

机密计算平台 最佳实践



腾讯云

【 版权声明 】

©2013–2024 腾讯云版权所有

本文档（含所有文字、数据、图片等内容）完整的著作权归腾讯云计算（北京）有限责任公司单独所有，未经腾讯云事先明确书面许可，任何主体不得以任何形式复制、修改、使用、抄袭、传播本文档全部或部分内容。前述行为构成对腾讯云著作权的侵犯，腾讯云将依法采取措施追究法律责任。

【 商标声明 】



及其它腾讯云服务相关的商标均为腾讯云计算（北京）有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标，依法由权利人所有。未经腾讯云及有关权利人书面许可，任何主体不得以任何方式对前述商标进行使用、复制、修改、传播、抄录等行为，否则将构成对腾讯云及有关权利人商标权的侵犯，腾讯云将依法采取措施追究法律责任。

【 服务声明 】

本文档意在向您介绍腾讯云全部或部分产品、服务的当时的相关概况，部分产品、服务的内容可能不时有所调整。您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或默示的承诺或保证。

【 联系我们 】

我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 4009100100或 95716。

文档目录

最佳实践

CVM 运行机密应用

TKE 部署机密镜像

最佳实践

CVM 运行机密应用

最近更新时间：2024-04-24 10:43:52

操作场景

本文介绍如何在云服务器（CVM）上运行机密应用。

前提条件

- 已开通 [密钥管理服务 KMS](#) 和 [容器服务 TKE](#)。
- 已同意为机密计算平台创建服务相关角色，并 [授权调用](#) 其他云服务接口。

步骤1：在信任的环境中封装机密应用

在信任的环境中封装机密应用，详情请参见命令行指南的 [封装机密应用](#)，并保存生成的机密应用文件，如下所述。

```
$ ls {appName}*  
{appName}.manifest.sgx {appName}.sig {appName}.token
```

步骤2：购买支持 SGX 特性的 M6ce 实例

在 [云服务器 CVM 页面](#)，购买用于运行机密应用的 CVM 实例，类型需要选择 **M6ce**，支持的操作系统包括 Ubuntu、CentOS 和 TencentOS，可用区选择南京二区、北京六区、广州六区、上海五区。

1.选择机型
2.设置主机
3.确认配置信息

标准型S4	标准网络优化型SN3ne	标准型S3	标准型SA1	标准型S2	标准型S1	高IO型IT5 NEW	高IO型IT3
高IO型I3	内存型M6	内存型MA3	内存型M6p	内存型M6mp	安全增强内存型M6ce	内存型MA2	内存型M5 NEW
内存型M4	内存型M3	内存型M2	内存型M1	计算型C6	计算型C5	计算型C4	计算网络增强型CN3
计算型C2	GPU计算型GN6	GPU计算型GN6S	GPU计算型GN7	GPU计算型GN8	GPU计算型GN10X	GPU计算型GN10Xp	
GPU推理型GI3X	GPU计算型GT4 NEW	GPU渲染型GI1 NEW	FPGA加速型FX4	大数据型D3 NEW	大数据型D2	大数据型D1	
大数据型DSW13t	大数据型DSW03	标准型黑石物理服务器BMS4 热	大数据型黑石物理服务器BMD2 热				
大数据型黑石物理服务器BMD3 热	大数据型黑石物理服务器BMD3s	高IO型黑石物理服务器BMIS 热	内存型黑石物理服务器BMM5r				
GPU型黑石物理服务器BMG5t	GPU型黑石物理服务器BMG5v ?						

机型	规格	vCPU	内存	处理器型号	内网带宽	网络收发包	支持可用区	备注	费用
<input type="radio"/> 安全增强内存型M6ce	M6ce.ME...	2核	16GB	Intel Ice Lake(2.7GHz/3.3G Hz)	2Gbps	30万PPS	4个可用区	含加密内存 8 GB	349.27元/月
<input type="radio"/> 安全增强内存型M6ce	M6ce.LAR...	4核	32GB	Intel Ice Lake(2.7GHz/3.3G Hz)	4Gbps	60万PPS	4个可用区	含加密内存 16 GB	698.54元/月
<input checked="" type="radio"/> 安全增强内存型M6ce	M6ce.2XL...	8核	64GB	Intel Ice Lake(2.7GHz/3.3G Hz)	7Gbps	120万PPS	4个可用区	含加密内存 32 GB	1397.09元/月
<input type="radio"/> 安全增强内存型M6ce	M6ce.4XL...	16核	128GB	Intel Ice Lake(2.7GHz/3.3G Hz)	13Gbps	250万PPS	4个可用区	含加密内存 64 GB	2794.18元/月

已选机型 M6ce.2XLARGE64 (安全增强内存型M6ce...)
配置费用 1397.09元 (费用明细)

