云加密机

操作指南

腾讯云

文档目录

操作指南
新建实例

最近更新时间：2025-01-24 15:04:52

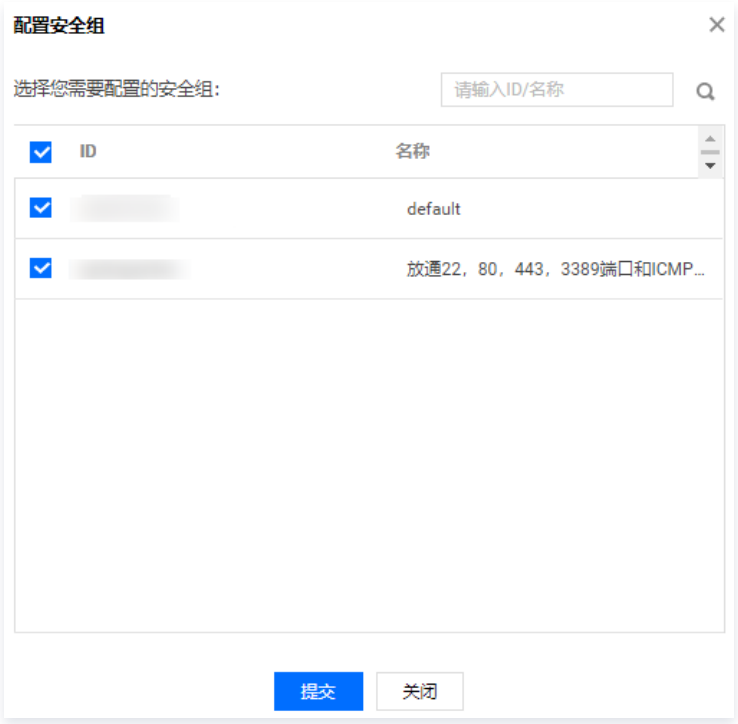
本文档为您介绍如何新建云加密机服务实例和配置安全组。

操作步骤

1. 登录 云加密机控制台 ，在控制台页面上方选择实例的可用地域，单击**新建**，进入云加密机购买页面。

2. 在购买页面选择和确认云加密机相关配置，配置详细说明，请参见云加密机 购买方式 。
3. 云加密机实例新建完成后，即可在 云加密机控制台 首页，查看该实例，同时可在该实例右侧操作栏，单击**配置安全组**，进入配置安全组页面。

4. 在配置安全组页面，勾选您需要配置的安全组，单击**提交**，即可完成安全组配置，具体安全组配置方式，请参见 配置安全组 。



使用实例

最近更新时间：2024-05-17 15:02:31

业务应用可依据接口文档通过 API 方式进行服务调用，也可以在应用主机上安装 TACSP 安全代理软件，通过本地代理方式调用加密服务实例。

- **加密服务接口调用服务**
  根据业务应用情况及使用的 VSM 类型，选择对应的 API 接口。
  - **金融数据密码机 EVSM 接口规范**：提供 Java 版本、C 版本接口类型。
  - **通用服务密码机 GVSM 接口规范**：支持 JCE 接口、PKCS#11接口或者 SDF 接口。
  - **签名验证服务器 SVSM 接口规范**：提供 Java 版本、C 版本接口类型。
  - **托管物理密码机 GHSM 接口规范**：支持 JCE 接口、PKCS#11接口或者 SDF 接口。
- **安全代理 TACSP 本地代理访问**
  安全代理客户端 TACSP 用于实现应用系统本地代理访问 VSM，并可用于搭建业务层高可用架构。

