机密计算平台

操作指南

腾讯云

版权所有：腾讯云计算（北京）有限责任公司

【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】

腾讯云

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

版权所有：腾讯云计算（北京）有限责任公司

操作指南
环境配置指南
配置 CVM 环境
TencentOS

最近更新时间：2024-04-24 10:43:51

操作场景

本文介绍如何在 M6ce 实例中构建 CCP 机密计算环境。

前提条件

已创建并登录 M6ce 实例，且操作系统为 TencentOS Server 3.1(TK4) 。

步骤1：检查内核版本

执行以下命令，检查 kernel 版本。

```
$ uname -a
```

如果版本低于5.4.119-19.0008，请执行以下命令更新 kernel。

```
$ yum update kernel
```

步骤2：下载并安装CCPCLI工具

登录 机密计算平台控制台，并进入工具下载页面，下载最新的 CCPCLI 并安装，详细操作请参见 安装 CCPCLI 。

步骤3：检验运行环境

完成安装后，请使用以下命令检验运行环境。

```
$ ccp-cli info sgx
```

如环境配置正确，以下列出项都被支持。

参数名称	描述

SGX cpu supported	true
SGX flexible lanch control supported	true
SGX1 supported	true
SGX2 supported	true
SGX driver available	true
SGX FSGSBASE available	true
SGX psw installed	true
SGX aesmd service available	true

版权所有：腾讯云计算（北京）有限责任公司

Ubuntu

最近更新时间：2024-04-24 10:43:51

操作场景

本文介绍如何在 M6ce 实例中构建 CCP 机密计算环境。

前提条件

已创建并登录 M6ce 实例，且操作系统为 Ubuntu 20.04 。

步骤1：检查内核版本

执行以下命令，检查 kernel 版本。

```
$ uname -a
```

如果内核版本低于5.11，需要自行升级内核至5.11以上版本。使用较新的内核存在一定潜在的风险，请您自行评估后使用。对于 Ubuntu20.04版本，可以使用 TuxInvader 的 PPA 来简约升级，以下命令仅供参考：

```
$ sudo add-apt-repository ppa:tuxinvader/lts-mainline
$ sudo apt-get update
$ sudo apt-get install linux-generic-5.16
$ sudo reboot
```

步骤2：下载并安装 CCPCLI 工具

登录 机密计算平台控制台，并进入工具下载页面，下载最新的 CCPCLI 并安装，详细操作请参见 安装 CCPCLI 。

步骤3：检验运行环境

完成安装后，请使用以下命令检验运行环境。

```
$ ccp-cli info sgx
```

如环境配置正确，以下列出项都被支持。

参数名称	描述
SGX cpu supported	true

SGX flexible lanch control supported	true
SGX1 supported	true
SGX2 supported	true
SGX driver available	true
SGX FSGSBASE available	true
SGX psw installed	true
SGX aesmd service available	true

