Your work
Home
Projects
Groups
Issues 14
Merge requests
To-Do List 125
Milestones
Snippets
Activity

https://www.ict.inaf.it/gitlab

Create new project

Create blank project

Create a blank project to store your files, plan your work, and collaborate on code, among other things.

Create from template

Create a project pre-populated with the necessary files to get you started quickly.

Import project

Migrate your data from an external source like GitHub, Bitbucket, or another instance of GitLab.

You can also create a project from the command line. Show command

What's new 3
Help
Collapse sidebar

Search or go to... /

14 0 99+

Your work

- Home
- Projects
- Groups
- Issues 14
- Merge requests
- To-Do List 125
- Milestones
- Snippets
- Activity

- What's new 3
- Help
- Collapse sidebar

Your work / Projects / New project / **Create blank project**

Create blank project

Create a blank project to store your files, plan your work, and collaborate on code, among other things.

Project name

DevOps course

Must start with a lowercase or uppercase letter, digit, emoji, or underscore. Can also contain dots, pluses, dashes, or spaces.

Project URL

https://www.ict.inaf.it/gitlab/ kevin.munari /

Project slug

devops-course

Visibility Level

- Private
  Project access must be granted explicitly to each user. If this project is part of a group, access is granted to members of the group.
- Internal
  The project can be accessed by any logged in user except external users.
- Public
  The project can be accessed without any authentication.

Project Configuration

- [x] Initialize repository with a README
  Allows you to immediately clone this project's repository. Skip this if you plan to push up an existing repository.
- [ ] Enable Static Application Security Testing (SAST)
  Analyze your source code for known security vulnerabilities. Learn more.
- [ ] Enable Secret Detection
  Scan your code for secrets and credentials to prevent unauthorized access. Learn more.

Create project Cancel

Search or go to... /

14 0 99+

Project

D DevOps course

Pinned
Issues 0
Merge requests 0

Manage
Plan
Code
Build
Secure
Deploy
Operate
Monitor
Analyze
Settings

What's new 3
Help
Collapse sidebar

Kevin Munari / **DevOps course** https://www.ict.inaf.it/gitlab/kevin.munari/devops-course

Project 'DevOps course' was successfully created.

D DevOps course

main devops-course + Find file Code

Star 0 Fork 0

Initial commit
Kevin Munari authored just now
9f167c09 History

Name	Last commit	Last update
README.md	Initial commit	just now

README.md

DevOps course

Getting started

To make it easy for you to get started with GitLab, here's a list of recommended next steps.

Already a pro? Just edit this README.md and make it your own. Want to make it easy? Use the template at the bottom!

Add your files

- Create or upload files
- Add files using the command line or push an existing Git repository with the following command:

```
cd existing_repo
git remote add origin https://www.ict.inaf.it/gitlab/kevin.munari/devops-course.git
git branch -M main
```

Project information

1 Commit
1 Branch
0 Tags
4 KiB Project Storage

README
Add LICENSE
Add CHANGELOG
Add CONTRIBUTING
Enable Auto DevOps
Add Kubernetes cluster
Set up CI/CD
Add Wiki
Configure Integrations

Created on
February 27, 2026

http://astri-sq.oas.inaf.it:9010/

Log in to SonarQube

Log in with GitLab

More options

My Favorites All

Search by project name or key

Create Project

GitLab
Manually
More

Filters

0 project(s)

Perspective: Overall Status

Sort by:

Quality Gate

Passed 0

Failed 0

Reliability (Bugs)

A A rating 0

B B rating 0

C C rating 0

D D rating 0

E E rating 0

Security (Vulnerabilities)

A A rating 0

B B rating 0

C C rating 0

D D rating 0

E E rating 0

Security Review (Security Hotspots)

A ≥ 80% 0

B 70% - 80% 0

C 50% - 70% 0

D 30% - 50% 0

E < 30% 0

Maintainability (Code Smells)

A A rating 0

You don't have any favorite projects yet.

Discover and mark as favorites projects you are interested in to have a quick access to them.

Explore Projects

0 of 0 shown

Create a project

All fields marked with * are required

Project display name *

DevOps course

Up to 255 characters. Some scanners might override the value you provide.

Project key *

devops-course

The project key is a unique identifier for your project. It may contain up to 400 characters. Allowed characters are alphanumeric, '-' (dash), '_' (underscore), '.' (period) and ':' (colon), with at least one non-digit.

Main branch name *

main

The name of your project's default branch Learn More

Set Up

DevOps course main

How do you want to analyze your repository?

Do you want to integrate with your favorite CI? Choose one of the following tutorials.

With Jenkins

With GitHub Actions

With Bitbucket Pipelines

With GitLab CI

With Azure Pipelines

Other CI

Are you just testing or have an advanced use-case? Analyze your project locally.

Locally

Analyze your project with GitLab CI

1 Set your project key

1. What option best describes your build?

Maven | Gradle | .NET | Other (for JS, TS, Go, Python, PHP, ...)

2. Add the following to your `pom.xml` file:

```
<properties>
  <sonar.qualitygate.wait>true</sonar.qualitygate.wait>
</properties>
```

Copy

Continue

2 Add environment variables

3 Create or update the configuration file

4 You're all set!

sonarqube Projects Issues Rules Quality Profiles Quality Gates

Search for projects... KM

DevOps course main

Overview Issues Security Hotspots Measures Code Activity

Project Information

Analyze your project with GitLab CI

1 Set your project key

2 Add environment variables

1. Define the SonarQube Token environment variable.

   In GitLab, go to **Settings > CI/CD > Variables** to add the following variable and make sure it is available for your project:

   a. In the **Key** field, enter `SONAR_TOKEN`

   b. In the **Value** field, enter an existing token, or a newly generated one: Generate a token

   c. Uncheck the **Protect Variable** checkbox.

   d. Check the **Mask Variable** checkbox.

2. Define the SonarQube URL environment variable.

   Still in **Settings > CI/CD > Variables** add a new variable and make sure it is available for your project:

   a. In the **Key** field, enter `SONAR_HOST_URL`

   b. In the **Value** field, enter `http://astri-sq.oas.inaf.it:9010`

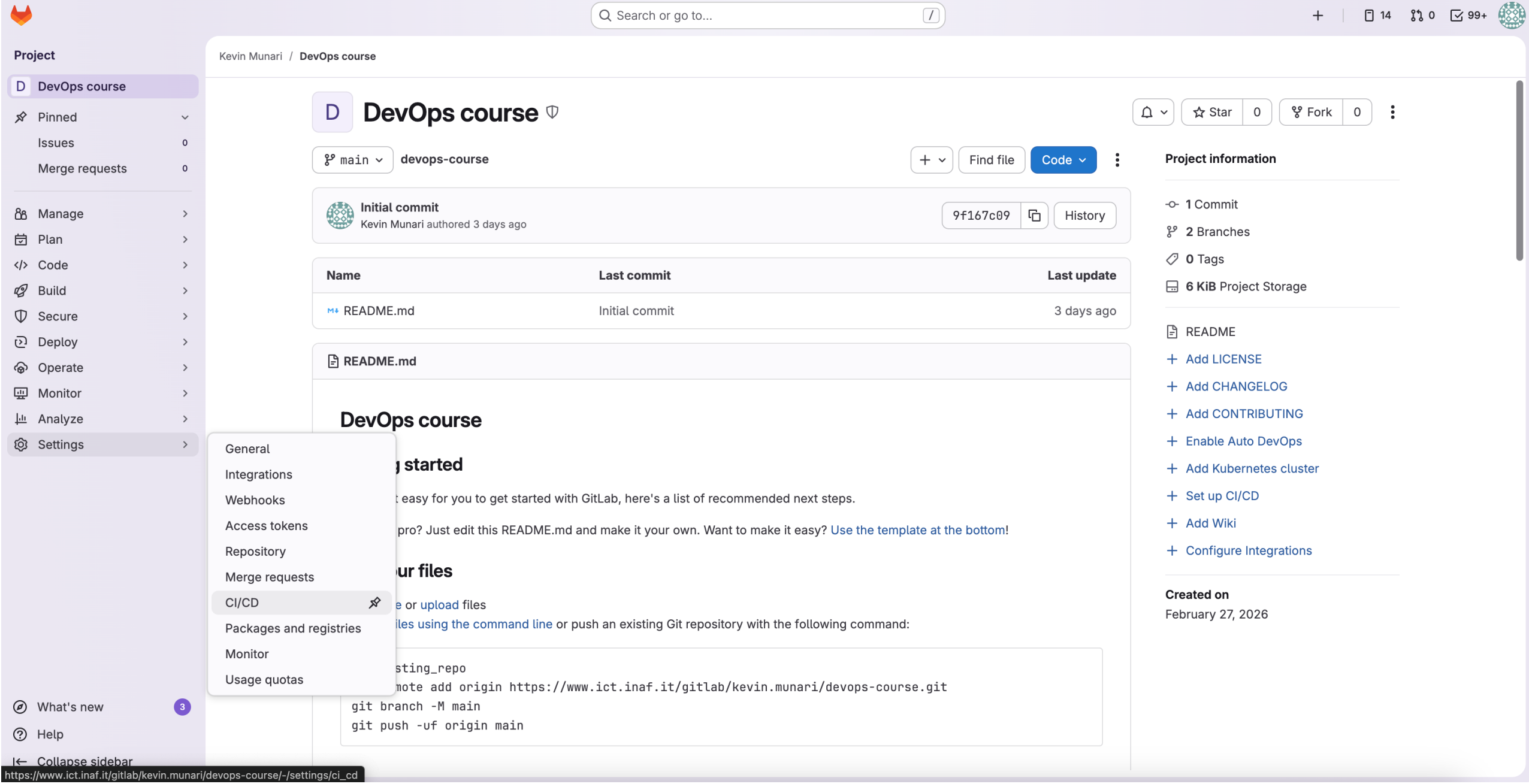
   c. Uncheck the **Protect Variable** checkbox.

   d. Leave the **Mask Variable** checkbox unchecked.

