auth_check_admin)
db/004_materik_timeseries_pg.sql	Хранение временных рядов и технических журналов в PostgreSQL (базовая редакция)
db/clickhouse	Схема временных рядов и учётная запись чтения ClickHouse
config/materik-realm.json	Область Keycloak: роли, клиент materik-web, атрибут db_role, передача роли и аудитории в токене
config/nginx.conf.example	Публикация веб-клиента и API
config/postgrest.conf.example	Параметры PostgREST
scripts/install-db.sh, scripts/install-static.sh	Создание БД и применение миграций; публикация веб-клиента
tests/db	Автоматическая проверка модели данных (32 проверки прав, аудита, версий, корзины)
licenses, THIRD-PARTY-NOTICES, materik-web.cdx.json	Лицензии и уведомления стороннего ПО, SBOM веб-клиента (CycloneDX 1.6)
SHA256SUMS.txt	Контрольные суммы файлов

Перед установкой проверить целостность: sha256sum -c SHA256SUMS.txt.

1.2 Роли и ответственность

Таблица 2 — Роли эксплуатации

Роль	Ответственность
Владелец системы	Утверждает состав, уровни доступа и правила эксплуатации
Администратор платформы	Установка, настройка, лицензия, обновления, резервное копирование
Администратор безопасности	Роли и пользователи, сертификаты TLS, журналы входа и аудита
Администратор данных	СУБД, миграции, резервное копирование и восстановление

2 Требования

Требования к программному окружению и аппаратным ресурсам приведены в разделе 8 документа «Описание функциональных характеристик». Дополнительно необходимы:

- DNS-имя приложения (далее — materik.example) и сертификат TLS, выданный доверенным центром сертификации;
- доступ администратора к серверам с правами установки пакетов и управления службами;
- учётная запись PostgreSQL с правами CREATEDB и CREATEROLE (например, postgres);

- синхронизация времени на всех серверах (NTP).

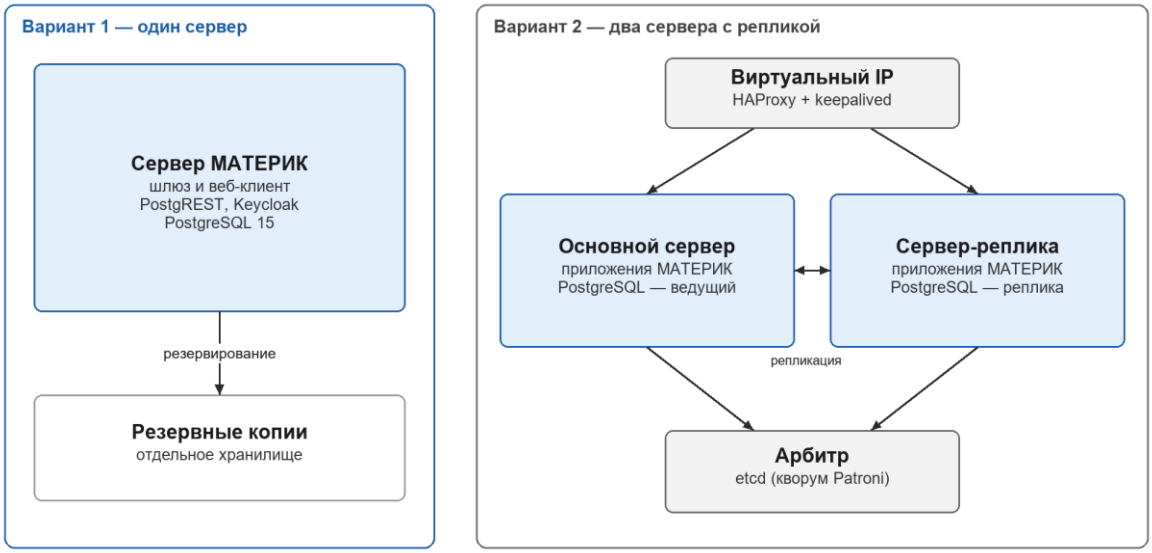


Рисунок 1 — Варианты размещения

2.1 Аппаратные требования

ПО «МАТЕРИК» устанавливается в одном из вариантов. Для каждого варианта ниже приведены узлы и их ресурсы.