配置 TKE 环境

最近更新时间：2024-04-24 10:56:51

操作场景

本文介绍如何在 TKE 集群中构建 CCP 机密计算环境。

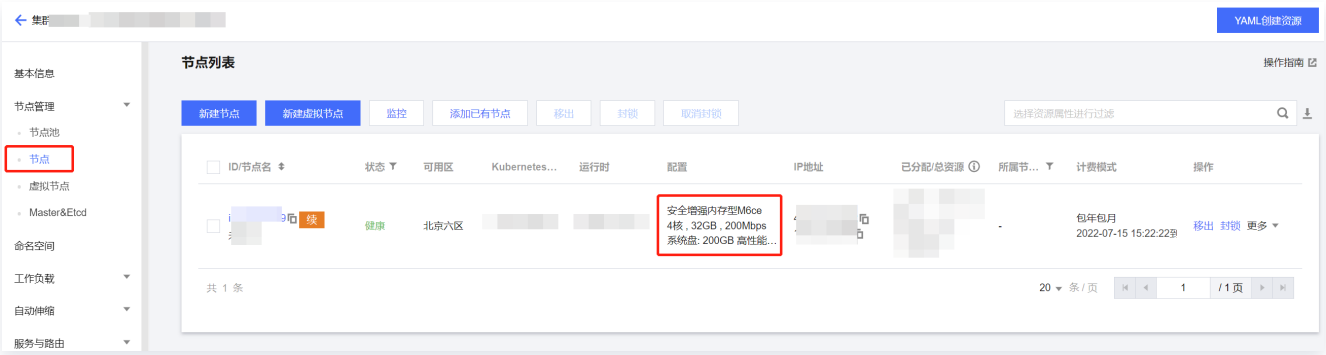
前提条件

已创建 TKE 集群，且所有节点均为 M6ce 实例。

步骤1：检查节点实例类型

1. 登录 容器服务控制台，在左侧导航栏选择集群。
2. 在集群管理页面，单击**集群 ID**，查看集群详细信息。

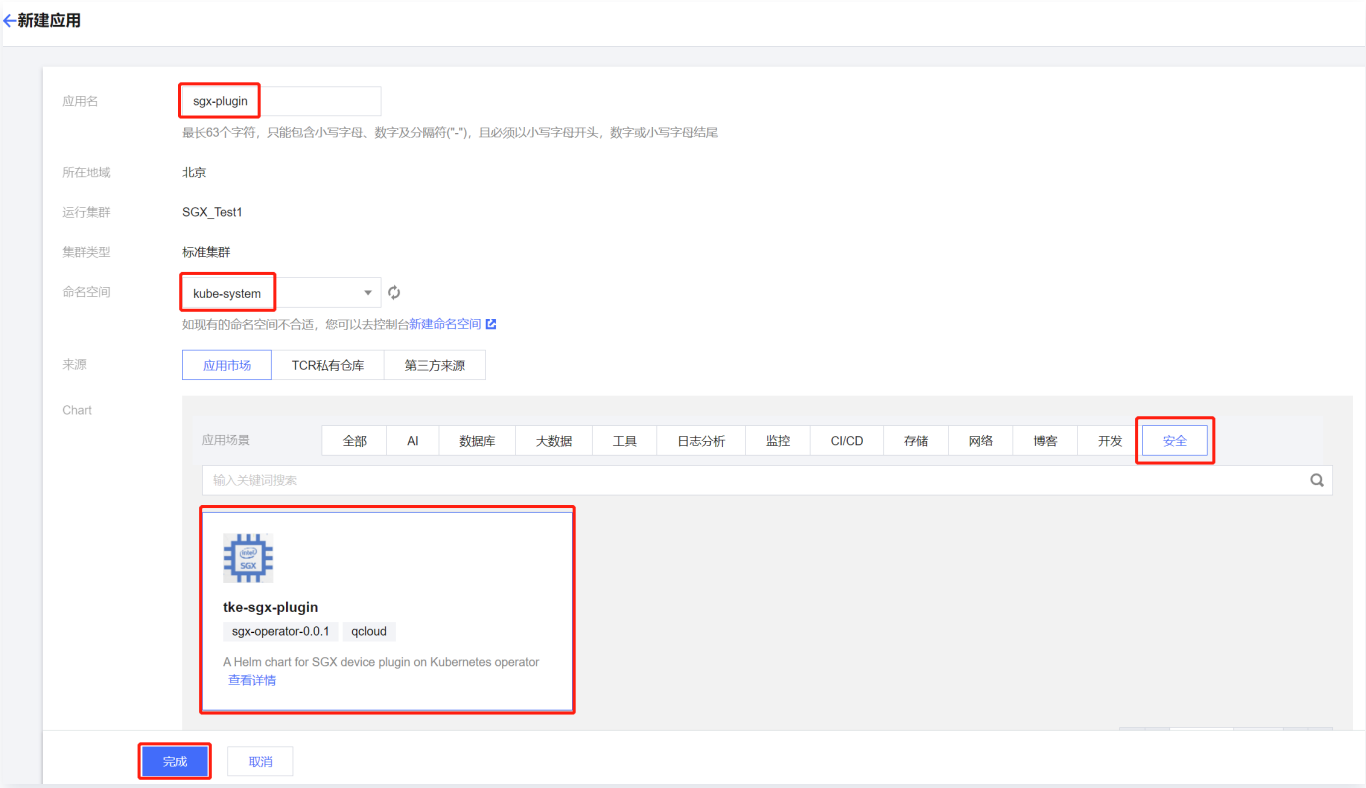
3. 单击**节点管理 > 节点**，可以查看集群节点的详细信息。在集群中使用机密计算，需确保所有节点均具备 SGX 能力，因此所有节点的配置都需要为 M6ce。



步骤2：安装 TKE-SGX 插件

1. 在 应用页面，在顶部选择正确的集群 ID，选择命名空间为**全部**。

2. 检查列表中是否存在 Chart 名称为 tke-sgx-plugin，命名空间为 kube-system 的应用。如存在，则说明已安装了 TKE-SGX 插件；如不存在，则单击**新建**来安装插件。



