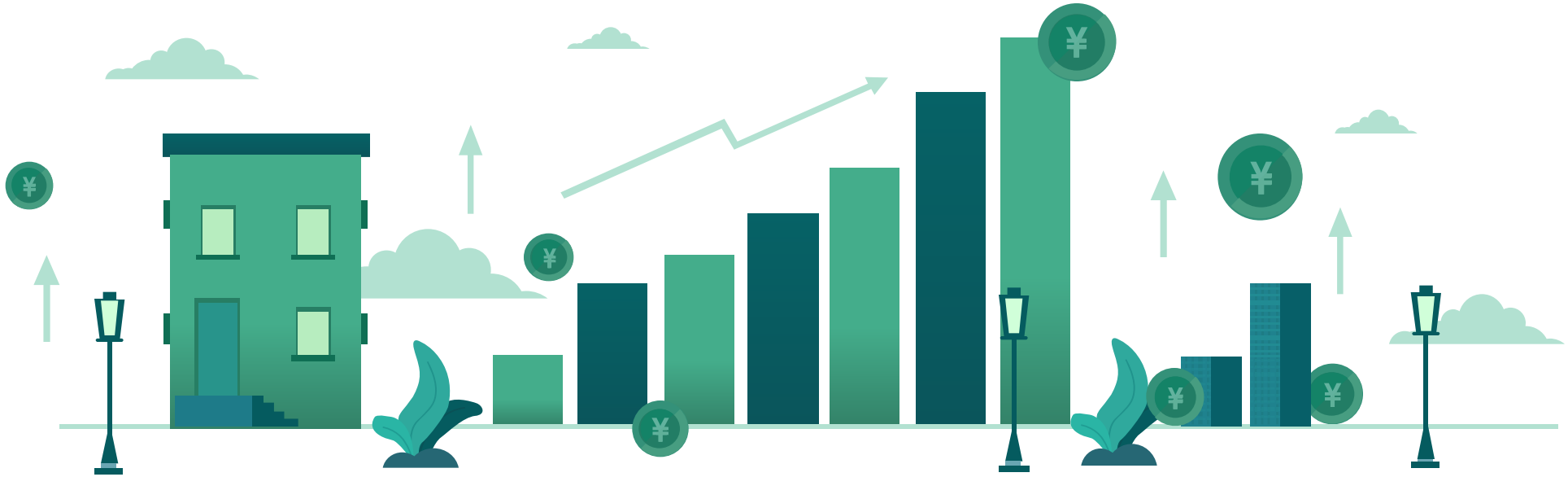
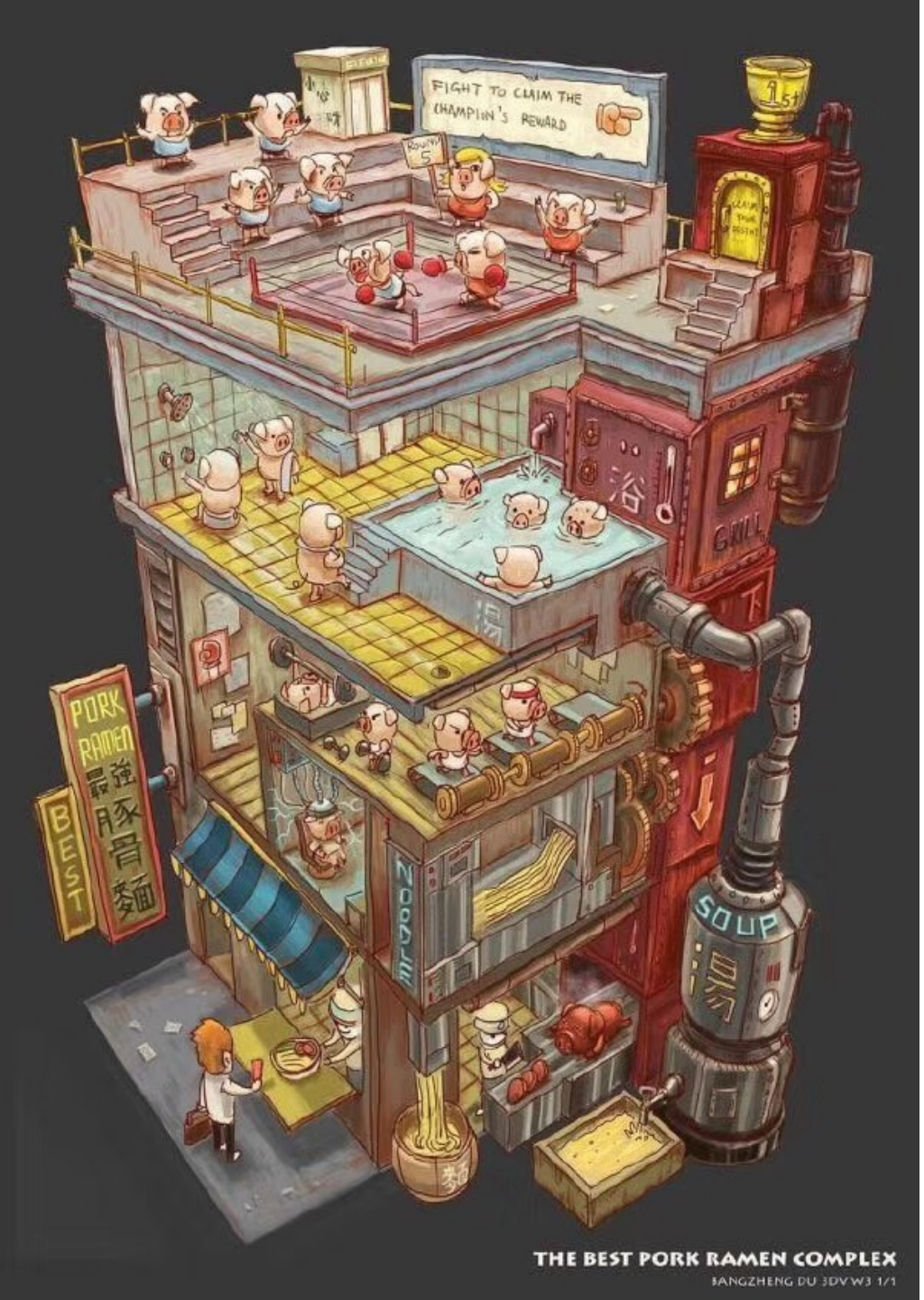
基于容器的持续集成中遇到的安全挑战

当引入容器进入到 DevOps 领域后提升了效率，同时引入了新的安全威胁。

马全一 - 腾讯云 PaaS 平台产品经理、专家工程师

cloud.tencent.com





DevOps is an operational philosophy that promotes better communication between development and operations as more elements of operations become programmable.

2018 Survey

The State of DevSecOps in the Enterprise

More than 60% of organizations now have DevSecOps teams in place

What are the most important elements of DevSecOps?

1. **61%** Apply Security Across the Application Lifecycle
2. **54%** Automate Application Security Controls
3. **43%** Involve DevOps in Security Processes

Other DevSecOps elements that were rated as important:

- Having cross-functional teams (Sec and DevOps)
- Shift-left security
- Involve security pros in the DevOps processes

Is the company ready for DevSecOps?

57% Have the budget and expertise to implement DevSecOps

70% Ready to embrace the cultural change fusing security and DevOps

63% Currently have a formal or informal DevSecOps team In house

▲ **X5 more compared to 2016**

How mature is your implementation of AppSec using DevSecOps?

14%	39%	20%	27%
Immature	**Maturing**	**Fairly mature**	**Very mature**
We're trailing behind our peers	It's getting more attention than before	Ahead of the curve	Leading edge / early adopter

How are AppSec budgets changing?

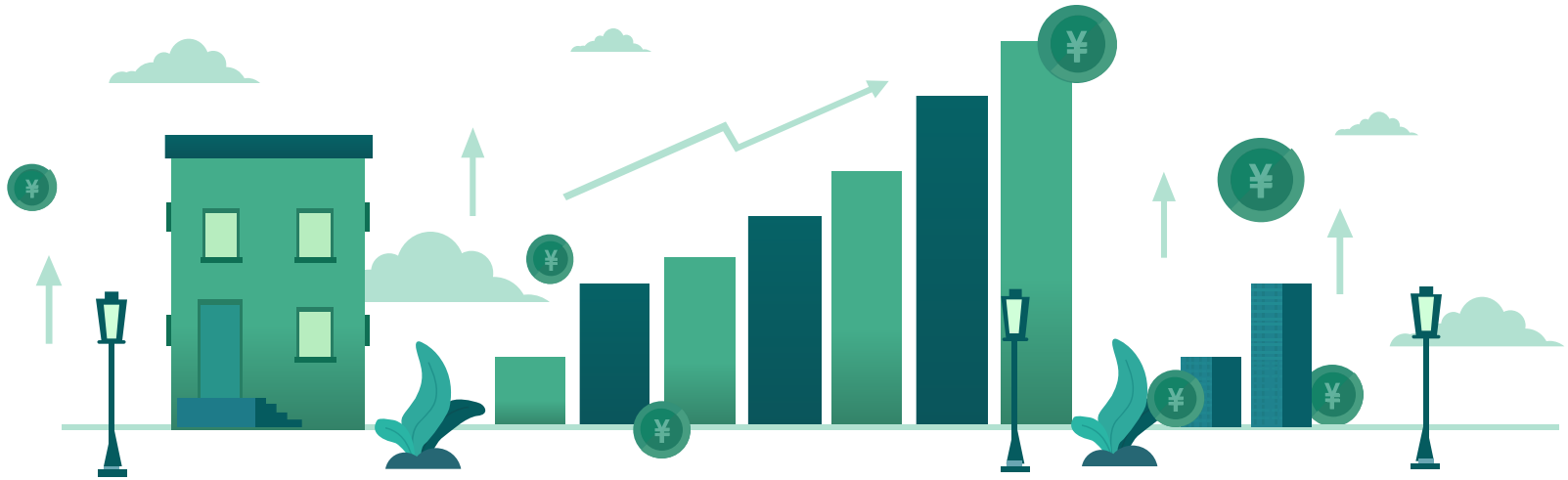
Over the past 5 years, organizations reported:

- **21%** Budget went UP by more than 30%
- **25%** AppSec budget went UP by less than 30%
- **4%** AppSec budget went DOWN

