ФОРСАЙТ

Форсайт. Мобильная платформа

Версия 20.02.03
Новые возможности

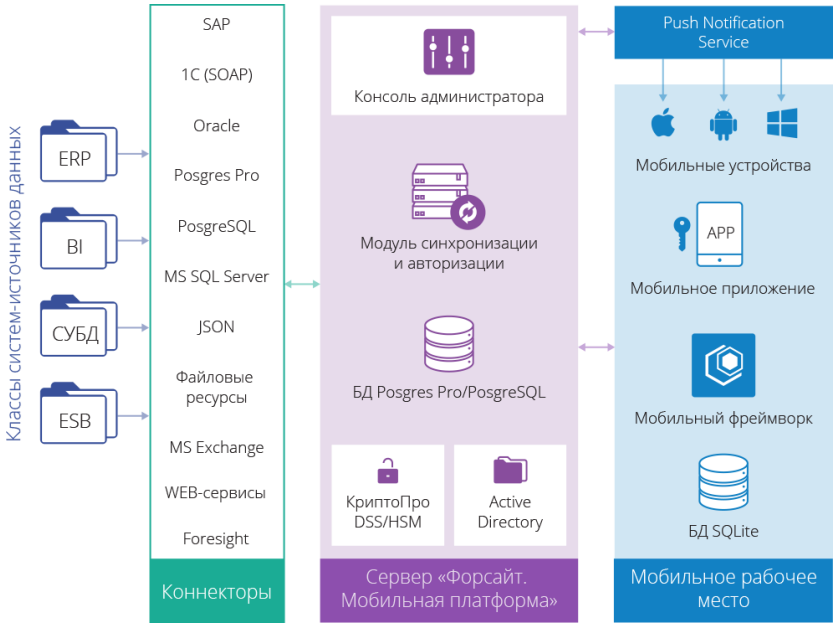
О ПРОДУКТЕ «ФОРСАЙТ. МОБИЛЬНАЯ ПЛАТФОРМА»

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, Sailfish.

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, Sailfish.
- подключение различных источников данных: SAP, 1С (SOAP/XML), PostgreSQL (включая версию Pro), Oracle Database, Microsoft SQL Server, JSON SOAP/XML веб сервисы, Microsoft Exchange, проектирование HTTP запросов, продукт «Форсайт. Аналитическая платформа», файловые ресурсы.
- Передача справочных и оперативных данных. Снижение нагрузки на бизнес-системы за счет кэширования данных в платформе
- значительное ускорение передачи данных за счет определения только измененной информации (расчет дельты), фильтрации и разделения блоков данных по параметрам
- Встроенные источники «Локальная БД» и «Локальное файловое хранилище».
- Доступ к данным в онлайн и офлайн-режиме.
- обеспечение информационной безопасности:
  - единая точка аутентификации для пользователей мобильных устройств,
  - аутентификация и авторизация в корпоративных системах,
  - использование шифрования,
  - шифрование сетевого трафика между сервером и мобильным устройством,
  - журналирование поведения системы и действий пользователей.
- разработка мобильного приложения с использованием фреймворка.
- интеграция с MDM (Citrix XenMobile).



Мультидоменная аутентификация (в одном лесу)

В новой версии платформы добавлена поддержка пользователей из различных дочерних доменов единого леса Active Directory.

Пользователи автоматически будут синхронизированы, как члены универсальной группы. Также для них будут работать, как аутентификация со стороны мобильного устройства, так и аутентификация на файловом и JSON источниках. Для синхронизации используется параметр user principal name.

Для синхронизации таких учетных записей реализована поддержка запросов к Глобальному каталогу Active Directory как в формате LDAP, так и с поддержкой LDAP SSL.

LDAP учетные записи для коннектора JSON

В новой версии сервера реализована поддержка использования учетных записей LDAP (Active Directory) для источника данных JSON.

