云加密机（CloudHSM）

产品文档

腾讯云TCE

版权所有：腾讯云金融专区

文档目录

产品简介
产品概述

最近更新时间: 2024-10-17 17:10:00

云加密机（Cloud Hardware Security Module，CloudHSM）基于国密局认证的物理加密机，利用虚拟化技术，提供弹性、高可用、高性能的数据加密和密钥管理等云上数据安全服务，符合国家监管合规要求，满足金融，互联网等行业加密需求，保障用户的业务数据隐私安全。

优势	腾讯云金融专区云加密机	传统物理密码机	开源软件加密
符合国密局标准	服务底层使用经国家密码管理局检测认证的硬件密码机，通过虚拟化技术，帮助用户满足数据安全方面的监管合规要求，保护云上业务数据的隐私。	采用符合国家和行业规范的物理密码机提供数据加密服务。	无法保证符合国家和行业规范，无法用于金融，政务等行业，存在较大的合规风险。
弹性扩展	采用云服务密码机的虚拟化技术，可根据您的业务需要，弹性的增加和缩减后端的虚拟实例，从容应对业务高峰压力，节约资源和成本。	不具备弹性伸缩的特点，只能以物理机为单位进行业务扩容，容易造成资源和成本的浪费。	弹性扩展能力依赖于提供加密服务的服务端。
安全可靠	采用国家密码管理局批准的硬件芯片实现各类密码算法；提供与实体密码设备相同的功能与接口，可完全兼容传统应用并方便其向云端迁移。	采用国内和国际的加密算法，保证数据加密安全；支持数据密钥的管理和备份，可以进行物理件的密钥同步；只能采用物理机设备的形式保证业务的可用性，容易造成资源浪费。	无法保证加密算法的加密安全性，加密密钥无法安全的备份和管理，高可靠高可用等性能需依托于加密服务器，自建和维护成本高。
方便云上使用	可以方便和您腾讯云金融专区上的业务和产品结合，在同一个 VPC 网络下，实现可靠，高效的数据加密和密钥管理。	无法在腾讯云金融专区上部署，不能与腾讯云金融专区上的业务和产品进行无缝对接。	自行部署和维护。

版权所有：腾讯云金融专区

产品功能

最近更新时间: 2024-10-17 17:10:00

设备厂商：TASS

金融数据密码机 EVSM

云加密机满足《GM/T 0045-2016 金融数据密码机技术规范》要求，可用于金融支付领域，确保金融数据安全，并符合金融磁条卡、IC 卡业务特点，主要实现 PIN 加密、PIN 转加密、MAC 产生和校验、数据加解密、签名验证以及密钥管理等密码管理功能的云加密实例。

加密算法

- **对称算法**：SM1/SM4/DES/3DES/AES128/AES256
- **非对称算法**：SM2、RSA(1024-2048)、ECC(NIST P192/P256、SECP192/256、BRAINPOOLP256、FRP256、X25519)
- **摘要算法**：SM3、SHA1/SHA256/SHA384

基础服务功能

- 支持雷卡相关指令集。
- 支持金融 IC 卡相关指令集。
- 支持国密算法的金融业务应用。
- 支持 PBOC2.0/3.0 规范。
- 支持 EMV 规范的应用。
- 支持 GP 规范、TSM 规范、ESIM规范的应用。
- 支持交通一卡通规范的应用。
- 支持其它各类行业 IC 卡的应用。
- 支持通用数据加解密、签名验签、摘要计算、密钥管理等服务功能。

性能

- 数据通讯协议：TCP/IP
- 最大并发连接：64

版权所有：腾讯云金融专区

- SM1 加密运算性能：600次/秒
- SM2 密钥产生性能：4000次/秒
- SM2 签名运算性能：3000次/秒
- SM2 验签运算性能：2000次/秒
- RSA2048 密钥产生性能：10对/秒
- RSA2048 公钥运算性能：3500次/秒
- RSA2048 私钥运算性能：400次/秒
- SM3 摘要运算性能：5000次/秒
- SM4 加密运算性能：5000次/秒
- AES128 运算性能：7000次/秒
- AES256 运算性能：6000次/秒

通用服务器密码机 GVSM

云加密机满足《GM/T 0030-2014 服务器密码机技术规范》要求，提供国际和国内通用的密码服务接口，能独立或并行为多个应用实体提供密码服务和密钥管理服务的云加密实例。

加密算法

- **对称算法**：SM1/SM4/DES/3DES/AES128/AES256
- **非对称算法**：SM2、RSA(1024-4096)、ECC(NIST P256、BRAINPOOLP256、FRP256)
- **摘要算法**：SM3、SHA1/SHA256/SHA384

基础服务功能

- 支持国密 GM/T 0018 密码设备应用接口规范。
- 支持 PKCS#11 接口规范。
- 支持 SUN JCE 接口规范。
- 支持国密算法的 PKI 业务应用。
- 支持通用数据加解密、签名验签、摘要计算、密钥管理等服务功能。

版权所有：腾讯云金融专区

性能

- 数据通讯协议：TCP/IP
- 最大并发连接：64
- SM1加密运算性能：600次/秒
- SM2 密钥产生性能：4000次/秒
- SM2 签名运算性能：3000次/秒
- SM2 验签运算性能：2000次/秒
- RSA2048 密钥产生性能：10对/秒
- RSA2048 公钥运算性能：3500次/秒
- RSA2048 私钥运算性能：400次/秒
- SM3 摘要运算性能：5000次/秒
- SM4 加密运算性能：5000次/秒
- AES128 运算性能：7000次/秒
- AES256 运算性能：6000次/秒

设备厂商：CETC

金融数据密码机 EVSM

云加密机满足GM/T 0045《金融数据密码机技术规范》要求，可用于银行金融业务系统，尤其是跨行的ATM/POS交易系统。除此之外，它还可广泛用于社保、电力、公交、证券、商贸、邮电、税收、保险等金融业务系统中。

加密算法

- **对称算法**：SM1/SM4/ZUC/3DES/AES等
- **非对称算法**：SM2/ RSA[1024~4096]等
- **摘要算法**：SM3/ SHA256/SHA512等

基础服务功能

支持国际标准算法，支持国密SM1/SM2/SM3/SM4算法，满足PBOC3.0规范。其主要功能如下：

- 密钥生成、存储、分发、注入和销毁等全生命周期管理
- 数据加解密
- 数字签名、验签
- 消息摘要
- 消息完整性保护（MAC计算和验证）
- 个人身份码（PIN）保护（PINBLOCK加密、转换、验证）
- CVV（卡校验值）、PVV（PIN校验值）计算
- 交易正确性验证（TAC计算和验证）
- IC卡交易（ARQC、ARPC）

性能

- 数据通讯协议：TCP/IP
- 最大并发连接：4096
- SM1加密运算性能：33.5万次/秒
- SM2密钥产生性能：20万次/秒
- SM2签名运算性能：20万次/秒
- SM2验签运算性能：8.5万次/秒
- RSA2048密钥产生性能：120对/秒
- RSA2048签名运算性能：1.05万次/秒
- RSA2048验签运算性能：16万次/秒
- SM3运算性能：67万次/秒
- SM4加密运算性能：68万次/秒
- 3DES运算性能：54万次/秒