Survey conducted among 80 security professionals, during the RSAC conference 2018

aqua www.aquasec.com

CONTENTS



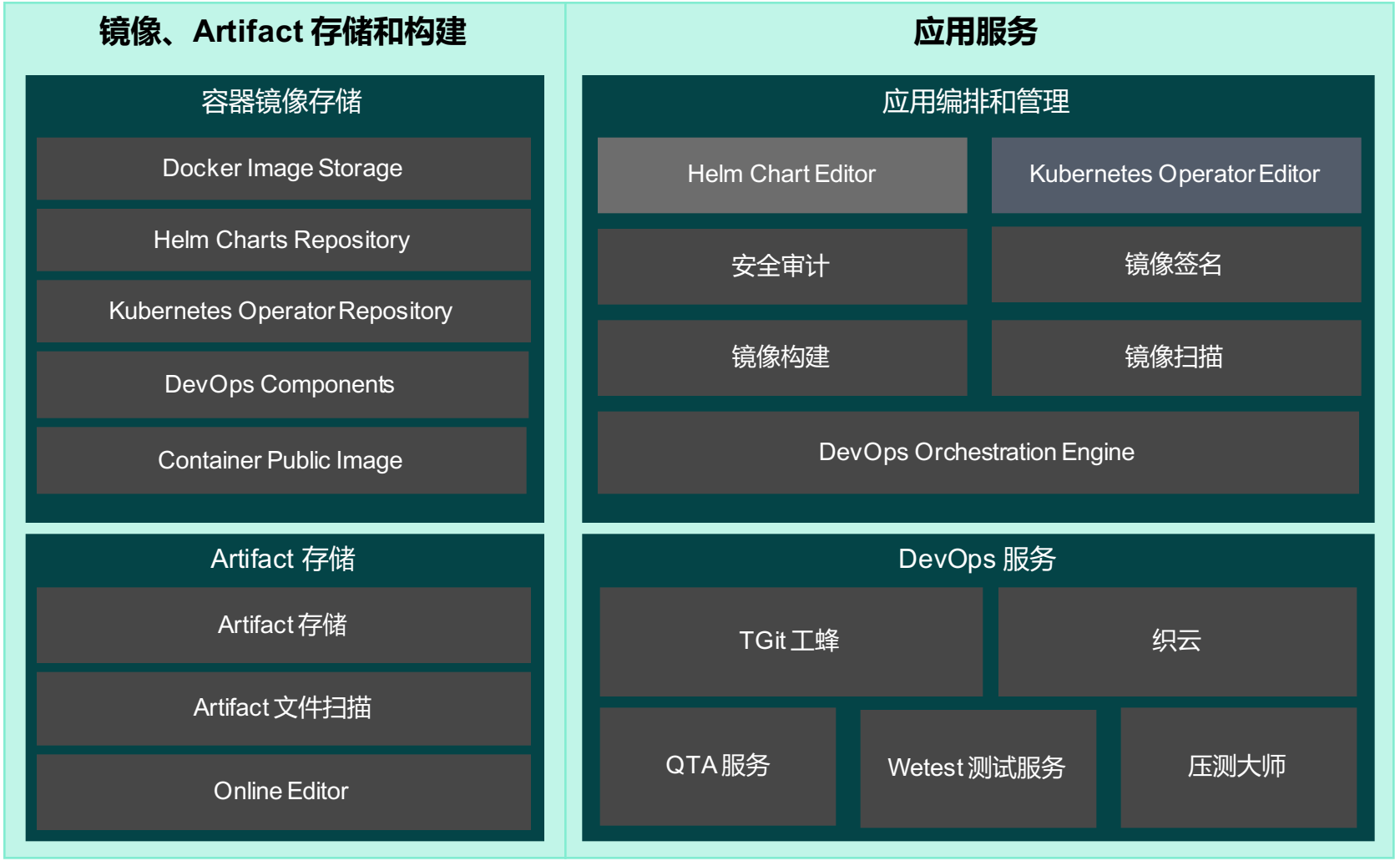
/01

腾讯云持续集成方案

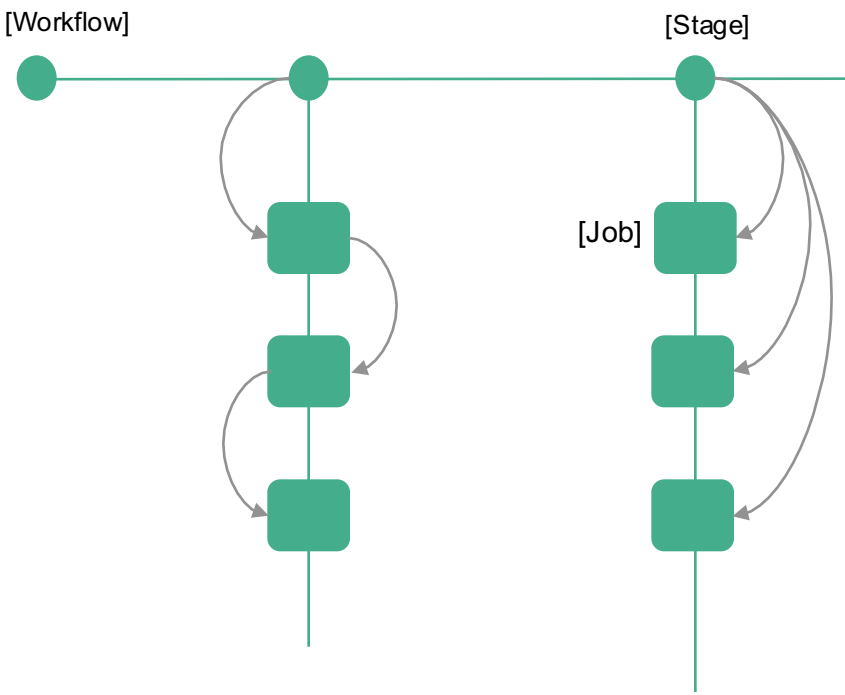
利用 DevOps 编排引擎，打通腾讯云上多种 DevOps 服务。

腾讯云 DevOps 解决方案

- Tencent Hub 是腾讯云 DevOps Hub ，为开发者提供一站式存储和 DevOps 任务编排能力。
- 提供 DevOps Supply Chain 安全审计、镜像和 Artifact 的安全扫描和签名。
- 对接丰富的 DevOps 服务。



腾讯云 DevOps 解决方案 – 通用的编排逻辑



Workflow 是基于 Tencent Hub 的流式任务执行引擎。将任务分解为不同 stage 的多个 jobs，执行更加高效、敏捷，是最佳的 DevOps 解决方案。

[**workflow**] 一组 DevOps Task 编排为一个 workflow。

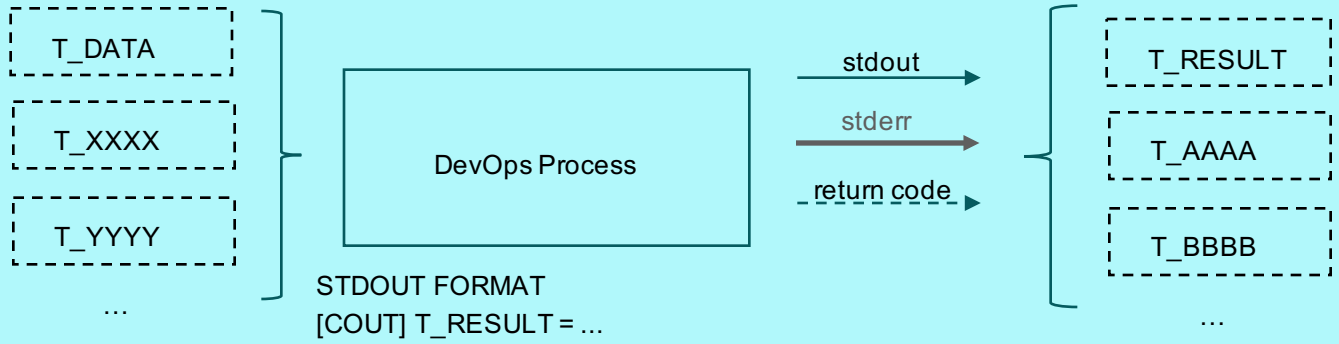
[**stage**] workflow 中的不同阶段工作划分为不同的 stage ，stage 有 4 种类型：start/normal/pause/end 。在 normal 的 stage 上使用 job 执行具体的 DevOps Task ，有顺序执行和并行执行两种方式。

