openEuler

The Cloud-Native Infrastructure Behind the openEuler Community

TommyLike<tommylikehu@gmail.com>
Maintainer of Infra SIG

Contents

- Who we are.
- Cloud native DevOps.
- Cloud native application design.
- Future plans.

Who we are

About openEuler

openEuler is an open source, free Linux distribution platform. The platform provides an open community for global developers to build an open, diversified, and architecture -inclusive software ecosystem. openEuler is also an innovative platform that encourages everyone to propose new ideas, explore new approaches, and practice new solutions.

Open source

Dec. 2019

Enterprise-lead

2020

openEuler Community Committee established

Donation

Nov. 2021

Community donated to the OpenAtom Foundation

Industry joint contribution

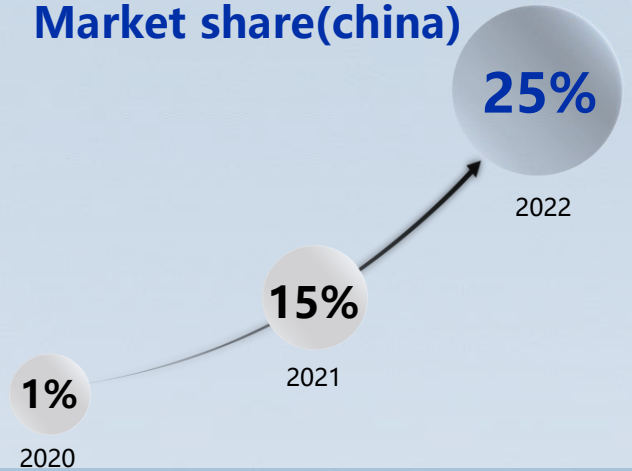
Community rapid growth

Dec. 2022

openEuler Project Group officially established

	Enterprise members (10x ↑)	Contributors (4x ↑)	Version downloads (30x ↑)	Commercial installations (100x ↑)
2022	600+	12,000+	1 M+	3 M+
2020	60	3,630	35,000	30,000

Market share(china)

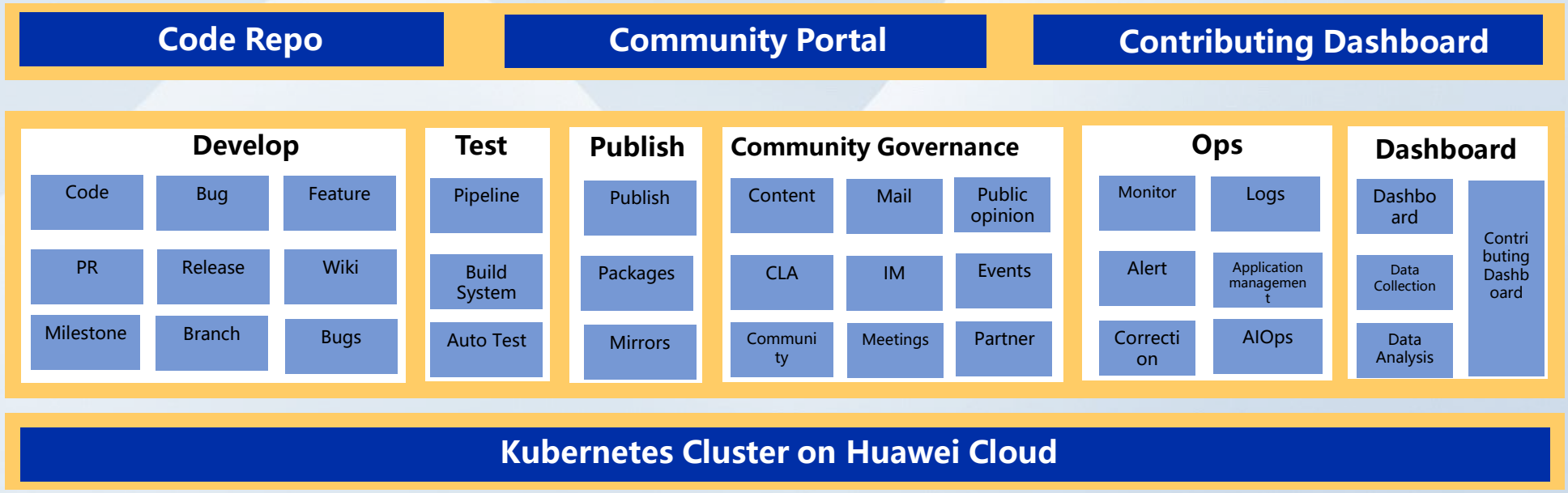


Infrastructure Landscape

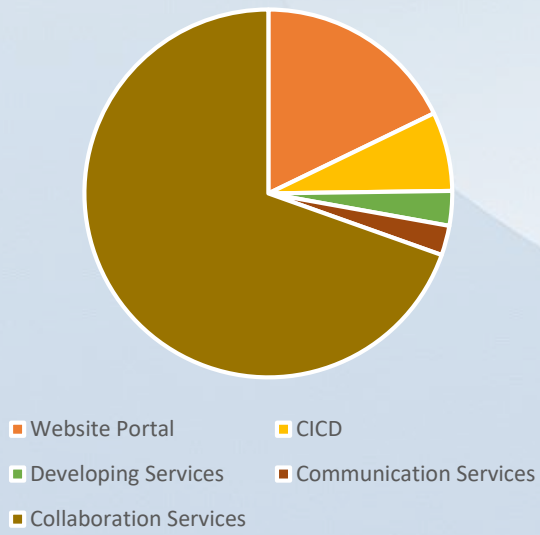
Most of the infra services are developed from open source projects, we utilize those projects and contribute bugfixes and features.