> **说明**
> 如需使用接口文档，可以 提交工单 联系我们，详情请参见 工具及接口文档获取指引 。

管理实例
VSM 管理主机配置

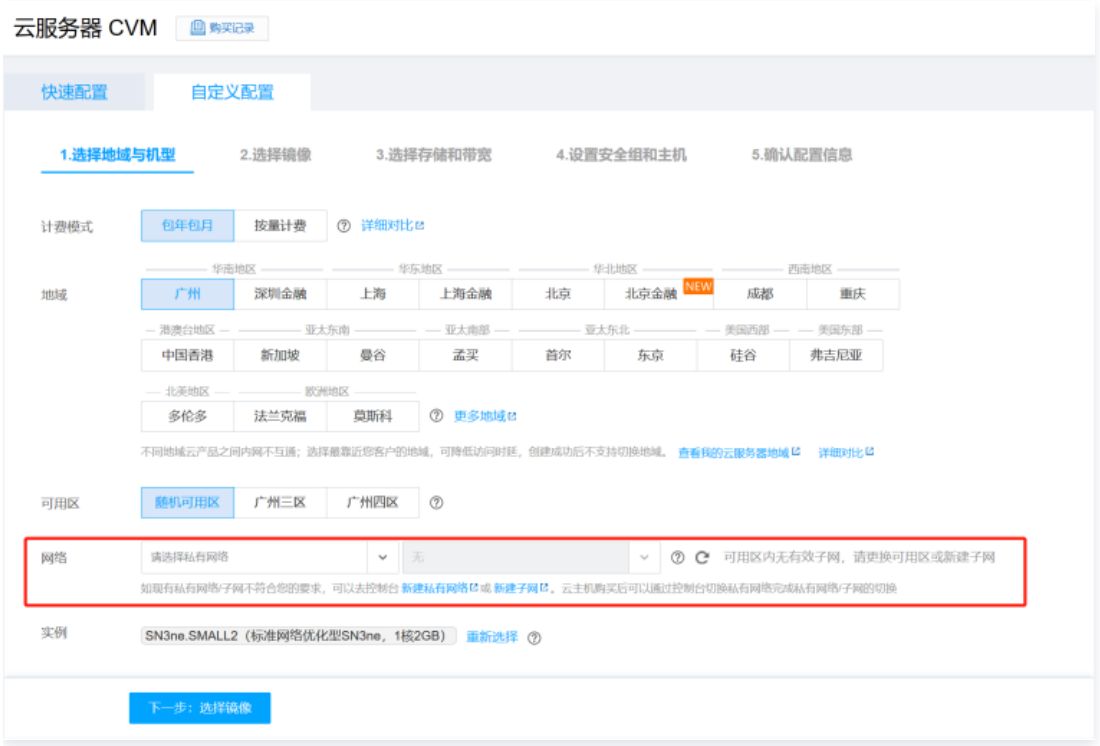
最近更新时间：2024-05-17 15:02:31

使用云加密机实例，需先通过与数据加密实例在同一个 VPC 内的 CVM 作为 VSM 管理主机，通过远程登录对 VSM 进行管理。

> **注意：**
> 如果所在的 VPC 下无可用的 CVM，您需要选购一台按量计费的 Windows 机型 CVM 作为管理服务器，并将该 CVM 加入指定 VPC 网络中，建议选择 CVM 最低配置即可。

VSM 管理主机选购配置

登录 云服务器购买页面，选择**自定义配置** > **按量付费模式**。

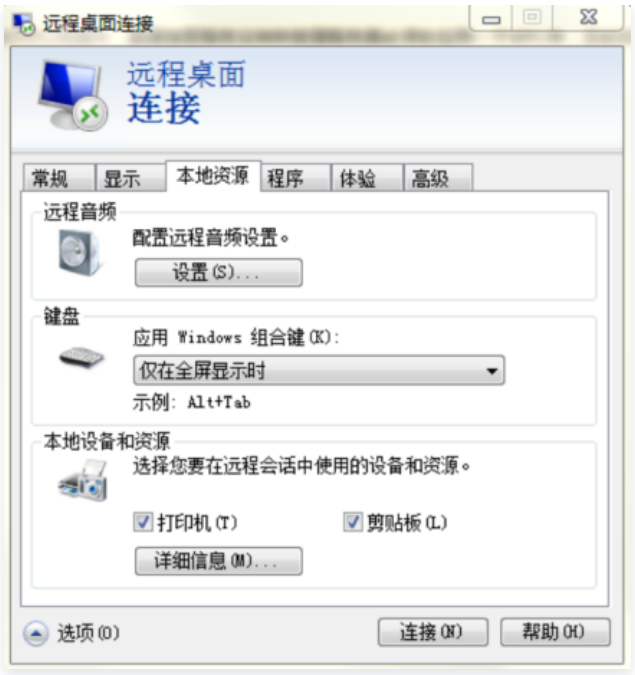


- **地域可用区**：根据业务情况选择，目前仅支持北京二区、广州三区、上海四区。
- **私有网络**：业务应用、云加密机实例、管理主机 CVM（管理 VSM 实例）需配置同一 VPC 网络下。
- **选择镜像**：操作系统推荐 Windows 机型 CVM 最低配置。

