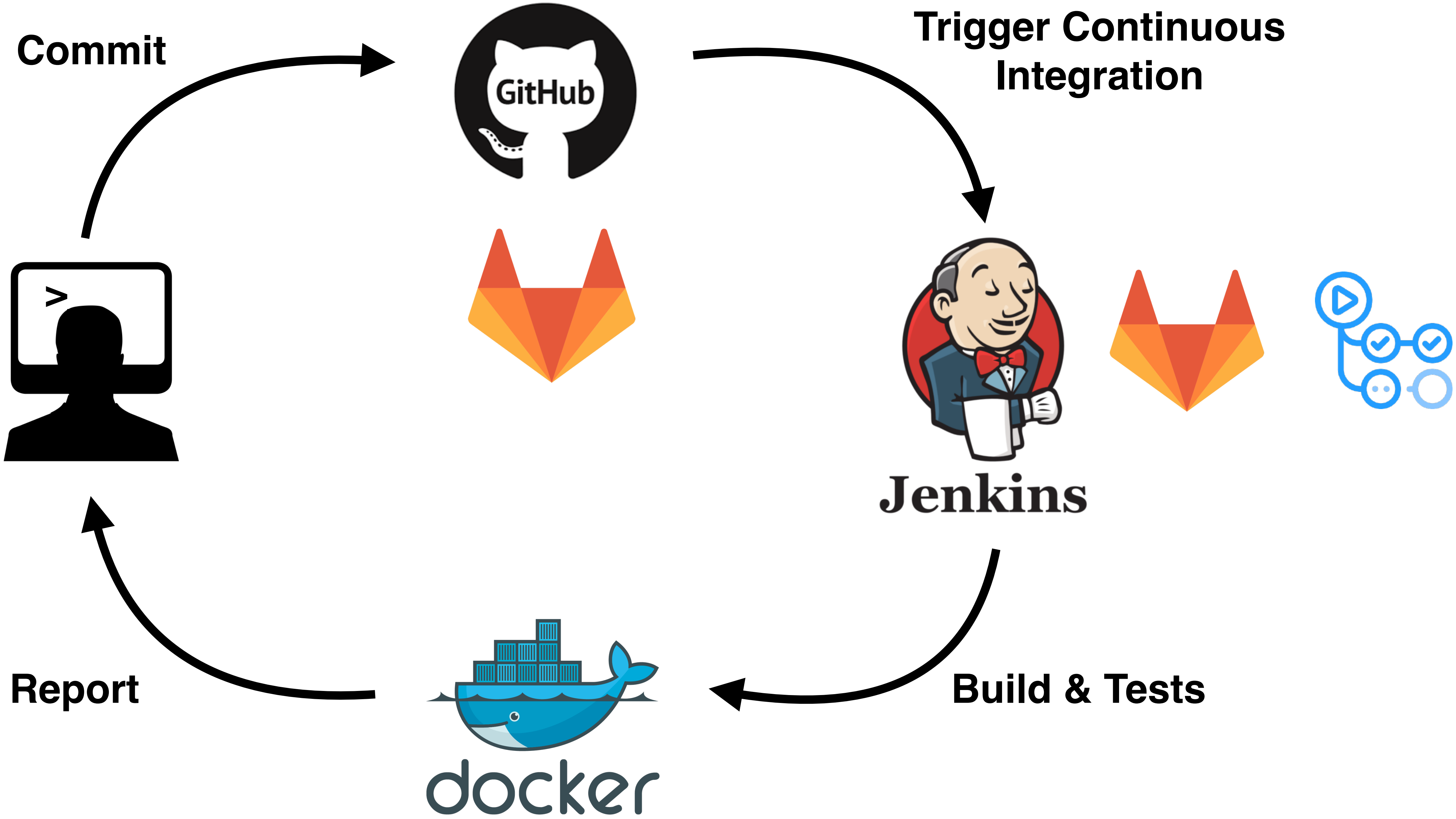
CI and CD on K8S @ CNAF

Andrea Ceccanti
andrea.ceccanti@cnaf.infn.it

Corso OLSS 2021

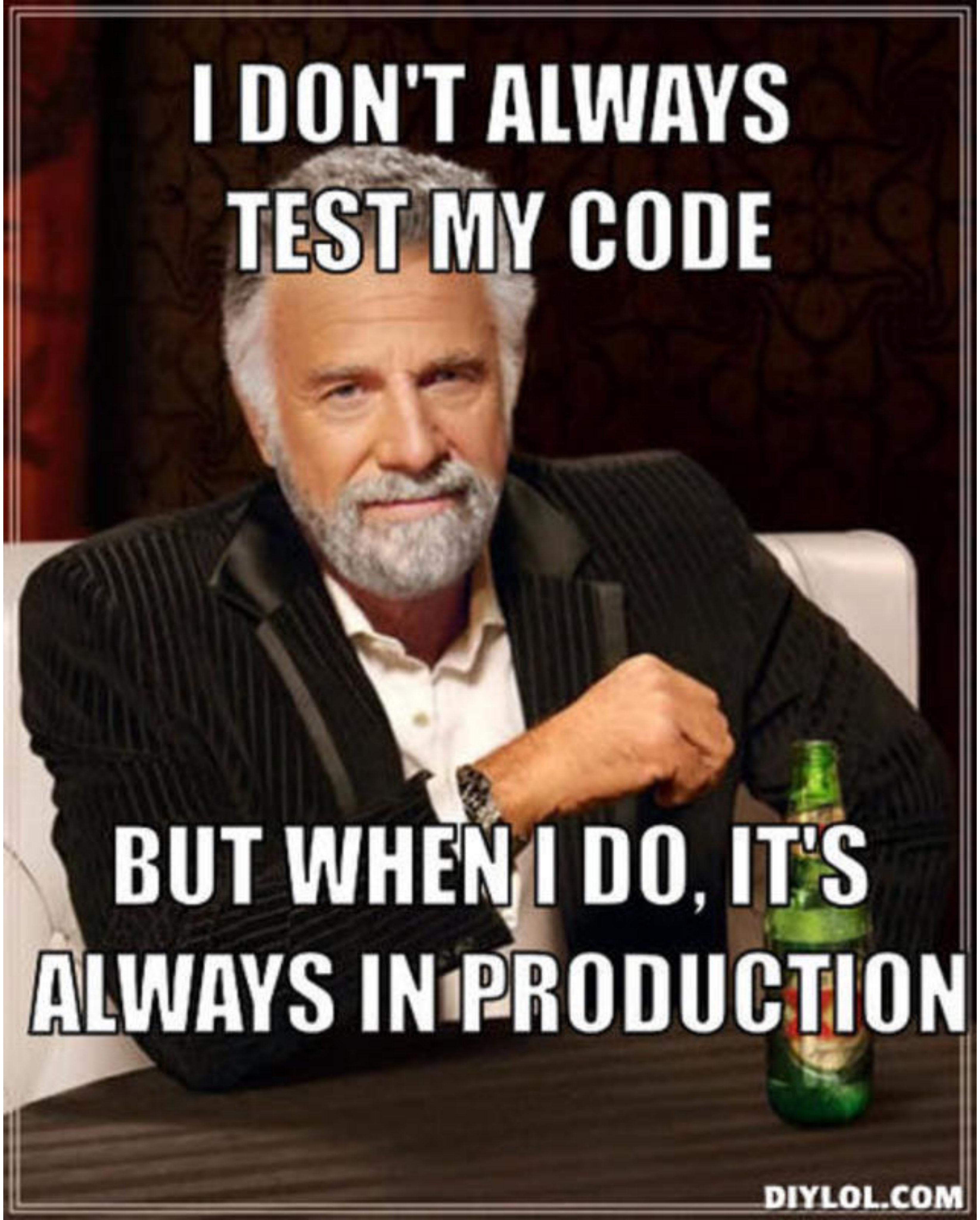
What I will talk about?

Our experience in developing a CI and (almost) CD pipeline for the middleware development team @ CNAF



Why CI and testing?

My code doesn't always work
But when it does, it works on my machine
quickmeme.com


I DON'T ALWAYS TEST MY CODE
BUT WHEN I DO, IT'S ALWAYS IN PRODUCTION
DIYLOL.COM

CI/CD = Process + Tools (+ Perseverance)

Process is **harder to get right** than a working CI/CD pipeline

- overkill process kills productivity, bores everyone to death and does not improve the quality of delivered code
- sloppy process only introduces overhead without quality improvements

The **hardest** thing to change is the developer attitude

- testing is **more important** than coding

Processes are **improved incrementally**, in small steps

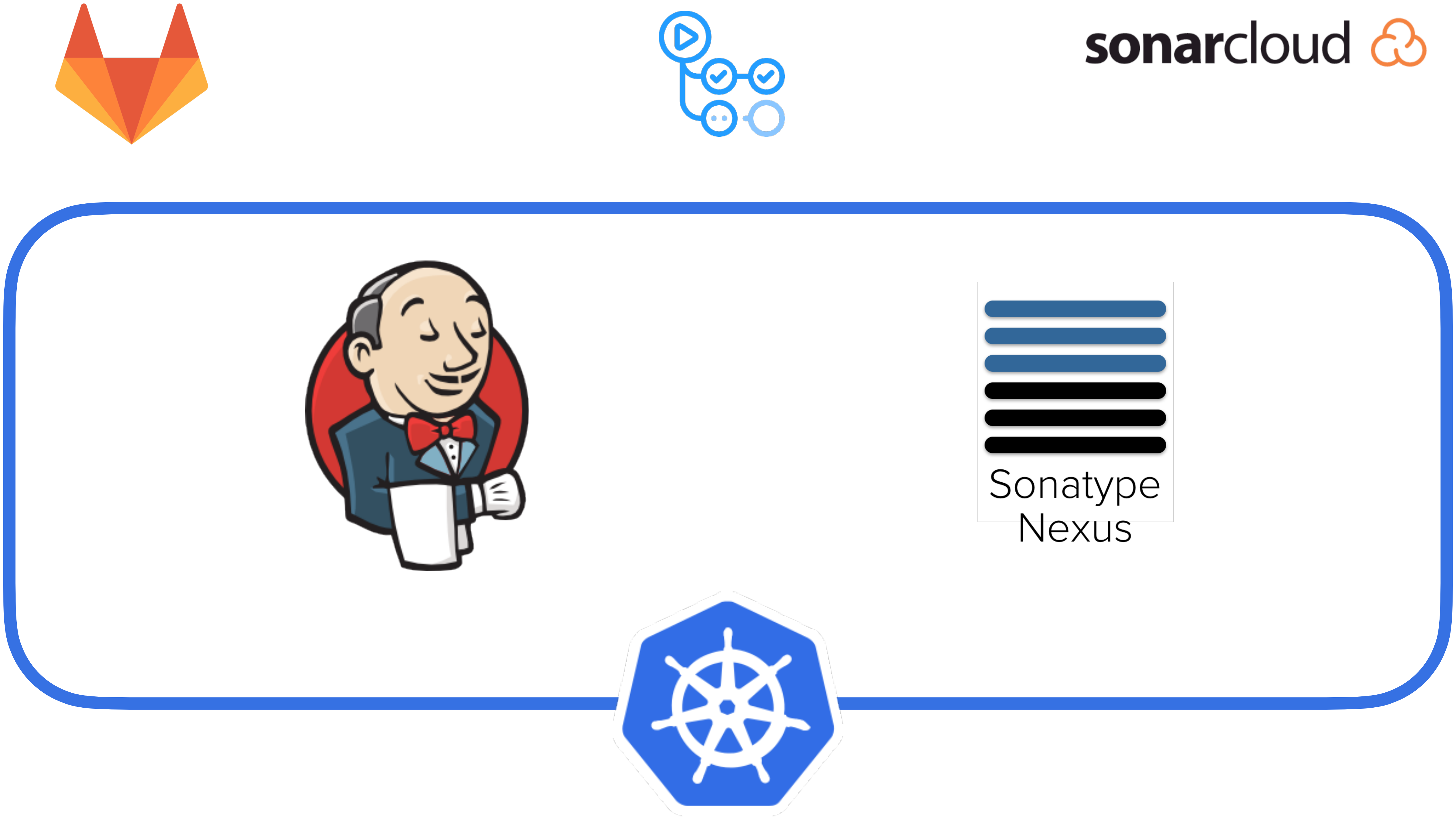
- especially for legacy codebases that mostly work fine in production

Tools are **learned incrementally**, in small steps

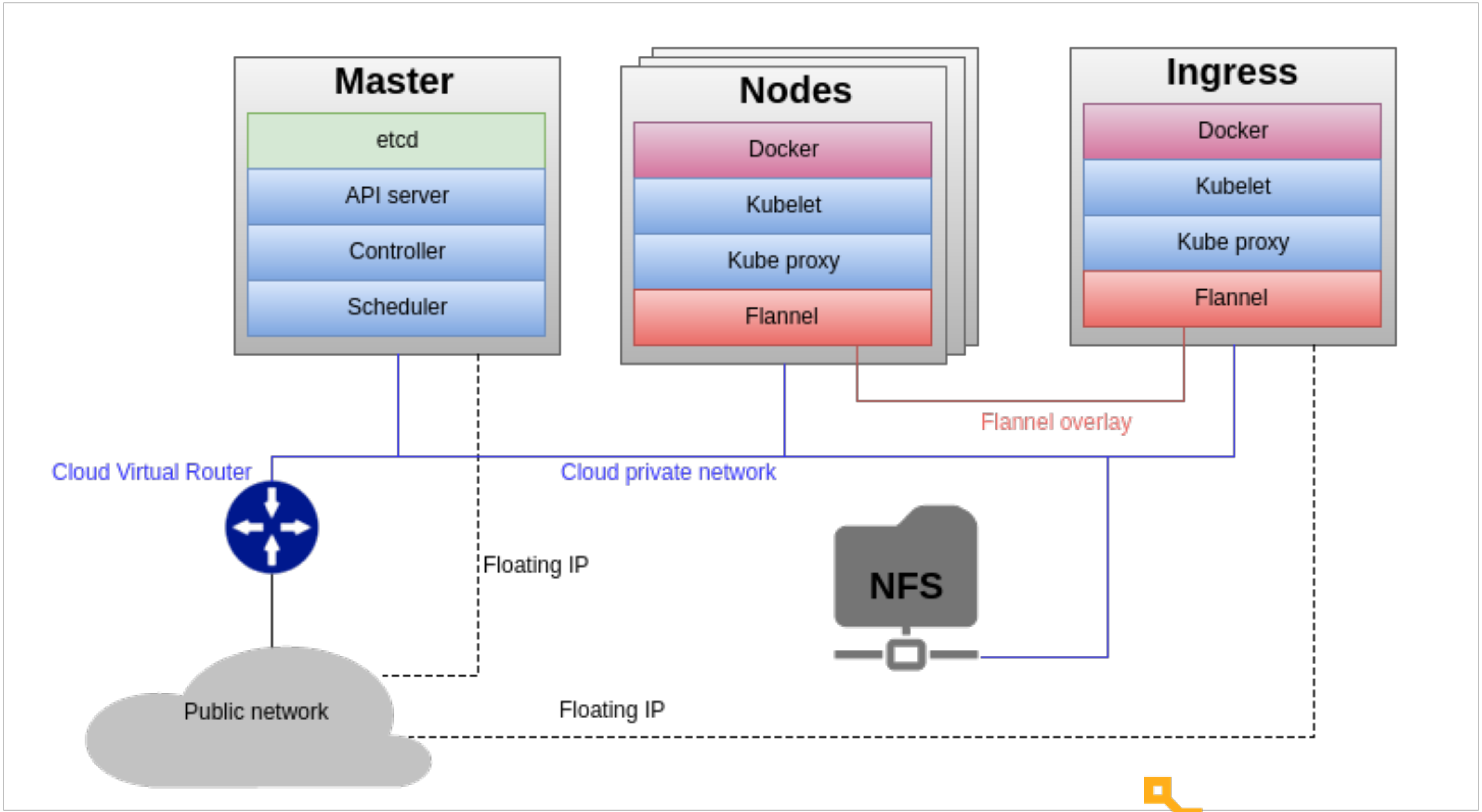
- it can take years to learn how develop and maintain an effective CI/CD pipeline

