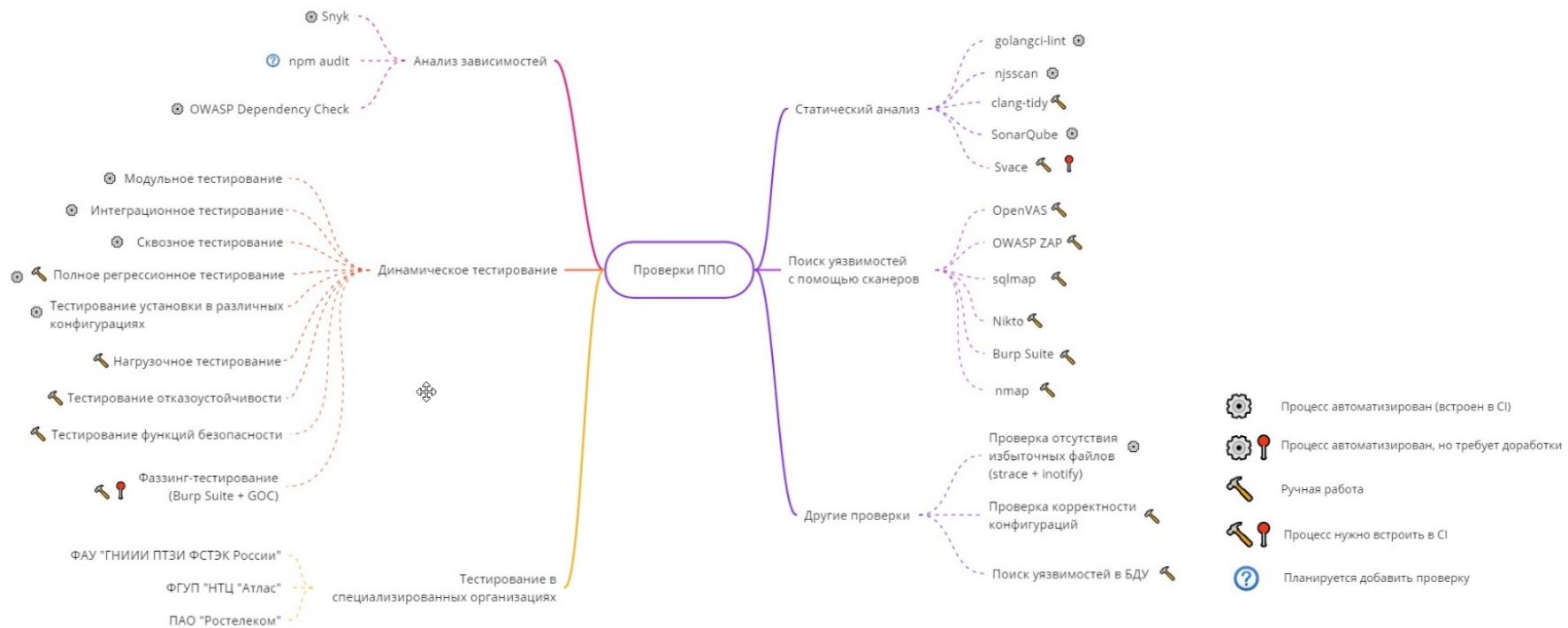


Безопасная разработка ППО «Аврора Центр»



Перечень проверок ППО



<https://confluence.omprussia.ru/pages/viewpage.action?pageId=53089225>

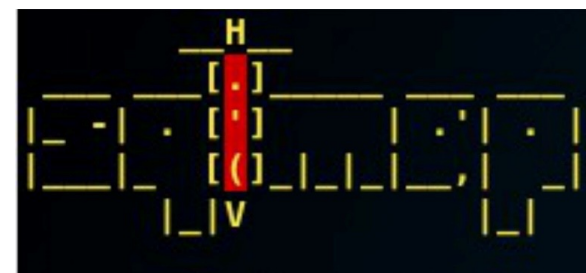
Инструменты для функционального тестирования ППО



