



Форсайт. Мобильная
платформа

Версия 19.03
Новые возможности

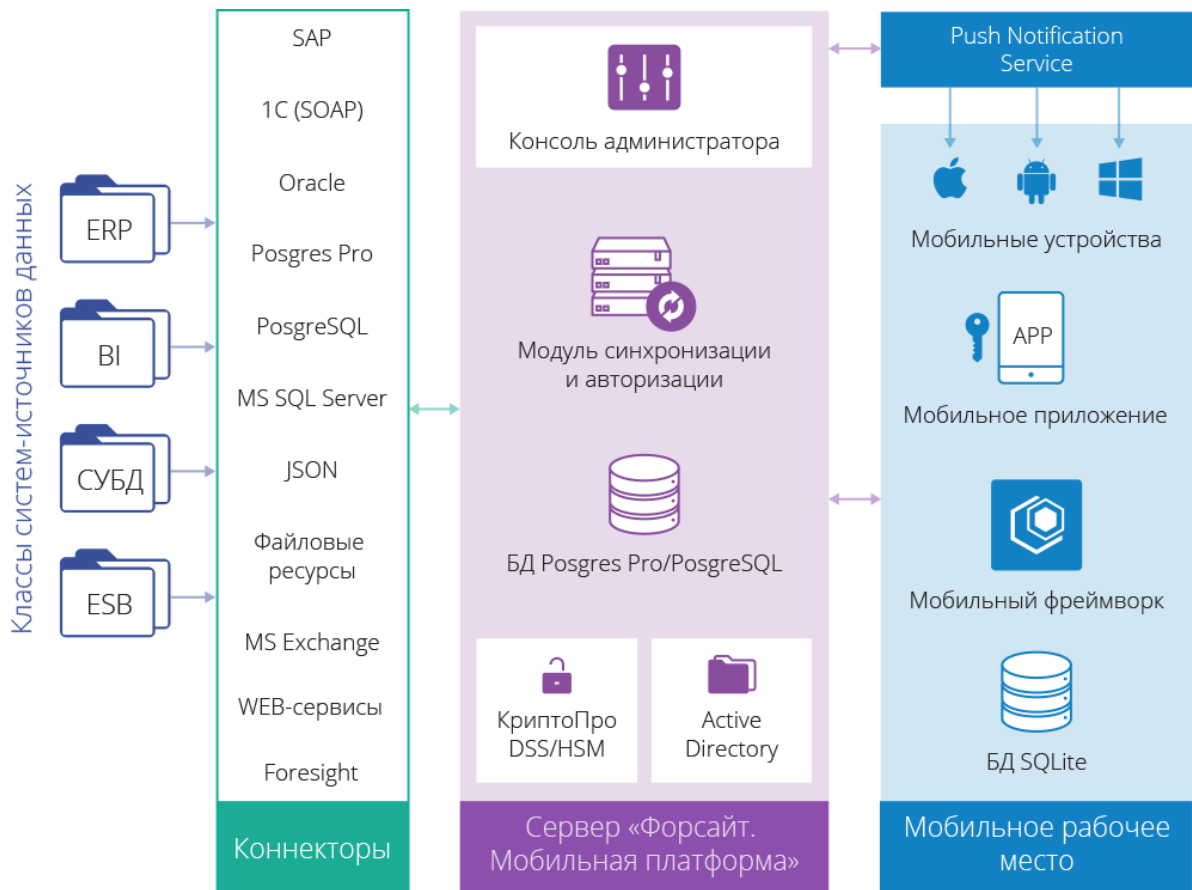
О ПРОДУКТЕ «ФОРСАЙТ. МОБИЛЬНАЯ ПЛАТФОРМА»

Форсайт. Мобильная платформа - современный продукт на рынке Mobile Application Development Platform (MADP). Платформа обладает комплексным решением по информационной безопасности и универсальным инструментарием для быстрой и эффективной разработки защищенных мобильных приложений на основе популярных мобильных операционных систем - iOS, Android, Windows.