Continue

3 Create or update the configuration file

4 You're all set!


Search or go to...
14
0
99+
Project
DevOps course
Pinned
Issues 0
Merge requests 0
Manage
Plan
Code
Build
Secure
Deploy
Operate
Monitor
Analyze
Settings
General
Integrations
Webhooks
Access tokens
Repository
Merge requests
CI/CD
Packages and registries
Monitor
Usage quotas
What's new 3
Help
Collapse sidebar
Kevin Munari / DevOps course
DevOps course
Star 0
Fork 0
main
devops-course
Find file
Code
Initial commit
Kevin Munari authored 3 days ago
9f167c09
History
Name
Last commit
Last update
README.md
Initial commit
3 days ago
README.md
DevOps course
started
easy for you to get started with GitLab, here's a list of recommended next steps.
pro? Just edit this README.md and make it your own. Want to make it easy? Use the template at the bottom!
ur files
or upload files
iles using the command line or push an existing Git repository with the following command:
sting_repo
mote add origin https://www.ict.inaf.it/gitlab/kevin.munari/devops-course.git
git branch -M main
git push -uf origin main
Project information
1 Commit
2 Branches
0 Tags
6 KiB Project Storage
README
Add LICENSE
Add CHANGELOG
Add CONTRIBUTING
Enable Auto DevOps
Add Kubernetes cluster
Set up CI/CD
Add Wiki
Configure Integrations
Created on
February 27, 2026
https://www.ict.inaf.it/gitlab/kevin.munari/devops-course/-/settings/ci_cd

Project
D DevOps course
Pinned
Issues 0
Merge requests 0
Manage
Plan
Code
Build
Secure
Deploy
Operate
Monitor
Analyze
Settings
General
Integrations
Webhooks
Access tokens
Repository
Merge requests
CI/CD
Packages and registries
What's new 3
Help
Collapse sidebar

Search page

General pipelines

Customize your pipeline configuration.

Auto DevOps

Automate building, testing, and deploying your applications based on your continuous integration and delivery configuration. How do I get started?

Runners

Runners are processes that pick up and execute CI/CD jobs for GitLab. What is GitLab Runner?

Artifacts

A job artifact is an archive of files and directories saved by a job when it finishes.

Variables

Variables store information that you can use in job scripts. Each project can define a maximum of 8000 variables. Learn more.

Pipeline trigger tokens

Trigger a pipeline for a branch or tag by generating a trigger token and using it with an API call. The token impersonates a user's project access and permissions. Learn more.

Deploy freezes

Add a freeze period to prevent unintended releases during a period of time for a given environment. You must update the deployment jobs in `.gitlab-ci.yml` according to the deploy freezes added here. Learn more. Specify deploy freezes using cron syntax.

Job token permissions

Control which groups and projects can use CI/CD job tokens to authenticate with this project. Learn more about job token security.

Project
D DevOps course
Pinned
Issues 0
Merge requests 0
Manage
Plan
Code
Build
Secure
Deploy
Operate
Monitor
Analyze
Settings
General
Integrations
Webhooks
Access tokens
Repository
Merge requests
CI/CD
Packages and registries
What's new 3
Help
Collapse sidebar

Variables

Variables store information that you can use in job scripts. Each project can define a maximum of 8000 variables. Learn more.

Minimum role to use pipeline variables

Select the minimum role that is allowed to run a new pipeline with pipeline variables. What are pipeline variables?

- ( ) No one allowed
  Pipeline variables cannot be used.
- ( ) Owner
- ( ) Maintainer
- (•) Developer

Save changes

Access protected resources in merge request pipelines

Make protected CI/CD variables and runners available in merge request pipelines. Protected resources will only be available in merge request pipelines if both the source and target branches of the merge request are protected. Learn more.

- [x] Allow merge request pipelines to access protected variables and runners

Save changes

Display manually-defined pipeline variables

Display all manually-defined variables in the pipeline details page after running a pipeline manually. Learn more.

- [ ] Display pipeline variables

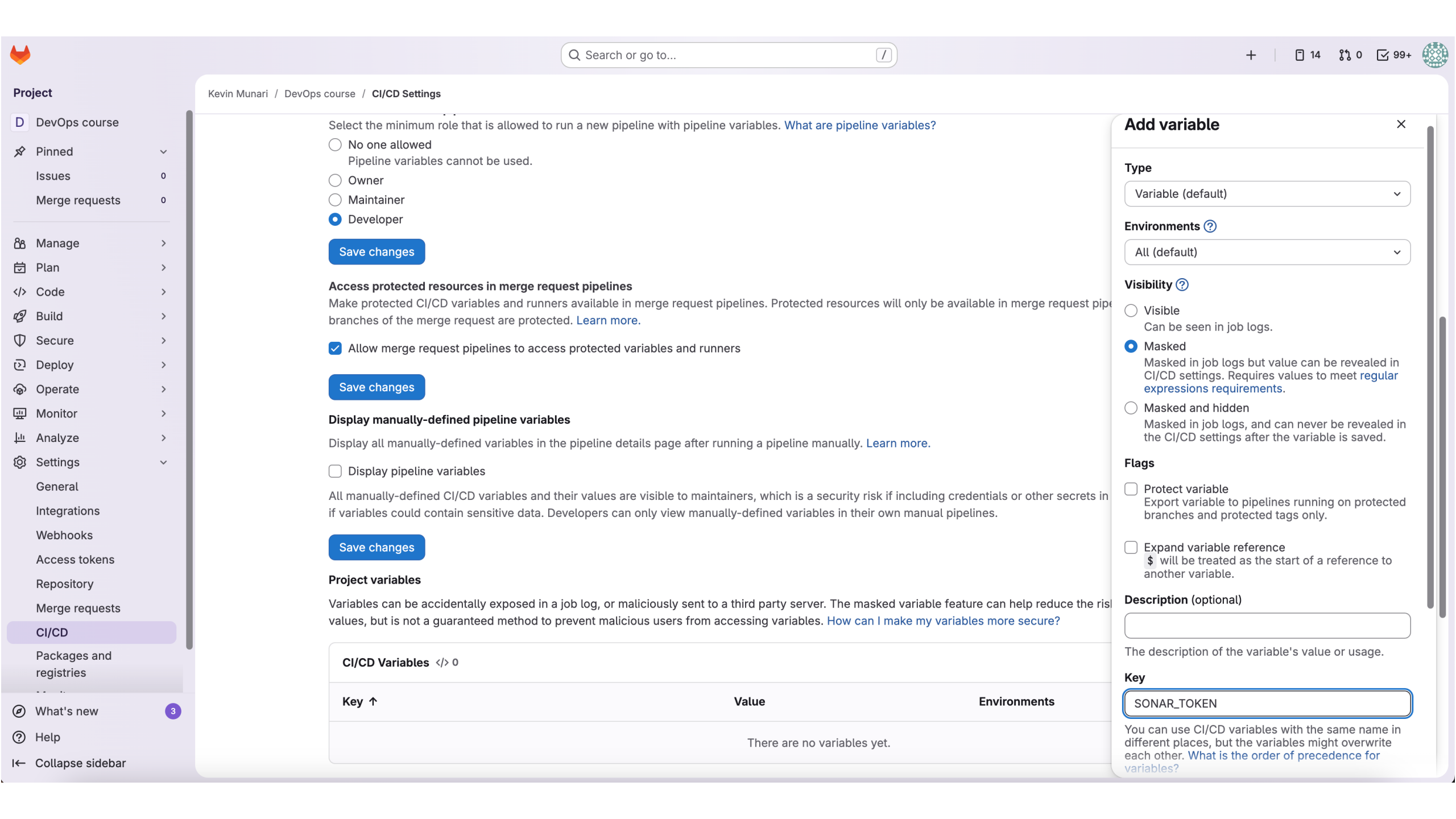
All manually-defined CI/CD variables and their values are visible to maintainers, which is a security risk if including credentials or other secrets in variables. Do not enable this feature if variables could contain sensitive data. Developers can only view manually-defined variables in their own manual pipelines.

Save changes

Project variables

Variables can be accidentally exposed in a job log, or maliciously sent to a third party server. The masked variable feature can help reduce the risk of accidentally exposing variable values, but is not a guaranteed method to prevent malicious users from accessing variables. How can I make my variables more secure?

CI/CD Variables </> 0 Add variable


Search or go to...
14
0
99+
Project
DevOps course
Pinned
Issues 0
Merge requests 0
Manage
Plan
Code
Build
Secure
Deploy
Operate
Monitor
Analyze
Settings
General
Integrations
Webhooks
Access tokens
Repository
Merge requests
CI/CD
Packages and registries
What's new 3
Help
Collapse sidebar
Kevin Munari / DevOps course / CI/CD Settings
Select the minimum role that is allowed to run a new pipeline with pipeline variables. What are pipeline variables?
No one allowed
Pipeline variables cannot be used.
Owner
Maintainer
Developer
Save changes
Access protected resources in merge request pipelines
Make protected CI/CD variables and runners available in merge request pipelines. Protected resources will only be available in merge request pipe
branches of the merge request are protected. Learn more.
Allow merge request pipelines to access protected variables and runners
Save changes
Display manually-defined pipeline variables
Display all manually-defined variables in the pipeline details page after running a pipeline manually. Learn more.
Display pipeline variables
All manually-defined CI/CD variables and their values are visible to maintainers, which is a security risk if including credentials or other secrets in
if variables could contain sensitive data. Developers can only view manually-defined variables in their own manual pipelines.
Save changes
Project variables
Variables can be accidentally exposed in a job log, or maliciously sent to a third party server. The masked variable feature can help reduce the ris
values, but is not a guaranteed method to prevent malicious users from accessing variables. How can I make my variables more secure?
CI/CD Variables 0
Key
Value
Environments
There are no variables yet.
Add variable
Type
Variable (default)
Environments
All (default)
Visibility
Visible
Can be seen in job logs.
Masked
Masked in job logs but value can be revealed in CI/CD settings. Requires values to meet regular expressions requirements.
Masked and hidden
Masked in job logs, and can never be revealed in the CI/CD settings after the variable is saved.
Flags
Protect variable
Export variable to pipelines running on protected branches and protected tags only.
Expand variable reference
$ will be treated as the start of a reference to another variable.
Description (optional)
The description of the variable's value or usage.
Key
SONAR_TOKEN
You can use CI/CD variables with the same name in different places, but the variables might overwrite each other. What is the order of precedence for variables?

sonarqube Projects Issues Rules Quality Profiles Quality Gates

Search for projects... KM

DevOps course main

Overview Issues Security Hotspots Measures Code Activity

Project Information

Analyze your project with GitLab CI

1 Set your project key

2 Add environment variables

1. Define the SonarQube Token environment variable.

   In GitLab, go to **Settings > CI/CD > Variables** to add the following variable and make sure it is available for your project:

   a. In the **Key** field, enter `SONAR_TOKEN`

   b. In the **Value** field, enter an existing token, or a newly generated one: **Generate a token**

   c. Uncheck the **Protect Variable** checkbox.

   d. Check the **Mask Variable** checkbox.

