ORACLE

OCI容器实例及OKE服务介绍

用于 Kubernetes 的 Oracle 容器引擎

Wenbin

SE Hub，JAPAC

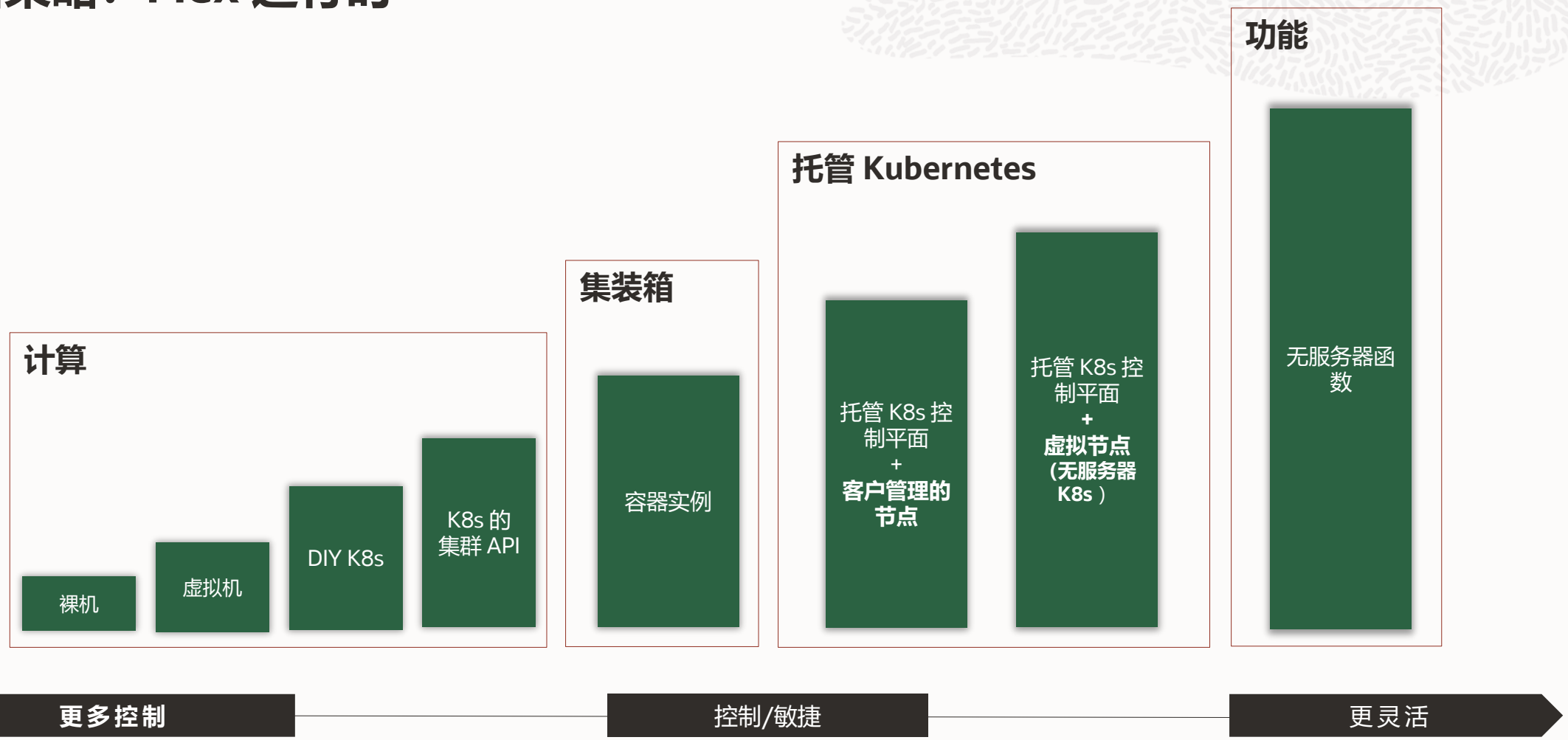
2023 年 6月

Safe harbor slide

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions.

The development, release, timing, and pricing of any features or functionality described for Oracle's products may change and remains at the sole discretion of Oracle Corporation.

容器策略：Flex 运行时



容器和 Kubernetes 服务

在 OCI 中运行容器工作负载

OCI 容器实例

无需管理 VM 即可运行容器的简单、快速且安全的方法

用于 Kubernetes OKE 的 OCI 容器引擎

OCI 中的托管 Kubernetes 服务

管理节点

您控制的节点

虚拟节点

无服务器 Kubernetes

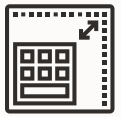
OCI 容器实例

OCI 容器实例

在 OCI 中运行容器的简单、快速和安全的方式

用于容器的
无服务器计算

快速启动应用程序

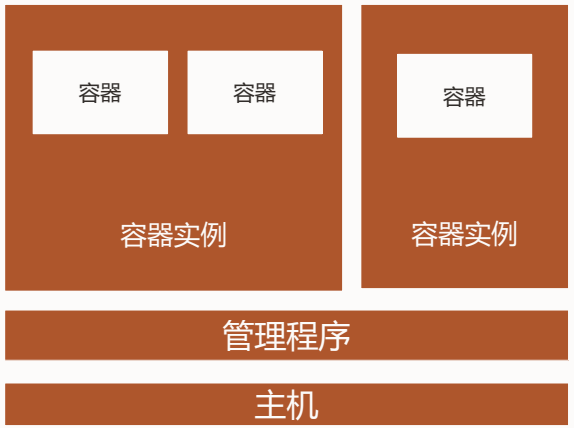


多达 128 个 vCPU 和
1024 GB 内存*

与“常规”计算相同的价格

* E3/E4 Flex Shapes 支持的 CPU/内存

主要特征



- 无服务器计算——无需管理服务器
  - 选择首选计算型号； E4/E3 Flex 已GA，计划添加更多
  - 指定 CPU/内存资源
  - 可以分配型号提供的所有资源来支持要求苛刻的应用程序
  - 包括 15 GB 临时存储
- 简单、快速、灵活
  - 使用控制台、CLI、API、Terraform 轻松启动
  - 每个实例一个或多个容器
  - 从 OCIR 或外部注册表中拉取图像
  - 可选配置——正常关机、重启策略、环境变量、启动选项、资源限制等。
- 安全、网络和可观察性
  - 强隔离——不共享内核，跨实例资源
  - 通过 VCN 进行安全通信，并可选择分配公共 IP
  - 使用资源主体的 IAM 访问控制
  - 内置指标
  - 在控制台上查看日志或使用 API 拉取

