

GIT repo ja CI/CD seadistamise juhend

Näidis ehitusplaan: <https://source.smit.sise/projects/EXAMPLES/repos/bookstore-backend>

Näidis paigaldus: <https://source.smit.sise/projects/EXAMPLES/repos/bookstore-backend-deploy/browse>

Jrk	Kirjeldus
1.	<p>Rakenduse lähtekood koos pipeline koodiga peab asuma meeskonna GIT projekti all (projekti formaat MSKXX). Eraldi rakendusepõhiseid GIT projekte ei looda. Projekti õigustes tohivad olla ainult SMIT meeskonna grupid ning sinna mitte lisada otse isikuid ega väliste partnerite gruppe (project permissions). Meeskonna grupid eristada kirjutamise, haldamise ja lugemise vaatest.</p> <p>Projekti all tuleb defineerida harude õiguste skeem (branch permissions) "main master" ja "develop" harudele:</p> <p>Prevent all changes: true (exceptioni alla määrata meeskonna x grupp, kellel on õigus sinna harusse muudatusi teha, näiteks: x_smit_bitbucket_euro_user) Prevent deletion: true Prevent rewriting history: true Prevent changes without a pull request: true</p> <p>Antud kitsendustega tagame, et harudele, mille pealt ehitatakse tulemeid test ja toodangukeskkondadesse või hallatakse paigaldusplaane, saab muudatusi teha ainult SMIT töötajatest meeskonna liikmed. Kui meeskond kasutab git-flow põhist lähtekoodi halduse protsessi, tuleb samad kitsendused määrata kõikidele "release hotfix" harudele.</p> <p>Projekti all seadistada koodi mestimise reeglid (merge checks):</p> <p>Minimum approvals: 1 Minimum successful builds: 1 No 'changes requested' status: true No incomplete tasks: true</p> <p>Konkreetselt rakenduse repole lisada eraldi write õigustes külge välise partneri õigusgrupp.</p> <p>Feature branched tuleb ära kustutada peale pullrequesti mergemist, selle toiminguga lihtsustamiseks palun aktiveerida vastav vöti:</p> <p>Workflow Branches Branch deletion on merge: On</p> <p>BitBucket > MSKxx > Project settings > Jira issues</p> <ul style="list-style-type: none">▪ Select how to verify Jira issues in commit messages: Must contain a Jira issue key that exists in Jira

Ekraanipildid

The image displays four screenshots of the BitBucket web interface, showing various configuration options for a project.

Branch deletion on merge

Set the default for deleting the source branch after merging a pull request.

Default

- ☐ Off - do not delete source branch on merge
- ☒ On - delete source branch on merge

Save Cancel

Merge checks

Merge checks can improve code quality by setting restrictions about when pull requests can be merged. Merge checks are installed by system administrators and can be enabled for all repositories in the workspace or disabled for each individual repository. [Learn more about merge checks.](#)

Title	Status
All reviewers approve Require all reviewers to approve the pull request.	DISABLED
Minimum approvals Require at least the specified number of approvals.	ENABLED
Minimum successful builds Require at least the specified number of successful builds.	ENABLED
No 'changes requested' status Block the merge if any reviewers have requested changes.	ENABLED
No incomplete tasks Require all tasks to be complete.	ENABLED

Branch permissions

With branch permissions you can control the actions users can perform on a single branch, branch type or branch pattern. [Learn more](#)

Branch	Prevent	Exemptions
develop Development branch from branching model	<input checked="" type="checkbox"/> Rewriting history <input checked="" type="checkbox"/> Deletion <input checked="" type="checkbox"/> Changes without a pull request	
main Production branch from branching model	<input checked="" type="checkbox"/> Rewriting history <input checked="" type="checkbox"/> Deletion <input checked="" type="checkbox"/> Changes without a pull request	<input checked="" type="checkbox"/> x_smit_bitbucket_euro...
release/ Release branches from branching model	<input checked="" type="checkbox"/> Rewriting history <input checked="" type="checkbox"/> Deletion <input checked="" type="checkbox"/> Changes without a pull request	<input checked="" type="checkbox"/> x_smit_bitbucket_euro...

Project settings

Project details

Security

Visibility

PROVISION

PULL REQUESTS

ADD-ONS

EXTENSION POINTS

Jira issue commit checker

Ensures that valid Jira issues are used in commits to support workflow transparency requirements and can be tracked for compliance rules. [Learn more about security](#)

Jira issues requirement

Bitbucket can verify that commits pushed to the repository contain a Jira issue key in their commit message.

Enter issue key(s) for issues in commit messages

Don't need a Jira issue key

☒ **Must contain a Jira issue key**

☒ **Must contain a Jira issue key that exists in Jira**

May impact Git push performance

Exemptions

You can create exemptions that will be skipped during the validation of the issues in commits.