- **Mailing List**: GNU Mailman (Free Software Foundation)
- **Secret manager**: Vault (HashiCorp)
- **Log System**: ELK (Elastic)
- **Data process**: Spark (Apache)
- **Cluster Ingress**: Nginx ingress (CNCF)
- **Developer Package Service**: COPR(Fedora)
- **Application Management**: Argo CD (CNCF)
- **Bot**: Prow(CNCF)
- **Build System**: Jenkins, OBS (Jenkins, openSUSE)
- **Certificate**: Cert Manager (CNCF)
- **Resource Dashboard:** Grafana (Grafana Labs)
- **Infrastructure as Code:** Terraform(HashiCorp)

Service Landscape



Service Categories



1+N k8s clusters

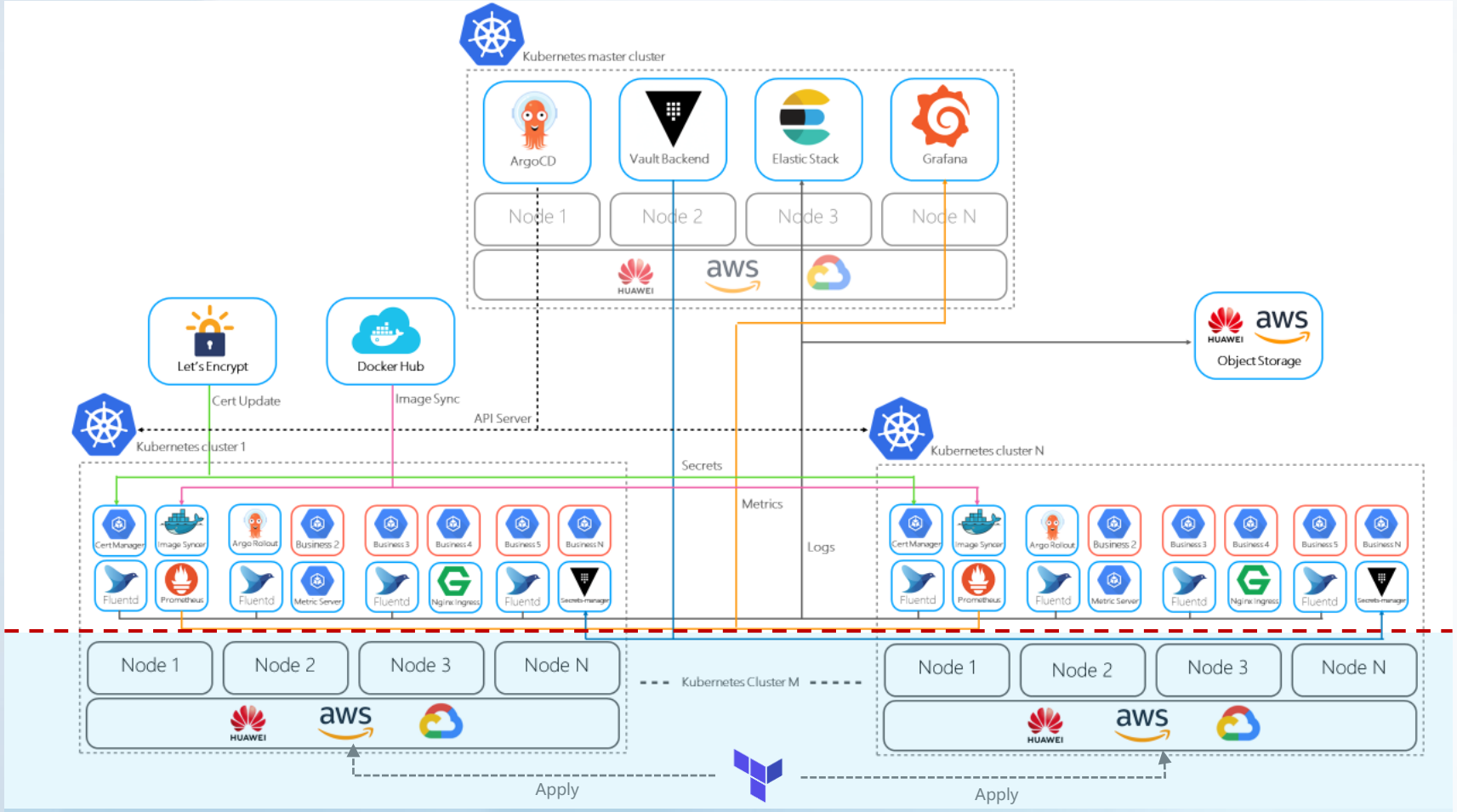
Now we have 155 services, 6 kubernetes clusters and 300 VMs supporting ten thousands of developers in openEuler.

Tier1: Terraform is responsible for managing all low level resource(Cluster, Database, Share and etc.)

Tier2: The key component is the master cluster, which is the DevOps center and consists of several key components including Argo CD, Vault, Grafana, Jenkins and etc. Worker clusters are created in different regions/clouds and configured with different architecture.

Tier2: Apps

Tier1: IaaS

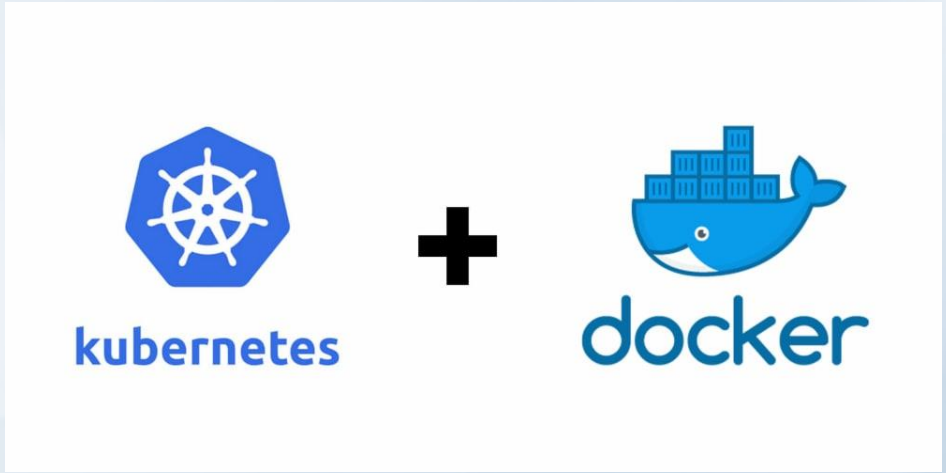


Cloud Native DevOps

Deploy Standardization & Config Separation

1. Most of the services are required to run on kubernetes clusters, thereby we will containerize application and upgrade deploy scripts before publishing, including:

- Containerized application(process per container).
- Kubernetes deploy semantics (helm charts, kustomize …).
- Standard log output.
- Configure via ENVs.
- Restricted image repo
- Trusted base images (openEuler base image).
- Expose health check endpoint.