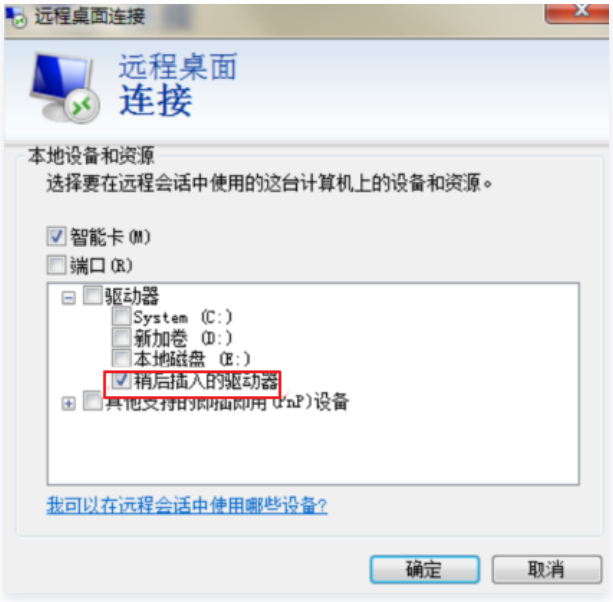
VSM 管理主机配置

远程登录购买的云服务器 CVM，登录前并做如图的配置，这样就可以在 VSM 管理主机中使用身份认卡 USBKey 了。

1. 在**本地资源**中，打开**详细信息**。



2. 勾选**稍后插入的驱动器**。



VSM 服务实例配置

最近更新时间：2024-05-17 15:02:31

通过 VSM 管理主机及提供的 VSM 管理工具，使用身份认证卡 USBKey 完成管理员身份注册，以管理员身份对 VSM 进行初始化、操作授权、配置及其它管理操作。其中，EVSM 提供基于 C/S 的 VsmManager 进行 VSM 的实例管理，GVSM、SVSM 提供基于 B/S 的管理终端（HTTPS）。

- EVSM 管理工具及使用手册
  将 VsmManager 安装到 VSM 管理主机 CVM 中，对 EVSM 加密服务进行管理配置。
- GVSM 管理工具及使用手册
  登录管理主机 CVM，以 B/S 方式对 GVSM 加密服务进行管理配置。

工具及接口文档获取指引

最近更新时间：2024-05-20 17:47:12

获取身份认证卡 Ukey

您可以 提交工单，反馈您的交易单号和收货地址。我们会尽快为您安排身份认卡 USBKey 的寄送，请确保您的联系方式正确且畅通。

获取 VSM 软件及文档工具

您可以 提交工单，获取相应 VSM 管理工具、使用手册、接口文档以及业务开发手册等工具包。

> **注意：**
> 不同 VSM 类型所需的管理工具及相应资料各有不同。

金融数据密码机 EVSM

- **VSM 管理主机：**安装 VsmManager。
- **加密服务接口：**根据业务侧研发情况，选择 Java 版本或者 C 版本。

通用服务器密码机 GVSM

- **VSM 管理主机：**安装 VsmManager。
- **加密服务接口：**根据业务侧研发情况，选择 JCE 接口、PKCS#11 接口或者 SDF 接口。

签名验证服务器 SVSM

- **VSM 管理主机：**安装身份认卡 USBKey 驱动。
- **加密服务接口：**根据业务侧研发情况，选择 Java 版本或者 C 版本。

托管物理密码机 GHSM

- **VSM 管理主机：**安装 VsmManager。
- **加密服务接口：**根据业务侧研发情况，选择 JCE 接口、PKCS#11接口或者 SDF 接口。