CI/CD infrastructure

Our CI/CD infrastructure



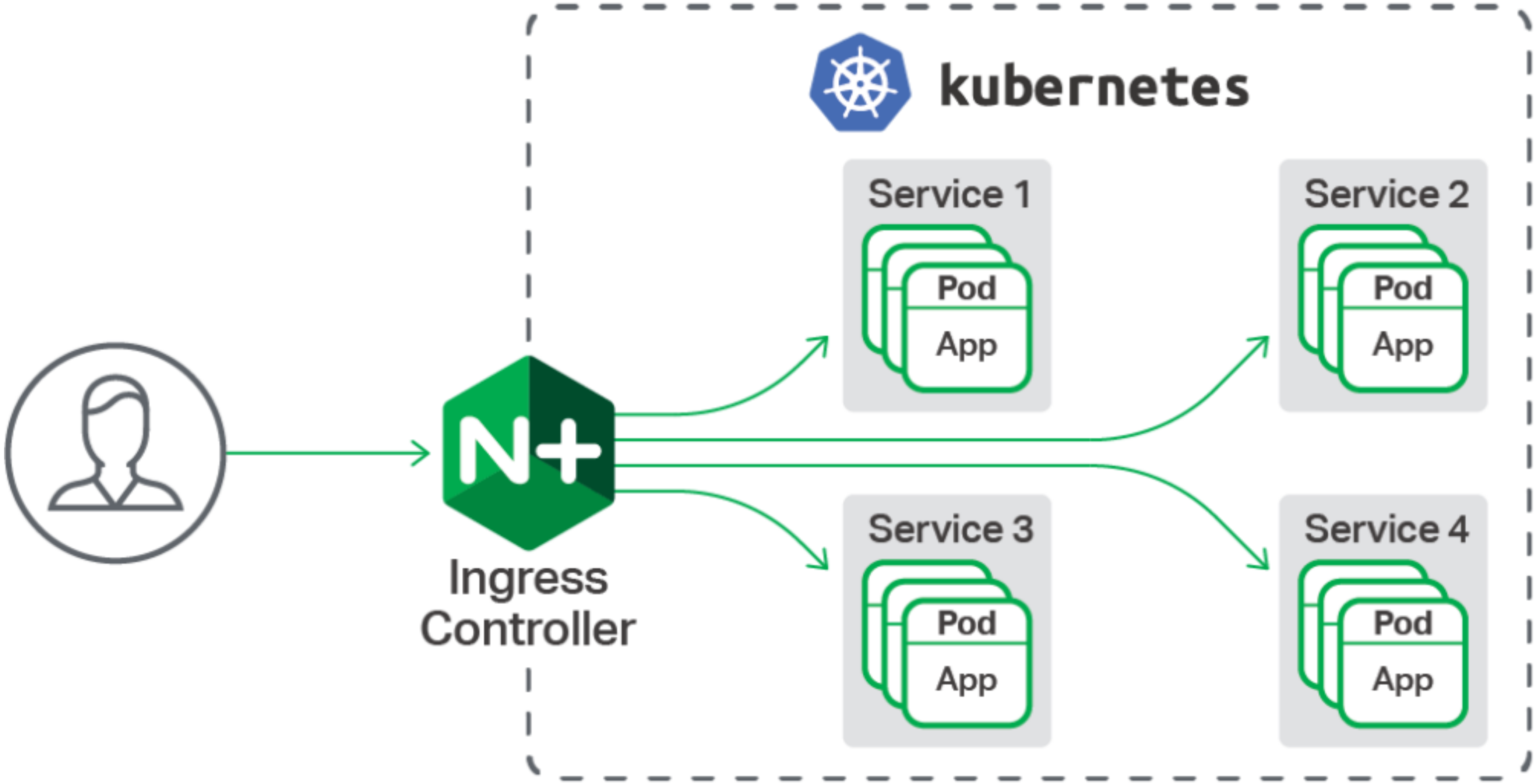
The K8S infrastructure



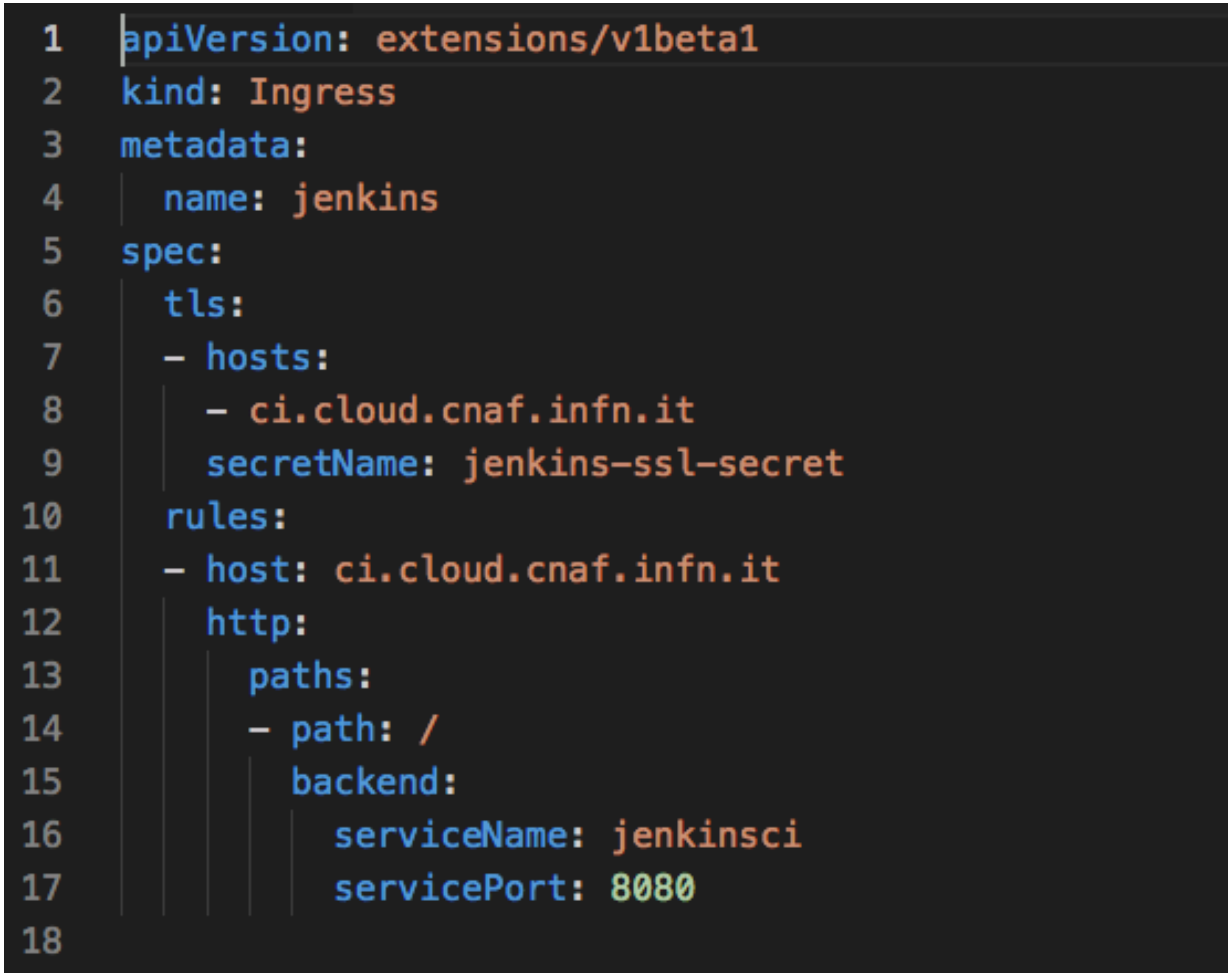
The K8S ingress controller

Allows access to K8S services from the external network

Deployed as a service inside the K8S cluster itself



Example ingress controller config



```
apiVersion: extensions/v1beta1
kind: Ingress
metadata:
  name: jenkins
spec:
  tls:
  - hosts:
    - ci.cloud.cnaf.infn.it
    secretName: jenkins-ssl-secret
  rules:
  - host: ci.cloud.cnaf.infn.it
    http:
      paths:
      - path: /
        backend:
          serviceName: jenkinsci
          servicePort: 8080

```

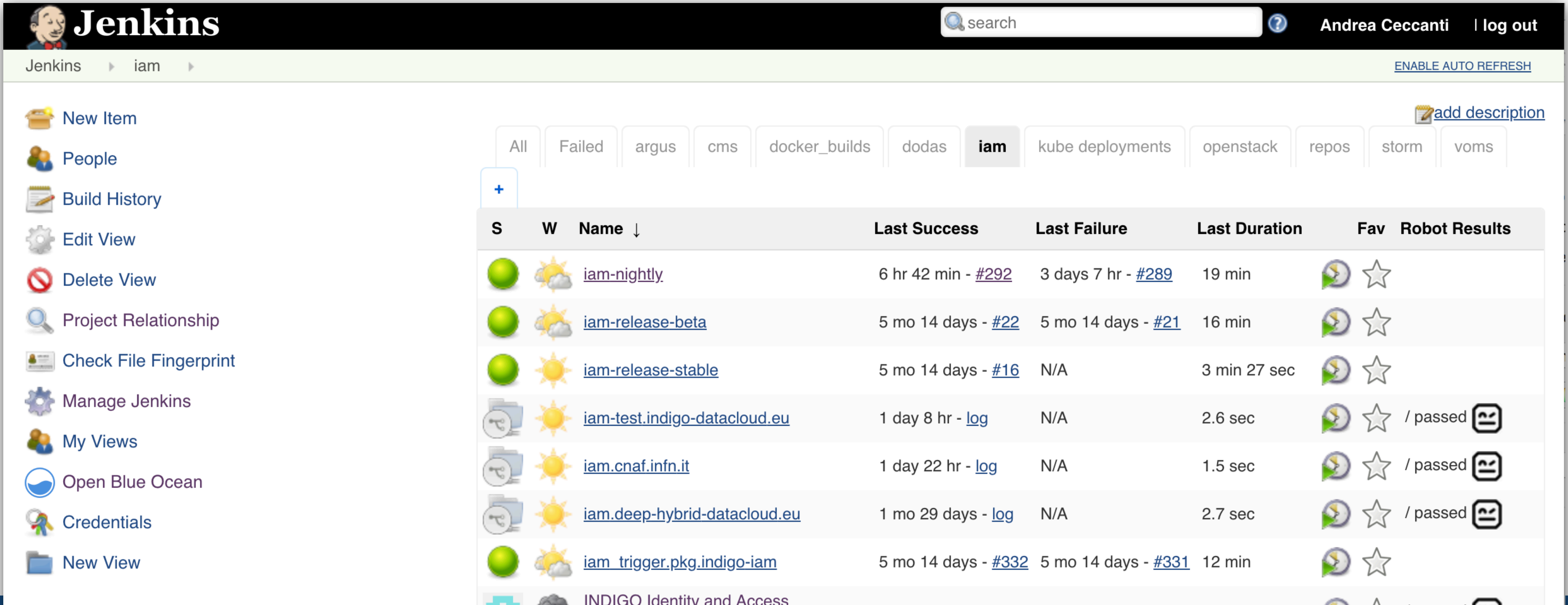
Jenkins

LTS release branch running as a K8S application

Slaves provisioned via the **Kubernetes** plugin

Jenkins Home provisioned as a persistent volume on NFS

- nightly backup



S	W	Name ↓	Last Success	Last Failure	Last Duration	Fav	Robot Results
●	⛅	iam-nightly	6 hr 42 min - #292	3 days 7 hr - #289	19 min	☆	
●	⛅	iam-release-beta	5 mo 14 days - #22	5 mo 14 days - #21	16 min	☆	
●	☀	iam-release-stable	5 mo 14 days - #16	N/A	3 min 27 sec	☆	
	☀	iam-test.indigo-datacloud.eu	1 day 8 hr - log	N/A	2.6 sec	☆	/ passed
	☀	iam.cnaf.infn.it	1 day 22 hr - log	N/A	1.5 sec	☆	/ passed
	☀	iam.deep-hybrid-datacloud.eu	1 mo 29 days - log	N/A	2.7 sec	☆	/ passed
●	⛅	iam_trigger.pkg.indigo-iam	5 mo 14 days - #332	5 mo 14 days - #331	12 min	☆	
		INDIGO Identity and Access					

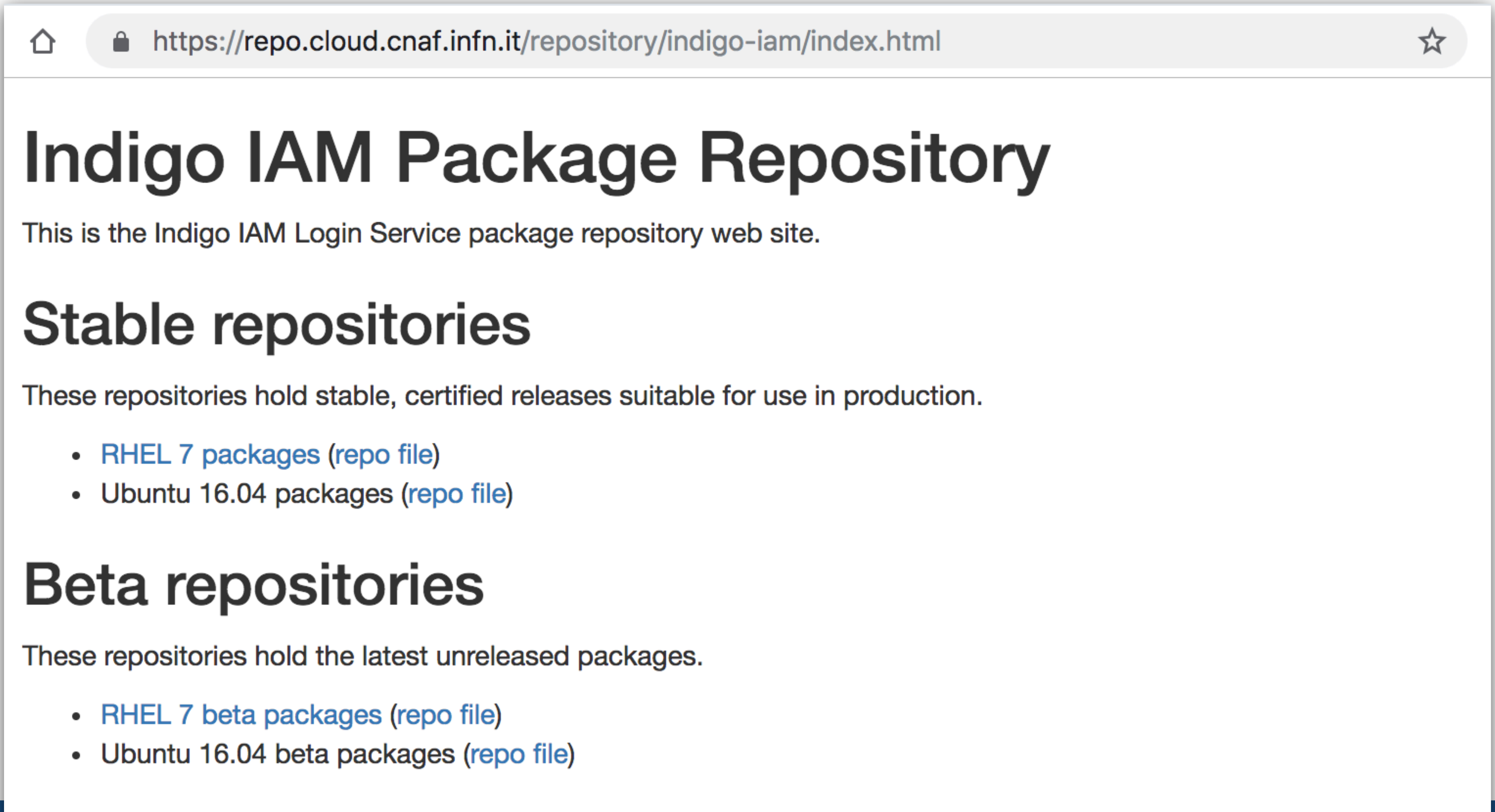
Nexus repository

Sonatype Nexus

Nexus is our CI repository

- Maven repo (local artifacts + Maven central mirror)
- Packages repository

Storage provided as a K8S persistent volume



https://repo.cloud.cnaf.infn.it/repository/indigo-iam/index.html

Indigo IAM Package Repository

This is the Indigo IAM Login Service package repository web site.