Containerized application

2. By completely separate the source code, configuration and application repo, we have gained these benefits:

- Cleaner audit log on deployed service and its version
- Separation access and responsibility , developer now focus more on service functionality while SREs on availability.
- One application with multiple configurations/instances

Application Developer

```
|-- conf.yaml
|-- dbinit
|   |-- Dockerfile
|   |-- getsqlitefile.py
|   `-- getsqlitefileTemp.py
|-- deploy
|   |-- configmap.yaml
|   |-- cronjob.yaml
|   |-- deployment.yaml
|   |-- kustomization.yaml
|   |-- namespace.yaml
|   |-- pvc.yaml
|   `-- service.yaml
|-- Dockerfile
|—src
```

DevOps Engineer

```
|-- debug
|   |-- ingress.yaml
|   `-- kustomization.yaml
|-- kustomization.yaml
`-- release
    |-- ingress.yaml
    `-- kustomization.yaml
```

Infra Maintainer

```
|-- dailybuild-lts.yaml
|-- etherpad.yaml
|-- jenkins-cn-north4-2.yaml
|-- jenkins.yaml
|-- mail.yaml
|-- meetings.yaml
|-- pkgmanage.yaml
|-- repo-mirror.yaml
```

3 Steps to deploy application

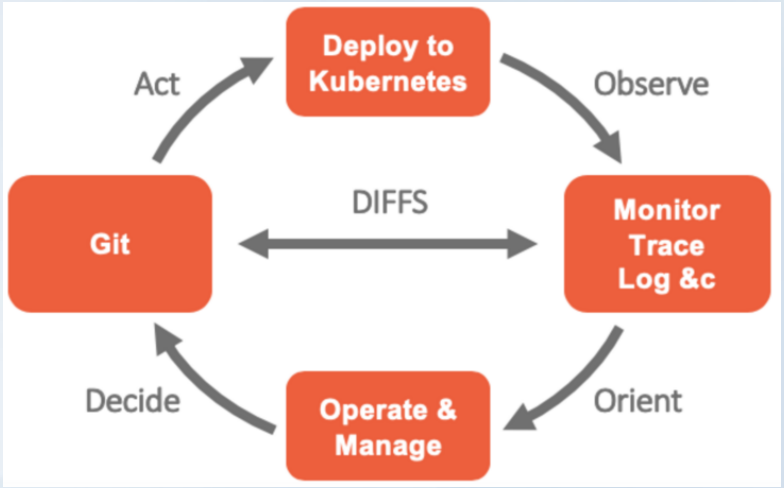
Mange with GitOps and Automation

1. All of infrastructure Services are organized in openEuler infra deploy repo:

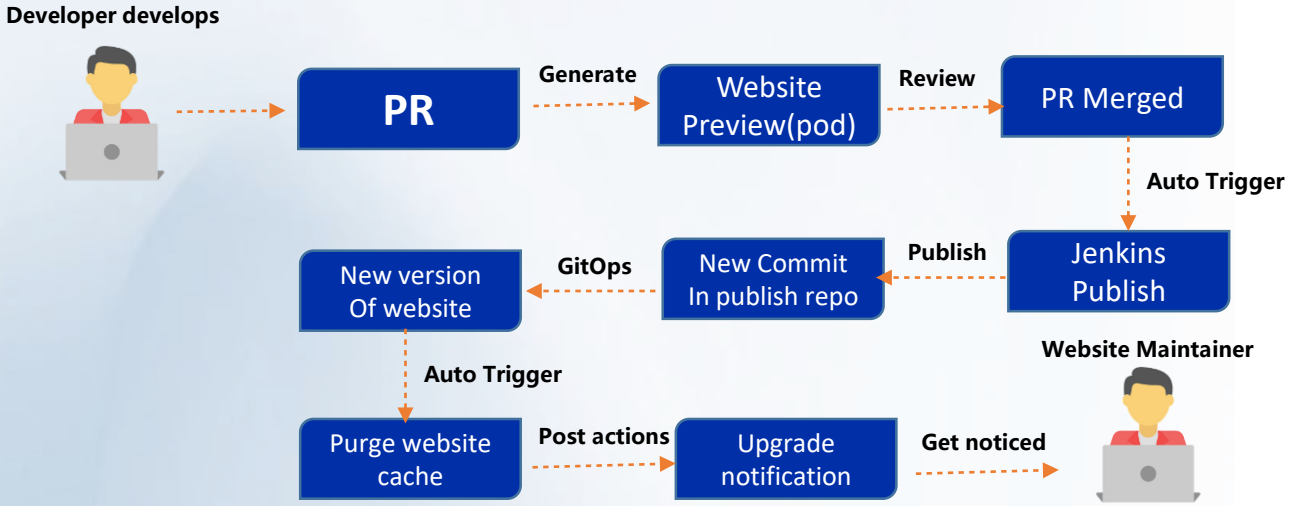
- Increased Productivity
- Improved Stability
- Higher Reliability
- Consistency and Standardization
- Stronger Security Guarantees

2. Along with service developing, we added some tools and pipelines for the purpose of efficiency:

- End to end pipeline for every service, including code lint, build, CVE scan, publish, post validation and notification,
- Self -service administration, for example, maillist templates, mirror lists, Jenkins slave clusters, review plugins and etc.
- Self-service operate, for example, log, metrics, k8s cluster operate, replicas, alarm rules.



