«Обновлять нельзя оставить»
Управляем зависимостями в CI/CD

Олег Ненашев, CloudBees
@oleg_nenashev

© 2020 CloudBees, Inc. All Rights Reserved.

> whoami

@oleg_nenashev

oleg-nenashev

CloudBees

Jenkins

- Principal SW Engineer, CloudBees
- Jenkins Core maintainer
- Jenkins Board Member
- CDF Ambassador

© 2020 CloudBees, Inc. All Rights Reserved.

О чём доклад?

V – Управление зависимостями

V – На примере Java/Maven

V - Стандартные тулы

X - Jenkins

X - Дебри Java

X - OSGi, модули, …

© 2020 CloudBees, Inc. All Rights Reserved.

Что в докладе?

CI/CD. И причем тут зависимости?

Maven и Maven Enforcer

Боты, на примере Dependabot

Bill of Materials

Демо

© 2020 CloudBees, Inc. All Rights Reserved.

CI/CD – это процесс, а не средства

Time to Market

Time to Recovery

© 2020 CloudBees, Inc. All Rights Reserved.

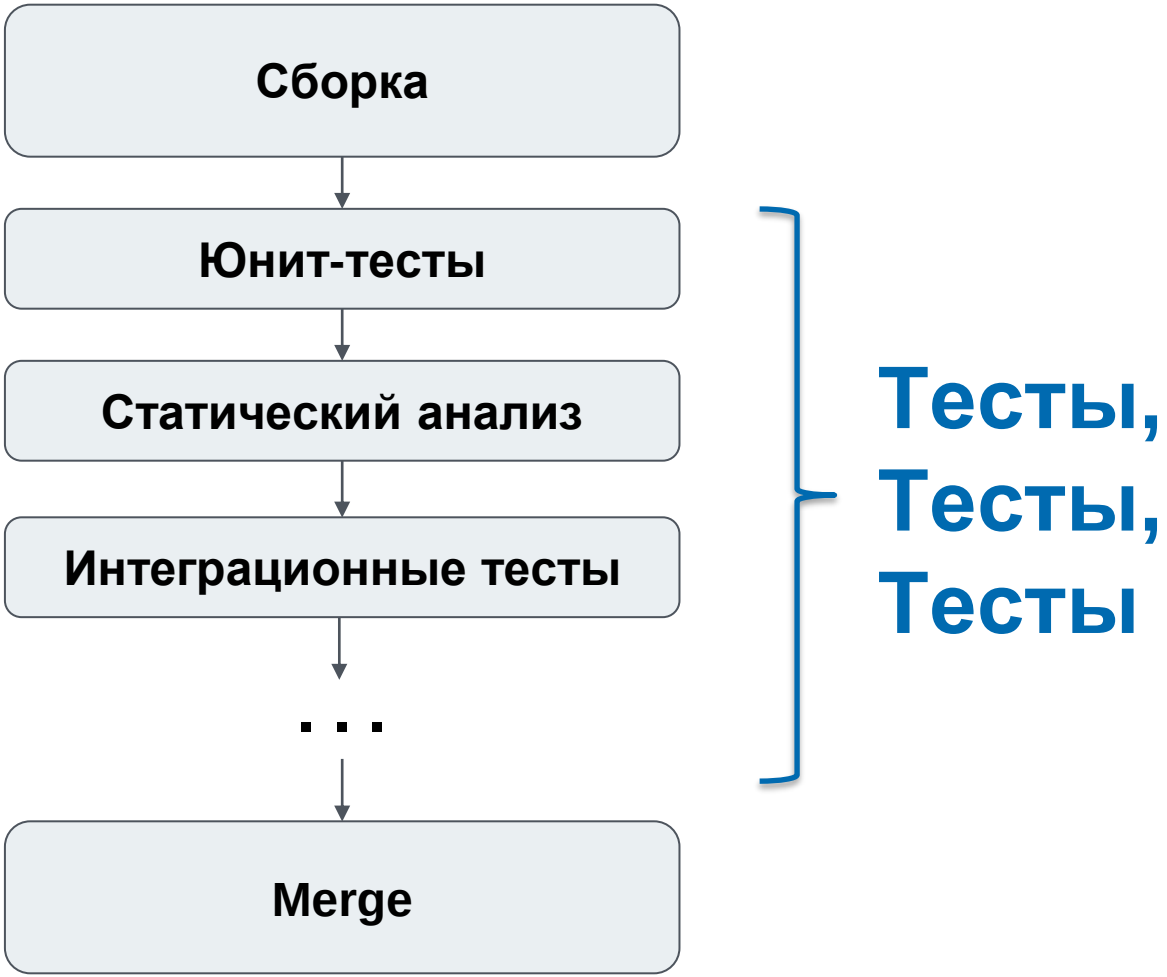
Основы Continuous Integration

- Ранняя интеграция и тестирование изменений
- Быстрый и частый мердж в мастер
- Автоматизация
- Тестовое покрытие
- Прозрачность статуса
- Минимальные изменения

https://martinfowler.com/articles/continuousIntegration.html

© 2020 CloudBees, Inc. All Rights Reserved.

Типовой Pipeline



© 2020 CloudBees, Inc. All Rights Reserved.

А зачем библиотеки?

1. Взять компоненты из библиотеки

© 2020 CloudBees, Inc. All Rights Reserved.

Что делать пользователям?

1. Взять компоненты из библиотеки

Просто добавь клея!

2. Собрать свой ~~велосипед~~ проект

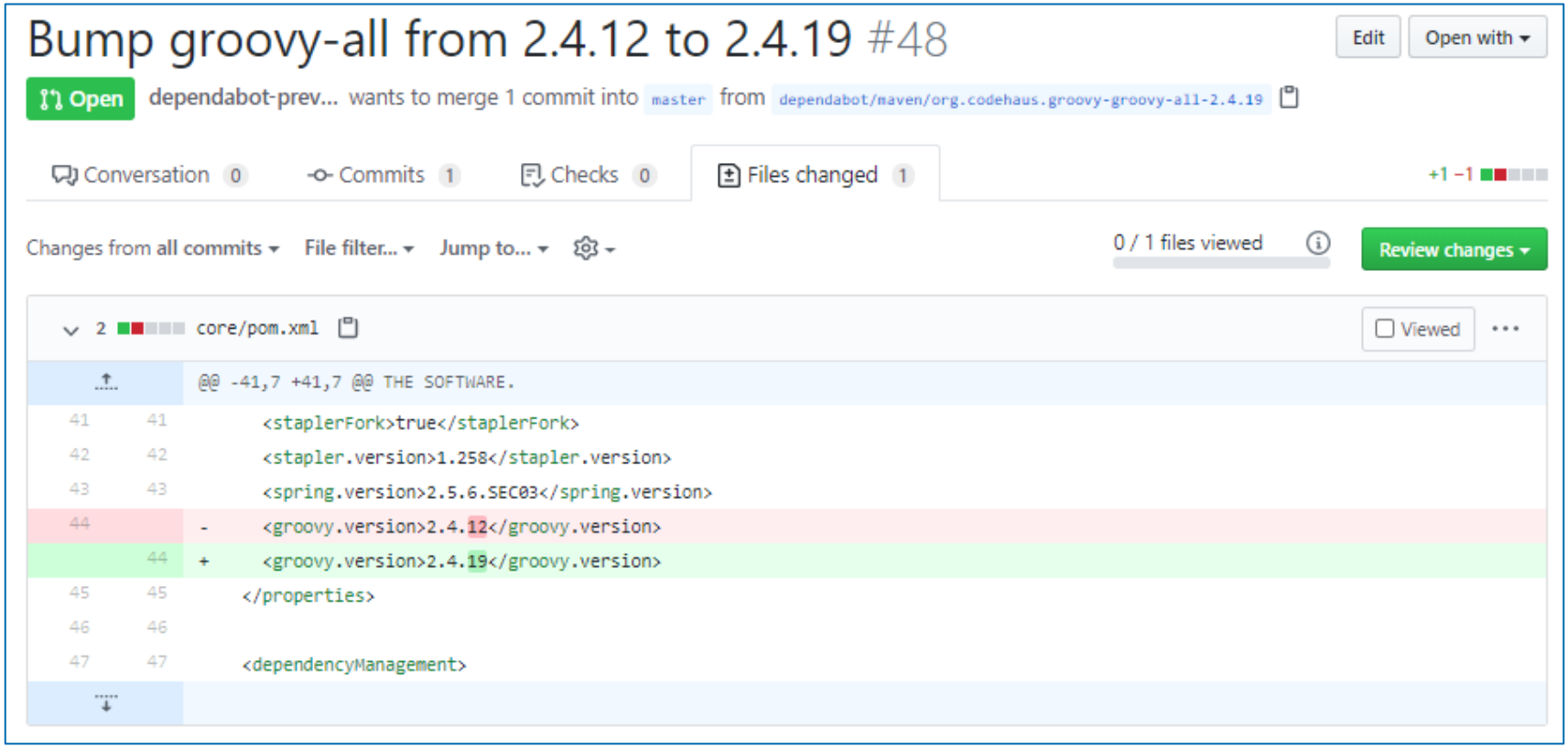
© 2020 CloudBees, Inc. All Rights Reserved.