2. Define the SonarQube URL environment variable.

   Still in **Settings > CI/CD > Variables** add a new variable and make sure it is available for your project:

   a. In the **Key** field, enter `SONAR_HOST_URL`

   b. In the **Value** field, enter `http://astri-sq.oas.inaf.it:9010`

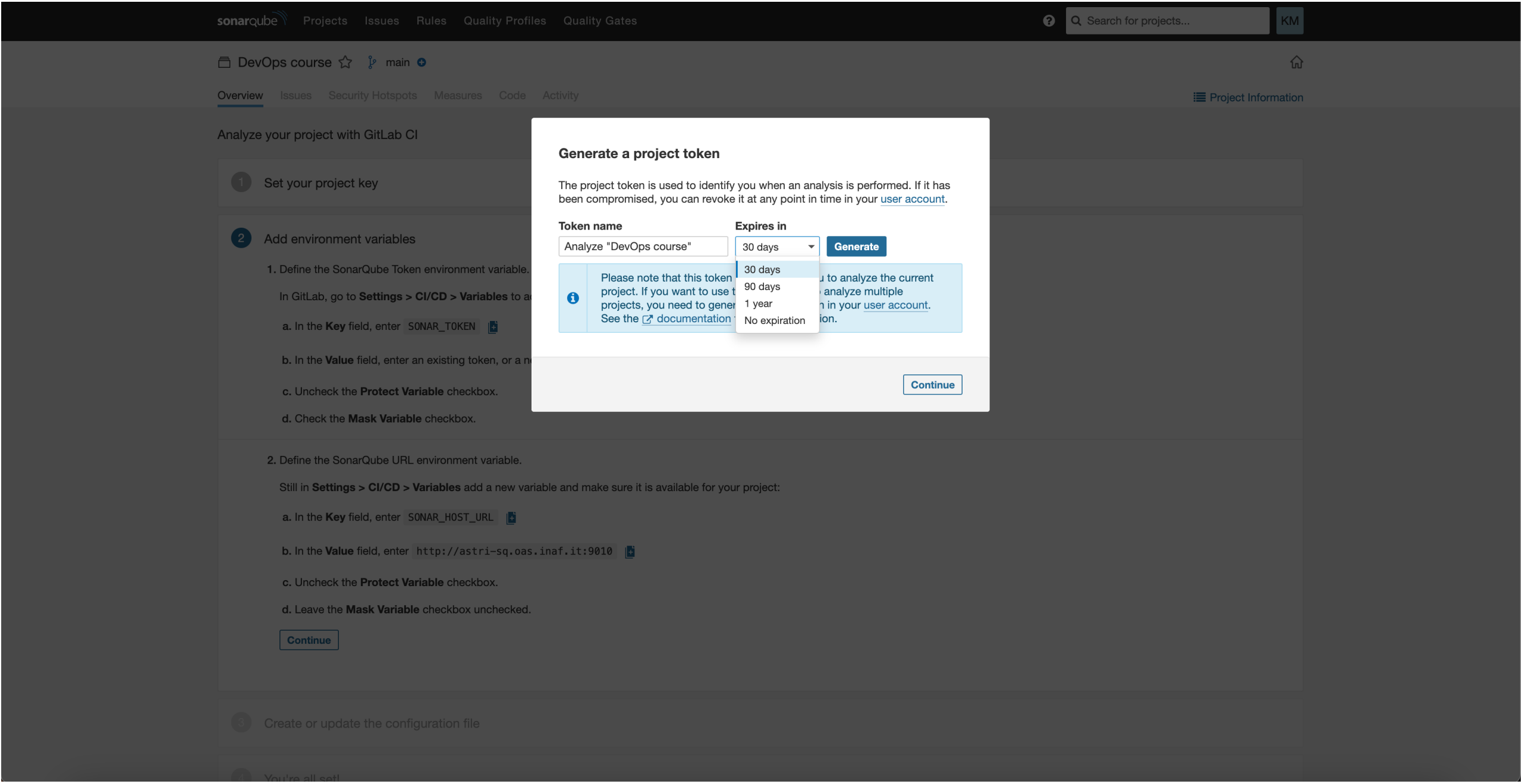
   c. Uncheck the **Protect Variable** checkbox.

   d. Leave the **Mask Variable** checkbox unchecked.

Continue

3 Create or update the configuration file

4 You're all set!


sonarqube
Projects
Issues
Rules
Quality Profiles
Quality Gates
Search for projects...
KM
DevOps course
main
Overview
Issues
Security Hotspots
Measures
Code
Activity
Project Information
Analyze your project with GitLab CI
1 Set your project key
2 Add environment variables
1. Define the SonarQube Token environment variable.
In GitLab, go to Settings > CI/CD > Variables to a
a. In the Key field, enter SONAR_TOKEN
b. In the Value field, enter an existing token, or a n
c. Uncheck the Protect Variable checkbox.
d. Check the Mask Variable checkbox.
2. Define the SonarQube URL environment variable.
Still in Settings > CI/CD > Variables add a new variable and make sure it is available for your project:
a. In the Key field, enter SONAR_HOST_URL
b. In the Value field, enter http://astri-sq.oas.inaf.it:9010
c. Uncheck the Protect Variable checkbox.
d. Leave the Mask Variable checkbox unchecked.
Continue
3 Create or update the configuration file
4 You're all set!
Generate a project token
The project token is used to identify you when an analysis is performed. If it has been compromised, you can revoke it at any point in time in your user account.
Token name
Analyze "DevOps course"
Expires in
30 days
Generate
30 days
90 days
1 year
No expiration
Please note that this token
u to analyze the current
project. If you want to use t
analyze multiple
projects, you need to gener
n in your user account.
See the documentation
ion.
Continue

sonarqube Projects Issues Rules Quality Profiles Quality Gates

Search for projects... KM

DevOps course main

Overview Issues Security Hotspots Measures Code Activity

Project Information

Analyze your project with GitLab CI

1 Set your project key

2 Add environment variables

1. Define the SonarQube Token environment variable.

In GitLab, go to **Settings > CI/CD > Variables** to a

a. In the **Key** field, enter `SONAR_TOKEN`

b. In the **Value** field, enter an existing token, or a n

c. Uncheck the **Protect Variable** checkbox.

d. Check the **Mask Variable** checkbox.

2. Define the SonarQube URL environment variable.

Still in **Settings > CI/CD > Variables** add a new variable and make sure it is available for your project:

a. In the **Key** field, enter `SONAR_HOST_URL`

b. In the **Value** field, enter `http://astri-sq.oas.inaf.it:9010`

c. Uncheck the **Protect Variable** checkbox.

d. Leave the **Mask Variable** checkbox unchecked.

Continue

3 Create or update the configuration file

4 You're all set!

Generate a project token

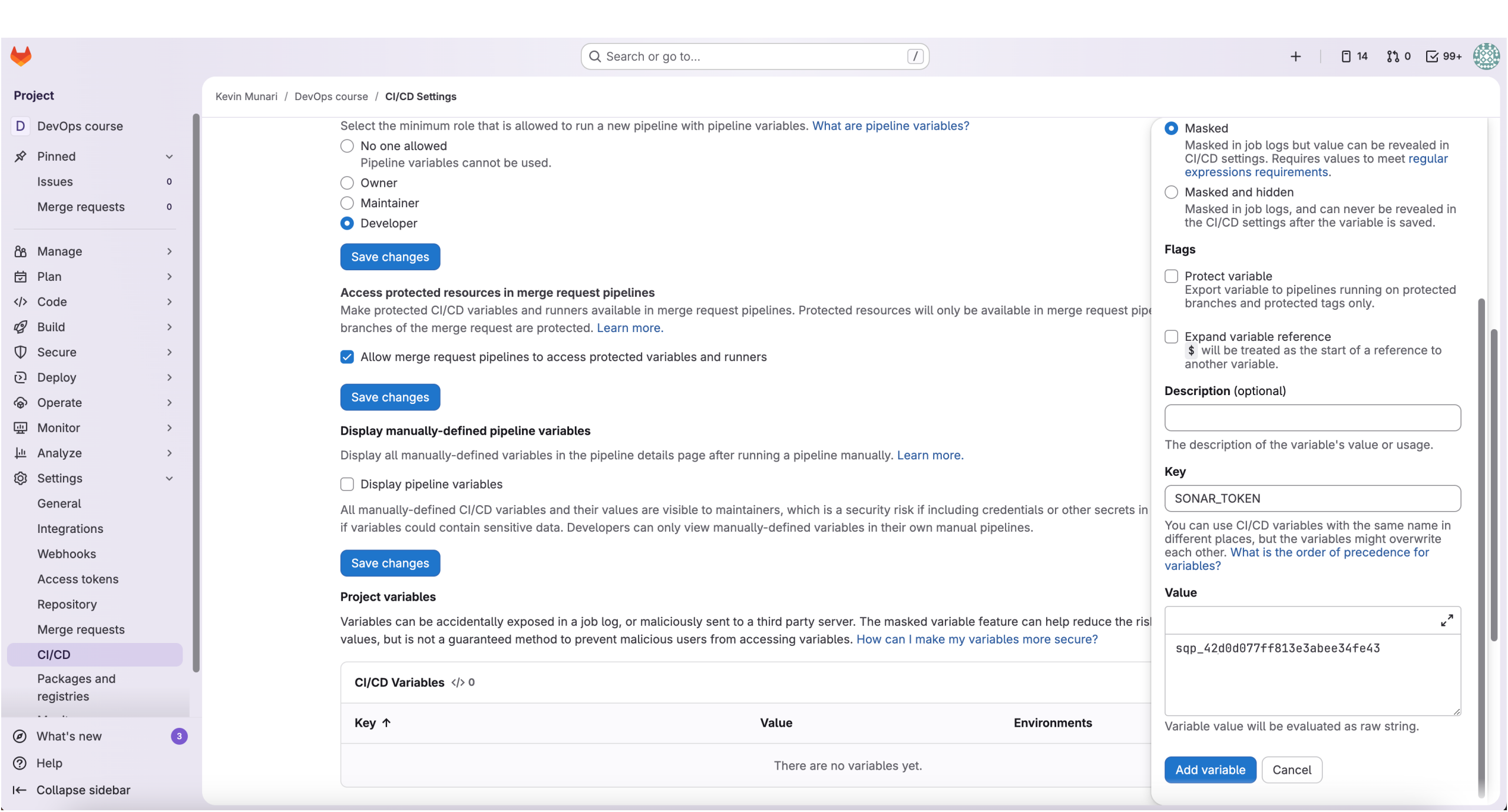
The project token is used to identify you when an analysis is performed. If it has been compromised, you can revoke it at any point in time in your user account.

Analyze "DevOps course":

`sqp_42d0d077ff813e3abee34fe43`

New token "sqp_42d0d077ff813e3abee34fe43 " has been created. Make sure you copy it now, you won't be able to see it again!