版权所有：腾讯云金融专区

通用服务器密码机 GVSM

云加密机满足GM/T 0030《服务器密码机技术规范》要求，可用于各级党政单位，以及互联网、金融、能源等行业，提供密钥安全管理、安全密码运算等管理功能。

加密算法

- **对称算法**：SM1/SM4/ZUC/3DES/AES等
- **非对称算法**：SM2/ RSA[1024~4096]等
- **摘要算法**：SM3/ SHA256/SHA512等

基础服务功能

- 支持SDF(GB/T 36322-2018《信息安全技术 密码设备应用接口规范》)接口规范。
- 支持JCE接口规范。
- 支持PKCS#11接口规范。
- 支持提供安全管理、安全通信、访问控制等服务功能。

性能

- 数据通讯协议：TCP/IP
- 最大并发连接：4096
- SM1加密运算性能：5.3Gbps，57万次/秒
- SM2密钥产生性能：20.8万次/秒
- SM2签名运算性能：20.8万次/秒
- SM2验签运算性能：8.5万次/秒
- RSA2048密钥产生性能：160对/秒
- RSA2048签名运算性能：1.6万次/秒
- RSA2048验签运算性能：25万次/秒
- SM3运算性能：9.2Gbps，80万次/秒
- SM4加密运算性能：8.6Gbps，57万次/秒

版权所有：腾讯云金融专区

- 3DES运算性能：4.2Gbps，93万次/秒

设备厂商：SANSEC

金融数据密码机 EVSM

云加密机EVSM满足《GM/T0045 金融数据密码机技术规范》要求，可用于金融领域（包括银行、证券、P2P金融等）应用的密码运算功能需求，例如发卡系统、POS系统等，提供了服务管理、密钥管理、设备组管理等管理功能。

加密算法

- **对称算法**：SM1、SM4、AES、3DES
- **非对称算法**：RSA、SM2
- **摘要算法**：SM3、SHA1、SHA256、SHA384、SHA512

基础服务功能

- 支持国际Racal相关指令集、自定义金融接口。
- 支持密钥分散、PIN加密、PIN转换、PIN/MAC/CVV/TAC生成及验证等服务功能。

性能

- 数据通讯协议：TCP
- 最大并发连接：64
- SM1 加密运算性能：1800次/秒
- SM4 加密运算性能：1800次/秒
- AES128 加密运算性能：6500次/秒
- AES256 加密运算性能：6400次/秒
- SM2密钥产生性能：3700次/秒
- SM2签名运算性能：3100次/秒
- SM2验签运算性能：2500次/秒
- RSA2048密钥产生性能：3对/秒

- RSA2048公钥运算性能：3500次/秒
- RSA2048私钥运算性能：200次/秒
- SM3摘要运算性能：6000次/秒

通用服务器密码机 GVSM

云加密机GVSM满足《GM/T0030 服务器密码机技术规范》要求，可用于各种行业应用的密码运算需求，例如身份认证、数据保护、SSL通信加速和密钥保护等，提供服务管理、密钥管理、设备组管理等管理功能。

加密算法

- **对称算法**：SM1、SM4、AES、3DES
- **非对称算法**：RSA、SM2
- **摘要算法**：SM3、SHA1、SHA256、SHA384、SHA512

基础服务功能

- 支持GM/T0018密码设备应用接口规范、
- 支持JCE接口规范、
- 支持PKCS#11接口规范、
- 支持数据加密/解密、数据签名/验签、数据杂凑、数据MAC等服务功能。

性能

- 数据通讯协议：TCP
- 最大并发连接：64
- SM1 加密运算性能：4000次/秒
- SM4 加密运算性能：5900次/秒
- AES128 加密运算性能：6200次/秒
- AES256 加密运算性能：6000次/秒
- SM2密钥产生性能：3700次/秒
- SM2签名运算性能：3100次/秒

- SM2验签运算性能：2500次/秒
- RSA2048密钥产生性能：3对/秒
- RSA2048公钥运算性能：3400次/秒
- RSA2048私钥运算性能：240次/秒
- SM3摘要运算性能：6000次/秒

签名验签服务器 SVSM

云加密机SVSM满足《GM/T0029签名验签服务器技术规范》要求，可用于各种基于证书的签名业务相关功能需求，比如CA系统、认证系统、证书验证、大量数据或文件的加密传输和身份认证等，提供容器管理、证书管理、密钥管理、设备组管理等管理功能。

加密算法

- **对称算法**：SM1、SM4、AES
- **非对称算法**：RSA、SM2
- **摘要算法**：SM3、SHA1、SHA256、SHA384、SHA512

基础服务功能

- 支持GM/T0019通用密码服务接口规范。
- 支持PKCS#1、PKCS#7数据签名/验签、PKCS#7数字信封封装和解封、证书验证等服务功能。

性能

- 数据通讯协议：TCP
- 最大并发连接：64
- SM2 RAW签名运算性能：2800次/秒
- SM2 RAW验签运算性能：2300次/秒
- SM2 Attach签名运算性能：1200次/秒
- SM2 Attach验签运算性能：1400次/秒
- SM2 Dettach签名运算性能：1200次/秒
- SM2 Dettach验签运算性能：1400次/秒

版权所有：腾讯云金融专区

- 2048位RSA RAW签名运算性能：240次/秒
- 2048位RSA RAW验签运算性能：2900次/秒
- 2048位RSA Attach签名运算性能：1200次/秒
- 2048位RSA Attach验签运算性能：1400次/秒
- 2048位RSA Dettach签名运算性能：1200次/秒
- 2048位RSA Dettach验签运算性能：1400次/秒

产品优势

最近更新时间: 2024-10-17 17:10:00

云加密机拥有以下产品优势：

- **符合国家和行业标准的数据加密算法**
  - 对称加密算法：SM1，SM4，DES，AES。
  - 非对称加密算法：SM2，RSA（1024-2048）ECC 等算法。
  - 摘要算法：SM3，MD5，SHA1，SHA256，SHA384 等算法。

- **权责分离** 云加密机提供权责分离的管理体系和严格的身份认证方法，保障权限安全可控；您可完全把控密钥管理的权限和应用访问的权限，除被授权人或者授权应用外，其它人或者其它应用都无法使用密钥和数据。

- **弹性扩展** 采用云服务密码机的虚拟化技术，可根据您的业务需要弹性增加和缩减后端的虚拟实例，从容应对业务高峰压力，节约资源和成本。

- **便捷管理** 提供与实体密码设备相同的功能与接口，可完全兼容传统应用并方便其向云端迁移。数据加密实例与VPC策略绑定，可以方便和您腾讯云金融专区上的业务结合，实现可靠、高效的数据加密和密钥管理服务。

版权所有：腾讯云金融专区

应用场景

最近更新时间: 2024-10-17 17:10:00

云加密机可应用于以下场景：

敏感数据加密

面临挑战

- 黑客攻破网络，拖库导致数据泄露风险。
- 用户非法访问，篡改数据、泄露数据风险。

解决方案

- 数据在数据库存储是通过 VSM 加密后存储，保证数据的机密性。
- 数据在数据库存储时，通过 VSM 进行完整性校验保证数据的完整性。
- 加密密钥采用 VSM 生成和管理的方式，保证了加密密钥的安全性。

