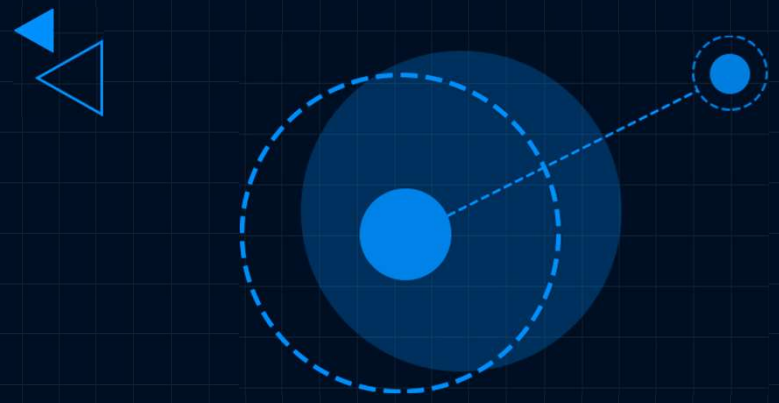
Inclavare Containers-业界首个面向机密计算场景的开源容器运行时

郝世荣
阿里云操作系统团队安全工程师



目录

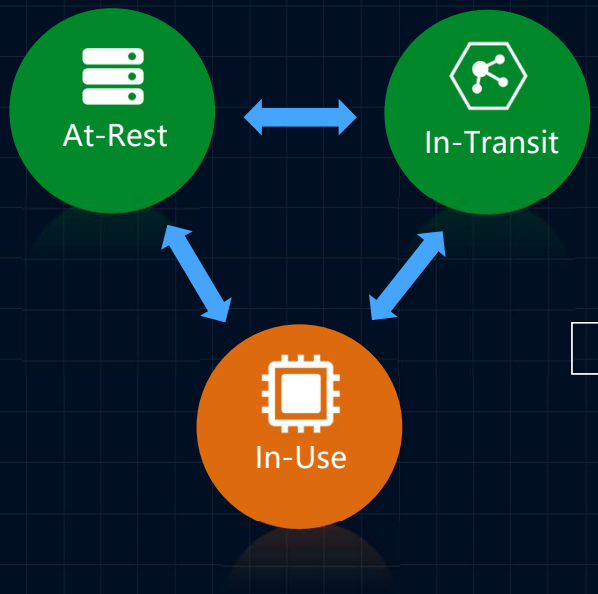
01 什么是机密计算

02 机密计算的痛点

03 Inclavare Containers

04 总结与展望

什么是机密计算?