用例

- 不需要容器编排的容器化应用程序（如 Kubernetes）
  - API 和 Web 应用程序
  - 临时工作负载
    - CI/CD 管道作业
    - 开发/测试环境
    - 数据/媒体处理
    - 自动化任务
- 直接在服务器/虚拟机上运行的独立容器工作负载
- 遗留应用程序的容器化，直到分解为云原生应用程序

注意：要在不管理基础设施的情况下在 Kubernetes 上运行应用程序，请使用OKE 的虚拟节点

用于 Kubernetes 的 Oracle 容器引擎 (OKE)

用于 Kubernetes 的 Oracle 容器引擎 (OKE)

内置管理

- 完全托管的控制平面
- 高度托管的数据平面组件
- 自动缩放

可靠性

- 默认高可用
- Node Doctor 可轻松排除故障
- 99.95% 的可用性 SLO

性价比

- 通过 Flex 型号和灵活的负载平衡器进行合理计算
- 可预测且一致的性能
- 包括企业支持

开放标准

- 符合 Kubernetes 标准
- 符合开放容器计划
- 没有供应商锁定

高级安全

- 私有集群和注册表（镜像仓库）
- 默认加密
- 容器镜像扫描和签名
- 符合 Kubernetes STIG、NSA、DoD、CISA
- 合规性（FedRAMP、 HIPAA、SOC等）

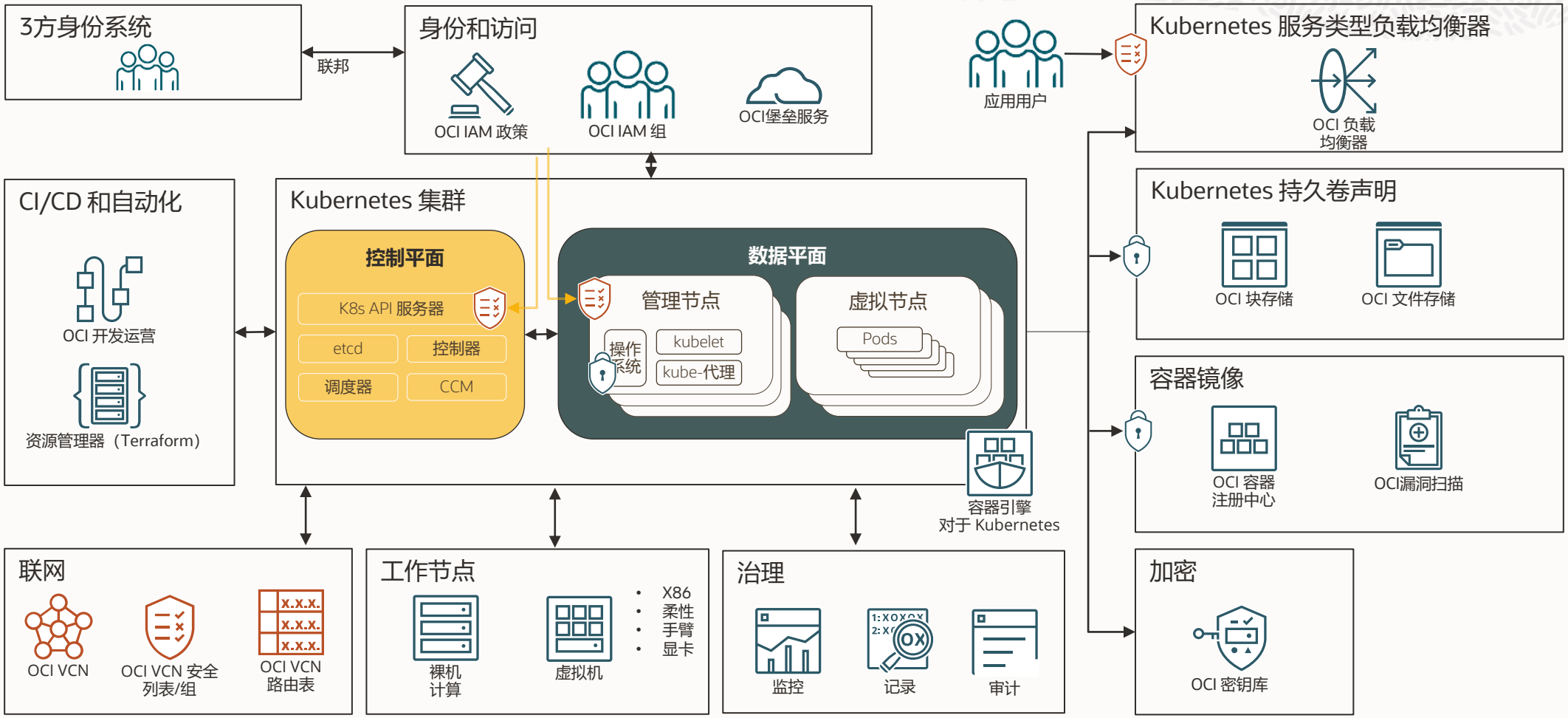
部署灵活性

- **从托管节点或虚拟节点中进行选择——以获得完整的无服务器体验**
- 用于部署的 DevOps 集成
- 丰富的计算形态支持：HPC、GPU、ARM、Flex、Bare Metal 和 VM
- 适用于所有商业区域和 OCI 专用区域