Stable repositories

These repositories hold stable, certified releases suitable for use in production.

- RHEL 7 packages (repo file)
- Ubuntu 16.04 packages (repo file)

Beta repositories

These repositories hold the latest unreleased packages.

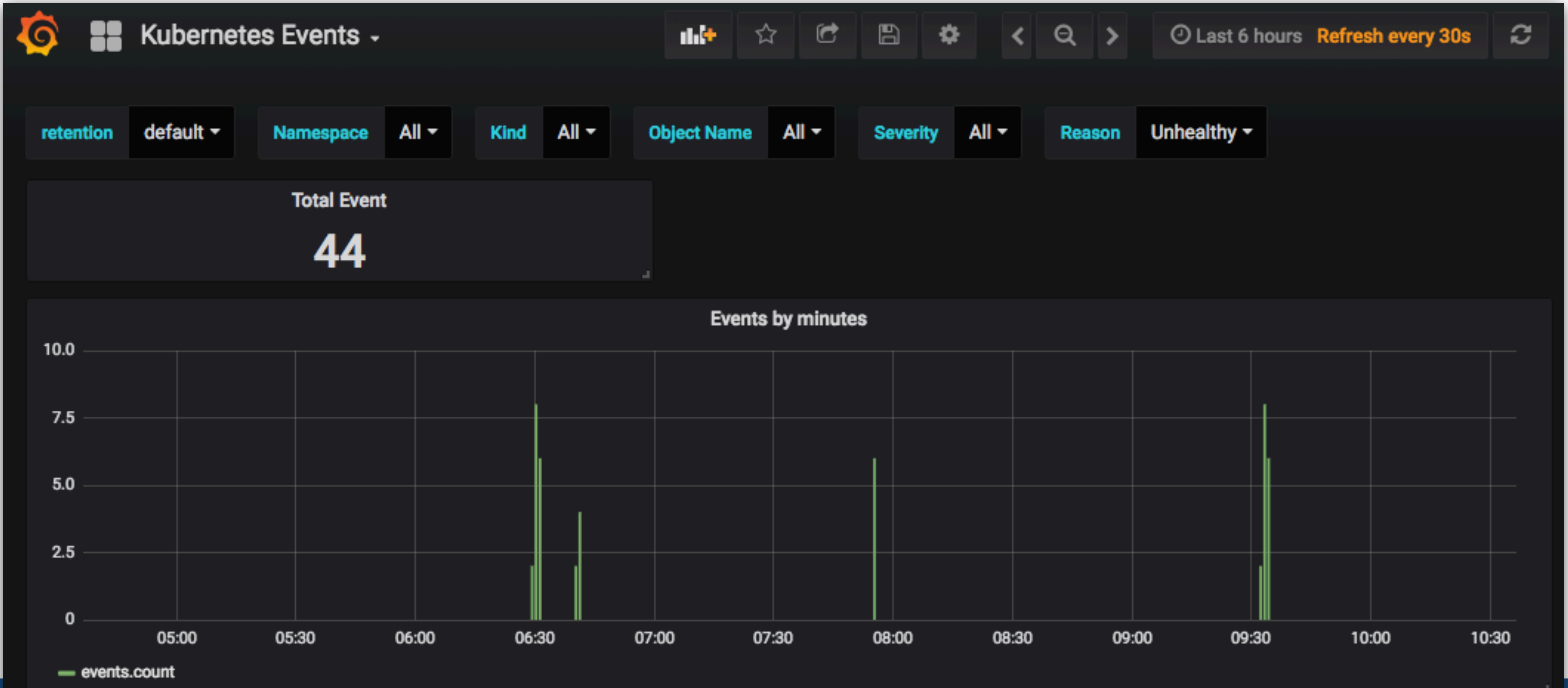
- RHEL 7 beta packages (repo file)
- Ubuntu 16.04 beta packages (repo file)

Monitoring infrastructure & services

All infrastructure nodes (VMs on Cloud@CNAF) monitored via Sensu

K8S monitored via Prometheus

Grafana/Kibana/Uchiwa dashboards



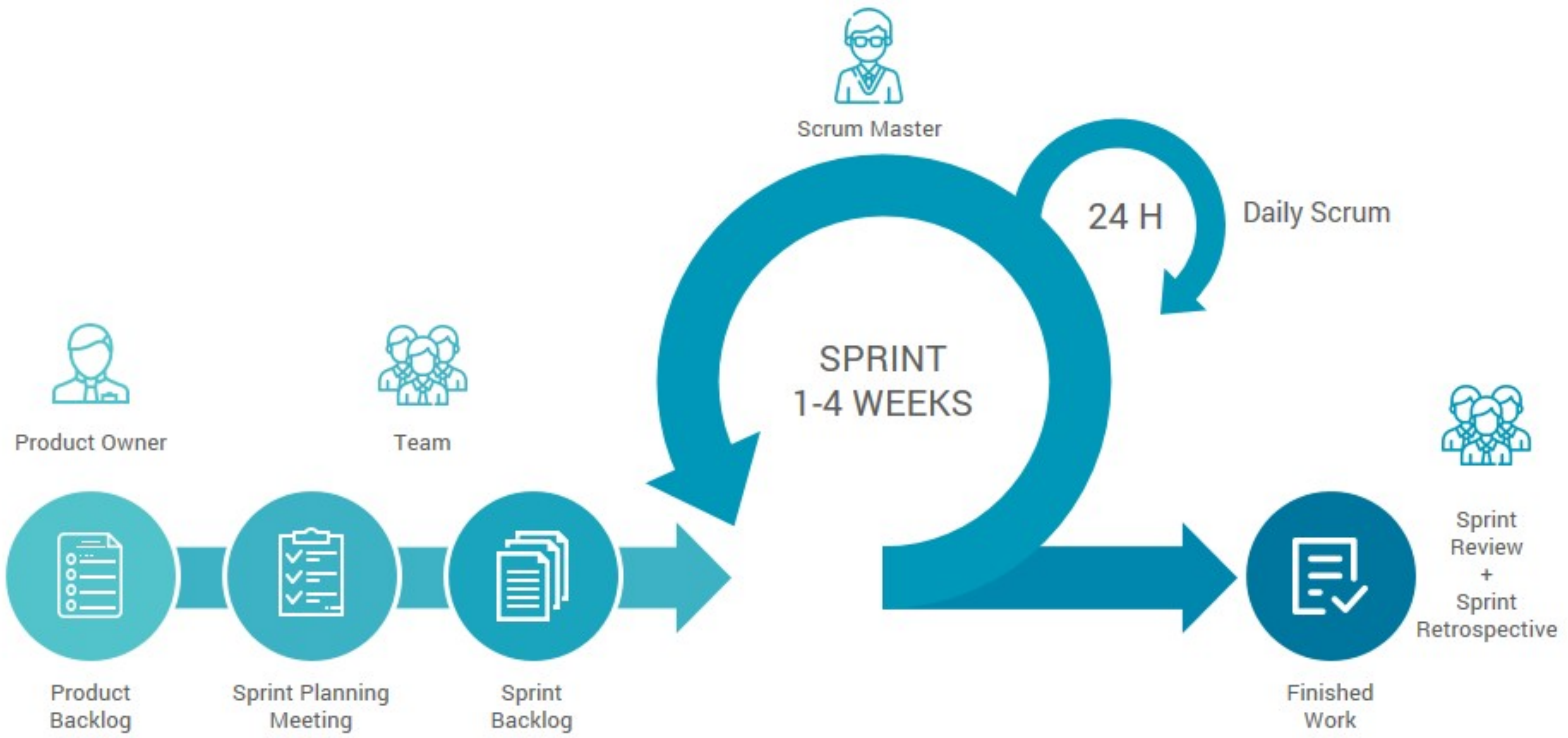
Kubernetes Events

retention: default
Namespace: All
Kind: All
Object Name: All
Severity: All
Reason: Unhealthy