标签
编辑标签

最近更新时间：2024-05-17 15:02:31

本文档将指导您如何对资源进行编辑标签的操作。

使用限制

使用标签内容（标签键及标签值）的限制条件，请参见标签的 使用限制 。

操作步骤

1. 登录 云加密机 控制台.
2. 在云加密机实例列表左上方可以切换不同地区，根据需求查看并编辑相关地域的云加密机实例标签。

- **单个凭据编辑标签**

  2.1 在加密机实例列表中，找到需编辑标签的云加密机实例，选择其右侧操作栏，单击**编辑标签**。

  2.2 在弹出的 “编辑标签” 窗口中，根据实际需求进行添加或删除标签。

> **说明：**
> 关于如何使用标签，请参见 使用标签管理实例 。

- **批量编辑标签**

  2.1 在加密机实例列表中，勾选需编辑标签的云加密机实例，单击**编辑标签**。

  2.2 在弹出的 “编辑标签” 窗口中，根据实际需求进行添加或删除标签。

> **说明：**
> 关于如何使用标签，请参见 使用标签管理实例 。

使用标签管理实例

最近更新时间：2024-05-17 15:02:31

本文档将指导您如何设置标签并通过标签筛选加密机实例。

操作场景

- 标签用于从不同维度对资源进行分类及权限管理。
- 在 云加密机 中，标签主要用于管理加密机实例。
- 在云加密机实例中添加标签，可方便用户对云加密机实例进行分类和跟踪管理，同时可以按照标签统计对应云加密机实例的使用情况。

使用限制

使用标签（标签键及标签值）的限制条件，请参见标签的 使用限制 。

操作步骤

设置标签

1. 登录 云加密机控制台 。
2. 在云加密机实例列表左上方可以切换不同地区，根据需求查看并编辑相关地域的云加密机实例标签。

3. 找到需编辑标签的云加密机实例，在右侧操作栏，单击**编辑标签**。

4. 在弹出的 “编辑标签” 窗口中设置标签，如下图所示：

5. 单击**确定**，系统将提示修改成功。

通过标签筛选加密机实例

1. 登录 **云加密机** 控制台。
2. 在云加密机实例列表左上方可以切换不同地区，根据需求查看并编辑相关地域的云加密机实例标签。

3. 在云加密机实例列表上方的搜索框中，选择以“标签”作为筛选条件，输入筛选内容，单击回车即可。
例如，若您希望筛选出 owner 为 alex 的密钥，可输入标签：owner:alex，单击回车即可。

访问管理
概述

最近更新时间：2024-10-17 20:30:11

如果您需要使用云加密机（CloudHSM）、私有网络（VPC）、云服务器、数据库等服务，且这些服务由不同人进行管理，但都共享您的云账号密钥，将存在以下问题：

- 您的密钥由多人共享，泄密风险高。
- 您无法限制其它人的访问权限，易产生误操作造成安全风险。

访问控制（CAM） 用于管理腾讯云账户下资源访问权限，您可以通过 CAM 的身份管理和策略管理功能，控制各子账号的资源操作权限。
例如，您的主账户下有个主密钥，您只想让子账号 A 使用该主密钥，而让子账号 B 不能使用，则可以通过在 CAM 中配置策略，对子账号的权限进行控制。
如果您不需要对子账户进行 CloudHSM 相关资源的访问控制，您可以跳过此章节，跳过此章节并不影响您对文档中其余部分的理解和使用。

CAM 基本概念

主账号通过给子账号绑定策略实现授权，策略设置可精确到多个（API、资源、用户、用户组、允许、拒绝及条件）维度。

- **账号**
  - **主账号**：腾讯云资源归属及资源使用计量计费的基本主体，可登录腾讯云服务。
  - **子账号**：由主账号创建的账号，有确定的身份 ID 和身份凭证，且能登录到腾讯云控制台。主账号可以创建多个子账号（用户）。**子账号默认不拥有资源，必须由所属主账号进行授权。**
  - **身份凭证**：包括登录凭证和访问证书两种，登录凭证是指用户登录名和密码，访问证书是指云 API 密钥（SecretId 和 SecretKey）。
- **资源与权限**
  - **资源**：资源是云服务中被操作的对象，如一个 CloudHSM 服务实例、云服务器实例、COS 存储桶及 VPC 实例等。
  - **权限**：权限是指允许或拒绝某些用户执行某些操作。默认情况下，主账号拥有其名下**所有**资源的访问权限，而子账号**没有**主账号下任何资源的访问权限。
  - **策略**：策略是定义和描述一条或多条权限的语法规范。主账号通过将策略关联到用户/用户组完成授权。

