POC infra results

Inputs from

- Christophe Closset
- Morgan Richomme
- sylvain.desbureaux
- david.blaisonneau
- Cedric Ollivier

Following up on testing various SCM and CICD infra :

Testing **Bitbucket, GitHub**, **CircleCI** and **TravisCI :**

contact: Christophe Closset

Following up on our call last week with the LFN infra workgroup and our action item :

https://wiki.lfnetworking.org/display/LN/LFN+Infra+Work+Group+1+Feb+19

I went ahead trying the SCM features and CI of github, my goal was to reach a point where I could replicate the verify job and see the hurdles I would face.

I did the following :

- Setup a new github account, clone an existing repo from ONAP (clamp in this case)
- Pull the code locally and setup a circleci account;
- read the doc from circleci
- CLAMP build is java (maven based) + docker, with some special features like running an integration test suite with containers
- Played around with circle CI options to reach a point where the build is successful
- Create a pull request to see the CI interactions and how smooth the integration is.

My feeling after this short POC

All in all, it went well and I think that technically, this option sounds a good one.

The +:

- Obviously github is very good, I feel bitbucket is a bit better in visibility. CicleCI is also very nice and clear.
- Documentation is good, but I've faced some problems requiring me to dig into forums and other sites to find the answers
- Integration is smooth with github; pull requests get the status of builds, I can also use the workflow ability to decide what is done when and from where.
- The CI allows for many cool features (you can log into the containers, vms running the builds, they stay available for 10 mins this is great for debugging)
- Builds are docker based, all is setup through yml files in the repo.
- You can provide your own custom images to run the builds on, but they already have a good set.

The –:

- It's unclear how expensive this will be for the whole ONAP, I mean hosting code on github will probably be free but the CI might be expensive on the long term :
    - Their pricing is 'minutes of build' based and depends on the type and number of containers you subscribe to.
    - Some features may imply additional fees : 'Docker layer caching' is well documented but when trying it, the ci tool said I must be 'whitelisted first'…
- There are some restrictions linked to the philosophy of the tool, for example, I couldn't mount a volume in a container in my build easily, so I've had to switch to a VM type of executor, which cost 'more minutes' to run…
- Next I'll try travisci if I get some cycle

Bitbucket and its pipeline feature

contact: Christophe Closset

I've also started doing the same thing with Bitbucket and its pipeline feature, but I fear that I'll be limited quickly since I get only 50 build minutes for free

Links :

- SCM with pull request open : https://github.com/ChrisC-att/clamp/pull/1

- CircleCI : https://circleci.com/gh/ChrisC-att/workflows/clamp/tree/circleci_poc
- Travis-CI : https://travis-ci.org/ChrisC-att/clamp

The + :

- Sounds like it is free for Open Source
- Very easy to setup, even easier than Circle-CI, I was able to even run sonarcloud on pull request in a breeze.

The - :

- Sounds limited to a pre-defined subset of actions (verify PR and build branches, no custom actions)
- The VM image is fixed, although you can get sudo access and install what you want

All in all, I don't see much limitations technically to go to one or another, it sounds rather a limitation on price and philosophy than real technical issues

Gitlab + gitlab-ci

contact: Sylvain Desbureaux, Dabid Blaisonneau, Morgan Richomme

Gitlab sounds also a very good technical option, and it is open source

gitlab provides a complex CI system that can be customized as well

the +

- All in one
- CI/CD
- artifact management
- documentation
- built-in web site
- open source solution
- it is free
- native integration with kubernetes /prometheus (even if we did not really used it so far)
- All of the features available for free for education & open source projects hosted on gitlab.com (https://about.gitlab.com/2018/06/05/gitlab-ultimate-and-gold-free-for-education-and-open-source/)