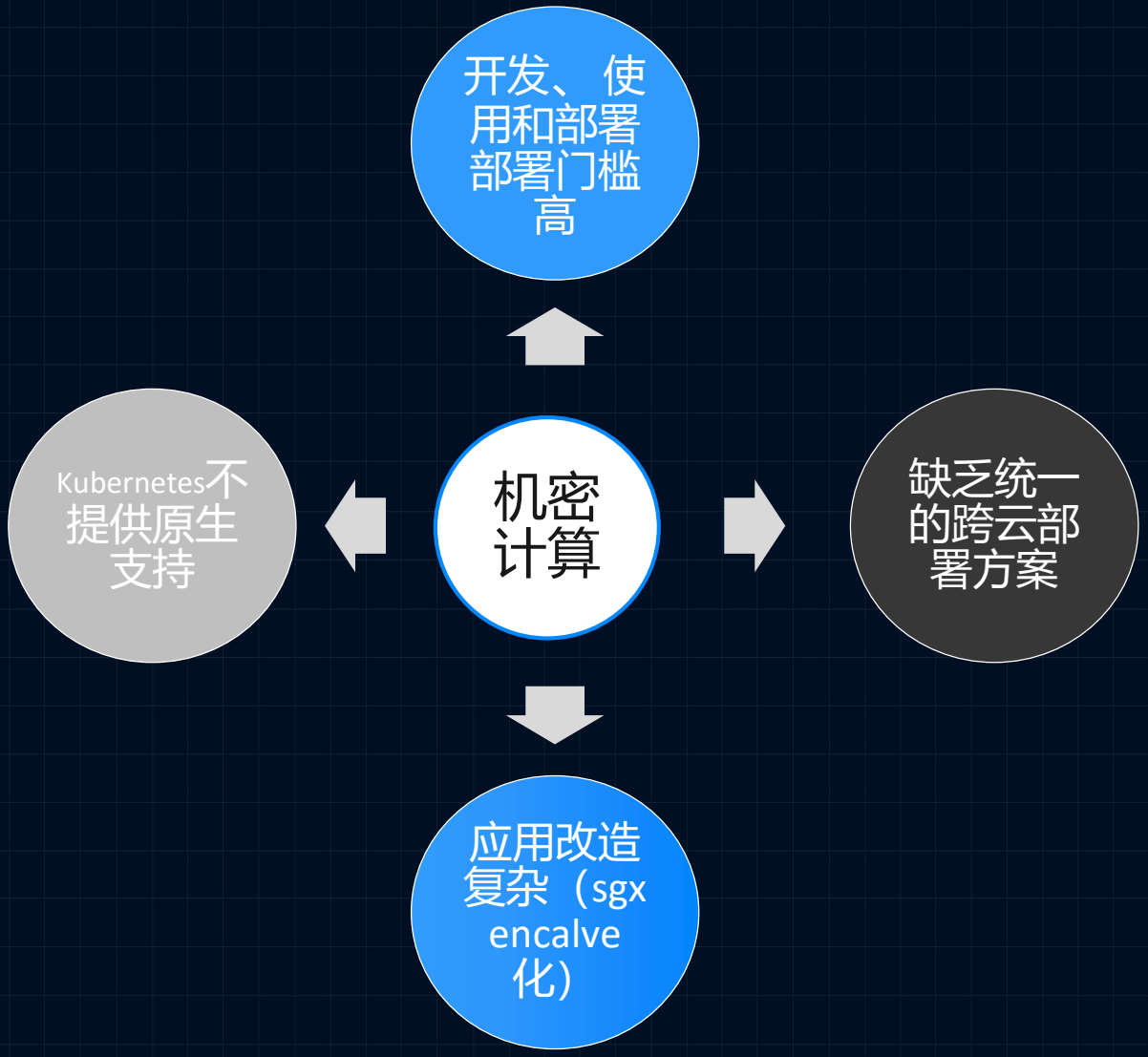
- 存储中的数据
  - 数据加密
- 传输中的数据
  - 加密协议（HTTPS，TLS等）
- 使用中的数据
  - 机密计算（HW-TEE）
    - 1. 保护 In-Use 数据的机密性；
    - 2. 保护 In-Use 数据的完整性；

“Confidential Computing protects data in use by performing computation in a Trusted Execution Environment.”

机密计算联盟 (CCC)