3. 应用名可自定义，命名空间选择 **kube-system**，在**应用市场 > 安全**中选择 tke-sgx-plugin，单击**完成**。

控制台指南
查看计算节点

最近更新时间：2024-04-24 10:43:51

操作场景

本文介绍如何在机密计算平台中查看运行着飞地的计算节点。

前提条件

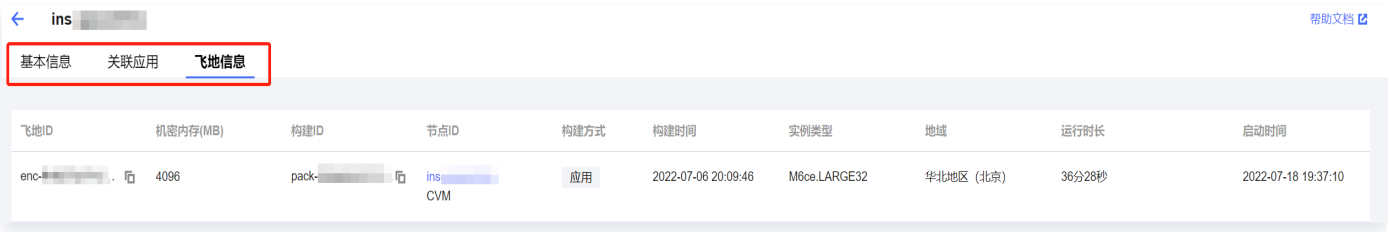
飞地正常运行在腾讯云的 云服务器 CVM 或 容器服务 TKE 服务中。

操作步骤

1. 登录 机密计算平台控制台，在左侧导航栏选择**节点管理**，并选择目标 CCP 实例。

2. 在 CVM 节点中，单击目标 CVM **实例 ID**，可切换 Tab 查看此节点的详细信息，包括飞地信息和对应的机密应用。

3. 单击 **TKE 集群**，单击目标 TKE **集群 ID**，可切换 Tab 查看此集群的详细信息，包括集群节点，飞地信息和对应的机密应用。



查看远程证明

最近更新时间：2024-04-24 10:43:51

操作场景

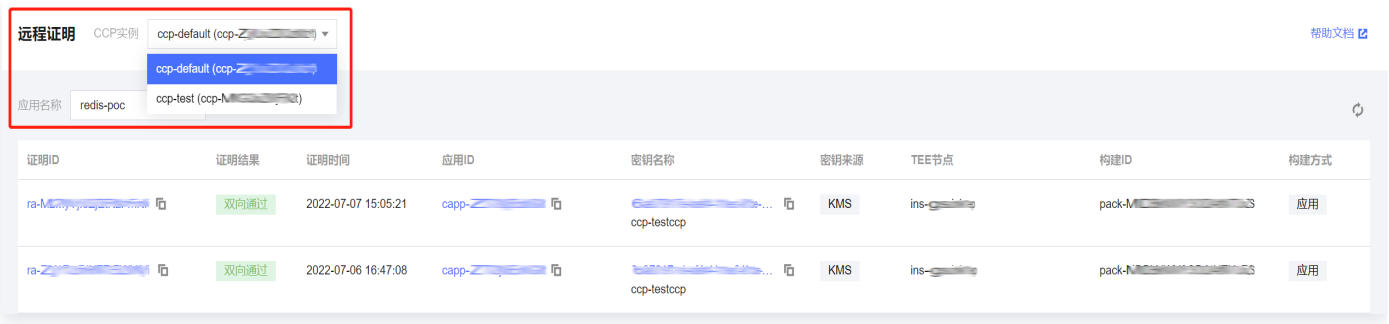
本文介绍如何在机密计算平台中查看飞地执行的远程证明。

前提条件

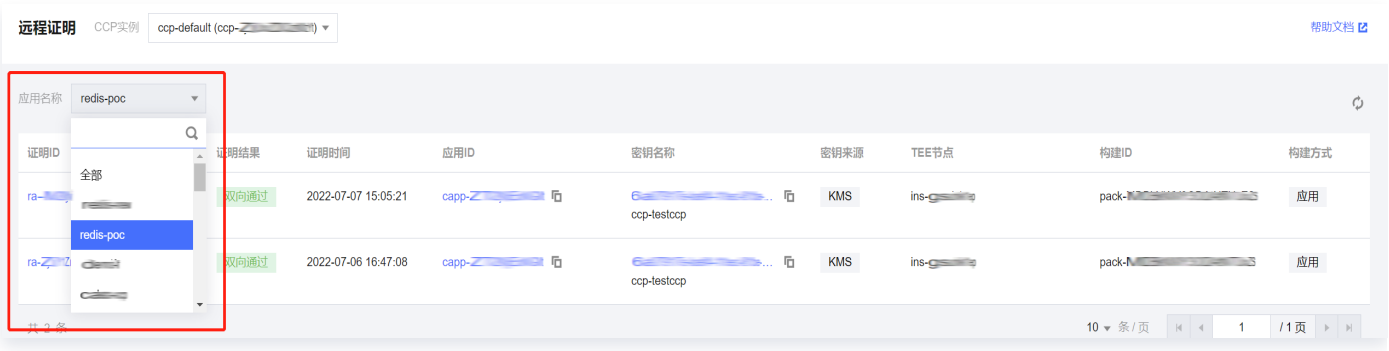
已创建机密计算应用，并运行了机密应用或机密镜像。

操作步骤