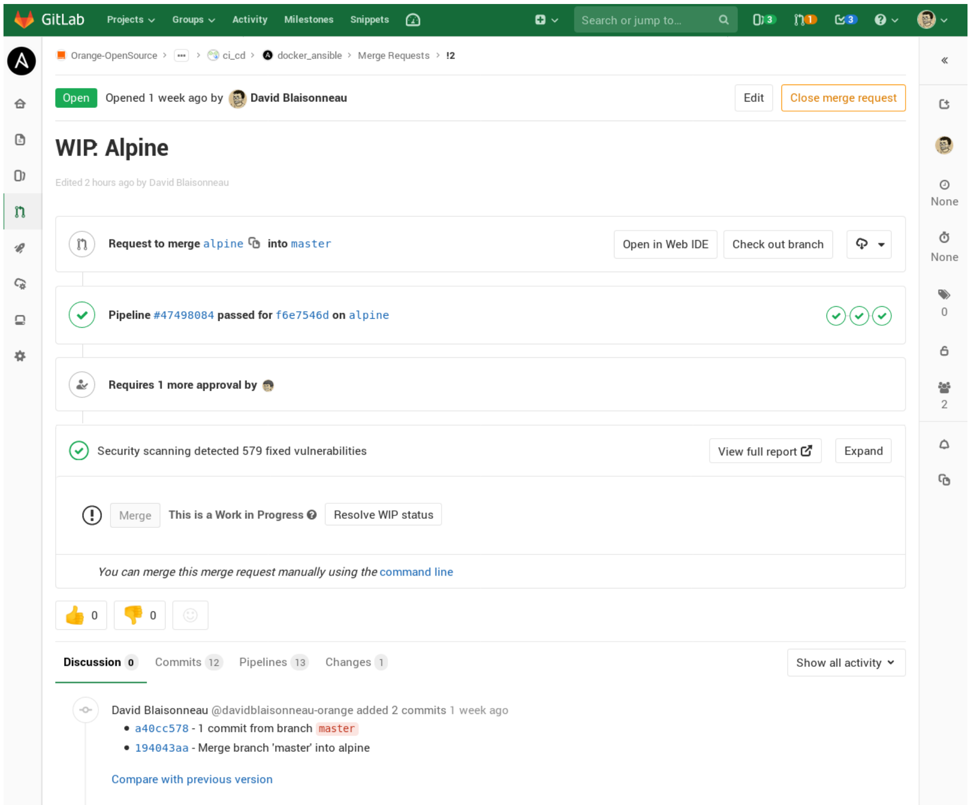
the -

- All in one
- no SLA on performance/availability (but we did not pay for an Ultimate or Gold version and on gitlab.com, the aaS is very good - we experienced rarely problem (e.g. after Microsoft announced they bought github, it was very slow, as lots of communities were moving to gitlab..))
- CI runners are available to launch CI jobs but you still need cloud ressources to do the job (we are using our own server), no idea how much it woudl cost if it was fully externalized
- no native integration so far with docker hub found (as github) BUT built-in docker registry

Focus on security aspects:

gitlab includes a docker registry and native integration with lots of open source tools
https://docs.gitlab.com/ee/user/project/merge_requests/

- Analyze the impact of your changes with **Code Quality reports**
- Manage the licenses of your dependencies with **License Management**
- Analyze your source code for vulnerabilities with **Static Application Security Testing**
- Analyze your running web applications for vulnerabilities with **Dynamic Application Security Testing**
- Analyze your dependencies for vulnerabilities with **Dependency Scanning**
- Analyze your Docker images for vulnerabilities with **Container Scanning**
- Determine the performance impact of changes with **Browser Performance Testing**



Opened 1 week ago by David Blaisonneau

WIP: Alpine

Edited 2 hours ago by David Blaisonneau

Request to merge alpine into master

Pipeline #47498084 passed for f6e7546d on alpine

Requires 1 more approval by

Security scanning detected 579 fixed vulnerabilities

This is a Work in Progress

You can merge this merge request manually using the command line

David Blaisonneau @davidblaisonneau-orange added 2 commits 1 week ago

- a40cc578 - 1 commit from branch master
- 194043aa - Merge branch 'master' into alpine

Compare with previous version

Static Application Security Testing

this testing focuses on code vulnerability

- java / Maven => find-sec-bugs https://find-sec-bugs.github.io/
- Python => bandit
- JavaScript => ESLint security plugin
- NodeJs => NodeJsScan

it also evaluate potential XXS attacks

Dynamic Application Security Testing

https://docs.gitlab.com/ee/user/project/merge_requests/dast.html
=> OWASP ZAProxy

Addon to chain CI pipelines shared at ONS Europe: https://events.linuxfoundation.org/wp-content/uploads/2017/12/Orange-Openlab-A-Full-Automated-Telco-Stack-for-the-Community-David-Blaisonneau-Nicolas-Edel-Orange.pdf

PoC in progress on OOM (ONAP Installer) gating: https://wiki.onap.org/display/DW/CD+-+Continuous+Deployment

Integration with test pipelines: https://wiki.onap.org/pages/viewpage.action?pageId=6593670&preview=%2F6593670%2F54722733%2Fonap_tests.pdf

CIaaS (OPNFV Functest)

contact Cedric Ollivier

As the process to interact with the CI/CD OPNFV legacy project (Releng) was long and complex and as the goal was to provide the ability for end users to setup their own CI/CD chain on demand, the functest project worked on a CIaaS allowing to setup a CI chain to perform all the tests integrated in functest OPNFV on any infrastructure independenlty from the Release enginnering project.

This automation includes the composition of the different components:

- Jenkins
- Minio
- S3www

- MongoDB (test DB)
- TestAPI
- Docker Registry

See for details: https://wiki.opnfv.org/pages/viewpage.action?pageId=32015004

Gates are already implemented in OPNFV: https://build.opnfv.org/ci/view/functest/job/functest-latest-gate/45/

Xtesting simplifies test integration in a complete LFN-based CI/CD toolchain (e.g. Jenkins, Testing Containers, Test API and dashboard): http://testresults.opnfv.org/functest/gambia/

Note xtesting has been reused for ONAP (see previous section)

available trhough an Ansible Role http://testresults.opnfv.org/functest/functest2019/