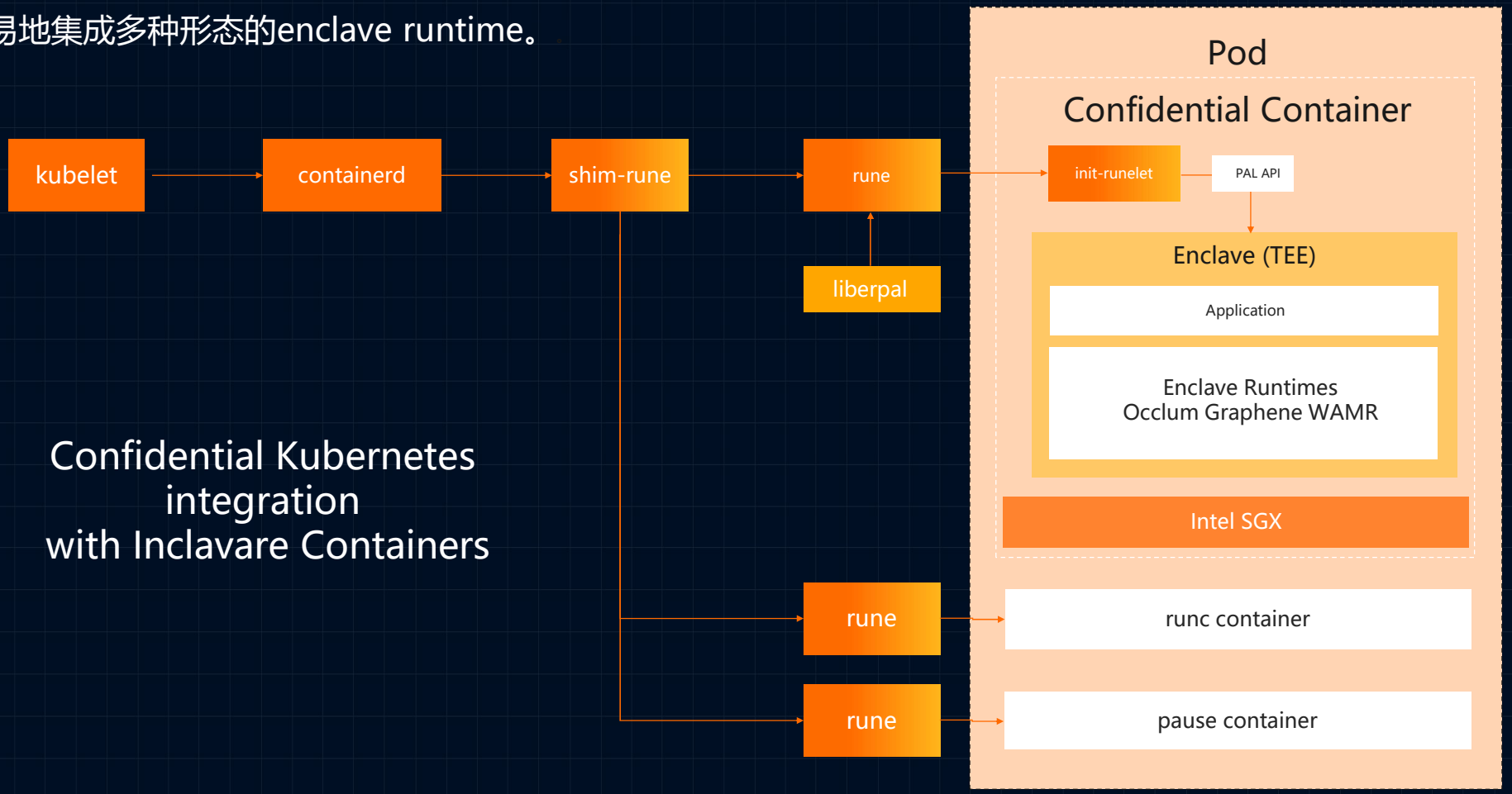
CONFIDENTIAL COMPUTING CONSORTIUM

机密计算的痛点


开发、使用和部署部署门槛高
Kubernetes不提供原生支持
机密计算
缺乏统一的跨云部署方案
应用改造复杂（sgx encalve化）

业界首个机密容器运行时——Inclavare Containers

- 一种在硬件强制实施的TEE中运行enclave runtime和可信应用的新型容器运行时。
- 将机密计算应用到云原生生态中。
- 可以很容易地集成多种形态的enclave runtime。