1. 登录 机密计算平台控制台，在左侧导航栏选择**远程证明**，并选择目标 CCP 实例。



2. 在远程证明页面，选择要查看的应用名称，列出对应的远程证明记录。



3. 在远程证明页面，单击某条记录的**证明 ID**，进入详细信息页面。
4. 在详细信息页面，单击**关联事件**，可查看远程证明执行的详细过程。

查看资源概览

最近更新时间：2024-04-24 10:43:51

操作场景

本文介绍如何在机密计算平台中查看实例的资源概览。

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。

操作步骤

1. 登录 机密计算平台控制台，在左侧导航栏选择**资源概览**，并选择目标 CCP 实例。

2. 在资源概览页面，将展示与此实例关联的所有资源。

> **注意：**
> 页面展示的内容为当前运行中的资源，若无飞地运行，则地域资源为空。

创建机密应用

最近更新时间：2024-04-24 10:43:51

操作场景

本文介绍如何在机密计算平台中创建机密计算应用。

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。

操作步骤

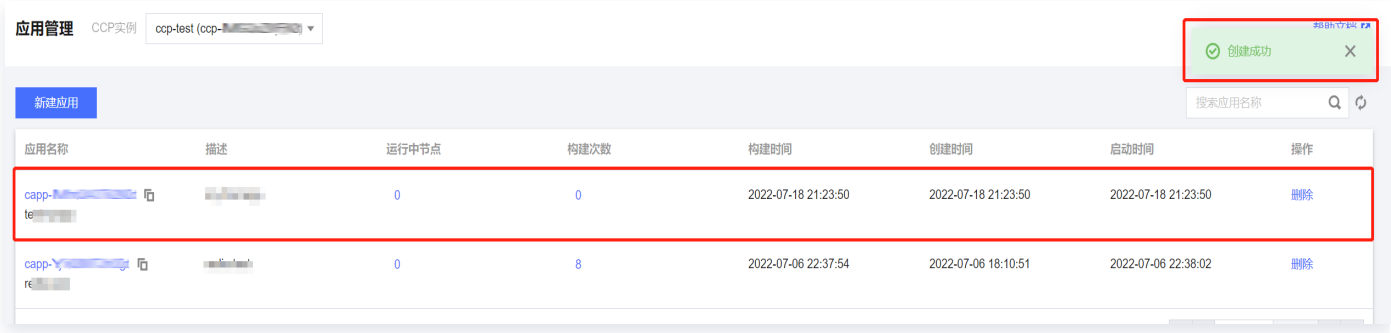
1. 登录 机密计算平台控制台，在左侧导航栏选择**应用管理**，并选择目标 CCP 实例。