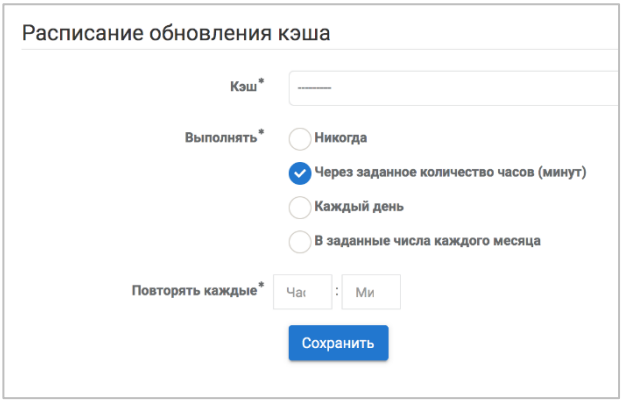
В случае поддержки источником данных учетных записей возможно выбрать в настройках платформы данный тип и установить его по умолчанию. Далее при обращении пользователя к веб- сервисам источника JSON будет передаваться логин и пароль в формате base64 (basic аутентификации).

Для учетных записей LDAP будет доступна возможность формирования уникального кэша для системных учетных данных.

Планирование расписания каждую минуту

В новой версии сервера вы сможете создать расписания с максимальной частотой 1 раз в минуту. Это позволит получить максимальную актуальность информации на сервер ФМП и соответственно мобильном устройстве. Новый интервал расписания доступен для операций:

- Обновление кэша
- Обновление устаревших кэшей
- Удаление истории транзакций



Исправленные баги в работе сервера

- Оптимизация механизма генерации идентификаторов в служебной базе данных.
- Сохранение настроек HTTPS при отмене старта и остановки платформы в консоли ОС.
- Сохранения настроек HTTPS платформы после перезагрузки сервера.

iOS, Android, Sailfish Frameworks

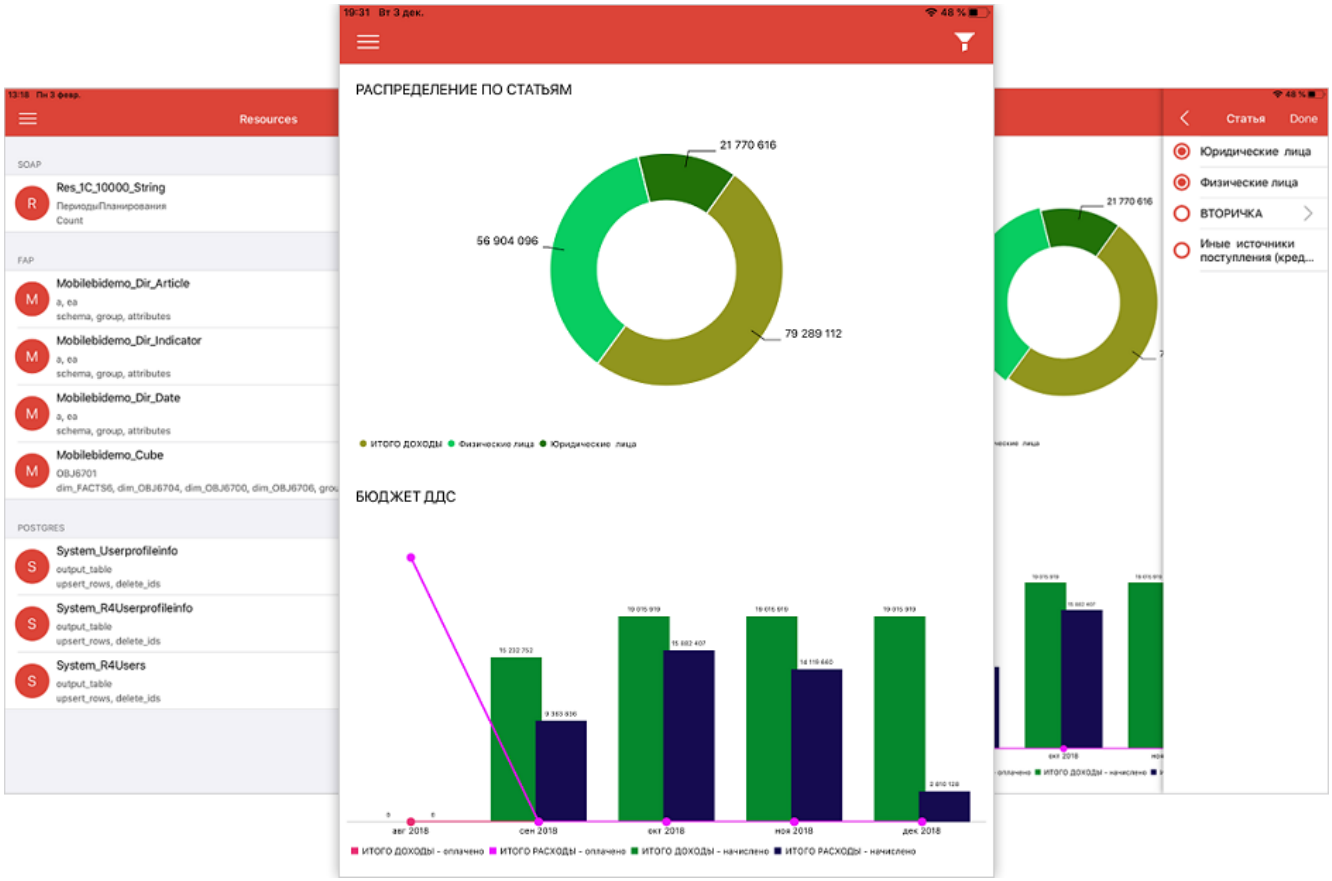
Во фреймворках были исправлены незначительные баги:

1. При изменении структуры со стороны источника данных, автоматически производится обновление структуры и перезагрузка данных ресурса на мобильном устройстве.
2. Запрос метаинформации файлов и папок возвращает их размер во фреймворке Android.

Шаблон построения мобильной аналитики на iOS на примере интеграции с ПО «Форсайт. Аналитическая платформа».

В шаблонном приложении для iOS была разработана функциональность, демонстрирующая возможности коннектора к «Форсайт. Аналитическая платформа». В рамках примера приведена возможность загрузки кубов и справочников с использованием механизмов кэширования и расчета дельты, которые помогут быстро получать актуальную информацию на мобильном устройстве после обновления данных в источнике.

Также приведены примеры по формированию стандартной функциональности: легенда для графиков, построения отчетов в различных разрезах, фильтрация информации и конечно же незаменимые Drill up и Drill down.



Анализ на известные ошибки безопасности ПО входящего в поставку ФМП (CVE)

Для поставки сервера ФМП версии 20.02.03 произведен анализ образов контейнеров на наличие уязвимостей в соответствии с CVE. Анализ проводится ПО Clair: https://github.com/quay/clair

В данной версии нет замечаний уровня: Critical

В данной версии содержаться образы контейнеров внешних компонентов Filebeat, Elastic и Kibana, которые содержат уязвимости уровня High.

В результате проверки определили, что в текущей архитектуре компоненты находятся в виртуальной изолированной сети docker и недоступны для подключения из любой другой сети. Данные уязвимости не применимы.

Известные ошибки безопасности ПО входящего в поставку ФМП

Elastic

RHSA-2020:0227: [High]

Found in: sqlite [3.7.17-8.el7]

Fixed By: 0:3.7.17-8.el7_7.1

SQLite is a C library that implements an SQL database engine. A large subset of SQL92 is supported. A complete database is stored in a single disk file. The API is designed for convenience and ease of use. Applications that link against SQLite can enjoy the power and flexibility of an SQL database without the administrative hassles of supporting a separate database server. Security Fix(es): * sqlite: fts3: improve shadow table corruption detection (CVE-2019-13734) For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.

https://access.redhat.com/errata/RHSA-2020:0227

Kibana

RHSA-2020:0227: [High]

Found in: sqlite [3.7.17-8.el7]

Fixed By: 0:3.7.17-8.el7_7.1

SQLite is a C library that implements an SQL database engine. A large subset of SQL92 is supported. A complete database is stored in a single disk file. The API is designed for convenience and ease of use. Applications that link against SQLite can enjoy the power and flexibility of an SQL database without the administrative hassles of supporting a separate database server. Security Fix(es): * sqlite: fts3: improve shadow table corruption detection (CVE-2019-13734) For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.

https://access.redhat.com/errata/RHSA-2020:0227

Filebeat

RHSA-2019:4190: [High]

Found in: nss-util [3.44.0-3.el7]

Fixed By: 0:3.44.0-4.el7_7

Network Security Services (NSS) is a set of libraries designed to support the cross-platform development of security-enabled client and server applications. The nss-softokn package provides the Network Security Services Softoken Cryptographic Module. The nss-util packages provide utilities for use with the Network Security Services (NSS) libraries. Security Fix(es): * nss: Out-of-bounds write when passing an output buffer smaller than the block size to NSC_EncryptUpdate (CVE-2019-11745) * nss: Empty or malformed p256-ECDH public keys may trigger a segmentation fault (CVE-2019-11729) For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.