Inclavare Containers 设计理念

设计哲学

紧密围绕云原生生态，与已有生态中的组件配合共同支持机密计算。

目标

为业界和开源社区提供面向云原生场景的机密计算容器技术、机密计算集群技术和安全架构。

价值

抹平机密计算的高使用门槛，为用户提供与普通容器一致的使用体感。

基于处理器提供的多种硬件安全技术，为用户的工作负载提供多种不同的Enclave形态，在安全和成本之间提供更多的选择和灵活性。

立足点

保持开放；中立化运营。

保持开源视角、阿里的业务视角以及外部合作的视角。

版本发布历史

项目开源
- 发布0.1.0
- 支持enclave runtime Occlum
- 基于SGX 1硬件

2020.5

发布 0.2.0 版本
- 开源 shim and runectl (改名为sgx-tools)
- 从host侧加载pal
- 更新 PAL API 为 v2

2020.6

发布 0.3.0 版本
- 支持创建机密计算K8s集群
- 适配v33 SGX in-tree 驱动
- 提供PM/DEB 安装包

2020.7

发布 0.4.1 版本
- Enclave-TLS PoC
- Enclave pooling manager
- 提供Dragonwell 11 (LTS for OpenJDK 11) 参考镜像
- Skeleton enclave runtime

2020.9

发布 0.5.2 版本
- 支持 bundle cache
- 集成 github CI/CD actions
- 支持WARM enclave runtime

2020.12

发布 0.6.1 版本
- 实现Enclave Attestation Architecture （EAA）
- 支持bundle cache level 2
- 修复若干CVE漏洞

2021.5

发布 0.6.3 版本
- 实现RATS-TLS, Verdictd, Verdict, and RBI
- 支持bundle cache level 2
- Rune rebase 到runc v1.0.1

2021.8

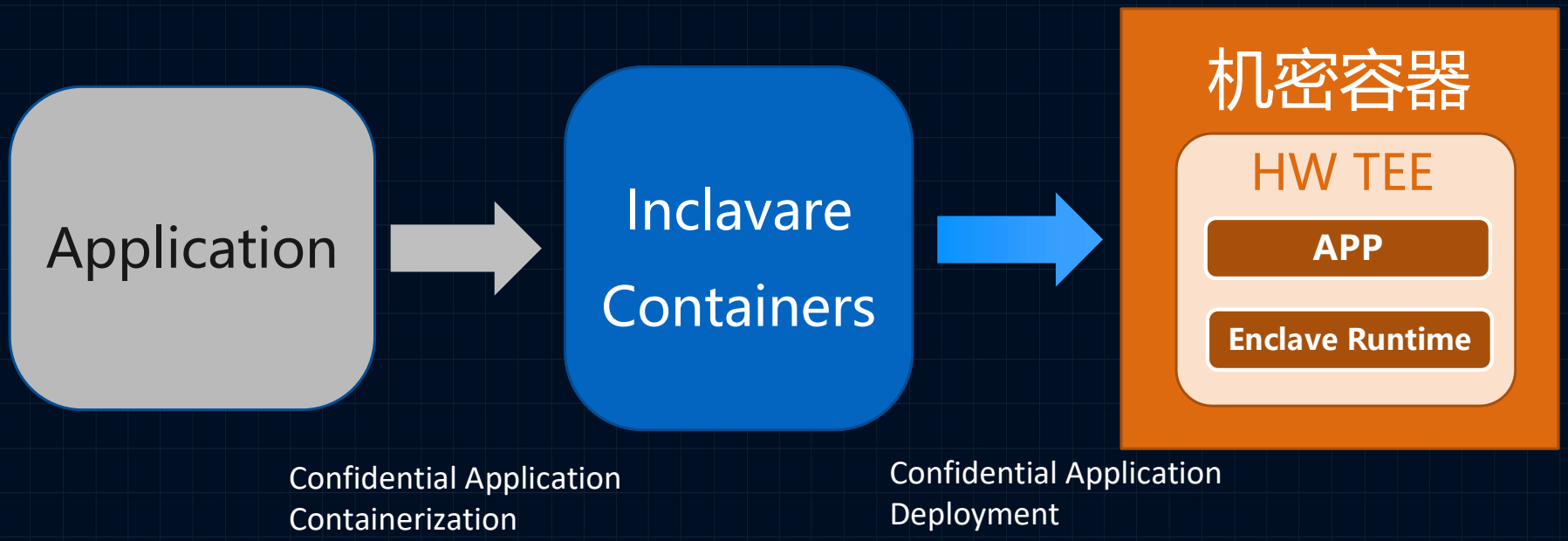
由于空间有限，只列出了部分版本发布情况，完整版本信息请参考链接：https://github.com/alibaba/inclavare-containers/releases