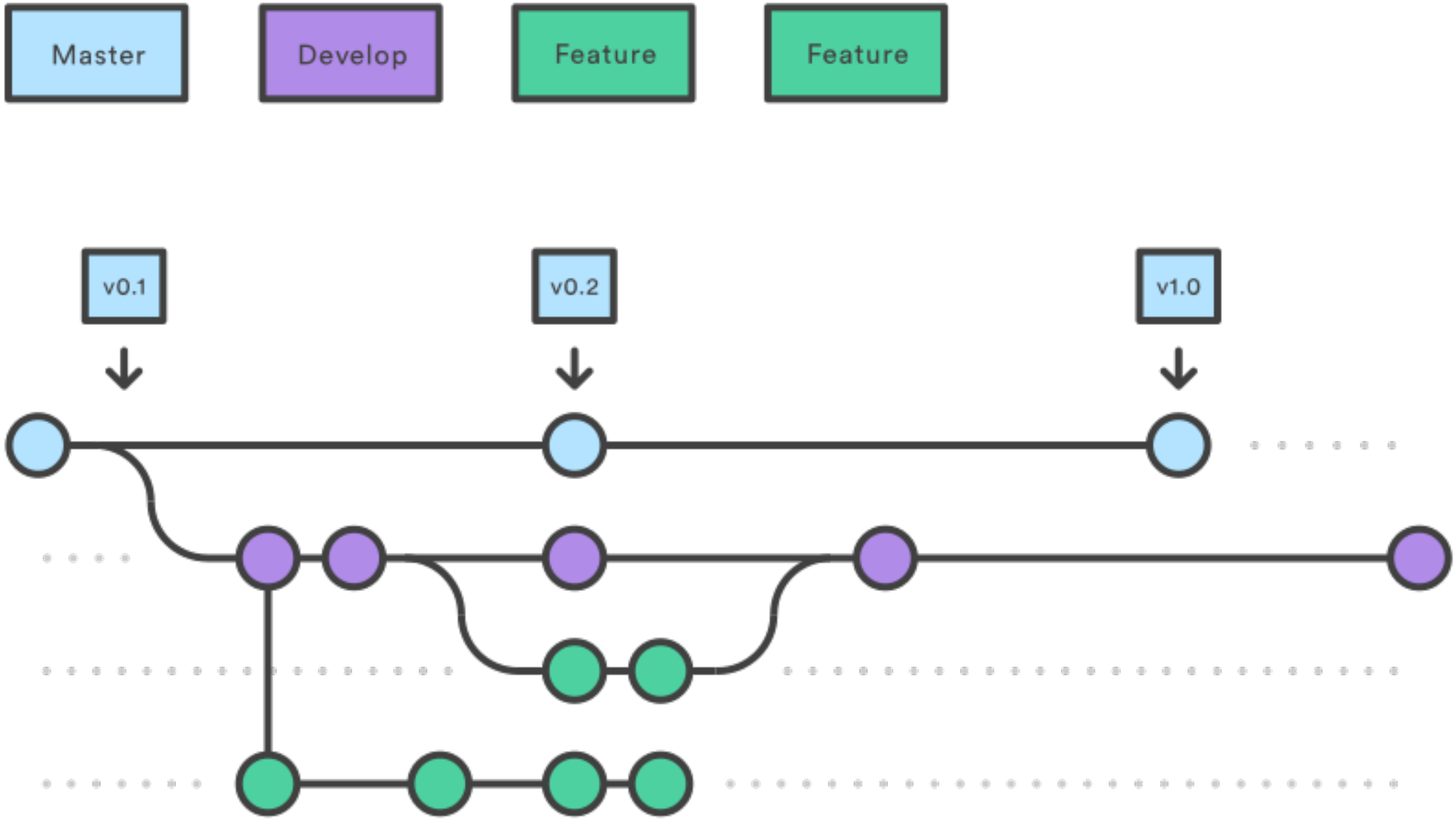
Total Event
44

Process

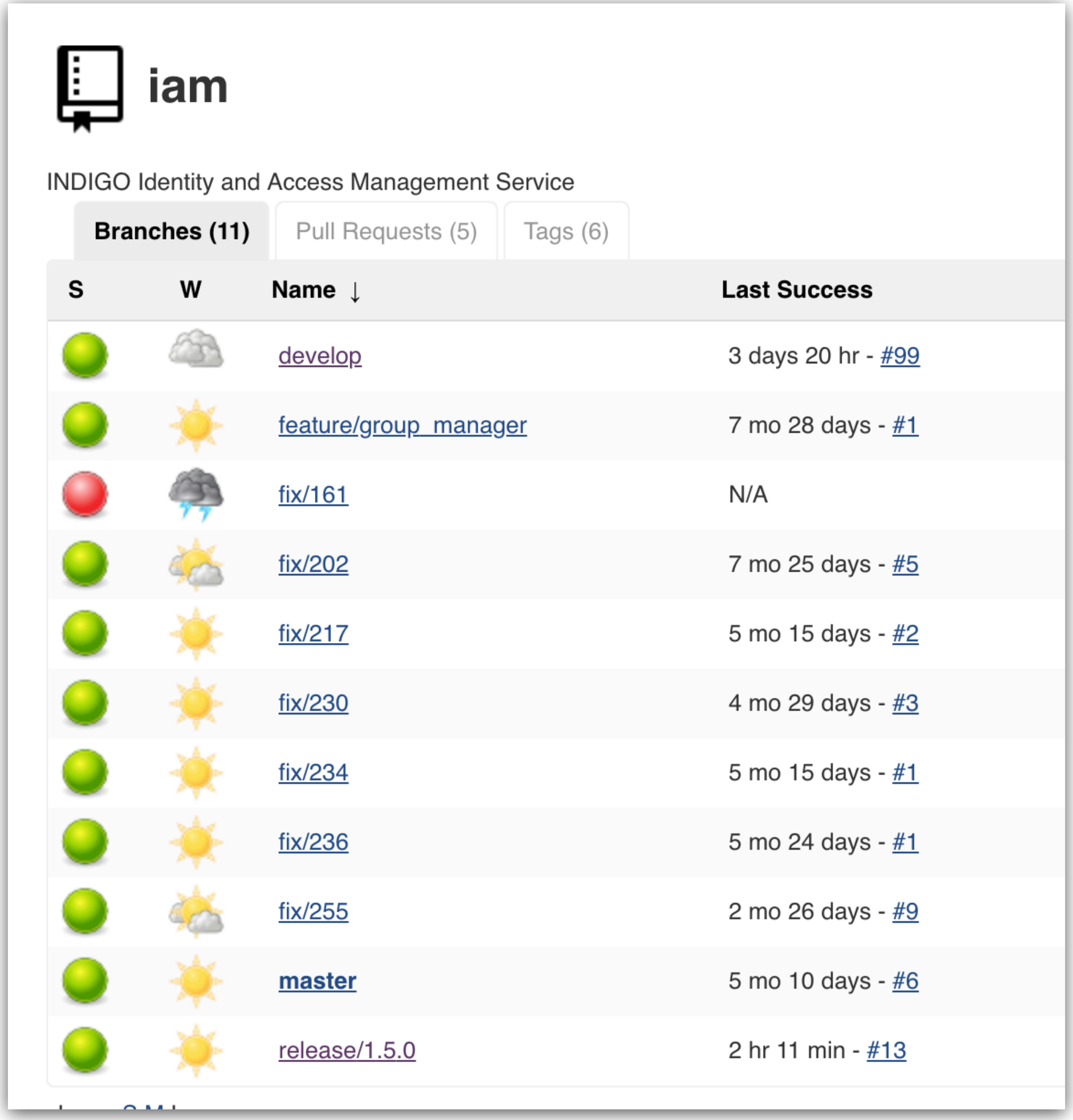
SCRUM-ish development process



Git-flowish branching model



Git-flowish branching model



iam

INDIGO Identity and Access Management Service

S	W	Name ↓	Last Success
🟢	☁	develop	3 days 20 hr - #99
🟢	☀	feature/group_manager	7 mo 28 days - #1
🔴	⛈	fix/161	N/A
🟢	⛅	fix/202	7 mo 25 days - #5
🟢	☀	fix/217	5 mo 15 days - #2
🟢	☀	fix/230	4 mo 29 days - #3
🟢	☀	fix/234	5 mo 15 days - #1
🟢	☀	fix/236	5 mo 24 days - #1
🟢	⛅	fix/255	2 mo 26 days - #9
🟢	☀	**master**	5 mo 10 days - #6
🟢	☀	release/1.5.0	2 hr 11 min - #13

Consistent development environment

For every service, we have a docker-compose to bootstrap a self-contained, embedded development environment

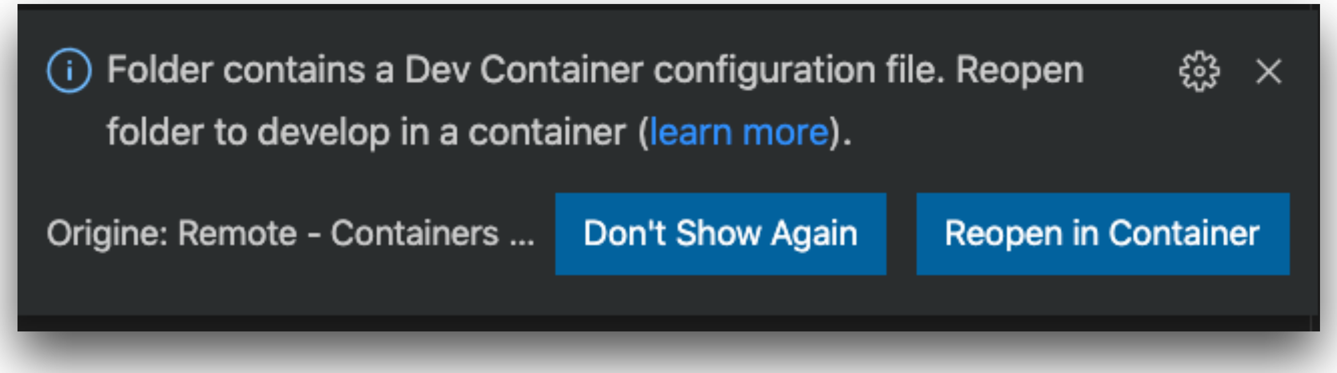
The main objective is avoiding the “builds/works on my machine” mantra

- just to replace it with “builds/works on my docker installation” mantra

VSCode and devcontainers

https://code.visualstudio.com/docs/remote/containers

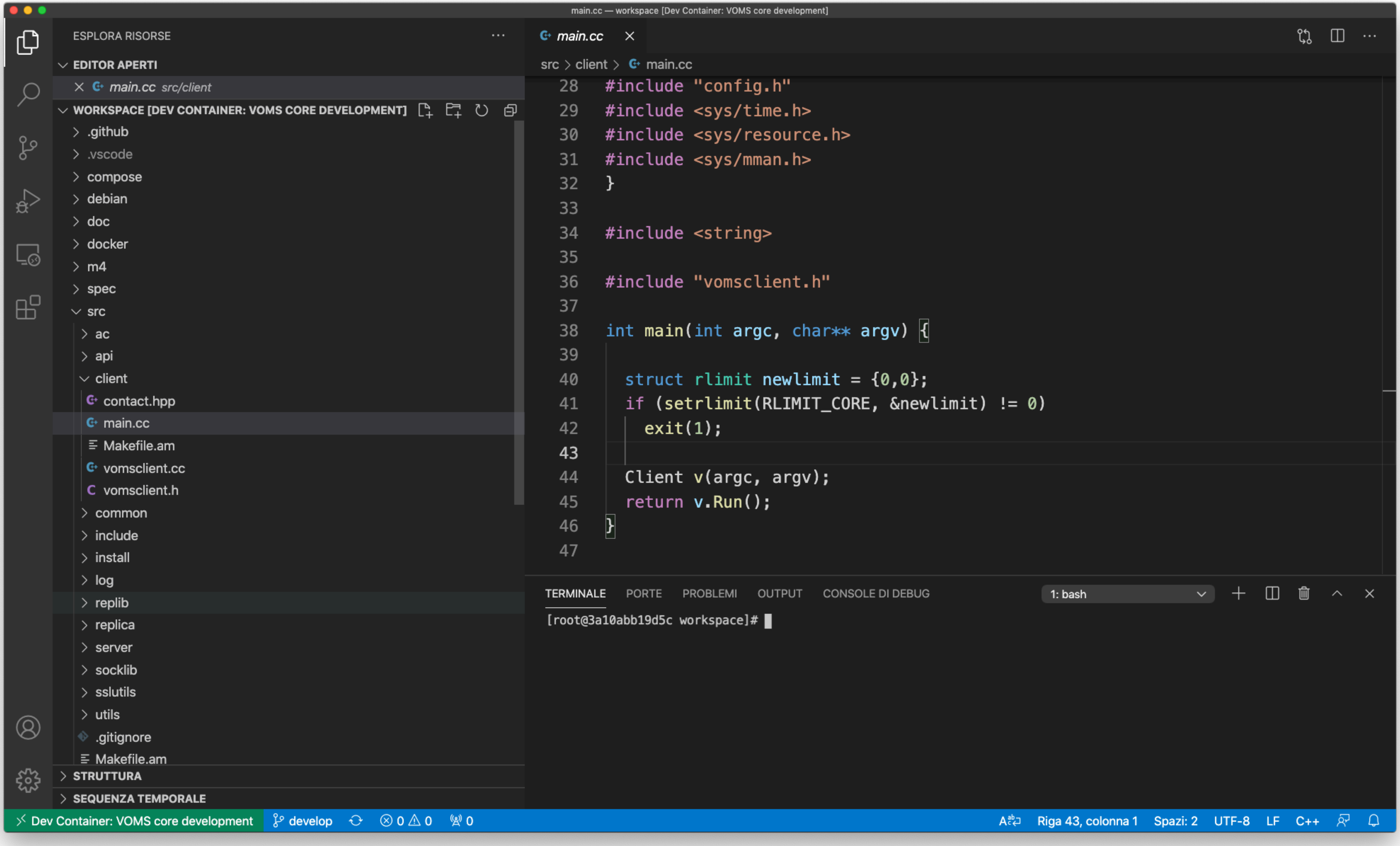
Makes it very easy to develop inside a container



Folder contains a Dev Container configuration file. Reopen folder to develop in a container (learn more).

Origine: Remote - Containers ...

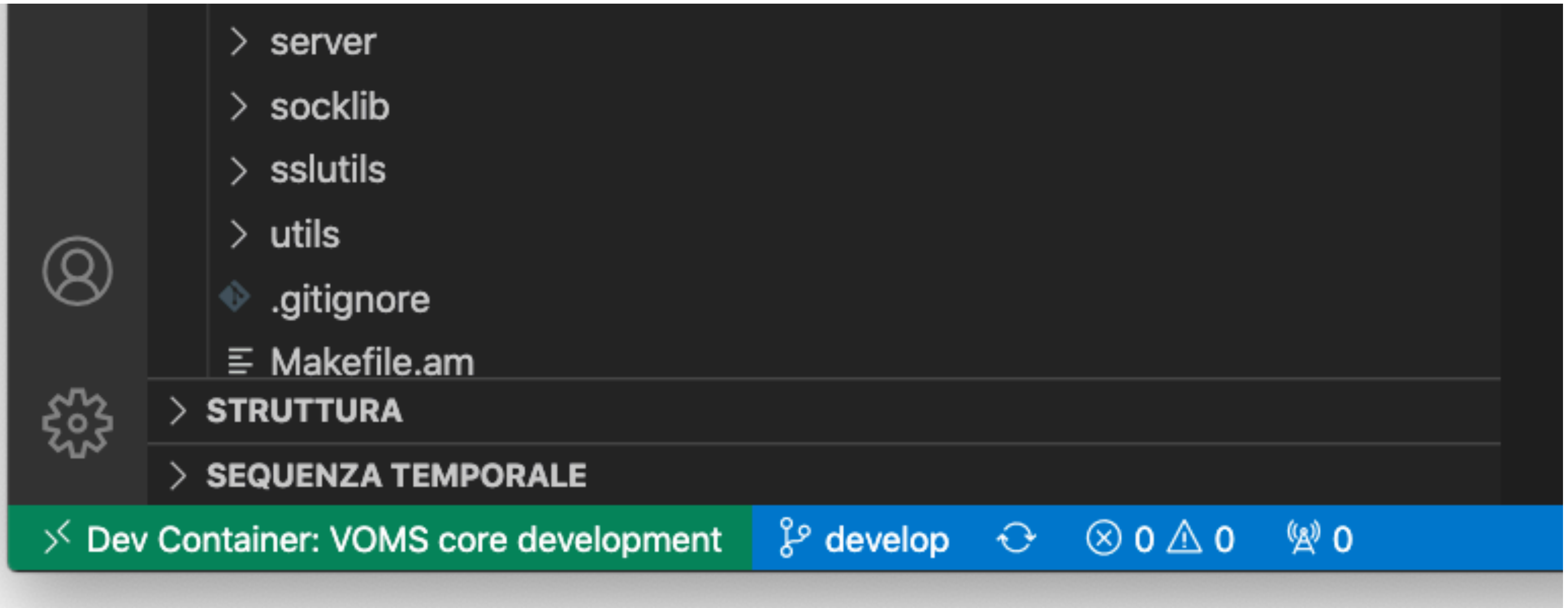
VSCode and devcontainers

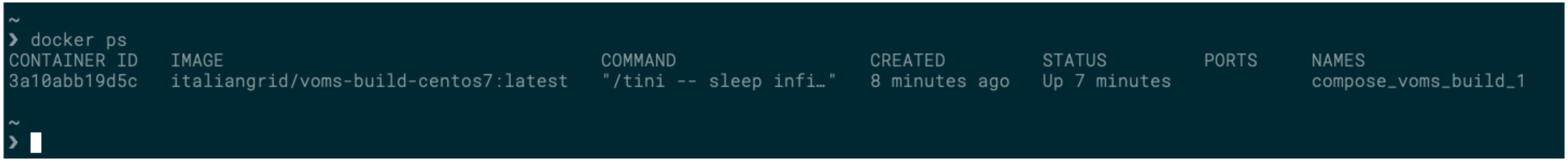


```
#include "config.h"
#include <sys/time.h>
#include <sys/resource.h>
#include <sys/mman.h>
}

#include <string>

#include "vomsclient.h"

int main(int argc, char** argv) {

  struct rlimit newlimit = {0,0};
  if (setrlimit(RLIMIT_CORE, &newlimit) != 0)
    exit(1);

  Client v(argc, argv);
  return v.Run();
}

```

```
[root@3a10abb19d5c workspace]#
```

VSCode and devcontainers

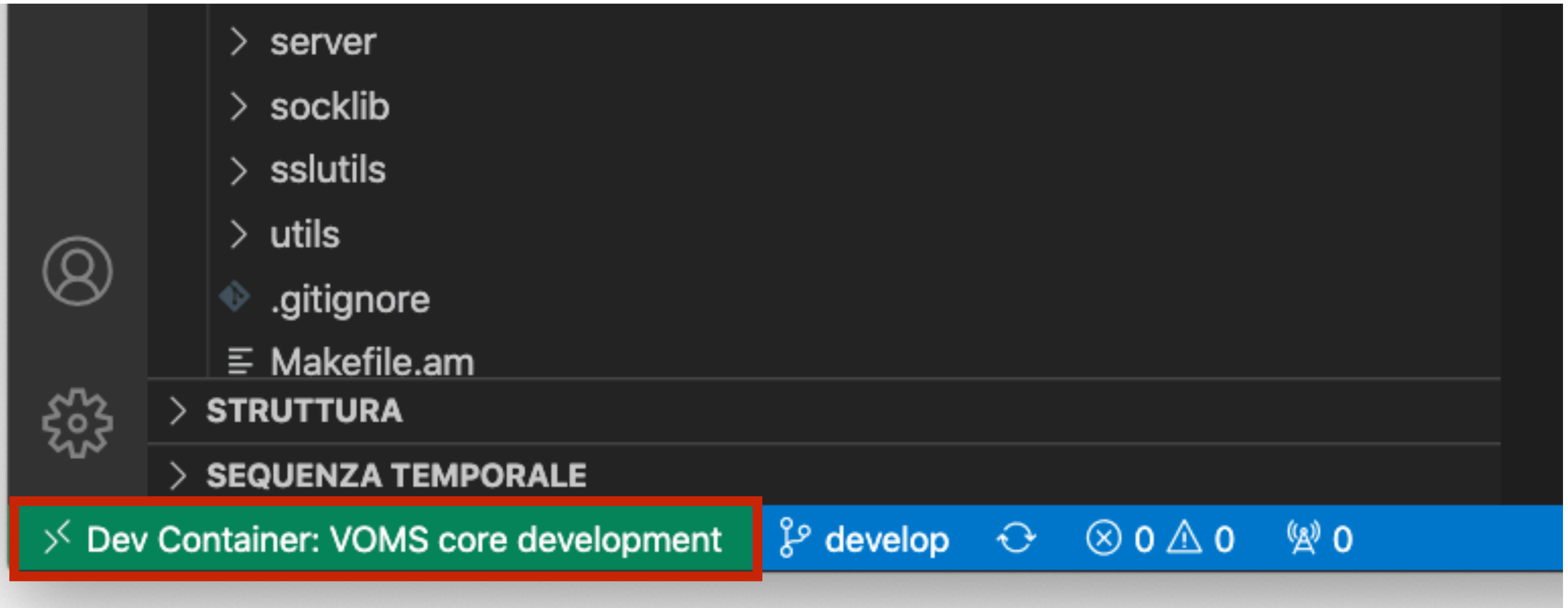


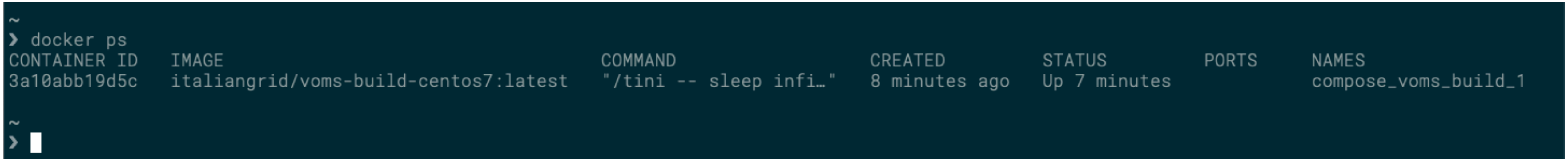


```
~
❯ docker ps
CONTAINER ID   IMAGE                                   COMMAND                  CREATED          STATUS          PORTS      NAMES
3a10abb19d5c   italiangrid/voms-build-centos7:latest   "/tini -- sleep infi…"   8 minutes ago    Up 7 minutes               compose_voms_build_1

~
❯ █
```