2. 在应用管理页面，单击**新建应用**。
3. 在新建应用弹窗中，输入机密应用的相关信息，单击**确定**。

参数说明：

- 应用名称：全局唯一不能重复，由字母、数字、中划线、下划线组合。
- 应用描述：用于描述您所创建的应用数据来源或应用的场景。

4. 提示创建成功，在列表中可见新创建的机密应用。



创建密钥

最近更新时间：2024-04-24 10:43:52

操作场景

本文介绍如何在机密计算平台中创建用于远程证明的密钥管理系统 KMS 密钥。

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。

操作步骤

1. 登录 机密计算平台控制台，在左侧导航栏选择**密钥管理**，并选择目标 CCP 实例。

2. 在密钥管理页面，单击**新建密钥**。
3. 在新建密钥对话框中，输入密钥名称，选择密钥所在区域，单击**确定**。

> **注意：**
> 密钥名称必须以 `ccp-` 开头。

4. 在密钥管理页面，可查看刚创建的密钥。

创建实例

最近更新时间：2024-04-24 10:43:52

操作场景

本文介绍如何在机密计算平台中创建 CCP 实例。

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。

操作步骤

1. 登录 机密计算平台控制台，在左侧导航栏选择**实例**，并单击**新建实例**。

2. 在新建实例弹窗中，输入实例名称，单击**确定**。

> **说明：**
> 实例名称需为2~32字符，且以字母或数字开头结尾，仅允许字母，数字，'-'和'_'。

3. 在实例列表中，可看到刚创建的实例，单击**实例 ID**，可以跳转到对应实例下的应用管理页面。

版权所有：腾讯云计算（北京）有限责任公司

服务授权

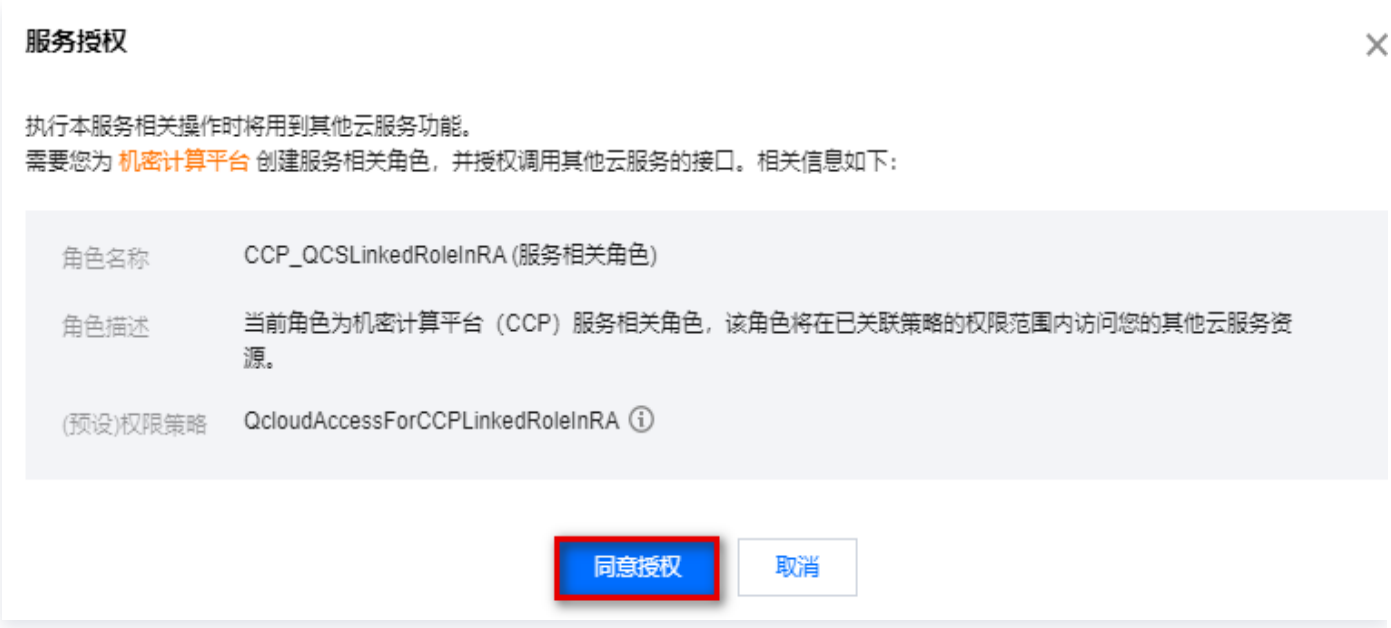
最近更新时间：2024-04-24 10:43:52

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。

操作步骤

1. 登录 机密计算平台控制台，默认进入实例页面，弹出服务授权弹窗。
2. 机密计算平台需要获取用户授权，以访问密钥管理服务 KMS 和容器服务 TKE，若同意请单击**同意授权**。



3. 选择同意授权将为用户创建服务相关角色 `CCP_QCSLinkedRoleInRA` ，用户可以在 访问管理 > **角色**中查看此角色的预设策略，也可根据需要删除此角色。