[**job**]每个Job 对应一个 Component 或 Service API，执行 Job 即运行指定的 Component 。

[**Component**]Job中执行任务的容器镜像，定义了输入及输出，完成用户的测试/编译/测试/部署/自定义任务。

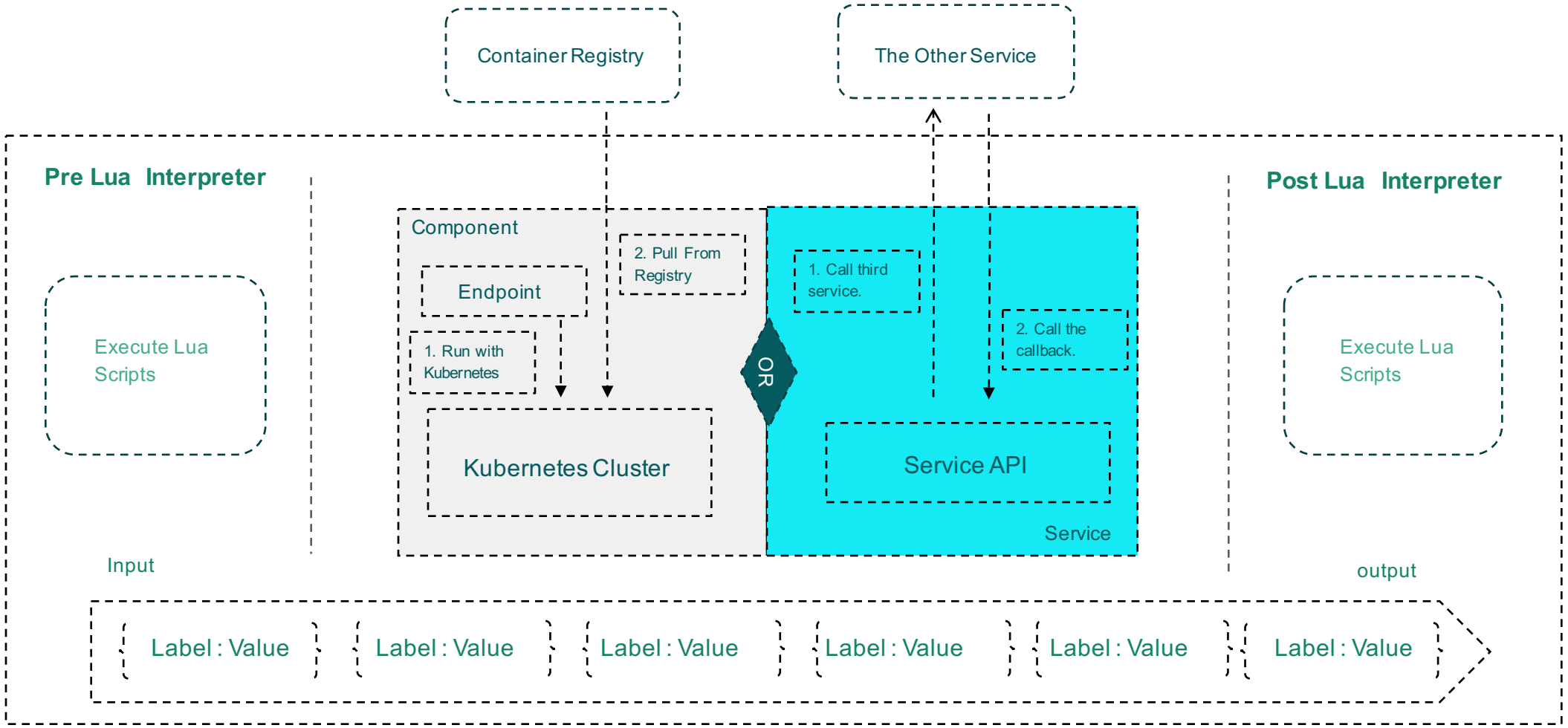
腾讯云 DevOps 解决方案 – 通用的插件机制

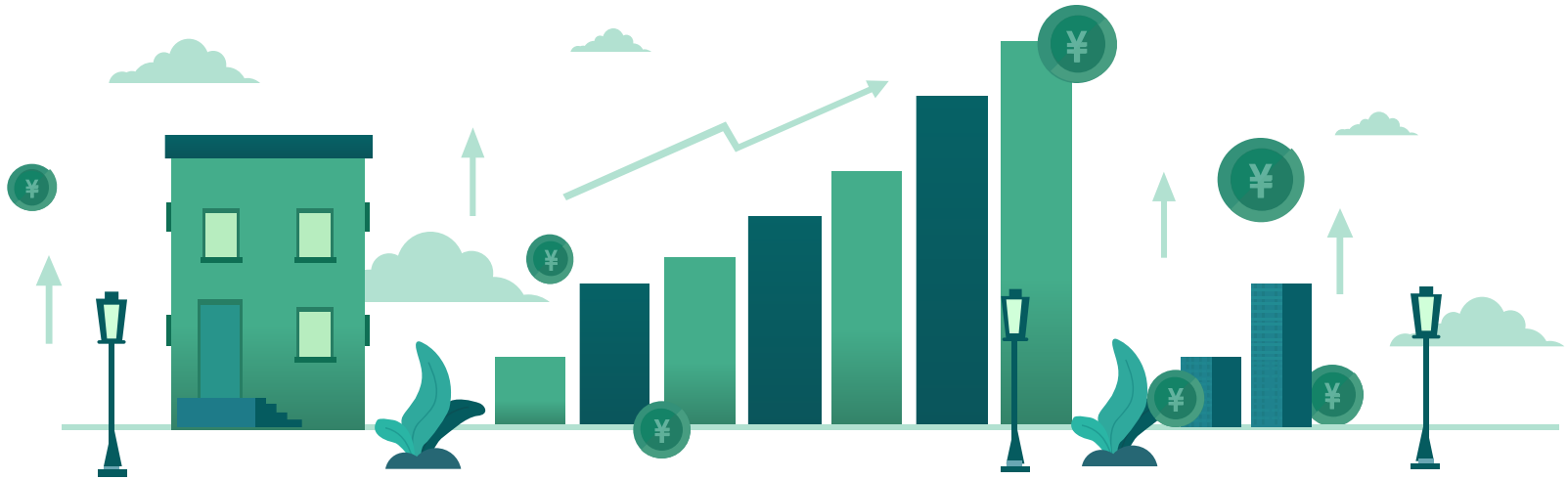
Reserved environment variable [T_DATA] for transfer data into container, user could define more variables and we suggest all variable name prefix with [T_].



[Base Image] https://hub.docker.com/r/phusion/baseimage

腾讯云 DevOps 解决方案 – 通用的执行方式





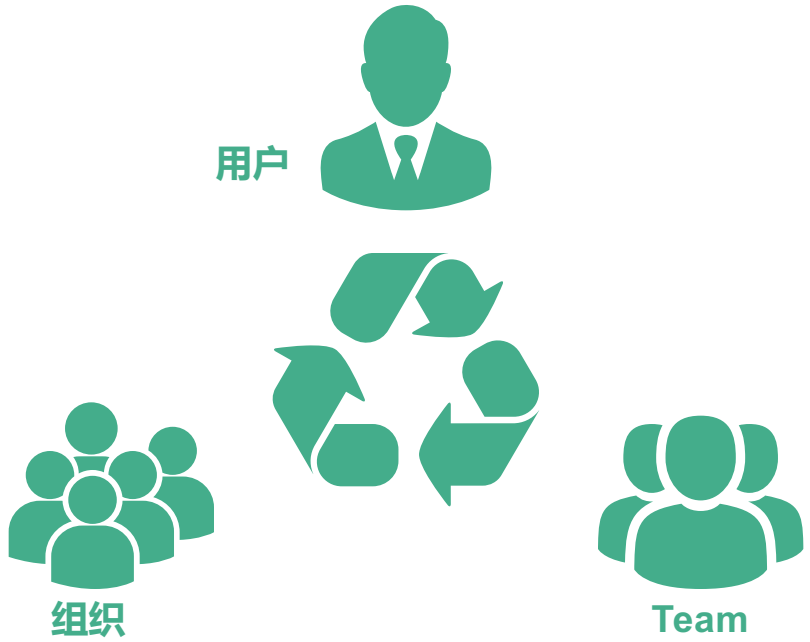
/02

账号体系互通带来的认证和权限问题

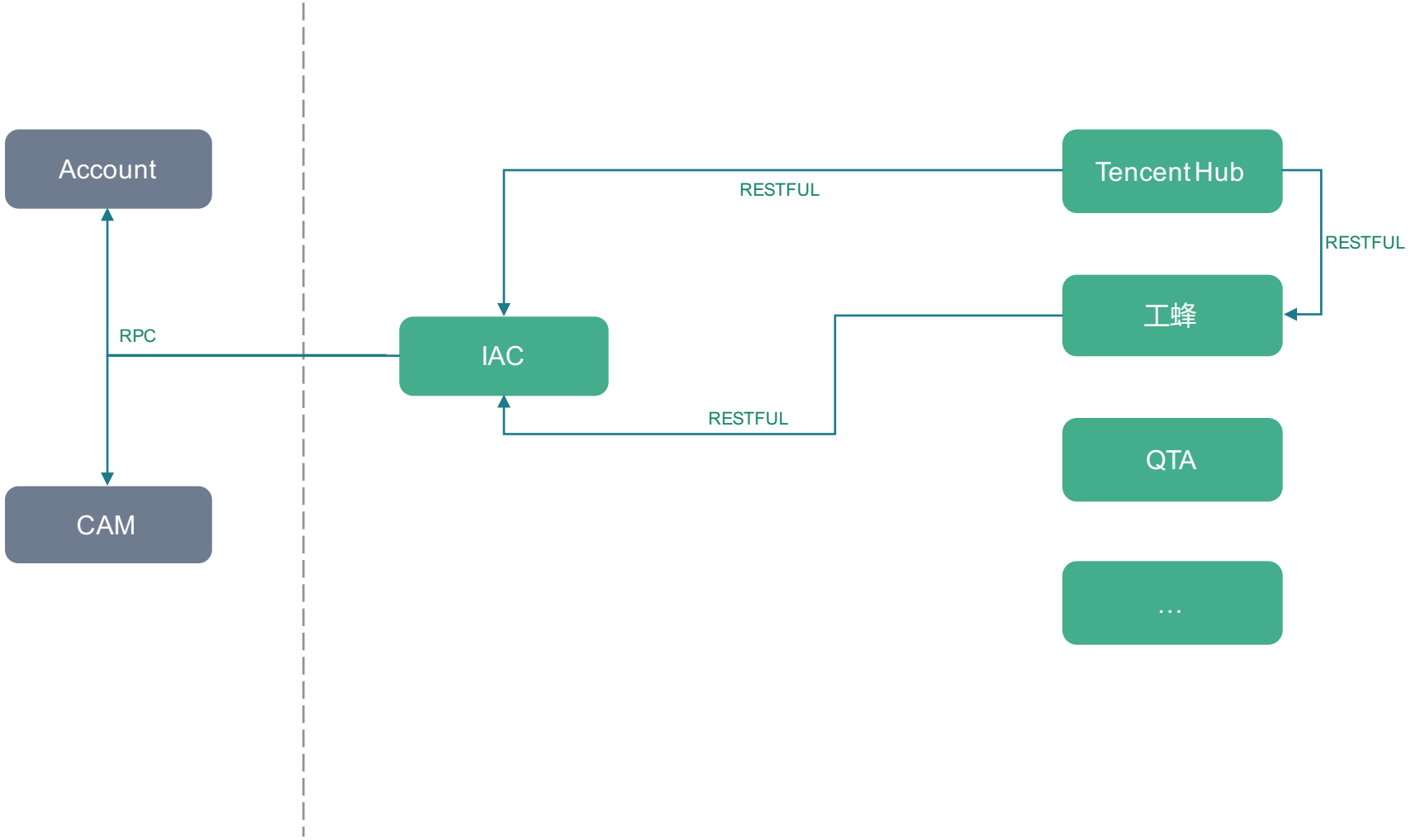
打通多种 DevOps 服务和腾讯云的帐号体系及权限，统一用户登录和权限设置的体验。