VSCode and devcontainers

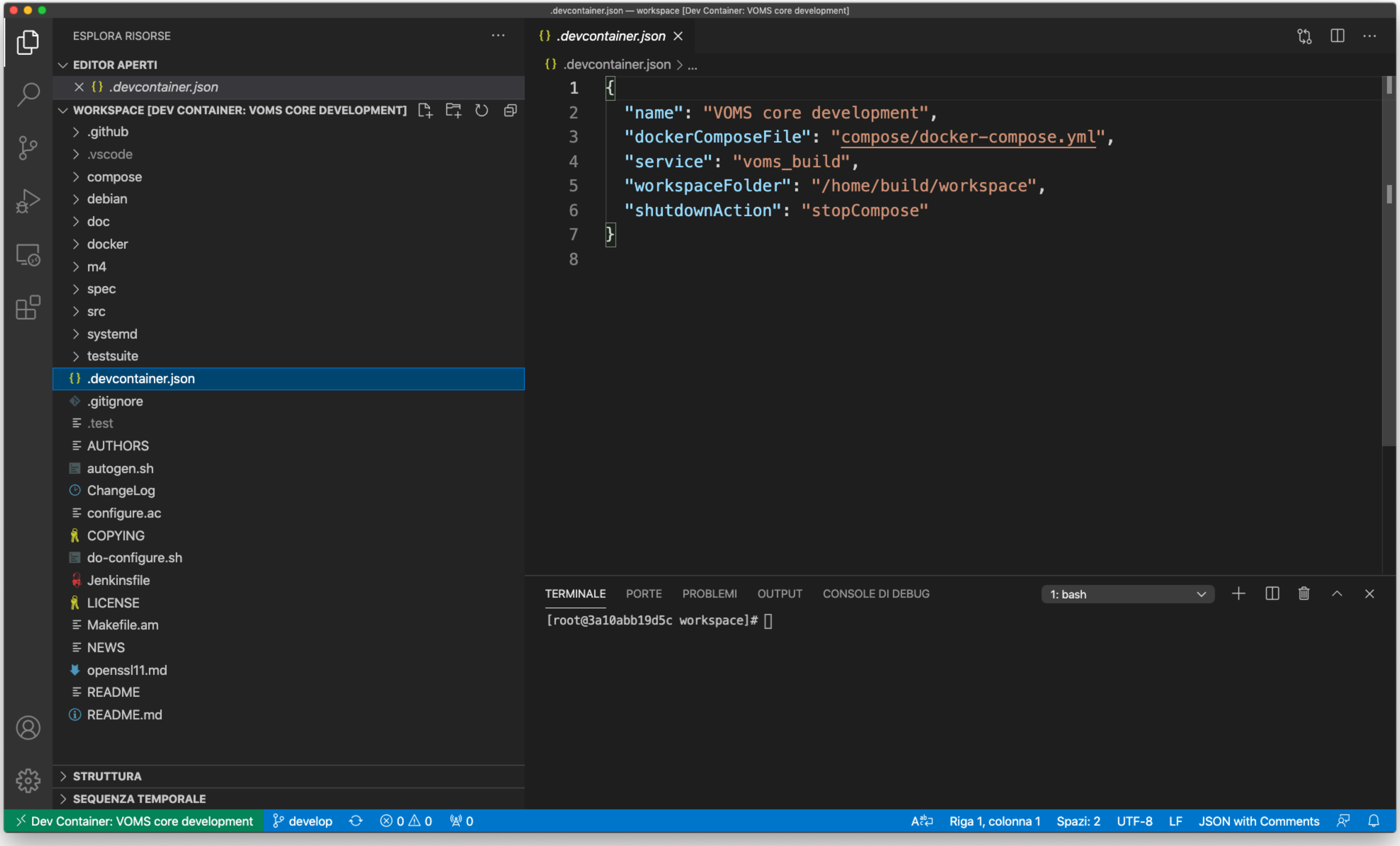
VSCode running in the container





```
~
❯ docker ps
CONTAINER ID   IMAGE                                 COMMAND                  CREATED         STATUS         PORTS      NAMES
3a10abb19d5c   italiangrid/voms-build-centos7:latest "/tini -- sleep infi…"   8 minutes ago   Up 7 minutes              compose_voms_build_1

~
❯ █
```

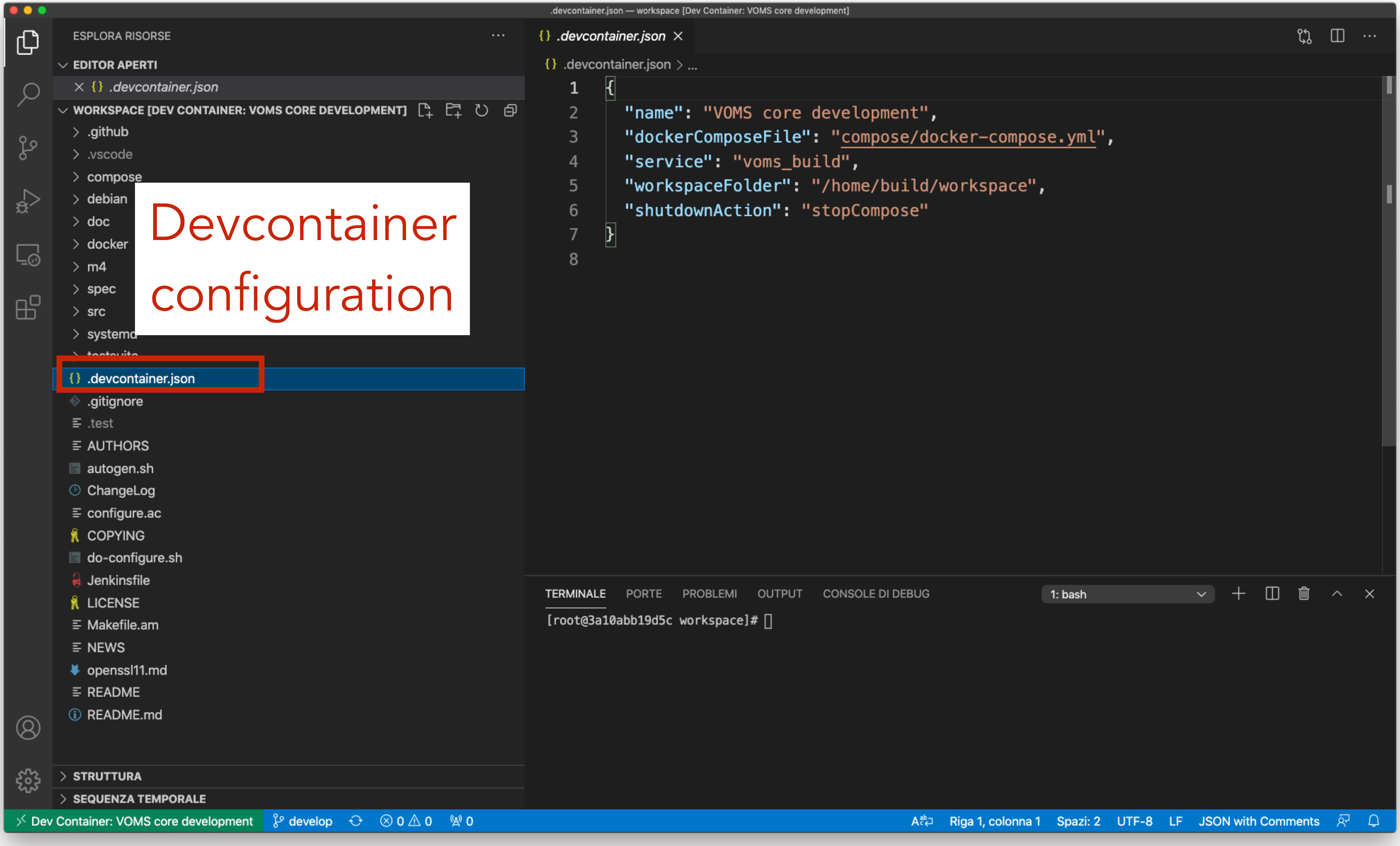
VSCode and devcontainers



```
{
  "name": "VOMS core development",
  "dockerComposeFile": "compose/docker-compose.yml",
  "service": "voms_build",
  "workspaceFolder": "/home/build/workspace",
  "shutdownAction": "stopCompose"
}

```

```
[root@3a10abb19d5c workspace]#
```

VSCode and devcontainers



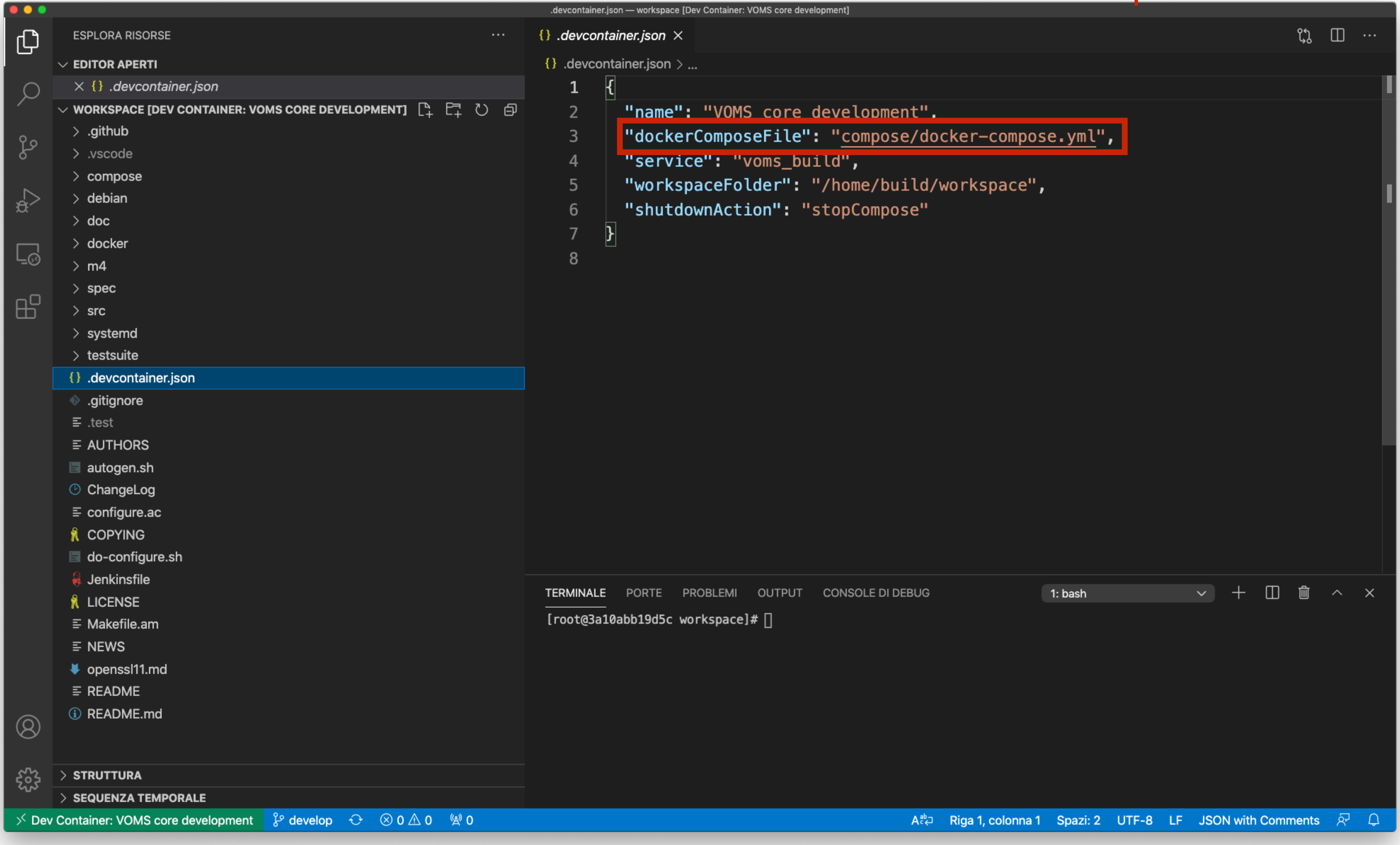
Devcontainer configuration

```
{
  "name": "VOMS core development",
  "dockerComposeFile": "compose/docker-compose.yml",
  "service": "voms_build",
  "workspaceFolder": "/home/build/workspace",
  "shutdownAction": "stopCompose"
}