The validation of the commit message contains the following items

Type a term and press enter

Stop validation when the commit is pushed by any of the following users

Start typing to find users

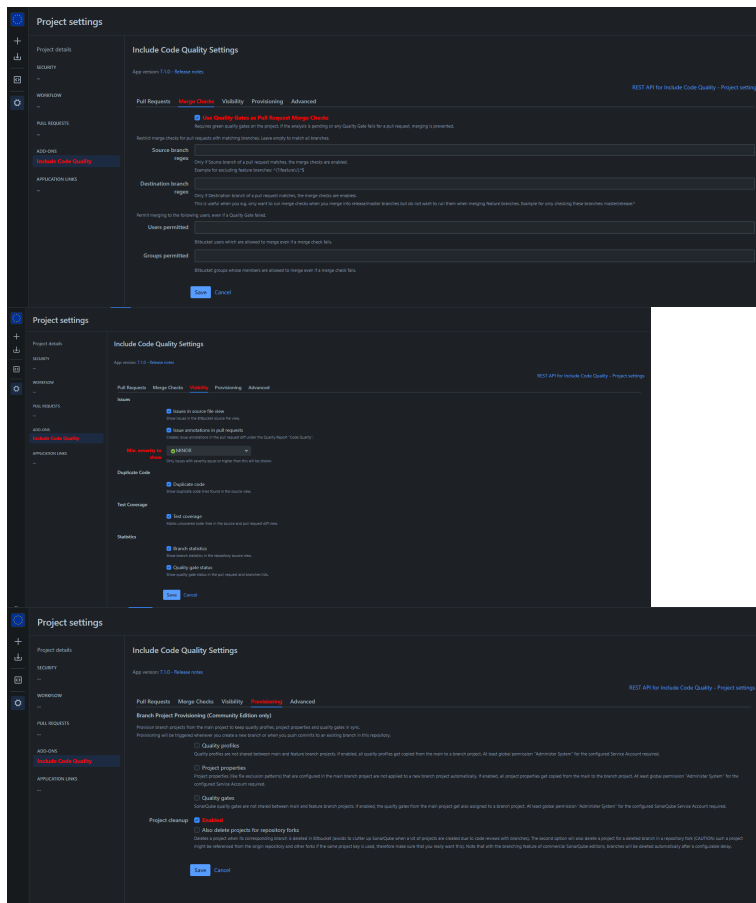
☒ Stop validation of the issues on merge commits

Save Cancel

2. BitBucket > MSKxx > Project Settings > Add-Ons > Include Code Quality:

1. **Merge Checks**
 - a. Use Quality Gates as Pull Request Merge Checks: **true**
2. **Visibility**
 - a. Min. severity to show: **MINOR**
3. **Provisioning**
 - a. Project cleanup - Enabled: **true**

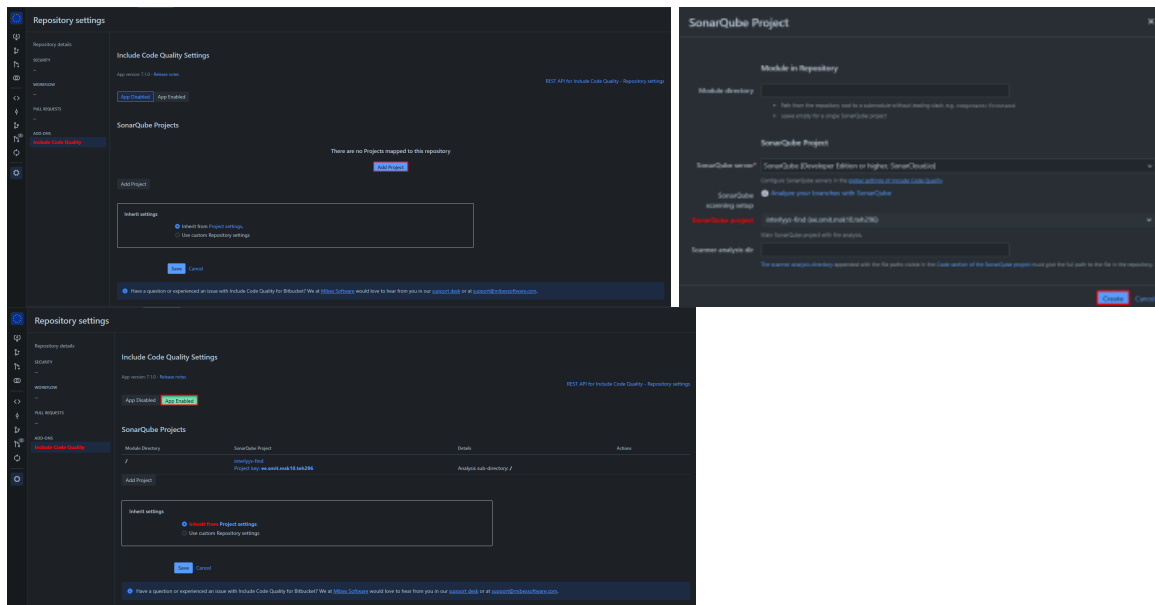
Ekraanipildid



BitBucket > MSKxx > rakendus > Repository settings > Include Code Quality:

1. Add Project
 - a. SonarQube project: **rakendus**
2. Include Code Quality Settings
 - a. App Enabled: **true**
 - b. Inherit Settings: **Project settings**

Ekraanipildid



Rakenduse bamboo-specs ehitusplaan:

- Seadistame ehitusplaani haru loomise triggeriks pull requesti.
- Säilitame ehitusplaani haru aktiivsena kuniks koodihoidlas haru kustutatakse.
- Säilitame koodihoidlas kustutatud harude ehitusplaane 7 päeva.

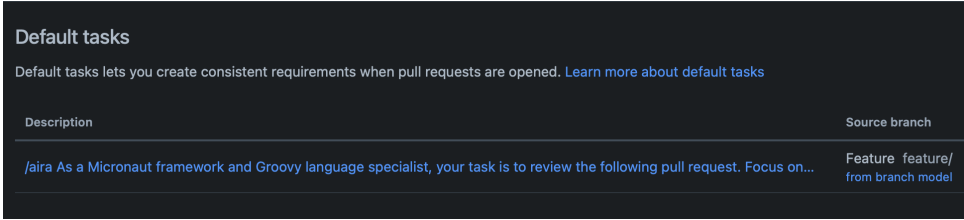
bamboo.yml

```
branches:
  create: for-pull-request
  delete:
    after-deleted-days: 7
    after-inactive-days: never
  link-to-jira: true
```

- Kontrollime SonarQube teenuste töötamist.
- Arendus- ning toodanguharude puhul rakendame SonarQube analüüsi tervele koodibaasile.
- Muul juhul rakendame SonarQube analüüsi ainult pull requestis muudetud sisule.

build.sh

```
if [[ "${bamboo_sonarStatusOk}" == "true" ]]; then
  if [[ "${bamboo_planRepository_branch}" == "develop" || "${bamboo_planRepository_branch}" == "main"
  ]]; then
    sonar-scanner -Dsonar.token="${bamboo_sonarTokenSecret}" \
      -Dsonar.branch.name="${bamboo_planRepository_branch}" \
      -Dsonar.projectVersion="${bamboo_planRepository_branch}"
  else
    sonar-scanner -Dsonar.token="${bamboo_sonarTokenSecret}" \
      -Dsonar.pullrequest.key="${bamboo_repository_pr_key}" \
      -Dsonar.pullrequest.branch="${bamboo_repository_pr_sourceBranch}" \
      -Dsonar.pullrequest.base="${bamboo_repository_pr_targetBranch}"
  fi
fi
```


7.	<p>Rakenduse Dockerfaili koostamisel tohib aluseks võtta ainult SMIT Dockerhubis asuva aluskonteineri, mille repo nimi on "RUNTIME" suffixiga. Ehitamiseks mõeldud konteinerit (reeglina ci suffixiga) ei tohi kasutada rakenduse pakendamiseks.</p> <p>Lubatud formaat: FROM docker.artifacts.smit.sise/dockerhub/XXXX</p> <p>Dockerfaili koostamisel kasutada semantilist versioneerimist (mõistlik kasutada rakenduse enda versiooninumbrit) ja Bamboo build numbrit ning vajadusel git harude nimetusi.</p> <div data-bbox="211 321 1484 636"> <p>i Lisainfo</p> <p>Dockerhubi uue aluskonteineri lisamise eelduseks on, et ei dubleerita mõnda olemasolevat (näiteks ei tehta mitut java 17 aluskonteinerit) ning tekib Bamboo plaan Dockerhub projekti (https://build.smit.sise/browse/TTT).</p> <p>Bamboo plaani sisuks on konteineris repode asendus Artifactoryga, konteineri ehitamine, x-ray docker skanneriga skaneerimine (XXX tasemega turvanõrkuste puhul peab ehitusprotsess katkema) ning Artifactorysse üles laadimine.</p> <p>Konteineri git-i reposse tuleb luua korrektne README.md fail koos vastutaja, versioonide ja kasutusinfoga. Kohustus on vastutajal perioodiliselt (vähemalt korra kvartalis) teha uuendusi.</p> <p>"Runtime" tüüpi konteinerid lepime kokku vastavalt kokkulepetele Developers koosolekul.</p> </div>				
8.	<p>Rakenduse lähtekoodi repo "feature" harudele vajadusel seadistada AI analüüsaator vastavalt oma rakenduse spetsiifikale.</p> <hr/> <h2 data-bbox="207 787 391 825">Ekraanipildid</h2> <div data-bbox="211 846 1170 1064">  <p>Default tasks</p> <p>Default tasks lets you create consistent requirements when pull requests are opened. Learn more about default tasks</p> <table border="1"> <thead> <tr> <th>Description</th> <th>Source branch</th> </tr> </thead> <tbody> <tr> <td>/aira As a Micronaut framework and Groovy language specialist, your task is to review the following pull request. Focus on...</td> <td>Feature feature/branch model</td> </tr> </tbody> </table> </div>	Description	Source branch	/aira As a Micronaut framework and Groovy language specialist, your task is to review the following pull request. Focus on...	Feature feature/branch model
Description	Source branch				
/aira As a Micronaut framework and Groovy language specialist, your task is to review the following pull request. Focus on...	Feature feature/branch model				
9.	<p>Ehitusplaanis tuleb kasutada Bamboo globaalseid muutujaid xrayStatusOk ja sonarStatusOk , mille abil saab teenuse haldaja Xray ja Sonari teenuste hoolduse või probleemide kestvuse ajal need pipelinedest välja lülitada ja nii ei häiri ehitusprotsessi.</p>				
10.	<p>Rakenduse GIT repositooriumi juurkausta tuleb lisada README.md formaadis dokumentatsioon mille sisu vastab formaadile: Rakenduse komponendi dokumentatsioon</p>				