Основы CI/CD

- Ранняя интеграция и тестирование изменений
- Автоматизация
- Быстрый и частый мердж в мастер
- Тестовое покрытие
- Прозрачность статуса
- **Минимальные изменения**

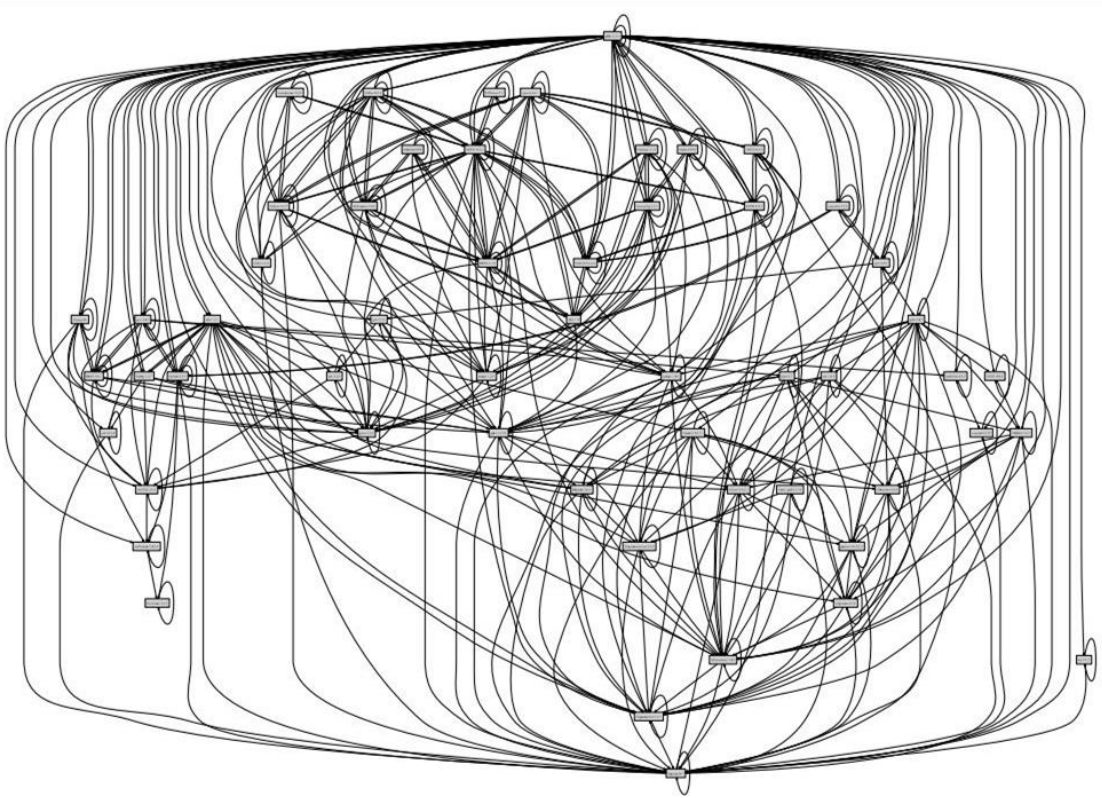
© 2020 CloudBees, Inc. All Rights Reserved.

“Минимальные изменения”?

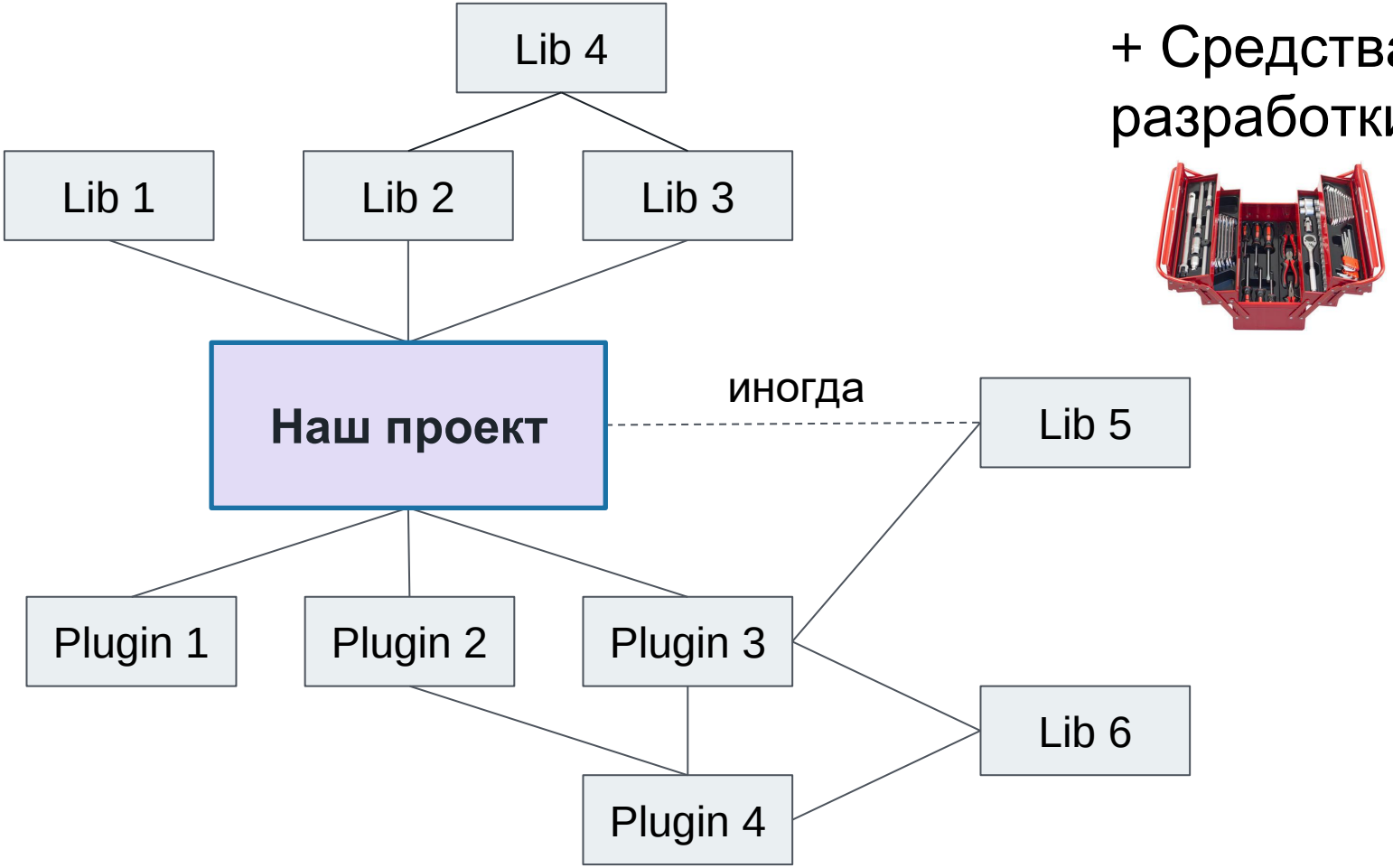


© 2020 CloudBees, Inc. All Rights Reserved.

Dependency Hell



© 2020 CloudBees, Inc. All Rights Reserved.



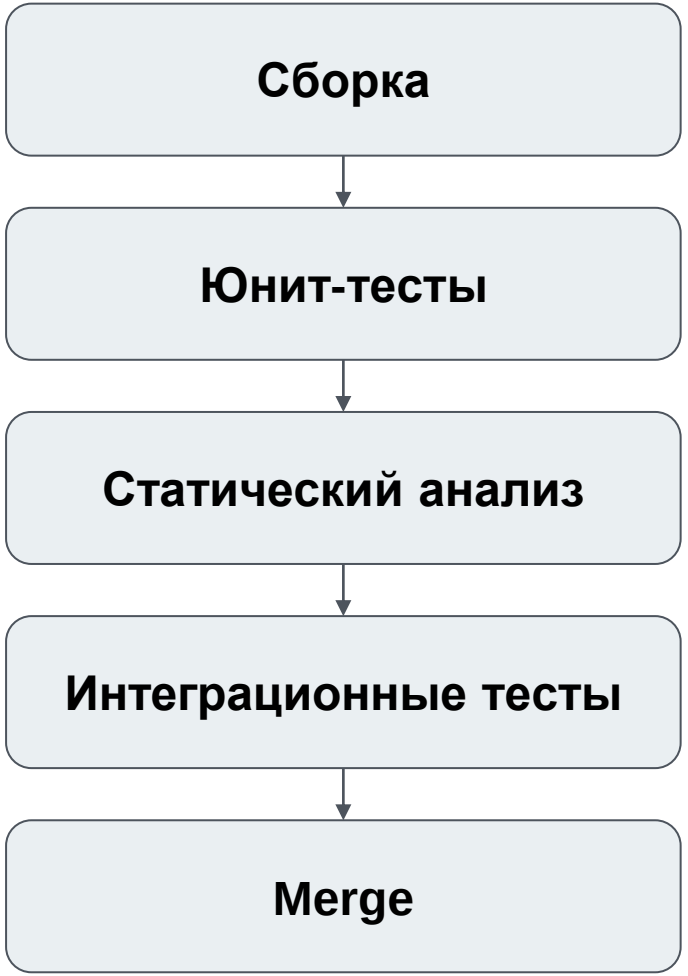
+ Средства разработки

© 2020 CloudBees, Inc. All Rights Reserved.