```

```
[root@3a10abb19d5c workspace]# 
```

VSCode and devcontainers

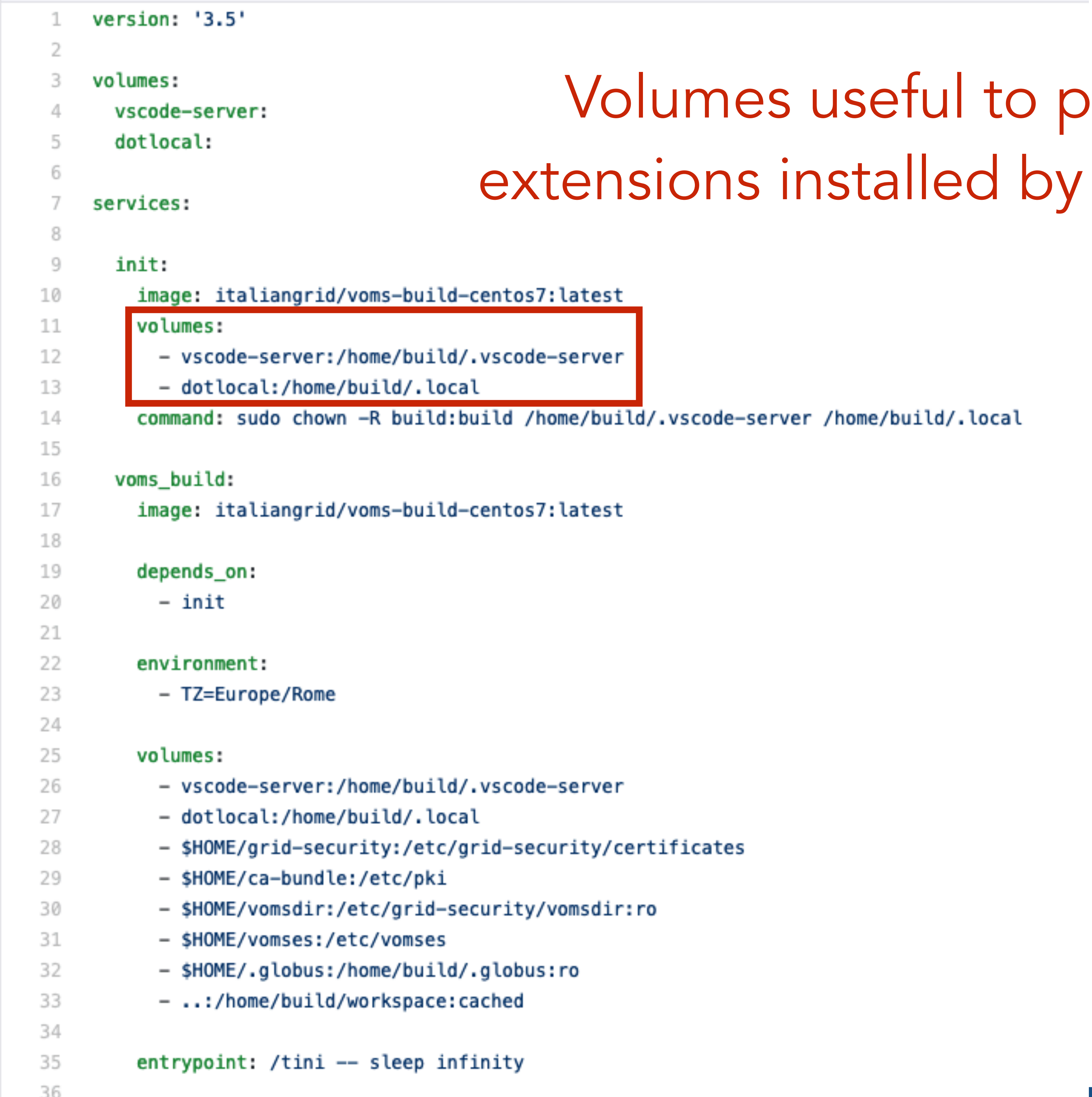
The dev environment is defined with a compose file



```
{
  "name": "VOMS core development",
  "dockerComposeFile": "compose/docker-compose.yml",
  "service": "voms_build",
  "workspaceFolder": "/home/build/workspace",
  "shutdownAction": "stopCompose"
}

```

```
[root@3a10abb19d5c workspace]# 
```

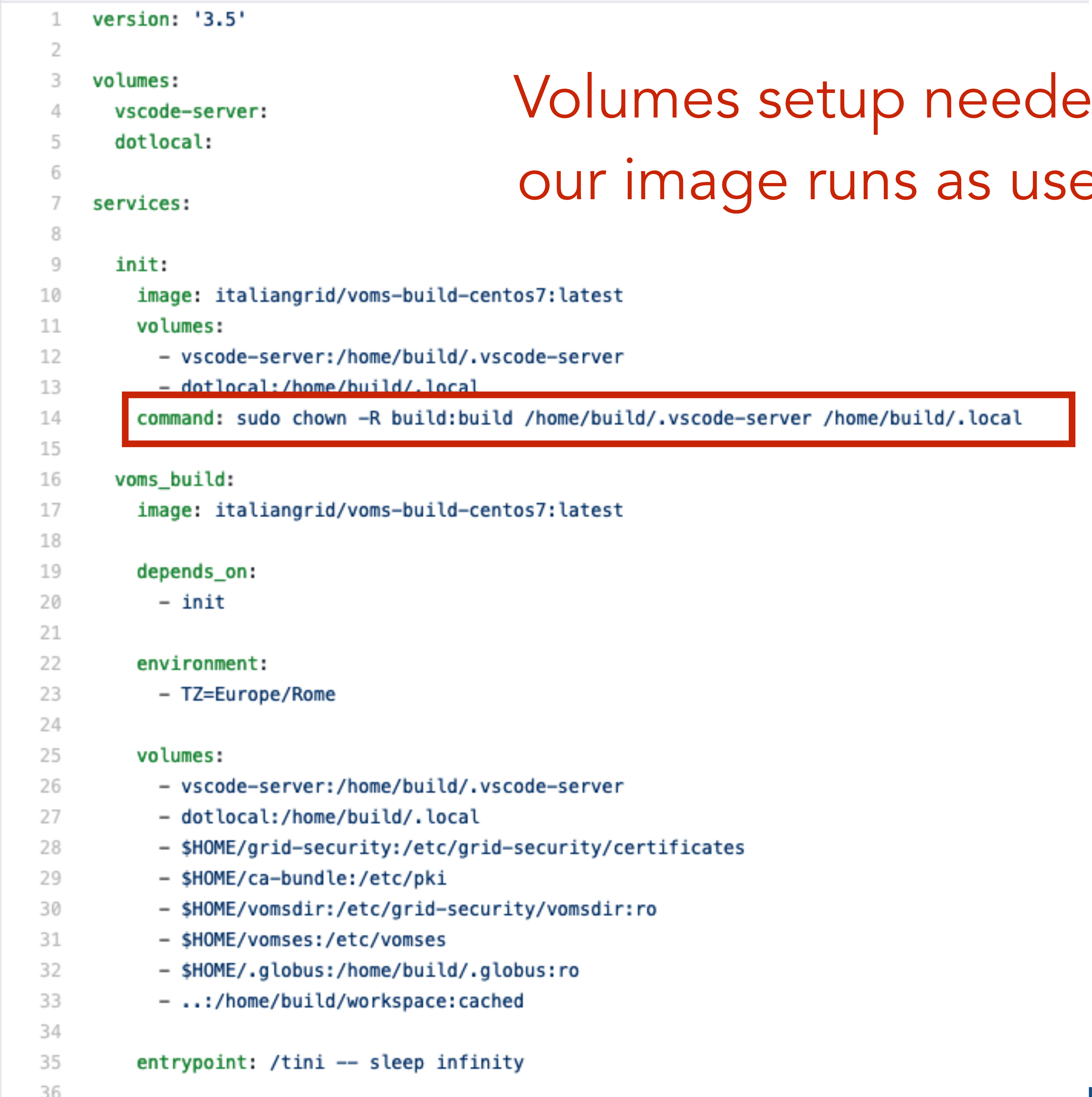
VSCode and devcontainers



```
version: '3.5'

volumes:
  vscode-server:
  dotlocal:

services:

  init:
    image: italiangrid/voms-build-centos7:latest
    volumes:
      - vscode-server:/home/build/.vscode-server
      - dotlocal:/home/build/.local
    command: sudo chown -R build:build /home/build/.vscode-server /home/build/.local

  voms_build:
    image: italiangrid/voms-build-centos7:latest

    depends_on:
      - init

    environment:
      - TZ=Europe/Rome

    volumes:
      - vscode-server:/home/build/.vscode-server
      - dotlocal:/home/build/.local
      - $HOME/grid-security:/etc/grid-security/certificates
      - $HOME/ca-bundle:/etc/pki
      - $HOME/vomsdir:/etc/grid-security/vomsdir:ro
      - $HOME/vomses:/etc/vomses
      - $HOME/.globus:/home/build/.globus:ro
      - ..:/home/build/workspace:cached

    entrypoint: /tini -- sleep infinity
```

Volumes useful to persist extensions installed by VSCode

VSCode and devcontainers



```yaml
version: '3.5'

volumes:
  vscode-server:
  dotlocal:

services:

  init:
    image: italiangrid/voms-build-centos7:latest
    volumes:
      - vscode-server:/home/build/.vscode-server
      - dotlocal:/home/build/.local
    command: sudo chown -R build:build /home/build/.vscode-server /home/build/.local

  voms_build:
    image: italiangrid/voms-build-centos7:latest

    depends_on:
      - init

    environment:
      - TZ=Europe/Rome

    volumes:
      - vscode-server:/home/build/.vscode-server
      - dotlocal:/home/build/.local
      - $HOME/grid-security:/etc/grid-security/certificates
      - $HOME/ca-bundle:/etc/pki
      - $HOME/vomsdir:/etc/grid-security/vomsdir:ro
      - $HOME/vomses:/etc/vomses
      - $HOME/.globus:/home/build/.globus:ro
      - ..:/home/build/workspace:cached

    entrypoint: /tini -- sleep infinity
```

Volumes setup needed since our image runs as user **build**

Testing

Unit tests

- JUnit + Mockito in Java, GTest + GMock in C++, unittest in python

Integration tests

- Spring MockMVC tests

Functionality acceptance tests

- Robot framework-based

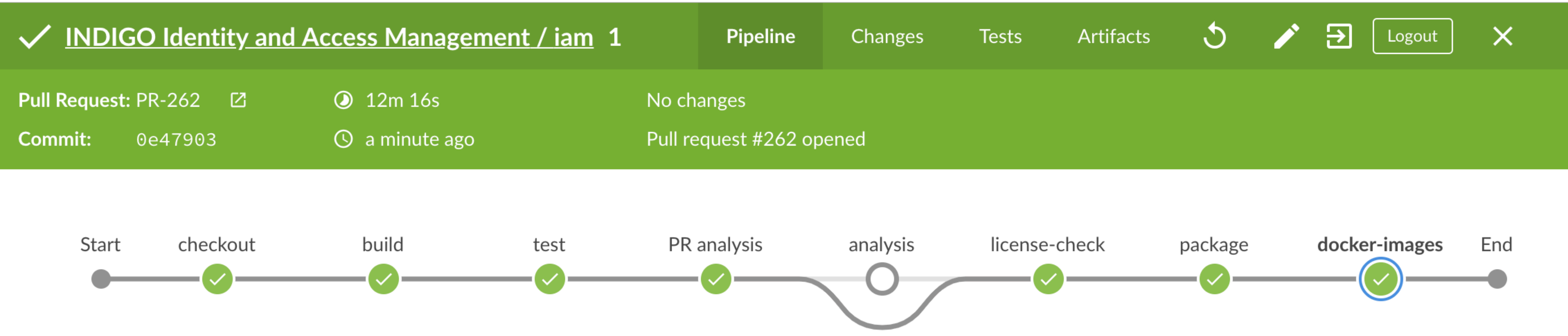
Deployment tests

- Installation from packages/docker image + run functionality/acceptance testsuite

Load tests

- Mainly based on the Grinder framework, to perform stress testing before and across releases

CI pipeline example: IAM



✓ INDIGO Identity and Access Management / iam 1

Pipeline Changes Tests Artifacts Logout ✕

Pull Request: PR-262

Commit: `0e47903`

12m 16s

a minute ago

No changes

Pull request #262 opened

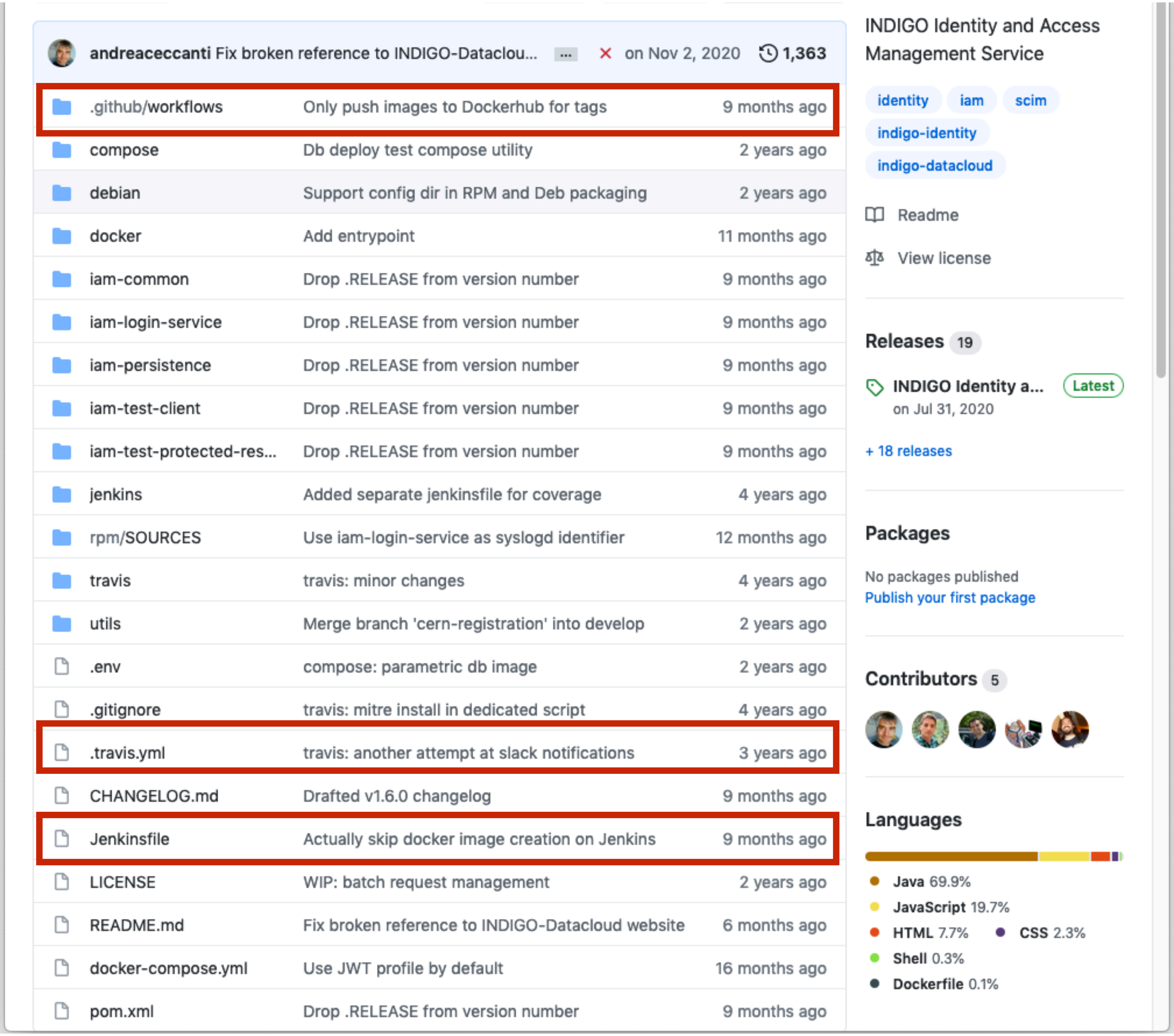
Conventional build & test process for maven-based Spring application

- with additional SonarQube static analysis in the middle

The main artifacts of the build are docker images

- pushed to Dockerhub (for some branches)

CI pipeline definitions live with the code



andreaceccanti Fix broken reference to INDIGO-Dataclou... ··· ✕ on Nov 2, 2020 🕓 1,363