GitOps cycle



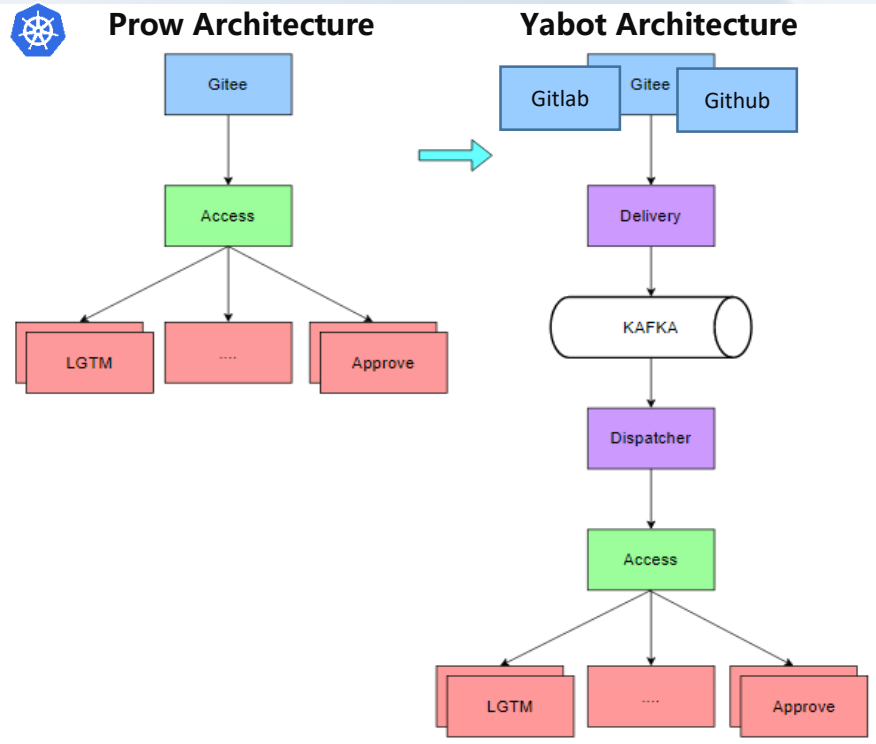
Website pipeline

Cloud native application design

Yabot: Automatic scaling bot with rich plugins

Yabot(Yet another bot) is based on the **prow** project from CNCF community and we improved it through several aspects

- **Robust**: Plugin in separated container
- **High throughput:** Use Kafka for message delivering
- **Automatic scaling**: Plugins will be scaled based on its abilities of handling request (HPA).
- **Easy to use**: Multiple platforms support & 50+ plugins
- **Easy to develop**: Scaffold code for plugin develop & multiple developing language support.



Prow vs Yabot

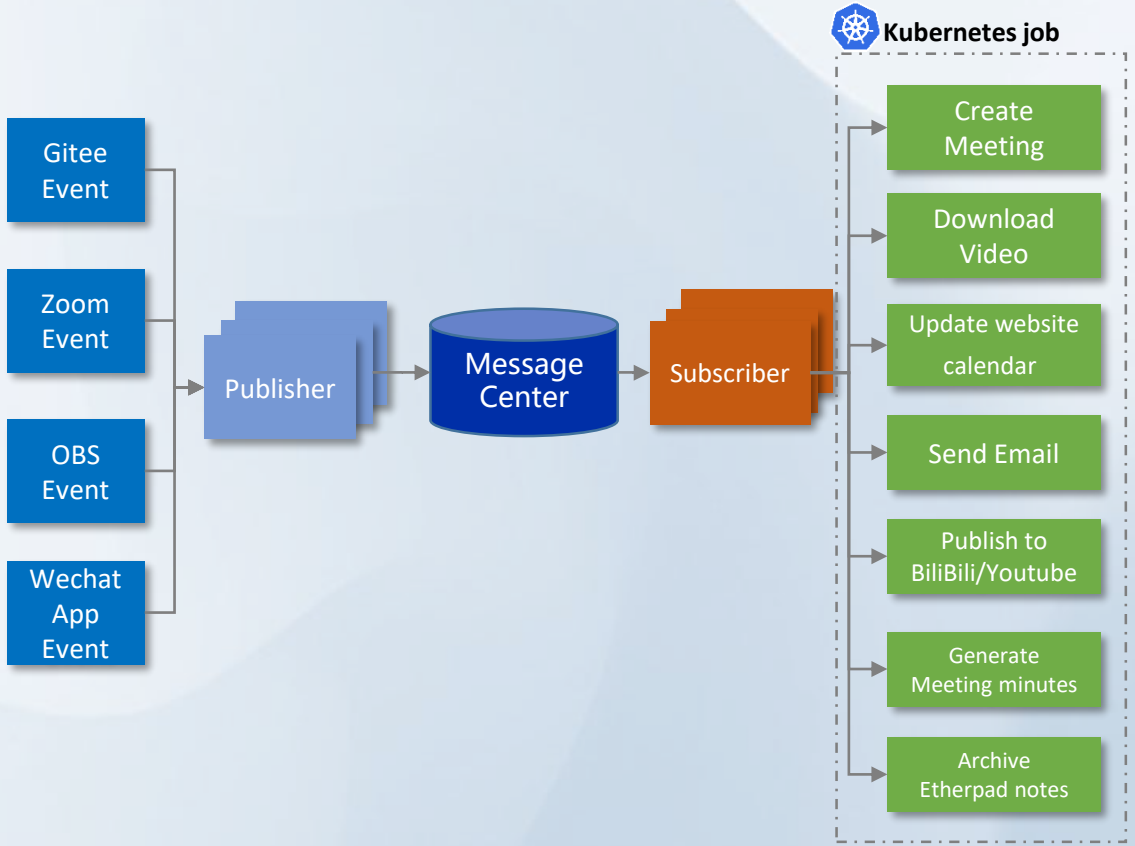
Command	Example	Description	Who Can Use
/check-cla	/check-cla	Forces rechecking of the CLA status of a Pull Request. If the Pull Request author has already signed CLA, the label openlookeng-cla/yes will be added in the Pull Request, If not, the label openlookeng-cla/no will be added.	Anyone
/lgtm [cancel]	/lgtm /lgtm cancel	Adds or removes the lgtm label which is typically used to gate merging.	Collaborators on the repository. /lgtm cancel can be used additionally by the Pull Request author.
/approve [cancel]	/approve /approve cancel	Adds or removes the approved label which is typically used to gate merging.	Collaborators on the repository.
/assign [[@]...]	/assign /assign @openEuler-bot	Assigns assignee(s) to the PR or issue.	Anyone can use the command, but the target user(s) must be an org member, a repo collaborator, or should have previously commented on the issue or PR. If no target user is specified, that means will be assigned to yourself.
/unassigne	/unassign /unassign @openlookeng-bot	Unassigns assignee(s) to the PR or issue.	Anyone can use the command, but the target user(s) must be an org member, a repo collaborator, or should have previously commented on the issue or PR. If no target user is specified, that means will be unassigned to yourself.
/[add|rm]-collaborator	/add-collaborator /rm-collaborator /add collaborator @openeuler-bot	assigns or unassigns collaborator(s) to the issue	Anyone can use the command, but the target user(s) must be the repo's member. If no target user is specified, that means will be unassigned to yourself.
/check-milestone	/check-milestone	Check whether the issue is set a milestone, remove or add needs-milestone label	Anyone
/check-issue	/check-milestone	Check whether the Pull Request is associated with at least an issue, remove or add needs-issue label	Anyone
/remove-needs-issue	/remove-needs-issue	remove the needs-issue label	Members of the project can use the /remove-needs-issuecommand
/check-ci	/check-ci	Forces rechecking the CI status and adding CI label if possible.	Anyone
/test ?	/test ?	List available test job(s) for a trusted PR.	Anyone
/retest	/retest	Rerun test jobs that have failed.	Anyone
/ok-to-test	/ok-to-test	Marks a PR as trusted and starts tests.	Members of the trusted organization for the repo.