IT IS OVER

9000 DEPENDENCIES

Pipeline
Pipeline'ов

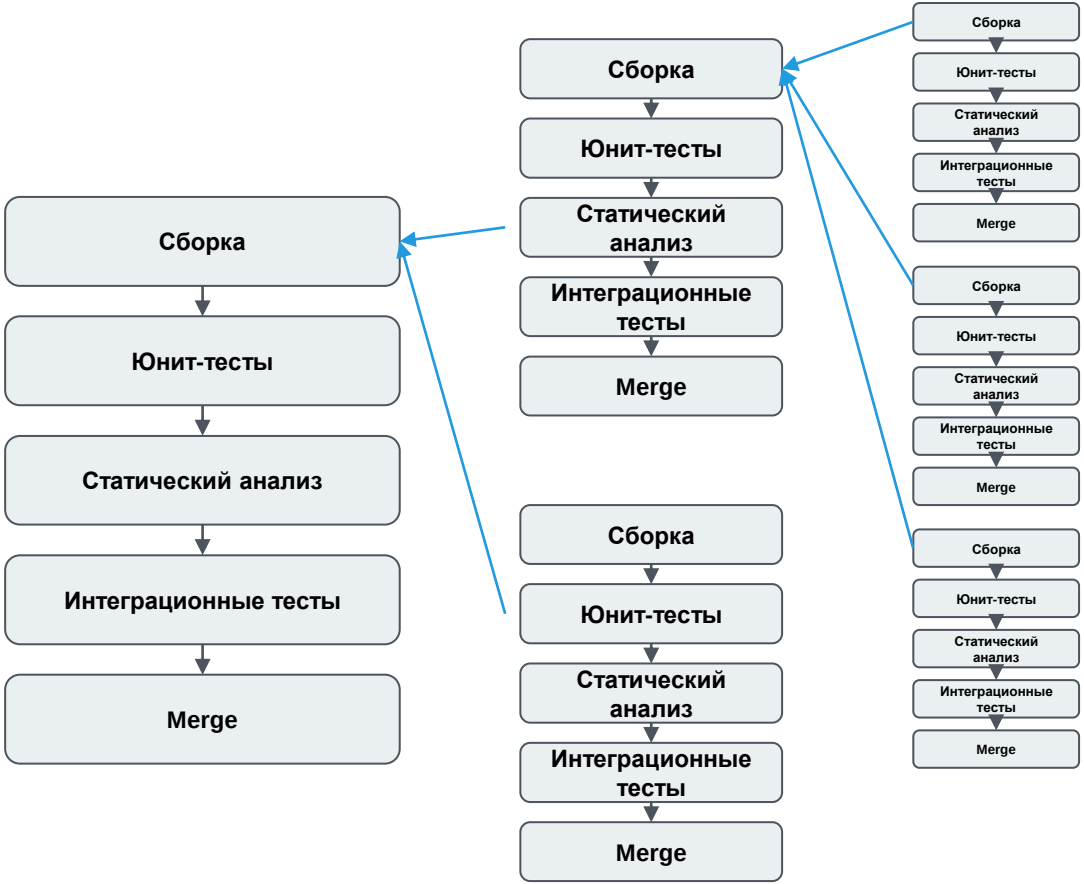


© 2020 CloudBees, Inc. All Rights Reserved.

Pipeline
Pipeline'ов

© 2020 CloudBees, Inc. All Rights Reserved.

Pipeline
Pipeline'ов



© 2020 CloudBees, Inc. All Rights Reserved.

Как часто Вы обновляете зависимости?

© 2020 CloudBees, Inc. All Rights Reserved.

Обновлять нельзя, оставить

aka “работает – не трогай”

© 2020 CloudBees, Inc. All Rights Reserved.

Почему?

Сложно тестировать

Нет времени

И так сойдет

© 2020 CloudBees, Inc. All Rights Reserved.

Не сойдёт!

Нужны новые фичи

Багфиксы

Security-апдейты ☹

Пример: jackson-databind

VULNERABILITY	VULNERABLE VERSIONS	SNYK PATCH	PUBLISHED
H Deserialization of Untrusted Data	[,2.10.0)	Not available	29 May, 2020
H Deserialization of Untrusted Data	[,2.9.10.4)	Not available	08 Apr, 2020
H Deserialization of Untrusted Data	[,2.9.10.4)	Not available	08 Apr, 2020
H Deserialization of Untrusted Data	[,2.9.10.4)	Not available	31 Mar, 2020
H Deserialization of Untrusted Data	[,2.9.10.4)	Not available	31 Mar, 2020
H Deserialization of Untrusted Data	[,2.9.10.4)	Not available	31 Mar, 2020
H Deserialization of Untrusted Data	[2.0.0,2.9.10.4)	Not available	26 Mar, 2020
H Deserialization of Untrusted Data	[2.0.0,2.9.10.4)	Not available	26 Mar, 2020
H Deserialization of Untrusted Data	[2.0.0,2.9.10.4)	Not available	18 Mar, 2020
H Deserialization of Untrusted Data	[2.0.0,2.9.10.4)	Not available	18 Mar, 2020
H Deserialization of Untrusted Data	[,2.6.7.3),[2.8.0,2.8.11.5),[2.9.0,2.9.10.3)	Not available	02 Mar, 2020
H Deserialization of Untrusted Data	[,2.9.10.4)	Not available	02 Mar, 2020
H Deserialization of Untrusted Data	[,2.8.11.5),[2.9.0,2.9.10.3)	Not available	11 Feb, 2020
H Deserialization of Untrusted Data	[,2.9.10.2)	Not available	03 Jan, 2020
H Deserialization of Untrusted Data	[2.0.0, 2.9.10.1)	Not available	13 Oct, 2019

https://snyk.io/vuln/maven:com.fasterxml.jackson.core%3Ajackson-databind

© 2020 CloudBees, Inc. All Rights Reserved.

Апдейт - возможность прочувствовать технический долг

© 2020 CloudBees, Inc. All Rights Reserved.

https://2019.jokerconf.com/2019/talks/rjhhmugp5tzqbmlmg3mcm/

© 2020 CloudBees, Inc. All Rights Reserved.

Экосистема Jenkins

Ядро и модули

Плагины

Дистрибутивы

Подпроекты

Библиотеки

Средства разработки

© 2020 CloudBees, Inc. All Rights Reserved.

Java 10 PoC - июнь 2018

Java 11 PoC - сентябрь 2018

Java 11 RC - декабрь 2018

Java 11 GA - март 2019

TODO:

- Обновить несколько библиотек
- Автоматизировать тесты

???

© 2020 CloudBees, Inc. All Rights Reserved.

Обновление и бинарная совместимость

© 2020 CloudBees, Inc. All Rights Reserved.

Наши “друзья”

ClassNotFoundException

MethodNotFoundException

AbstractMethodError

LinkageError

© 2020 CloudBees, Inc. All Rights Reserved.

Тулы не работают

Нет фиксов для Java 9+

Несовместимые изменения

Библиотеки требуют Java 9+

Мёртвые проекты

© 2020 CloudBees, Inc. All Rights Reserved.

Апдейт - возможность прочувствовать технический долг

© 2020 CloudBees, Inc. All Rights Reserved.

Обновлять, нельзя оставить

© 2020 CloudBees, Inc. All Rights Reserved.

