FINOS

Fintech
Open Source
Foundation

FDX and ODP Program Working Session

Opensourcestrategyforum.org
London, 15 November 2018


Maurizio Pillitu


Diane Mueller


Jamie Jones

Agenda

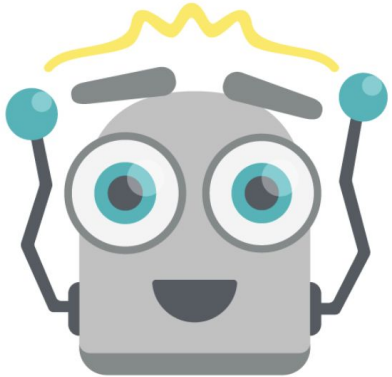
- A Pull Request is submitted to a FINOS GitHub repository ….
  - Check contributors CLAs
  - Check transitive software libraries
    - Security vulnerabilities
    - Licenses
  - Building, linting and testing
  - Continuous (dev) deployment
  - Merging to master, deploying to production
  - More ODP validation tools

A Pull Request is submitted to a FINOS GitHub repository

Check contributors CLAs

cla-bot is a GitHub bot for automation of Contributor Licence Agreements (CLAs).

View the Project on GitHub



What is a CLA?
Installing cla-bot
Configuration options
Development
This project is maintained by ColinEberhardt

Hosted on GitHub Pages — Theme by orderedlist

cla-bot

cla-bot is a GitHub Application for automation of Contributor Licence Agreements (CLAs). It checks whether contributors have signed an agreement, adding labels to PRs if they have, or prompting for signature if they have not.

This bot has the following features:

- Easy integration on projects or whole organisation as a GitHub App
- Automatically checks every pull request and every commit
- Pull requests are re-check on each push
- The approved contributor list can be maintained in various ways including JSON files or a webhook
- A re-check for a pull request can be triggered
- Uses labels and status checks to make the process visible
- Provides a fully-hosted solution, you don't have to maintain your own bit installation
- You can provide templates for the various messages this bot posts

Used by ...

This bot is used by a number of prominent open source projects including:

Gauge FINOS Predix dev/color Gladius Storj Skylight

colineberhardt.github.io/cla-bot

finos-fdx / **bot-github-chatops**

Unwatch 3 | Star 4 | Fork 1

Code | Issues 12 | Pull requests 0 | Projects 0 | Insights | Settings

Fix sorting of repos in list-repos command #46

Edit

Open

Conversation 0 | Commits 2 | Checks 0 | Files changed 2 | +2 −2

pmonks commented on 8 Jul — Collaborator

No description provided.

pmonks added some commits on 8 Jul

`Merge pull request #45 from finos-osr/master` Verified `e11ffc8`

`Fix sorting of repos in list-repos command` `8d57fd2`

Reviewers

maoo

Assignees

maoo

Labels

Fix sorting of repos in list-repos command #46

Edit

Open

Conversation 0 | Commits 2 | Checks 0 | Files changed 2 | +2 −2

pmonks commented on 8 Jul — Collaborator

No description provided.

pmonks added some commits on 8 Jul

- Merge pull request #45 from finos-osr/master ··· Verified e11ffc8
- Fix sorting of repos in list-repos command 8d57fd2

finos-admin added the **cla-present** label on 8 Jul

Reviewers

maoo

Assignees

maoo

Labels

cla-present

finos-admin commented 15 days ago — Collaborator

Thank you for your pull request and welcome to our community! We require contributors to sign a Contributor License Agreement and we don't seem to have CLAs on file for these contributors to the Pull Request: (@). In order for your PR to be reviewed and merged, please follow the directions at the link above.

Project team: please **do not merge this Pull Request** until Foundation staff have confirmed that a CLA is in place for the new contributor(s) listed above.