Таблица 3 — Вариант 1 — один сервер (без резервирования)

Роль узла	Кол-во	vCPU	ОЗУ	Диски	Размещаемые компоненты
Сервер МАТЕРИК	1	8	32 ГБ	SSD 100 ГБ (система) + SSD 500 ГБ (данные)	Шлюз materik-gate и веб-клиент, PostgREST, Keycloak, PostgreSQL 15
Хранилище резервных копий	1	—	—	Не менее двукратного объёма БД	Отдельный сервер или сетевой ресурс; копии не хранятся на сервере МАТЕРИК

При отказе сервера работа восстанавливается из резервной копии; время восстановления определяется объёмом БД.

Таблица 4 — Вариант 2 — два сервера с репликой (отказоустойчивый)

Роль узла	Кол-во	vCPU	ОЗУ	Диски	Размещаемые компоненты
Сервер МАТЕРИК — основной	1	8	32 ГБ	SSD 100 ГБ (система) + SSD 600 ГБ (данные)	Шлюз и веб-клиент, PostgREST, Keycloak; PostgreSQL — ведущий узел (Patroni)
Сервер МАТЕРИК — реплика	1	8	32 ГБ	SSD 100 ГБ (система) + SSD 600 ГБ (данные)	Те же компоненты в горячем резерве; PostgreSQL — реплика с потоковой репликацией
Арбитр (кворум)	1	2	4 ГБ	SSD 40 ГБ	etcd для Patroni; размещается на отдельном физическом хосте, исключает одновременную работу двух ведущих узлов
Балансировка	—	—	—	—	HAProxy и keepalived на серверах МАТЕРИК; единый виртуальный IP-адрес для пользователей
Хранилище резервных копий	1	—	—	Не менее двукратного объёма БД	Отдельный сервер или сетевой ресурс

При отказе основного сервера ведущим автоматически становится реплика; пользователи продолжают работу по тому же адресу. Узлы размещаются на разных физических хостах.

Таблица 5 — Дополнительные узлы для интеграционных функций (к варианту 1 или 2)

Роль узла	Кол-во	vCPU	ОЗУ	Диски	Размещаемые компоненты
ClickHouse	2	8	64 ГБ	SSD 100 ГБ + от 2 ТБ под данные	Временные ряды; два узла — реплики одного шарда
Координация ClickHouse и Kafka	3	2	8 ГБ	SSD 80 ГБ	ClickHouse Keeper или Apache ZooKeeper; нечётное число узлов для кворума
Apache Kafka	3	8	16 ГБ	SSD 500 ГБ	Приём измерений; фактор репликации топиков 2
OpenSearch	1–3	8	32 ГБ	SSD от 1 ТБ	Технические журналы сервисов; Fluent Bit — на каждом узле
BI и мониторинг	1	4	16 ГБ	SSD 200 ГБ	Apache Superset, Grafana, Prometheus

Профили ориентировочные и предназначены для планирования. Процессоры — x86-64 с частотой от 2,0 ГГц; сеть между узлами — не менее 1 Гбит/с. Итоговые ресурсы уточняются расчётом по числу пользователей, интенсивности обмена, объёму данных и сроку хранения.

3 Установка

3.1 Порядок установки

1) установить сторонние компоненты базового профиля: PostgreSQL 15+, Keycloak 25, PostgREST 12, nginx — по документации их изготовителей;
2) создать БД и применить миграции МАТЕРИК (п. 3.2);
3) импортировать область Keycloak и создать первого администратора (п. 3.3);
4) настроить PostgREST (п. 3.4);
5) опубликовать веб-клиент и настроить nginx (п. 3.5);
6) при необходимости подключить ClickHouse, Kafka, журналы и панели (раздел 4);
7) выполнить проверку (раздел 5).

3.2 База данных

Создание БД materik и применение скриптов 001–004 выполняет scripts/install-db.sh. Скрипт создаёт роли materik_anon, materik_viewer, materik_writer, materik_admin и служебную роль materik_authenticator и задаёт её пароль из переменной окружения.

```
export PGHOST=postgres.internal PGUSER=postgres PGPASSWORD='<пароль владельца>'
export MATERIK_AUTH_PASSWORD='<пароль materik_authenticator>'
sh scripts/install-db.sh
```

Ожидаемый результат — строка «База materik готова». Скрипты 002 и 003 допускают повторное применение. Корректность модели можно проверить без СУБД командой npm install && npm test в каталоге tests/db (встроенный PostgreSQL, 32 проверки).

3.3 Keycloak

Keycloak публикуется по относительному пути /api/keycloak (параметр запуска --http-relative-path=/api/keycloak, за обратным прокси — --proxy-headers=xforwarded и --hostname=https://materik.example/api/keycloak).