Rocket Science

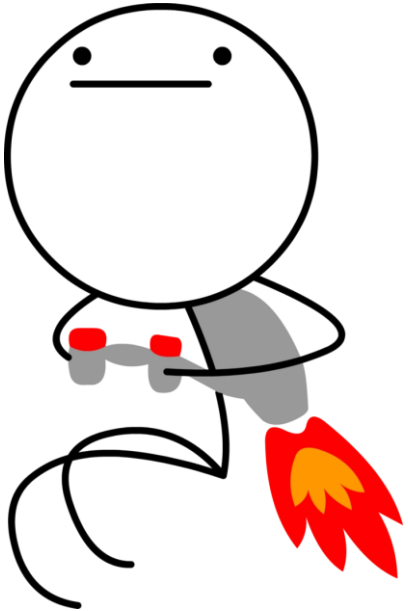
Переписать всё на Go/Kotlin/{ваш язык}

Перейти на микросервисы

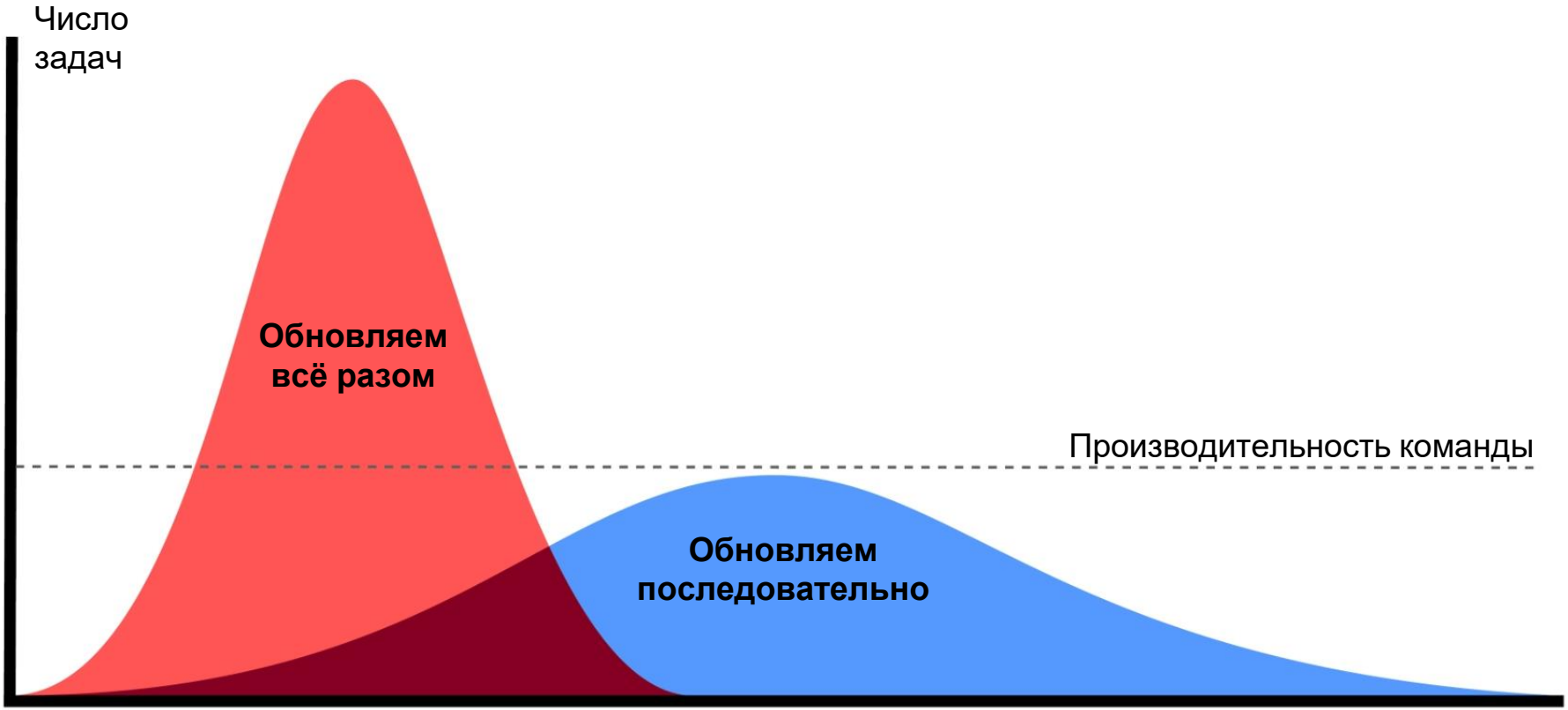
OSGi

Модули Java

… нет

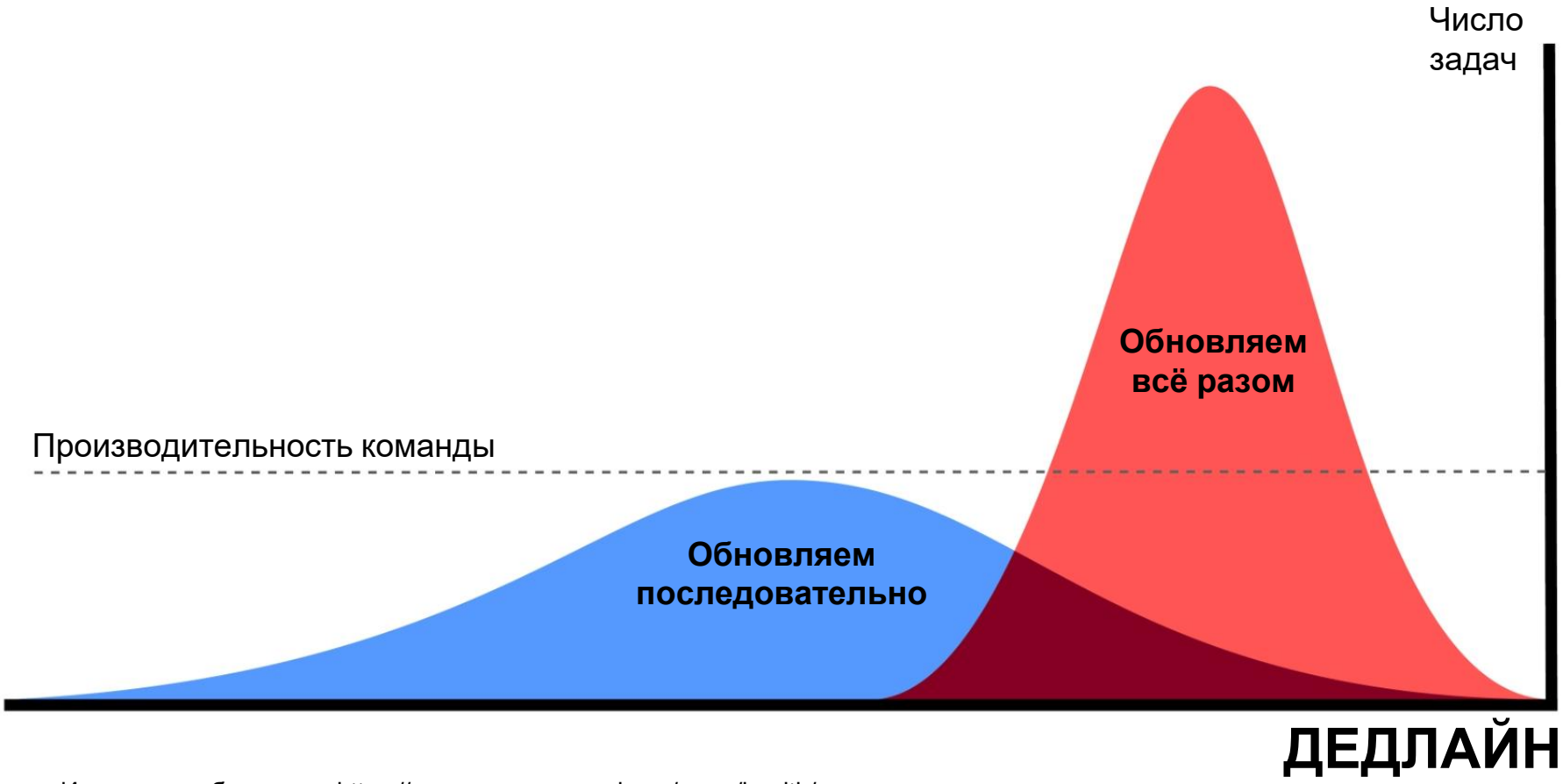


© 2020 CloudBees, Inc. All Rights Reserved.



Источник изображения: https://newsroom.unsw.edu.au/news/health/we-can-shrink-covid-19-curve-rather-just-flatten-it

© 2020 CloudBees, Inc. All Rights Reserved.



Источник изображения: https://newsroom.unsw.edu.au/news/health/we-can-shrink-covid-19-curve-rather-just-flatten-it

© 2020 CloudBees, Inc. All Rights Reserved.

> *mvn versions:display-dependency-updates*

? ? ?

© 2020 CloudBees, Inc. All Rights Reserved.

Maven-плагины

> *mvn versions:display-dependency-updates*

```
The following dependencies in Dependencies have newer versions:
[INFO]  com.github.tomakehurst:wiremock ..... 1.57 -> 2.26.3
[INFO]  com.tngtech.java:junit-dataprovider ..... 1.10.0 -> 1.13.1
[INFO]  io.jenkins:configuration-as-code ..... 1.32 -> 1.41
[INFO]  io.rest-assured:rest-assured ..... 3.3.0 -> 4.3.0
[INFO]  org.apache.commons:commons-lang3 ..... 3.7 -> 3.10
[INFO]  org.hamcrest:hamcrest-core ..... 2.1 -> 2.2
[INFO]  org.hamcrest:hamcrest-library ..... 2.1 -> 2.2
[INFO]  org.jenkins-ci.modules:instance-identity ..... 2.1 -> 2.2
...
```

© 2020 CloudBees, Inc. All Rights Reserved.

Наши тулы

- Maven /Gradle
- Parent POM
- Maven SureFire, JUnit/etc.
- SpotBugs, Animal Sniffer, Maven Enforcer
- JaCoCo и Cobertura
- Свои Maven-плагины

© 2020 CloudBees, Inc. All Rights Reserved.

Maven
не контролирует
зависимости
по умолчанию

© 2020 CloudBees, Inc. All Rights Reserved.

Транзитивные зависимости...

© 2020 CloudBees, Inc. All Rights Reserved.

Барух Садогурский, Кирилл Толкачев — Баттл инструментов для сборки — Maven vs Gradle

© 2020 CloudBees, Inc. All Rights Reserved.

Что поможет?

- Maven Enforcer Plugin

  https://maven.apache.org/enforcer/maven-enforcer-plugin/

- Extra Enforcer Rules Plugin

  https://www.mojohaus.org/extra-enforcer-rules/

© 2020 CloudBees, Inc. All Rights Reserved.

Транзитивные зависимости

- И снова Maven Enforcer Plugin
- requireUpperBoundDeps

```
<requireUpperBoundDeps>
  <excludes>
    <exclude>commons-logging:commons-logging</exclude>
    <exclude>com.google.code.findbugs:jsr305</exclude>
    <exclude>net.java.dev.jna:jna</exclude>
  </excludes>
</requireUpperBoundDeps>
```

© 2020 CloudBees, Inc. All Rights Reserved.

Extra Enforcer Rules Plugin

- banDuplicateClasses
- enforceBytecodeVersion
- banCircularDependencies
- …

https://www.mojohaus.org/extra-enforcer-rules/

© 2020 CloudBees, Inc. All Rights Reserved.

```
<plugin>
  <artifactId>maven-enforcer-plugin</artifactId>
  <executions>
    <execution>
    ...
      <configuration>
        <rules>
          <enforceBytecodeVersion>
            <maxJdkVersion>1.8</maxJdkVersion>
            <ignoredScopes>
              <ignoredScope>test</ignoredScope>
            </ignoredScopes>
          </enforceBytecodeVersion>
    ...
  </executions>
  <dependencies>
  ...
   <artifactId>extra-enforcer-rules</artifactId>
  ...
```