删除机密应用

最近更新时间：2024-04-24 10:43:52

操作场景

本文介绍如何在机密计算平台中删除机密计算应用。

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。

操作步骤

1. 登录 机密计算平台控制台，在左侧导航栏选择**应用管理**，并选择目标 CCP 实例。

2. 在应用管理页面，选择需要删除的机密应用，单击**删除**。

3. 在弹出的对话框中，单击**确认**。

> **注意：**
> 一旦删除机密应用，所有与该应用相关的记录将丢失，封装的机密应用和机密镜像将无法启动。

4. 提示删除成功，查看列表可以确认指定的机密应用已被删除。

删除密钥

最近更新时间：2024-04-24 10:43:52

操作场景

本文介绍如何在机密计算平台中删除指定密钥。

前提条件

已购买 密钥管理系统 KMS，并授权机密计算平台使用 KMS 服务。

操作步骤

1. 登录 机密计算平台控制台，在左侧导航栏选择**密钥管理**，并选择目标 CCP 实例。

2. 在密钥管理页面，确定需要删除的密钥，单击**删除**。

> **注意：**
> 必须删除所有与密钥关联的应用后，才允许删除该密钥。

3. 在确认删除弹窗中，单击**确认**。

4. 在密钥管理页面的密钥列表中，可以确认指定密钥被删除。

> **注意：**

> 当密钥来源于密钥管理服务 KMS 时，删除该密钥将会禁用密钥且设置为7天计划删除，在计划删除期间将无法创建相同名称的密钥。

删除实例

最近更新时间：2024-04-24 10:43:52

操作场景

本文介绍如何在机密计算平台中删除 CCP 实例。

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。

操作步骤

1. 登录 机密计算平台控制台，在左侧导航栏选择**实例**。
2. 在实例管理页面，选择目录实例，单击**删除**。

> **注意：**
> 必须删除该实例下所有的应用和密钥后，才允许删除该实例。

3. 在确认删除弹窗中，单击**确认**。

4. 在实例列表中，可以确认指定实例被删除。


实例管理
帮助文档
机密计算免费公测中，欢迎试用。
删除成功
使用指南
① 创建实例； ② 创建密钥； ③ 创建应用； ④ 工具下载； ⑤ 打包构建；
1. 在【实例管理】中创建实例
2. 在【密钥管理】中创建密钥
3. 在【应用管理】中创建应用，关联密钥用于远程证明
4. 在【工具下载】中下载最新版本的ccpcli
5. 使用pack命令构建机密应用和镜像，参考文档
新建实例
搜索实例名称
实例ID/名称
应用数量/应用上限
节点数量/节点上限
飞地数量
服务版本
创建时间
到期时间
状态
操作
18/100
1/100
1
公测版
2022-07-05 18:19:16
永久有效
正常服务
删除

命令行指南
安装 CCPCLI

最近更新时间：2024-04-24 10:49:11

操作场景

本文介绍如何安装机密计算命令行工具 CCPCLI。

步骤1：获取 CCPCLI 下载命令

1. 登录机密计算平台控制台，在左侧导航栏选择**工具下载**。
2. 在工具下载页面，选择合适的版本，单击右侧的**复制下载命令**后，可见复制成功提示。

步骤2：下载 CCPCLI

登录 Linux 系统，然后将**步骤1**中获取的下载命令黏贴到命令行中执行，即可完成 CCPCLI 下载。

步骤3：安装 CCPCLI

解压安装包，执行脚本进行安装。

> **注意：**
> 请使用 root 权限进行安装。

```
$ tar jxvf ccp-1.0.0.tar.bz2
$ cd ccp-1.1.0
$ ./deploy.sh -i
source ~/.bashrc
```

步骤4：检查安装

测试 CCPCLI，使用 version 命令查看版本号，成功显示版本号说明安装正确。

```
$ ccp-cli version
1.1.0
```

封装机密镜像

最近更新时间：2024-04-24 10:49:11

操作场景

本文介绍如何使用 CCPCLI 封装机密镜像。

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：创建机密应用

创建机密应用，指定有效的远程证明密钥。详情请参见控制台指南中的 创建机密应用 。

步骤2：安装 CCPCLI 命令行工具

在信任的设备中，安装 CCPCLI 命令行工具，详情请参见 安装 CCPCLI 。

步骤3：准备目标镜像

在本示例中，我们使用 dockerfile 创建一个包含 redis 服务的 ubuntu 镜像作为目标镜像。

```
$ echo 'FROM ubuntu:20.04' > Dockerfile
$ echo 'RUN apt-get update' >> Dockerfile
$ echo 'RUN apt-get -y install redis' >> Dockerfile
$ docker build -t myredis .

$ docker images
REPOSITORY    TAG       IMAGE ID       CREATED          SIZE
myredis       latest    0f261dd3de17   36 seconds ago   111MB
ubuntu        20.04     2b4cba85892a   3 days ago       72.8MB
```

步骤4：封装目标镜像

使用 CCPCLI 的 pack 指令来封装机密镜像，其中 `--capp-id` 需要设置为 步骤1 创建的机密应用的 ID，`--app-image` 需要设置为 步骤3 创建的目标镜像名称，其他参数配置可查询 命令行指南-常用命令 。

> ⚠ **注意：**
> - 生成的机密镜像名称为 `sec_<image_name>` ，如果存在同名的镜像，可使用 `--force` 参数覆盖。
> - 生成的 `sec_<镜像名称>` 即为封装的机密镜像。

版权所有：腾讯云计算（北京）有限责任公司

```
$ ccp-cli pack --app-entry="/usr/bin/redis-server" \
        --memsize=2048M --thread=32 \
        --tmpl=default \
        --secret-id=<user_secret_id> \
        --secret-key=<user_secret_key> \
        --capp-id=<application_id> \
        --app-image=<image_name> \
        --app-type=image
...
Successfully built 96d181069a7e
Successfully tagged sec_<image_name>:latest
```

封装机密应用

最近更新时间：2024-04-24 10:49:11

操作场景

本文介绍如何使用 CCPCLI 封装机密应用。

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：创建机密应用

创建机密应用，并指定有效的远程证明密钥。详情请参见控制台指南中的 创建机密应用 。

步骤2：安装 CCPCLI 命令行工具

在信任的设备中，安装 CCPCLI 命令行工具，详情请参见 安装 CCPCLI 。

步骤3：准备目标应用

在本示例中，我们使用 Redis 服务作为目标应用，并使用 apt 命令来简化安装。

```
$ sudo apt-get update
$ sudo apt-get install -y redis
$ sudo /etc/init.d/redis-server stop
```