1) в файле config/materik-realm.json заменить materik.example на DNS-имя приложения (redirectUris, webOrigins, post.logout.redirect.uris);
2) импортировать область: консоль администратора → Create realm → Resource file, либо kc.sh import --file materik-realm.json;
3) создать первого администратора: Users → Add user; на вкладке Attributes задать db_role = materik_admin; на вкладке Role mapping назначить роль admin; задать пароль;
4) последующих пользователей создавать из интерфейса МАТЕРИК (раздел «Пользователи») — роль и db_role назначаются автоматически.

Таблица 6 — Соответствие уровней доступа

Уровень	Роль Keycloak	Атрибут db_role / роль СУБД
Наблюдатель	viewer	materik_viewer
Оператор	user_rw	materik_writer
Администратор	admin	materik_admin

Шаблон области задаёт политику паролей (не менее 10 символов, цифры, строчные и прописные буквы), защиту от подбора пароля, журналирование событий входа и действий администраторов. Значение db_role принимается только из перечня ролей МАТЕРИК.

Подключение каталога LDAP или Active Directory выполняется в разделе User federation консоли Keycloak. Импортированным пользователям атрибут db_role назначается сопоставителем (mapper) или вручную.

3.4 PostgREST

Скопировать config/postgrest.conf.example в /etc/materik/postgrest.conf и задать строку подключения с паролем materik_authenticator. Сохранить набор открытых ключей области в файл, указанный в jwt-secret:

```
curl -fsS https://materik.example/api/keycloak/realms/materik/protocol/openid-
connect/certs \
  -o /etc/materik/keycloak-jwks.json
```

PostgREST проверяет подпись, срок действия и аудиторию materik-api токена и выполняет запрос от роли из утверждения role. При смене ключей области файл обновляется, PostgREST перезапускается. Служба слушает только 127.0.0.1:3000.

3.5 Веб-клиент и nginx

```
MATERIK_WEB_ROOT=/var/www/materik sh scripts/install-static.sh
cp config/nginx.conf.example /etc/nginx/conf.d/materik.conf
nginx -t && systemctl reload nginx
```

В конфигурации nginx заменить DNS-имя, пути сертификатов и адреса сервисов. Маршрут /api/pg передаётся в PostgREST; маршруты /api/ch и /api/os открываются только

после проверки токена (auth_request к функциям auth_check и auth_check_admin); учётные данные ClickHouse и OpenSearch подставляет nginx, браузеру они не передаются. Сервисы, которые не устанавливаются, оставить закрытыми.

Пересборка веб-клиента из исходных текстов (Node.js 20 или новее): npm ci && npm run build. Адреса подключаемых панелей задаются переменными VITE_MATERIK_BI_URL (по умолчанию /bi) и VITE_MATERIK_GRAFANA_URL (по умолчанию /grafana/).

3.6 Установка варианта с репликой

1) подготовить два сервера МАТЕРИК и арбитр на разных физических хостах (таблица варианта 2, п. 2.1);
2) на арбитре установить etcd; на серверах МАТЕРИК — PostgreSQL 15 и Patroni с общим кластером etcd; убедиться, что один узел ведущий, второй — реплика;
3) выполнить п. 3.2 один раз — на ведущем узле; схема и данные передаются на реплику потоковой репликацией;
4) на обоих серверах установить Keycloak (общая БД keycloak в том же кластере PostgreSQL), PostgREST, шлюз и веб-клиент по п. 3.3–3.5;
5) настроить HAProxy и keepalived: виртуальный IP-адрес для пользователей, подключение PostgREST и Keycloak к текущему ведущему узлу PostgreSQL;
6) проверить переключение: остановить основной сервер и убедиться, что вход и работа с данными продолжаются по тому же адресу.

4 Подключение компонентов расширенного профиля

Таблица 7 — Компоненты по составу внедрения

Компонент	Действия
ClickHouse	Выполнить db/clickhouse/001_materik_timeseries.sql; в таблице kafka_measurements указать брокеры, топик и группу; разместить materik-reader.xml в users.d, задать SHA-256 пароля; указать учётную запись в nginx (X-ClickHouse-User/Key)
Apache Kafka	Создать входной топик (topic-processor-1 или собственный), выдать права группе materik-clickhouse; формат сообщений JSONEachRow: {"equipment_code":"P-1","value":4.2,"ts":"2026-01-01 00:00:00"}
OpenSearch и Fluent Bit	Направить журналы сервисов в индекс fluentbit-logs; создать учётную запись только для поиска в этом индексе; указать её в nginx
Apache Superset, Grafana	Опубликовать на путях /bi и /grafana/ того же DNS-имени (или задать адреса при сборке); настроить вход через Keycloak

