Koda : Forge pour les laboratoires

Présentation de Koda, la forge pour les laboratoires

JoSy, Septembre 2021

DIRECTION DES SYSTEMES D'INFORMATION CNRS | Stéphane Deraco | stephane.deraco@dsi.cnrs.fr

0

Sommaire de présentation

1

Forge Logicielle ?

1

Objectifs d'une forge logicielle

- **Gestion du code source**
  - Historisation
  - Travail collaboratif
- **Construction du projet (= « build », « intégration continue »)**
  - Génération automatique des binaires
  - Lancement des tests unitaires
  - Reproductibilité de la construction de l'application
    - "L'intégration continue est le principe de faire d'un processus d'intégration logicielle un «non-évènement»." (Martin Fowler)
- **Stockage des artéfacts générés**
  - Stockage du résultats du build (binaires exécutables, PDF, zip, …)
  - Gestion des dépendances
- **Analyse de la qualité du code**
  - Suivi de l'évolution de la qualité du code dans le temps

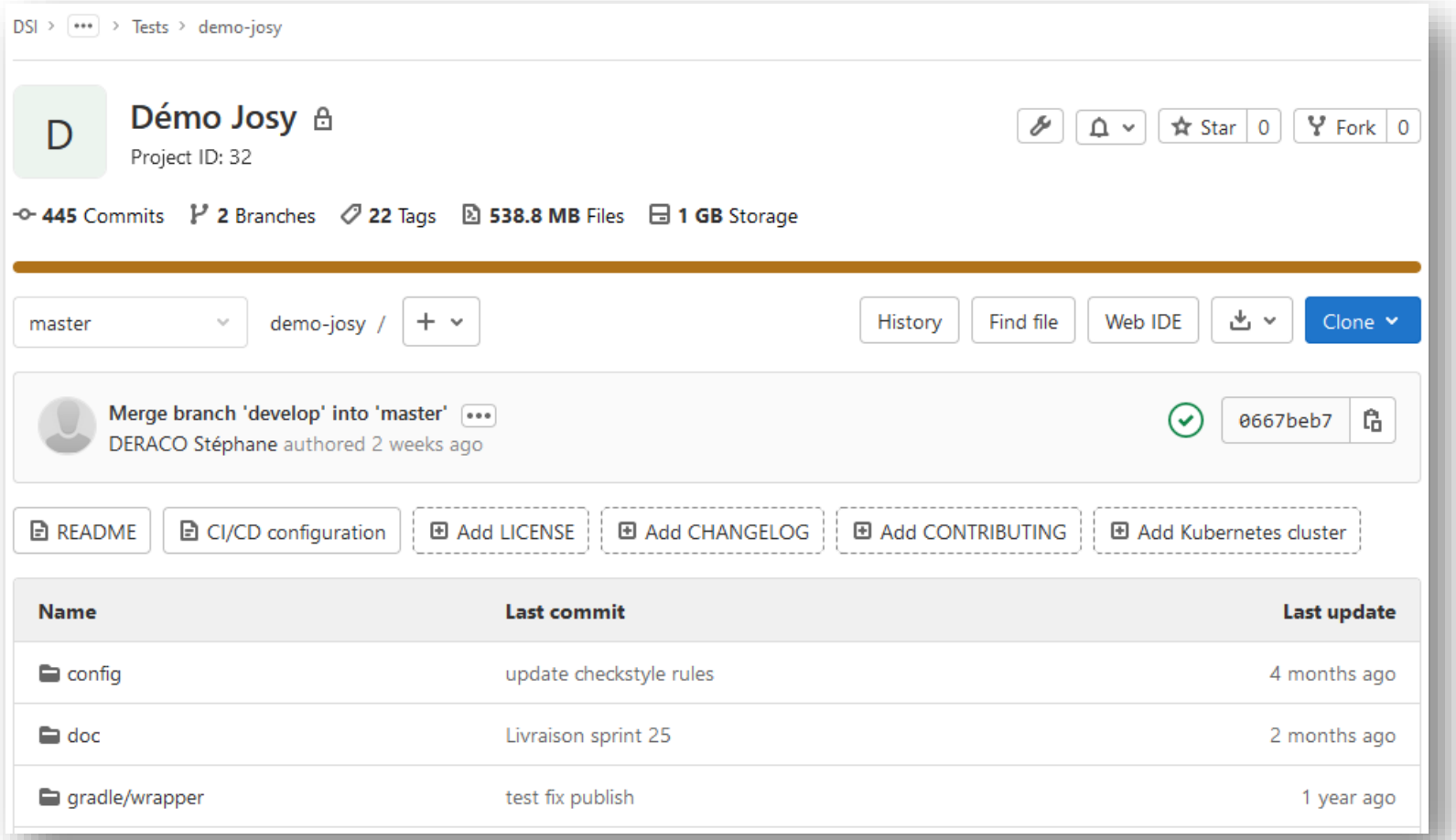
1

Historique

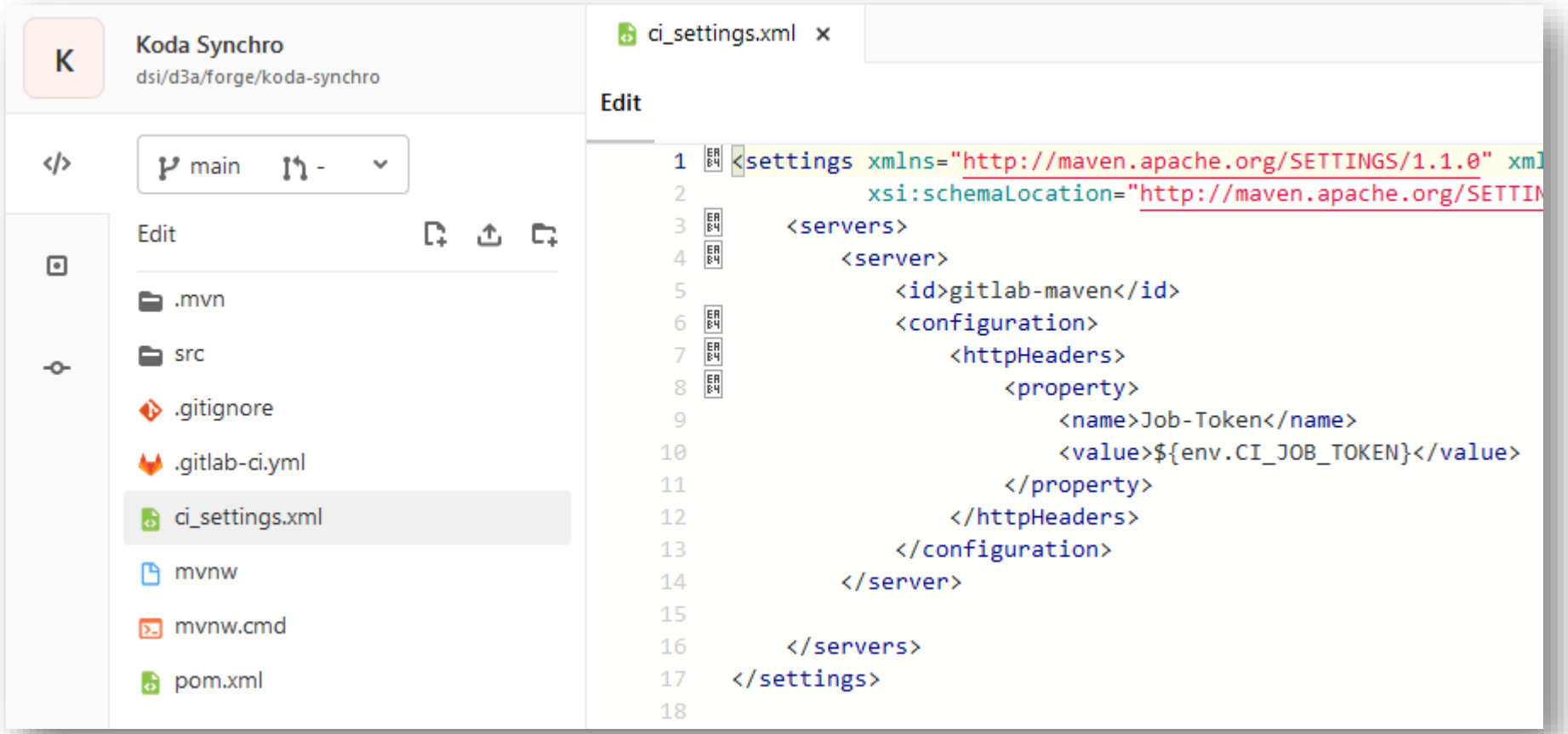
- **Utilisation d'une forge par la DSI depuis plus de 10 ans**
  - CVS
  - Subversion (2012), Git (2013) avec annuaire LDAP dédié
  - Puis Hudson (→ Jenkins) pour les builds
  - Et Nexus pour le stockage des artéfacts (et proxy Maven)
- **2021 → Mise à niveau de la forge DSI**
  - Gitlab
    - Code source
    - Build
    - Artéfacts
  - Sonar
  - Pour le personnel de la DSI et des SSI des délégations régionales