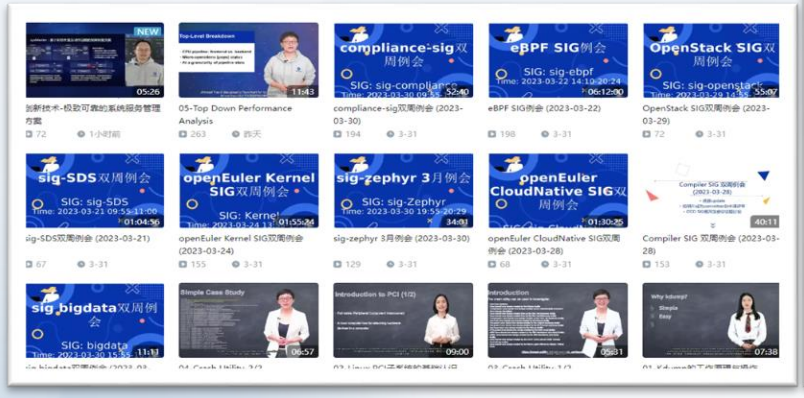
Notable Plugins

MeetingBot: E2E solution for online meetings & events

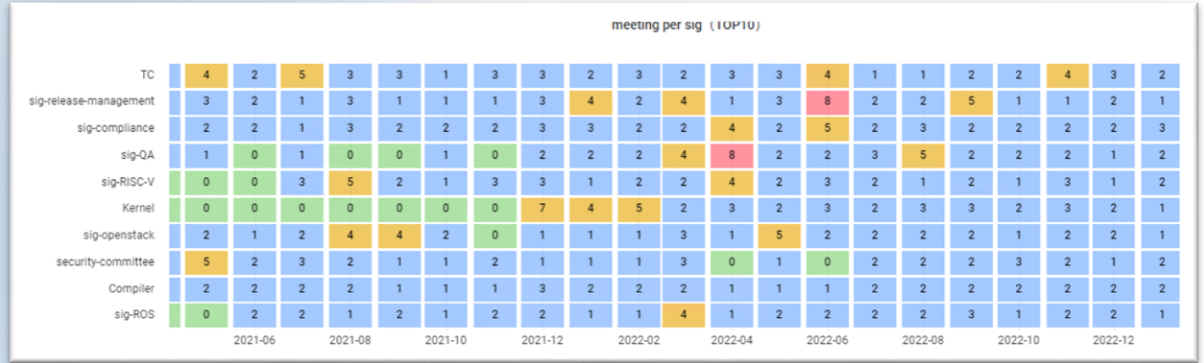
MeetingBot is the application provides all functionality related to online meetings and events. it’ s triggered by events and done by different kinds of kubernetes jobs. We have created **1100** meetings and about **9120** developers participated by far.

- **Pluggable Backend**: Support Zoom/Welink/Tencent meetings.
- **Website/Wechat App:** Support Book meeting via website or Wechat App.
- **Multiple social platform**: Support publish video to Youtube & Bilibill.