可扩展性

- OCI 服务和 Oracle DB 的操作器
- 利用任意 Kubernetes 软件
- 与 OCI 服务无缝集成

与其他 OCI 服务无缝集成

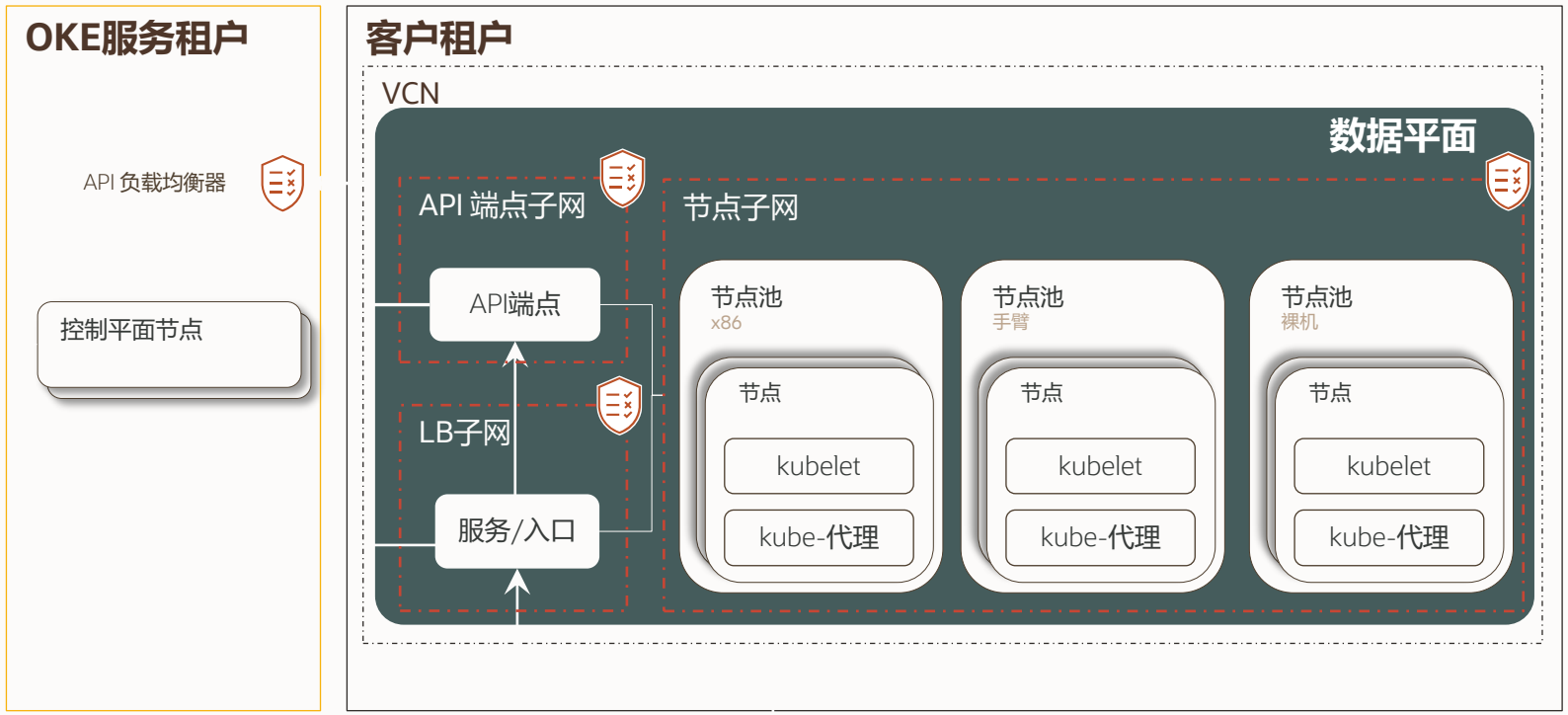


OKE 托管节点

带有托管节点的 OKE

Kubernetes 集群控制平面由 OKE 管理。集群数据平面在客户的租户中运行。

高度管理的 Kubernetes 工作节点



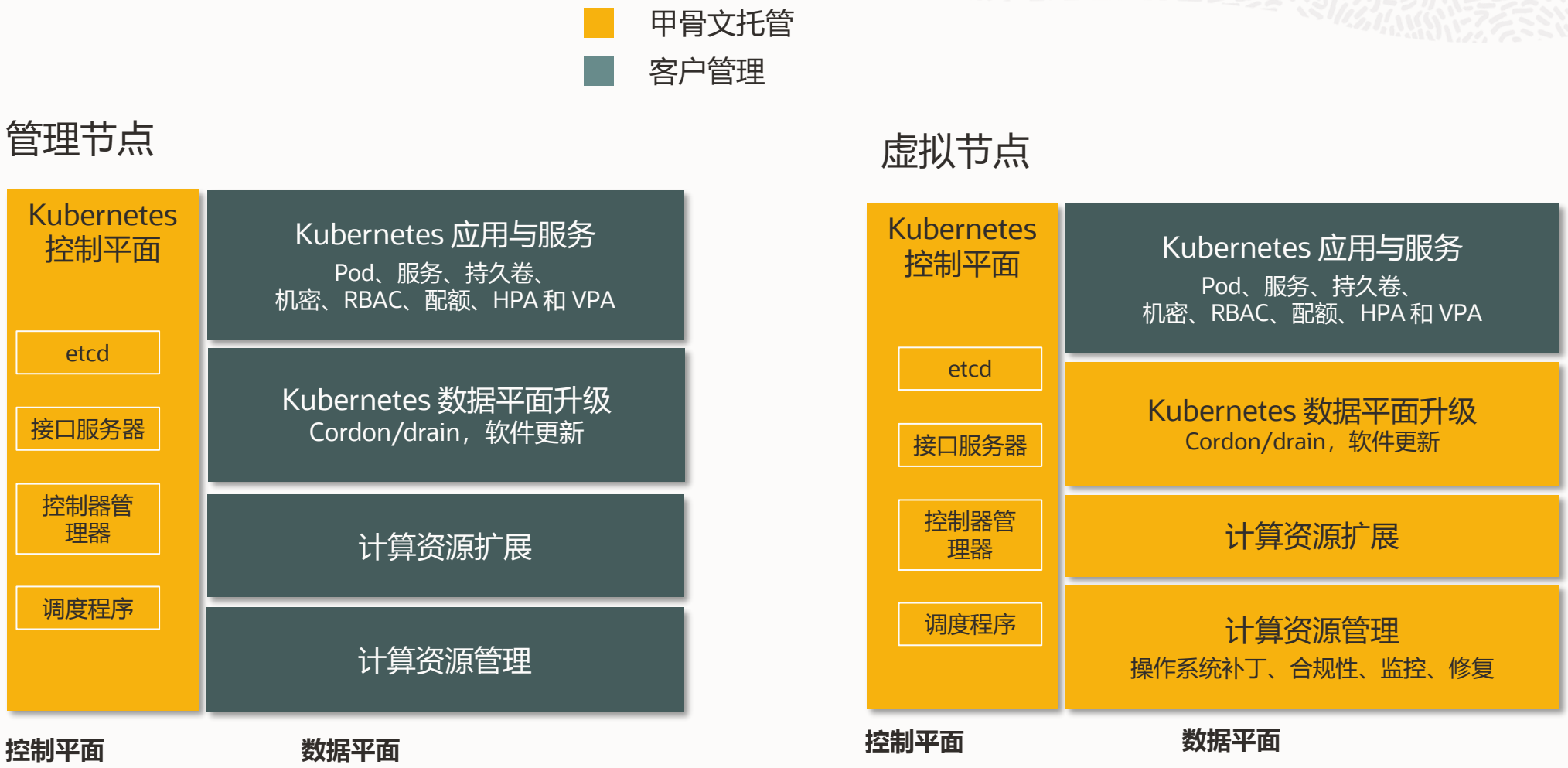
灵活的数据平面

- ✓ 异构节点