Continue


Search or go to...
14
0
99+
Project
DevOps course
Pinned
Issues 0
Merge requests 0
Manage
Plan
Code
Build
Secure
Deploy
Operate
Monitor
Analyze
Settings
General
Integrations
Webhooks
Access tokens
Repository
Merge requests
CI/CD
Packages and registries
What's new 3
Help
Collapse sidebar
Kevin Munari / DevOps course / CI/CD Settings
Select the minimum role that is allowed to run a new pipeline with pipeline variables. What are pipeline variables?
No one allowed
Pipeline variables cannot be used.
Owner
Maintainer
Developer
Save changes
Access protected resources in merge request pipelines
Make protected CI/CD variables and runners available in merge request pipelines. Protected resources will only be available in merge request pipe
branches of the merge request are protected. Learn more.
Allow merge request pipelines to access protected variables and runners
Save changes
Display manually-defined pipeline variables
Display all manually-defined variables in the pipeline details page after running a pipeline manually. Learn more.
Display pipeline variables
All manually-defined CI/CD variables and their values are visible to maintainers, which is a security risk if including credentials or other secrets in
if variables could contain sensitive data. Developers can only view manually-defined variables in their own manual pipelines.
Save changes
Project variables
Variables can be accidentally exposed in a job log, or maliciously sent to a third party server. The masked variable feature can help reduce the ris
values, but is not a guaranteed method to prevent malicious users from accessing variables. How can I make my variables more secure?
CI/CD Variables 0
Key
Value
Environments
There are no variables yet.
Masked
Masked in job logs but value can be revealed in CI/CD settings. Requires values to meet regular expressions requirements.
Masked and hidden
Masked in job logs, and can never be revealed in the CI/CD settings after the variable is saved.
Flags
Protect variable
Export variable to pipelines running on protected branches and protected tags only.
Expand variable reference
$ will be treated as the start of a reference to another variable.
Description (optional)
The description of the variable's value or usage.
Key
SONAR_TOKEN
You can use CI/CD variables with the same name in different places, but the variables might overwrite each other. What is the order of precedence for variables?
Value
sqp_42d0d077ff813e3abee34fe43
Variable value will be evaluated as raw string.
Add variable
Cancel

- ( ) No one allowed
  Pipeline variables cannot be used.
- ( ) Owner
- ( ) Maintainer
- (•) Developer

Save changes

Access protected resources in merge request pipelines

Make protected CI/CD variables and runners available in merge request pipelines. Protected resources will only be available in merge request pipelines if both the source and target branches of the merge request are protected. Learn more.

- [x] Allow merge request pipelines to access protected variables and runners

Save changes

Display manually-defined pipeline variables

Display all manually-defined variables in the pipeline details page after running a pipeline manually. Learn more.

- [ ] Display pipeline variables

All manually-defined CI/CD variables and their values are visible to maintainers, which is a security risk if including credentials or other secrets in variables. Do not enable this feature if variables could contain sensitive data. Developers can only view manually-defined variables in their own manual pipelines.

Save changes

Project variables

Variables can be accidentally exposed in a job log, or maliciously sent to a third party server. The masked variable feature can help reduce the risk of accidentally exposing variable values, but is not a guaranteed method to prevent malicious users from accessing variables. How can I make my variables more secure?

CI/CD Variables </> 1 Hide values Add variable

Key ↑	Value	Environments	Actions
SONAR_TOKEN Masked	sqp_42d0d077ff813e3abee34fe43...	All (default)	

sonarqube Projects Issues Rules Quality Profiles Quality Gates

Search for projects... KM

DevOps course main

Overview Issues Security Hotspots Measures Code Activity

Project Information

Analyze your project with GitLab CI

1 Set your project key

2 Add environment variables

1. Define the SonarQube Token environment variable.

   In GitLab, go to **Settings > CI/CD > Variables** to add the following variable and make sure it is available for your project:

   a. In the **Key** field, enter `SONAR_TOKEN`

   b. In the **Value** field, enter an existing token, or a newly generated one: Generate a token

   c. Uncheck the **Protect Variable** checkbox.

   d. Check the **Mask Variable** checkbox.

2. Define the SonarQube URL environment variable.

   Still in **Settings > CI/CD > Variables** add a new variable and make sure it is available for your project:

   a. In the **Key** field, enter `SONAR_HOST_URL`

   b. In the **Value** field, enter `http://astri-sq.oas.inaf.it:9010`

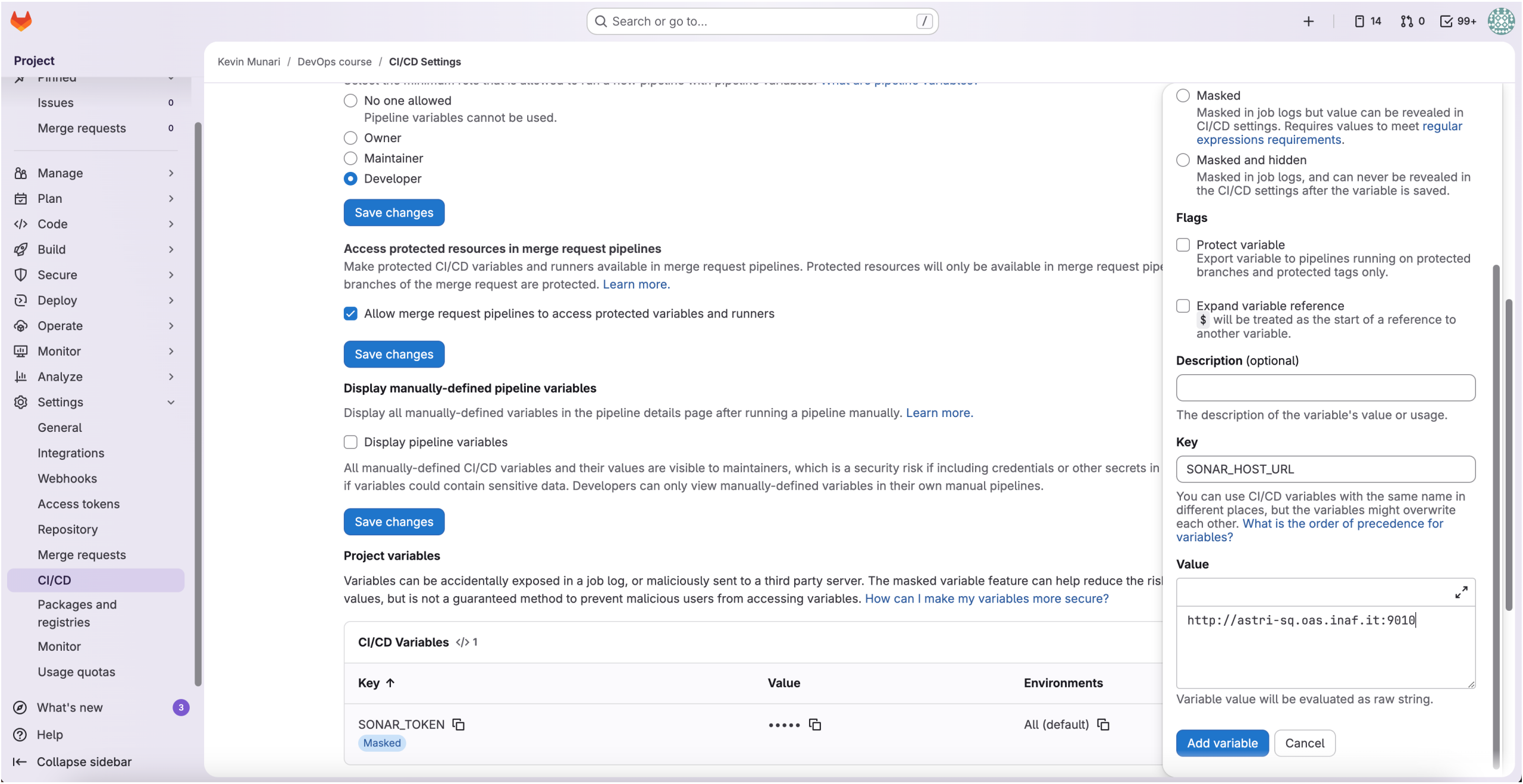
   c. Uncheck the **Protect Variable** checkbox.

   d. Leave the **Mask Variable** checkbox unchecked.

Continue

3 Create or update the configuration file

4 You're all set!


Search or go to...
14
0
99+
Project
Issues 0
Merge requests 0
Manage
Plan
Code
Build
Secure
Deploy
Operate
Monitor
Analyze
Settings
General
Integrations
Webhooks
Access tokens
Repository
Merge requests
CI/CD
Packages and registries
Monitor
Usage quotas
What's new 3
Help
Collapse sidebar
Kevin Munari / DevOps course / CI/CD Settings
No one allowed
Pipeline variables cannot be used.
Owner
Maintainer
Developer
Save changes
Access protected resources in merge request pipelines
Make protected CI/CD variables and runners available in merge request pipelines. Protected resources will only be available in merge request pipe
branches of the merge request are protected. Learn more.
Allow merge request pipelines to access protected variables and runners
Save changes
Display manually-defined pipeline variables
Display all manually-defined variables in the pipeline details page after running a pipeline manually. Learn more.
Display pipeline variables
All manually-defined CI/CD variables and their values are visible to maintainers, which is a security risk if including credentials or other secrets in
if variables could contain sensitive data. Developers can only view manually-defined variables in their own manual pipelines.
Save changes
Project variables
Variables can be accidentally exposed in a job log, or maliciously sent to a third party server. The masked variable feature can help reduce the ris
values, but is not a guaranteed method to prevent malicious users from accessing variables. How can I make my variables more secure?
CI/CD Variables 1
Key
Value
Environments
SONAR_TOKEN
Masked
All (default)
Masked
Masked in job logs but value can be revealed in CI/CD settings. Requires values to meet regular expressions requirements.
Masked and hidden
Masked in job logs, and can never be revealed in the CI/CD settings after the variable is saved.
Flags
Protect variable
Export variable to pipelines running on protected branches and protected tags only.
Expand variable reference
$ will be treated as the start of a reference to another variable.
Description (optional)
The description of the variable's value or usage.
Key
SONAR_HOST_URL
You can use CI/CD variables with the same name in different places, but the variables might overwrite each other. What is the order of precedence for variables?
Value
http://astri-sq.oas.inaf.it:9010
Variable value will be evaluated as raw string.
Add variable
Cancel

- Owner
- Maintainer
- Developer

Save changes

Access protected resources in merge request pipelines

Make protected CI/CD variables and runners available in merge request pipelines. Protected resources will only be available in merge request pipelines if both the source and target branches of the merge request are protected. Learn more.

- [x] Allow merge request pipelines to access protected variables and runners

Save changes

Display manually-defined pipeline variables

Display all manually-defined variables in the pipeline details page after running a pipeline manually. Learn more.