1 Exemples

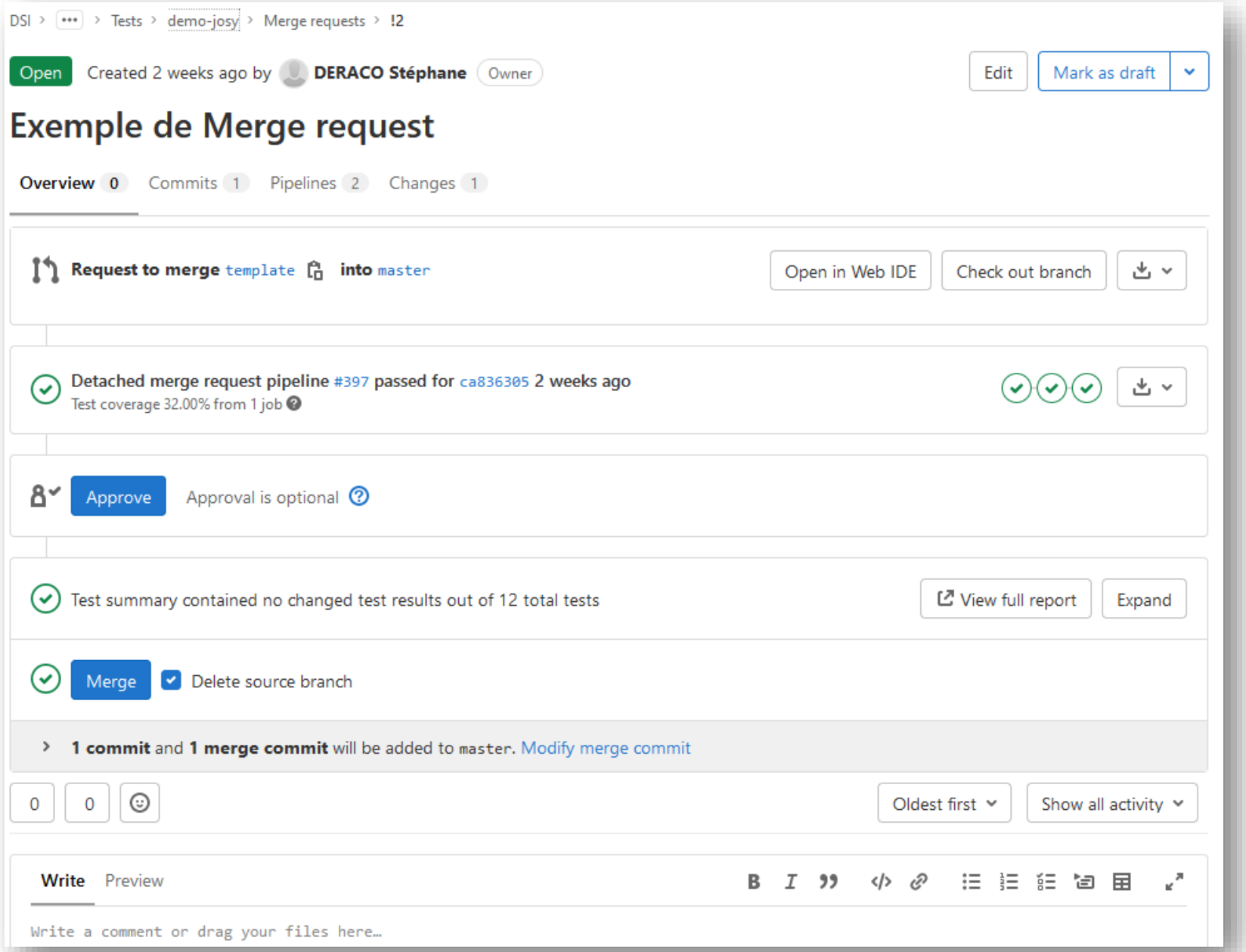
- **Code source : Gitlab**



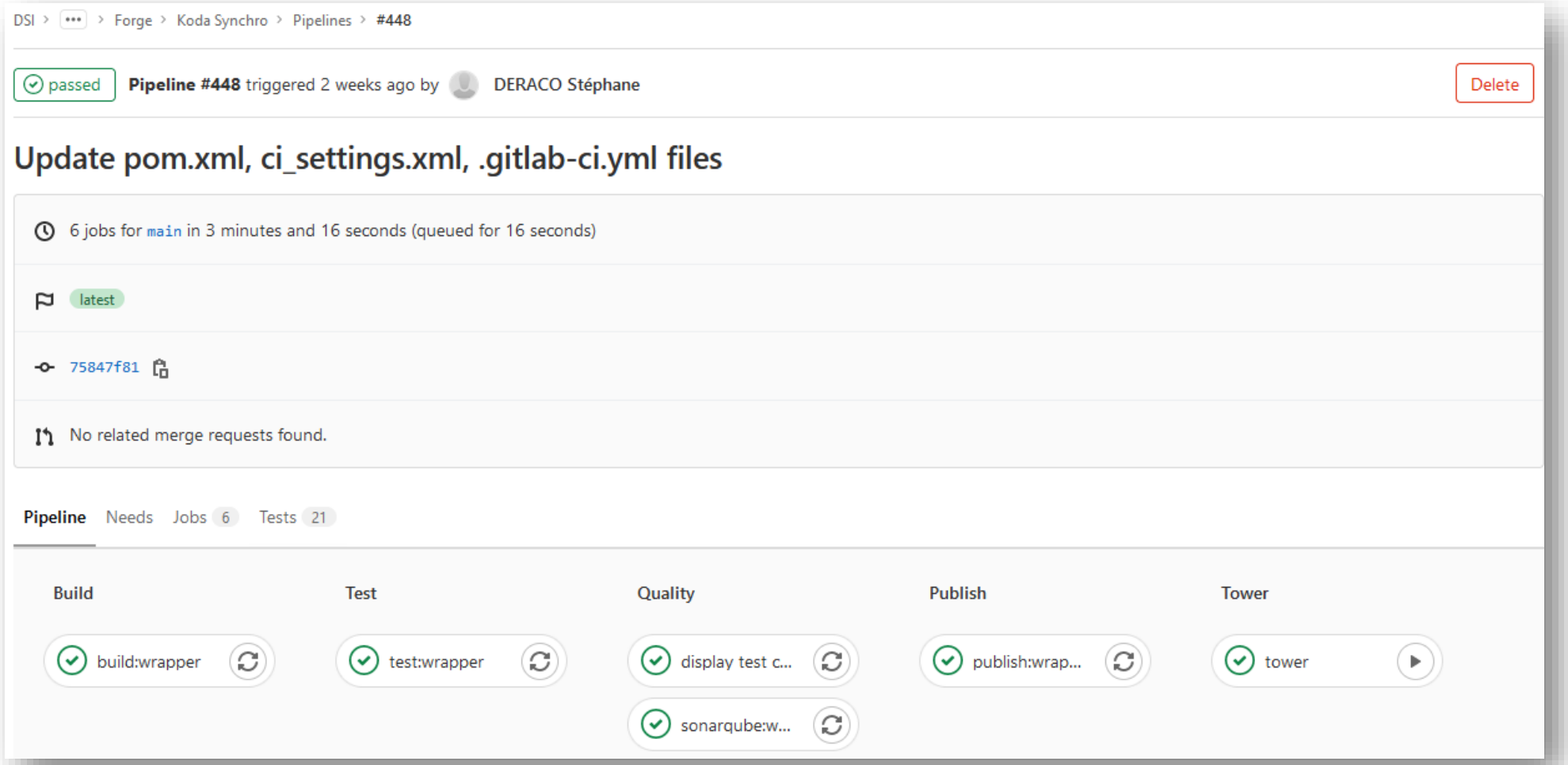
1


K
Koda Synchro
dsi/d3a/forge/koda-synchro
main
-
Edit
.mvn
src
.gitignore
.gitlab-ci.yml
ci_settings.xml
mvnw
mvnw.cmd
pom.xml
ci_settings.xml
Edit
1 <settings xmlns="http://maven.apache.org/SETTINGS/1.1.0" xml
2 xsi:schemaLocation="http://maven.apache.org/SETTIN
3 <servers>
4 <server>
5 <id>gitlab-maven</id>
6 <configuration>
7 <httpHeaders>
8 <property>
9 <name>Job-Token</name>
10 <value>${env.CI_JOB_TOKEN}</value>
11 </property>
12 </httpHeaders>
13 </configuration>
14 </server>
15
16 </servers>
17 </settings>
18

1


DSI › ••• › Tests › demo-josy › Merge requests › !2
Open
Created 2 weeks ago by DERACO Stéphane
Owner
Edit
Mark as draft
Exemple de Merge request
Overview 0
Commits 1
Pipelines 2
Changes 1
Request to merge template into master
Open in Web IDE
Check out branch
Detached merge request pipeline #397 passed for ca836305 2 weeks ago
Test coverage 32.00% from 1 job
Approve
Approval is optional
Test summary contained no changed test results out of 12 total tests
View full report
Expand
Merge
Delete source branch
1 commit and 1 merge commit will be added to master. Modify merge commit
0
0
Oldest first
Show all activity
Write
Preview
Write a comment or drag your files here…