步骤4：封装目标应用

使用 CCPCLI 的 pack 指令来封装机密镜像，其中 `--capp-id` 需要设置为 步骤1 创建的机密应用的 ID，其他参数配置可查询 命令行指南-常用命令 。

```
$ ccp-cli pack --app-entry="/usr/bin/redis-server" \
        --memsize=2048M --thread=32 \
        --tmpl=default \
        --secret-id=<user secret id> \
        --secret-key=<user secret key> \
        --capp-id=<application_id> \
        --app-type=app
```

请保存生成的 {appName}.manifest.sgx、{appName}.sig、{appName}.token 三个文件，用于后续运行机密应用，{appName} 指在 步骤1 中创建机密计算应用的名称。

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

启动机密镜像

最近更新时间：2024-04-24 10:49:11

操作场景

本文介绍如何启动机密镜像。

前提条件

- 已封装了机密镜像。
- 已配置了机密计算环境。

步骤1：准备容器运行时

本示例中使用 Docker 管理容器，用户可根据 Docker 官方的 安装文档 进行安装。

步骤2： 拉取机密镜像

本示例中使用 DockerHub 作为镜像仓库，使用以下命令拉取机密镜像，其中 `{sec_image}` 为机密镜像名称。

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

$ docker pull {sec_image}
```

步骤3：运行机密镜像

使用 Docker 命令启动镜像前，需要配置参数将 sgx 相关设备映射入容器，参考以下命令。

```
# 本命令仅作为demo，在实际使用redis时，请务必设置访问密码
$ docker run -ti --device /dev/sgx_enclave \
                 --device /dev/sgx_provision \
                 {sec_image}
```

启动机密应用

最近更新时间：2023-10-08 14:37:33

操作场景

本文介绍如何启动机密应用。

前提条件

- 已封装了机密应用。
- 已配置了机密计算环境。

步骤1：准备机密应用文件

将封装机密应用生成的 sgx、.sig、.token 文件准备到当前目录。

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

步骤2：运行机密应用

使用以下命令启动机密应用，其中 `{appName}` 为机密应用名称，`{Parameters}` 为应用程序的启动参数。

```
$ ccp-cli run {appName} {Parameters}
```

常见命令

最近更新时间：2024-04-24 10:49:11

操作场景

本文档主要针对 ccp 客户端命令行工具（ccp-cli）进行相关参数说明。

主命令参数说明

参数名称	描述
genrsa	生成用于机密应用或机密镜像签名的私钥
help	查看 ccp-cli 帮助
info	查看机密计算环境相关信息（sgx/manifest）
pack	构建机密应用或机密镜像
run	运行机密应用或机密镜像
tmpl	管理机密计算模板
version	查看当前命令行工具版本

子命令参数说明

genrsa

您可以使用此命令生成用户唯一私钥，对机密应用或机密镜像进行签名。

```
ccp-cli genrsa
参数: 无
```

pack

您可以使用此命令构建您的机密应用或机密镜像。

ccp-cli pack	参数

capp-id	指定 Web 端新建应用时返回的应用 ID
secret-id	指定用户访问云 API 的凭据 ID
secret-key	指定用户访问云 API 的凭据
role	指定用户访问云 API 的角色列表
pri	指定用户私钥
app-type	指定用户应用类型。app：机密应用；image：机密镜像。默认 app
tmpl	指定 manifest 模板，支持多个模板列表，模板之间使用逗号分割，默认使用 default
app-image	指定机密镜像转换时用户的应用镜像
app-entry	指定用户应用入口
app-cmd	指定机密镜像转换时用户的应用参数
heartbeat-cycle	指定机密计算应用运行时上报心跳的周期(秒)
capi-target	指定云 API 访问地址
force	指定机密镜像转换时是否强制覆盖已有镜像
log	指定 gramine 日志级别(none|error|warning|debug|trace|all)，默认 error
aslr	指定是否禁用地址空间布局随机化(ASLR)，默认 false
palsize	指定 gramine 自身内存使用大小，默认64M
stacksize	指定每个 gramine 进程中每个线程的栈大小，默认256K，单位 K(KiB)、M(MiB)、G(GiB)
breaksize	指定每个 gramine 进程的最大 brk 大小，默认246K，单位 K(KiB)、M(MiB)、G(GiB)

版权所有：腾讯云计算（北京）有限责任公司

eventfd	指定是否允许系统调用 eventfd() 和 eventfd2()，默认 false
sigterm	指定是否允许一次性将 SIGTERM 信号注入 gramine
root	指定 gramine 根目录，默认为当前主机执行目录，模板目前默认配置为'/'
mount	指定主机需要 mount 到 gramine 的路径映射关系，格式: [:, ...]，默认'/':'/'
tmpfs	指定 sgx enclave 内存临时文件路径，主机不存在，随 encalve 产生和销毁，格式: [, ...]
start	指定 gramine 内部起始(当前工作)目录，默认为--root 目录
debug	指定 sgx enclave 是否为 debug 模式（true：debug 模式 enclave；false：release 模式 encalve），默认 false
memsize	指定 sgx enclave 大小，默认256M
nonpie	指定是否支持 non-PIE，默认 false
thread	指定 sgx enclave 内可以创建的最大线程数
exitless	指定 sgx enclave 外创建的 RPC 线程数，默认0
avx	指定是否开启 cpu avx 特性，默认 false
avx512	指定是否开启 cpu avx512特性，默认 false
mpx	指定是否开启 cpu mpx 特性，默认 false
pkru	指定是否开启 cpu pkru 特性，默认 false
allow	指定允许无条件创建或加载到 sgx enclave 中的文件或目录，格式: [, ...]，文件或目录状态读写
trust	指定 sgx enclave 中主机信任文件或目录，构建机密应用进行 hash 并在运行时校验，文件或目录状态只读
protect	指定 sgx enclave 加密存储文件或目录，构建机密应用时指定，运行时透明读写，文件或目录状态读写，目前不支持
filekey	指定 sgx enclave 加密存储文件或目录的密钥，安全性差不建议使用，目前不支持
ra	指定是否开启 dcap 远程证明，默认 false

run

您可以使用此命令运行您的机密应用或机密镜像。