腾讯云多账号体系现状

Tencent Hub 账号体系

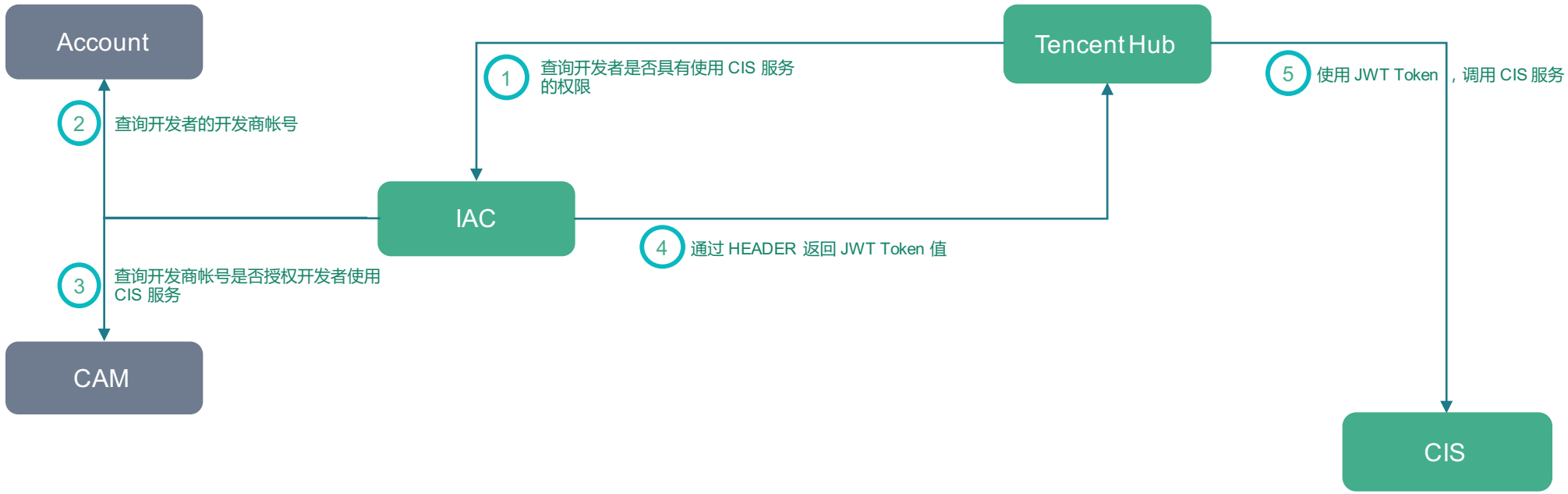


构建独立服务屏蔽腾讯云帐号和 ACM 系统

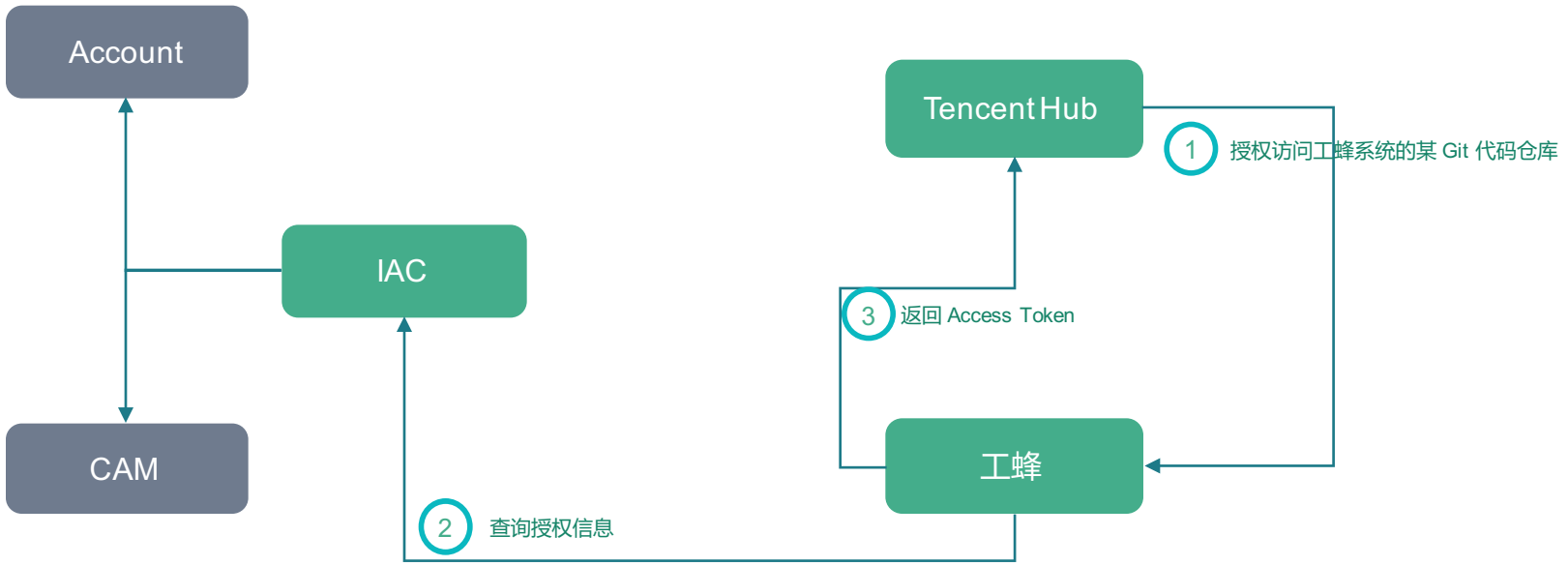


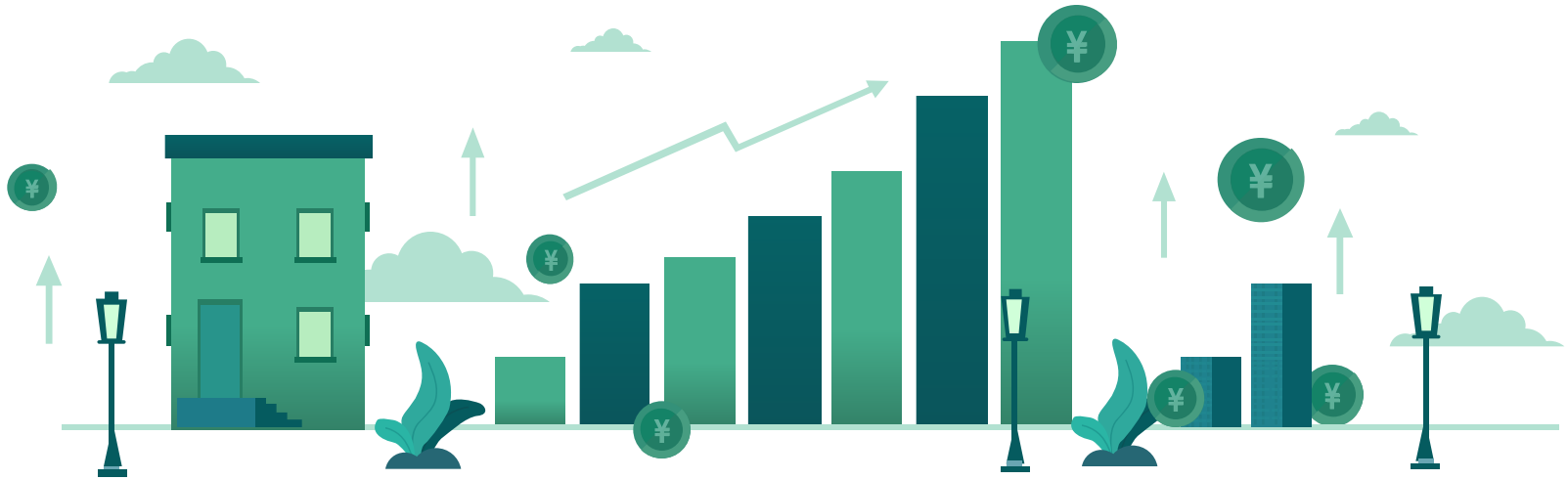
什么是 JSON Web Token <JWT> ？

利用 JWT 打通腾讯云服务和 DevOps 之间的帐号和权限



利用 OAuth2 打通 DevOps 服务之间的帐号和权限





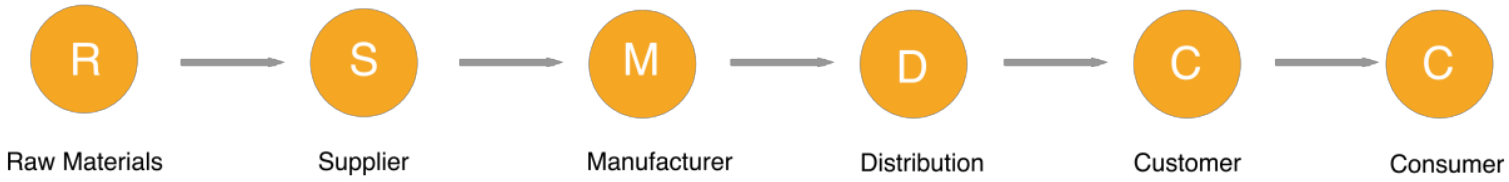
/03

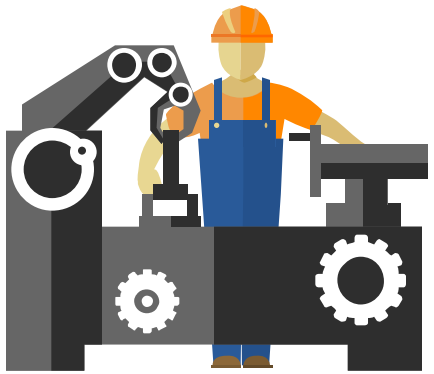
Supply Chain Audit

对 Supply Chain 进行审计，保证从服务从源代到构建、直到部署环节没有被恶意篡改。

Supply Chain 安全威胁和挑战

- 软件更新污染 Software Update
- 软件库污染 Software Library
- 固件污染 Firmware
- 水洞污染 Waterhole

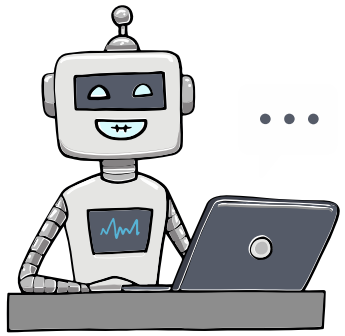




- 不停增长地、碎片化的工具集
- 分布式的协作
- 大量使用了开源软件
- 业务多云服务商
- 基础架构都是微服务

Grafeas – cloud artifact metadata CRUD API and resource specifications

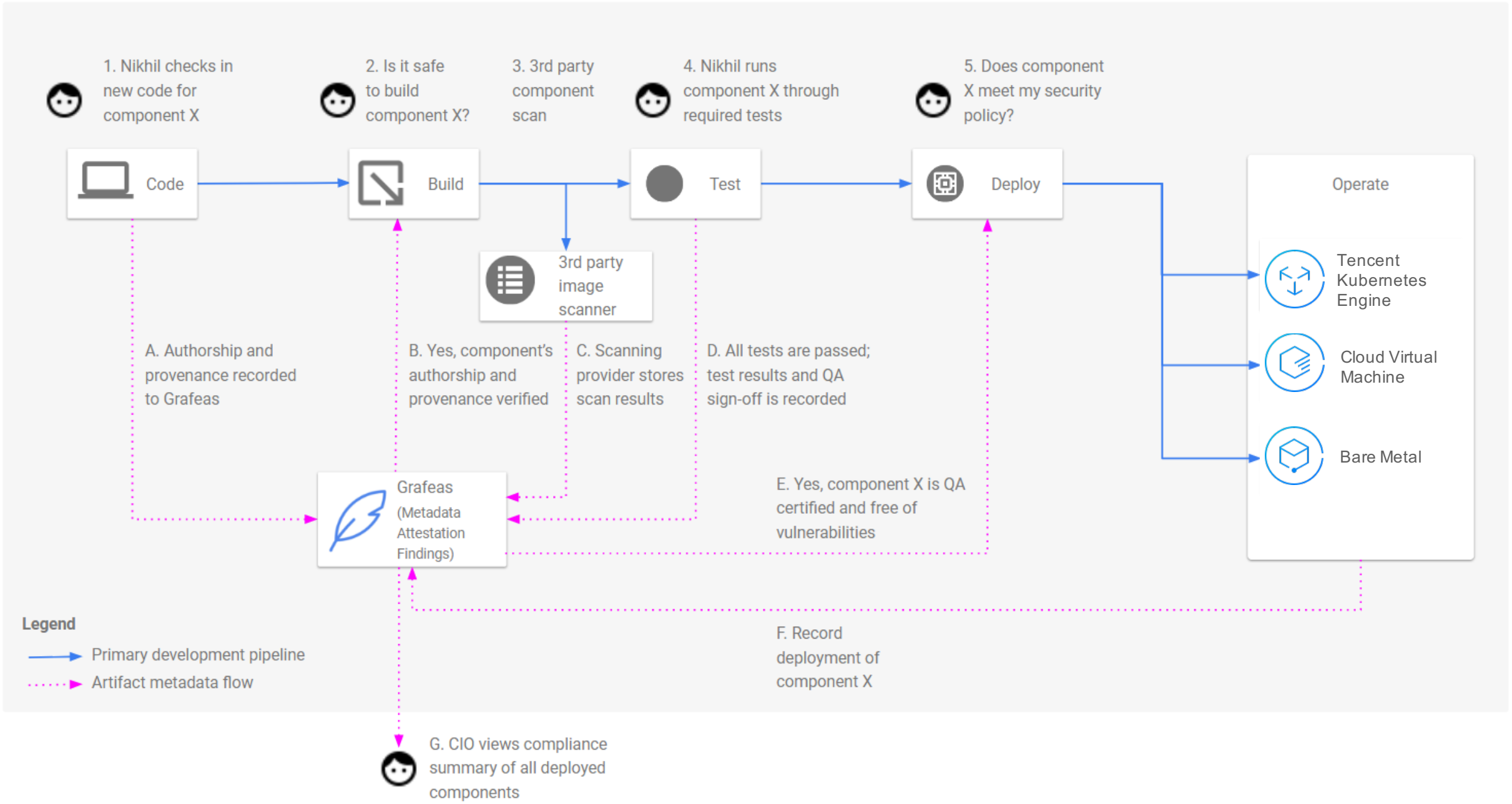
Notes: A note is an item or condition that can be found via an analysis or something that is used multiple times in a process.