数量 - 1 + 时长 1个月 ?
带宽费用 0.00元

下一步: 设置主机

有奖调研

联系我们

步骤3：配置 CVM 环境

登录 CVM 设备后，配置 CVM 环境，详情请参见环境配置指南的 [配置 CVM 环境](#)。

步骤4：启动应用

用户将 [步骤1](#) 生成的文件上传到 CVM 中，并使用 CCPCLI 启动机密应用，详情请参考命令行指南的 [启动机密应用](#)。

步骤5：查看远程证明和应用运行状态

登录 [机密计算平台控制台](#)，查看远程证明和应用运行状态。详情请参见控制台指南的 [查看远程证明](#)、[查看计算节点](#)。

TKE 部署机密镜像

最近更新时间：2024-04-24 10:43:52

操作场景

本文介绍如何在 TKE 上运行机密镜像。

前提条件

- 已开通 [密钥管理服务 KMS](#) 和 [容器服务 TKE](#)。
- 已同意为机密计算平台创建服务相关角色，并 [授权调用](#) 其他云服务接口。

步骤1. 封装机密镜像

在信任的环境中封装机密镜像，并 Push 到镜像仓库，详细操作方法见命令行指南的 [封装机密镜像](#)，在本例中使用 DockerHub 镜像仓库存储名称为 {sec_image} 的机密镜像，相关命令如下：

```
$ docker login -u {USERNAME}
Password: [PASSWORD]
Login Succeeded

$ docker push {sec_image}
```

步骤2：购买 TKE 集群

- 登录 [容器服务控制台](#)，在左侧导航栏选择集群。
- 在集群页面，单击**新建**。
- 在创建集群页面，配置相关参数，创建集群。更多详情请参见 [创建集群](#)。

⚠ 注意：

- 目前所有机密计算节点机型必须均为 M6ce 型号。
- 购买用于运行机密应用的 CVM 实例，类型需要选择 M6ce，支持的操作系统包括 Ubuntu、CentOS 和 TencentOS。

Worker 节点配置

可用区① 北京二区 北京三区 北京四区 北京五区 **北京六区** 北京七区

节点网络① 共125个子网IP, 剩123个可用

CIDR

如现有的网络不合适, 您可以去控制台[新建私有网络](#) 或 [新建子网](#)

机型 M6ce.2XLARGE64(安全增强内存型M6ce, 8核64GB)

系统盘 高性能云硬盘 50GB

数据盘 暂不购买

公网带宽 按使用流量计费 1Mbps

主机名 自动生成

云服务器数量 - 1 +

VPC网络限制: 当前节点网络最大可用IP数为123

高级设置

确定 取消

添加机型

费用 0.13元/小时 (集群管理费用) | 2.77元/小时 (配置费用) | 0.80元/GB (网络费用-按使用流量)

使用 Serverless 容器集群, 免集群管理费用, 无初始配置费用及网络费用, 按需使用, 按实际用量付费。立即领取 100 元无门槛代金券, 试用 Serverless 容器集群。

上一步 下一步

步骤3: 配置 TKE 环境

配置 TKE 环境, 安装机密计算插件。详情请参见环境配置指南的 [配置 TKE 环境](#)。

步骤4: 创建工作负载

创建工作负载, 配置容器信息。

1. 登录 [容器服务控制台](#), 在左侧导航栏选择集群。
2. 在集群页面, 选择工作负载 > Deployment, 单击新建。

集群(北京) / 默认

YAML创建资源

Deployment 操作指南

新建 监控

default 名称只能搜索一个关键字, Label格式要求: 名称只能搜索一个关键字, Label格式要求: 名称只能搜索一个关键字, Label格式要求:

名称	Labels	Selector	运行/期望Pod...	Request/Limits	操作
jfs	kubernetes.io/cluster=... kubernetes.io/role=...	...	1/1	CPU : 0.5 / 4 核 内存 : 2048 / 4096 Mi	更新Pod数量 更新Pod配置 更多

第 1 页 20 条 / 页

3. 在实例内容容器中输入容器名称, 镜像选择 [步骤1](#) 中 Push 的机密镜像。

数据卷（选填）

[添加数据卷](#)

为容器提供存储，目前支持临时路径、主机路径、云硬盘数据卷、文件存储NFS、配置文件、PVC，还需挂载到容器的指定路径中。[使用指引](#)

实例内容器

名称

c

最长63个字符，只能包含小写字母、数字及分隔符("-")，且不能以分隔符开头或结尾

镜像

ydc

[选择镜像](#)

镜像版本（Tag）

[选择镜像版本](#)

镜像拉取策略

Always

IfNotPresent

Never

总是从远程拉取该镜像


CPU/内存限制

CPU限制

内存限制

创建Workload

取消

4. 在本示例中，我们通过配置特权容器来简化操作，提供不限空间的机密内存。在实例内容器面板下方，单击显示高级设置，在最下方特权级容器选项中单击 ，并单击**创建 Workload** 完成容器创建。

结束前执行①

[新增](#)

容器健康检查①

☐

存活检查 检查容器是否正常，不正常则重启实例

☐

就绪检查 检查容器是否就绪，不就绪则停止转发流量到当前实例

查看健康检查和就绪检查[使用指引](#)

初始化容器



容器标识为init container，[查看详情](#)。

特权级容器



容器开启特权级，将拥有宿主机的root权限

[隐藏高级设置](#)[添加容器](#)

创建Workload

取消

步骤5：查看远程证明和应用运行状态

登录 [机密计算平台控制台](#)，查看远程证明和应用运行状态。详情请参见控制台指南的 [查看远程证明](#)、[查看计算节点](#)。