.github/workflows	Only push images to Dockerhub for tags	9 months ago
compose	Db deploy test compose utility	2 years ago
debian	Support config dir in RPM and Deb packaging	2 years ago
docker	Add entrypoint	11 months ago
iam-common	Drop .RELEASE from version number	9 months ago
iam-login-service	Drop .RELEASE from version number	9 months ago
iam-persistence	Drop .RELEASE from version number	9 months ago
iam-test-client	Drop .RELEASE from version number	9 months ago
iam-test-protected-res...	Drop .RELEASE from version number	9 months ago
jenkins	Added separate jenkinsfile for coverage	4 years ago
rpm/SOURCES	Use iam-login-service as syslogd identifier	12 months ago
travis	travis: minor changes	4 years ago
utils	Merge branch 'cern-registration' into develop	2 years ago
.env	compose: parametric db image	2 years ago
.gitignore	travis: mitre install in dedicated script	4 years ago
.travis.yml	travis: another attempt at slack notifications	3 years ago
CHANGELOG.md	Drafted v1.6.0 changelog	9 months ago
Jenkinsfile	Actually skip docker image creation on Jenkins	9 months ago
LICENSE	WIP: batch request management	2 years ago
README.md	Fix broken reference to INDIGO-Datacloud website	6 months ago
docker-compose.yml	Use JWT profile by default	16 months ago
pom.xml	Drop .RELEASE from version number	9 months ago

INDIGO Identity and Access Management Service

identity iam scim indigo-identity indigo-datacloud

Readme

View license

Releases 19

INDIGO Identity a... Latest
on Jul 31, 2020

+ 18 releases

Packages

No packages published
Publish your first package

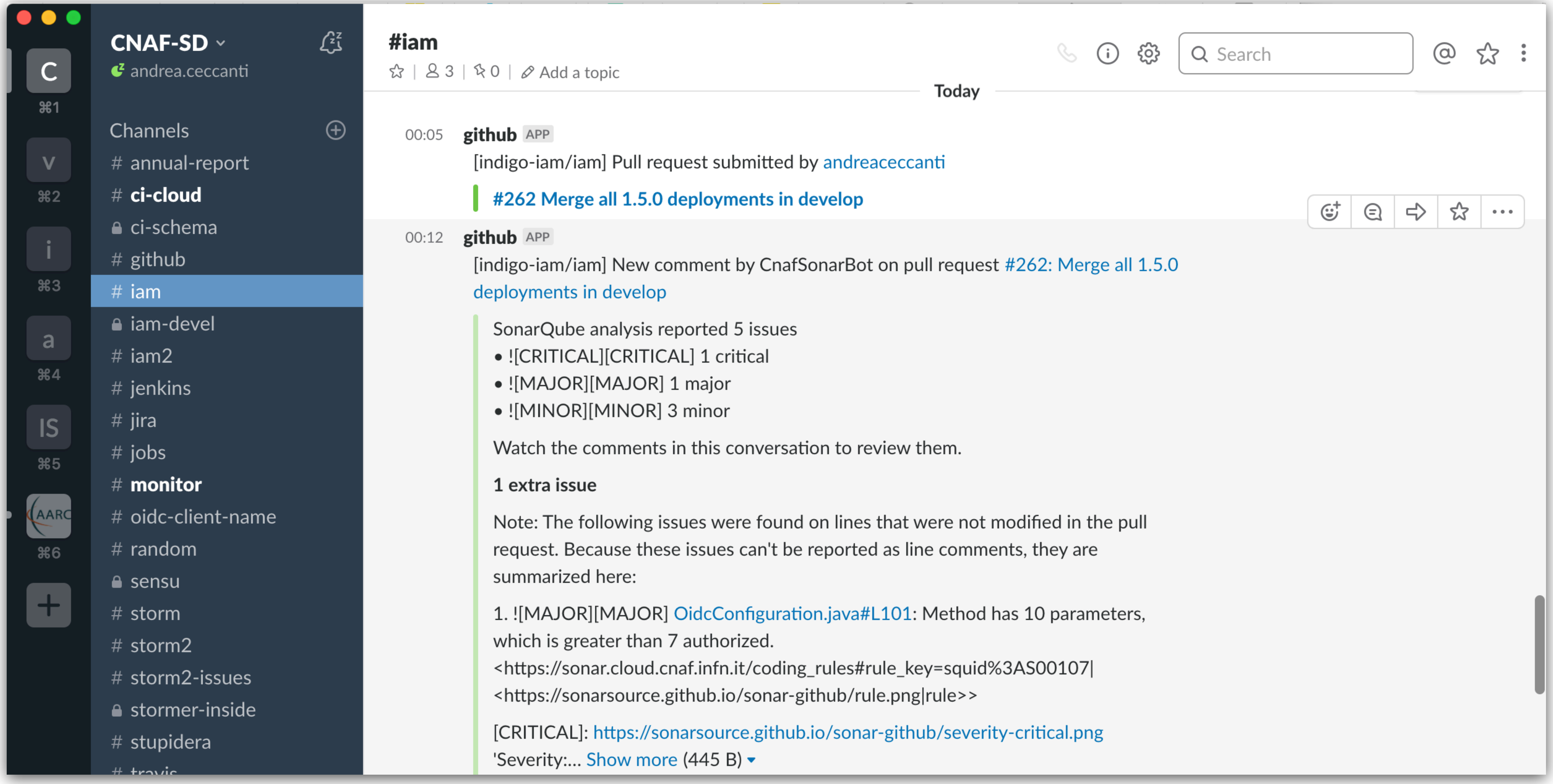
Contributors 5

Languages

- Java 69.9%
- JavaScript 19.7%
- HTML 7.7%
- CSS 2.3%
- Shell 0.3%
- Dockerfile 0.1%

Slack integration

All interesting events trigger a slack notification



00:05 **github** APP

[indigo-iam/iam] Pull request submitted by andreaceccanti

#262 Merge all 1.5.0 deployments in develop

00:12 **github** APP

[indigo-iam/iam] New comment by CnafSonarBot on pull request #262: Merge all 1.5.0 deployments in develop

SonarQube analysis reported 5 issues

- ![CRITICAL][CRITICAL] 1 critical
- ![MAJOR][MAJOR] 1 major
- ![MINOR][MINOR] 3 minor

Watch the comments in this conversation to review them.

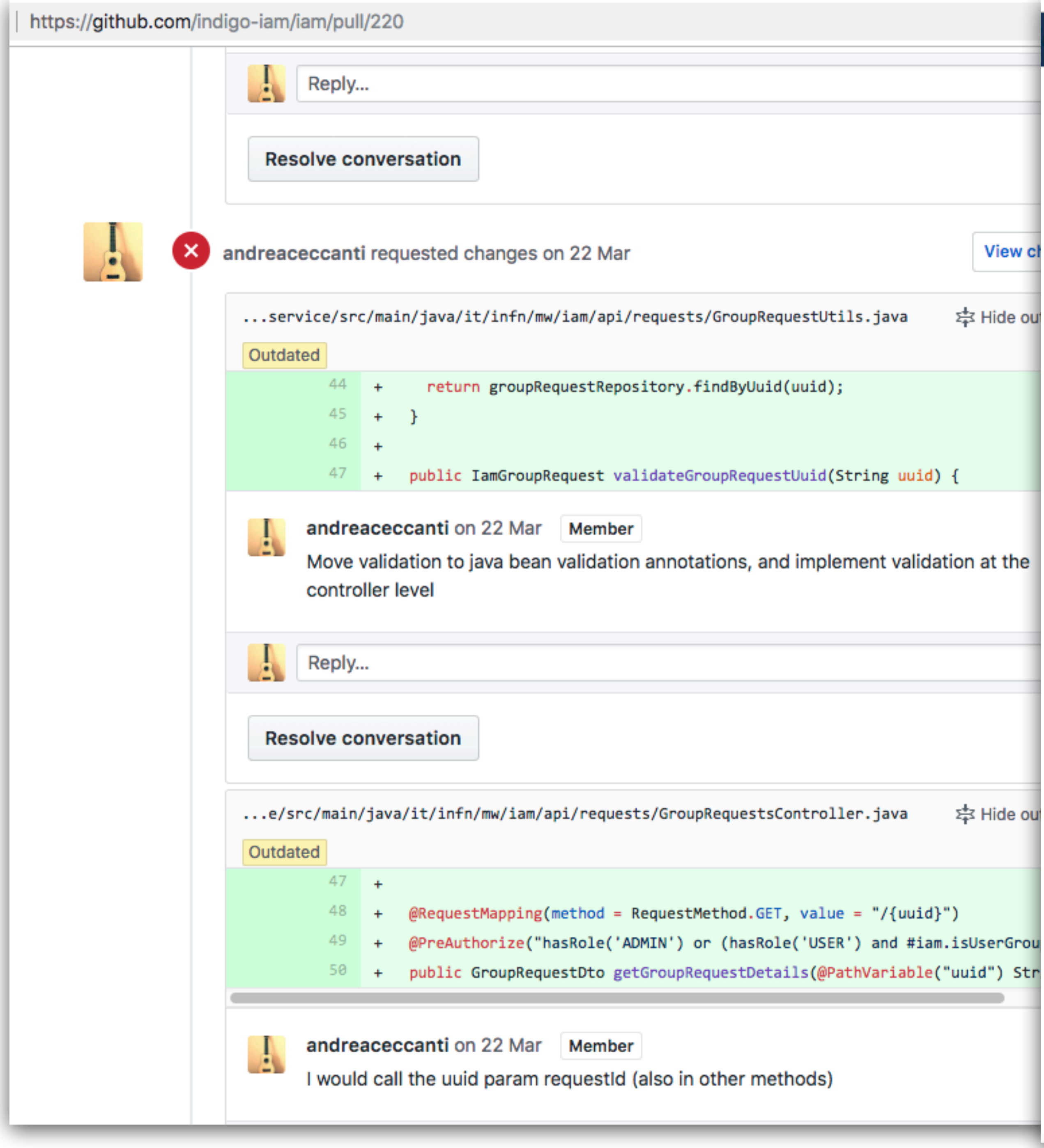
1 extra issue

Note: The following issues were found on lines that were not modified in the pull request. Because these issues can't be reported as line comments, they are summarized here:

1. ![MAJOR][MAJOR] OidcConfiguration.java#L101: Method has 10 parameters, which is greater than 7 authorized.
<https://sonar.cloud.cnaf.infn.it/coding_rules#rule_key=squid%3AS00107|
<https://sonarsource.github.io/sonar-github/rule.png|rule>>

[CRITICAL]: https://sonarsource.github.io/sonar-github/severity-critical.png
'Severity:... Show more (445 B) ▾

Code reviews



https://github.com/indigo-iam/iam/pull/220

andreaceccanti requested changes on 22 Mar

```
...service/src/main/java/it/infn/mw/iam/api/requests/GroupRequestUtils.java
+     return groupRequestRepository.findByUuid(uuid);
+   }
+
+   public IamGroupRequest validateGroupRequestUuid(String uuid) {
```

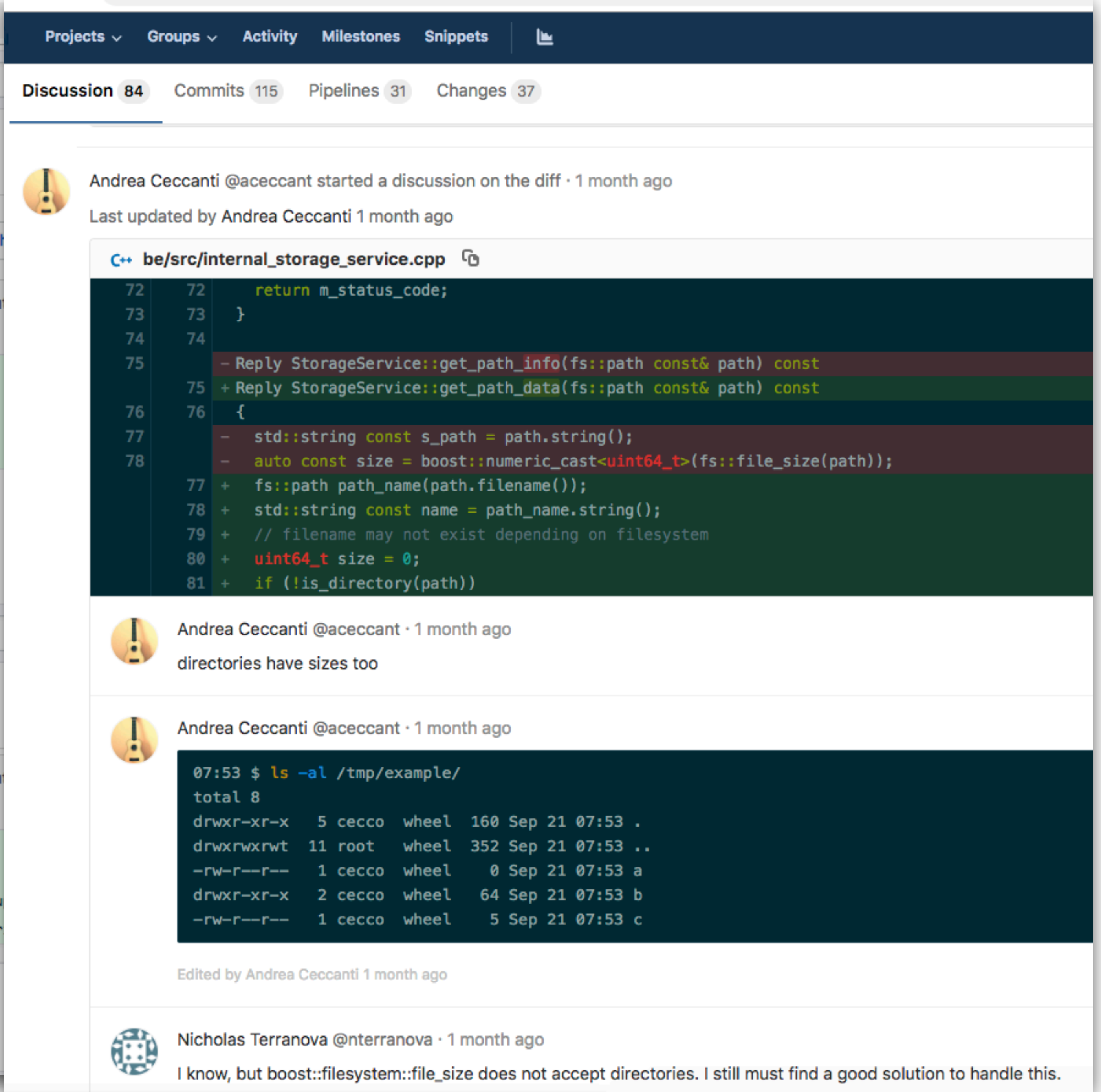
andreaceccanti on 22 Mar

Move validation to java bean validation annotations, and implement validation at the controller level

```
...e/src/main/java/it/infn/mw/iam/api/requests/GroupRequestsController.java
+
+   @RequestMapping(method = RequestMethod.GET, value = "/{uuid}")
+   @PreAuthorize("hasRole('ADMIN') or (hasRole('USER') and #iam.isUserGrou
+   public GroupRequestDto getGroupRequestDetails(@PathVariable("uuid") Str
```

andreaceccanti on 22 Mar

I would call the uuid param requestId (also in other methods)



Andrea Ceccanti @aceccant started a discussion on the diff · 1 month ago

Last updated by Andrea Ceccanti 1 month ago

be/src/internal_storage_service.cpp

```
    return m_status_code;
  }

- Reply StorageService::get_path_info(fs::path const& path) const
+ Reply StorageService::get_path_data(fs::path const& path) const
  {
-   std::string const s_path = path.string();
-   auto const size = boost::numeric_cast<uint64_t>(fs::file_size(path));
+   fs::path path_name(path.filename());
+   std::string const name = path_name.string();
+   // filename may not exist depending on filesystem
+   uint64_t size = 0;
+   if (!is_directory(path))
```