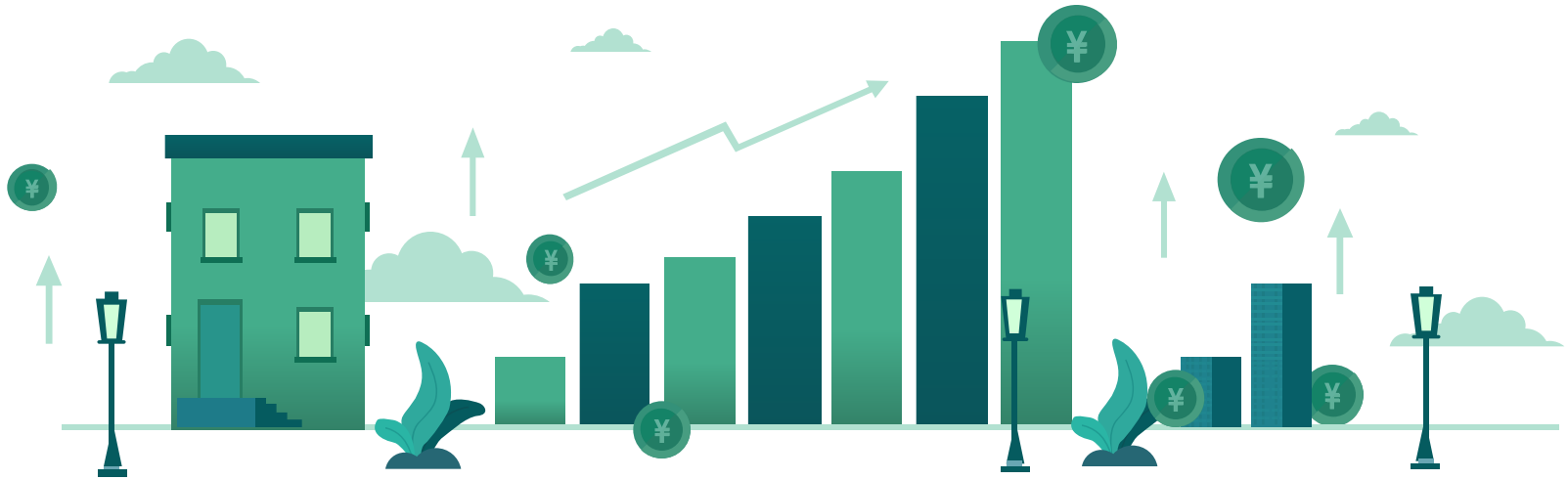


Kind	Note Summary	Occurrence Summary
PACKAGE_VULNERABILITY	CVE or vulnerability description and details including severity, versions	Affected packages/versions in a specific resource
BUILD_DETAILS	Builder version and signature	Details of this specific build including inputs and outputs
IMAGE_BASIS	Base Image for a container	An image that uses the base image, and layers included on top of base image
PACKAGE_MANAGER	Package Descriptions	Filesystem locations of where the package is installed in a specific resource
DEPLOYMENT_HISTORY	A resource that can be deployed	Details of each deployment of the resource
ATTESTATION	Anchor for attestations for this authority	An attestation on a specific component

Occurrences: An occurrence can be thought of as an instantiation of a note and describes how the note was found in a specific cloud resource or project (e.g., location, specific remediation steps, etc.), or what the results of a specific note were (e.g., the container images that resulted from a build).

Audit and govern your software supply chain with Grafeas



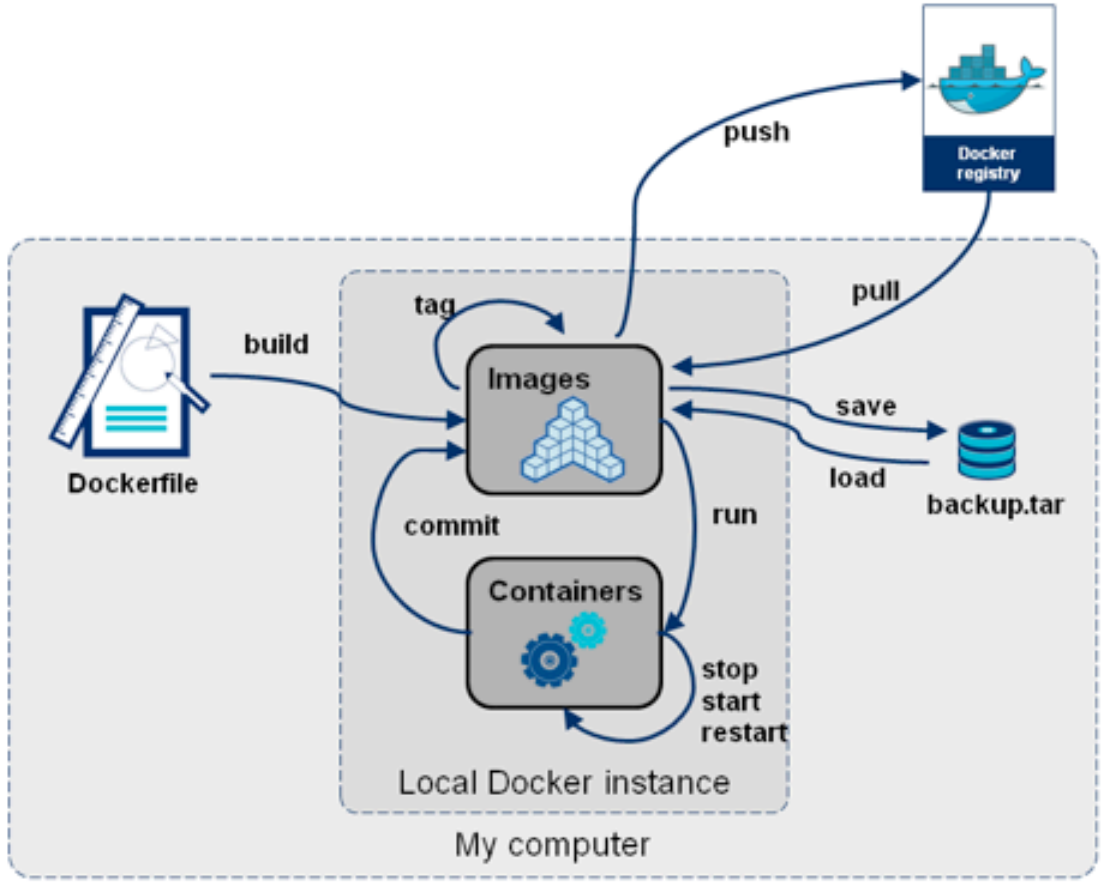


/04

容器和 Artifacts 的安全构建

在多租户场景下提供安全隔离的容器及 Artifacts 构建环境。

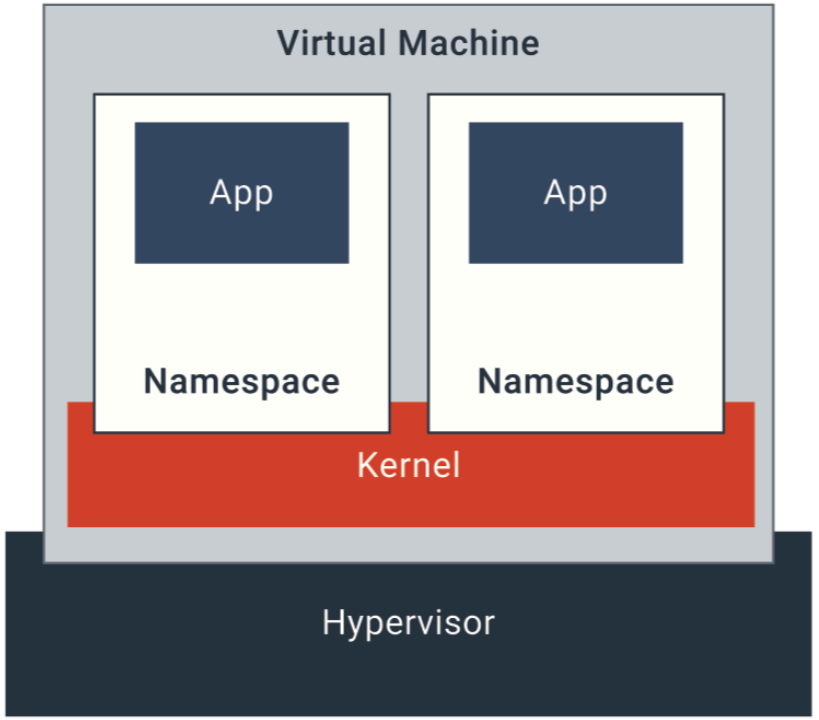
Docker 构建带来的安全隐患



Docker 构建的安全隐患主要是由 Docker Daemon 使用 root 权限执行引发的，所以一种解决方案是实现非 root 权限的构建能力。

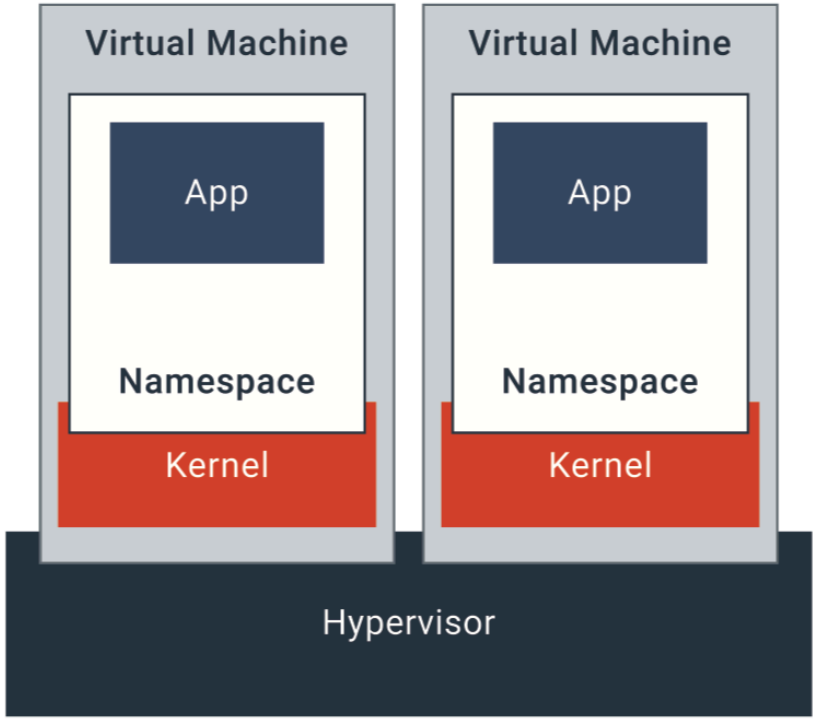
- Kaniko https://github.com/GoogleContainerTools/kaniko
- Buildah https://github.com/projectatomic/buildah