- [ ] Display pipeline variables

All manually-defined CI/CD variables and their values are visible to maintainers, which is a security risk if including credentials or other secrets in variables. Do not enable this feature if variables could contain sensitive data. Developers can only view manually-defined variables in their own manual pipelines.

Save changes

Project variables

Variables can be accidentally exposed in a job log, or maliciously sent to a third party server. The masked variable feature can help reduce the risk of accidentally exposing variable values, but is not a guaranteed method to prevent malicious users from accessing variables. How can I make my variables more secure?

CI/CD Variables </> 2 Hide values Add variable

Key ↑	Value	Environments	Actions
SONAR_HOST_URL	http://astri-sq.oas.inaf.it:9010	All (default)	
SONAR_TOKEN Masked	sqp_42d0d077ff813e3abee34fe43...	All (default)	

sonarqube Projects Issues Rules Quality Profiles Quality Gates

Search for projects... KM

DevOps course main

Overview Issues Security Hotspots Measures Code Activity

Project Information

Analyze your project with GitLab CI

1 Set your project key

2 Add environment variables

3 Create or update the configuration file

Create or update your `.gitlab-ci.yml` file with the following content.

```
sonarqube-check:
  image: maven:3.6.3-jdk-11
  variables:
    SONAR_USER_HOME: "${CI_PROJECT_DIR}/.sonar"  # Defines the location
    GIT_DEPTH: "0"  # Tells git to fetch all the branches of the project
  cache:
    key: "${CI_JOB_NAME}"
    paths:
      - .sonar/cache
  script:
    - mvn verify sonar:sonar -Dsonar.projectKey=devops-course
  allow_failure: true
  only:
    - main
```

Copy

Note that this is a minimal base configuration to run a SonarQube analysis on your main branch.
If you already have a pipeline configured and running, you might want to add the example from this step to your existing yml file.

Finish this tutorial ›

4 You're all set!

Project
D DevOps course
Pinned
Issues 0
Merge requests 0
Manage
Plan
Code
Merge requests 0
Repository
Branches
Commits
Tags
Repository graph
Compare revisions
Snippets
Build
Secure
Deploy
Operate
Monitor
Analyze
Settings
What's new 3
Help
Collapse sidebar

implement_example devops-course / .gitlab-ci.yml

.gitlab-ci.yml

Find file | Blame | Edit

Add .gitlab-ci.yml
Kevin Munari authored 4 minutes ago

326991ed | History

✓ This GitLab CI configuration is valid. Learn more

.gitlab-ci.yml 512 B

```yaml
sonarqube-check:
  image: maven:3.6.3-jdk-11
  variables:
    SONAR_USER_HOME: "${CI_PROJECT_DIR}/.sonar"  # Defines the location of the analysis task cache
    GIT_DEPTH: "0"  # Tells git to fetch all the branches of the project, required by the analysis task
  cache:
    key: "${CI_JOB_NAME}"
    paths:
      - .sonar/cache
  script:
    - mvn verify sonar:sonar -Dsonar.projectKey=devops-course -Dsonar.coverage.jacoco.xmlReportPaths="./*/target/site/jacoco/*.xml"
  allow_failure: true
  only:
    - main

```

DevOps course main

Analyze your project with GitLab CI

1 Set your project key

2 Add environment variables

3 Create or update the configuration file

4 You're all set!

You're all set and ready to improve the quality and security of your code!

Commit and push your code to start the analysis.
Each new push you make on your main branch will trigger a new analysis in SonarQube.

This page will then refresh with your analysis results.
If the page doesn't refresh after a while, please double-check the analysis configuration, and check your logs.

Waiting for the first analysis to come in...

Project
D DevOps course
Pinned
Issues 0
Merge requests 0
Manage
Plan
Code
Build
Secure
Deploy
Operate
Monitor
Analyze
Settings
General
Integrations
Webhooks
Access tokens
Repository
Merge requests
CI/CD
Packages and registries
What's new 3
Help
Collapse sidebar

Search page

General pipelines

Customize your pipeline configuration.

Auto DevOps

Automate building, testing, and deploying your applications based on your continuous integration and delivery configuration. How do I get started?

Runners

Runners are processes that pick up and execute CI/CD jobs for GitLab. What is GitLab Runner?

Artifacts

A job artifact is an archive of files and directories saved by a job when it finishes.

Variables

Variables store information that you can use in job scripts. Each project can define a maximum of 8000 variables. Learn more.

Pipeline trigger tokens

Trigger a pipeline for a branch or tag by generating a trigger token and using it with an API call. The token impersonates a user's project access and permissions. Learn more.

Deploy freezes

Add a freeze period to prevent unintended releases during a period of time for a given environment. You must update the deployment jobs in `.gitlab-ci.yml` according to the deploy freezes added here. Learn more. Specify deploy freezes using cron syntax.

Job token permissions

Control which groups and projects can use CI/CD job tokens to authenticate with this project. Learn more about job token security.

Project
D DevOps course
Pinned
Issues 0
Merge requests 0
Manage
Plan
Code
Build
Secure
Deploy
Operate
Monitor
Analyze
Settings
General
Integrations
Webhooks
Access tokens
Repository
Merge requests
CI/CD
Packages and registries
What's new 3
Help
Collapse sidebar

Search page

General pipelines

Customize your pipeline configuration.

Auto DevOps

Automate building, testing, and deploying your applications based on your continuous integration and delivery configuration. How do I get started?

Runners

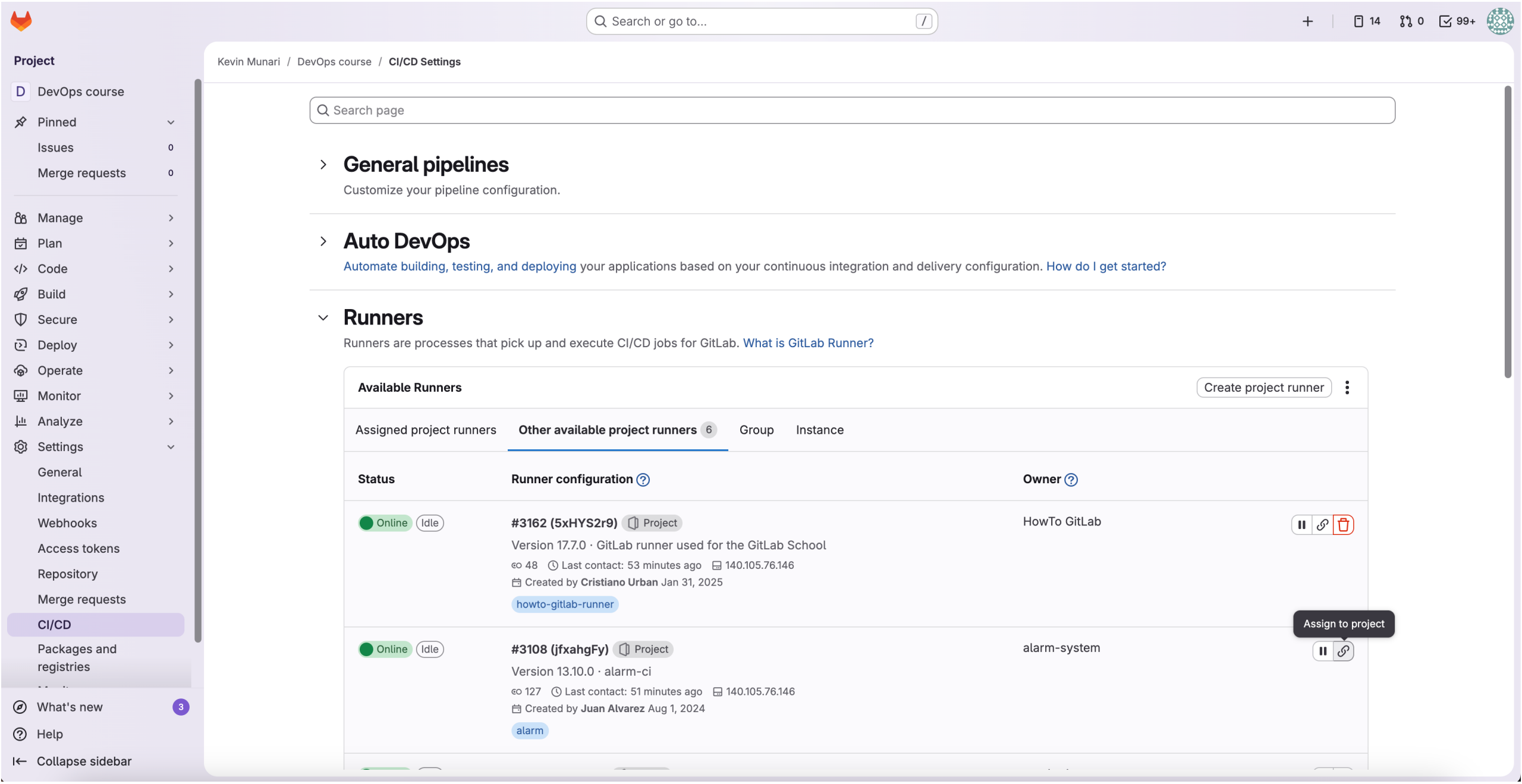
Runners are processes that pick up and execute CI/CD jobs for GitLab. What is GitLab Runner?

Available Runners Create project runner

Assigned project runners | Other available project runners 6 | Group | Instance

No project runners found

This project does not have any project runners yet. To add them, select **Create project runner**.


Search or go to... /
14
0
99+
Project
DevOps course
Pinned
Issues 0
Merge requests 0
Manage
Plan
Code
Build
Secure
Deploy
Operate
Monitor
Analyze
Settings
General
Integrations
Webhooks
Access tokens
Repository
Merge requests
CI/CD
Packages and registries
What's new 3
Help
Collapse sidebar
Kevin Munari / DevOps course / CI/CD Settings
Search page
General pipelines
Customize your pipeline configuration.
Auto DevOps
Automate building, testing, and deploying your applications based on your continuous integration and delivery configuration. How do I get started?
Runners
Runners are processes that pick up and execute CI/CD jobs for GitLab. What is GitLab Runner?
Available Runners
Create project runner
Assigned project runners
Other available project runners 6
Group
Instance
Status
Runner configuration
Owner
Online Idle
#3162 (5xHYS2r9) Project
Version 17.7.0 · GitLab runner used for the GitLab School
48 Last contact: 53 minutes ago 140.105.76.146
Created by Cristiano Urban Jan 31, 2025
howto-gitlab-runner
HowTo GitLab
Assign to project
Online Idle
#3108 (jfxahgFy) Project
Version 13.10.0 · alarm-ci
127 Last contact: 51 minutes ago 140.105.76.146
Created by Juan Alvarez Aug 1, 2024
alarm
alarm-system

Project
D DevOps course
Pinned
Issues 0
Merge requests 0
Manage
Plan
Code
Build
Secure
Deploy
Operate
Monitor
Analyze
Settings
General
Integrations
Webhooks
Access tokens
Repository
Merge requests
CI/CD
Packages and registries
What's new 3
Help
Collapse sidebar

Search page

General pipelines

Customize your pipeline configuration.