Inclavare Containers 开源项目当前状态

- Inclavare Containers 开源项目成为 CNCF 官方沙箱项目。
- 为阿里云 ACK-TEE 产品提供了使用机密容器的最佳实践。
- rune作为兼容OCI Runtime规范的机密容器引擎已写入 OCI Runtime 实现列表中。
- Inclavare Containers 成为龙蜥社区云原生机密计算 SIG 的初创项目。
- 具备通过 Kubernetes 和 Docker 运行机密容器。
- 提供了针对云场景的通用且跨平台的远程证明架构 EAA（Enclave Attestation Architecture）。
- 实现了基于 Intel SGX 技术的机密容器。
- 支持 Occlum，Graphene，以及 WebAssembly Micro Runtime。
- 面向社区发布了 0.1.0 到 0.6.3 的 11 个binary release版本。

提供了基于Golang、Java开发的web服

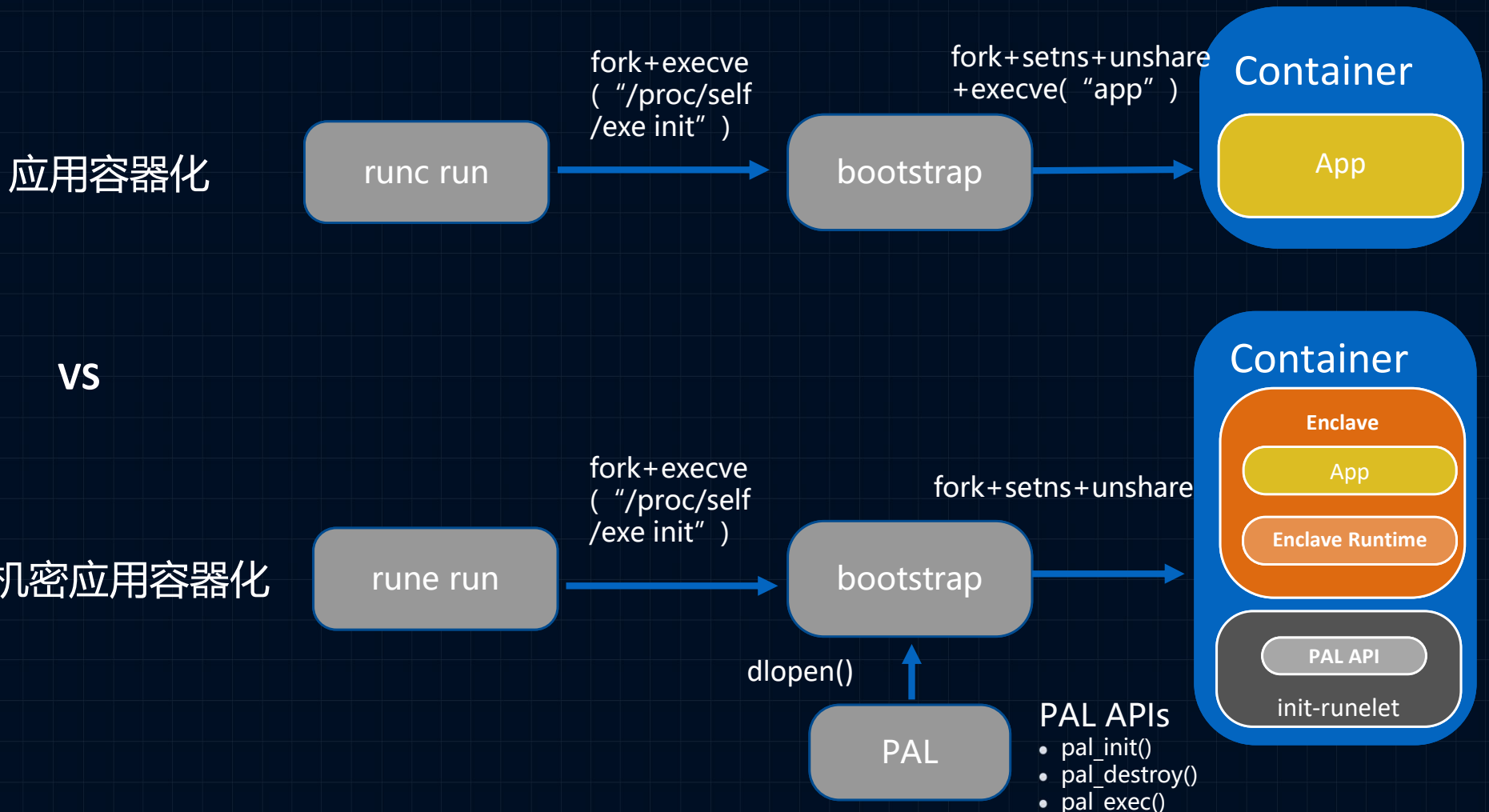
Inclavare Containers是如何工作的?