Использование сканеров уязвимостей



Nikto



OWASP ZAP



BURPSUITE

Методики тестирования: <https://confluence.omprussia.ru/pages/viewpage.action?pageId=53089550>

Инструменты проверки исходного кода ППО

Статический анализ исходного кода ППО



golangci-lint



njsscan

sonarqube

Svace

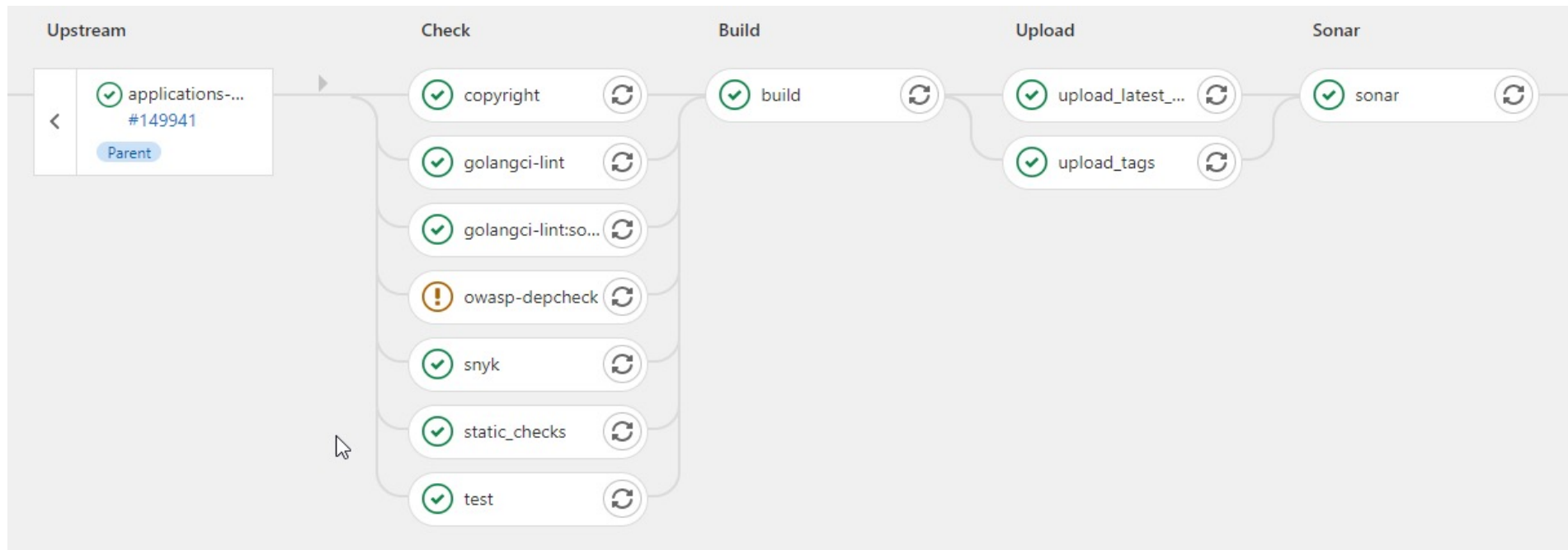
Анализ зависимостей



CI/CD (Непрерывная интеграция и непрерывная доставка)