Auto DevOps

Automate building, testing, and deploying your applications based on your continuous integration and delivery configuration. How do I get started?

Runners

Runners are processes that pick up and execute CI/CD jobs for GitLab. What is GitLab Runner?

Available Runners — Create project runner

Assigned project runners 1 | Other available project runners 5 | Group | Instance

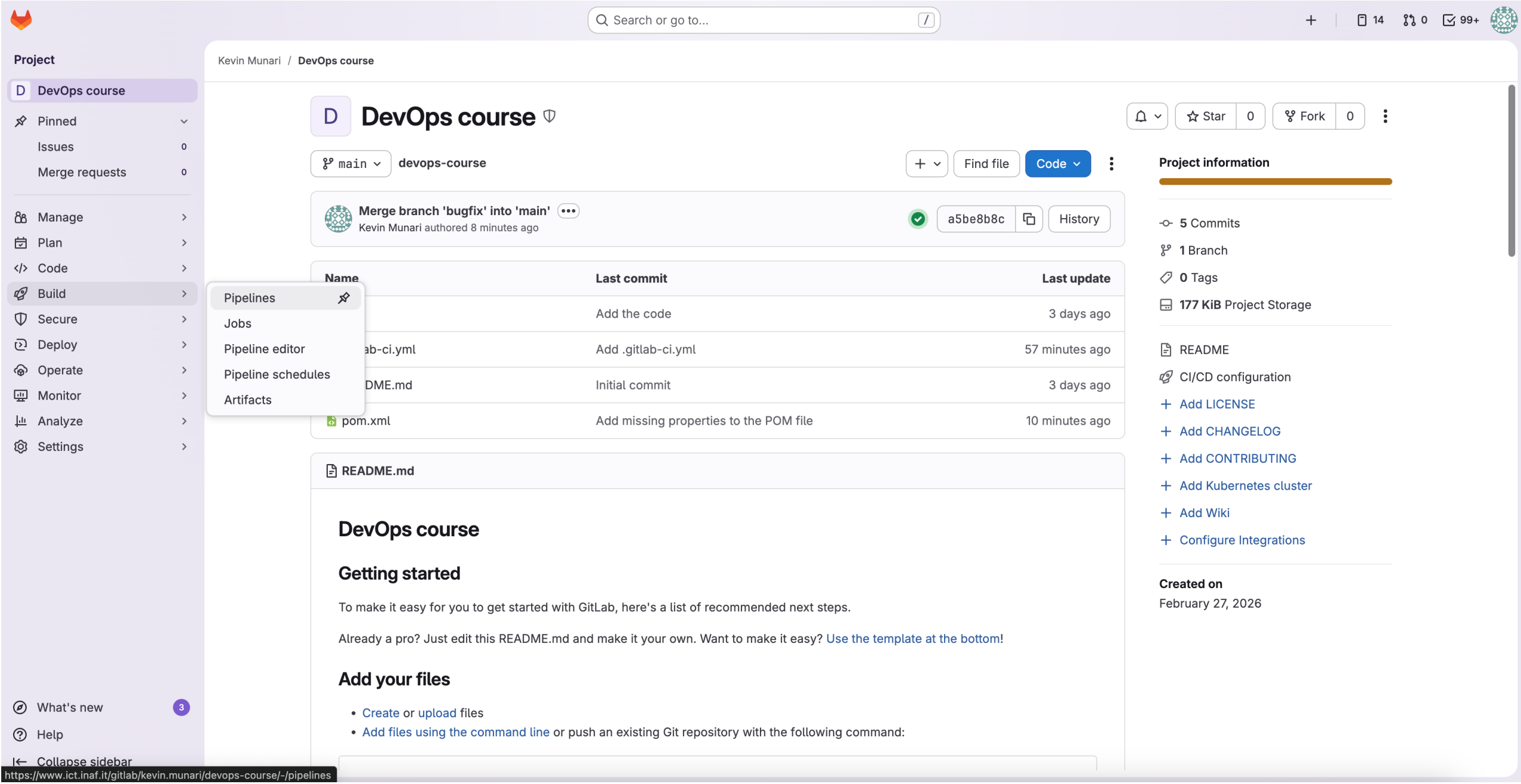
Status	Runner configuration	Owner
Online Idle	#3108 (jfxahgFy) Project Version 13.10.0 · alarm-ci 127 Last contact: 1 minute ago 140.105.76.146 Created by **Juan Alvarez** Aug 1, 2024 alarm	alarm-system

Artifacts

A job artifact is an archive of files and directories saved by a job when it finishes.

Variables

Variables store information that you can use in job scripts. Each project can define a maximum of 8000 variables. Learn more.


Search or go to...
14
0
99+
Project
DevOps course
Pinned
Issues 0
Merge requests 0
Manage
Plan
Code
Build
Secure
Deploy
Operate
Monitor
Analyze
Settings
What's new 3
Help
Collapse sidebar
Kevin Munari / DevOps course
DevOps course
Star 0
Fork 0
main
devops-course
Find file
Code
Merge branch 'bugfix' into 'main'
Kevin Munari authored 8 minutes ago
a5be8b8c
History
Pipelines
Jobs
Pipeline editor
Pipeline schedules
Artifacts
Name
Last commit
Last update
Add the code
3 days ago
ab-ci.yml
Add .gitlab-ci.yml
57 minutes ago
DME.md
Initial commit
3 days ago
pom.xml
Add missing properties to the POM file
10 minutes ago
README.md
DevOps course
Getting started
To make it easy for you to get started with GitLab, here's a list of recommended next steps.
Already a pro? Just edit this README.md and make it your own. Want to make it easy? Use the template at the bottom!
Add your files
Create or upload files
Add files using the command line or push an existing Git repository with the following command:
Project information
5 Commits
1 Branch
0 Tags
177 KiB Project Storage
README
CI/CD configuration
Add LICENSE
Add CHANGELOG
Add CONTRIBUTING
Add Kubernetes cluster
Add Wiki
Configure Integrations
Created on
February 27, 2026
https://www.ict.inaf.it/gitlab/kevin.munari/devops-course/-/pipelines

Search or go to... /

14 0 99+

Project

D DevOps course

- Pinned
  - Issues 0
  - Merge requests 0
- Manage
- Plan
- Code
- Build
  - Pipelines
  - Jobs
  - Pipeline editor
  - Pipeline schedules
  - Artifacts
- Secure
- Deploy
- Operate
- Monitor
- Analyze
- Settings

What's new 3

Help

Collapse sidebar

Kevin Munari / DevOps course / **Pipelines**

All 2 | Finished | Branches | Tags

View analytics | Clear runner caches | New pipeline

Filter pipelines | Show Pipeline ID

Status	Pipeline	Created by	Stages	Actions
Passed 00:00:55 8 minutes ago	Merge branch 'bugfix' into 'main' #34859 main a5be8b8c latest branch			
Warning 00:00:29 31 minutes ago	Merge branch 'implement_example' into '... #34857 main 5eefa29b branch			

Search or go to... /

14 0 99+

Project

D DevOps course

Pinned
- Issues 0
- Merge requests 0

Manage
Plan
Code
Build
- Pipelines
- Jobs
- Pipeline editor
- Pipeline schedules
- Artifacts

Secure
Deploy
Operate
Monitor
Analyze
Settings

What's new 3
Help
Collapse sidebar

Kevin Munari / DevOps course / Pipelines / #34859

Merge branch 'bugfix' into 'main'