机密应用程序在不知道基于硬件的 TEE 的情况下被透明地容器化。

- 轻松将机密应用程序带入云原生。
- 在基于硬件的 TEE 中运行修改/未修改的应用程序（取决于 enclave runtime）。
- 为应用程序的数据和代码提供机密性、完整性和可证明性。

rune VS runc


应用容器化
runc run
fork+execve
(“/proc/self
/exe init”)
bootstrap
fork+setns+unshare
+execve(“app”)
Container
App
VS
机密应用容器化
rune run
fork+execve
(“/proc/self
/exe init”)
bootstrap
fork+setns+unshare
Container
Enclave
App
Enclave Runtime
PAL API
init-runelet
dlopen()
PAL
PAL APIs
pal_init()
pal_destroy()
pal_exec()
pal_kill()
pal_attest()
...

灵活的部署方式

```
{
   "runtimes": {
      "rune": {
         “path”: “/usr/local/bin/rune”,
          "runtimeArgs": []
       }
   }
}
```

Dockerd集成

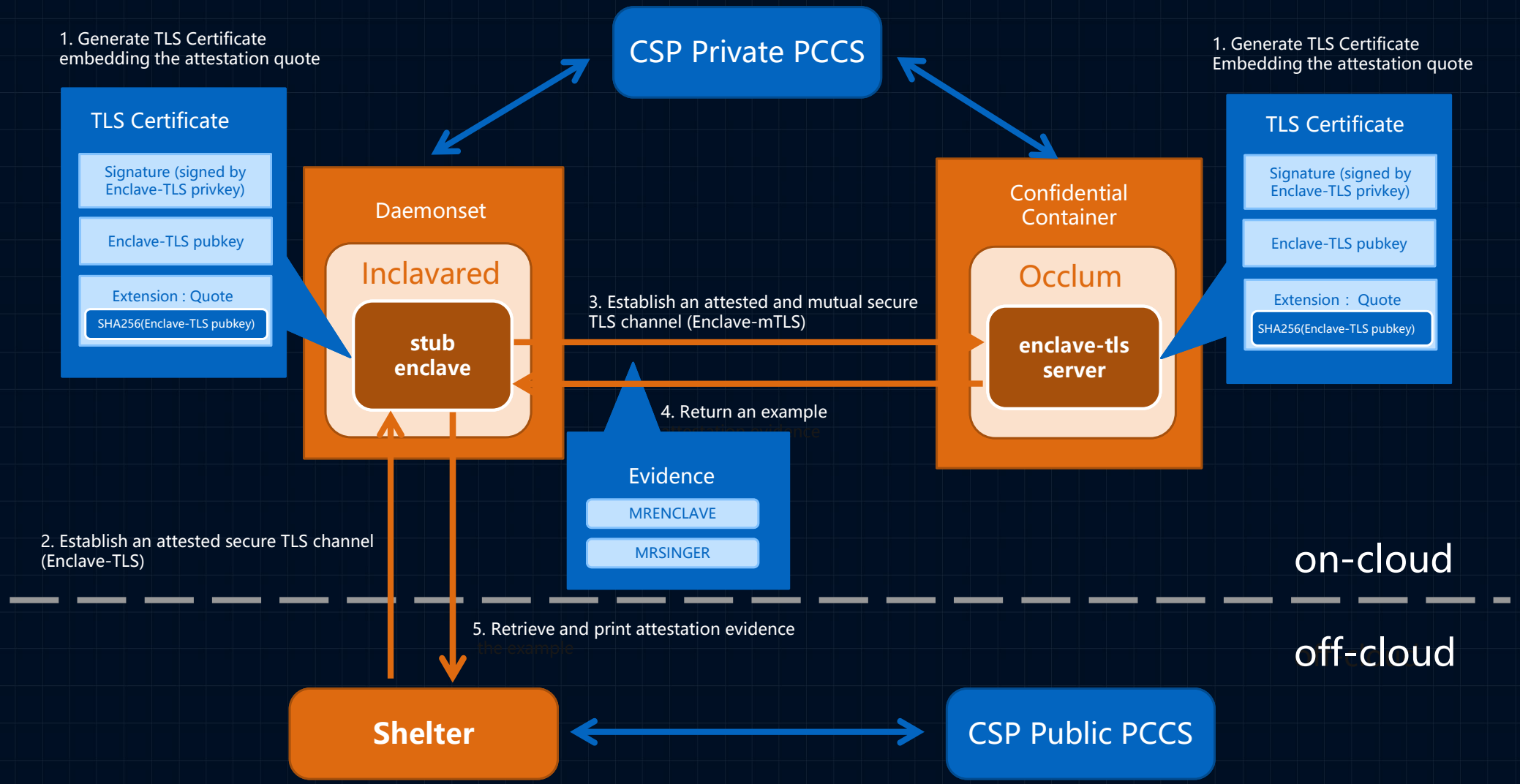
