机密容器

提供端到端零信任的云原生数据服务

刘秉伟

英特尔软件与先进技术事业部 系统软件高级总监

机密容器

提供端到端零信任的云原生数据服务

机密容器

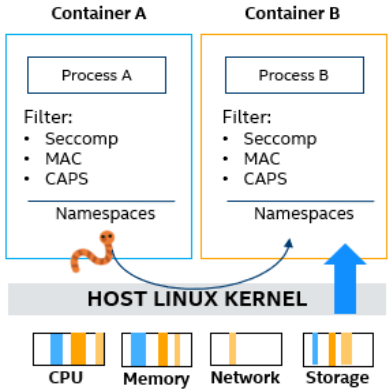
机密容器（Confidential Containers）

应用场景

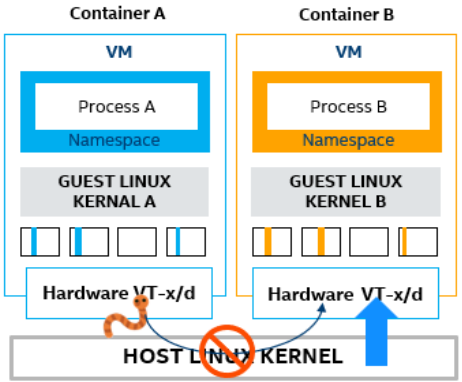
关键特性

容器运行时安全的演进

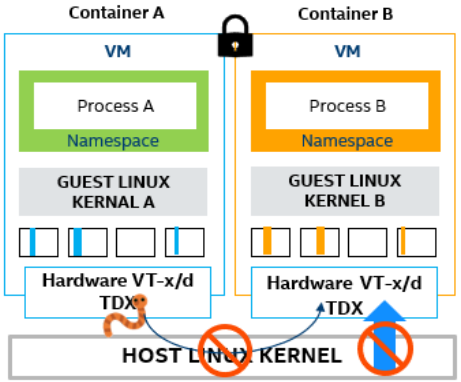
传统RUNC容器
共享内核



沙箱容器
虚拟机级别的故障隔离和安全隔离
保护宿主机/云厂商



机密容器
硬件TEE保护的客户机内存，保护客户代码和
数据不能被宿主机/云厂商窥探



机密容器（Confidential Containers）

机密计算

- 利用Hardware TEE保护应用/模型/数据
- 基于远程证明构建信任
- 把基础设施服务提供者排除在可信计算基（TCB）之外
- 提供安全上云的新范式

状态

- 广泛的业界支持
- 2022年3月成为CNCF沙箱项目
- 完整的安全特性
- 应用场景驱动

CONFIDENTIAL CONTAINERS

云原生

- 容器和K8S生态
- 聚焦应用
- 弹性
- 高密

设计原则

- 易用无需应用修改
- 容易部署和运维
- 非常容易和各种云服务集成
- Pod级TCB，IT运维人员天然不可信
- 端到端零信任覆盖运行时/存储/网络/secrets

发展路线图

https://github.com/confidential-containers

启动

2021.7

独立社区

V0

2021.11

- 镜像加解密
- Guest镜像下载
- 实现TDX/SEV远程证明
- 基本K8S集成

0.1.0-0.4.0

2022

- 加入CNCF
- 轻量级TD-SHIM
- 镜像签名
- CI/CD
- Operator
- 可信临时存储
- 可度量启动
- 流式下载

0.5.0-0.7.0

2023.7

- 通用KBS
- 通用 AS
- Enclave-CC
- Intel® Trust Authority 客户端
- Peer Pods

0.8

2023.10

- Confidential Data Hub
- Sealed Secrets
- 密钥管理服务集成
- 可信持久存储
- 运行时远程证明
- 镜像共享
- OPA策略