客户价值

- 杜绝了明文数据被泄露和篡改的风险，提升了系统的健壮性和客户价值。

应用领域

- 可应用于政务、电商、门户、Web 站点等各类包含大量个人敏感信息的系统应用。

金融支付加密

面临挑战

- 支付业务都在强监管要求范围内，必须采取硬件密码设备保证系统安全性。
- 必须保证支付数据在传输、存储过程中完整性、保密性，支付身份认证和支付过程的不可否认性等。

解决方案

- 通过 VSM 生成和管理支付终端、支付渠道的主密钥和工作密钥。
- 通过 VSM 提供完整周期的 PIN 加密传输和验证，传输报文的完整验证。
- 通过 VSM 提供支付介质或者用户身份的认证。

客户价值

- 符合监管合规要求，保障了业务的安全性。

应用领域

- 可应用于 POS 收单、互联网支付、预付费卡支付等各类第三方支付应用中。

企业信息系统加密

面临挑战

- 企业各类信息系统存有大量企业资产、财务报表、人员信息等敏感数据，存在泄漏风险。
- 企业各类信息系统存有大量用户信息，需要认证企业用户身份和权限。

解决方案

- 通过 VSM 生成和管理各类型企业信息系统所需的对称和非对称密钥管理。
- 通过 VSM 提供用户身份认证服务。
- 通过 VSM 提供敏感数据加密服务。

客户价值

- 保障企业资产安全性，防止非法用户授权的访问。

应用领域

- 可应用于大型企业和事业单位。

电子票据

面临挑战

- 电子票据类的应用用户身份的真实性需要安全手段保证。
- 票据数据的生产，传输，存储过程中的完整性和安全性需要进行保证。

解决方案

- 通过 VSM 生成和管理各类型的对称密钥和非对称密钥。
- 通过 VSM 提供对称和非对称密钥的数据加密、解密、转加密等服务。
- 通过 VSM 提供证书签发、数据签名、数据验签、身份认证等服务。

客户价值

- 符合监管合规要求，保障了电子化安全性，促进电子化业务发展。

应用领域

- 可用于电子病例、电子发票、电子合同、电子保单等各类应用。
- 可用于银行、保险、政务、企业等多种领域。

快速入门
使用流程

最近更新时间: 2024-10-17 17:10:00

步骤说明

1. **新建服务实例**：获取内测资格后，可在云加密机控制台新建云加密机实例，详情请参见文档 新建实例。

2. **管理服务实例**：选择与数据加密实例位于同一个 VPC 内的云服务器 CVM 作为 VSM 管理主机，管理 VSM 实例，详情请参见文档 管理实例。

3. **调用服务实例**：根据接口文档及应用代理软件，通过 API 或本地代理的方式调用云加密机。详情参见文档 使用实例。

新建实例

最近更新时间: 2024-10-17 17:10:00

登录腾讯云金融专区云加密机控制台，新建加密服务实例，进行配置。

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】，进入实例配置页面。

2. 在实例配置页面根据需求进行配置，配置页面共包括以下字段：

地域可用区：根据业务情况选择地域可用区。

VSM 类型：根据不同的业务场景选择金融数据密码机 EVSM 或通用服务器密码机 GVSM，同时下方会列出所选 VSM 对应的运算性能和加密算法。

私有网络：为云加密机实例绑定所属的 VPC 网络、VPC 交换机、以及私网 IP 地址。

业务应用和云加密机实例需配置同一 VPC 下。

购买数量：根据业务情况，确定购买一个或是多个加密服务实例。

结算方式：云加密机以服务实例为单位，包年包月预付费模式进行售卖。

续费方式：用户可以决定在账户余额充足时是否可以自动续费。

3. 配置完成后，单击【立即购买】，根据实际费用进行付费即可完成新建实例。

4. 云加密机实例新建完成后，即可在云加密机控制台首页，查看到该实例。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。

5. 在配置安全组页面，勾选您需要的安全组，单击【提交】，即可完成安全组配置，具体安全组配置方式。

版权所有：腾讯云金融专区

管理实例
VSM管理主机配置

最近更新时间: 2024-10-17 17:10:00

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。

配置云加密机管理主机

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: 2024-10-17 17:10:00

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。

使用实例

最近更新时间: 2024-10-17 17:10:00

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。
- **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。

加密服务网络配置

最近更新时间: 2024-10-17 17:10:00

1. 新建数据加密服务实例后，可以根据需要在数据加密服务控制台 ，找到需要配置安全组的实例所在行，单击操作栏中的【配置安全组】，进入配置页面进行配置。

2. 在您电脑的“远程桌面连接”窗口中，单击【详细信息】。

3. 勾选【稍后插入的驱动器】

4. 远程登录购买的 CVM，在虚拟主机中使用 UKey 。

5. 请根据腾讯云金融专区提供给您的操作文档初始化您的 UKey 和服务实例，并根据发放的开发手册进行业务开发。

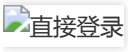
角色授权

最近更新时间: 2024-10-17 17:10:00

1 直接登录

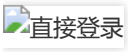
1.1打开 VsmManager.exe 文件

单击【系统】>【VSM 登录管理】，如下图：



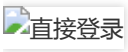
1.2 登录 VSM 管理系统

在弹出的页面中，输入VSM 的 IP 地址及端口号（端口号固定为8013），单击【登录】即可登录 VSM 管理系统，如下图：



1.3 登录成功

管理工具面板上显示登录成功状态信息，登录按钮变为不可用，证明成功登录，如下图：



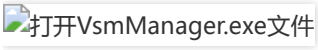
用户在没有注册管理员的情况下直接登录系统，不可以对 VSM 进行原始初始化和恢复初始化工作，即不可以更改 VSM 的主密钥，仅可以在测试主密钥的环境下进行密钥管理。

2 管理员登录

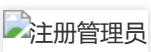
2.1 注册管理员

2.1.1 打开 VsmManager.exe 文件

单击【系统】>【VSM 登录管理】，在弹出的页面中，输入VSM 的 IP 地址及端口号（端口号固定为8013），如下图：



2.1.2 注册管理员

单击【注册管理员】，在弹出的页面中，选择插入的 UKEY 并单击【确定】，如下图： 

2.1.3 输入口令

输入口令单击【确定】完成管理员的注册。VSM 出厂时默认的 UKEY 管理登录口令为"12345678"。

2.2 登录系统

2.2.1 选择管理员 KEY

在登录界面单击【登录】，在 KEY 列表中选择管理员 KEY 并确定，如下图：

2.2.2 输入管理员口令

输入管理员口令，单击【确定】完成登录。如下图：

2.2.3 添加管理员KEY

- **建议**：在系统登录成功后，请另外添加一把管理员 KEY，以防管理员 KEY 丢失或损坏，将无法正常使用 VSM 管理工具对加密机进行管理操作。添加管理员 KEY 的方法如下：

在【设备管理】中找到【UKEY 管理】，如下图：

插入一把空 KEY 并选择后，单击【添加管理员】，如下图：

输入口令，完成管理员 KEY 的添加。

网络配置

最近更新时间: 2024-10-17 17:10:00

- 新建完数据加密服务实例后，可以根据需要到安全组页面配置安全组，勾选您需要的安全组，单击【提交】。
- 业务应用、云加密机实例、安装管理 VSMmanager 实例需配置同一 VPC 下，在购买云加密机实例 以及 CVM 时候注意私有网络配置。