- ✓ 集群自动缩放器支持
- ✓ 托管的附加组件
- ✓ 轻松升级节点
- ✓ 节点镜像定制
- ✓ 完全控制硬化

OKE 虚拟节点：无服务器 Kubernetes

无需管理任何基础设施即可运行 Kubernetes

OKE Virtual Nodes：我们管理 K8s 基础设施，因此您不必这样做！



有效的资源扩展和成本优化

对于**托管节点**, 在节点池基本管理工作节点的CPU与内存:

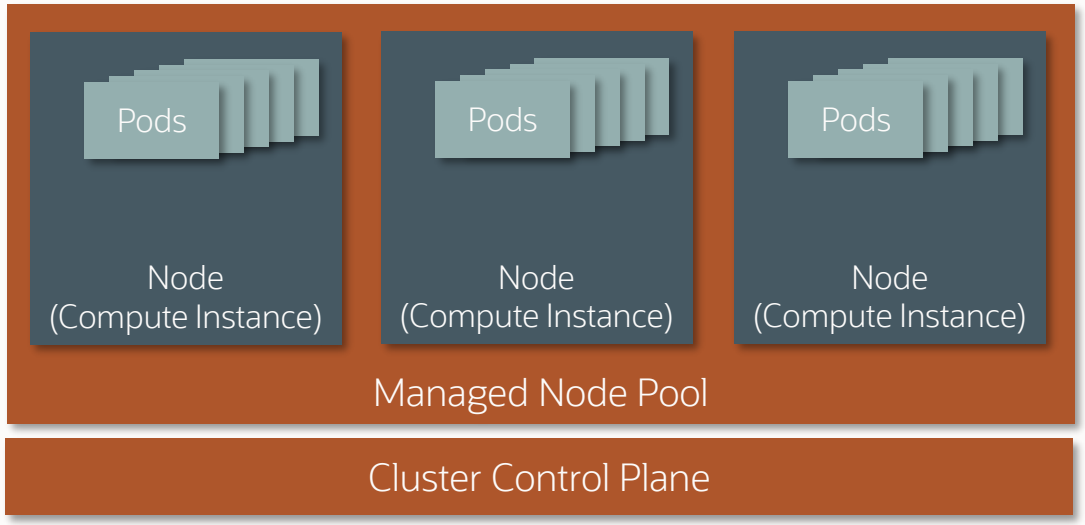
- 手工添加/删除节点
- 或使用Cluster Autoscaler进行自动管理