下一步

2024

- 可信IO
- GPU
- CNCF Incubation

机密容器

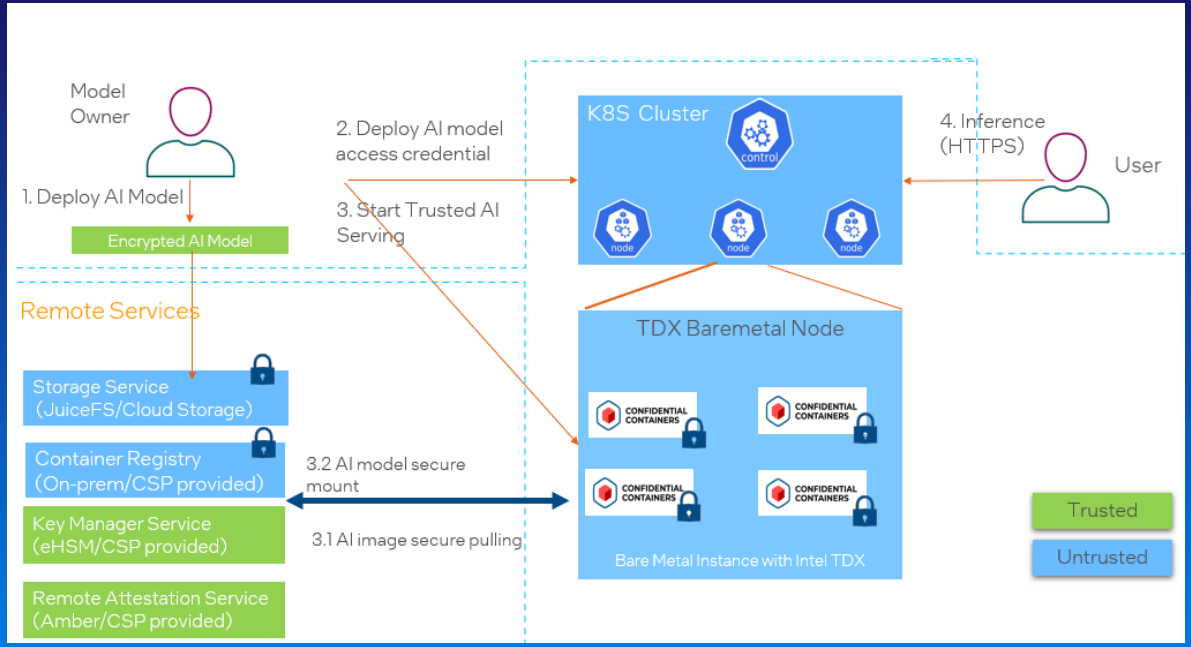
机密容器（Confidential Containers）

应用场景

关键特性

使用TDX机密容器构建可信AI应用

- 模型/数据是加密保护的
- 解密密钥以Sealed Secrets部署
- 模型/数据和应用分离，置于持久存储服务
- 应用加密
- Intel® AMX加持的深度学习加速