11. Bamboo paigaldusplaani tuleb lisada git-is eraldi repona meeskonna projekti ning rakenduse repost lahus. Nimekuju peab olema **"XXX-deploy"**, kus XXX võib olla näiteks rakenduse/infosüsteemi nimi.

Paigaldusplaani git-i repo peab eksisteerima ainult **"main|master"** haruna ning erinevad keskkonnad defineeritakse paigaldusplaani sees. Sellega tagatakse, et keskne harude õiguste lahendus, mis tuleneb projekti õigustest laieneb ka paigaldusplaanidele (ilma pullrequestita paigaldusplaanidesse muudatusi teha ei saa ning pullrequesti vastuvõtmine on võimalik ainult piiratud grupil).

Vastavalt vajadustele võib paigaldusplaanis keskkondadesse paigaldamise anda ka välistele partneritele (näiteks arendus). Vt: [Välise partneri ligipääsude juhend](#), aga git-is deploy repole muutmis/lugemisõiguseid ei väljastata. Soovitus on paigaldusplaanis eraldada ära rakenduse paigaldus ja infrastruktuuri loomine (näiteks virtuaalmasinad).

```
---
version: 2

deployment:
  name: micronaut-vue
  source-plan: MSKYY-XXXX

release-naming:
  applies-to-branches: false
  next-version-name: ${bamboo.version}-${bamboo.buildNumber}

environments:
  - dev
  - test
  - live
  - dev infra

---
version: 2

deployment: micronaut-vue
deployment-permissions:
  - groups:
    - x_smit_bamboo_euro_deploy
    permissions:
      - view
  - groups:
    - x_smit_bamboo_euro_admin
    permissions:
      - view
      - edit
default-environment-permissions:
  - groups:
    - x_smit_bamboo_euro_deploy
    permissions:
      - view
      - deploy
  - groups:
    - x_smit_bamboo_euro_admin
    permissions:
      - view
      - edit
      - deploy

#external partner permission
environment-permissions:
  - dev:
    - groups:
      - x_smit_bamboo_euro_interlyys_build
    permissions:
      - view
      - deploy
```

12.	<p>Kõik terraformi ja kubernetesi failid tuleb enne käivitamist skaneerida trivy skänneriga, probleemide leidmisel (kõik mis medium või kõrgem) peab deploy plaan katkestama töö. Skanner on olemas deploy konteineris.</p> <pre>trivy --debug config --severity HIGH,CRITICAL,MEDIUM --exit-code 1 --checks-bundle-repository docker.artifacts.smit.sise/aquasecurity/trivy-checks:0 .</pre>
13.	<p>Paigaldusplaanis kõik saladused tuleb lugeda Vaultist kasutades Bamboo Secret plugina võimalusi (saladused lisada meeskonna kataloogi Vaultis). https://windtunnel.io/products/smb/#/topics/syntax</p>
14.	<p>Paroolid ja rakenduse konfiguratsioon tuleb saata Bamboo kaudu serveritesse või Kubernetesesse. Rakendustest sh Kubernetesest Bitbucketi poole ei ole lubatud pöörduda.</p>