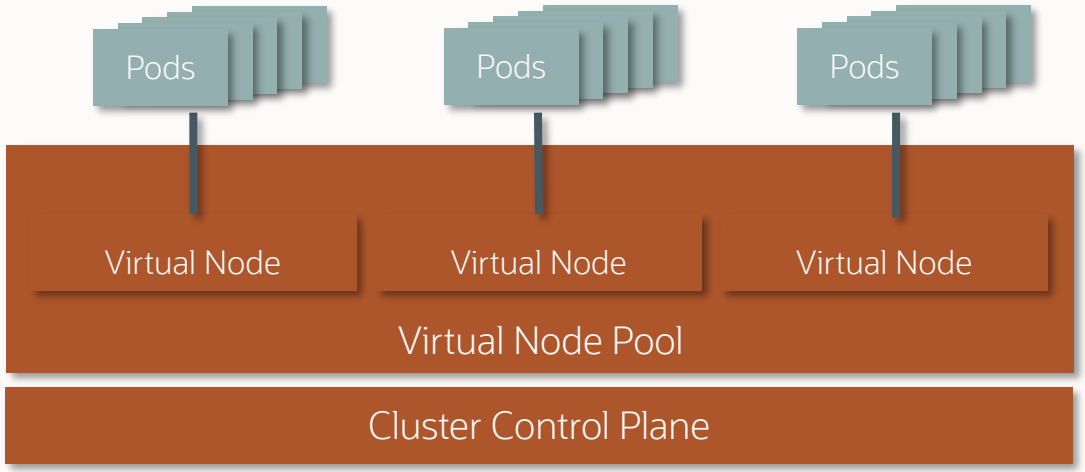
为节点资源付费

对于 **虚拟节点**, 你在pod spec中指定CPU与内存需求

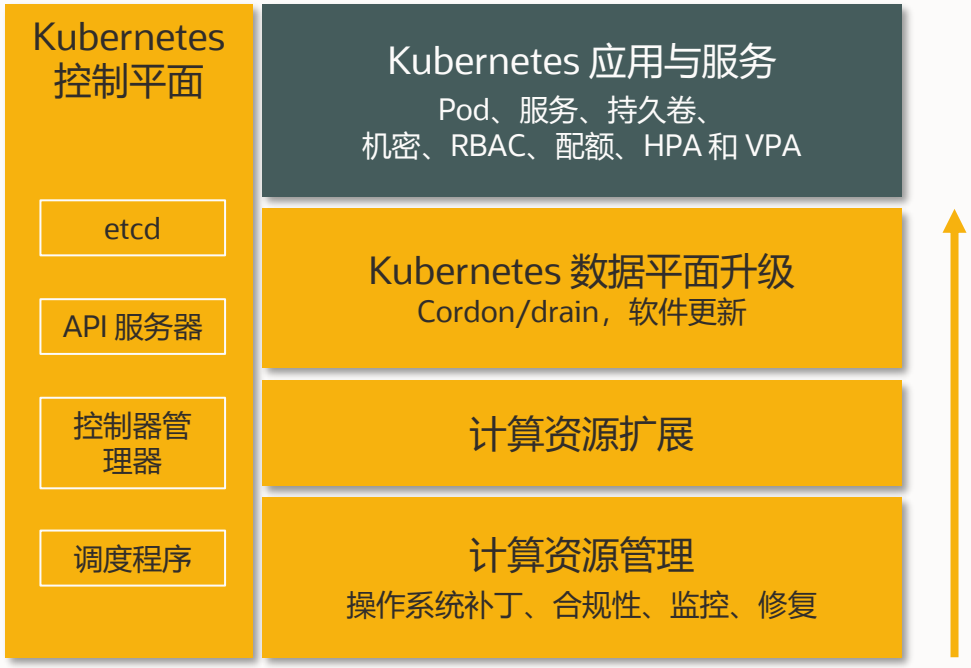
虚拟节点根据需要提供适当大小的计算，从而消除了管理集群数据平面容量的需要。

为pod 资源付费.





OKE虚拟节点



虚拟节点提供**无服务器 Kubernetes 体验**

简化的 Kubernetes 操作

- 无基础设施管理
- 简化资源扩展
- 无缝 Kubernetes 升级

灵活支持您的应用需求

- 可选处理器型号和高垂直可扩展性
- 约束拓扑传播
- 为每个 pod 提供强隔离
- VCN 安全（路由、NSG、流日志）

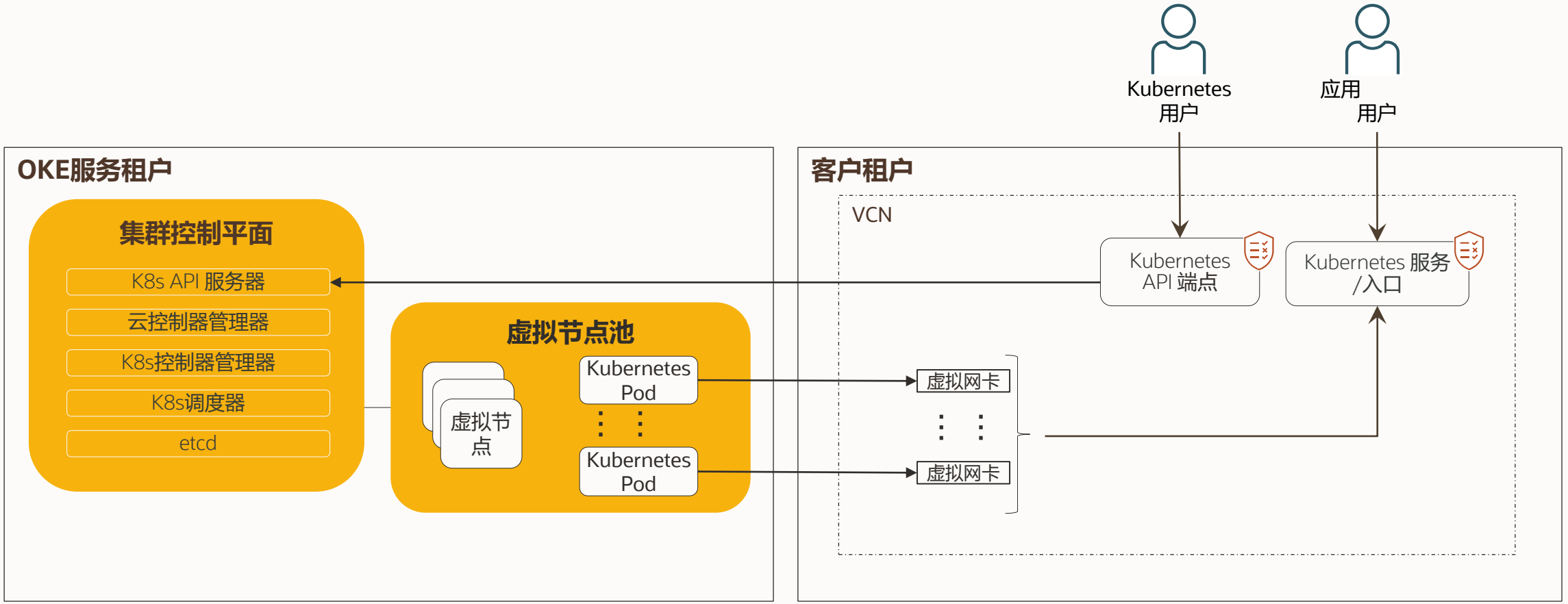
成本优化

- 以计算价格 + 小额虚拟节点费用支付 Kubernetes Pod 使用的资源

带有托管节点的 OKE

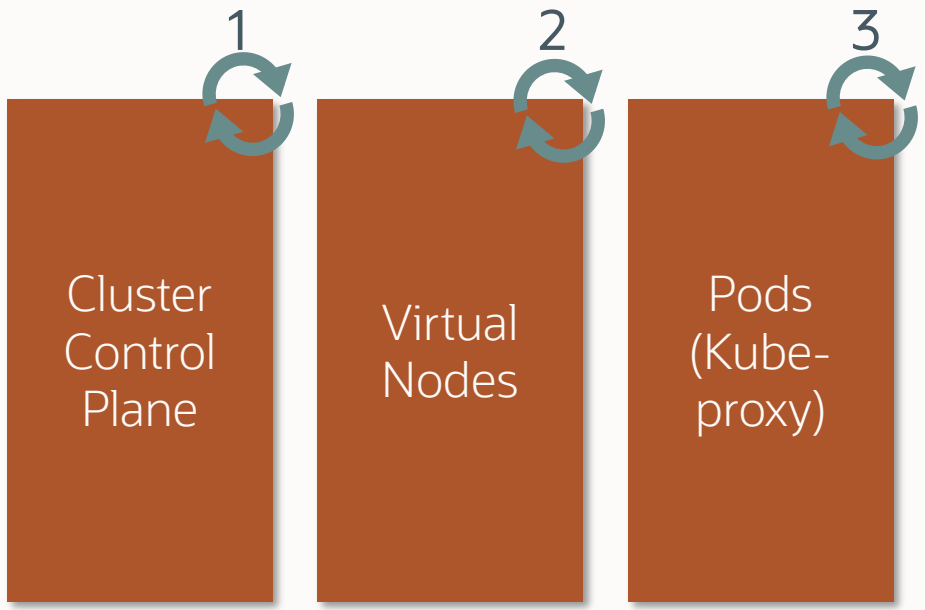
Kubernetes 集群控制平面由 OKE 管理。集群数据平面在客户的租约中运行。