If there are any questions, please don't hesitate to get in touch with our Infrastructure Support team.
/CC **@finos-admin**

1

maoo commented 5 days ago

@finos-cla-bot[bot] check

1

finos-admin commented 5 days ago — Collaborator

The cla-bot has been summoned, and re-checked this pull request!

finos-admin added the **cla-present** label 5 days ago

A Pull Request is submitted to a FINOS GitHub repository

Building, linting and testing

finos-fdx / bot-github-chatops

Current Branches Build History Pull Requests > Build #153

✓ **Pull Request #46** Fix sorting of repos in list-repos command

#153 passed

Commit `68fcd3c`

#46: Fix sorting of repos in list-repos command

Branch `master`

Ran for 1 min 17 sec

Total time 2 min 46 sec

4 months ago

Peter Monks

Build Jobs

✓	# 153.1		JDK: oraclejdk8 Lein: 2.8.1 Clojure	no environment variables set
✓	# 153.2		JDK: oraclejdk9 Lein: 2.8.1 Clojure	no environment variables set
✓	# 153.3		JDK: oraclejdk10 Lein: 2.8.1 Clojure	no environment variables set

.travis.yml

```
script: lein do git-info-edn, version, check

deploy:
  # Deploy binaries to OpenShift
  - provider: script
    skip_cleanup: true
    script: lein do git-info-edn, uberjar && mkdir -p target/oc && cp
      target/*-standalone.jar target/oc/ && ./deploy-to-openshift.sh $TRAVIS_BRANCH
      $TRAVIS_PULL_REQUEST
    on:
      all_branches: true
      condition: $TRAVIS_BRANCH -eq "master" || $TRAVIS_BRANCH -eq "dev"
      jdk: openjdk11
  # Update Whitesource
  - provider: script
    skip_cleanup: true
    script: lein pom && mvn org.whitesource:whitesource\-maven\-plugin:18.6.2:update
      -Dorg.whitesource.orgToken=$WHITESOURCE_TOKEN
      -Dorg.whitesource.ignoredScopes=test,runtime,provided,system
    on:
      branch: master
      jdk: openjdk11
```

A Pull Request is submitted to a FINOS GitHub repository

Check transitive software libraries

WhiteSource | FINOS

Home Dashboards Organizations Products Projects

Home > Products > bot-github-chatops

bot-github-chatops

Top Alerts 5 4

Library	Type	Description
joda-time-2.10.1.jar	Policy Violation	Unspecified or pending review licenses
jersey-media-json-jackson-2.25.1.jar	New Version	Version 2.27 is available
jersey-client-2.25.1.jar	New Version	Version 2.27.0.redhat-1 is available
jersey-common-2.25.1.jar	New Version	Version 2.27.0.redhat-1 is available
ant-1.8.2.jar	Security Vulnerability	Medium: 1 details
javax.activation-api-1.2.0.jar	Policy Violation	Reject problematic (Category X license) libraries
commons-codec-1.11.jar	Security Vulnerability	Low: 1 details
guava-20.0.jar	Security Vulnerability	Medium: 1 details
hamcrest-core-1.3.jar	New Version	Version 1.3-redhat-1 is available

Home > Security Vulnerability (CVE-2012-2098)

Security Vulnerability

General Details

Name	Severity	CVSS 3 Score	CVSS 2 Score	Date	Modified
CVE-2012-2098	Medium	-	5.0	30-06-2012	29-08-2017

Algorithmic complexity vulnerability in the sorting algorithms in bzip2 compressing stream (BZip2CompressorOutputStream) in Apache Commons Compress before 1.4.1 allows remote attackers to cause a denial of service (CPU consumption) via a file with many repeating inputs.

Vulnerable Libraries

Library Name
ant-1.8.2.jar

Home > bot-github-chatops > Library Details (JavaBeans Activation Framework API jar)

javax.activation-api-1.2.0.jar (view impact analysis)

Information is provided on an a

JavaBeans Activation Framework API jar

SHA-1 Checksum: 85262acf3ca9816f9537ca47d5adeabaead7cb16

Library Found In:

/home/travis/.m2/repository/javax/activation/javax.activation-api/1.2.0/javax.activation-api-1.2.0.jar

JavaBeans Activation Fra..