Продукт позволяет создать надежные сервисы для обмена данными между источниками и приложениями, как нативными, так и кроссплатформенными веб-приложениями.

Ключевые возможности:

- поддержка мобильных операционных систем - iOS, Android, Windows
- подключение различных источников данных: Postgres Pro, PostgreSQL, SAP, Oracle Database, Microsoft SQL Server, JSON, 1C (SOAP), Microsoft Exchange, WEB-сервисы, продукт «Форсайт. Аналитическая платформа», файловые ресурсы
- передача транзакционных данных
- создание источника данных на базе мобильной платформы
- доступ к данным в онлайн и офлайн-режиме
- обеспечение информационной безопасности:
 - аутентификация и авторизация в корпоративных системах
 - использование шифрования
 - журналирование поведения системы и действий пользователей
- снижение нагрузки на бизнес-системы за счет кэширования данных в платформе
- разработка мобильного приложения с использованием фреймворка
- формирование отчетов и проведение аудита
- интеграция с MDM (Citrix XenMobile)
- унификация средств разработки и подходов к выпуску приложений
- снижение затрат на разработку мобильных приложений



Мы развиваем и улучшаем продукт в соответствии с требованиями рынка и наших партнеров. Для новой версии «Форсайт. Мобильная платформа» реализовано:

1. [Новый коннектор к продукту «Форсайт. Аналитическая платформа»](#)
2. [Отказоустойчивый кластер и кластер непрерывной доступности на основе технологии Kubernetes](#)
3. [Шаблонное приложение](#)
4. [Примеры использования Android и iOS-фреймворков](#)
5. [Улучшение производительности системы](#)
6. [Дополнительные настройки безопасности системы](#)
7. [Управление паролями](#)

1. Новый коннектор к продукту «Форсайт. Аналитическая платформа»

Реализовано подключение к серверу продукта «Форсайт. Аналитическая платформа» для загрузки данных на мобильное устройство.

Ключевые возможности нового коннектора:

- аутентификация и авторегистрация пользователей
- загрузка данных кубов, справочников и таблиц
- фильтрация загрузки данных по параметрам, отметкам измерения
- кэширование и обновление данных

2. Отказоустойчивый кластер и кластер непрерывной доступности на основе технологии Kubernetes

Кластеры используются для распределения трафика, поддержки баз данных, хранения файлов и бизнес-приложений в сети. Для обеспечения горизонтального масштабирования всех компонентов системы реализован новый подход к развёртыванию кластера.

Схема архитектуры развёртывания:

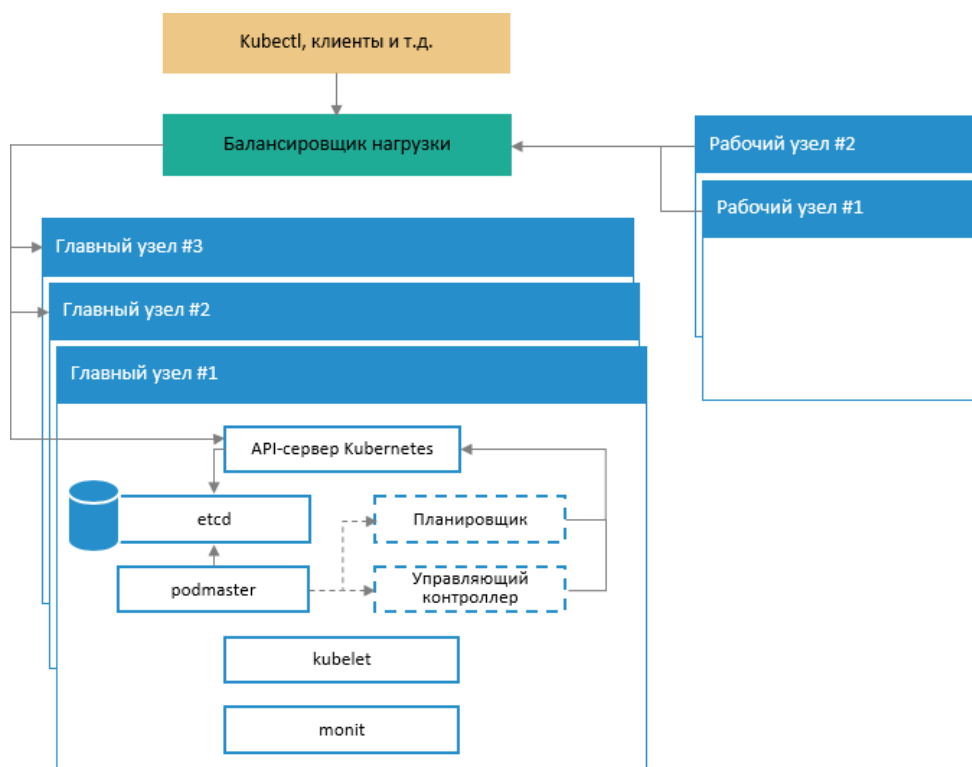
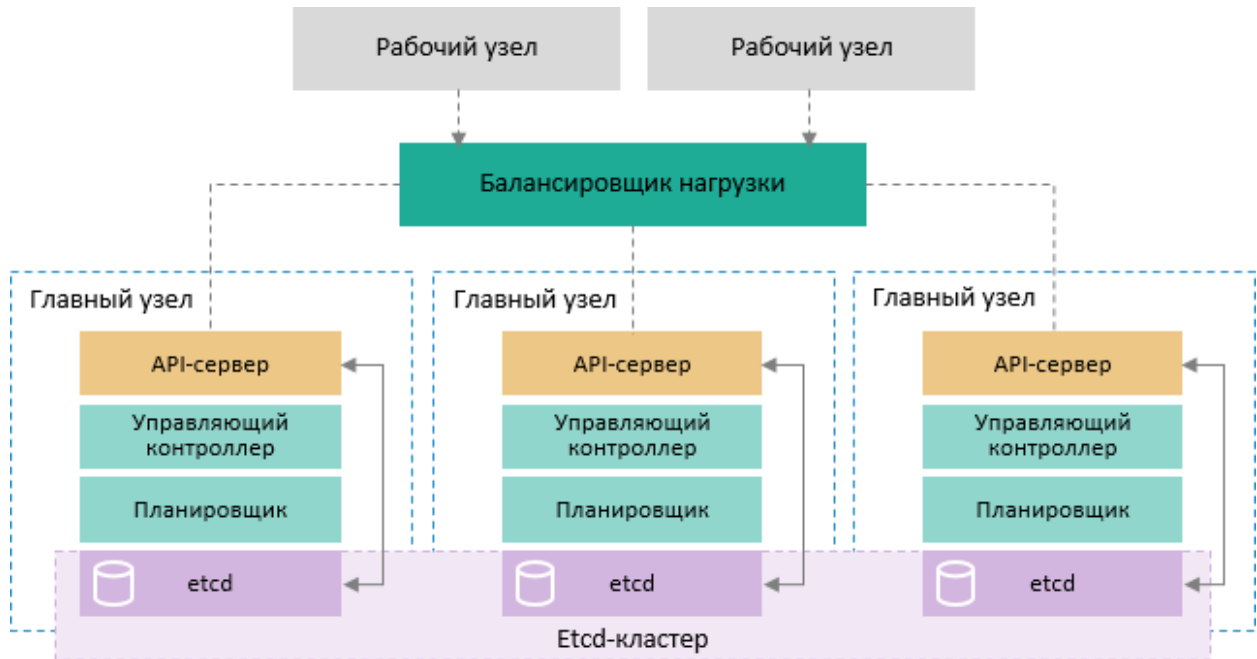