带有虚拟节点的 OKE



Kubernetes 集群控制平面和数据平面由 OKE 管理。

Kubernetes无缝升级



- Kubernetes组件一起升级
  1. 控制面升级不影响工作负载
  2. 虚拟节点升级不影响工作负载
  3. 运行在每个Pod中的Kube-proxy 将异步升级，对工作负载的可用性影响降到最低
- Pod中断预算(Pod Disruption Budgets / PDBs)可以避免应用停机

使用 OKE 虚拟节点来消除数据平面的管理工作

客户责任	带有受管节点的 OKE	带有虚拟节点的 OKE
工作节点监控	是的	不
工作节点扩展	是的	不
工作节点操作系统修补	是的	不
Kubernetes 升级	半托管/ 完全托管（路线图）	完全托管并与集群升级同步

提高开发人员生产力和总体拥有成本（TCO）：
通过消除 Kubernetes 节点的生命周期管理，OKE 虚拟节点每天都可以将几个小时的时间返还到工程设计中。

虚拟节点当前不支持的特性

不支持以下特性

- LB直接把流量发给Pod而非worknode
- 只支持 VCN-Native CNI，不支持Flannel
- Liveness and readiness probes 不支持gRPC、exec、TCP、https，只支持http
- 不支持Volume类型：emptyDir、ConfigMap、Secret，不支持PVCs
- 不支持VolumeMount.Subpath Expression
- 不支持kubectl logs –f、kubectl exec
- 不支持Pod/Container securityContext的一些配置
- Container.Resources.Requests无效

不支持以下特性

- 无法ssh到虚拟节点
- 不能自定义初始化脚本
- 没有Node检测脚本
- 不能自动增减虚拟节点数量
- 没有Intel、Arm、GPU类型的虚拟节点
- 创建集群时，只能选择虚拟节点或托管节点，当前在同一个集群中不支持2种节点

不支持以下通用附加组件

- Kube-proxy(kube-system中)
- K8s dashboard
- Nginx ingress controller
- K8s CA
- VPA
- K8s mertrics server

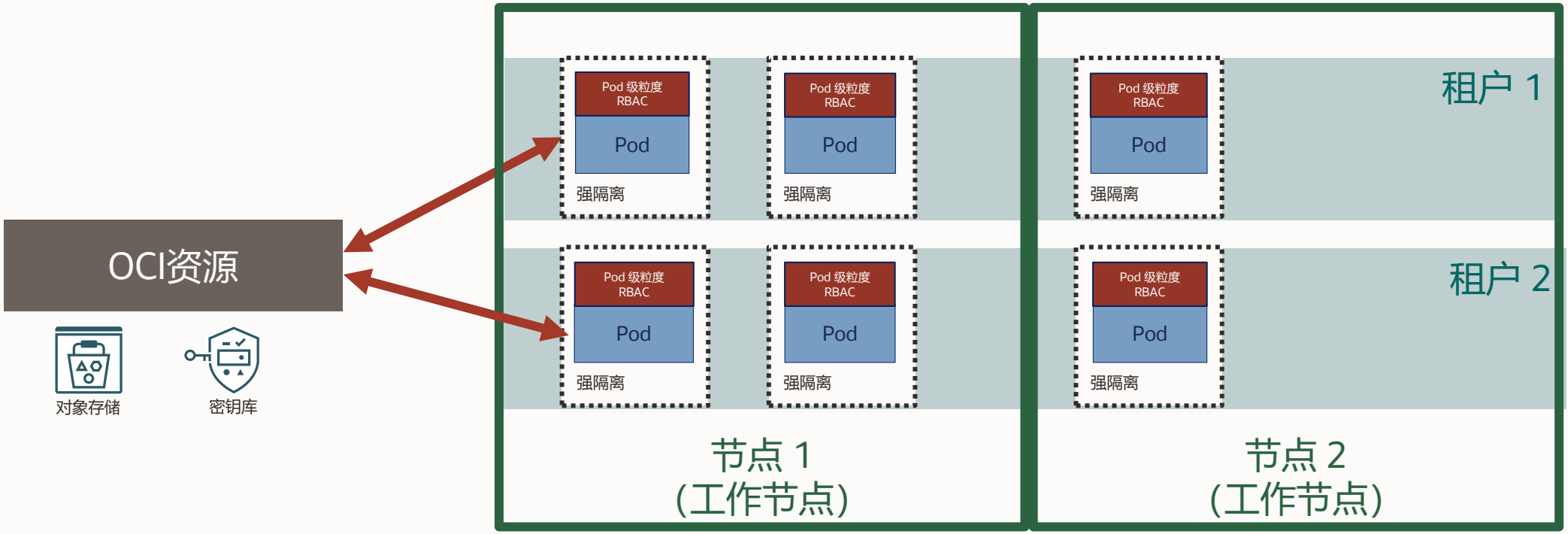
托管节点与虚拟节点区别明细 https://docs.oracle.com/en-us/iaas/Content/ContEng/Tasks/contengcomparingvirtualwithmanagednodes_topic.htm#contengusingvirtualormanagednodes_topic

