机密计算平台

最佳实践

腾讯云

文档目录

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。

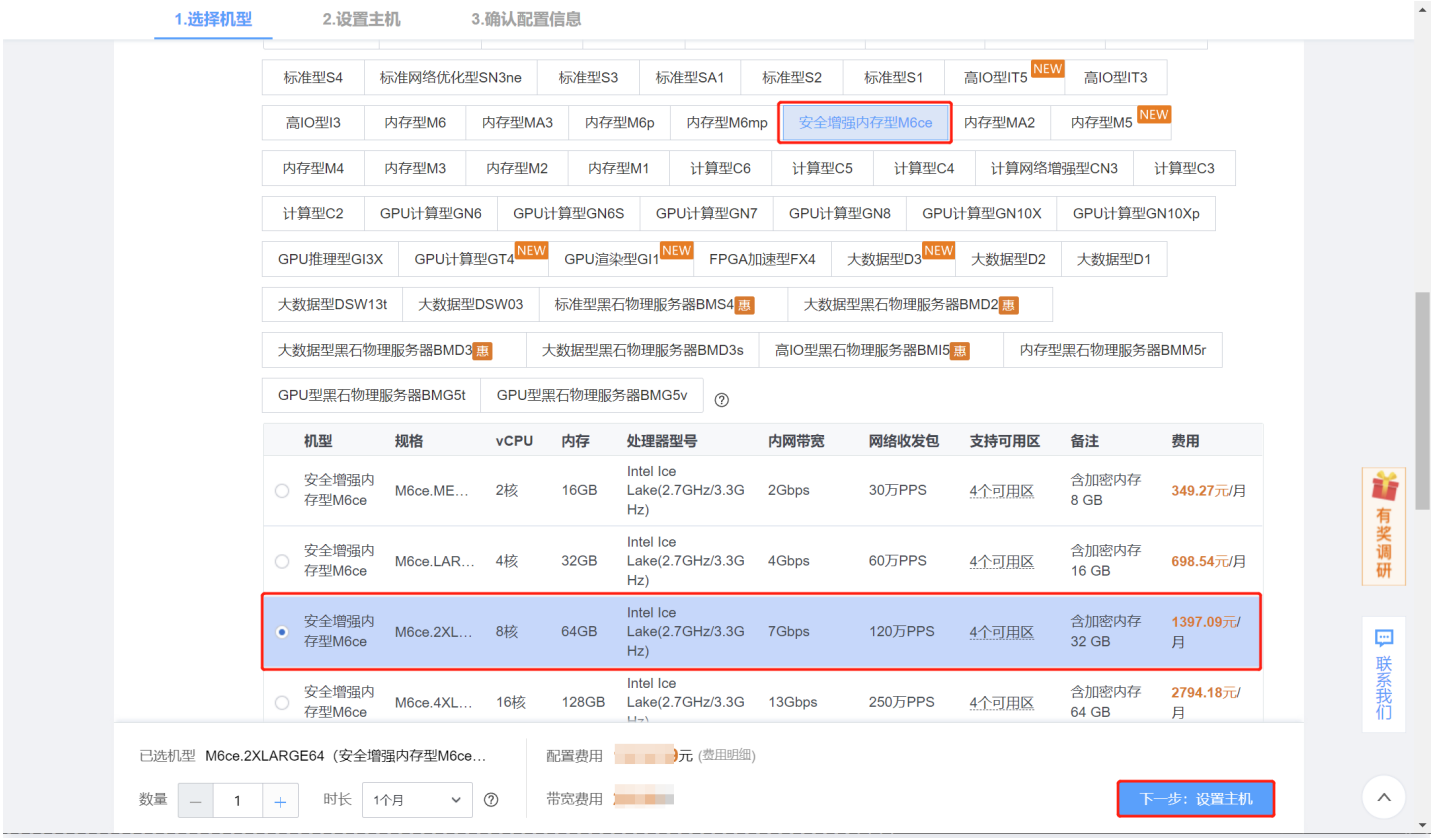
步骤1：在信任的环境中封装机密应用

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。



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

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，单击**新建**。
3. 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。

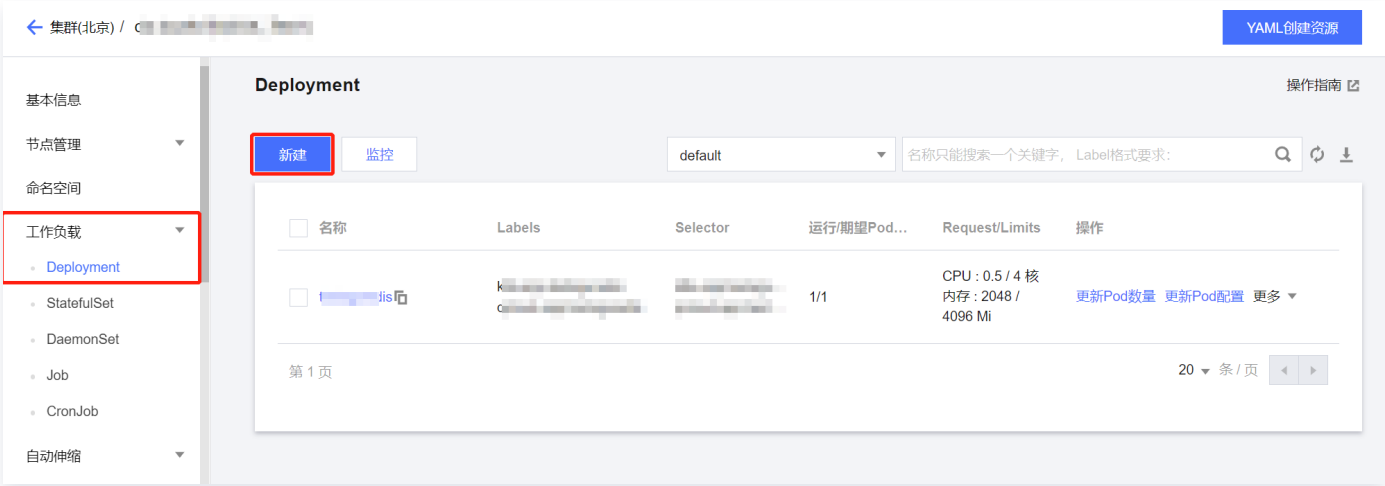
步骤3：配置 TKE 环境

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**。



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

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。

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 。