Hyper + Clear Linux = Kata Container



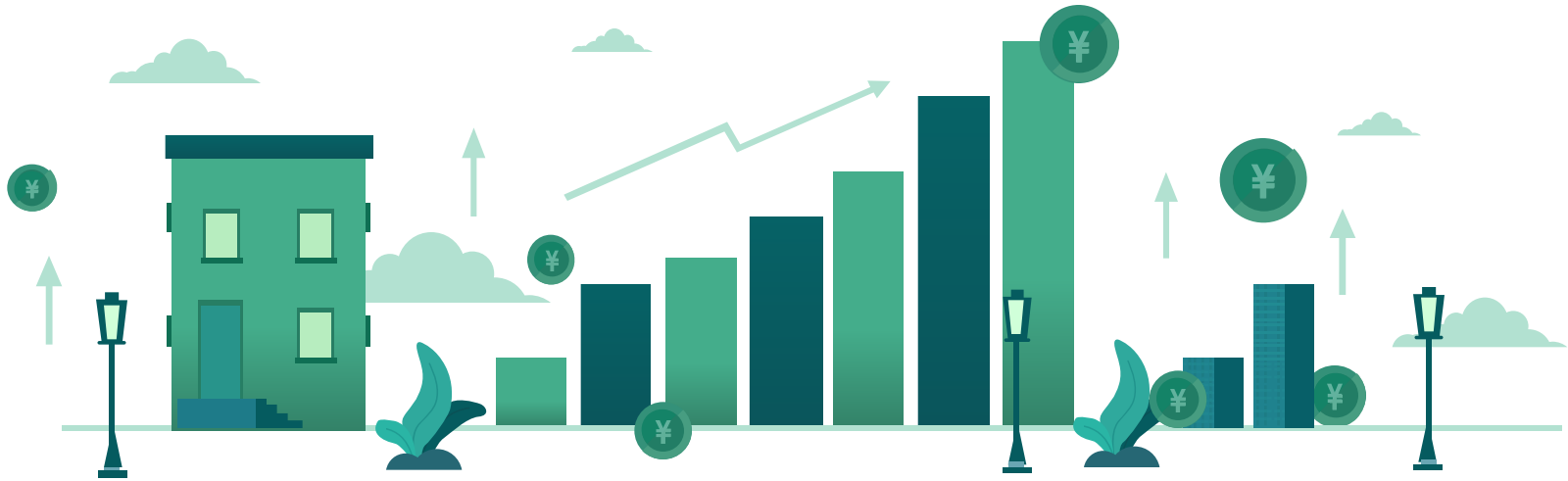
Containers in cloud today

(Shared kernel, isolation within namespace)



Kata Containers

(Each container/pod is hypervisor isolated, As secure as a VM, As fast as a container, Seamless integration with the container ecosystem and management layers)

