# Requirements of the CI

## Seapath must provide many guarantees

- The CI is launched at every pull requests
- The build must succeed AND all the tests must pass
- Avoid regression and display future requirements to meet
- Visible for everyone on GitHub

## System-level testing

- All customer code is in the virtual machines
- Functional testing is impossible here
- Unit testing to check the requirements

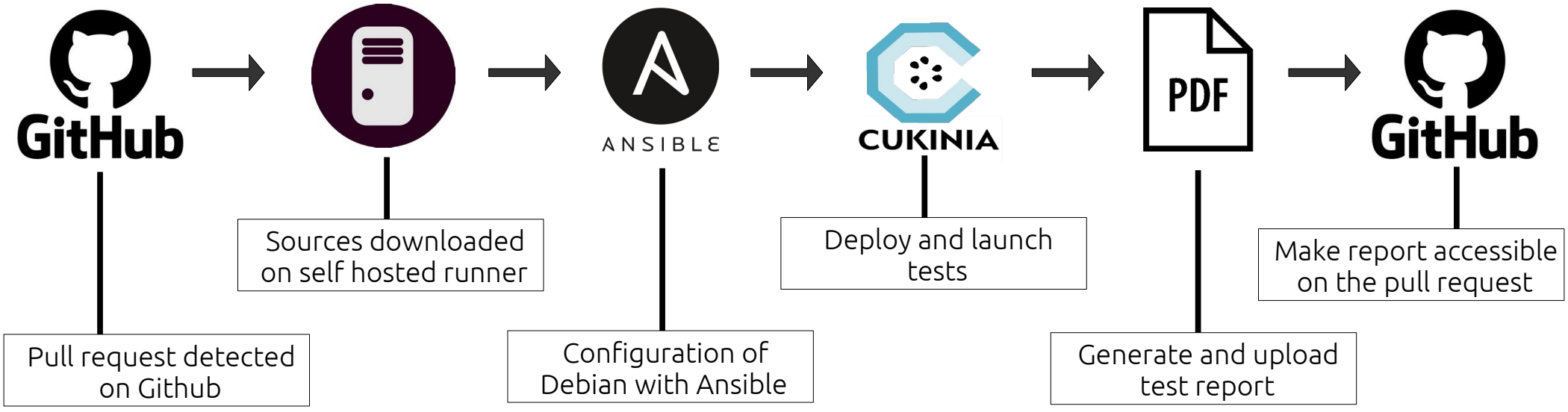
# Writing tests

## System-level testing

- All customer code is in the virtual machines
- Functional testing is impossible here
- Unit testing to check the requirements

| |
|---|
| Check /etc/ssh/ssh_host_ed25519_key permissions |
| Check /etc/ssh/ssh_host_rsa_key permissions |
| root password was randomized at boot |
| root password is randomized at each boot |
| root password is encrypted with a cryto at least equivalent as sha512 |
| bash timeout is set read-only to 300s |
| sshd forbids setting environment variables |

# The complete CI



# Generating a test report

- Organizing more than 1500 tests
- Link all test to specific requirements
- Automatically separate non-regression part and future work
- Tests are visible on the Github repository

## Tests hypervisoriommu for virtu-ci1

| Test ID | Tests | Results |
|---|---|---|
| SEAPATH-00030 | iommu enabled in passthrough mode | PASS |
| SEAPATH-00031 | iommu is loaded | PASS |
| SEAPATH-00032 | iommu is populated | PASS |
| SEAPATH-00050 | Linux kernel *iommu* : INTEL_IOMMU is enabled | PASS |
| SEAPATH-00050 | Linux kernel *iommu* : AMD_IOMMU is enabled | PASS |
| SEAPATH-00050 | Linux kernel *iommu* : AMD_IOMMU_V2 is enabled | PASS |
| SEAPATH-00050 | Linux kernel *iommu* : IOMMU_IOVA is enabled | PASS |

- number of tests: 8
- number of failures: 0

## Tests hypervisorsecurity for virtu-ci1

| Test ID | Tests | Results |
|---|---|---|
| SEAPATH-00033 | /etc/group is consistent | PASS |
| SEAPATH-00033 | /etc/gshadow is consistent | PASS |
| SEAPATH-00034 | /etc/group does not include extra group | FAIL |
| SEAPATH-00034 | /etc/gshadow does not include extra group | FAIL |
| SEAPATH-00006 | Audit subsystem is disabled on cmdline | FAIL |
| SEAPATH-00008 | Slab merging is disabled on cmdline | PASS |
| SEAPATH-00009 | Kernel Page Table Isolation is always enabled on cmdline | PASS |
| SEAPATH-00010 | SLUB redzoning and sanity checking enabled on cmdline | PASS |
| SEAPATH-00004 | libvirtd can not acquire new privileges | FAIL |
| SEAPATH-00005 | libvirtd capabilities are bounded | FAIL |
| SEAPATH-00125 | libvirtd system calls are filtered | FAIL |
| SEAPATH-00039 | openvswitch user is created and locked | FAIL |
| SEAPATH-00040 | openvswitch user is part of hugepages group | FAIL |
| SEAPATH-00041 | openvswitch user is part of vfio-net group | FAIL |
| SEAPATH-00042 | ovs-vswitchd is running as user openvswitch | FAIL |
| SEAPATH-00043 | ovsdb-server is running as user openvswitch | FAIL |
| SEAPATH-00126 | ovs-vswitchd system calls are filtered | PASS |

# Implementation
## 1/2

debian

Use an already deployed Debian

- Already set up Debian on all machines
- No compilation needed
- Avoid the big problem of flashing the machines

ANSIBLE

LVM

Control default state

- Configuration through Ansible
- LVM implement a rollback mechanism

# Future works

## Deploy a CI for the Yocto version

- Implies deploying **other runners** for the compilation
- Handle concurrency problems
- All machines need to be **flashed** on every launch. It can be done either with an **update mechanism** or with **usb gadget**

## Run long-term tests

- Real-time tests
- Cyclictests in virtual machines
- Launch at **every release** to certify that it meet the requirements