Andrea Ceccanti @aceccant · 1 month ago

directories have sizes too

Andrea Ceccanti @aceccant · 1 month ago

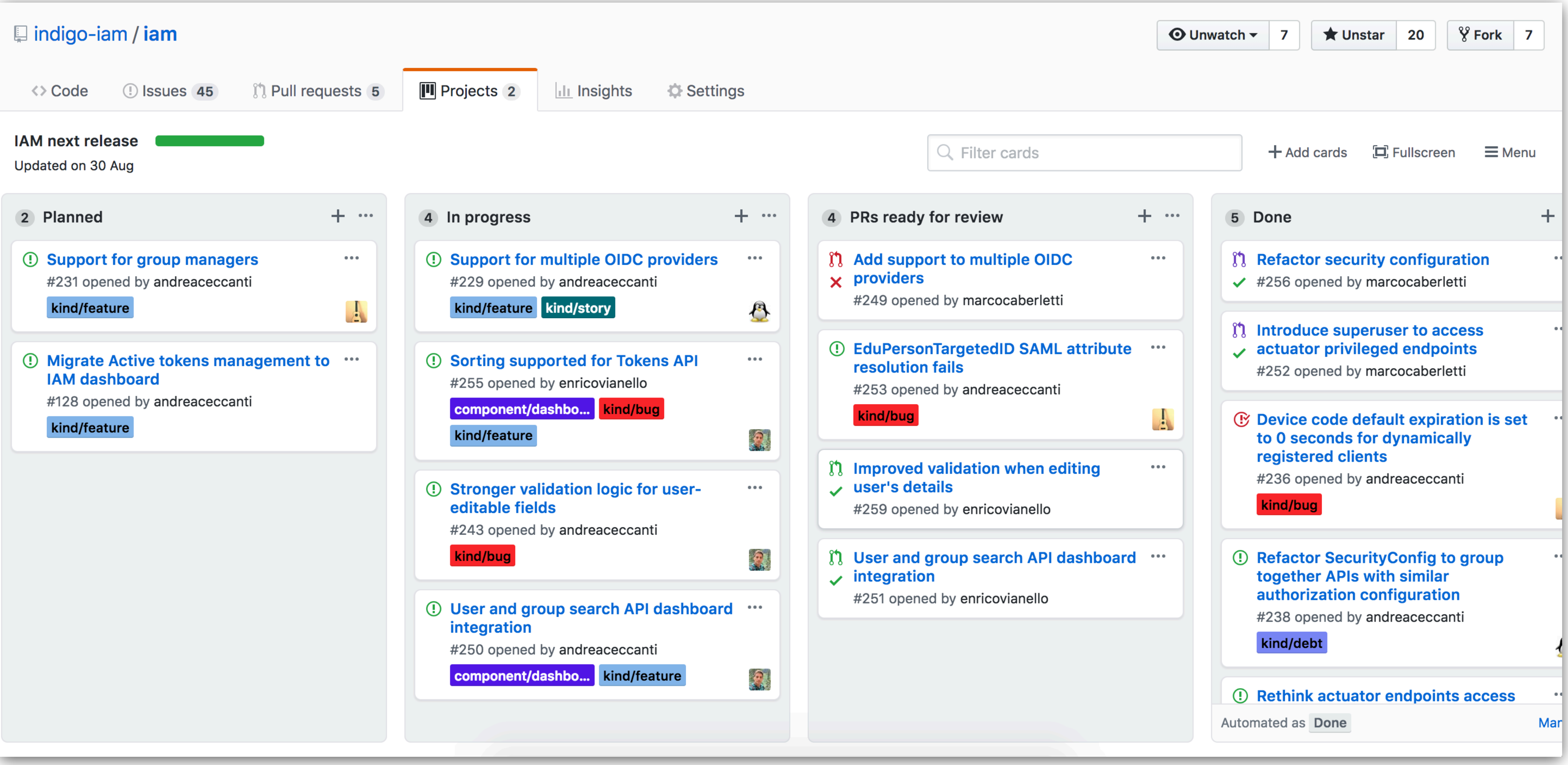
```
07:53 $ ls -al /tmp/example/
total 8
drwxr-xr-x   5 cecco  wheel  160 Sep 21 07:53 .
drwxrwxrwt  11 root   wheel  352 Sep 21 07:53 ..
-rw-r--r--   1 cecco  wheel    0 Sep 21 07:53 a
drwxr-xr-x   2 cecco  wheel   64 Sep 21 07:53 b
-rw-r--r--   1 cecco  wheel    5 Sep 21 07:53 c
```

Edited by Andrea Ceccanti 1 month ago

Nicholas Terranova @nterranova · 1 month ago

I know, but boost::filesystem::file_size does not accept directories. I still must find a good solution to handle this.

Git(hub/lab) projects to track sprint progress



IAM next release

Updated on 30 Aug

2 Planned

- Support for group managers
  #231 opened by andreaceccanti
  kind/feature
- Migrate Active tokens management to IAM dashboard
  #128 opened by andreaceccanti
  kind/feature

4 In progress

- Support for multiple OIDC providers
  #229 opened by andreaceccanti
  kind/feature kind/story
- Sorting supported for Tokens API
  #255 opened by enricovianello
  component/dashbo... kind/bug kind/feature
- Stronger validation logic for user-editable fields
  #243 opened by andreaceccanti
  kind/bug
- User and group search API dashboard integration
  #250 opened by andreaceccanti
  component/dashbo... kind/feature

4 PRs ready for review

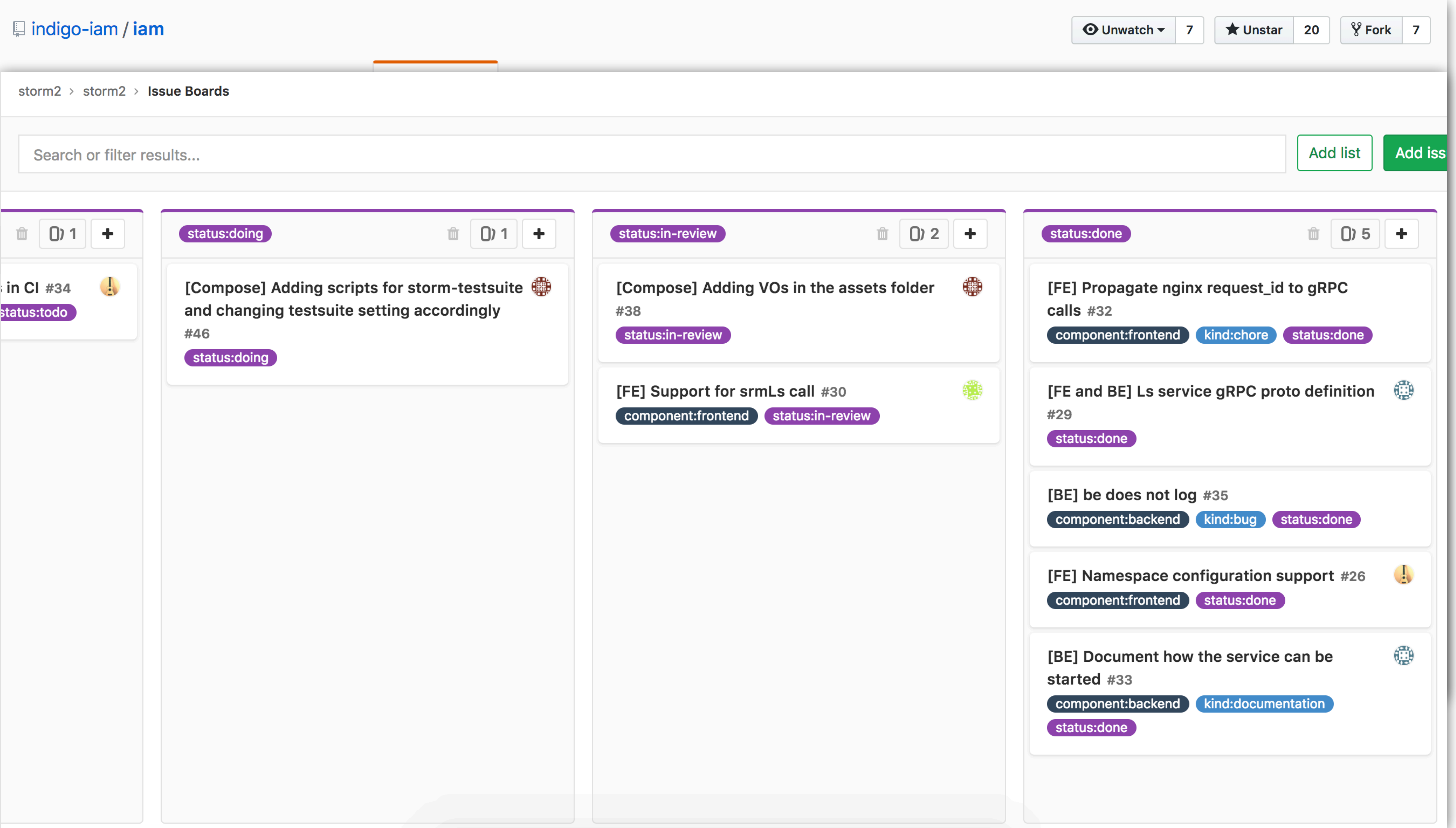
- Add support to multiple OIDC providers
  #249 opened by marcocaberletti
- EduPersonTargetedID SAML attribute resolution fails
  #253 opened by andreaceccanti
  kind/bug
- Improved validation when editing user's details
  #259 opened by enricovianello
- User and group search API dashboard integration
  #251 opened by enricovianello

5 Done

- Refactor security configuration
  #256 opened by marcocaberletti
- Introduce superuser to access actuator privileged endpoints
  #252 opened by marcocaberletti
- Device code default expiration is set to 0 seconds for dynamically registered clients
  #236 opened by andreaceccanti
  kind/bug
- Refactor SecurityConfig to group together APIs with similar authorization configuration
  #238 opened by andreaceccanti
  kind/debt
- Rethink actuator endpoints access

Automated as Done

Git(hub/lab) projects to track sprint progress



indigo-iam / iam

storm2 › storm2 › Issue Boards

in CI #34
status:todo

status:doing

[Compose] Adding scripts for storm-testsuite and changing testsuite setting accordingly #46
status:doing

status:in-review

[Compose] Adding VOs in the assets folder #38
status:in-review

[FE] Support for srmLs call #30
component:frontend status:in-review

status:done

[FE] Propagate nginx request_id to gRPC calls #32
component:frontend kind:chore status:done

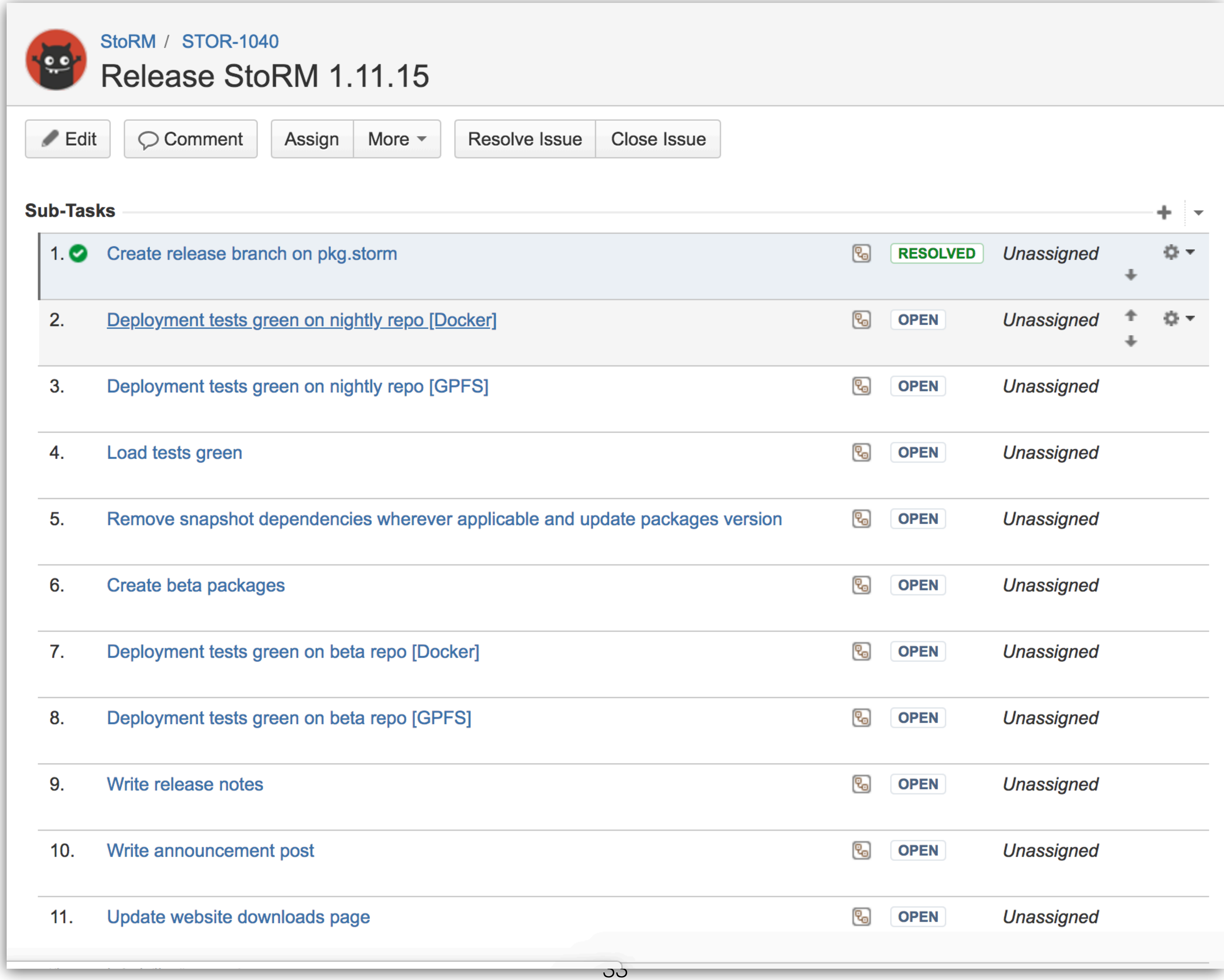
[FE and BE] Ls service gRPC proto definition #29
status:done

[BE] be does not log #35
component:backend kind:bug status:done

[FE] Namespace configuration support #26
component:frontend status:done

[BE] Document how the service can be started #33
component:backend kind:documentation status:done

Release preparation



StoRM / STOR-1040

Release StoRM 1.11.15

Sub-Tasks

1. ✓	Create release branch on pkg.storm	RESOLVED	*Unassigned*
2.	Deployment tests green on nightly repo [Docker]	OPEN	*Unassigned*
3.	Deployment tests green on nightly repo [GPFS]	OPEN	*Unassigned*
4.	Load tests green	OPEN	*Unassigned*
5.	Remove snapshot dependencies wherever applicable and update packages version	OPEN	*Unassigned*
6.	Create beta packages	OPEN	*Unassigned*
7.	Deployment tests green on beta repo [Docker]	OPEN	*Unassigned*
8.	Deployment tests green on beta repo [GPFS]	OPEN	*Unassigned*
9.	Write release notes	OPEN	*Unassigned*
10.	Write announcement post	OPEN	*Unassigned*
11.	Update website downloads page	OPEN	*Unassigned*