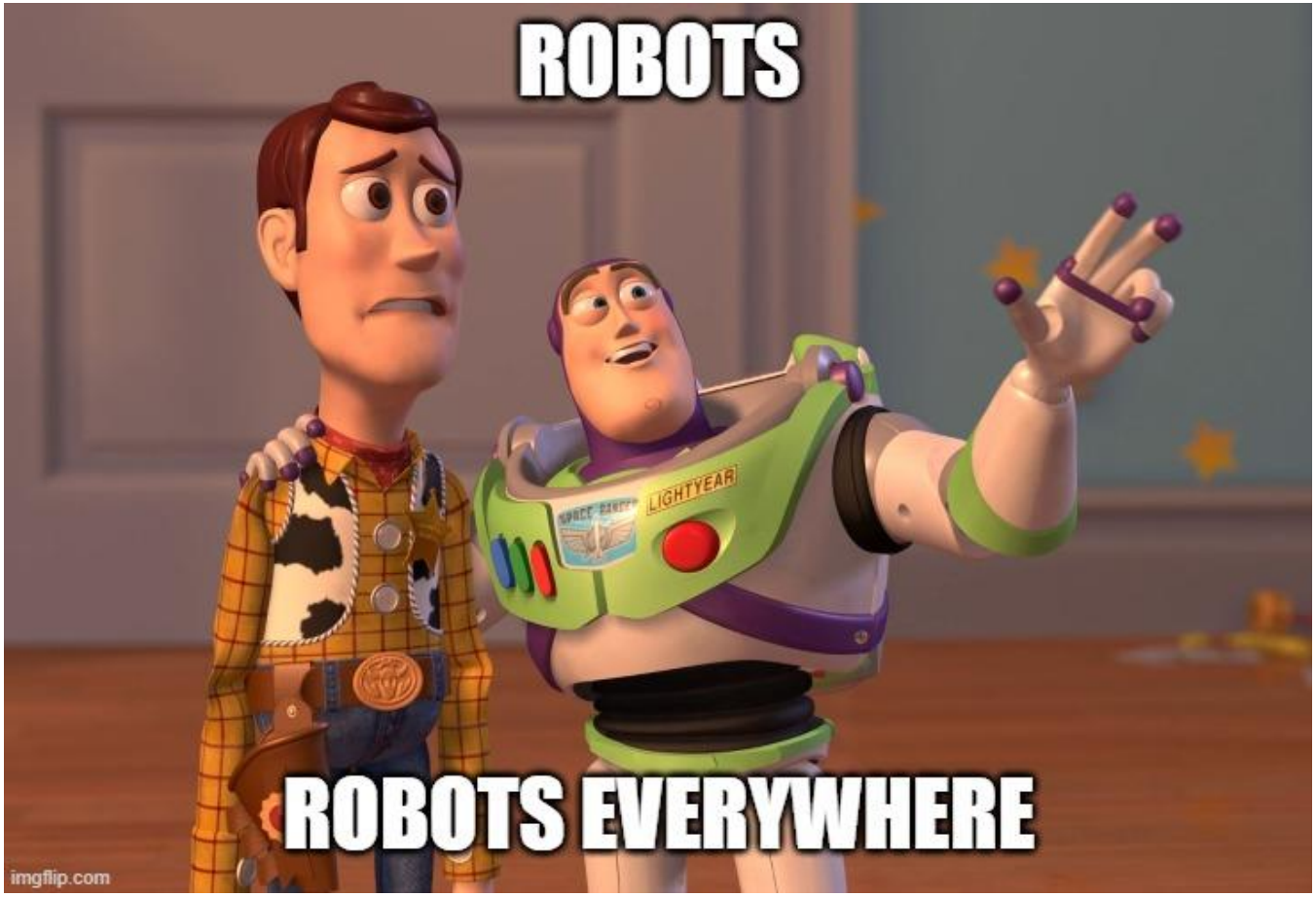
© 2020 CloudBees, Inc. All Rights Reserved.

```
<plugin>
  <artifactId>maven-enforcer-plugin</artifactId>
  <executions>
    <execution>
    ...
      <configuration>
        <rules>
          <enforceBytecodeVersion>
            <maxJdkVersion>1.8</maxJdkVersion>
            <ignoredScopes>
              <ignoredScope>test</ignoredScope>
            </ignoredScopes>
          </enforceBytecodeVersion>
    ...
  </executions>
  <dependencies>
  ...
    <artifactId>extra-enforcer-rules</artifactId>
  ...
```

© 2020 CloudBees, Inc. All Rights Reserved.

Автоматизация зависимостей?

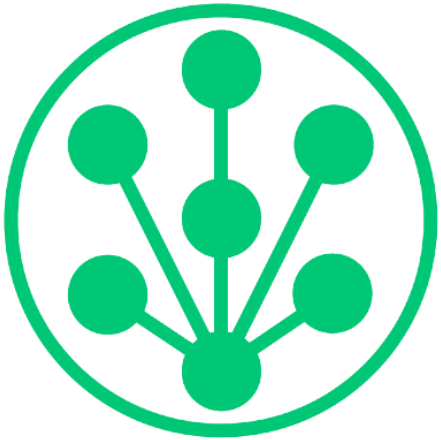
© 2020 CloudBees, Inc. All Rights Reserved.



https://github.com/marketplace

© 2020 CloudBees, Inc. All Rights Reserved.





Dependabot, Renovate, Greenkeeper, etc.

Dependabot

dependabot.com, acquired by GitHub

© 2020 CloudBees, Inc. All Rights Reserved.

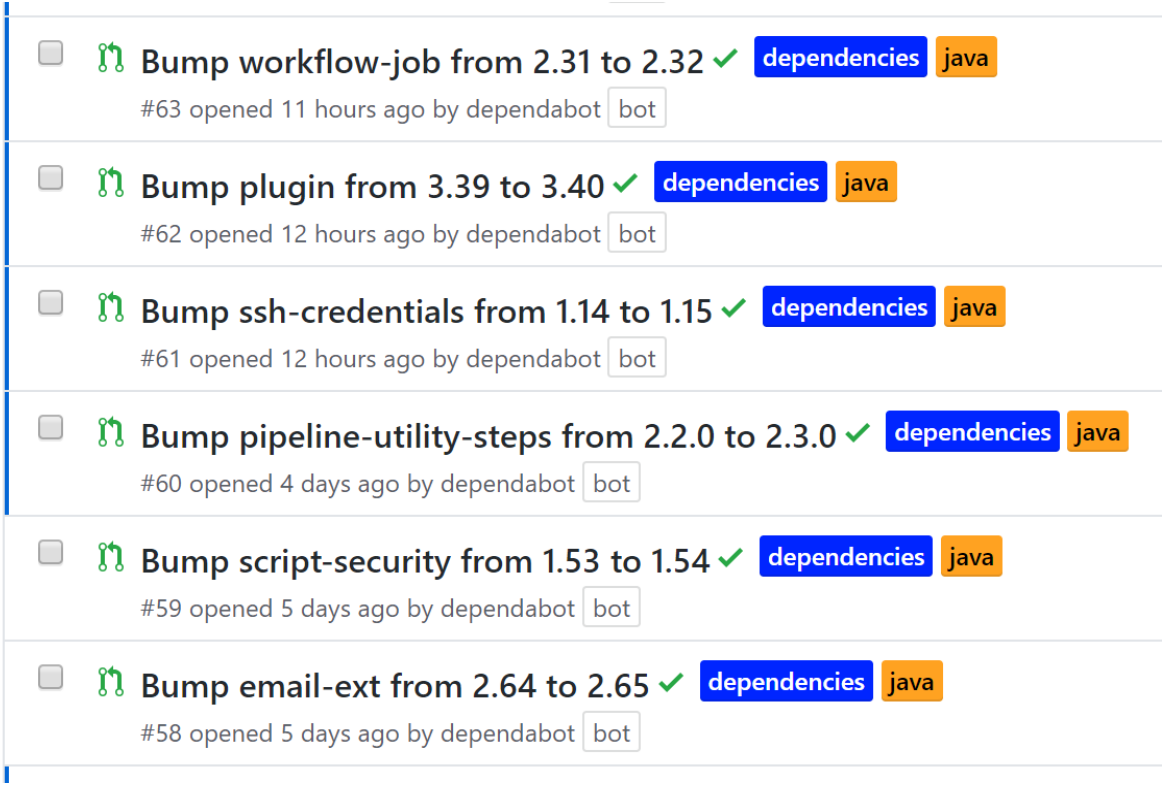
Dependabot

- CLI – для GitHub, GitLab и Azure DevOps
- SaaS + GitHub App

dependabot.com, acquired by GitHub

© 2020 CloudBees, Inc. All Rights Reserved.

Automatic scans and updates



© 2020 CloudBees, Inc. All Rights Reserved.