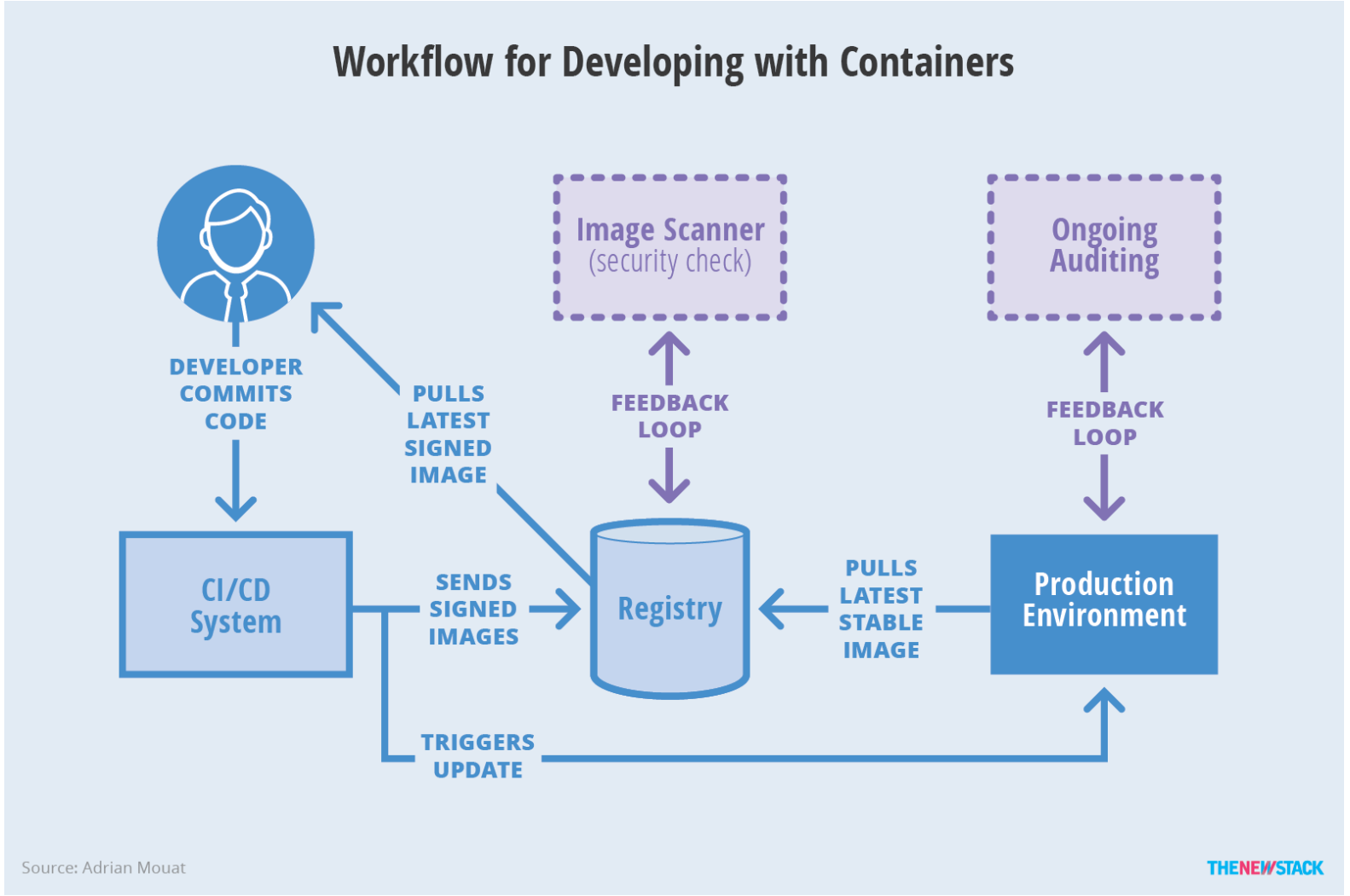


/05

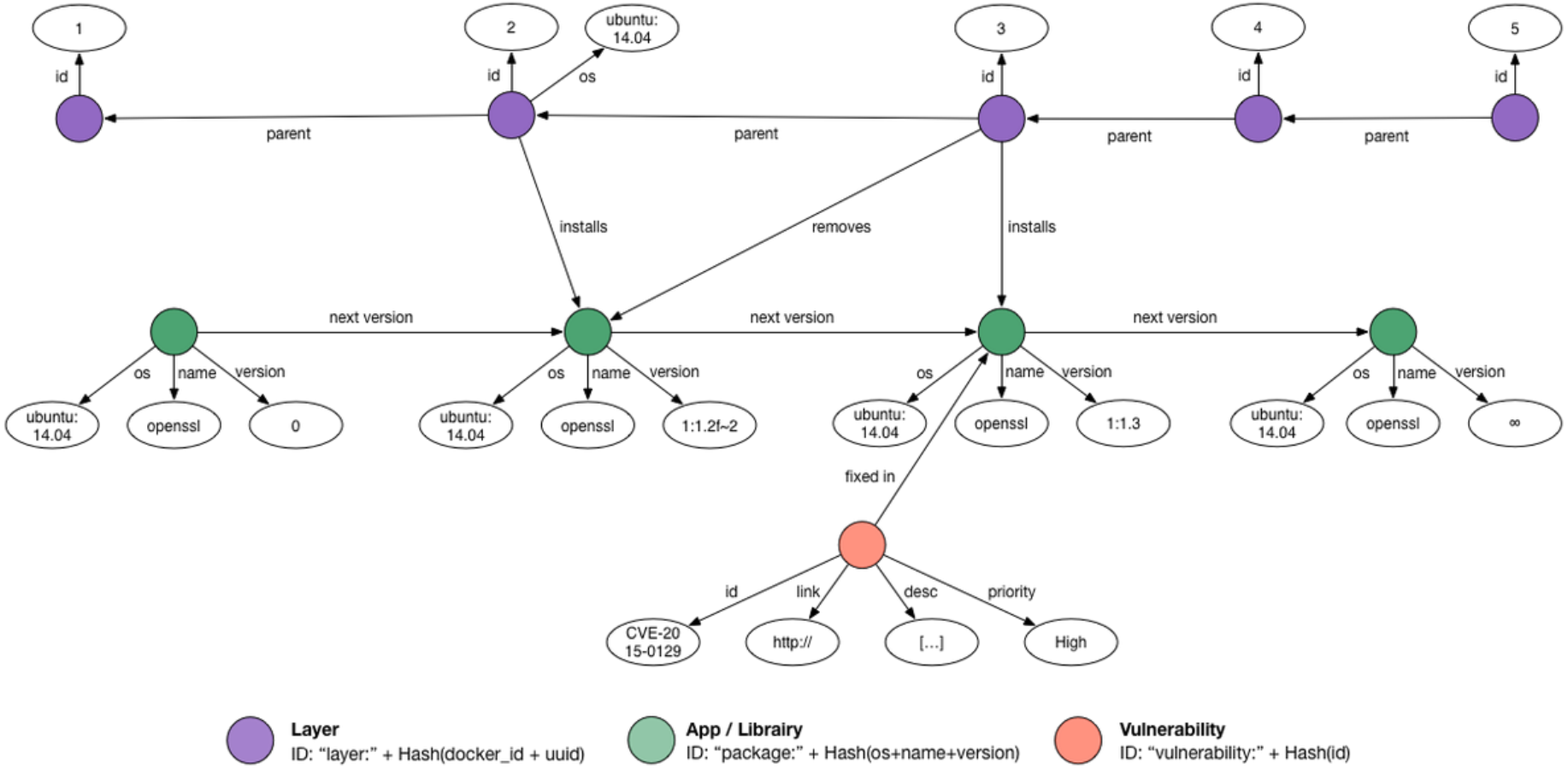
容器镜像扫描

对容器镜像进行静态扫描，第一时间发现系统的安全漏洞。

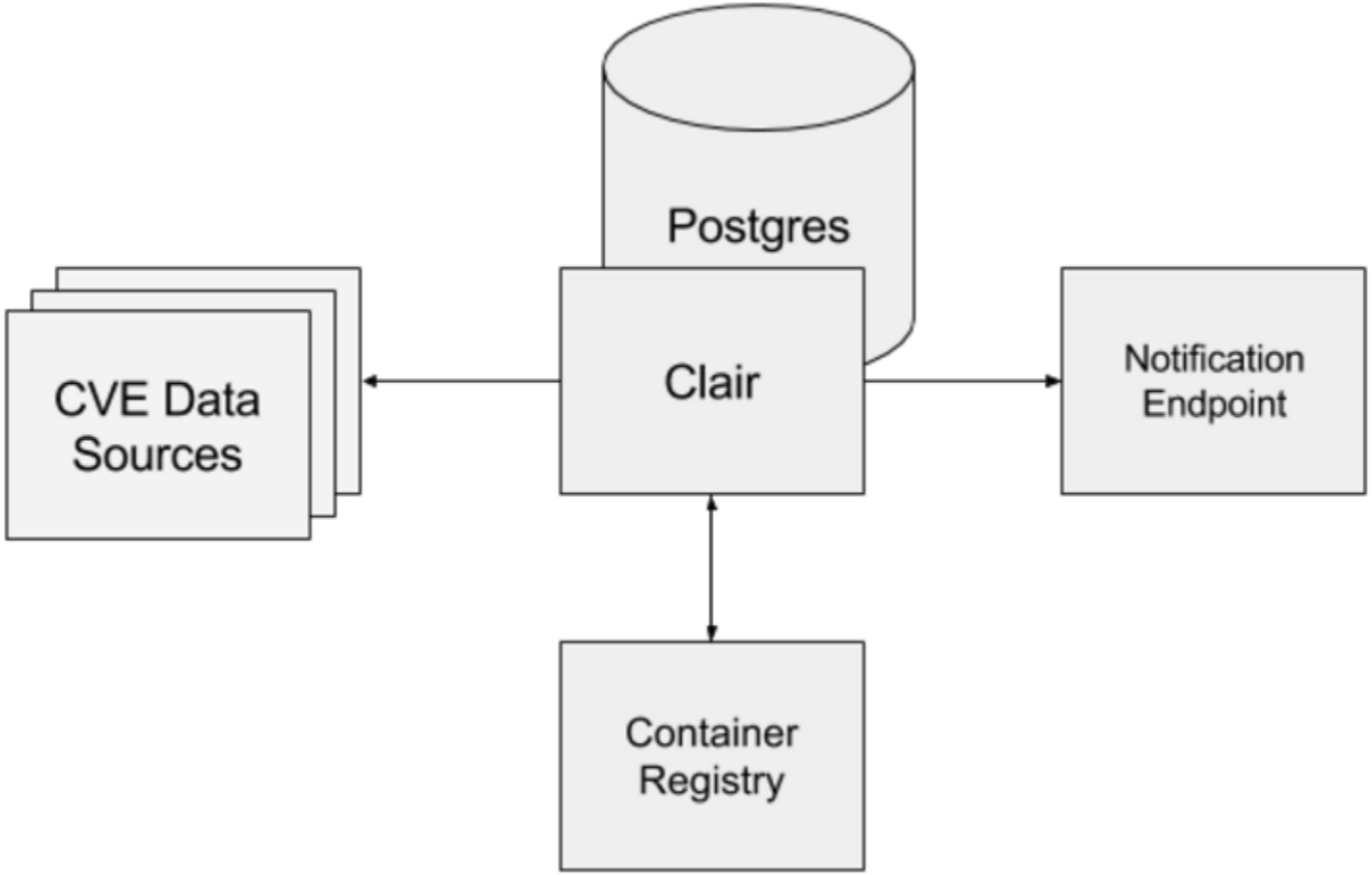
容器镜像扫描是 DevOps 中的标准环节



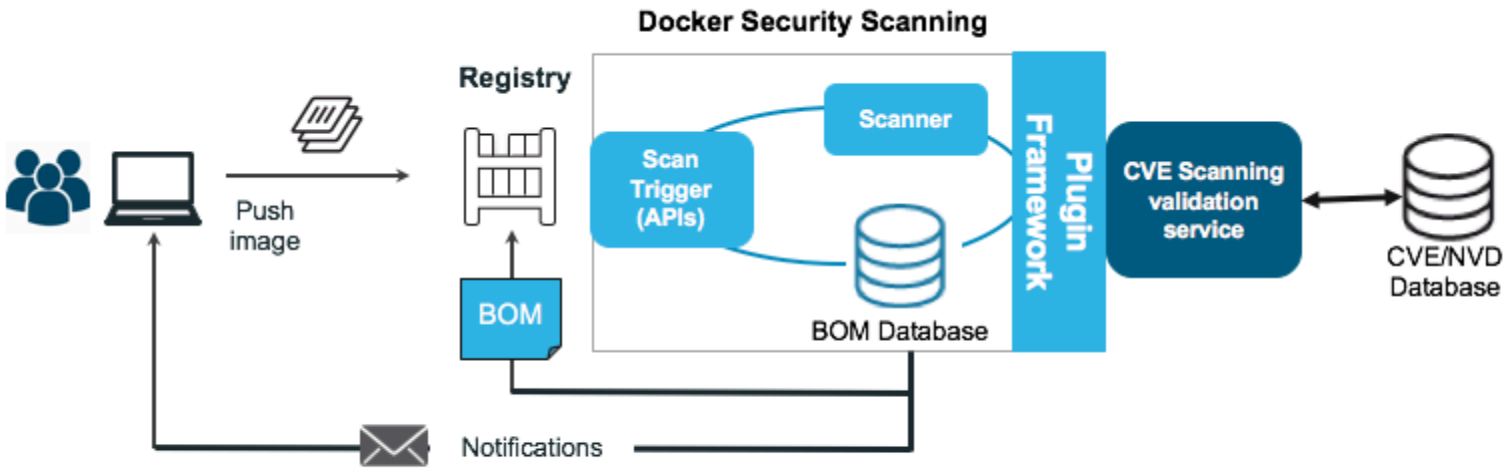
如何实现容器镜像静态扫描

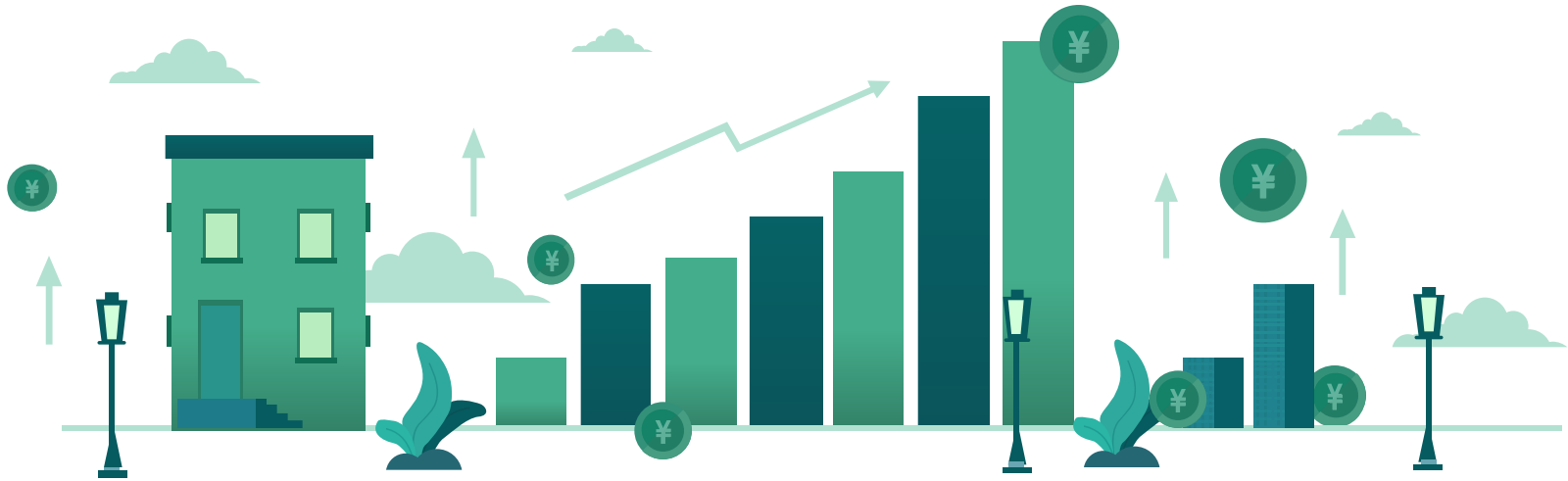


Tencent Hub 集成 CoreOS Clair 静态扫描能力



Docker 企业级解决方案 Nautilus



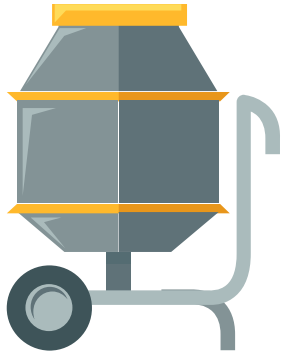


/06

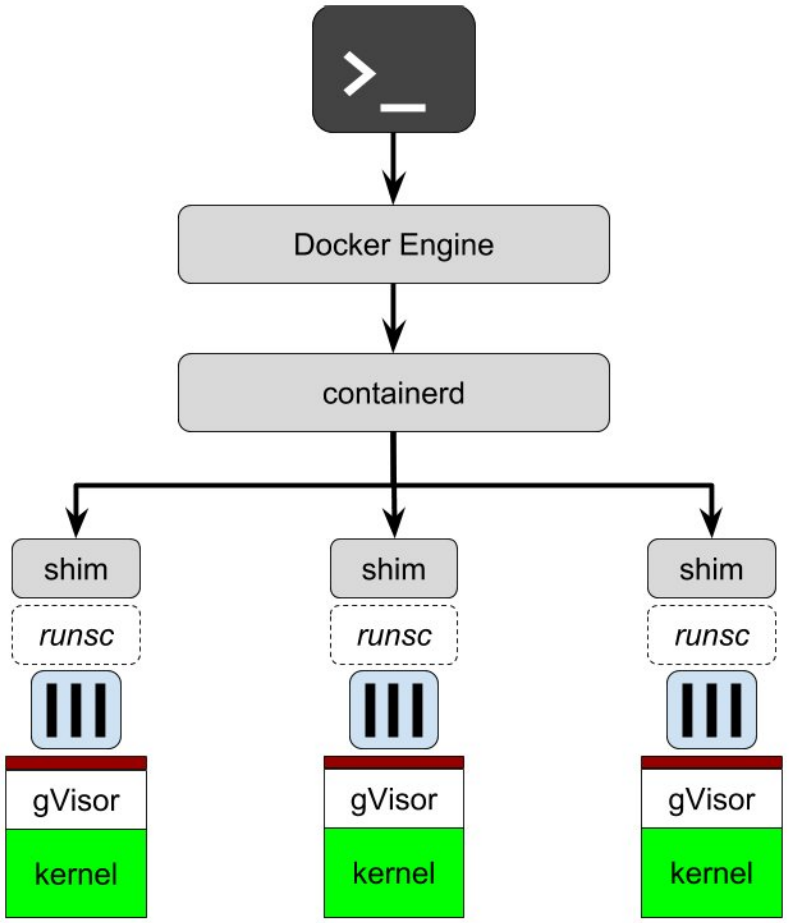
构建安全的运行环境

安全的运行环境是天然的屏障。

Google 的安全沙箱项目 - gVisor