▼Sig meetings/month ▲Meeting Videos ▶Book Meeting in App

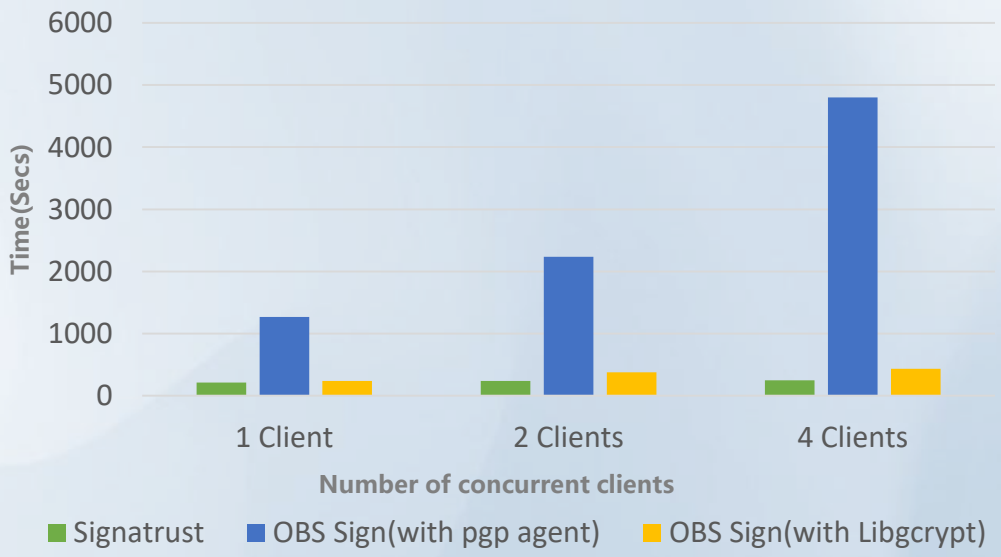


Signatrust: Secure and efficient solution for signing Linux packages

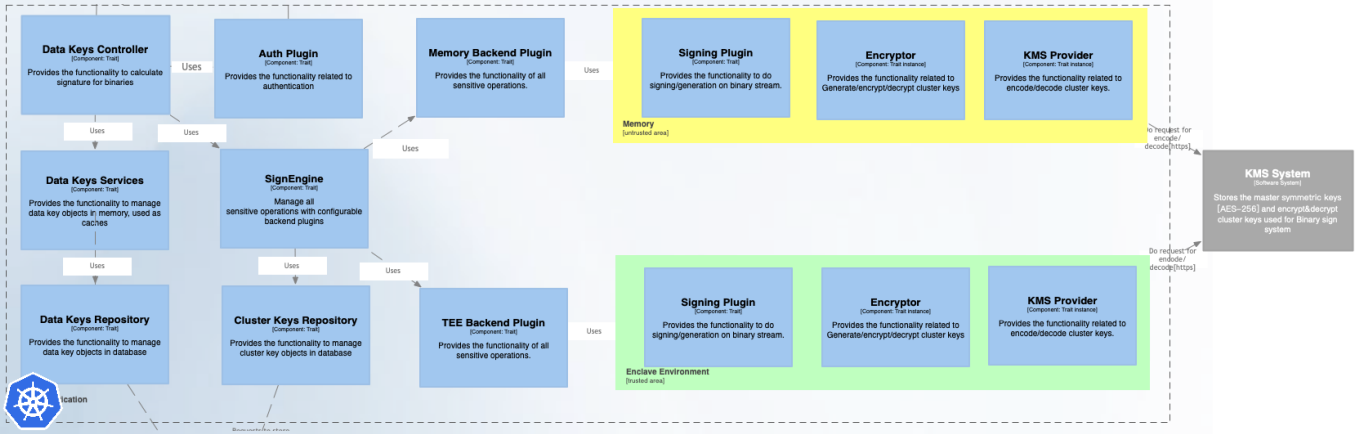
Signatrust: is a project based on the idea of **obs-sign** from openSUSE while provide a more comprehensive, efficient and cloud native solution for packages sign.

- **E2E security design**: keys encrypted with KMS system/Signature calculated in HuaweiCloud Enclave(TEE) environment/Pure Rust/mTLS
- **High throughput**: Replicated data servers/gRPC stream/Fully async tasks
- **Complete binaries support**: RPM//ISO/Kernel Module/EFI/Container Image/WSL Image
- **User-friendly key management**: Standalone management interface and can be integrated with account systems via OIDC

Performance of Sign RPM



Signatrust System Components(Use Huawei Enclave)