Ruby

JavaScript

Python

PHP

Elixir

Rust

Java - Maven
BETA

Java - Gradle
BETA

.NET
BETA

Go
ALPHA

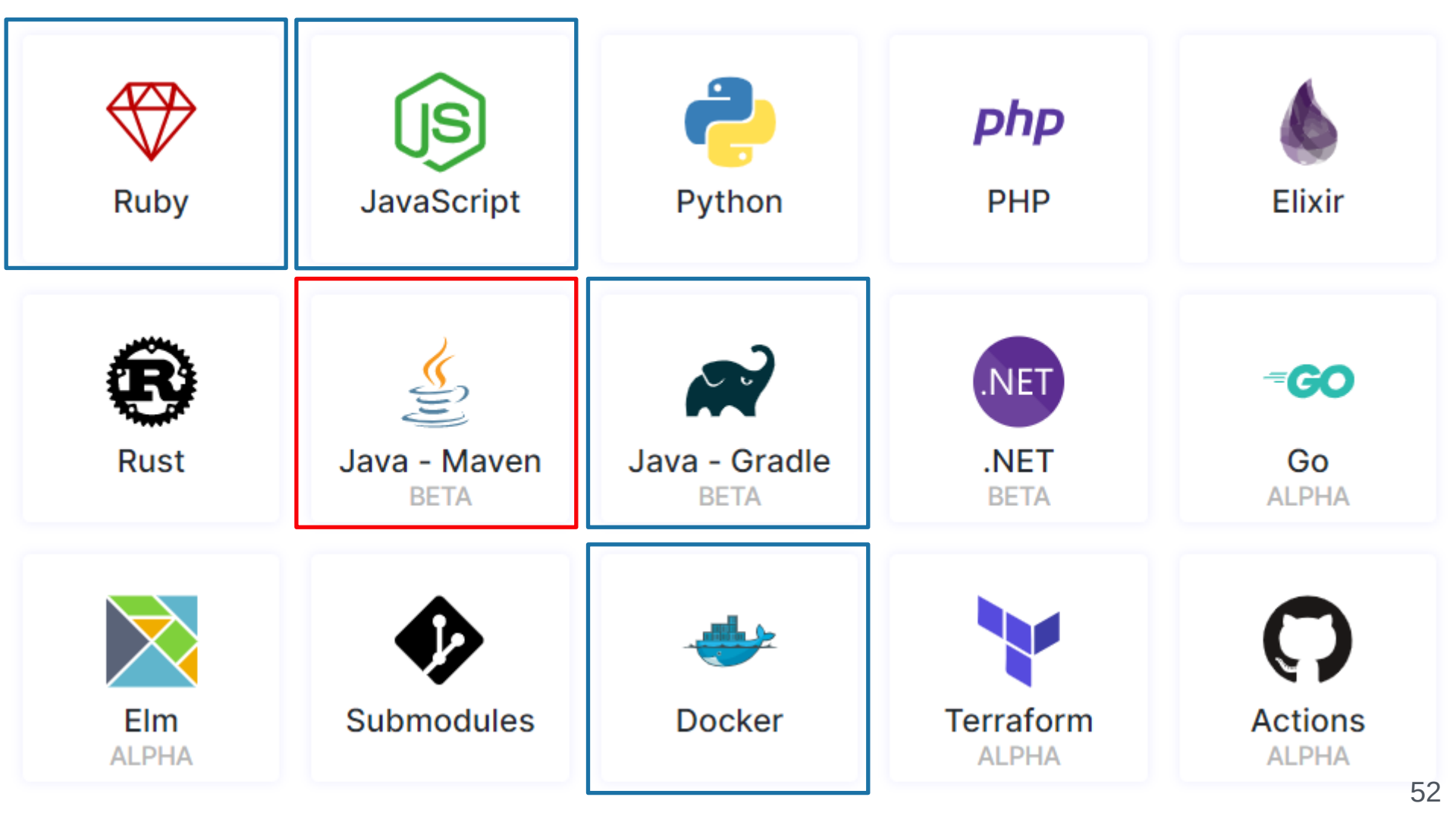
Elm
ALPHA

Submodules

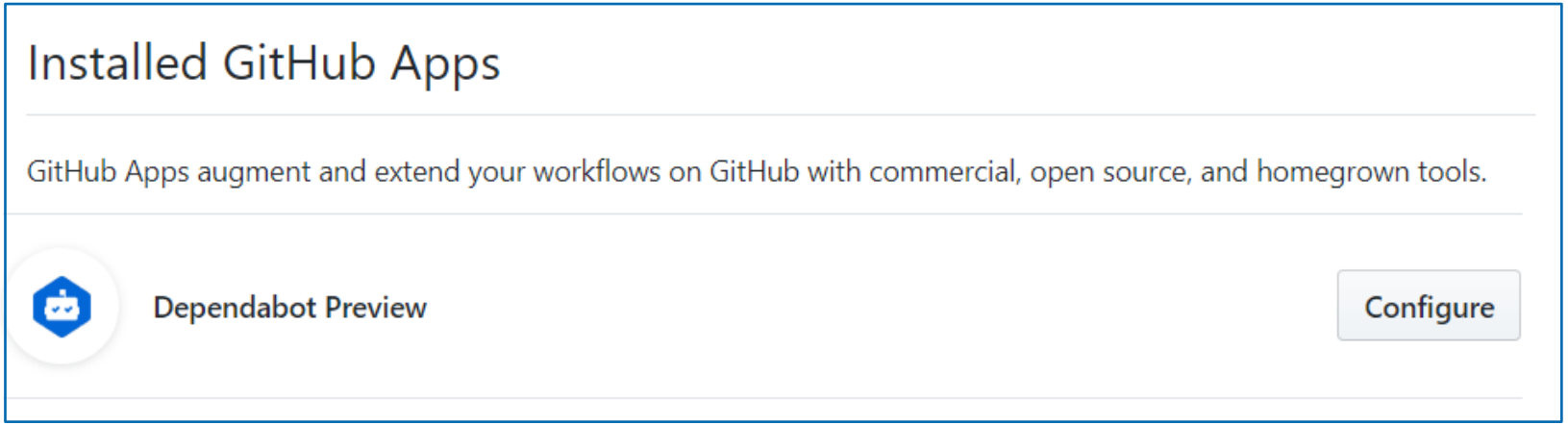
Docker

Terraform
ALPHA

Actions
ALPHA

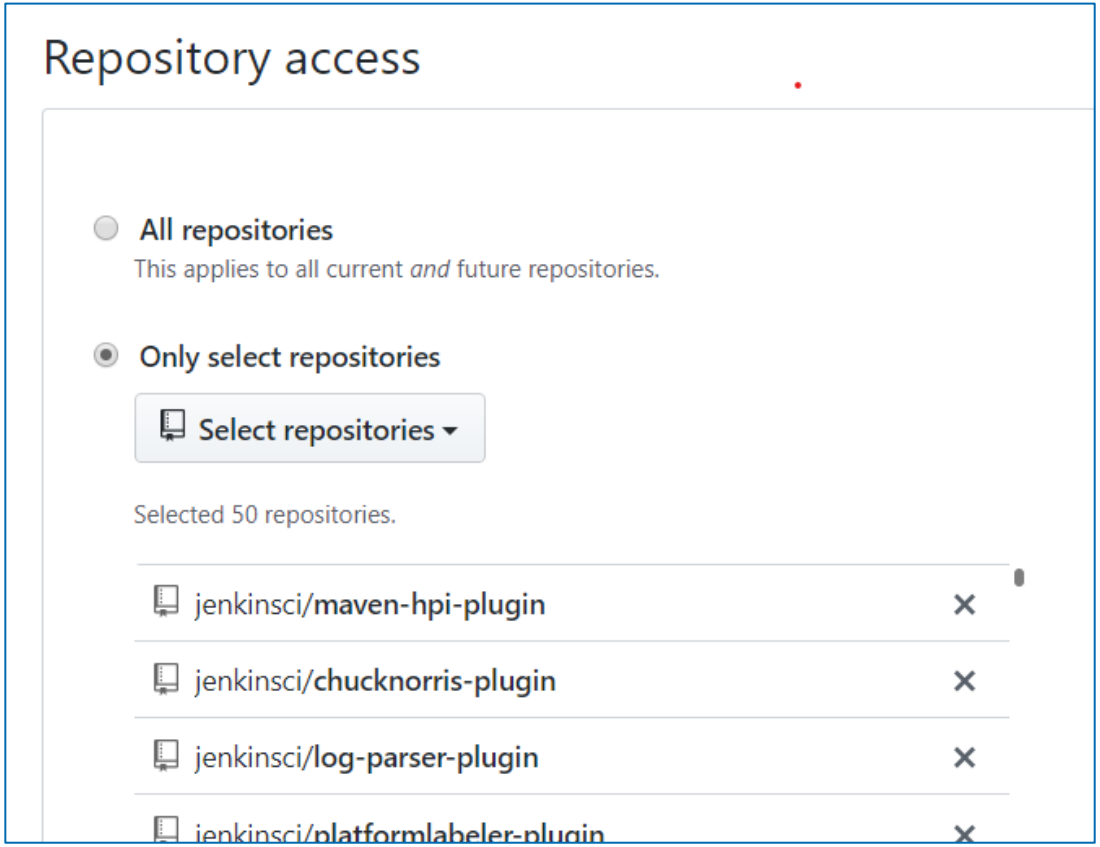

Ruby
JavaScript
Python
PHP
Elixir
Rust
Java - Maven
BETA
Java - Gradle
BETA
.NET
BETA
Go
ALPHA
Elm
ALPHA
Submodules
Docker
Terraform
ALPHA
Actions
ALPHA

War 1. Enable Dependabot



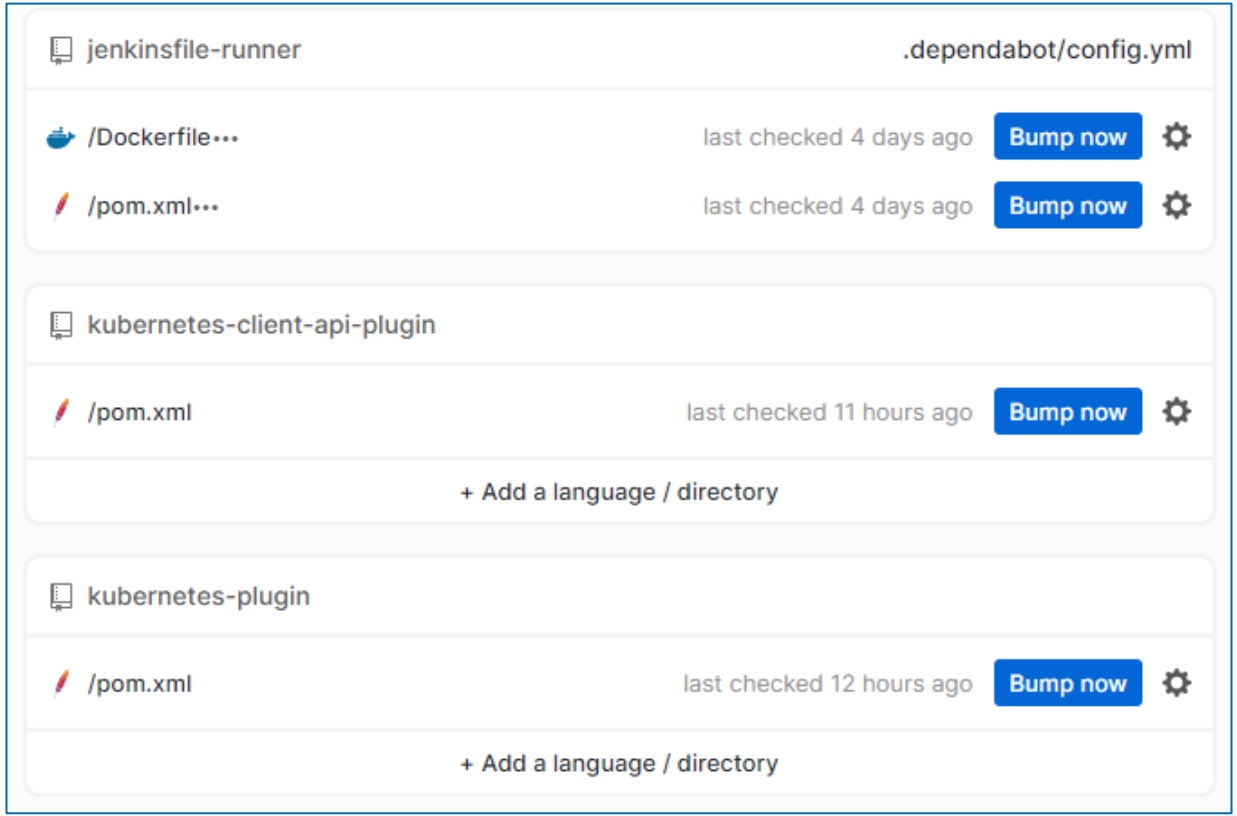
© 2020 CloudBees, Inc. All Rights Reserved.