Схема обеспечения отказоустойчивости управляющей части кластера:



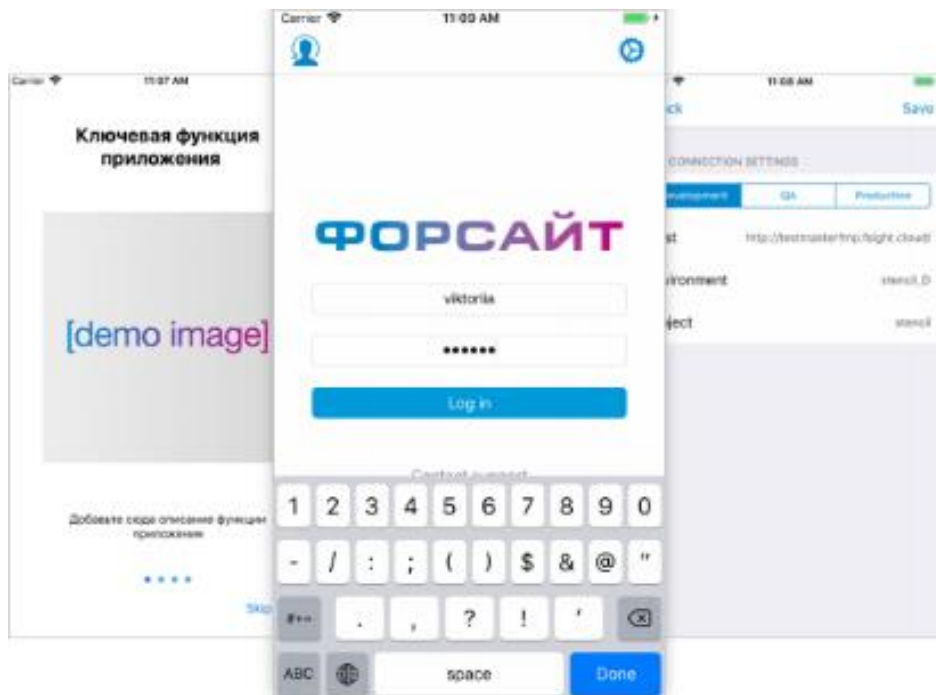
Преимущества нового подхода:

- использование новых средств развертывания и обслуживания компонентов кластера без простоя системы для регламентных работ
- использование бесплатного программного обеспечения с возможностью платной поддержки
- поддержка современной системы файлового распределенного хранилища CEPH
- быстрая установка и удобные механизмы обслуживания продукта «Форсайт. Мобильная платформа»
- удобный графический интерфейс Rancher для диагностики текущего состояния программного обеспечения

3. Шаблонное приложение

Шаблонное приложение – это готовое мобильное приложение с открытым исходным кодом, в котором реализованы формы аутентификации и базового представления данных, удобный интерфейс и адаптивная функциональность для iOS или Android.

Шаблонное приложение помогает быстро ознакомиться с основными принципами работы с мобильной платформой, сократить время на разработку мобильного приложения «с нуля» и настроить параметры приложения в соответствии с требованиями заказчика.