选项配置

最近更新时间: 2024-10-17 17:10:00

创建加密服务实例后，登录腾讯云金融专区数据加密服务管理控制台，定位到已购买的加密服务实例，开始配置。

- **购买数量：根据业务情况，确定购买一个或是多个加密服务实例。**
- **地域可用区：根据业务情况选择。**
- **VSM 类型：根据不用的业务场景选择金融数据密码机 EVSM 或通用服务器密码机 GVSM。**

VSM类型

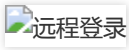
- **私有网络：为数据加密服务实例绑定所属的 VPC 网络、VPC 交换机、以及私网 IP 地址。**

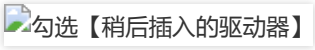
私有网络

初始化实例
初始化VSM实例

最近更新时间: 2024-10-17 17:10:00

客户购买加密服务后，通过远程桌面访问 VPC 中的 CVM，在 CVM 上安装 VSM 客户端管理工具，打开工具，输入数据加密服务实例的 IP 及端口号开始实例管理。远程登录购买的 CVM，登录前并做如下配置，即可以在虚拟主机中使用 UKey 。

1. 在【本地资源】中，打开【详细信息】。 

2. 勾选【稍后插入的驱动器】。 

3. 通过远程桌面访问 VPC 中的 CVM，在 CVM 上安装 VSM 客户端管理工具，打开工具，输入数据加密服务实例的 IP 及端口号开始实例管理。
4. 请根据给您发放的使用文档初始化您的 USB Key 和服务实例，并根据发放的开发手册进行业务开发。

常见问题

最近更新时间: 2024-10-17 17:10:00

如何部署云加密机？

- 如果您的业务部署在与云加密机相同的可用区，可以将云加密机实例加入该区的 VPC 中，直接通过内网网络使用。
- 其他区域可以通过 VPN 通道使用云加密机。

内测时，单账号能申请多少云加密机实例？

单个账号最多可以申请5个实例，如果您的需求超过5个实例，请您联系工程师进行申请。

云加密机客户端必须选用 Windows Server 2008 操作系统吗?

云加密机实例管理客户端必须为 Windows 系统，考虑到兼容性问题，推荐您使用 Windows Server 2008 操作系统。

如何获取身份识别卡（USB key）？

您购买云加密机实例后，需要使用身份识别卡（USB key）来进行实例的管理。 请您登录腾讯云金融专区官网，填写申请单并留下您的交易单号和收货地址，我们会尽快为您安排身份识别卡（USB key）的寄送。

词汇表

最近更新时间: 2024-10-17 17:10:00

硬件安全模块

硬件安全模块（Hardware Security Module，HSM）是以硬件形式提供安全加密服务的服务模块。

云加密机实例

云加密机实例是以硬件安全模块为基础、以虚拟化服务器形式提供的云加密服务实例。

UKey

UKey（USB Key）是与具体云服务密码机对应的唯一身份识别认证设备。结合 UKey 与服务实例管理客户端，完成对服务实例的密钥管理。

私有网络

私有网络（Virtual Private Cloud，VPC）是能够为您提供全方位网络解决方案、稳定、灵活、安全的云上私有网络空间。

虚拟安全模块

虚拟安全模块（virtual security module，VSM）是以虚拟化形式提供安全加密服务的服务模块。

版权所有：腾讯云金融专区

API文档
数据加密服务（cloudhsm）
版本（2019-11-12）
API概览

最近更新时间: 2024-10-18 10:38:24

API版本

V3

其他接口

接口名称	接口功能
DescribeRegions	获取地域列表
DescribeSubnet	查询子网列表
DescribeSupportedHsm	获取当前地域所支持的设备列表
DescribeUsg	获取用户安全组列表
DescribeUsgRule	获取安全组详情
DescribeVpc	查询私有网络列表
DescribeVsmProperty	获取VSM参数信息列表

虚拟加密机实例相关接口

接口名称	接口功能
CreateResource	创建VSM
DescribeHSMBySubnetId	通过SubnetId获取Hsm资源数
DescribeHSMByVpcId	通过VpcId获取Hsm资源数
DescribeVsmAttributes	获取VSM属性
DescribeVsms	获取用户VSM列表
InquiryPriceBuyVsm	询价
ModifyVsmAttributes	修改VSM属性

版权所有：腾讯云金融专区

接口名称	接口功能
TerminateVsm	退还虚拟加密机

调用方式
接口签名v1

最近更新时间: 2024-10-18 10:38:24

tcecloud API 会对每个访问请求进行身份验证，即每个请求都需要在公共请求参数中包含签名信息（Signature）以验证请求者身份。 签名信息由安全凭证生成，安全凭证包括 SecretId 和 SecretKey；若用户还没有安全凭证，请前往云API密钥页面申请，否则无法调用云API接口。

1. 申请安全凭证

在第一次使用云API之前，请前往云API密钥页面申请安全凭证。 安全凭证包括 SecretId 和 SecretKey：

- SecretId 用于标识 API 调用者身份
- SecretKey 用于加密签名字符串和服务器端验证签名字符串的密钥。
- 用户必须严格保管安全凭证，避免泄露。

申请安全凭证的具体步骤如下：

1. 登录tcecloud管理中心控制台。
2. 前往云API密钥的控制台页面
3. 在云API密钥页面，点击【新建】即可以创建一对SecretId/SecretKey

注意：开发商帐号最多可以拥有两对 SecretId / SecretKey。

2. 生成签名串

有了安全凭证SecretId 和 SecretKey后，就可以生成签名串了。以下是生成签名串的详细过程：

假设用户的 SecretId 和 SecretKey 分别是：

- SecretId: AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE
- SecretKey: Gu5t9xGARNpq86cd98joQYCN3EXAMPLE

注意：这里只是示例，请根据用户实际申请的 SecretId 和 SecretKey 进行后续操作！

以云服务器查看实例列表(DescribeInstances)请求为例，当用户调用这一接口时，其请求参数可能如下:

参数名称	中文	参数值
Action	方法名	DescribeInstances
SecretId	密钥Id	AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE
Timestamp	当前时间戳	1465185768
Nonce	随机正整数	11886
Region	实例所在区域	ap-guangzhou

参数名称	中文	参数值
InstanceIds.0	待查询的实例ID	ins-09dx96dg
Offset	偏移量	0
Limit	最大允许输出	20
Version	接口版本号	2017-03-12

2.1. 对参数排序

首先对所有请求参数按参数名的字典序（ ASCII 码）升序排序。注意：1）只按参数名进行排序，参数值保持对应即可，不参与比大小；2）按 ASCII 码比大小，如 InstanceIds.2 要排在 InstanceIds.12 后面，不是按字母表，也不是按数值。用户可以借助编程语言中的相关排序函数来实现这一功能，如 php 中的 ksort 函数。上述示例参数的排序结果如下:

```
{
'Action' : 'DescribeInstances',
'InstanceIds.0' : 'ins-09dx96dg',
'Limit' : 20,
'Nonce' : 11886,
'Offset' : 0,
'Region' : 'ap-guangzhou',
'SecretId' : 'AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE',
'Timestamp' : 1465185768,
'Version': '2017-03-12',
}
```