Шаг 2. Доступ к репозиториям



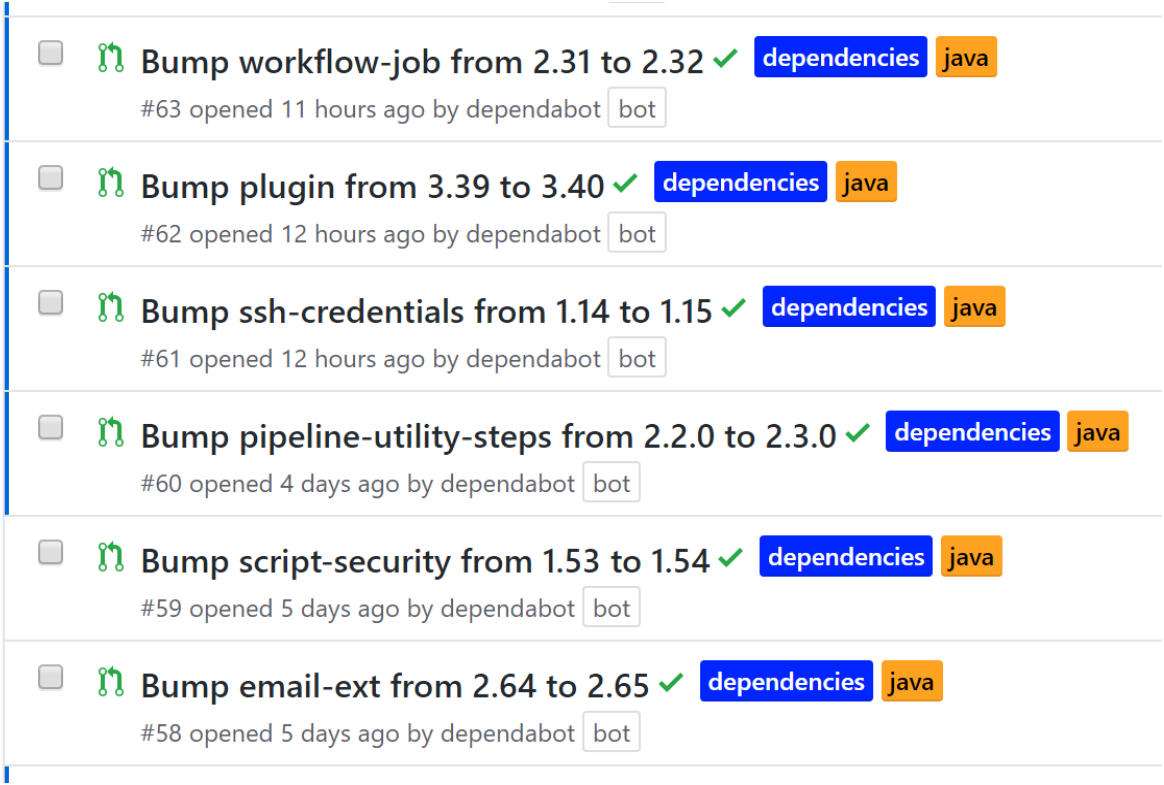
© 2020 CloudBees, Inc. All Rights Reserved.

Шаг 3. Настройка



© 2020 CloudBees, Inc. All Rights Reserved.

Шаг 4. Подождём...

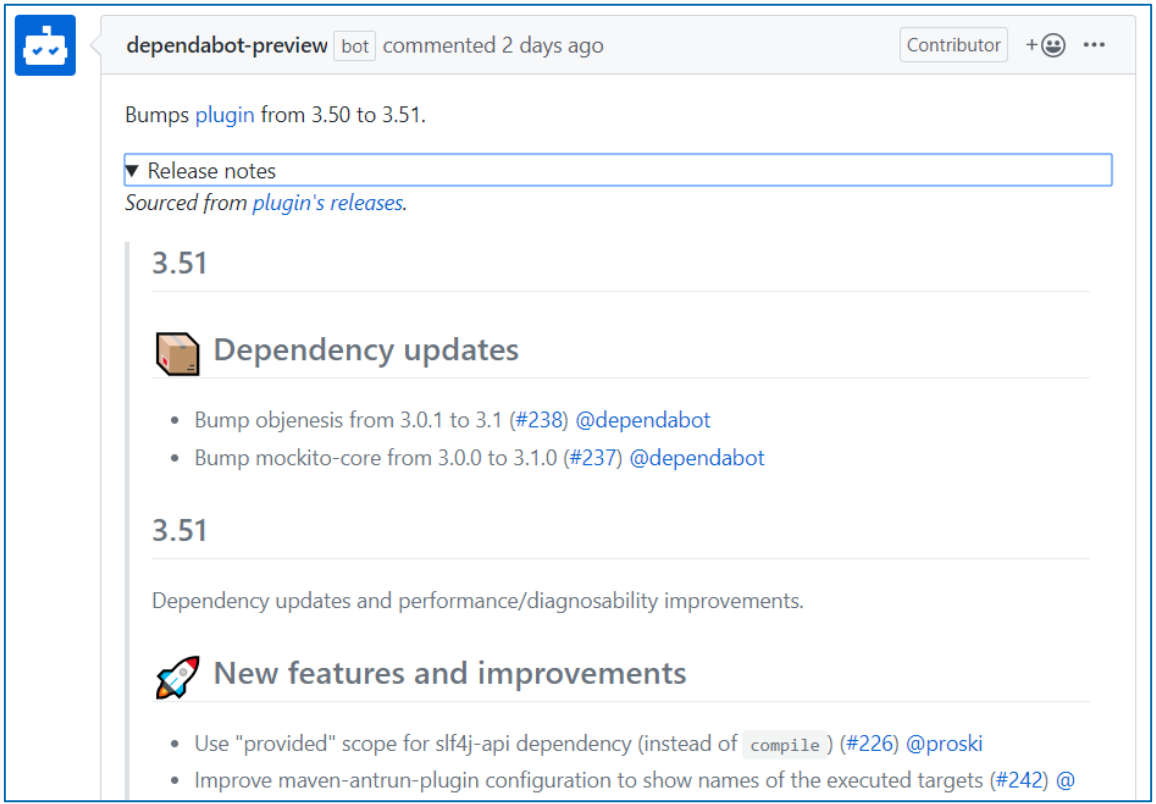


© 2020 CloudBees, Inc. All Rights Reserved.

Dependabot –
это не только pull request

© 2020 CloudBees, Inc. All Rights Reserved.

Release notes



dependabot-preview bot commented 2 days ago — Contributor

Bumps plugin from 3.50 to 3.51.

▼ Release notes

Sourced from plugin's releases.

3.51

Dependency updates

- Bump objenesis from 3.0.1 to 3.1 (#238) @dependabot
- Bump mockito-core from 3.0.0 to 3.1.0 (#237) @dependabot

3.51

Dependency updates and performance/diagnosability improvements.

New features and improvements

- Use "provided" scope for slf4j-api dependency (instead of `compile`) (#226) @proski
- Improve maven-antrun-plugin configuration to show names of the executed targets (#242) @

© 2020 CloudBees, Inc. All Rights Reserved.

CommentOps

▼ Dependabot commands and options

You can trigger Dependabot actions by commenting on this PR:

- `@dependabot rebase` will rebase this PR
- `@dependabot recreate` will recreate this PR, overwriting any edits that have been made to it
- `@dependabot merge` will merge this PR after your CI passes on it
- `@dependabot squash and merge` will squash and merge this PR after your CI passes on it
- `@dependabot cancel merge` will cancel a previously requested merge and block automerging
- `@dependabot reopen` will reopen this PR if it is closed
- `@dependabot ignore this [patch|minor|major] version` will close this PR and stop Dependabot creating any more for this minor/major version (unless you reopen the PR or upgrade to it yourself)
- `@dependabot ignore this dependency` will close this PR and stop Dependabot creating any more for this dependency (unless you reopen the PR or upgrade to it yourself)
- `@dependabot use these labels` will set the current labels as the default for future PRs for this repo and language

© 2020 CloudBees, Inc. All Rights Reserved.

Configuration-as-Code

Branch: master ▾ plugin-pom / .dependabot / config.yml

 oleg-nenashev Dependabot: Ignore slf4j

2 contributors  

23 lines (20 sloc) | 465 Bytes

```
1  version: 1
2  update_configs:
3  - package_manager: "java:maven"
4    directory: "/"
5    update_schedule: "weekly"
6
7    default_reviewers:
8      - "jglick"
9      - "oleg-nenashev"
10     - "batmat"
11
12   ignored_updates:
13     - match:
14         dependency_name: "jenkins-core"
15     - match:
16         dependency_name: "slf4j-api"
17     - match:
18         dependency_name: "log4j-over-slf4j"
```

© 2020 CloudBees, Inc. All Rights Reserved.