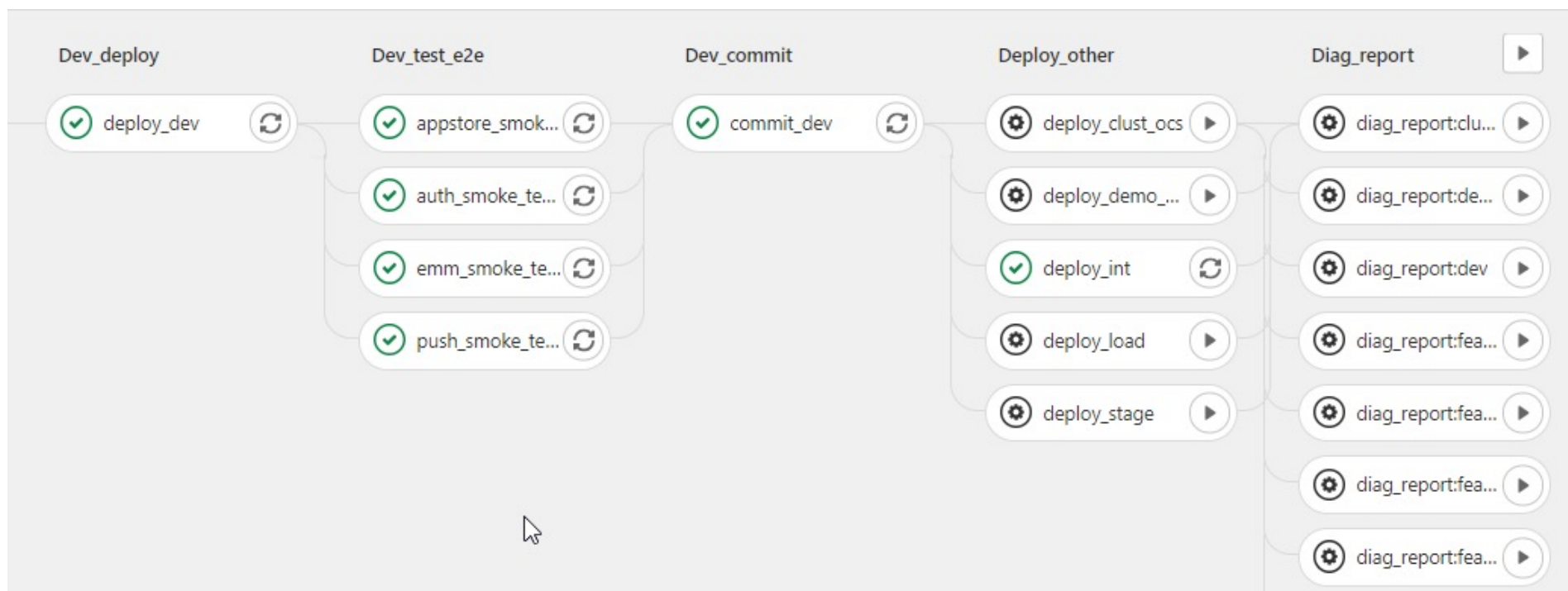


CI Pipeline (конвейер непрерывной интеграции)



