KYLINSOFT
麒麟软件

麒麟安全镜像构建工具KTIB 介绍

打造中国操作系统核心力量

kylinos.cn

索小聪 2023.11

前言

麒麟安全镜像构建工具KTIB 是麒麟内部孵化的一个关于容器镜像构建，镜像审计，镜像安全相关的一体化工具，将容器镜像相关的操作集成到统一的工具中，使开发者在使用过程中尽量减少认知负载的同时，提供最大化的镜像安全能力。

该工具也可集成到CI/CD流水线中，在构建容器镜像结束后就可提供审计报表，将安全和审计左移，可以将CI/CD流程缩短，避免推送到镜像仓库之后再进行扫描带来的滞后性。

目前开发进度约50%，后续希望托管到Cloudnative Sig 进行开源和持续孵化，吸收社区意见，将其打造的更方便，更易用。

目录

KYLINSOFT
麒麟软件

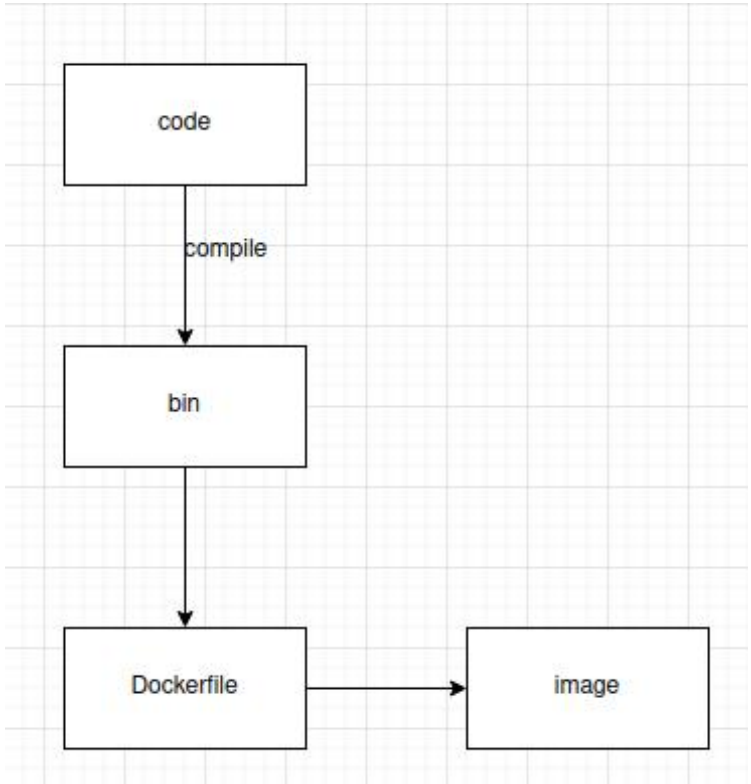
背景

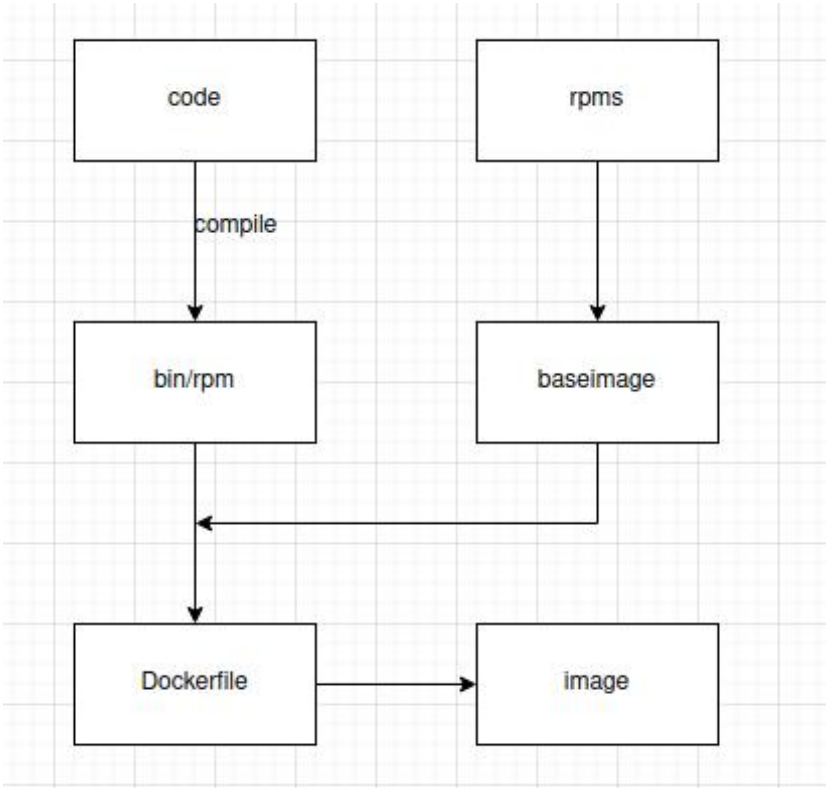
中国操作系统核心力量

kylinos.cn

诞生背景

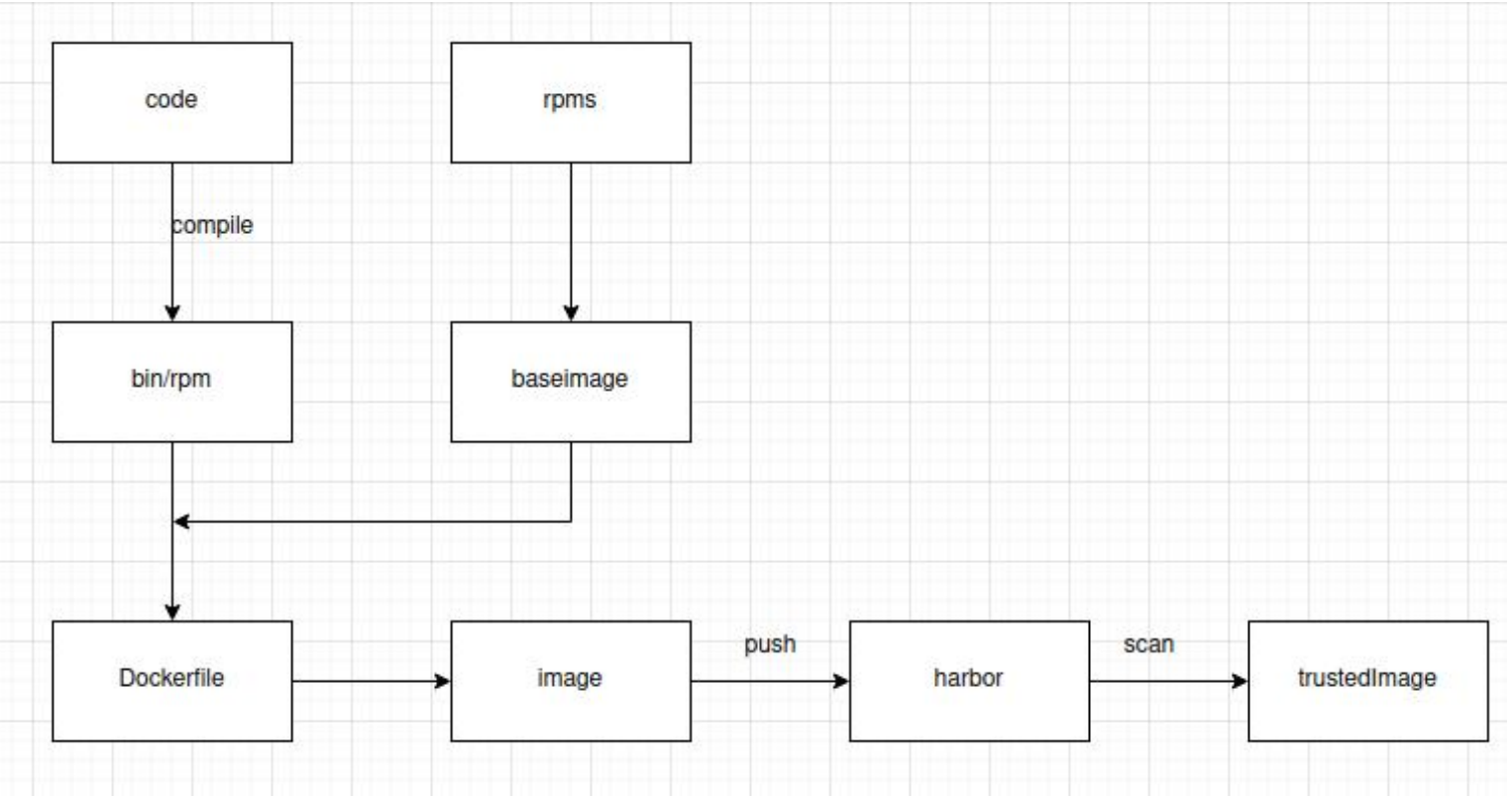
docker build镜像的流程:





诞生背景

加一点安全保障：docker build + harbor scan 构建可信镜像流程



诞生背景

问题：如何增加更多安全保障？

诞生背景

从以上镜像构建流程可以发现有以下问题:

1: 容器镜像的开发者有时候不具有能力去跟踪自己依赖的软件包生态是否有漏洞

2: 当前生态中现有的扫描工具能在镜像仓库中进行检测，但流程较长，在构建过程中开发者无法提前进行扫描

3: 对于Dockerfile的审计规则，对于开发者来讲了解也比较少，因此同样需要一个工具来进行检测和提示

4: 基于docker的镜像构建流程是依赖于容器引擎的，而在有一些轻量级engine的场景下如iSulad, containerd, crio，不具有构建能力，需要依赖额外的工具如buildah

5: 通过扫描的镜像，需要保障传输安全，确保镜像仓库的安全可靠。

结合以上问题, 麒麟提供了Kylin Trusted Image Builder（KTIB） 工具，针对开发者提供一整套完整的镜像安全可信构建流程。

KYLINSOFT
麒麟软件

技术特性

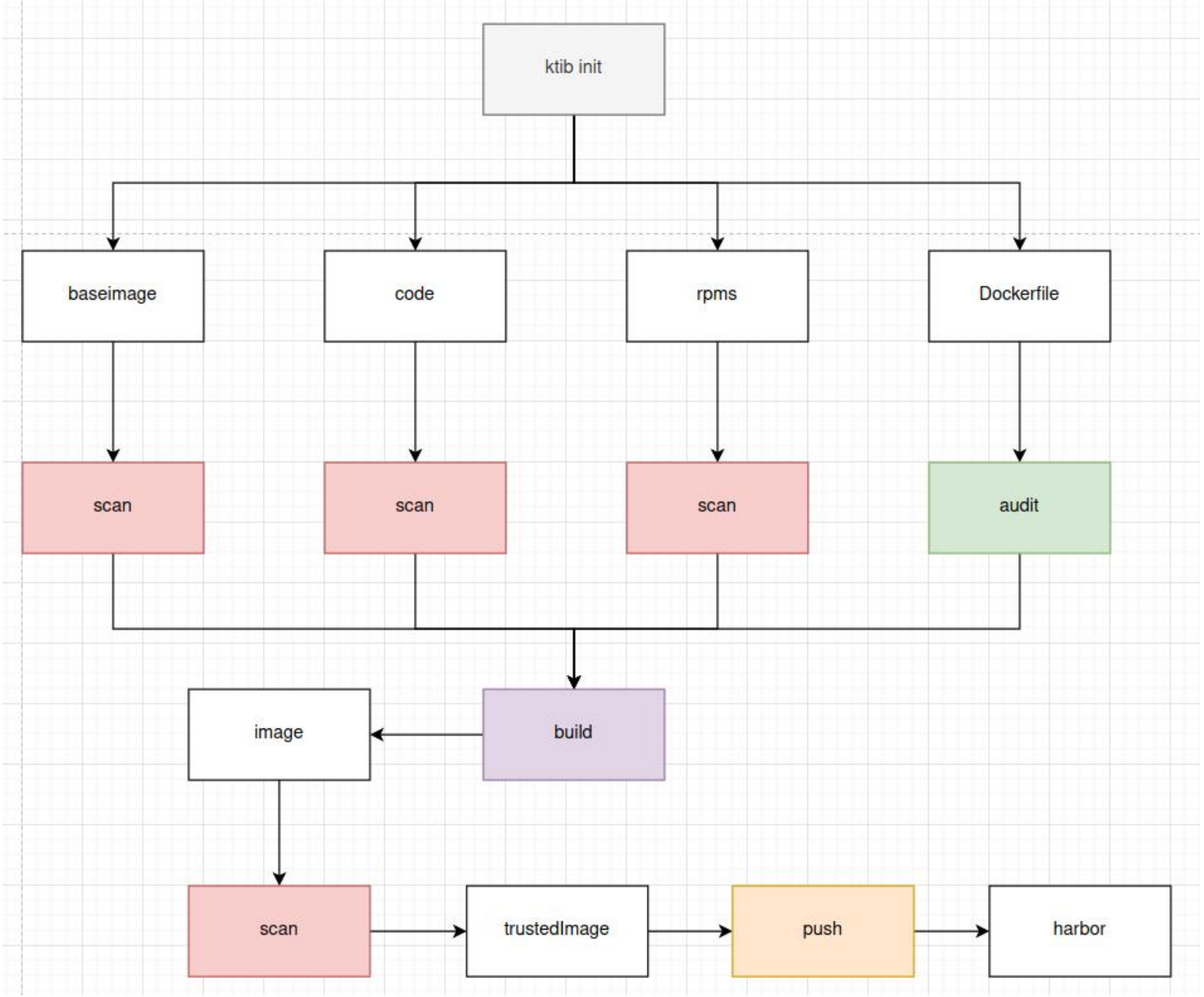
中国操作系统核心力量

kylinos.cn

技术特性

KTIB工作流是什么样子的:

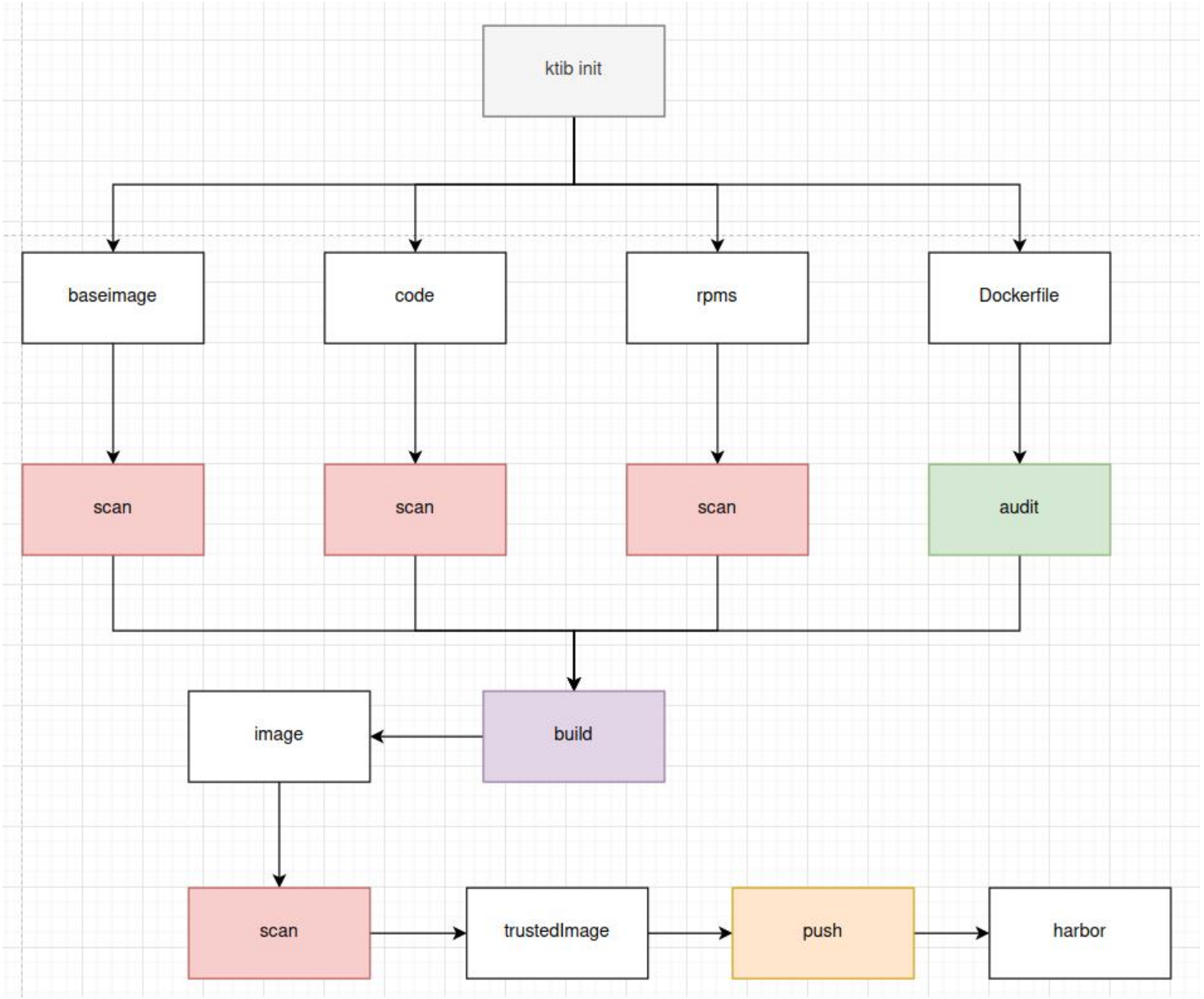
- 初始化标准项目结构
- 对baseimage, code, rpm分别进行扫描，扫描过程默认自动执行
- 对Dockerfile进行合规审查
- 构建镜像之后再次扫描
- 可信镜像标记
- 可信传输