详情请查阅文档

Containerd集成

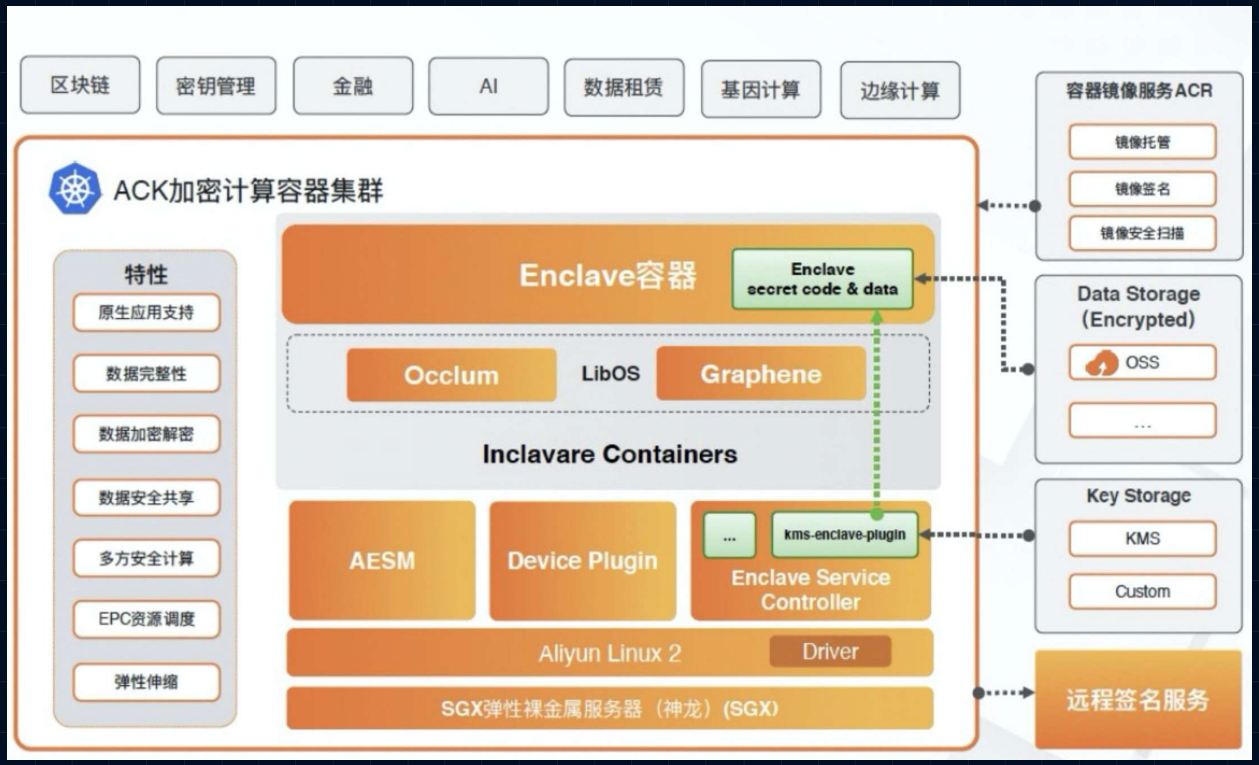
```
[plugins.cri.containerd]
 ...
  [plugins.cri.containerd.runtimes.rune]
   runtime_type = "io.containerd.rune.v2"
```

详情请查阅文档

Kubernetes集群级远程证明架构



如何在阿里云上使用 Inclavare Containers?



ACK-TEE是基于硬件加密技术的云原生一站式机密计算容器平台。

ACK-TEE 依托 Inclavare Containers，能够无缝地运行用户制作的机密容器镜像，并保持与普通容器相同的使用体感。

- 在ACK-TEE集群中使用Inclavare Containers机密容器
- 在ACK-TEE集群中使用Inclavare Containers机密容器实现远程证明

五大特色功能，为用户数据保驾护航

1. 移除对云服务提供商的信任
2. 提供通用的远程证明安全架构
3. 定义了通用的Enclave Runtime API 规范
4. OCI兼容，实现了机密容器形态
5. 与Kubernetes生态无缝结合

Inclavare Containers TODO Items

- 在支持一代机密容器技术（Intel SGX）的基础上，扩展对二代机密容器技术——机密虚拟机（例如Intel TDX / AMD SEV等）的支持，实现真正服务于机密计算场景的通用机密容器技术。
- 为 CNCF 提供面向云原生场景的机密容器解决方案。
- 使用 Inclavare Containers 的 EAA 满足机密计算场景下对远程证明的需求。
- Enclave-TLS（后改名为RATS-TLS） 实现对业务应用无感知，对主流框架的支持（gRPC等）。
- 从 RATS-TLS 中派生出跨平台的远程证明原语库，解决跨 HW-TEE 平台无法进行远程证明的用户痛点问题。

RATS： Remote ATtestation ProcedureS

欢迎大家参与 Inclavare Containers 开源项目

Inclavare Containers技术讨论群

Github

https://github.com/alibaba/inclavare-containers

https://github.com/alibaba/inclavare-containers

主页

https://inclavare-containers.io/

Contribution Guidelines

https://github.com/alibaba/inclavare-containers/blob/master/CONTRIBUTING.md

https://github.com/alibaba/inclavare-containers/blob/master/ROADMAP.md

Thanks_