GroupId	javax.activation
ArtifactId	javax.activation-api
Version	1.2.0
Classifier	
Extension	jar

License (1)

GPL 2.0 Classpath

Reference	POM file
Information	Repo - May be downloaded from a Maven repository
Comment	CDDL or GPL version 2 plus the Classpath Exception

Alerts 1

Type	Description
Policy Violation	Reject problematic (Category X license) libraries

A Pull Request is submitted to a FINOS GitHub repository

Continuous (dev) deployment

[DEV] Bot GitHub ChatOps

Search Catalog | Add to Project

Name | Filter by name | List by Application

APPLICATION

bot-github-chatops-dev

http://bot-github-chatops-dev-jolokia-bot-github-chatops-dev.b9ad.pro-us-east-1.openshiftapps.com

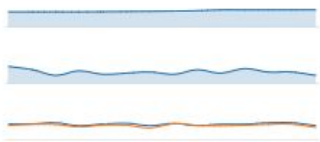
DEPLOYMENT CONFIG

bot-github-chatops-dev, #9

CONTAINERS

bot-github-chatops-dev

- **Image:** bot-github-chatops-dev/bot-github-chatops-dev d5e5382 280.8 MiB
- **Build:** bot-github-chatops-dev, #9
- **Source:** Binary
- **Ports:** 8778/TCP (jolokia)



400 Mib Memory

0.004 Cores CPU

1.2 Kib/s Network

Average Usage Last 15 Minutes

NETWORKING

Service - Internal Traffic

github-chatops-jolokia

8778/TCP (bot-github-chatops-dev-jolokia-port) → 8778

Routes - External Traffic

http://bot-github-chatops-dev-jolokia-bot-github-chatops-dev.b9ad.pro-us-east-1.openshiftapps.com