使用其它程序设计语言开发时，可对上面示例中的参数进行排序，得到的结果一致即可。

2.2. 拼接请求字符串

此步骤生成请求字符串。 将把上一步排序好的请求参数格式化成"参数名称"="参数值"的形式，如对 Action 参数，其参数名称为 "Action" ，参数值为 "DescribeInstances" ，因此格式化后就为 Action=DescribeInstances 。 **注意：“参数值”为原始值而非url编码后的值。**

然后将格式化后的各个参数用"&"拼接在一起，最终生成的请求字符串为:

```
Action=DescribeInstances&InstanceIds.0=ins-09dx96dg&Limit=20&Nonce=11886&Offset=0&Region=ap-guangzhou&SecretId=AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE&Timestamp=1465185768&Version=2017-03-12
```

2.3. 拼接签名原文字符串

此步骤生成签名原文字符串。 签名原文字符串由以下几个参数构成:

1. 请求方法: 支持 POST 和 GET 方式，这里使用 GET 请求，注意方法为全大写。
2. 请求主机:查看实例列表(DescribeInstances)的请求域名为：cvm.finance.cloud.tencent.com。实际的请求域名根据接口所属模块的不同而不同，详见各接口说明。
3. 请求路径: 当前版本云API的请求路径固定为 / 。
4. 请求字符串: 即上一步生成的请求字符串。

签名原文串的拼接规则为: 请求方法 + 请求主机 +请求路径 + ? + 请求字符串

示例的拼接结果为：

```
GETcvm.finance.cloud.tencent.com/?Action=DescribeInstances&InstanceIds.0=ins-09dx96dg&Limit=20&Nonce=11886&Offset=0&Region=ap-guangzhou&SecretId=AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE&Timestamp=1465185768&Version=2017-03-12
```

2.4. 生成签名串

此步骤生成签名串。 首先使用 HMAC-SHA1 算法对上一步中获得的**签名原文字符串**进行签名，然后将生成的签名串使用 Base64 进行编码，即可获得最终的签名串。

具体代码如下，以 PHP 语言为例:

```
$secretKey = 'Gu5t9xGARNpq86cd98joQYCN3EXAMPLE';
$srcStr = 'GETcvm.finance.cloud.tencent.com/?Action=DescribeInstances&InstanceIds.0=ins-09dx96dg&Limit=20&Nonce=11886&Offset=0&Region=ap-guangzhou&SecretId=AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE&Timestamp=1465185768&Version=2017-03-12';
$signStr = base64_encode(hash_hmac('sha1', $srcStr, $secretKey, true));
echo $signStr;
```

最终得到的签名串为:

```
EliP9YW3pW28FpsEdkXt/+WcGeI=
```

使用其它程序设计语言开发时，可用上面示例中的原文进行签名验证，得到的签名串与例子中的一致即可。

3. 签名串编码

生成的签名串并不能直接作为请求参数，需要对其进行 URL 编码。

如上一步生成的签名串为 EliP9YW3pW28FpsEdkXt/+WcGeI= ，最终得到的签名串请求参数（Signature）为：EliP9YW3pW28FpsEdkXt%2f%2bWcGeI%3d，它将用于生成最终的请求 URL。

注意：如果用户的请求方法是 GET，或者请求方法为 POST 同时 Content-Type 为 application/x-www-form-urlencoded，则发送请求时所有请求参数的值均需要做 URL 编码，参数键和=符号不需要编码。非 ASCII 字符在 URL 编码前需要先以 UTF-8 进行编码。

注意：有些编程语言的 http 库会自动为所有参数进行 urlencode，在这种情况下，就不需要对签名串进行 URL 编码了，否则两次 URL 编码会导致签名失败。

注意：其他参数值也需要进行编码，编码采用 RFC 3986。使用 %XY 对特殊字符例如汉字进行百分比编码，其中"X"和"Y"为十六进制字符（0-9 和大写字母 A-F），使用小写将引发错误。

4. 签名失败

根据实际情况，存在以下签名失败的错误码，请根据实际情况处理

错误代码	错误描述
AuthFailure.SignatureExpire	签名过期
AuthFailure.SecretIdNotFound	密钥不存在
AuthFailure.SignatureFailure	签名错误

错误代码	错误描述
AuthFailure.TokenFailure	token 错误
AuthFailure.InvalidSecretId	密钥非法（不是云 API 密钥类型）

5. 签名演示

在实际调用 API 3.0 时，推荐使用配套的tcecloud SDK 3.0 ，SDK 封装了签名的过程，开发时只关注产品提供的具体接口即可。详细信息参见 SDK 中心。当前支持的编程语言有：

- Python
- Java
- PHP
- Go
- JavaScript
- .NET

为了更清楚的解释签名过程，下面以实际编程语言为例，将上述的签名过程具体实现。请求的域名、调用的接口和参数的取值都以上述签名过程为准，代码只为解释签名过程，并不具备通用性，实际开发请尽量使用 SDK 。

最终输出的 url 可能为： http://imgcache.finance.cloud.tencent.com:80cvm.finance.cloud.tencent.com/?Action=DescribeInstances&InstanceIds.0=ins-09dx96dg&Limit=20&Nonce=11886&Offset=0&Region=ap-guangzhou&SecretId=AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE&Signature=EliP9YW3pW28FpsEdkXt%2F%2BWcGeI%3D&Timestamp=1465185768&Version=2017-03-12

注意：由于示例中的密钥是虚构的，时间戳也不是系统当前时间，因此如果将此 url 在浏览器中打开或者用 curl 等命令调用时会返回鉴权错误：签名过期。为了得到一个可以正常返回的 url ，需要修改示例中的 SecretId 和 SecretKey 为真实的密钥，并使用系统当前时间戳作为 Timestamp 。

注意：在下面的示例中，不同编程语言，甚至同一语言每次执行得到的 url 可能都有所不同，表现为参数的顺序不同，但这并不影响正确性。只要所有参数都在，且签名计算正确即可。