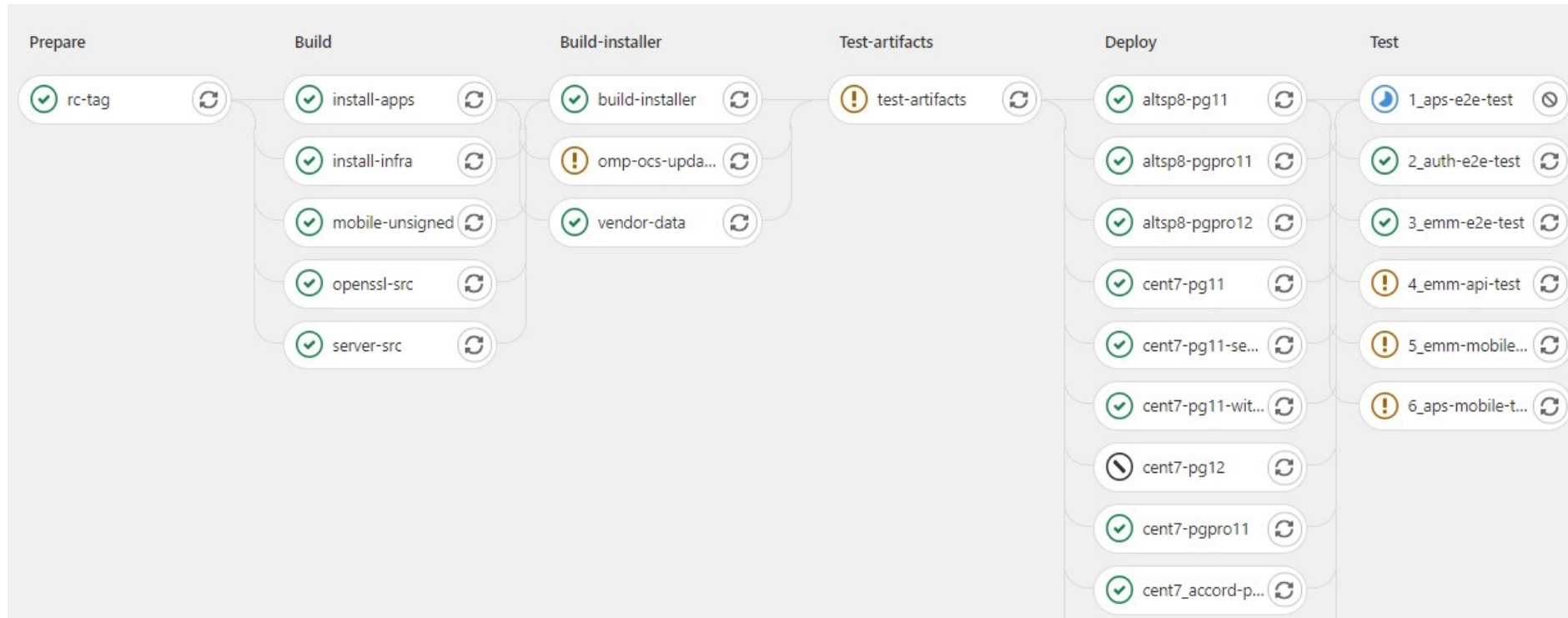
<https://git.omprussia.ru/appstore/applications-api/-/pipelines/142340>

CD pipeline (конвейер непрерывного развертывания)



<https://git.omprussia.ru/appstore/applications-api/-/pipelines/142340>

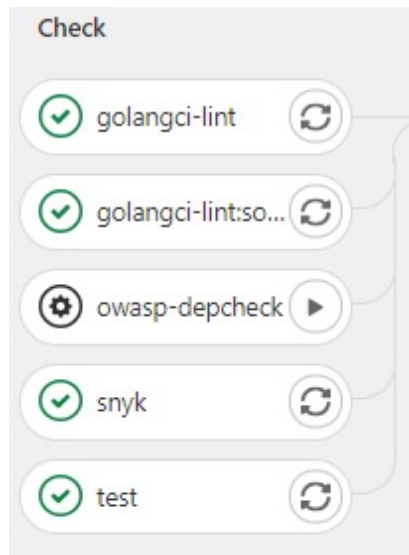
Конвейер выпуска релиза



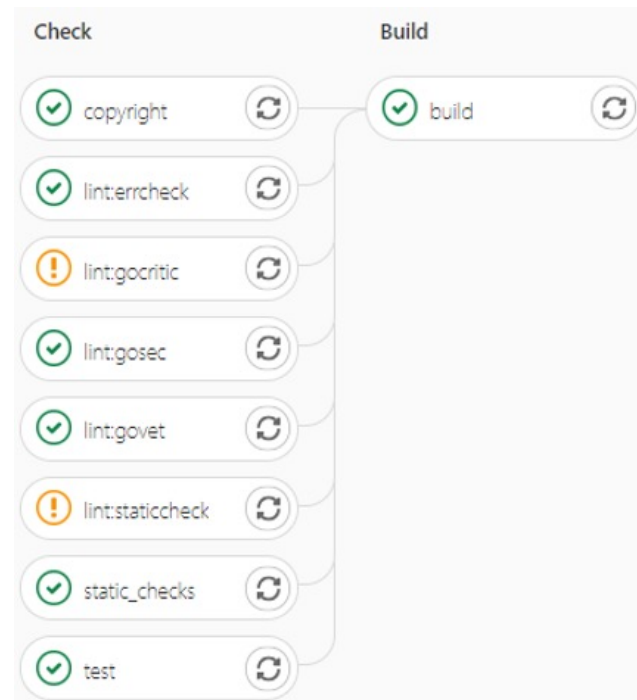
<https://git.omprussia.ru/ocs-infra/ocs-download-src/-/pipelines/149147>