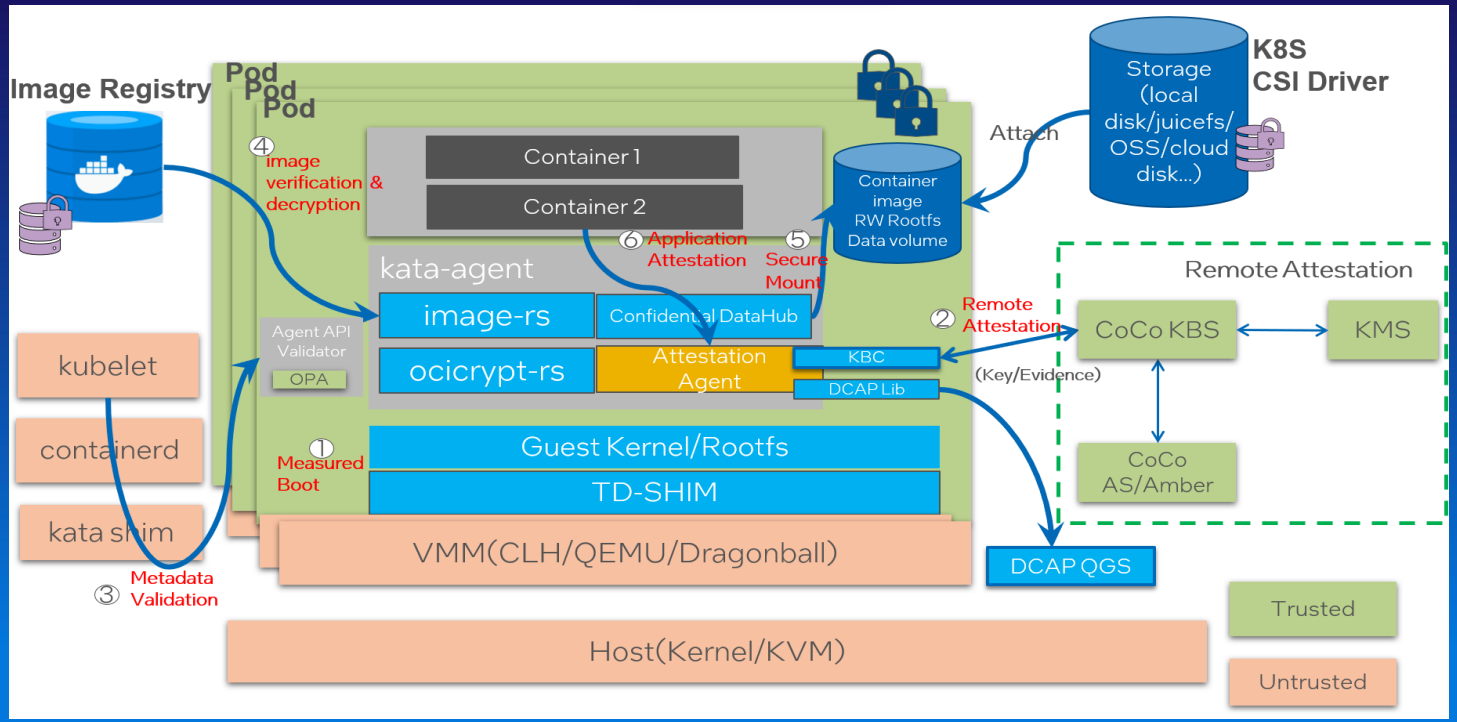
机密容器

机密容器（Confidential Containers）

应用场景

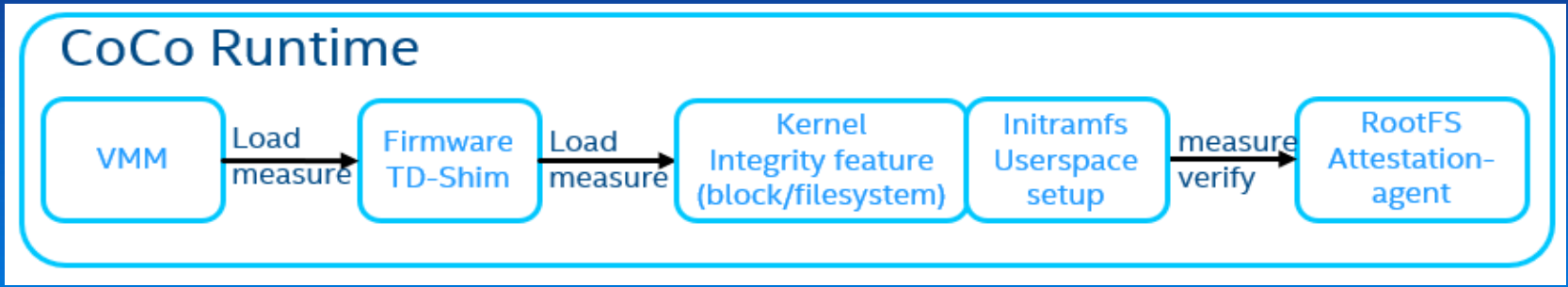
关键特性

TDX机密容器安全特性 – 零信任， 端到端



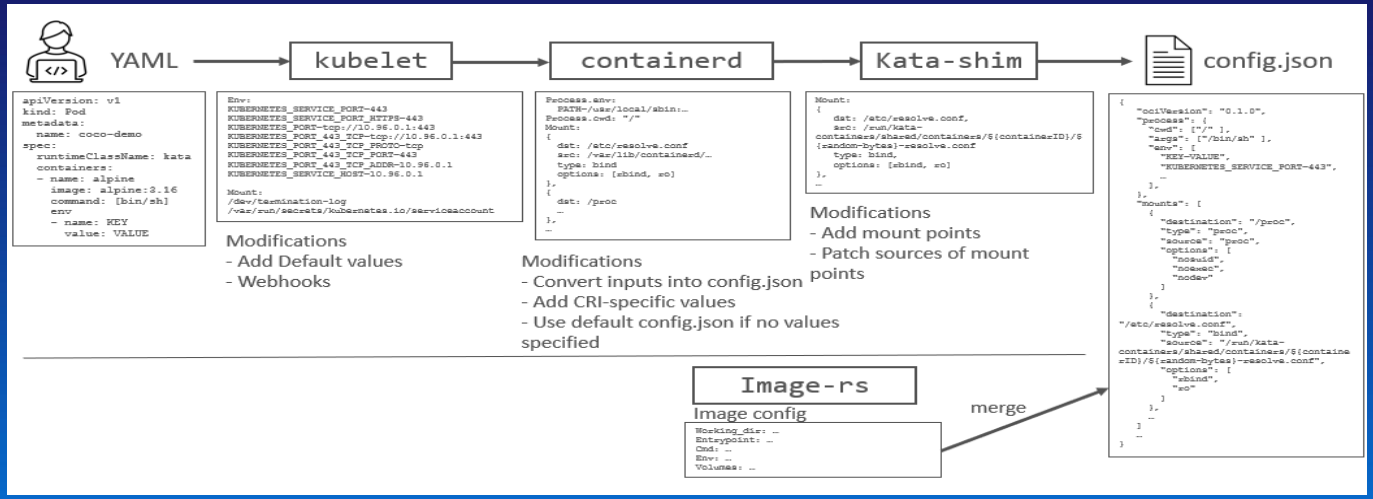
容器运行时环境完整性保证

- 确保App容器运行在可信运行时环境
- 可度量的guest rootfs
  - 利用dm-verity提供根文件系统的完整性
  - 对启动和运行时性能影响小
  - 基于远程证明



容器元数据验证

- 确保App容器以期待的方式拉起
  - 环境变量
  - mount points
  - OCI API
  - …
- 基于远程证明
- 基于OPA policy