Route bot-github-chatops-dev-jolokia

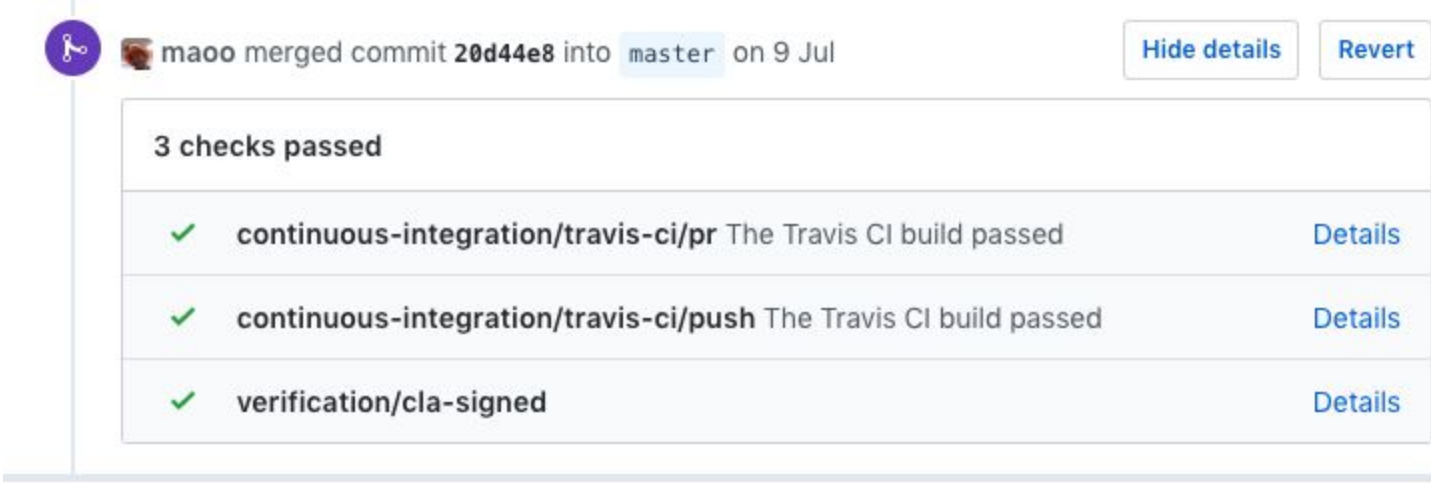
BUILDS

bot-github-chatops-dev

✔ Build #9 is complete created 22 minutes ago

A Pull Request is submitted to a FINOS GitHub repository

Merging to master, deploying to production


maoo merged commit 20d44e8 into master on 9 Jul
Hide details
Revert
3 checks passed
continuous-integration/travis-ci/pr The Travis CI build passed
Details
continuous-integration/travis-ci/push The Travis CI build passed
Details
verification/cla-signed
Details

[PROD] Bot GitHub ChatOps

Search Catalog | Add to Project

Name | Filter by name | List by Application

APPLICATION

bot-github-chatops-prod

http://bot-github-chatops-prod-jolokia-bot-github-chatops-prod.b9ad.pro-us-east-1.openshiftapps.com

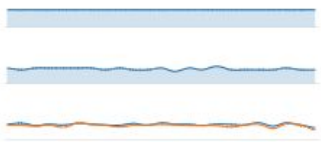
DEPLOYMENT CONFIG

bot-github-chatops-prod, #2

CONTAINERS

bot-github-chatops-prod

- **Image:** bot-github-chatops-prod/bot-github-chatops-prod 6557375 280.3 MiB
- **Build:** bot-github-chatops-prod, #2
- **Source:** Binary
- **Ports:** 8778/TCP (jolokia)



340 Mib Memory

0.004 Cores CPU

1.1 Kib/s Network

Average Usage Last 15 Minutes

NETWORKING

Service - Internal Traffic

github-chatops-jolokia

8778/TCP (bot-github-chatops-prod-jolokia-port) → 8778

Routes - External Traffic

http://bot-github-chatops-prod-jolokia-bot-github-chatops-prod.b9ad.pro-us-east-1.openshiftapps.com

Route bot-github-chatops-prod-jolokia

BUILDS

bot-github-chatops-prod

✔ Build #2 is complete created 9 days ago

A Pull Request is submitted to a FINOS GitHub repository

More ODP validation tools

	C#	Clojure	Java	Javascript	Python
Legal compliance					
Check libraries for problematic/undefined licenses	WhiteSource	WhiteSource	WhiteSource	WhiteSource	WhiteSource
Generates legal reports	WhiteSource	WhiteSource	WhiteSource	WhiteSource	WhiteSource
Security					
Scans code for security vulnerabilities	CoverityScan, SonarCloud		CodeClimate, CoverityScan, SonarCloud	CodeClimate, NodeSecurity, SonarCloud	
Check libraries for security vulnerabilities	WhiteSource	WhiteSource	WhiteSource	WhiteSource, BitHound	WhiteSource
Quality					
Measures test coverage	SonarCloud		CodeClimate, SonarCloud	CodeClimate, SonarCloud	
Check libraries for bugs	WhiteSource	WhiteSource	WhiteSource	WhiteSource, BitHound	WhiteSource
Check libraries for outdated versions	WhiteSource	WhiteSource	WhiteSource	WhiteSource, BitHound	WhiteSource
Check unused libraries				BitHound	
Check libraries for release activity	WhiteSource	WhiteSource	WhiteSource	WhiteSource	WhiteSource
Scans code for hacks and todos				BitHound	
Scans code for bad practices	CoverityScan		CodeClimate, CoverityScan	CodeClimate	
Scans code for bugs	CoverityScan		CoverityScan		

finos.org/odp/docs > Development Infrastructure > Code Validation

FINOS

Fintech
Open Source
Foundation

Thanks!