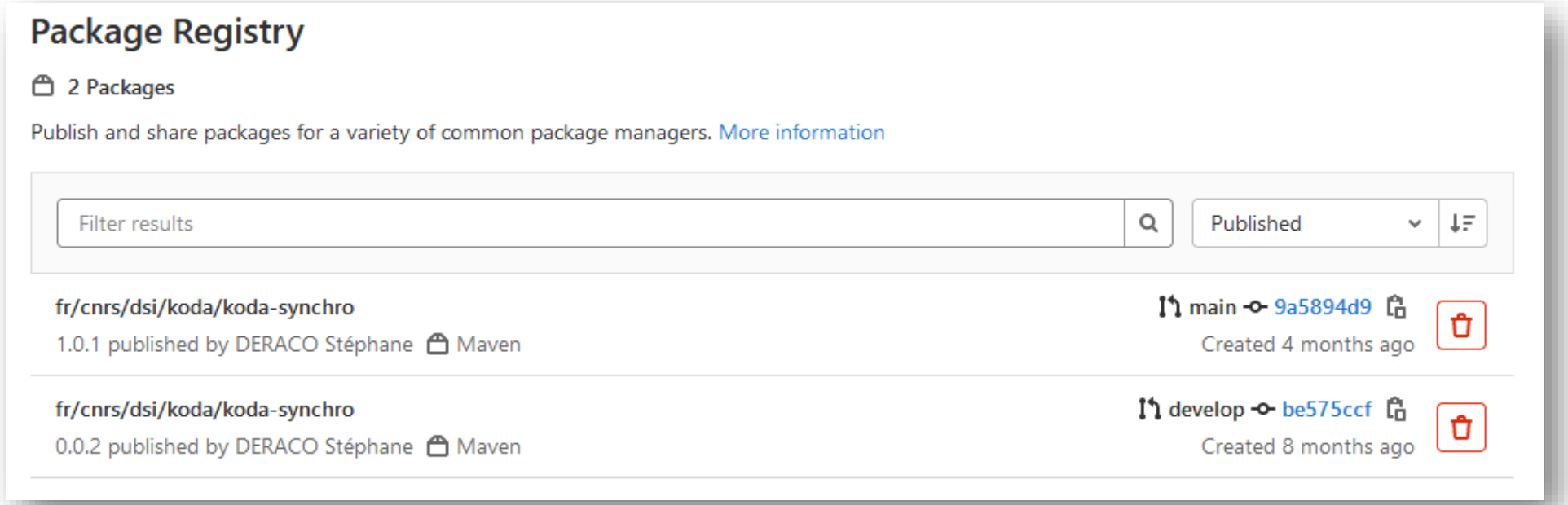
• Intégration continue : Gitlab CI



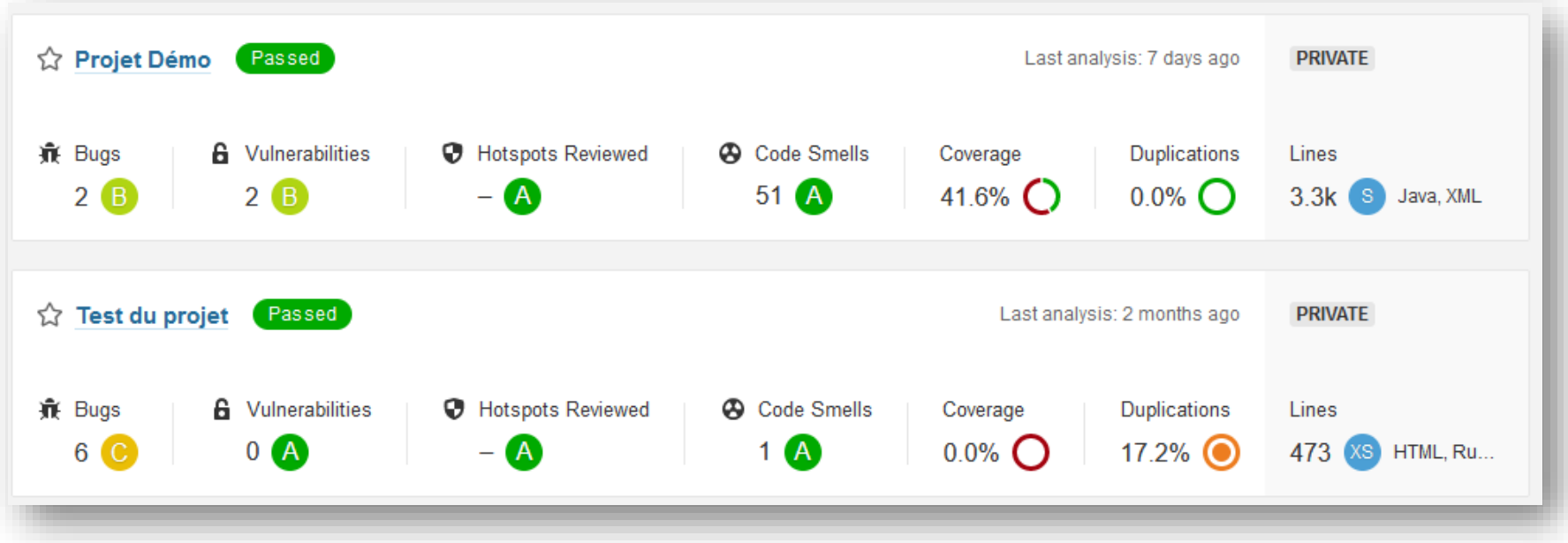
1


passed
#395
latest
master 0667beb7
Merge branch 'develop' into...
00:09:55
2 weeks ago
passed
#394
latest
detached
1 4ecbcdbf
Déduplication
00:08:03
2 weeks ago
passed
#393
detached
1 e26eae7f
Ajout env
00:07:22
2 weeks ago