注意：以下代码仅适用于 API 3.0，不能直接用于其他的签名流程，即使是旧版的 API ，由于存在细节差异也会导致签名计算错误，请以对应的实际文档为准。

Java

```
import java.io.UnsupportedEncodingException;
import java.net.URLEncoder;
import java.util.Random;
import java.util.TreeMap;
import javax.crypto.Mac;
import javax.crypto.spec.SecretKeySpec;
import javax.xml.bind.DatatypeConverter;

public class TceCloudAPIDemo {
private final static String CHARSET = "UTF-8";

public static String sign(String s, String key, String method) throws Exception {
Mac mac = Mac.getInstance(method);
```

```
SecretKeySpec secretKeySpec = new SecretKeySpec(key.getBytes(CHARSET), mac.getAlgorithm());
mac.init(secretKeySpec);
byte[] hash = mac.doFinal(s.getBytes(CHARSET));
return DatatypeConverter.printBase64Binary(hash);
}

public static String getStringToSign(TreeMap<String, Object> params) {
StringBuilder s2s = new StringBuilder("GETcvm.finance.cloud.tencent.com/?");
// 签名时要求对参数进行字典排序，此处用TreeMap保证顺序
for (String k : params.keySet()) {
s2s.append(k).append("=").append(params.get(k).toString()).append("&");
}
return s2s.toString().substring(0, s2s.length() - 1);
}

public static String getUrl(TreeMap<String, Object> params) throws UnsupportedEncodingException {
StringBuilder url = new StringBuilder("http://imgcache.finance.cloud.tencent.com:80cvm.finance.cloud.tencent.com/?");
// 实际请求的url中对参数顺序没有要求
for (String k : params.keySet()) {
// 需要对请求串进行urlencode，由于key都是英文字母，故此处仅对其value进行urlencode
url.append(k).append("=").append(URLEncoder.encode(params.get(k).toString(), CHARSET)).append("&");
}
return url.toString().substring(0, url.length() - 1);
}

public static void main(String[] args) throws Exception {
TreeMap<String, Object> params = new TreeMap<String, Object>(); // TreeMap可以自动排序
// 实际调用时应当使用随机数，例如：params.put("Nonce", new Random().nextInt(java.lang.Integer.MAX_VALUE));
params.put("Nonce", 11886); // 公共参数
// 实际调用时应当使用系统当前时间，例如： params.put("Timestamp", System.currentTimeMillis() / 1000);
params.put("Timestamp", 1465185768); // 公共参数
params.put("SecretId", "AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE"); // 公共参数
params.put("Action", "DescribeInstances"); // 公共参数
params.put("Version", "2017-03-12"); // 公共参数
params.put("Region", "ap-guangzhou"); // 公共参数
params.put("Limit", 20); // 业务参数
params.put("Offset", 0); // 业务参数
params.put("InstanceIds.0", "ins-09dx96dg"); // 业务参数
params.put("Signature", sign(getStringToSign(params), "Gu5t9xGARNpq86cd98joQYCN3EXAMPLE", "HmacSHA1")); // 公共
参数
System.out.println(getUrl(params));
}
}
```

Python

注意：如果是在 Python 2 环境中运行，需要先安装 requests 依赖包： `pip install requests` 。

```
# -*- coding: utf8 -*-
import base64
import hashlib
import hmac
import time

import requests
```

```
secret_id = "AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE"
secret_key = "Gu5t9xGARNpq86cd98joQYCN3EXAMPLE"

def get_string_to_sign(method, endpoint, params):
s = method + endpoint + "/?"
query_str = "&".join("%s=%s" % (k, params[k]) for k in sorted(params))
return s + query_str

def sign_str(key, s, method):
hmac_str = hmac.new(key.encode("utf8"), s.encode("utf8"), method).digest()
return base64.b64encode(hmac_str)

if __name__ == '__main__':
endpoint = "cvm.finance.cloud.tencent.com"
data = {
'Action' : 'DescribeInstances',
'InstanceIds.0' : 'ins-09dx96dg',
'Limit' : 20,
'Nonce' : 11886,
'Offset' : 0,
'Region' : 'ap-guangzhou',
'SecretId' : secret_id,
'Timestamp' : 1465185768, # int(time.time())
'Version': '2017-03-12'
}
s = get_string_to_sign("GET", endpoint, data)
data["Signature"] = sign_str(secret_key, s, hashlib.sha1)
print(data["Signature"])
# 此处会实际调用，成功后可能产生计费
# resp = requests.get("http://imgcache.finance.cloud.tencent.com:80" + endpoint, params=data)
# print(resp.url)
```

接口签名v3

最近更新时间: 2024-10-18 10:38:24

tcecloud API 会对每个访问请求进行身份验证，即每个请求都需要在公共请求参数中包含签名信息（Signature）以验证请求者身份。 签名信息由安全凭证生成，安全凭证包括 SecretId 和 SecretKey；若用户还没有安全凭证，请前往云API密钥页面申请，否则无法调用云API接口。

1. 申请安全凭证

在第一次使用云API之前，请前往云API密钥页面申请安全凭证。 安全凭证包括 SecretId 和 SecretKey：

- SecretId 用于标识 API 调用者身份
- SecretKey 用于加密签名字符串和服务器端验证签名字符串的密钥。
- 用户必须严格保管安全凭证，避免泄露。

申请安全凭证的具体步骤如下：

1. 登录tcecloud管理中心控制台。
2. 前往云API密钥的控制台页面
3. 在云API密钥页面，点击【新建】即可以创建一对SecretId/SecretKey

注意：开发商帐号最多可以拥有两对 SecretId / SecretKey。

2. TC3-HMAC-SHA256 签名方法

注意：对于GET方法，只支持 Content-Type: application/x-www-form-urlencoded 协议格式。对于POST方法，目前支持 Content-Type: application/json 以及 Content-Type: multipart/form-data 两种协议格式，json 格式默认所有业务接口均支持，multipart 格式只有特定业务接口支持，此时该接口不能使用 json 格式调用，参考具体业务接口文档说明。

下面以云服务器查询广州区实例列表作为例子，分步骤介绍签名的计算过程。我们仅用到了查询实例列表的两个参数：Limit 和 Offset，使用 GET 方法调用。

假设用户的 SecretId 和 SecretKey 分别是：AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE 和 Gu5t9xGARNpq86cd98joQYCN3EXAMPLE

2.1. 拼接规范请求串

按如下格式拼接规范请求串（CanonicalRequest）：

```
CanonicalRequest =
HTTPRequestMethod + '\n' +
CanonicalURI + '\n' +
CanonicalQueryString + '\n' +
CanonicalHeaders + '\n' +
SignedHeaders + '\n' +
HashedRequestPayload
```

- HTTPRequestMethod：HTTP 请求方法（GET、POST ），本示例中为 GET；

- CanonicalURI：URI 参数，API 3.0 固定为正斜杠（/）；
- CanonicalQueryString：发起 HTTP 请求 URL 中的查询字符串，对于 POST 请求，固定为空字符串，对于 GET 请求，则为 URL 中问号（?）后面的字符串内容，本示例取值为：Limit=10&Offset=0。注意：CanonicalQueryString 需要经过 URL 编码。
- CanonicalHeaders：参与签名的头部信息，至少包含 host 和 content-type 两个头部，也可加入自定义的头部参与签名以提高自身请求的唯一性和安全性。拼接规则：1）头部 key 和 value 统一转成小写，并去掉首尾空格，按照 key:value\n 格式拼接；2）多个头部，按照头部 key（小写）的字典排序进行拼接。此例中为：`content-type:application/x-www-form-urlencoded\nhost:cvm.finance.cloud.tencent.com\n`
- SignedHeaders：参与签名的头部信息，说明此次请求有哪些头部参与了签名，和 CanonicalHeaders 包含的头部内容是一一对应的。content-type 和 host 为必选头部。拼接规则：1）头部 key 统一转成小写；2）多个头部 key（小写）按照字典排序进行拼接，并且以分号（;）分隔。此例中为：`content-type;host`
- HashedRequestPayload：请求正文的哈希值，计算方法为 Lowercase(HexEncode(Hash.SHA256(RequestPayload)))，对 HTTP 请求整个正文 payload 做 SHA256 哈希，然后十六进制编码，最后编码串转换成小写字母。注意：对于 GET 请求，RequestPayload 固定为空字符串，对于 POST 请求，RequestPayload 即为 HTTP 请求正文 payload。

根据以上规则，示例中得到的规范请求串如下（为了展示清晰，\n 换行符通过另起打印新的一行替代）：

```
GET
/
Limit=10&Offset=0
content-type:application/x-www-form-urlencoded
host:cvm.finance.cloud.tencent.com

content-type;host
e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
```