相关文档

- 如需了解策略和用户之间关系，请参见 策略 。
- 如需了解策略的基本结构，请参见 元素参考 。
- 如需了解还有哪些产品支持 CAM，请参见 支持 CAM 的产品 。

如需了解更多，请参见 访问管理（CAM） 产品文档。

后续步骤

- 如需创建子账号，并授权子账号管理云加密机（CloudHSM）的权限，请参见 子账号管理 。
- 如需创建访问控制策略，请参见 创建访问控制策略 。

子账号管理

最近更新时间：2024-05-17 15:02:31

本文为您介绍如何创建子账号，并授权子账号管理云加密机（CloudHSM）的权限。

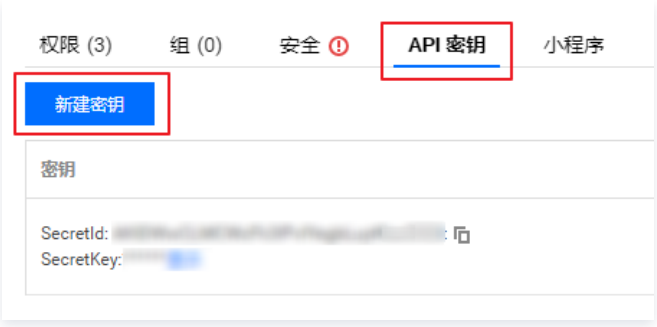
操作步骤

步骤1：创建子账号

1. 使用主账号登录腾讯云 访问管理 CAM 控制台，在左侧导航中，选择**用户** > **用户列表**。
2. 在“用户列表”页面下，单击**新建用户**，即可创建子账号。

步骤2：创建 API 密钥

1. 在 用户列表 中，单击子账号名称，进入子账号详情页。
2. 在子账号详情页，选择**API 密钥** > **新建密钥**，即可创建 SecretId 和 SecretKey，通过该 API 密钥用来访问 CloudHSM。



步骤3：授权子账号

对于新创建的子账号，通过授权 CloudHSM 策略，即可允许该子账号访问 CloudHSM。

1. 在子账号详情页，选择**权限** > **关联策略**，进入添加策略页面。

2. 在添加策略页面，单击**从策略列表中选取策略关联**，选择合适的 CloudHSM 策略，选择**下一步** > **确定**，即可授权子账号 CloudHSM 权限。

> **说明：**
> - 如果您希望用户拥有查询和管理云加密机实例的权限，您可以对该用户使用名称为：QcloudCloudhsmFullAccess 的策略

- 如果您希望用户拥有查询云加密机实例的权限，但是不具有修改云加密机属性的权限，您可以对该用户使用名称为：QcloudCloudhsmReadOnlyAccess 的策略。

策略列表 （共2条，已选择0条）

策略名	描述	引用次数	策略类型
QcloudCloudhsmFullAccess	云加密机（cloudhsm）全读写访问权限	1	预设策略
QcloudCloudhsmReadOnlyAccess	云加密机（cloudhsm）只读权限	1	预设策略

支持按住 shift 键进行多选

创建访问控制策略

最近更新时间：2024-10-17 20:30:11

本文档将为您介绍如何创建访问控制策略。

可授权的资源类型

资源级权限是能够指定用户对哪些资源具有执行操作的能力。
云加密机部分接口支持使用资源级权限对密钥进行操作，可控制允许用户何时执行操作或是否允许用户使用特定资源，云加密机目前可授权的资源类型如下：

资源类型	授权策略中资源描述方法
所有的密钥资源	`qcs::cloudhsm:$Region:uin/$Uin:vsm/*`
主账号为$Uin，资源ID为$ResourceId的资源	`qcs::kms:$region:uin/$uin:key/creatorUin/$creatorUin/*`