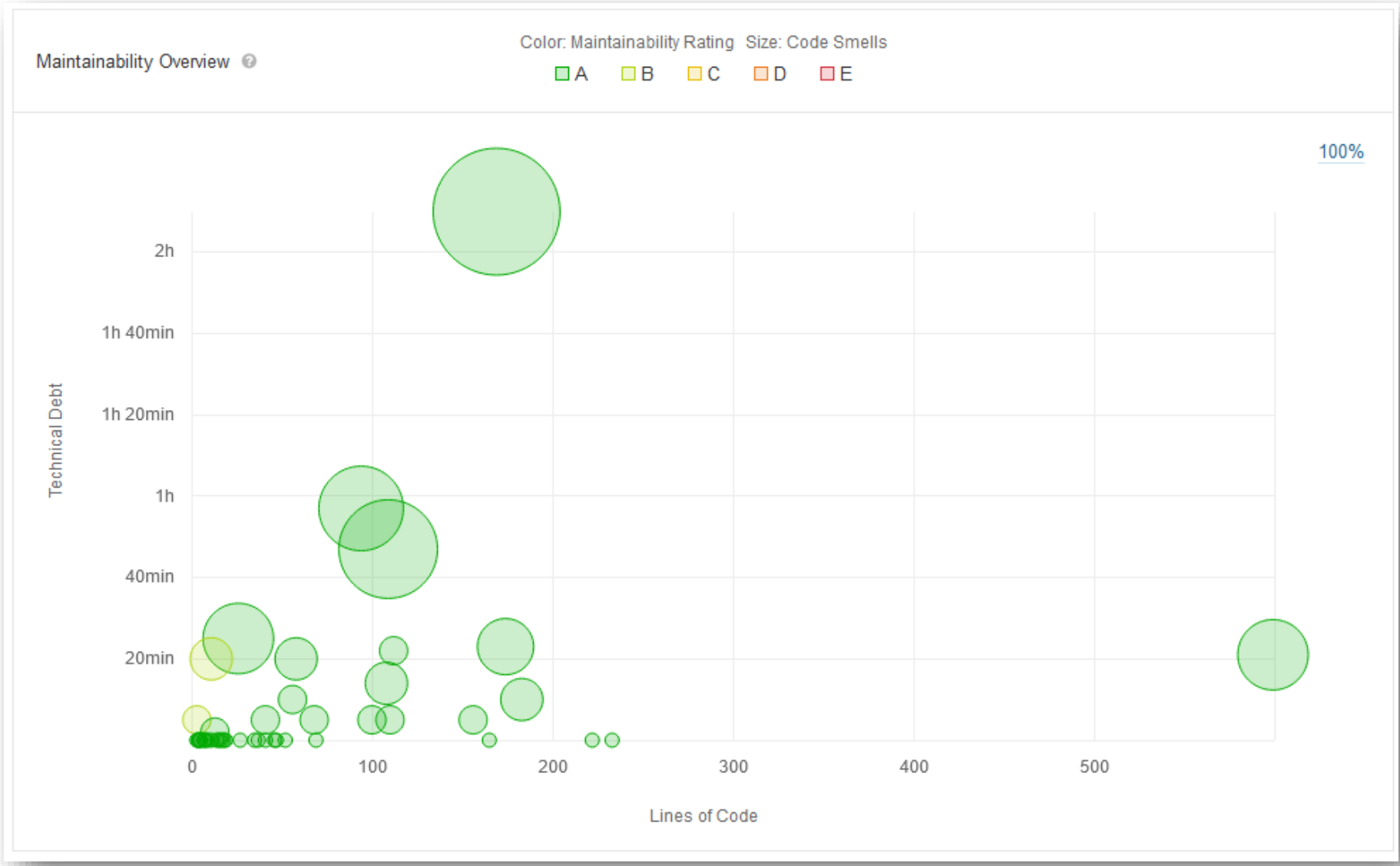
• Stockage d'artéfacts : Gitlab



• Analyse statique de code : Sonarqube

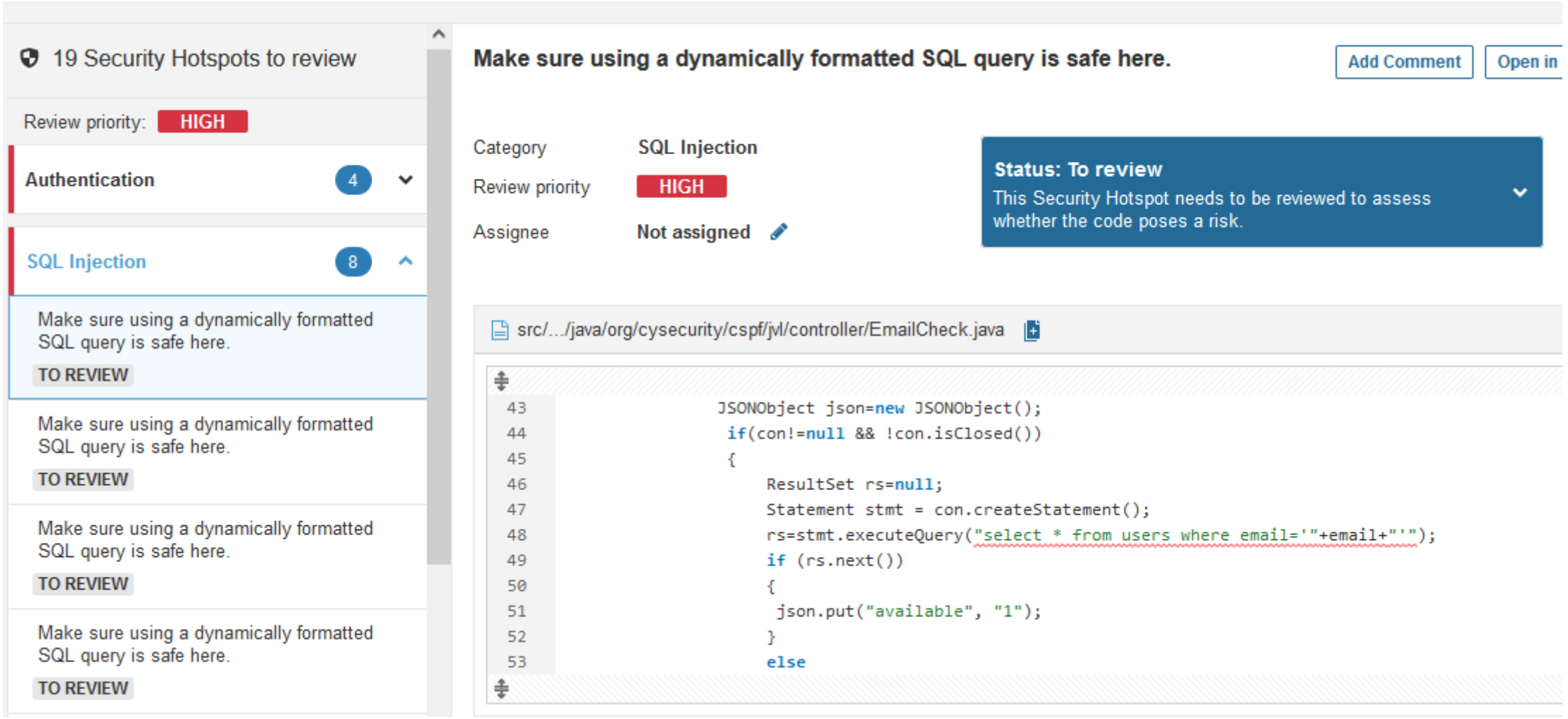


1


Maintainability Overview
Color: Maintainability Rating Size: Code Smells
A B C D E
100%
2h
1h 40min
1h 20min
1h
40min
20min
Technical Debt
0
100
200
300
400
500
Lines of Code

1

https://github.com/CSPF-Founder/JavaVulnerableLab



1

Démarche DSI

- **Beaucoup de demandes d'utilisation de la forge DSI par des personnels en laboratoire**
  - Les aspects techniques et organisationnels ne permettaient pas d'y répondre favorablement jusqu'à présent
  - Mais le besoin n'a pas été oublié
- **Entretiens avec des labos entre fin 2019 et mi 2021 pour identifier au mieux les besoins**
  - Confirmation du besoin pour une forge « institutionnelle » CNRS

2

Fonctionnalités / outils prévue pour la Forge labos

2 Gestion du code source

- **Gitlab**
  - Version Community Edition
  - Logiciel connu et reconnu
  - Beaucoup de fonctionnalités
  - Git over HTTPS ✅
  - Git over SSH : à l'étude ❓
  - Wiki ✅
  - Issues ✅