Delete

Passed Created 13 minutes ago by **Kevin Munari**, finished 12 minutes ago

For commit `a5be8b8c`

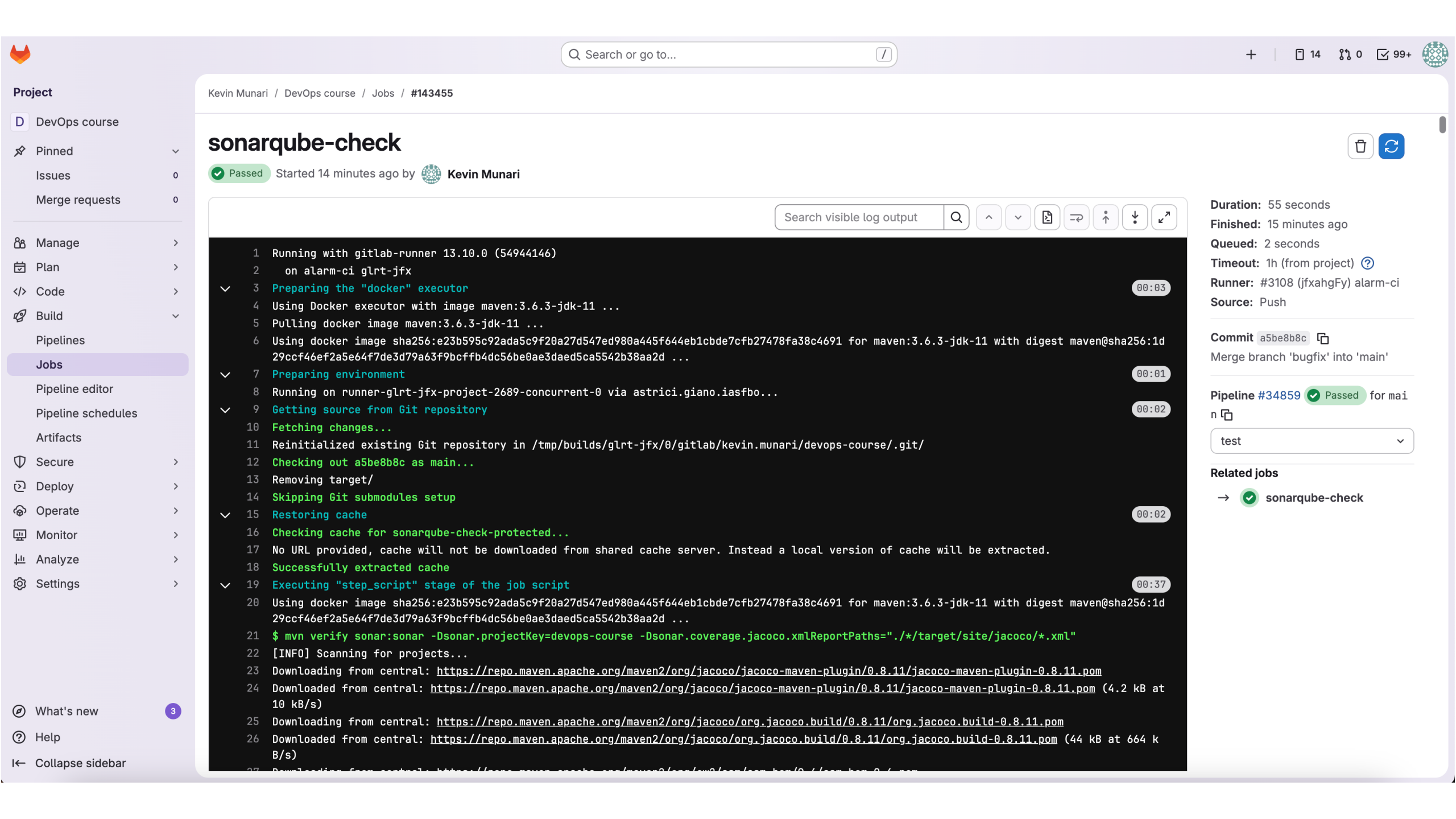
In `main`

latest branch 1 job 55 seconds, queued for 5 seconds

Pipeline Jobs 1 Tests 0

test

sonarqube-check


Search or go to...
14
0
99+
Project
DevOps course
Pinned
Issues 0
Merge requests 0
Manage
Plan
Code
Build
Pipelines
Jobs
Pipeline editor
Pipeline schedules
Artifacts
Secure
Deploy
Operate
Monitor
Analyze
Settings
What's new 3
Help
Collapse sidebar
Kevin Munari / DevOps course / Jobs / #143455
sonarqube-check
Passed Started 14 minutes ago by Kevin Munari
Search visible log output
1 Running with gitlab-runner 13.10.0 (54944146)
2 on alarm-ci glrt-jfx
3 Preparing the "docker" executor 00:03
4 Using Docker executor with image maven:3.6.3-jdk-11 ...
5 Pulling docker image maven:3.6.3-jdk-11 ...
6 Using docker image sha256:e23b595c92ada5c9f20a27d547ed980a445f644eb1cbde7cfb27478fa38c4691 for maven:3.6.3-jdk-11 with digest maven@sha256:1d29ccf46ef2a5e64f7de3d79a63f9bcffb4dc56be0ae3daed5ca5542b38aa2d ...
7 Preparing environment 00:01
8 Running on runner-glrt-jfx-project-2689-concurrent-0 via astrici.giano.iasfbo...
9 Getting source from Git repository 00:02
10 Fetching changes...
11 Reinitialized existing Git repository in /tmp/builds/glrt-jfx/0/gitlab/kevin.munari/devops-course/.git/
12 Checking out a5be8b8c as main...
13 Removing target/
14 Skipping Git submodules setup
15 Restoring cache 00:02
16 Checking cache for sonarqube-check-protected...
17 No URL provided, cache will not be downloaded from shared cache server. Instead a local version of cache will be extracted.
18 Successfully extracted cache
19 Executing "step_script" stage of the job script 00:37
20 Using docker image sha256:e23b595c92ada5c9f20a27d547ed980a445f644eb1cbde7cfb27478fa38c4691 for maven:3.6.3-jdk-11 with digest maven@sha256:1d29ccf46ef2a5e64f7de3d79a63f9bcffb4dc56be0ae3daed5ca5542b38aa2d ...
21 $ mvn verify sonar:sonar -Dsonar.projectKey=devops-course -Dsonar.coverage.jacoco.xmlReportPaths="./*/target/site/jacoco/*.xml"
22 [INFO] Scanning for projects...
23 Downloading from central: https://repo.maven.apache.org/maven2/org/jacoco/jacoco-maven-plugin/0.8.11/jacoco-maven-plugin-0.8.11.pom
24 Downloaded from central: https://repo.maven.apache.org/maven2/org/jacoco/jacoco-maven-plugin/0.8.11/jacoco-maven-plugin-0.8.11.pom (4.2 kB at 10 kB/s)
25 Downloading from central: https://repo.maven.apache.org/maven2/org/jacoco/org.jacoco.build/0.8.11/org.jacoco.build-0.8.11.pom
26 Downloaded from central: https://repo.maven.apache.org/maven2/org/jacoco/org.jacoco.build/0.8.11/org.jacoco.build-0.8.11.pom (44 kB at 664 kB/s)
Duration: 55 seconds
Finished: 15 minutes ago
Queued: 2 seconds
Timeout: 1h (from project)
Runner: #3108 (jfxahgFy) alarm-ci
Source: Push
Commit a5be8b8c
Merge branch 'bugfix' into 'main'
Pipeline #34859 Passed for main
test
Related jobs
sonarqube-check

Search or go to... /

14 0 99+

Project

D DevOps course

Pinned
Issues 0
Merge requests 0

Manage
Plan
Code
Build
Pipelines
Jobs
Pipeline editor
Pipeline schedules
Artifacts
Secure
Deploy
Operate
Monitor
Analyze
Settings

What's new 3
Help
Collapse sidebar

Kevin Munari / DevOps course / Jobs / #143455

Search visible log output

```
657 -------------------------------------------------------
658  T E S T S
659 -------------------------------------------------------
660 Running it.inaf.devops.ExampleTest
661 Tests run: 1, Failures: 0, Errors: 0, Skipped: 0, Time elapsed: 0.143 sec
662 Results :
663 Tests run: 1, Failures: 0, Errors: 0, Skipped: 0
664 [INFO]
665 [INFO] --- jacoco-maven-plugin:0.8.11:report (report) @ sonar-qube-example ---
666 [INFO] Loading execution data file /tmp/builds/glrt-jfx/0/gitlab/kevin.munari/devops-course/target/jacoco.exec
667 [INFO] Analyzed bundle 'sonar-qube-example' with 1 classes
668 [INFO]
669 [INFO] --- maven-jar-plugin:2.4:jar (default-jar) @ sonar-qube-example ---
670 Downloading from central: https://repo.maven.apache.org/maven2/org/apache/maven/maven-archiver/2.5/maven-archiver-2.5.pom
671 Downloaded from central: https://repo.maven.apache.org/maven2/org/apache/maven/maven-archiver/2.5/maven-archiver-2.5.pom (4.5 kB at 91 kB/s)
672 Downloading from central: https://repo.maven.apache.org/maven2/org/codehaus/plexus/plexus-archiver/2.1/plexus-archiver-2.1.pom
673 Downloaded from central: https://repo.maven.apache.org/maven2/org/codehaus/plexus/plexus-archiver/2.1/plexus-archiver-2.1.pom (2.8 kB at 56 k
    B/s)
674 Downloading from central: https://repo.maven.apache.org/maven2/org/codehaus/plexus/plexus-utils/3.0/plexus-utils-3.0.pom
675 Downloaded from central: https://repo.maven.apache.org/maven2/org/codehaus/plexus/plexus-utils/3.0/plexus-utils-3.0.pom (4.1 kB at 75 kB/s)
676 Downloading from central: https://repo.maven.apache.org/maven2/org/sonatype/spice/spice-parent/16/spice-parent-16.pom
677 Downloaded from central: https://repo.maven.apache.org/maven2/org/sonatype/spice/spice-parent/16/spice-parent-16.pom (8.4 kB at 104 kB/s)
678 Downloading from central: https://repo.maven.apache.org/maven2/org/sonatype/forge/forge-parent/5/forge-parent-5.pom
679 Downloaded from central: https://repo.maven.apache.org/maven2/org/sonatype/forge/forge-parent/5/forge-parent-5.pom (8.4 kB at 133 kB/s)
680 Downloading from central: https://repo.maven.apache.org/maven2/org/codehaus/plexus/plexus-io/2.0.2/plexus-io-2.0.2.pom
681 Downloaded from central: https://repo.maven.apache.org/maven2/org/codehaus/plexus/plexus-io/2.0.2/plexus-io-2.0.2.pom (1.7 kB at 33 kB/s)
682 Downloading from central: https://repo.maven.apache.org/maven2/org/codehaus/plexus/plexus-components/1.1.19/plexus-components-1.1.19.pom
683 Downloaded from central: https://repo.maven.apache.org/maven2/org/codehaus/plexus/plexus-components/1.1.19/plexus-components-1.1.19.pom (2.7
    kB at 49 kB/s)
684 Downloading from central: https://repo.maven.apache.org/maven2/org/codehaus/plexus/plexus/3.0.1/plexus-3.0.1.pom
685 Downloaded from central: https://repo.maven.apache.org/maven2/org/codehaus/plexus/plexus/3.0.1/plexus-3.0.1.pom (19 kB at 358 kB/s)
686 Downloading from central: https://repo.maven.apache.org/maven2/org/codehaus/plexus/plexus-interpolation/1.15/plexus-interpolation-1.15.pom
687 Downloaded from central: https://repo.maven.apache.org/maven2/org/codehaus/plexus/plexus-interpolation/1.15/plexus-interpolation-1.15.pom (1.
    0 kB at 20 kB/s)
688 Downloading from central: https://repo.maven.apache.org/maven2/commons-lang/commons-lang/2.1/commons-lang-2.1.pom
```

Duration: 55 seconds
Finished: 16 minutes ago
Queued: 2 seconds
Timeout: 1h (from project)
Runner: #3108 (jfxahgFy) alarm-ci
Source: Push