OKE 其他特性

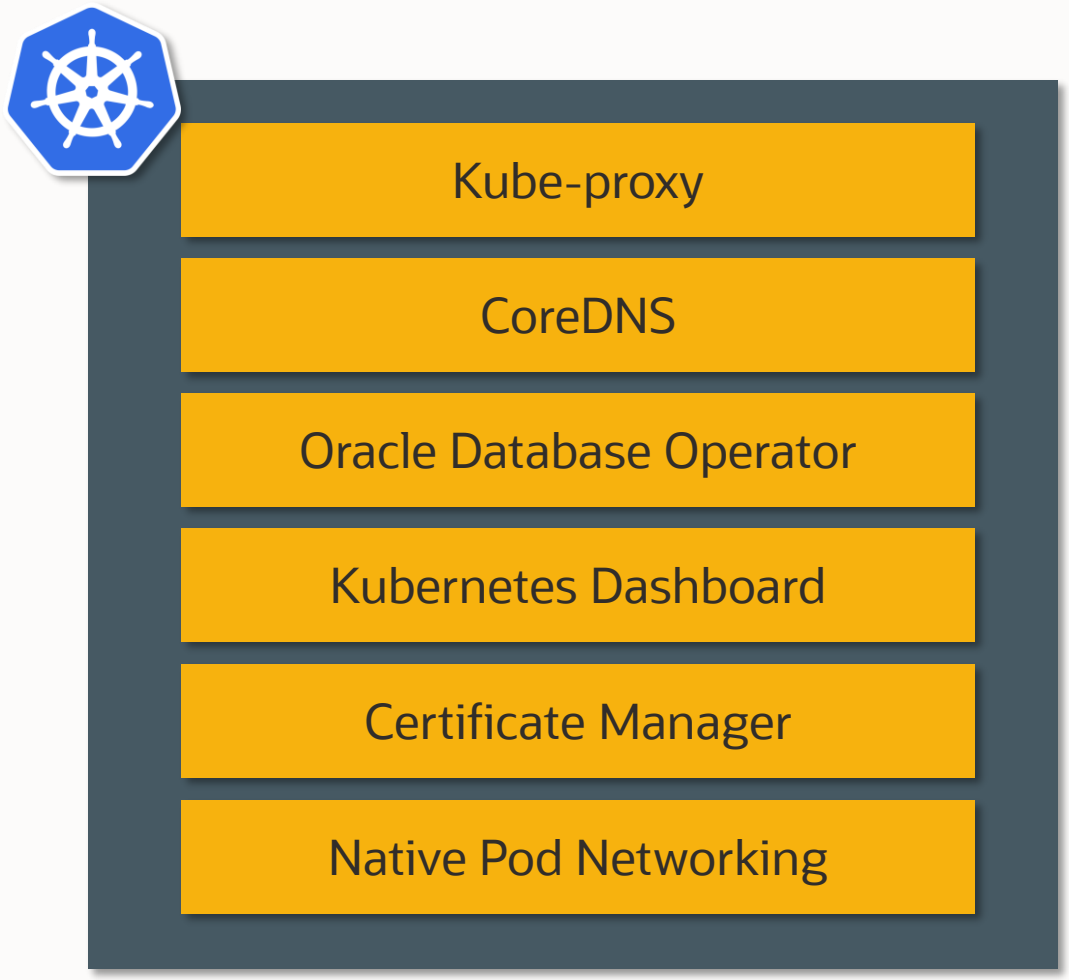
结合新功能更简单地实施多租户架构：虚拟节点 和工作负载身份

提高常见 ISV / SaaS 应用程序设计的 COGS 和可管理性：

- 更容易集中管理在不同租户或应用程序之间共享的 SaaS 基础架构（同时确保隔离不受信任的工作负载）
- 跨多个租户共享集群资源，提高资源利用率



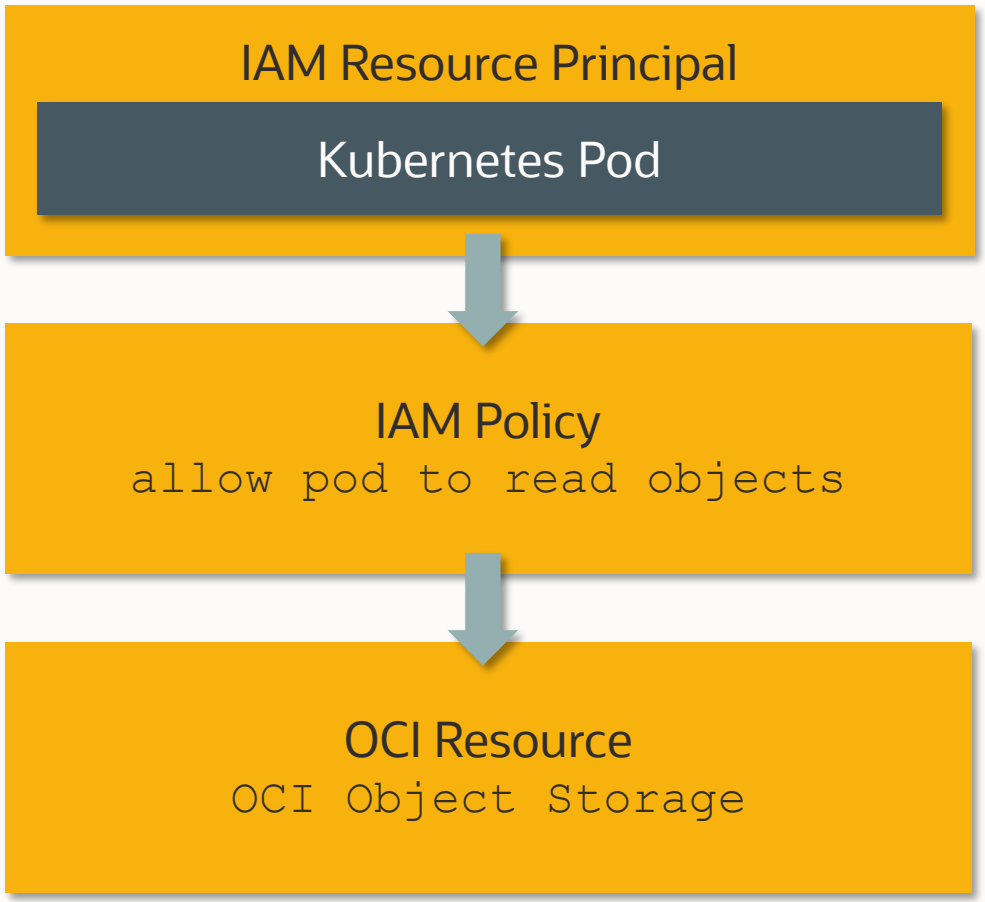
附加组件(Add-on)生命周期管理



获得集群中操作软件的控制权– 使用OCI管理软件的整个生命周期

- 部署必要的集群附加组件
- 通过特定于附加组件的自定义和高级配置获得控制
- 选择不使用oracle提供的附加组件来安装你自己的软件——比如CNI等等。
- 未来会不断增加新的可用组件