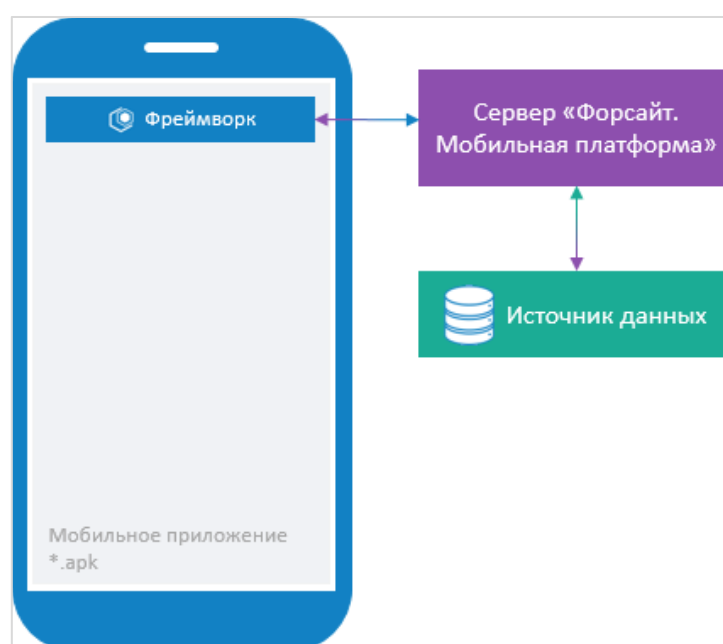


4. Примеры использования Android и iOS-фреймворков

Для Android и iOS-фреймворков реализованы примеры в виде отдельных мини-приложений, в которых используются возможности мобильной платформы от базовых функций аутентификации и загрузки/обновления данных до подписания документов и офлайн-аутентификации.

В примерах используются модули фреймворка на языках Java и Swift.

Примеры помогают быстро ознакомиться с основными принципами работы с мобильной платформой и приступить к разработке частных мобильных приложений.



5. Улучшение производительности системы

Увеличена скорость выполнения запросов на 15-25% в результате использования асинхронного механизма сохранения логов и замены движка базы постоянного хранения логов на современный движок Elasticsearch.

6. Дополнительные настройки безопасности системы

Параметры безопасности системы определяют политику безопасности при аутентификации пользователя.

Ключевые возможности:

- изменение срока действия токена при выполнении аутентификации
- обработка событий неуспешной авторизации
- блокировка устройств и пользователей

The screenshot displays the 'Безопасность' (Security) configuration page in the Citrix Mobile Platform administration console. The interface is in Russian and includes a sidebar menu on the left with options like 'Администрирование', 'Безопасность', and 'Управление приложениями'. The main content area is titled 'Безопасность' and contains several sections:

- Шифрование** (Encryption): Includes checkboxes for 'API' and 'Панель управления' (checked), and a 'Сертификат' dropdown menu.
- Relay сервер** (Relay server): Includes a checkbox for 'Использовать relay сервер'.
- Настройки аутентификации** (Authentication settings): Includes input fields for 'Время жизни JWT' (14 days, 0 hours), 'Время жизни учётной записи пользователя (дни)', and a note about token invalidation.
- Обработка событий неуспешной авторизации** (Failed authentication event processing): Includes input fields for 'Количество неудачных попыток ввода пароля до блокировки устройства', 'Интервал, в течение которого измеряются попытки ввода пароля', 'Период, на который блокируется устройство', 'Количество заблокированных устройств до блокировки пользователя', 'Интервал, в течение которого измеряется блокировка устройств', and 'Период, на который блокируется пользователь'.

A 'Сохранить' (Save) button is located at the bottom of the configuration area.

7. Управление паролями

Парольная политика повышает безопасность системы и позволяет задавать требования к паролям пользователя.

Ключевые возможности:

- настройка требований к сложности пароля
- установка срока действия пароля
- проверка пароля на соответствие заданным требованиям при смене пароля пользователем

ФОРСАЙТ MOBILE PLATFORM

Форсайт: Мобильная платформа

Выйти (Admin)

Администрирование / Безопасность

Безопасность

сертификаты | настройки | управление паролями

Требования к сложности пароля

Минимальная длина пароля: символов

Обязательно наличие и заглавного, и прописного регистра у пароля:

Обязательно наличие цифр в пароле:

Наличие спецсимволов в пароле:
Список допустимых спецсимволов: ~!@#\$%^&*~

Срок действия пароля

Максимальный период действия пароля: дней

Минимальный период действия пароля: дней

Валидация при смене пароля

Минимально возможная разница нового пароля с предыдущим: символов

Количество запрещенных старых паролей: предыдущих паролей

Сохранить