2 Intégration continue

- **Gitlab CI**
  - Jenkins était une piste, mais gestion des droits plus compliquée
  - Des runners à disposition (RHEL + docker)
    - Toujours possible de monter son propre runner
    - Restrictions sur les flux de sortie (en réflexion) :
      - Via proxy squid avec allow-list
      - Via un gestionnaire d'artéfacts dédiés = Artifactory
    - Déjà ouvert pour les outils les plus communs : Maven Central, Pypi, Packagist, Npm, Github, Gitlab, Docker Hub, … (plus d'autres à définir comme CPAN, CRAN, …)
    - → Ticket e-dem à faire si nouveau besoin (validation par équipe sécurité)
  - Images Docker : allow-list également (éviter des images potentiellement malicieuses)

2 Stockage des artéfacts

- **A priori : Artifactory**
  - On peut stocker des artéfacts dans Gitlab
    - + : gestion des droits liée à celle du projet Gitlab
    - - : dans Gitlab CE, on n'a pas toutes les fonctionnalités
  - Licence Artifactory Pro (1 serveur)
    - Artifactory OSS gère uniquement Maven, Gradle et Ivy
    - Artifactory Pro gère en plus Bower, Chef, Cocoa, Conan, Debian, Docker, Git LFS, NPM, Nuget, PHP Composer, Puppet, Pypi, RPM, Rubygems, Vagrant, …
- **Problématique sur le volume**

2 Analyse de la qualité du code

- **Sonarqube**
  - Version Community Edition
  - Suivi d'une branche du projet (recommandé)
  - Analyse statique du code pour différents langages
    - Bonnes pratiques
    - « code smell » (variables non utilisées, condition du if toujours true, …)
    - Points bloquants/critiques
    - Problèmes de sécurité (SQL Injection, Command Injection, mots de passe en clair, …)
    - Suivi de l'évolution de ces critères
  - Possibilité de mettre en place une « Quality Gateway » pour s'assurer que le nouveau code commité respecte les critères de qualité (et ne dégrade pas la qualité du projet)
- **Depuis Gitlab CI**
  - Possibilité d'appeler Sonar et d'attendre la Quality Gateway pour continuer le build ou non

3

Utilisateurs identifiés

3

Qui aura accès

- **Entretiens avec des labos**
  - Des besoins différents et parfois antagonistes
    - Forge la plus ouverte possible
    - vs projets sensibles et confidentiels
- **Décision de s'orienter vers 2 forges**

	Forge « ouverte »	Forge « sécurisée »
Population	Janus (+ UHPI et ext)	Janus
Authentification	Janus	MFA (clé Yubikey)
Visibilité des projets	Interne par défaut	Privé par défaut
Visibilité max. possible	Publique	Interne
Runners	Dédiés	Dédiés (distincts des autres)
Mises à jour (OS, composants)	Standard	ASAP

3

MFA = Multi-Factor Authentification

- **Objectif : renforcer l'authentification**
- **Clé FIDO, type Yubikey**

⚠ Modèles de clés autorisés : à l'étude

- Login = « ce que je suis »
- Mot de passe = « ce que je sais »
- **Clé = « ce que je possède »**

4

Autres fonctionnalités

4 Fonctionnalités supplémentaires

- **Gitlab**
  - Wiki
  - Issues / milestones
  - Étude de faisabilité
    - mattermost intégré à Gitlab
    - Gitlab Pages
- **Sécurité**
  - A l'étude !
  - OWASP Dependency-Track (https://dependencytrack.org/)
    - Analyse des dépendances obsolètes / vulnérables
    - Proposition de mise à jour dans une merge-request

5

Organisation

5 Technique

- **Serveurs hébergés à l'IN2P3**
- **Gitlab**
  - 2 instances de Gitlab-Rails
  - base PG dédiée
  - stockage git dédié (Gitaly)
  - serveur Redis dédié

5 Humaine

- **Opéré par la DSI**
- **Taux de Disponibilité, support**
  - Mode Best Effort
- **Demandes d'accès, création de comptes, …**
  - Automatique à l'authentification
- **Communauté**
  - Liste Sympa : koda@services.cnrs.fr

6

Planning

6 Planning prévisionnel

- **(non contractuel ;)**
- **Forge « ouverte »**
  - Fin 2021 : Accès Gitlab de base
  - T1 2022 : Ajout Sonar
  - T1 2022 : Ajout Artifactory
  - T1/T2 2022 : Si possible : mattermost
  - T2 2022 : Si possible Gitlab Pages
- **Forge « sécurisée »**
  - Nécessite de l'organisation sur l'enrôlement des clés FIDO
  - T1 2022 : Accès Gitlab de base
  - T2 2022 : Accès Sonar + Artifactory

7

Mot de la fin

7

- **Ces services seront gratuits**
- **La DSI CNRS fait son maximum pour répondre à ces besoins**
  - Mais pas d'équipe **dédiée** « Forge »

- **Si des labos souhaitent être pilotes :**
  - dsi.forge2@cnrs.fr

7

Merci !

Questions ?