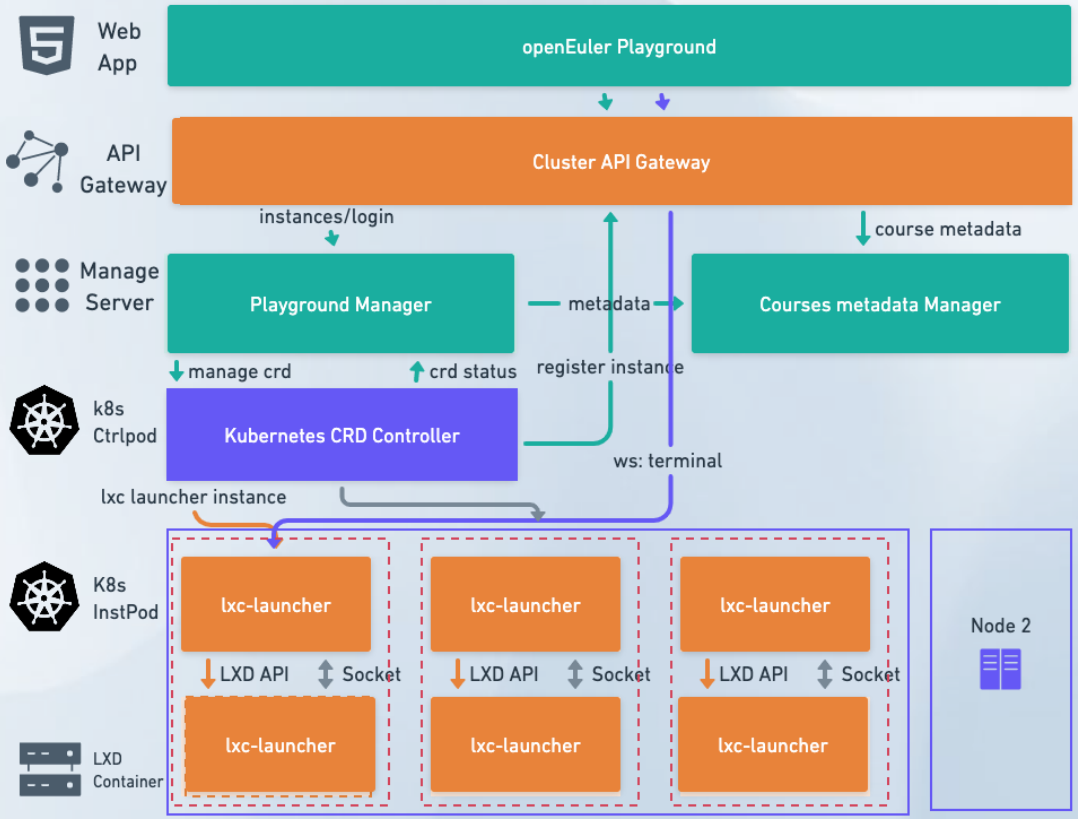


MoocStudio: Native terminal playground in browser

MoocStudio is based on **kubernetes operator** and provides a openEuler terminal environment for community developers.

- **Rapid Distribution**: Establish connection to brand-new environment in 20s.
- **Multiple Environment:** Support application container/system container/virtual machine(LXD),
- **Customized Image**: Environment can be highly customized, including base OS, architecture, additional files/packages.
- **Automatic Release**: Environment will be released when disconnected, different release strategies for compute and storage resource.

MoocStudio Architecture

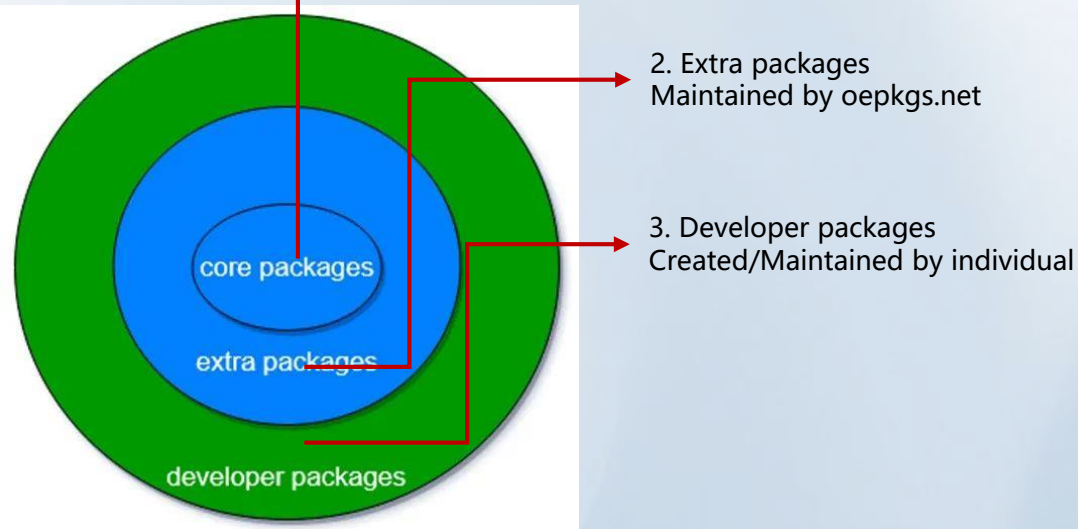


Screenshot of learning git in openEuler

EUR: Lightweight package build & distribute platform for individual

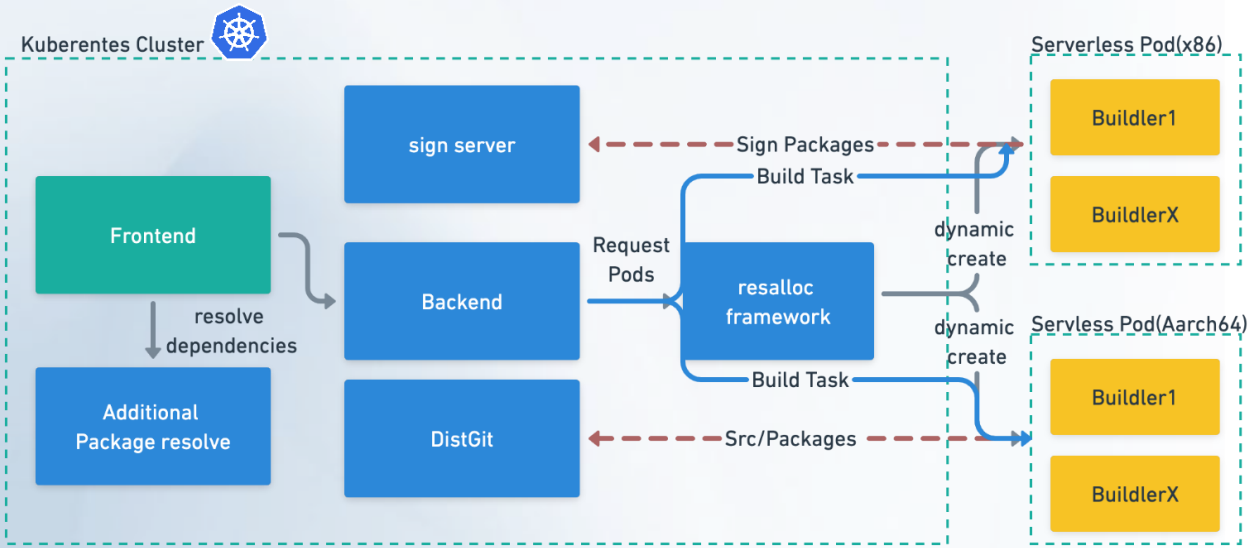
EUR(openEuler User Repository) is forked from **COPR** project from Fedora and components have been customized for openEuler.