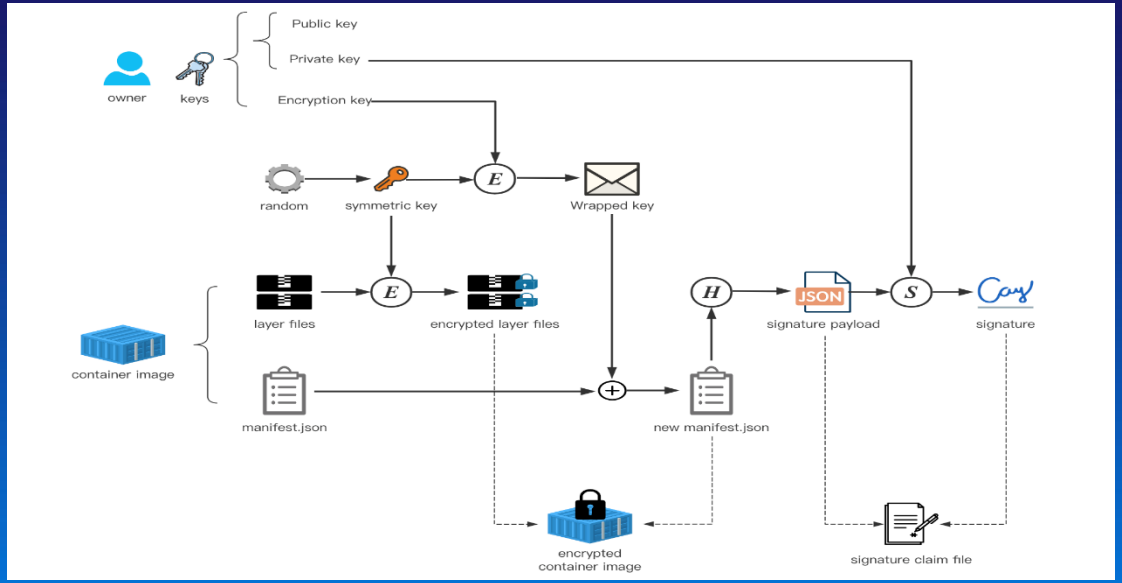
容器镜像的完整性保证

- 确保容器镜像在拉起的时候没有被修改或者替换
- 通过镜像签名机制来实现
  - 校验密钥从Key Broker Service获得
  - 校验policy从Key Broker Service获得
  - 支持多种校验方式： CoSign/sigstore, GPG key

```
{
    "default": [{"type": "reject"}],
    "transports": {
        "docker": {
            "docker.io/my_private_registry": [
                {
                    "type": "signedBy",
                    "keyType": "GPGKeys",
                    "keyData": "<public Key>",
                }
            ],
```

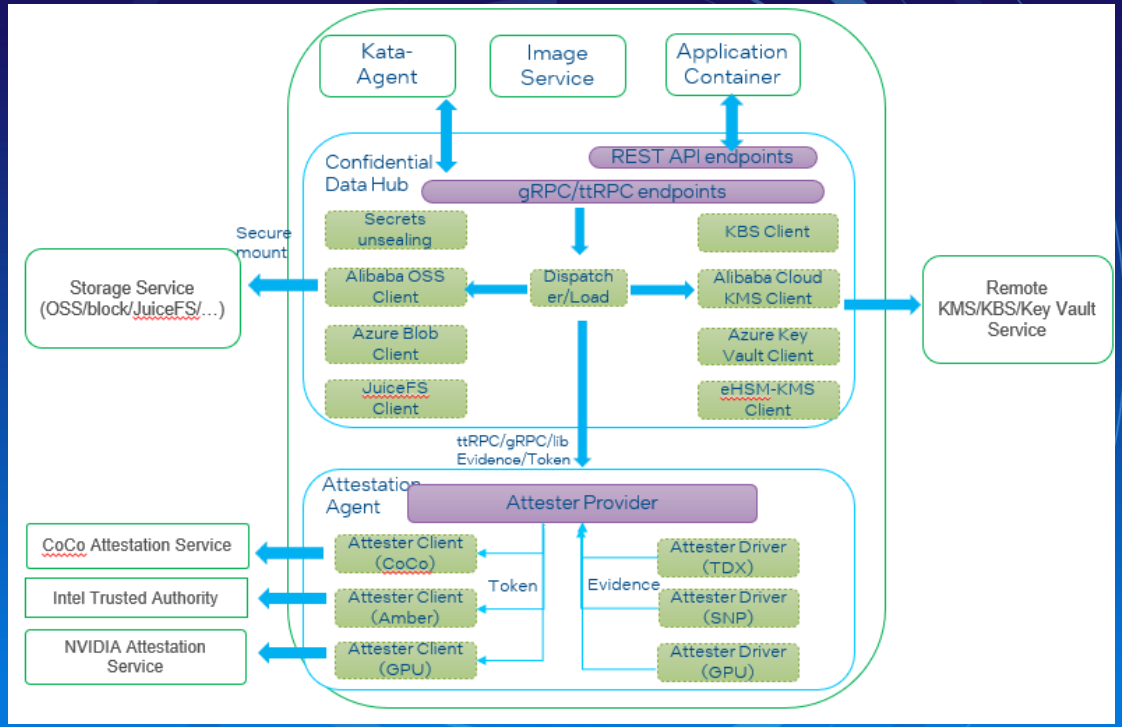
容器的机密性保证

- 容器在运行时对host不可见
- 容器镜像在仓库里是加密的
- 容器镜像在硬件TEE里下载
- 容器镜像解密后拉起
  - 兼容OCI image和distribution
  - 按层加密，并且支持可选层加密
  - 解密密钥在通过远程证明验证后发放