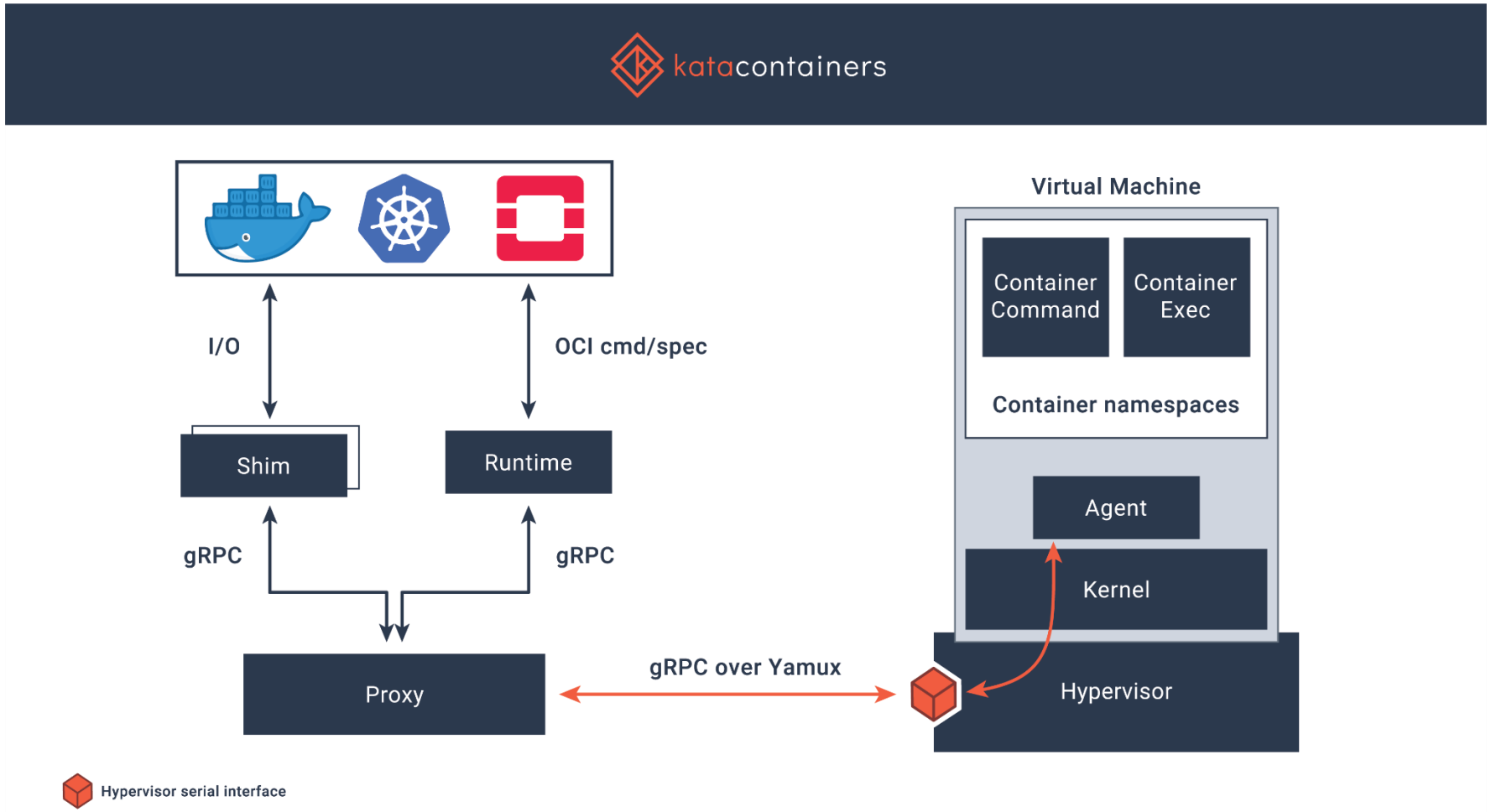


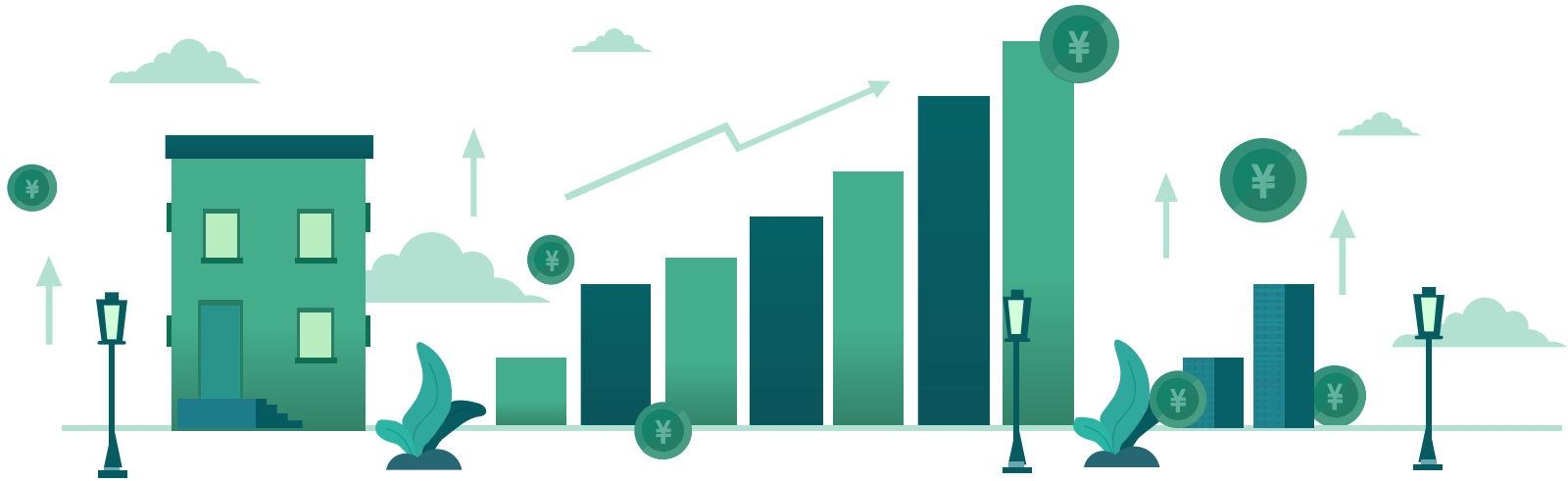
- 轻量级安全容器沙箱运行时
- 作为一个普通的非特权进程来运行的内核，它支持大多数Linux系统调用。
- 用Go编写，选择这种语言是由于它具有内存安全和类型安全的特性。
- 通过拦截应用程序的系统调用，并充当访客系统的内核，提供强大的隔离边界，一直在用户空间中运行。



Docker with gVisor Architecture

如何使用 Kata Container 做 Container 构建



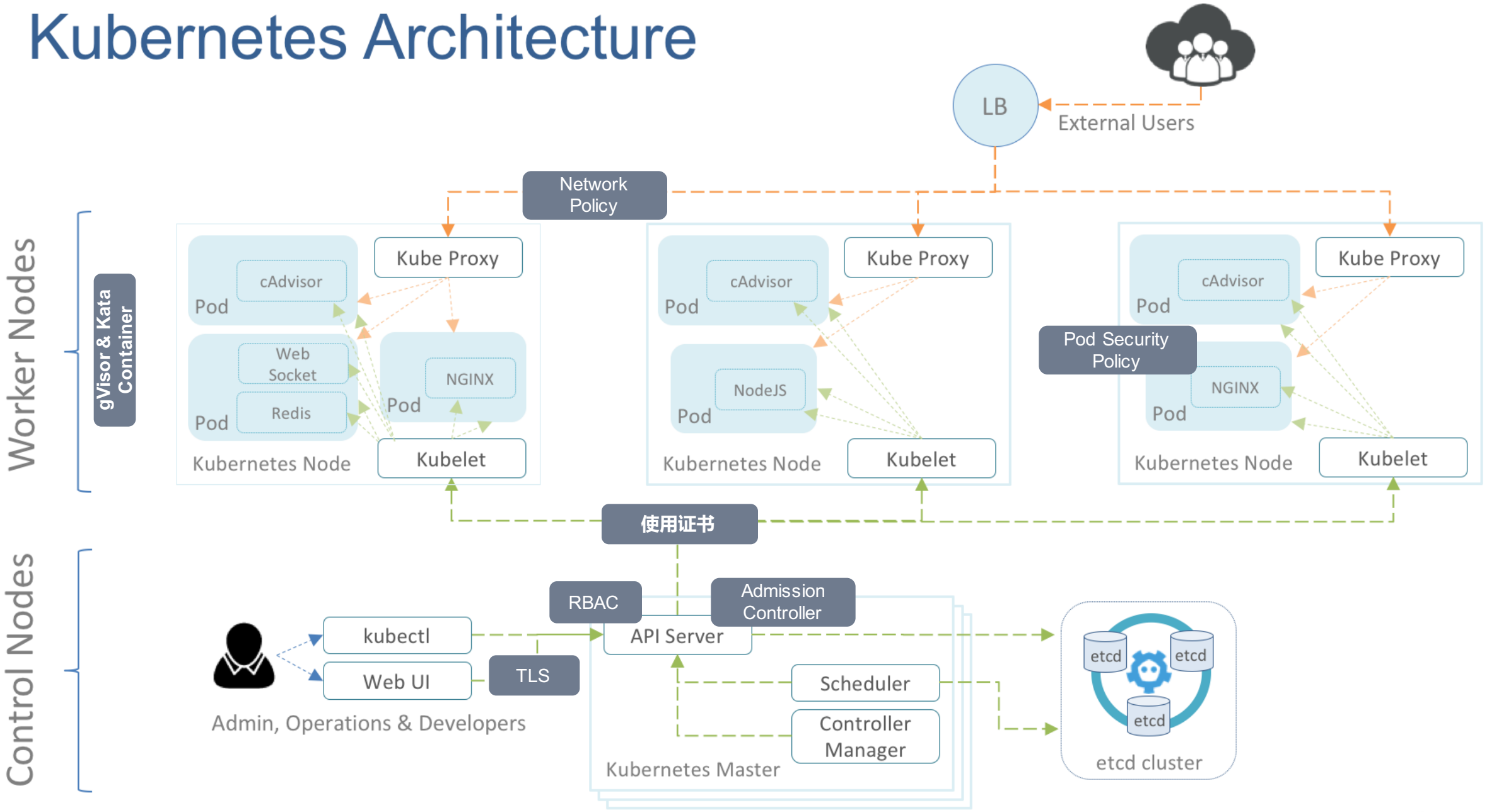


/07

Kubernetes 中的安全策略

基础设施中提供更多的安全策略补充。

Kubernetes Architecture



Source William Caban

Thanks

马全一 <maquanyi@tencent.com>
cloud.tencent.com