https://access.redhat.com/errata/RHSA-2019:4190

RHSA-2019:4190: [High]

Found in: nss-tools [3.44.0-4.el7]

Fixed By: 0:3.44.0-7.el7_7

Network Security Services (NSS) is a set of libraries designed to support the cross-platform development of security-enabled client and server applications. The nss-softokn package provides the Network Security Services Softoken Cryptographic Module. The nss-util packages provide utilities for use with the Network Security Services (NSS) libraries. Security Fix(es): * nss: Out-of-bounds write when passing an output buffer smaller than the block size to NSC_EncryptUpdate (CVE-2019-11745) * nss: Empty or malformed p256-ECDH public keys may trigger a segmentation fault (CVE-2019-11729) For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.

https://access.redhat.com/errata/RHSA-2019:4190

RHSA-2019:4190: [High]

Found in: nss-sysinit [3.44.0-4.el7]

Fixed By: 0:3.44.0-7.el7_7

Network Security Services (NSS) is a set of libraries designed to support the cross-platform development of security-enabled client and server applications. The nss-softokn package provides the Network Security Services Softoken Cryptographic Module. The nss-util packages provide utilities for use with the Network Security Services (NSS) libraries. Security Fix(es): * nss: Out-of-bounds write when passing an output buffer smaller than the block size to NSC_EncryptUpdate (CVE-2019-11745) * nss: Empty or malformed p256-ECDH public keys may trigger a segmentation fault (CVE-2019-11729) For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.

https://access.redhat.com/errata/RHSA-2019:4190

RHSA-2019:4190: [High]

Found in: nss [3.44.0-4.el7]

Fixed By: 0:3.44.0-7.el7_7

Network Security Services (NSS) is a set of libraries designed to support the cross-platform development of security-enabled client and server applications. The nss-softokn package provides the Network Security Services Softoken Cryptographic Module. The nss-util packages provide utilities for use with the Network Security Services (NSS) libraries. Security Fix(es): * nss: Out-of-bounds write when passing an output buffer smaller than the block size to NSC_EncryptUpdate (CVE-2019-11745) * nss: Empty or malformed p256-ECDH public keys may trigger a segmentation fault (CVE-2019-11729) For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.

https://access.redhat.com/errata/RHSA-2019:4190

RHSA-2020:0227: [High]

Found in: sqlite [3.7.17-8.el7]

Fixed By: 0:3.7.17-8.el7_7.1

SQLite is a C library that implements an SQL database engine. A large subset of SQL92 is supported. A complete database is stored in a single disk file. The API is designed for convenience and ease of use. Applications that link against SQLite can enjoy the power and flexibility of an SQL database without the administrative hassles of supporting a separate database server. Security Fix(es): * sqlite: fts3: improve shadow table corruption detection (CVE-2019-13734) For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.

https://access.redhat.com/errata/RHSA-2020:0227

RHSA-2019:4190: [High]

Found in: nss-softokn-freebl [3.44.0-5.el7]

Fixed By: 0:3.44.0-8.el7_7

Network Security Services (NSS) is a set of libraries designed to support the cross-platform development of security-enabled client and server applications. The nss-softokn package provides the Network Security Services Softoken Cryptographic Module. The nss-util packages provide utilities for use with the Network Security Services (NSS) libraries. Security Fix(es): * nss: Out-of-bounds write when passing an output buffer smaller than the block size to NSC_EncryptUpdate (CVE-2019-11745) * nss: Empty or malformed p256-ECDH public keys may trigger a segmentation fault (CVE-2019-11729) For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.

https://access.redhat.com/errata/RHSA-2019:4190

RHSA-2019:4190: [High]

Found in: nss-softokn [3.44.0-5.el7]

Fixed By: 0:3.44.0-8.el7_7

Network Security Services (NSS) is a set of libraries designed to support the cross-platform development of security-enabled client and server applications. The nss-softokn package provides the Network Security Services Softoken Cryptographic Module. The nss-util packages provide utilities for use with the Network Security Services (NSS) libraries. Security Fix(es): * nss: Out-of-bounds write when passing an output buffer smaller than the block size to NSC_EncryptUpdate (CVE-2019-11745) * nss: Empty or malformed p256-ECDH public keys may trigger a segmentation fault (CVE-2019-11729) For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.

https://access.redhat.com/errata/RHSA-2019:4190