技术特性

解决的问题:

- 1. 使用统一的工具进行构建和管理安全镜像
- 2. 标准化构建目录，使得所有项目遵循统一的规则，方便维护
- 3. 不依赖任何容器引擎
- 4. 增加了Dockerfile的合规审计, 且容易扩展
- 5. 增加了安全传输，使得镜像从本地到远程的传输安全



KYLINSOFT
麒麟软件

对比其他现有工具

中国操作系统核心力量

kylinos.cn

对比其他现有工具

构建工具

	buildah	buildx	ktib
支持单步构建			是
独立于容器引擎	是		是
支持dockerfile构建	是	是	是
支持镜像仓库操作		是	是
支持多种镜像格式	是	是	是
构建速度快		是	
漏洞扫描			是
安全合规审计			是
可信上传			是
跨平台构建		是	

对比其他现有工具

扫描工具

	clair	trivy	ktib
镜像扫描	是	是	是
源码扫描		是	是
rpm扫描			是
配置扫描		是	是
方便维护		是	是

对比其他现有工具

审计工具

	openSCAP	Anchore	docker-bench-security
CIS基准测试	是		是
可维护性		是	是
CVE漏洞		是	
自定义策略		是	

KYLINSOFT
麒麟软件

现状与展望

中国操作系统核心力量

kylinos.cn

现状与展望

1. 当前KTIB工具是在麒麟内部孵化开发，开发进度约50%，后续希望托管到Cloudnative Sig 进行后续的持续孵化和开发，以吸收来自社区的更多优秀人才的优秀想法，将其打造成openeuler社区面向开发者的更好工具。

2. 当前漏洞数据来源为麒麟内部源，后续考虑和其他开源数据进行对接，或者将数据托管到gitee平台。

3. 合规审计规则可进行插件化扩展，适配各个细分场景下的审计规则。

4. 与NestOS-Kubernetes-Deployer (NKD)对接，完善NestOS生态，打造容器构建安全和运行时安全闭环。

KYLINSOFT
麒麟软件

谢 谢