- **Cloud Native**: All components have been upgraded for kubernetes environment.
- **Dynamic Task builder:** Use serverless kubernetes pod as backend builder(X86&Aarch64 supported).
- **Automatic Dependency Resolve:** Resolve package dependency and auto import.
- **Integration**: EUR is highly integrated into our package develop process.



1. Why we need EUR?

2. Package develop process

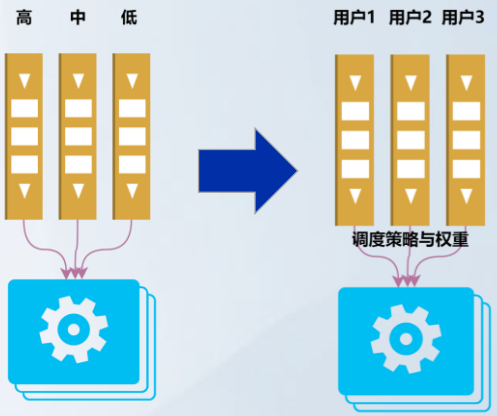


3. Upgraded architecture to support serverless pod resource

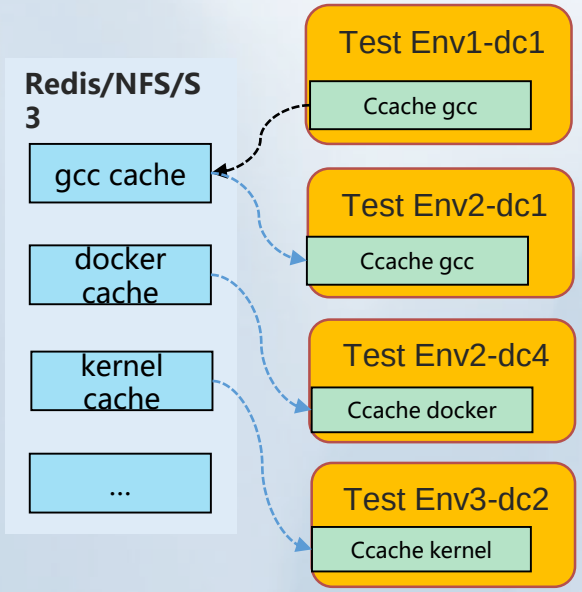
EulerMaker: OS build system for different scenarios

EulerMaker: we used to use OBS for package building and now developed our own build system with several improvements:

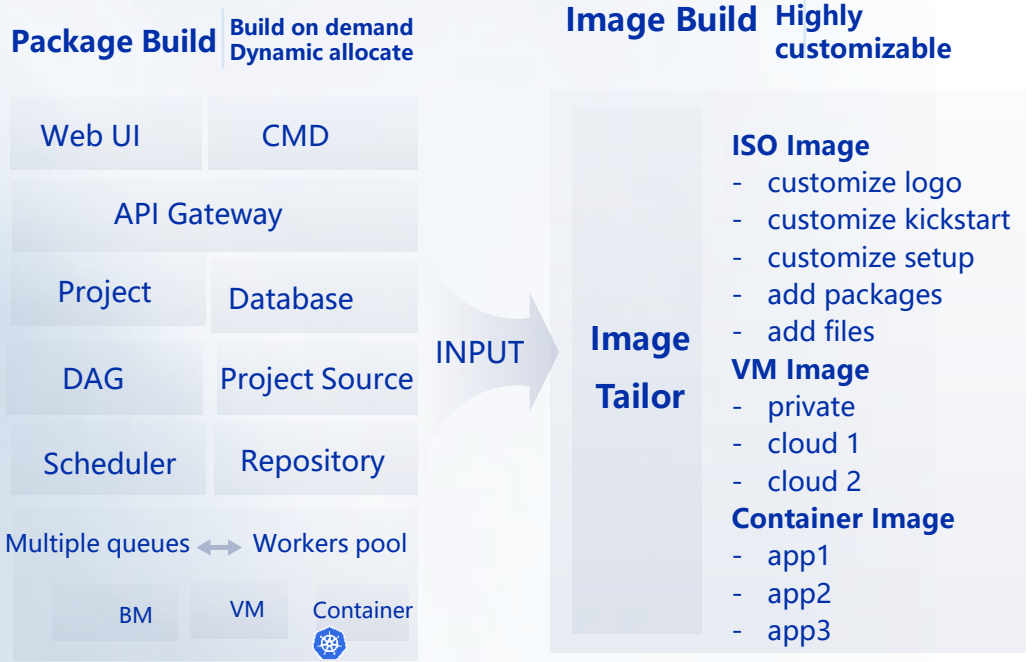
- **Dynamic Workers**: Workers are dynamically created including(VM/BM/Container). 3 times faster in build performance compared with OBS.
- **Job queue per user with priorities:** Less waiting time for individual developer.
- **Global Build Cache**: Support global build cache, build performance improved 30% for single package in average.
- **Image Build:** highly customized for image generation, including image format/setup process/additional packages.



1. Job queue per user



2. Global build cache



3. Build Packages & Images

Future Plans

Future Plans

- **SSO:** Introduce SSO solution and connect all applications to SSO platform.
- **Cloud IDE**: Support develop & test with cloud environments and cloud IDE.
- **Message Center**: Integrate all application with message center by Cloud Events.
- **Service Mesh.**

How to Engage

@openEuler
https://twitter.com/openEuler

r/openEuler
https://new.reddit.com/r/openEuler/

openEuler
https://www.youtube.com/@openeuler/

openEuler
https://www.linkedin.com/company/86315548/

Official website

LinkedIn newsletter

Join SIGs

Download

Thanks