5 Проверка после установки

Таблица 8 — Проверки

№	Действие	Ожидаемый результат
1	Открыть https://materik.example в новом окне браузера	Перенаправление на страницу входа Keycloak
2	Войти под администратором	Открыт Дашборд; в заголовке — роль admin
3	Запросить https://materik.example/api/pg/equipment без токена	Данные не возвращаются для записи; изменение отклоняется (401/403)

№	Действие	Ожидаемый результат
4	Создать пользователя-оператора в разделе «Пользователи», войти под ним, создать запись оборудования	Запись создана, владелец — оператор
5	Под другим оператором изменить эту запись	Отказ: «Редактировать и удалять запись может только её владелец или администратор»
6	Под администратором открыть «История изменений»	Видны операции шагов 4–5 с пользователем и временем
7	Удалить запись и восстановить её функцией restore_deleted	Запись возвращена; операции отражены в аудите
8	При расширенном профиле: передать измерение в Kafka, открыть «Тренды»	Значение отображается на графике

6 Эксплуатация

6.1 Резервное копирование и восстановление

- БД МАТЕРИК: pg_dump -Fc materik > materik_$(date +%F).dump; восстановление — pg_restore -d materik --clean materik_<дата>.dump;
- Keycloak: резервная копия его БД либо экспорт области (kc.sh export --realm materik);
- конфигурации: каталоги /etc/materik и /etc/nginx/conf.d;
- ClickHouse: BACKUP DATABASE materik TO Disk(...) либо средствами хранилища.

Целевые показатели: допустимая потеря данных (RPO) — не более 8 ч, время восстановления (RTO) — не более 8 ч. Периодичность резервного копирования выбирается так, чтобы обеспечить RPO; срок хранения копий определяется регламентом эксплуатирующей организации. Восстановление проверяется на отдельном стенде не реже одного раза в квартал.

6.2 Обновление

Обновление поставляется архивом новой версии с перечнем изменений и скриптами миграции с номерами больше установленных. Порядок: резервная копия → применение новых скриптов db → замена файлов веб-клиента → проверка по разделу 5. Возврат к предыдущей версии выполняется восстановлением резервной копии БД и прежних файлов.

6.3 Журналы и мониторинг

Действия пользователей с данными фиксируются в журнале аудита (раздел «История изменений»); события входа — в Keycloak; ошибки сервисов — в журналах служб (journalctl) и, при наличии, в OpenSearch. Контролировать: доступность https-адреса, свободное место на дисках СУБД, срок действия сертификатов TLS, ошибки PostgREST.

6.4 Типовые неисправности

Таблица 9 — Неисправности и действия

Признак	Причина	Действие
Бесконечное перенаправление на вход	Несовпадение redirectUris или DNS-имени	Проверить адреса клиента materik-web в Keycloak
Ошибка 401 при работе с данными	Устарел файл JWKS или не совпадает аудитория	Обновить keycloak-jwks.json, перезапустить PostgREST; проверить mapper api-audience

Признак	Причина	Действие
Пользователь видит данные, но не может их изменять	Отсутствует или неверен атрибут db_role	Назначить уровень доступа в разделе «Пользователи»
Пустые графики	Нет данных в ClickHouse или закрыт маршрут /api/ch	Проверить приём из Kafka и настройки nginx
Ошибка при сохранении записи	Запись принадлежит другому пользователю	Изменение выполняет владелец или администратор

7 Лицензия

1) до получения лицензии получить код запроса сервера: materik-gate --request; передать его ООО «СТ ЦР» вместе с реквизитами договора;
2) полученный файл лицензии разместить в /etc/materik/license.json (права 0640, владелец — служба шлюза);
3) состояние лицензии отображается в интерфейсе администратора; срок, редакция и квоты указаны в файле лицензии;
4) при замене сервера, установке резервного сервера или продлении запрашивается соответствующая лицензия; файл привязан к целевому серверу.

Подробно — документ «Порядок лицензирования».

8 Вывод из эксплуатации

1) остановить приём новых данных и зафиксировать дату окончания эксплуатации;
2) выгрузить данные и журналы аудита (pg_dump), проверить полноту и контрольные суммы;
3) отключить учётные записи и закрыть сетевой доступ;
4) удалить данные, файл лицензии и секреты в соответствии с политикой заказчика и оформить акт;
5) уведомить ООО «СТ ЦР» о прекращении использования лицензии.