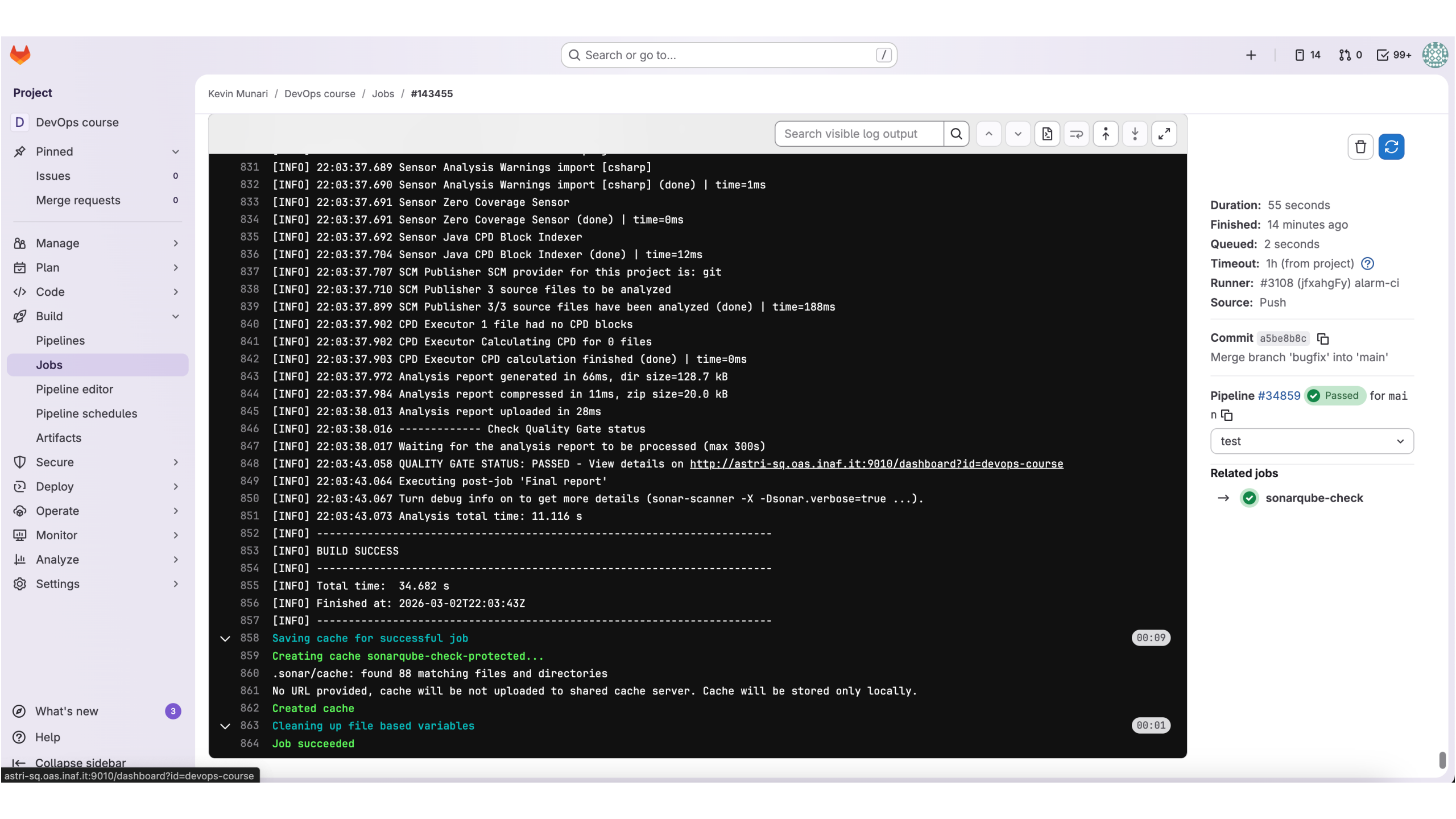
Commit a5be8b8c
Merge branch 'bugfix' into 'main'

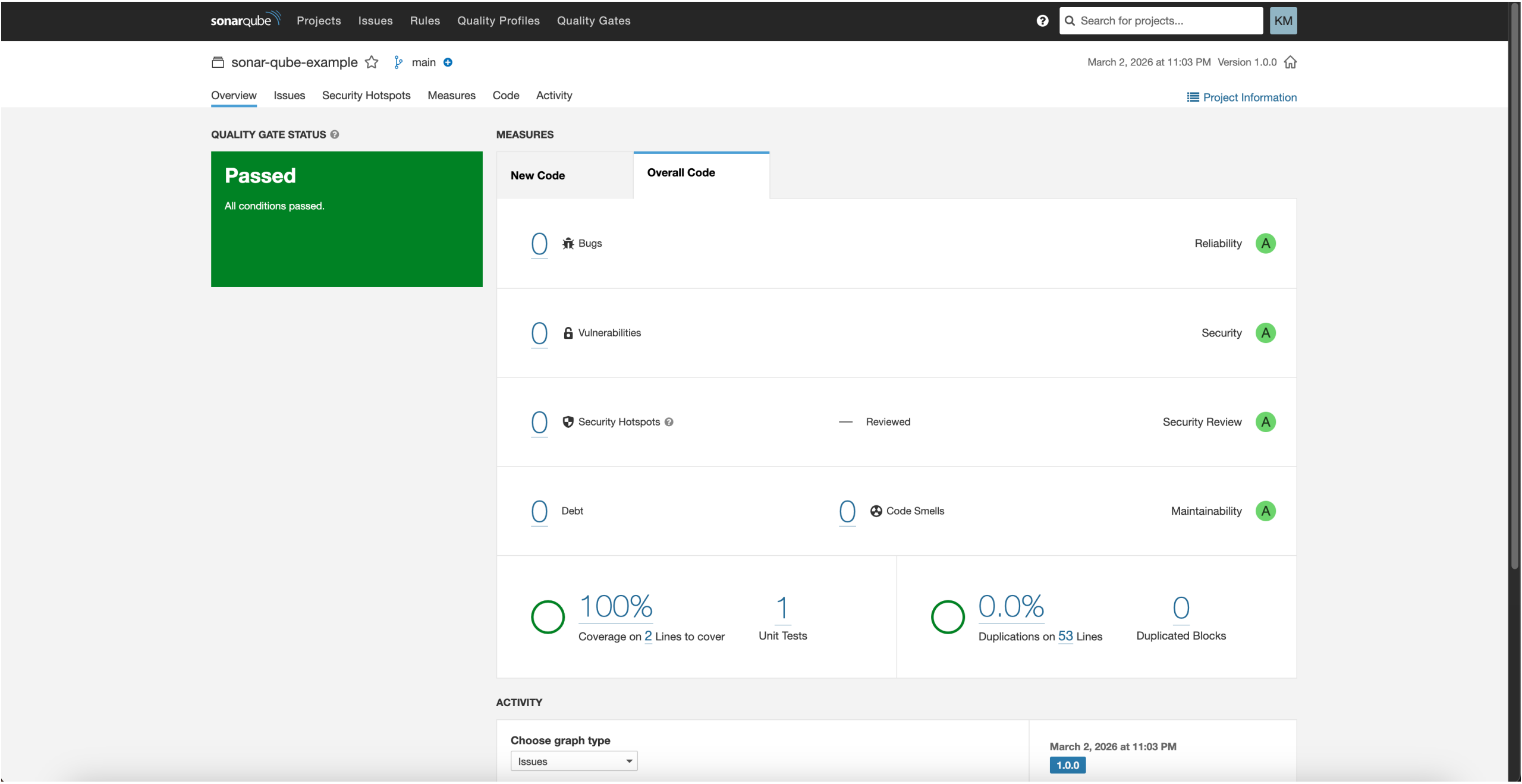
Pipeline #34859 Passed for mai
n

test

Related jobs

→ sonarqube-check


Search or go to...
14
0
99+
Project
DevOps course
Pinned
Issues 0
Merge requests 0
Manage
Plan
Code
Build
Pipelines
Jobs
Pipeline editor
Pipeline schedules
Artifacts
Secure
Deploy
Operate
Monitor
Analyze
Settings
What's new 3
Help
Collapse sidebar
Kevin Munari / DevOps course / Jobs / #143455
Search visible log output
831 [INFO] 22:03:37.689 Sensor Analysis Warnings import [csharp]
832 [INFO] 22:03:37.690 Sensor Analysis Warnings import [csharp] (done) | time=1ms
833 [INFO] 22:03:37.691 Sensor Zero Coverage Sensor
834 [INFO] 22:03:37.691 Sensor Zero Coverage Sensor (done) | time=0ms
835 [INFO] 22:03:37.692 Sensor Java CPD Block Indexer
836 [INFO] 22:03:37.704 Sensor Java CPD Block Indexer (done) | time=12ms
837 [INFO] 22:03:37.707 SCM Publisher SCM provider for this project is: git
838 [INFO] 22:03:37.710 SCM Publisher 3 source files to be analyzed
839 [INFO] 22:03:37.899 SCM Publisher 3/3 source files have been analyzed (done) | time=188ms
840 [INFO] 22:03:37.902 CPD Executor 1 file had no CPD blocks
841 [INFO] 22:03:37.902 CPD Executor Calculating CPD for 0 files
842 [INFO] 22:03:37.903 CPD Executor CPD calculation finished (done) | time=0ms
843 [INFO] 22:03:37.972 Analysis report generated in 66ms, dir size=128.7 kB
844 [INFO] 22:03:37.984 Analysis report compressed in 11ms, zip size=20.0 kB
845 [INFO] 22:03:38.013 Analysis report uploaded in 28ms
846 [INFO] 22:03:38.016 ------------ Check Quality Gate status
847 [INFO] 22:03:38.017 Waiting for the analysis report to be processed (max 300s)
848 [INFO] 22:03:43.058 QUALITY GATE STATUS: PASSED - View details on http://astri-sq.oas.inaf.it:9010/dashboard?id=devops-course
849 [INFO] 22:03:43.064 Executing post-job 'Final report'
850 [INFO] 22:03:43.067 Turn debug info on to get more details (sonar-scanner -X -Dsonar.verbose=true ...).
851 [INFO] 22:03:43.073 Analysis total time: 11.116 s
852 [INFO] --
853 [INFO] BUILD SUCCESS
854 [INFO] --
855 [INFO] Total time: 34.682 s
856 [INFO] Finished at: 2026-03-02T22:03:43Z
857 [INFO] --
858 Saving cache for successful job
00:09
859 Creating cache sonarqube-check-protected...
860 .sonar/cache: found 88 matching files and directories
861 No URL provided, cache will be not uploaded to shared cache server. Cache will be stored only locally.
862 Created cache
863 Cleaning up file based variables
00:01
864 Job succeeded
Duration: 55 seconds
Finished: 14 minutes ago
Queued: 2 seconds
Timeout: 1h (from project)
Runner: #3108 (jfxahgFy) alarm-ci
Source: Push
Commit a5be8b8c
Merge branch 'bugfix' into 'main'
Pipeline #34859 Passed for main
test
Related jobs
sonarqube-check
astri-sq.oas.inaf.it:9010/dashboard?id=devops-course


sonarqube
Projects
Issues
Rules
Quality Profiles
Quality Gates
Search for projects...
KM
sonar-qube-example
main
March 2, 2026 at 11:03 PM Version 1.0.0
Overview
Issues
Security Hotspots
Measures
Code
Activity
Project Information
QUALITY GATE STATUS
Passed
All conditions passed.
MEASURES
New Code
Overall Code
0 Bugs
Reliability A
0 Vulnerabilities
Security A
0 Security Hotspots
— Reviewed
Security Review A
0 Debt
0 Code Smells
Maintainability A
100%
Coverage on 2 Lines to cover
1
Unit Tests
0.0%
Duplications on 53 Lines
0
Duplicated Blocks
ACTIVITY
Choose graph type
Issues
March 2, 2026 at 11:03 PM
1.0.0