Режимы проверок

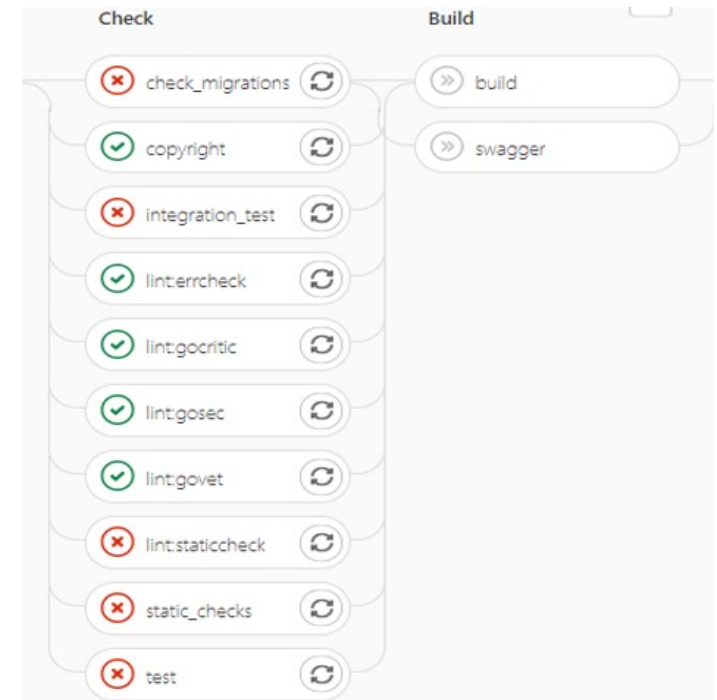
Ручной запуск



Режим «Информирования»



Режим «Блокирования»