Продвинутые опции

Фильтрация артефактов

Фильтрация версий

```
ignored_updates:
  - match:
      dependency_name: "org.jenkins-ci.main:jenkins-core"
  - match:
      dependency_name: "org.jenkins-ci.plugins*"
      dependency_type: "production"
  - match:
      dependency_name: "io.jenkins.plugins*"
```

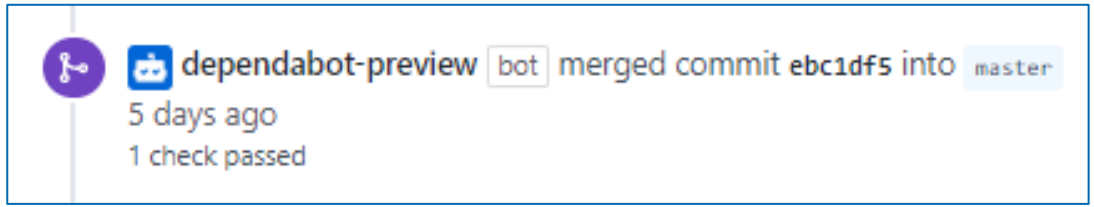
© 2020 CloudBees, Inc. All Rights Reserved.

Продвинутые опции

Фильтрация артефактов

Фильтрация версий

Validated merge



© 2020 CloudBees, Inc. All Rights Reserved.

Продвинутые опции

Фильтрация артефактов

Фильтрация версий

Validated merge

Интеграция с GitHub Security

dependabot bot commented on Nov 7, 2018

Bumps javax.servlet.jsp.jstl-api from 1.2.1 to 1.2.2. **This update includes security fixes.**

▼ Vulnerabilities fixed

Sourced from The Sonatype OSS Index.

> **[CVE-2015-0254] Apache Standard Taglibs before 1.2.3 allows remote attackers to**
> Apache Standard Taglibs before 1.2.3 allows remote attackers to execute arbitrary co
> external XML entity (XXE) attacks via a crafted XSLT extension in a (1) <x:parse> or (2
> JSTL XML tag.
>
> Affected versions: <= 1.2.1

▼ Commits

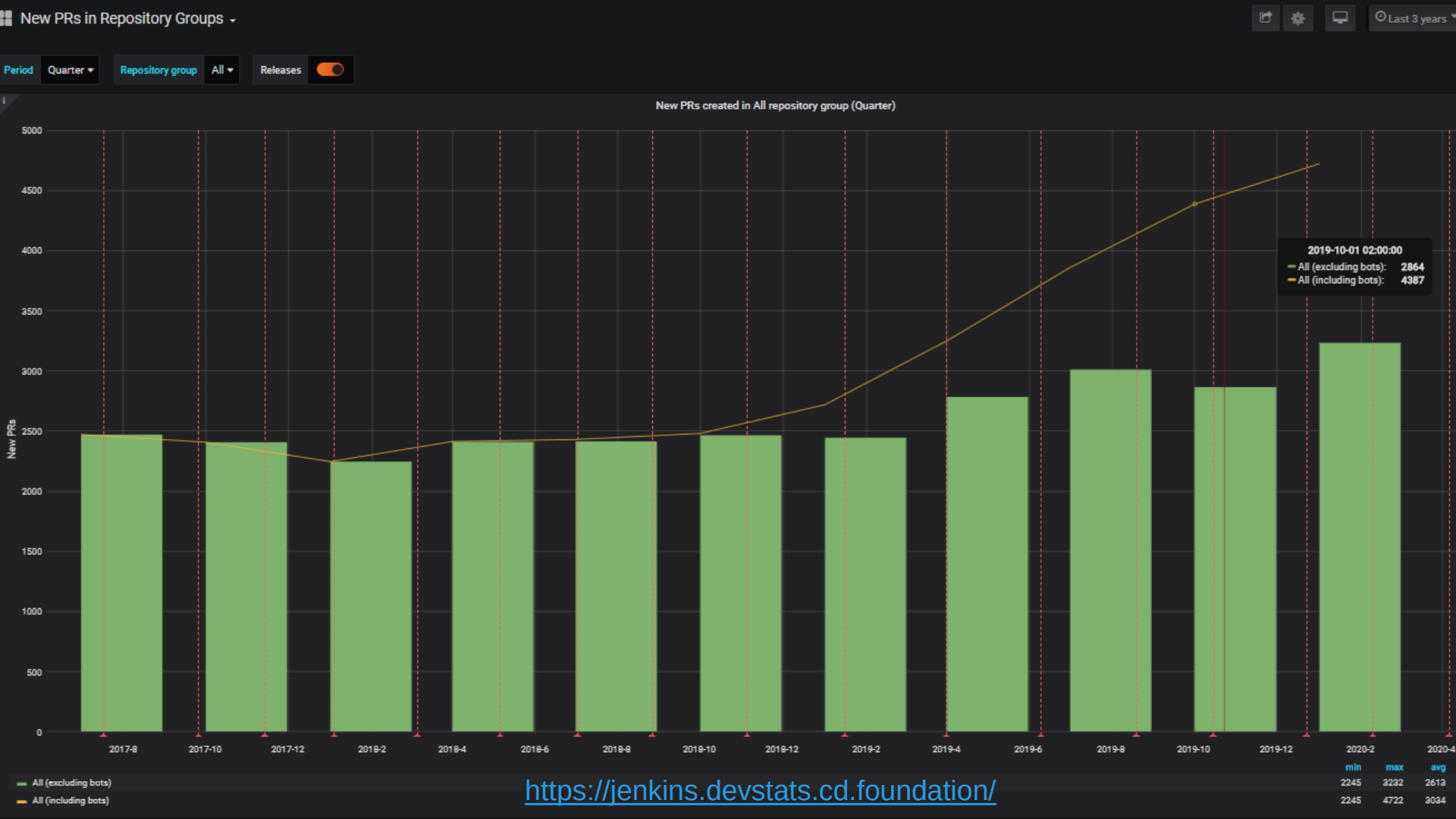
- `391fe91` [maven-release-plugin] copy for tag javax.servlet.jsp.jstl-1.2.2
- `65ef80a` [maven-release-plugin] prepare release javax.servlet.jsp.jstl-1.2.2
- `24294da` Some minor pom.xml fix
- `286e72a` Issue http://java.net/jira/browse/JSTL-7
- `6ce794c` [maven-release-plugin] prepare for next development iteration
- `c8373f6` [maven-release-plugin] prepare release javax.servlet.jsp.jstl-1.2.1
- `5f227bf` [maven-release-plugin] prepare for next development iteration
- See full diff in compare view

compatibility unknown

Dependabot в Jenkins

- Начали использовать в 2019
- 80+ репозиториев
- 4500+ pull requests
- Экономит время!

© 2020 CloudBees, Inc. All Rights Reserved.



https://jenkins.devstats.cd.foundation/

Стоимость CI/CD

Ресурсы для сборки

API rate limit

Время на ревью

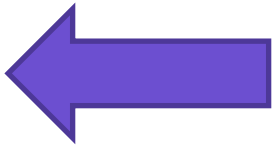
© 2020 CloudBees, Inc. All Rights Reserved.

Bill of Materials (BOM)

© 2020 CloudBees, Inc. All Rights Reserved.

BOM – “Библиотека зависимостей”

Наш проект



Зависимости и версии

Bill of Materials

- Версионирование
- Интеграционные тесты
- Анализ зависимостей

© 2020 CloudBees, Inc. All Rights Reserved.

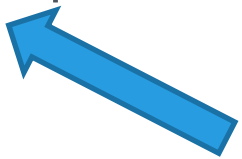
Включаем BOM в Maven

```
<dependencyManagement>
  <dependencies>
    <dependency>
      <groupId>${GROUP_ID}</groupId>
      <artifactId>${ARTIFACT_ID}</artifactId>
      <version>${VERSION_ID}</</version>
      <scope>import</scope>
      <type>pom</type>
    </dependency>
  </dependencies>
</dependencyManagement>
```

© 2020 CloudBees, Inc. All Rights Reserved.

Используем BOM в Maven

```
...
<dependency>
  <groupId>org.jenkins-ci.plugins.workflow</groupId>
  <artifactId>workflow-cps</artifactId>
  <scope>test</scope>
</dependency>
...
```



ВЕРСИИ НЕТ!

© 2020 CloudBees, Inc. All Rights Reserved.

Пример

https://github.com/jenkinsci/jenkins/tree/master/bom

https://github.com/jenkinsci/bom

© 2020 CloudBees, Inc. All Rights Reserved.

CI/CD – Pipeline of Pipeline

- Версионирование
- Интеграционные тесты
- Анализ зависимостей
- CI/CD

© 2020 CloudBees, Inc. All Rights Reserved.

Demo!

https://github.com/jenkinsci/jenkinsfile-runner

© 2020 CloudBees, Inc. All Rights Reserved.

Заключение

- От апдейта не убежишь
- Зависимости - отличная возможность прочувствовать технический долг
- Обновляться лучше постоянно
- Есть средства разработки

© 2020 CloudBees, Inc. All Rights Reserved.

Что Вы можете сделать после доклада?

Добавьте Maven Enforcer и правила в свой проект

Попробуйте Dependabot или подобные тулы

© 2020 CloudBees, Inc. All Rights Reserved.

ВОПРОСЫ?

Contacts:

E-mail: onenashev@cloudbees.com

GitHub: oleg-nenashev

Twitter: @oleg_nenashev

© 2020 CloudBees, Inc. All Rights Reserved.