2.2. 拼接待签名字符串

按如下格式拼接待签名字符串：

```
StringToSign =
Algorithm + \n +
RequestTimestamp + \n +
CredentialScope + \n +
HashedCanonicalRequest
```

- Algorithm：签名算法，目前固定为 TC3-HMAC-SHA256；
- RequestTimestamp：请求时间戳，即请求头部的 X-TC-Timestamp 取值，如上示例请求为 1539084154；
- CredentialScope：凭证范围，格式为 Date/service/tc3_request，包含日期、所请求的服务和终止字符串（tc3_request）。**Date 为 UTC 标准时间的日期，取值需要和公共参数 X-TC-Timestamp 换算的 UTC 标准时间日期一致**；service 为产品名，必须与调用的产品域名一致，例如 cvm。如上示例请求，取值为 2018-10-09/cvm/tc3_request；
- HashedCanonicalRequest：前述步骤拼接所得规范请求串的哈希值，计算方法为 Lowercase(HexEncode(Hash.SHA256(CanonicalRequest)))。

注意：

> 1. Date 必须从时间戳 X-TC-Timestamp 计算得到，且时区为 UTC+0。如果加入系统本地时区信息，例如东八区，将导致白天和晚上调用成功，但是凌晨时调用必定失败。假设时间戳为 1551113065，在东八区的时间是 2019-02-26 00:44:25，但是计算得到的 Date 取 UTC+0 的日期应为 2019-02-25，而不是 2019-02-26。

> 2. Timestamp 必须是当前系统时间，且需确保系统时间和标准时间是同步的，如果相差超过五分钟则必定失败。如果长时间不和标准时间同步，可能导致运行一段时间后，请求必定失败（返回签名过期错误）。

根据以上规则，示例中得到的待签名字符串如下（为了展示清晰，\n 换行符通过另起打印新的一行替代）：

```
TC3-HMAC-SHA256
1539084154
2018-10-09/cvm/tc3_request
91c9c192c14460df6c1ffc69e34e6c5e90708de2a6d282cccf957dbf1aa7f3a7
```

2.3. 计算签名

1）计算派生签名密钥，伪代码如下

```
SecretKey = "Gu5t9xGARNpq86cd98joQYCN3EXAMPLE"
SecretDate = HMAC_SHA256("TC3" + SecretKey, Date)
SecretService = HMAC_SHA256(SecretDate, Service)
SecretSigning = HMAC_SHA256(SecretService, "tc3_request")
```

- SecretKey：原始的 SecretKey；
- Date：即 Credential 中的 Date 字段信息，如上示例，为2018-10-09；
- Service：即 Credential 中的 Service 字段信息，如上示例，为 cvm；

2）计算签名，伪代码如下

```
Signature = HexEncode(HMAC_SHA256(SecretSigning, StringToSign))
```

- SecretSigning：即以上计算得到的派生签名密钥；
- StringToSign：即步骤2计算得到的待签名字符串；

2.4. 拼接 Authorization

按如下格式拼接 Authorization：

```
Authorization =
Algorithm + ' ' +
'Credential=' + SecretId + '/' + CredentialScope + ', ' +
'SignedHeaders=' + SignedHeaders + ', '
'Signature=' + Signature
```

- Algorithm：签名方法，固定为 TC3-HMAC-SHA256；
- SecretId：密钥对中的 SecretId；
- CredentialScope：见上文，凭证范围；
- SignedHeaders：见上文，参与签名的头部信息；
- Signature：签名值

根据以上规则，示例中得到的值为：

```
TC3-HMAC-SHA256 Credential=AKIDEXAMPLE/Date/service/tc3_request, SignedHeaders=content-type;host, Signature=5da7a33f6993f0614b047e5df4582db9e9bf4672ba50567dba16c6ccf174c474
```

最终完整的调用信息如下：

```
http://imgcache.finance.cloud.tencent.com:80cvm.finance.cloud.tencent.com/?Limit=10&Offset=0

Authorization: TC3-HMAC-SHA256 Credential=AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE/2018-10-09/cvm/tc3_request, SignedHeaders=content-type;host, Signature=5da7a33f6993f0614b047e5df4582db9e9bf4672ba50567dba16c6ccf174c474
Content-Type: application/x-www-form-urlencoded
Host: cvm.finance.cloud.tencent.com
X-TC-Action: DescribeInstances
X-TC-Version: 2017-03-12
X-TC-Timestamp: 1539084154
X-TC-Region: ap-guangzhou
```

3. 签名失败

根据实际情况，存在以下签名失败的错误码，请根据实际情况处理

错误代码	错误描述
AuthFailure.SignatureExpire	签名过期
AuthFailure.SecretIdNotFound	密钥不存在
AuthFailure.SignatureFailure	签名错误
AuthFailure.TokenFailure	token 错误
AuthFailure.InvalidSecretId	密钥非法（不是云 API 密钥类型）

4. 签名演示

Java

```
import java.io.BufferedReader;
import java.io.InputStream;
import java.io.InputStreamReader;
import java.net.URL;
import java.text.SimpleDateFormat;
import java.util.Date;
import java.util.Map;
import java.util.TimeZone;
import java.util.TreeMap;
import javax.crypto.Mac;
import javax.crypto.spec.SecretKeySpec;
import javax.net.ssl.HttpsURLConnection;
import javax.xml.bind.DatatypeConverter;

import org.apache.commons.codec.digest.DigestUtils;

public class TceCloudAPITC3Demo {
private final static String CHARSET = "UTF-8";
```

```
private final static String ENDPOINT = "cvm.finance.cloud.tencent.com";
private final static String PATH = "/";
private final static String SECRET_ID = "AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE";
private final static String SECRET_KEY = "Gu5t9xGARNpq86cd98joQYCN3EXAMPLE";
private final static String CT_X_WWW_FORM_URLENCODED = "application/x-www-form-urlencoded";
private final static String CT_JSON = "application/json";
private final static String CT_FORM_DATA = "multipart/form-data";

public static byte[] sign256(byte[] key, String msg) throws Exception {
Mac mac = Mac.getInstance("HmacSHA256");
SecretKeySpec secretKeySpec = new SecretKeySpec(key, mac.getAlgorithm());
mac.init(secretKeySpec);
return mac.doFinal(msg.getBytes(CHARSET));
}

public static void main(String[] args) throws Exception {
String service = "cvm";
String host = "cvm.finance.cloud.tencent.com";
String region = "ap-guangzhou";
String action = "DescribeInstances";
String version = "2017-03-12";
String algorithm = "TC3-HMAC-SHA256";
String timestamp = "1539084154";
//String timestamp = String.valueOf(System.currentTimeMillis() / 1000);
SimpleDateFormat sdf = new SimpleDateFormat("yyyy-MM-dd");
// 注意时区，否则容易出错
sdf.setTimeZone(TimeZone.getTimeZone("UTC"));
String date = sdf.format(new Date(Long.valueOf(timestamp + "000")));

// ************ 步骤 1：拼接规范请求串 ************
String httpRequestMethod = "GET";
String canonicalUri = "/";
String canonicalQueryString = "Limit=10&Offset=0";
String canonicalHeaders = "content-type:application/x-www-form-urlencoded\n" + "host:" + host + "\n";
String signedHeaders = "content-type;host";
String hashedRequestPayload = DigestUtils.sha256Hex("");
String canonicalRequest = httpRequestMethod + "\n" + canonicalUri + "\n" + canonicalQueryString + "\n"
+ canonicalHeaders + "\n" + signedHeaders + "\n" + hashedRequestPayload;
System.out.println(canonicalRequest);

// ************ 步骤 2：拼接待签名字符串 ************
String credentialScope = date + "/" + service + "/" + "tc3_request";
String hashedCanonicalRequest = DigestUtils.sha256Hex(canonicalRequest.getBytes(CHARSET));
String stringToSign = algorithm + "\n" + timestamp + "\n" + credentialScope + "\n" + hashedCanonicalRequest;
System.out.println(stringToSign);

// ************ 步骤 3：计算签名 ************
byte[] secretDate = sign256(("TC3" + SECRET_KEY).getBytes(CHARSET), date);
byte[] secretService = sign256(secretDate, service);
byte[] secretSigning = sign256(secretService, "tc3_request");
String signature = DatatypeConverter.printHexBinary(sign256(secretSigning, stringToSign)).toLowerCase();
System.out.println(signature);

// ************ 步骤 4：拼接 Authorization ************
String authorization = algorithm + " " + "Credential=" + SECRET_ID + "/" + credentialScope + ", "
+ "SignedHeaders=" + signedHeaders + ", " + "Signature=" + signature;
System.out.println(authorization);
```

```
TreeMap<String, String> headers = new TreeMap<String, String>();
headers.put("Authorization", authorization);
headers.put("Host", host);
headers.put("Content-Type", CT_X_WWW_FORM_URLENCODED);
headers.put("X-TC-Action", action);
headers.put("X-TC-Timestamp", timestamp);
headers.put("X-TC-Version", version);
headers.put("X-TC-Region", region);
}
}
```