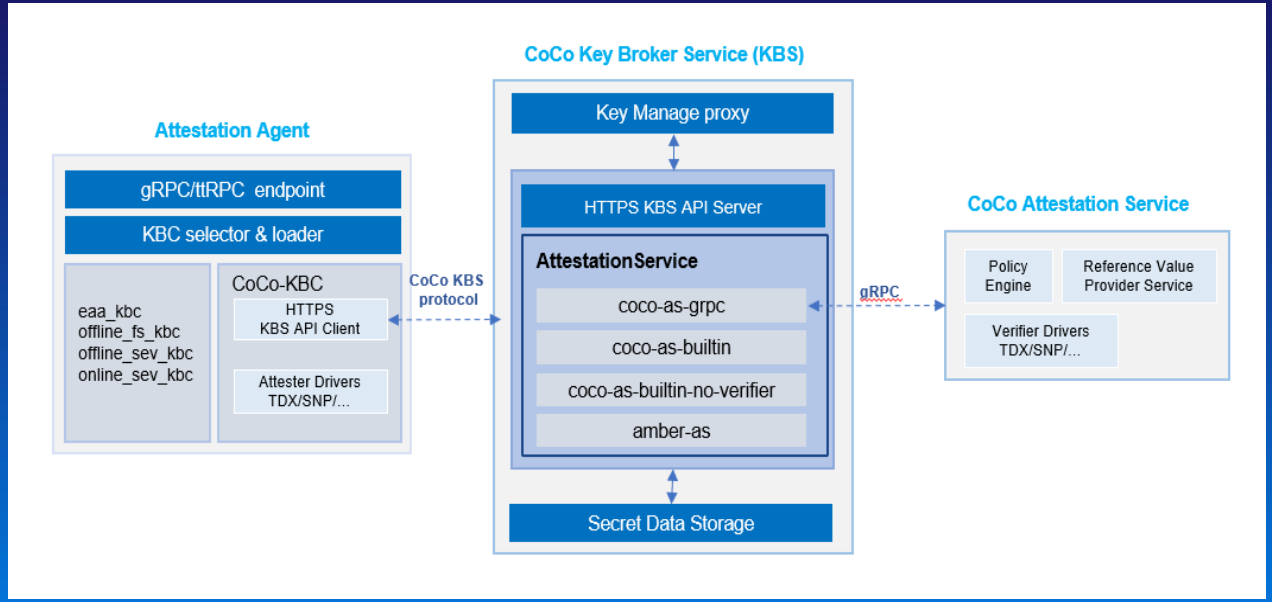
机密数据Hub（Confidential Data Hub)

- 支持在TEE guest 访问 KMS、 KBS、 Key Vault Service
- 支持不同的认证协议以获得机密数据访问授权
- 支持K8S sealed secrets 用户无感知解密
- 支持安全挂载存储， 用户无感知的加密数据的解密
- 模块化设计，支持多个云厂商的密钥管理、存储服务
- API既可以被系统服务访问，也可以被容器应用访问



CoCo远程证明架构

- 完整的远程证明框架，包括
  - Attestation Agent
  - Key Broker Service
  - Attestation Service
  - Plugin机制对接多个密钥管理服务
  - Plugin机制对接第三方远程证明服务
- 不仅仅是HWTEE的证明
  - 验证完整的guest代码软件栈
  - 验证不可信的输入
  - 从远端服务获取证书和密钥
  - CoCo安全机制的根本保障



Thanks