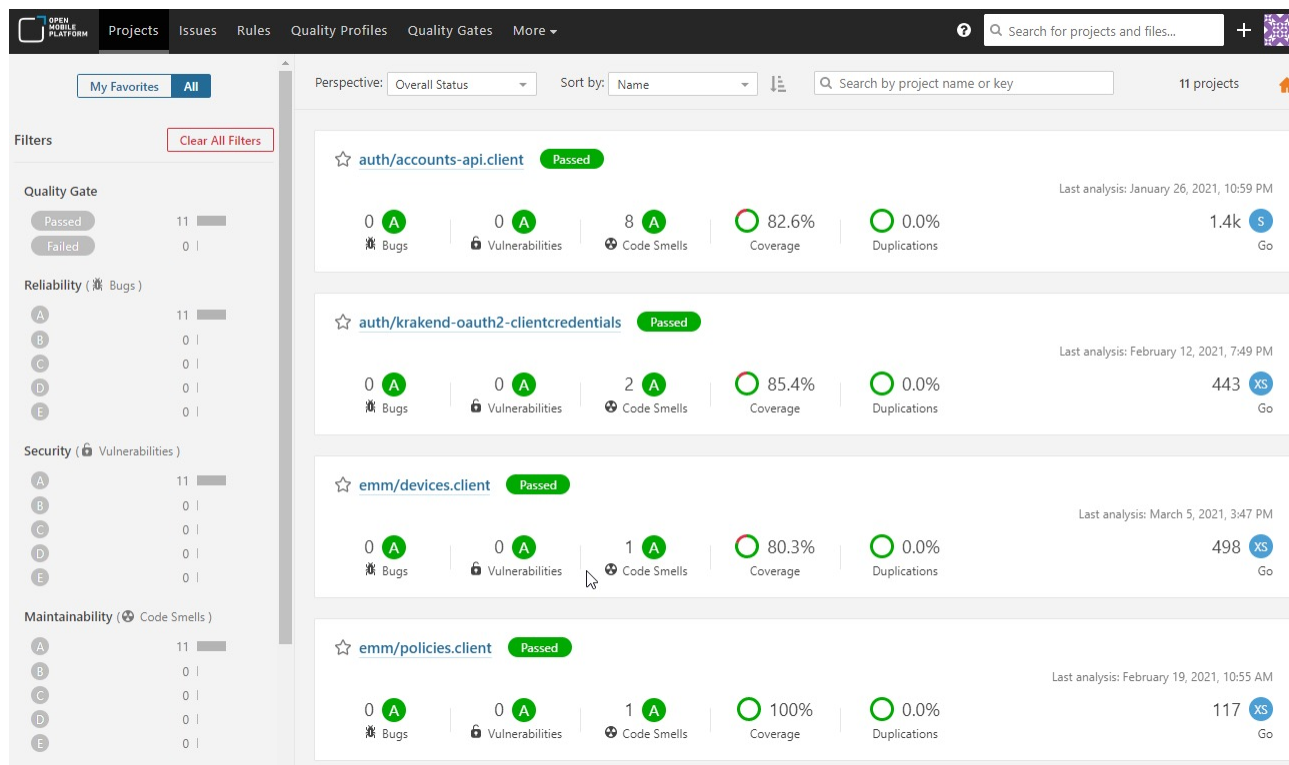


Агрегация отчетов функционального тестирования в Report Portal

The screenshot displays the Report Portal web interface. On the left is a dark sidebar with navigation icons for Dashboard, Launches, Filters, and Debug. The top header bar includes the 'APPSTORE' dropdown, user profile 'P.FOMIN', and settings icons. The main content area shows a filter for 'ALL LAUNCHES' and a specific launch view for 'Devops Tests (ocs-infra/deploy-acimaster) #1003'. A progress bar indicates 'Passed 100.00%' with a total of 136 tests and a duration of 8m 46s. Below this, a 'REFINE' section allows filtering by suite name. The central table lists four test suites, each with its name, start time, total tests, passed tests, and a checkbox for investigation. The first suite, 'Выпуск и обновление Андроид приложения', has 18 tests, all passed. The second, 'Выпуск и обновление Аврора приложения', has 48 tests, all passed. The third, 'Отображения событий аудита для администратора', has 30 tests, all passed. The fourth, 'Отображения событий аудита для Пользователя Аврора Маркет', has 10 tests, all passed.

NAME	START TIME ^	TOTAL	PASSED	FAILED	SKIPPED	PRODUCT BUG	AUTO BUG	SYSTEM ISSUE	TO INVESTIGATE
Выпуск и обновление Андроид приложения 1m 28s authorize.aps_admin.admin_api browser smoke authorize.aps_developer.dev_api fixture.android_dashboard authorize.aps_device_user.appstore_api fixture.new_android_app_without_code fixture.app_draft_empty_release	a month ago	18	18						<input type="checkbox"/>
Выпуск и обновление Аврора приложения 2m 50s authorize.aps_admin.admin_api fixture.aurora_dashboard browser smoke authorize.aps_developer.dev_api fixture.os_releases fixture.key_pairs fixture.new_app_template authorize.aps_device_user.appstore_api	a month ago	48	48						<input type="checkbox"/>
Отображения событий аудита для администратора 1m 57s authorize.aps_admin.admin_api browser smoke	a month ago	30	30						<input type="checkbox"/>
Отображения событий аудита для Пользователя Аврора Маркет 50s browser smoke authorize.aps_device_user.appstore_api	a month ago	10	10						<input type="checkbox"/>

Агрегация отчетов безопасности в SonarQube



- агрегация отчетов тестирования исходного кода;
- удобное представление информации о найденных дефектах;
- выгрузка отчетов.

<https://ocs-sonar.devel.pro/projects>

Ближайшие планы

- Разработка REST API фаззера (уже есть рабочий прототип)
- Встраивание Svace в CI.

Спасибо за внимание!