Kubernetes Workload Identity



通过粒度pod级访问控制改善安全状态和可管理性

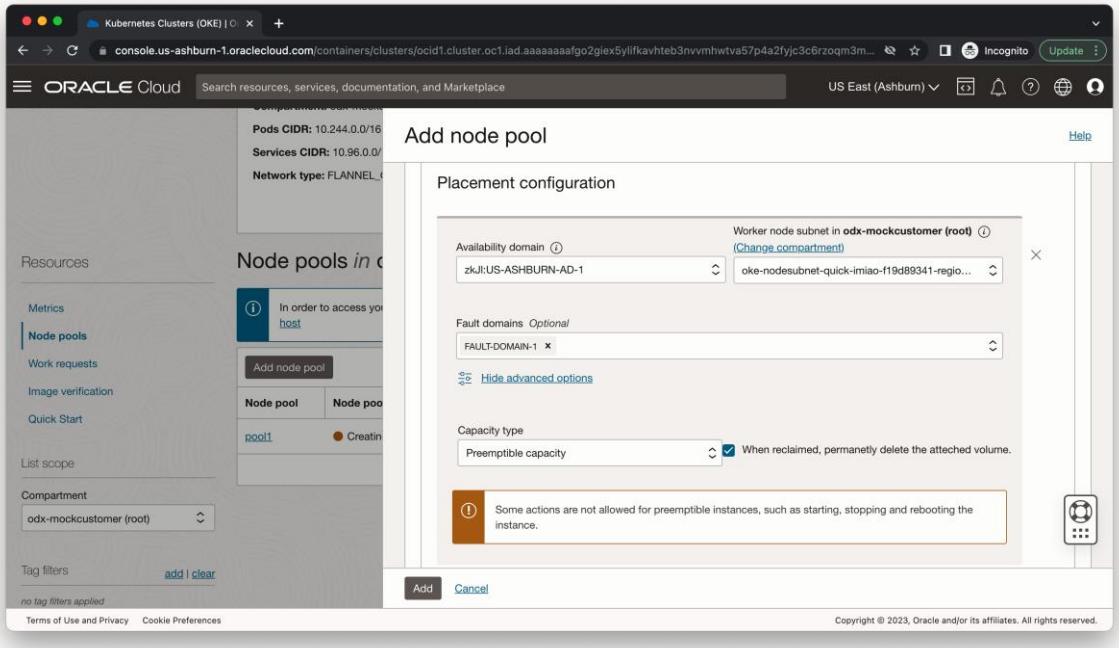
- A授权特定的Kubernetes pod进行OCI API调用和访问OCI资源
- 授予在这些pod中运行的应用程序对OCI API的策略驱动访问权限
- 对容器化应用程序应用最小权限原则
- 使用OCI审计日志自动跟踪来自Kubernetes pod的API调用
- 工作负载:需要OCI IAM策略来访问其他OCI服务和具有多租户工作负载的客户的应用程序

其他改进

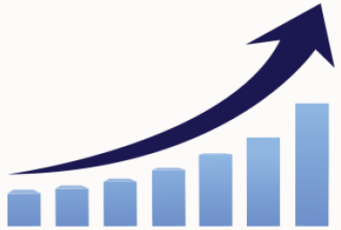
- 控制平面的**SLA**

- 对托管节点的
  抢占式（“spot”实例）支持
  - 与按需实例相比，可中断工作负载的成本降低**50%**，可用性保证较低
  - 集群可以是异构的：由按需节点和可抢占节点组成
  - 客户可以使用 Kubernetes 标签、污点和容忍度来控制 pod 运行的节点类型

- **更大的集群规模：**默认 2,000 个节点
  - 2倍于先前的默认限制；可以轻松增加



用例



工作负载用例

- 高度可扩展的无状态应用程序
  示例：在自治数据库中具有状态的 Web 应用程序
- 高度可扩展的有状态应用程序
  示例：Spark
- 作业、Cron 作业、批处理等。
- 工作流程
  示例：Argo 工作流程
- 扩展到 0 个应用程序
  示例：Knative

操作用例

- 通过内置弹性处理使用高峰
- 没有基础设施操作的 Kubernetes
- 将工作负载突发到虚拟节点池
- 多租户集群
- 应用层计费

OKE 定价

凭借它们提供的新功能和可观的优势，更新了服务定价：

- **增加了控制平面管理的象征性费用：**
  - **0.10 美元/集群/小时**（最高74.40美元/月）
  - 包括用于 Kubernetes API 服务器的有经济支持的 SLA
  - 与所有其他云提供商一致
  - 新功能使客户能够更轻松地运行支持多个应用程序 (pod) 的单个（更大）集群，同时确保隔离和优化资源消耗

- **增加了虚拟节点管理的象征性费用：**
  - 每个选定的虚拟节点**0.015 美元/节点/小时**
  - 托管节点没有变化

✓ **OCI依然具有极高的性价比**

总结

在 OCI 的什么地方运行容器?

OCI 容器实例

- 在几秒钟内运行容器，无需管理任何服务器
- 适用于不需要 Kubernetes 编排的工作负载
- 简单，不需要 Kubernetes 技能

带有虚拟节点的 OKE

- Kubernetes 编排
- 容器由为 Kubernetes 节点提供抽象的虚拟节点执行
- 消除节点基础设施的管理、扩展、升级和故障排除的运营开销
- 需要较少的 Kubernetes 技能

带有托管节点的 OKE

- Kubernetes 编排
- 容器由 OCI Compute 实例执行，生命周期通过 OKE API 管理
- 您可以根据您的要求控制节点的配置
- 需要 Kubernetes 技能

Our mission is to help people see data in new ways, discover insights, unlock endless possibilities.

附录

ServerLess Kubernetes 示意图