```
ccp-cli run <application-name> <parameter-list>
参数:
    <application-name>: web端新建应用时指定的应用名称
    <parameter-list>:   用户应用运行时需要的参数列表
```

tmpl

您可以使用此命令管理您的机密计算模板。

ccp-cli tmpl	参数
tmpl	指定基础模板，支持多个模板列表，模板之间使用逗号分割，默认使用 default
out	指定输出的新模板
force	指定是否强制覆盖已有模板
log	指定 gramine 日志级别(none|error|warning|debug|trace|all)，默认 error
aslr	指定是否禁用地址空间布局随机化(ASLR)，默认 false
palsize	指定 gramine 自身内存使用大小，默认64M
stacksize	指定每个 gramine 进程中每个线程的栈大小，默认256K，单位 K(KiB)、M(MiB)、G(GiB)
breaksize	指定每个 gramine 进程的最大 brk 大小，默认246K，单位 K(KiB)、M(MiB)、G(GiB)
eventfd	指定是否允许系统调用 eventfd() 和 eventfd2()，默认 false
sigterm	指定是否允许一次性将 SIGTERM 信号注入 gramine
root	指定 gramine 根目录，默认为当前主机执行目录，模板目前默认配置为'/'
mount	指定主机需要 mount 到 gramine 的路径映射关系，格式: [:, ...]，默认'/':'/'
tmpfs	指定 sgx enclave 内存临时文件路径，主机不存在，随 encalve 产生和销毁，格式: [, ...]

版权所有：腾讯云计算（北京）有限责任公司

start	指定 gramine 内部起始(当前工作)目录，默认为--root 目录
debug	指定 sgx enclave 是否为 debug 模式（true：debug 模式 enclave；false：release 模式 encalve），默认 false
memsize	指定 sgx enclave 大小，默认256M
nonpie	指定是否支持 non-PIE，默认 false
thread	指定 sgx enclave 内可以创建的最大线程数
exitless	指定 sgx enclave 外创建的 RPC 线程数，默认0
avx	指定是否开启 cpu avx 特性，默认 false
avx512	指定是否开启 cpu avx 512特性，默认 false
mpx	指定是否开启 cpu mpx 特性，默认 false
pkru	指定是否开启 cpu pkru 特性，默认 false
allow	指定允许无条件创建或加载到 sgx enclave 中的文件或目录，格式: [, ...]，文件或目录状态读写
trust	指定 sgx enclave 中主机信任文件或目录，构建机密应用进行 hash 并在运行时校验，文件或目录状态只读
protect	指定 sgx enclave 加密存储文件或目录，构建机密应用时指定，运行时透明读写，文件或目录状态读写，目前不支持
filekey	指定 sgx enclave 加密存储文件或目录的密钥，安全性差不建议使用，目前不支持
ra	指定是否开启 dcap 远程证明，默认 false

info

您可以使用此命令查询您的机密计算节点相关信息。

```
// 查询机密计算运行节点环境信息
ccp-cli info sgx
参数: 无

// 查询机密应用或镜像的manifest配置信息
ccp-cli info manifest
```

参数:
--app-image: 指定用户机密镜像
--app-name: 指定用户机密应用名称

version

您可以使用此命令查询 ccp 客户端命令行工具版本信息。

ccp-cli version
参数: 无