其中以$为前缀的单词均为代称：

- $uin：指代主账号 ID。
- $region：指代地域。
- $creatorUin：指代创建该资源的账号 ID。
- $keyId：指代密钥 ID。

支持资源级授权的 API 列表

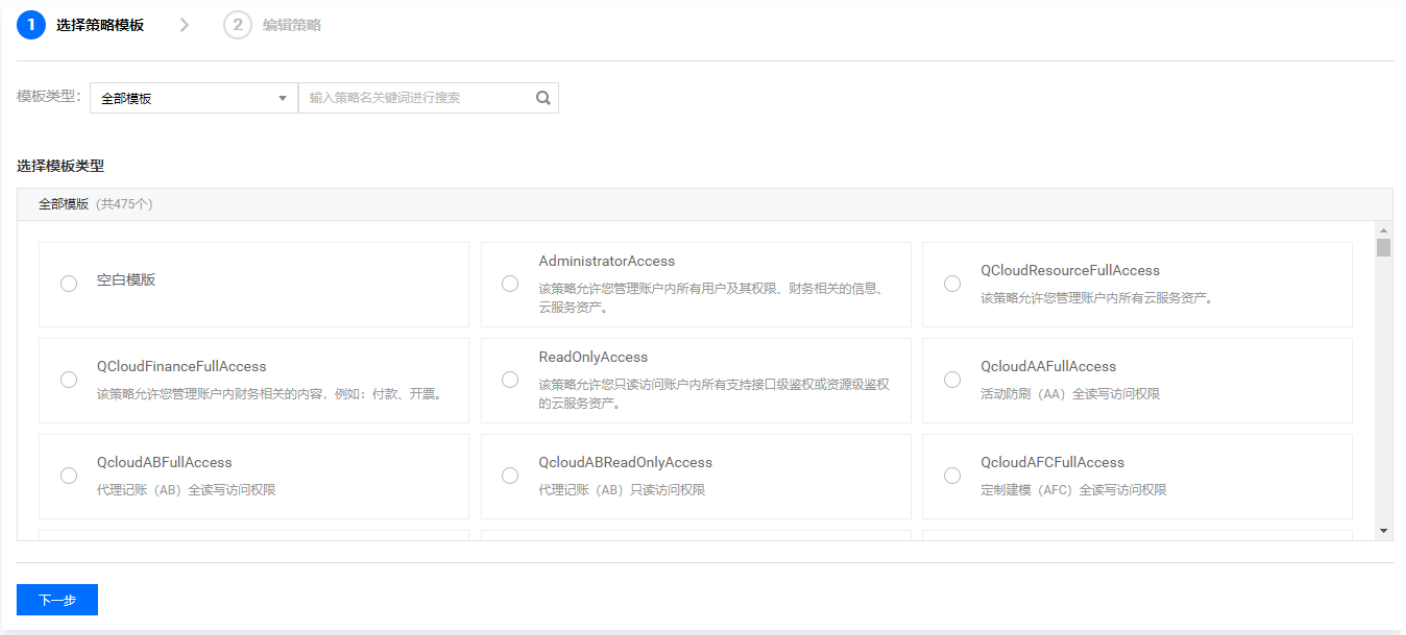
云加密机部分接口支持资源级授权，您可以指定子账号拥有特定资源的接口权限。

API 接口	描述信息
DescribeVsmAttributes	获取资源详情
ModifyVsmAttributes	修改资源详情
DescribeVsms	获取资源列表

创建策略

1. 登录 访问管理 控制台。
2. 在左侧导航中，单击**策略**，进入“策略”页面。
3. 在“策略”页面，选择**新建自定义策略** > **按策略语法创建**，进入策略创建页面。

4. 根据需求选择合适的策略模板，单击**下一步**。



5. 在编辑策略页面，输入策略名称和策略内容，策略内容可参见下方示例。

```
{
 "version": "2.0",
 "statement": [
     {
         "effect": "allow",
         "resource": [
             "qcs::cloudhsm::uin/2942368751:vsm/hsm-tounrmcg",
             "qcs::cloudhsm::uin/2942368751:vsm/hsm-iteb2nt0"
         ],
         "action": [
             "cloudhsm:*"
         ]
     },
     {
         "effect": "allow",
         "resource": [
             "*"
         ],
         "action": [
             "cloudhsm:DescribeHSMBySubnetId",
             "cloudhsm:DescribeHSMByVpcId",
             "cloudhsm:DescribeVpc",
             "cloudhsm:InquiryPriceBuyVsm",
             "cloudhsm:DescribeUsg",
             "cloudhsm:DescribeUsgRule",
             "cloudhsm:DescribeSubnet"
         ]
     }
 ]
}
```

6. 单击**完成**，即可创建相应策略。