Python

```
# -*- coding: utf-8 -*-
import hashlib, hmac, json, os, sys, time
from datetime import datetime

# 密钥参数
secret_id = "AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE"
secret_key = "Gu5t9xGARNpq86cd98joQYCN3EXAMPLE"

service = "cvm"
host = "cvm.finance.cloud.tencent.com"
endpoint = "http://imgcache.finance.cloud.tencent.com:80" + host
region = "ap-guangzhou"
action = "DescribeInstances"
version = "2017-03-12"
algorithm = "TC3-HMAC-SHA256"
timestamp = 1539084154
date = datetime.utcfromtimestamp(timestamp).strftime("%Y-%m-%d")
params = {"Limit": 10, "Offset": 0}

# ************* 步骤 1：拼接规范请求串 *************
http_request_method = "GET"
canonical_uri = "/"
canonical_querystring = "Limit=10&Offset=0"
ct = "x-www-form-urlencoded"
payload = ""
if http_request_method == "POST":
canonical_querystring = ""
ct = "json"
payload = json.dumps(params)
canonical_headers = "content-type:application/%s\nhost:%s\n" % (ct, host)
signed_headers = "content-type;host"
hashed_request_payload = hashlib.sha256(payload.encode("utf-8")).hexdigest()
canonical_request = (http_request_method + "\n" +
canonical_uri + "\n" +
canonical_querystring + "\n" +
canonical_headers + "\n" +
signed_headers + "\n" +
hashed_request_payload)
print(canonical_request)

# ************* 步骤 2：拼接待签名字符串 *************
credential_scope = date + "/" + service + "/" + "tc3_request"
```

```
hashed_canonical_request = hashlib.sha256(canonical_request.encode("utf-8")).hexdigest()
string_to_sign = (algorithm + "\n" +
str(timestamp) + "\n" +
credential_scope + "\n" +
hashed_canonical_request)
print(string_to_sign)


# ************* 步骤 3：计算签名 *************
# 计算签名摘要函数
def sign(key, msg):
return hmac.new(key, msg.encode("utf-8"), hashlib.sha256).digest()
secret_date = sign(("TC3" + secret_key).encode("utf-8"), date)
secret_service = sign(secret_date, service)
secret_signing = sign(secret_service, "tc3_request")
signature = hmac.new(secret_signing, string_to_sign.encode("utf-8"), hashlib.sha256).hexdigest()
print(signature)

# ************* 步骤 4：拼接 Authorization *************
authorization = (algorithm + " " +
"Credential=" + secret_id + "/" + credential_scope + ", " +
"SignedHeaders=" + signed_headers + ", " +
"Signature=" + signature)
print(authorization)

# 公共参数添加到请求头部
headers = {
"Authorization": authorization,
"Host": host,
"Content-Type": "application/%s" % ct,
"X-TC-Action": action,
"X-TC-Timestamp": str(timestamp),
"X-TC-Version": version,
"X-TC-Region": region,
}
```

请求结构

最近更新时间: 2024-10-18 10:38:24

1. 服务地址

地域（Region）是指物理的数据中心的地理区域。tcecloud交付验证不同地域之间完全隔离，保证不同地域间最大程度的稳定性和容错性。为了降低访问时延、提高下载速度，建议您选择最靠近您客户的地域。

您可以通过 API接口 **查询地域列表** 查看完成的地域列表。

2. 通信协议

tcecloud API 的所有接口均通过 HTTPS 进行通信，提供高安全性的通信通道。

3. 请求方法

支持的 HTTP 请求方法:

- POST（推荐）
- GET

POST 请求支持的 Content-Type 类型：

- application/json（推荐），必须使用 TC3-HMAC-SHA256 签名方法。
- application/x-www-form-urlencoded，必须使用 HmacSHA1 或 HmacSHA256 签名方法。
- multipart/form-data（仅部分接口支持），必须使用 TC3-HMAC-SHA256 签名方法。

GET 请求的请求包大小不得超过 32 KB。POST 请求使用签名方法为 HmacSHA1、HmacSHA256 时不得超过 1 MB。POST 请求使用签名方法为 TC3-HMAC-SHA256 时支持 10 MB。

4. 字符编码

均使用UTF-8编码。

返回结果

最近更新时间: 2024-10-18 10:38:24

正确返回结果

以云服务器的接口查看实例状态列表 (DescribeInstancesStatus) 2017-03-12 版本为例，若调用成功，其可能的返回如下为：

```
{
"Response": {
"TotalCount": 0,
"InstanceStatusSet": [],
"RequestId": "b5b41468-520d-4192-b42f-595cc34b6c1c"
}
}
```

- Response 及其内部的 RequestId 是固定的字段，无论请求成功与否，只要 API 处理了，则必定会返回。
- RequestId 用于一个 API 请求的唯一标识，如果 API 出现异常，可以联系我们，并提供该 ID 来解决问题。
- 除了固定的字段外，其余均为具体接口定义的字段，不同的接口所返回的字段参见接口文档中的定义。此例中的 TotalCount 和 InstanceStatusSet 均为 DescribeInstancesStatus 接口定义的字段，由于调用请求的用户暂时还没有云服务器实例，因此 TotalCount 在此情况下的返回值为 0， InstanceStatusSet 列表为空。

错误返回结果

若调用失败，其返回值示例如下为：

```
{
"Response": {
"Error": {
"Code": "AuthFailure.SignatureFailure",
"Message": "The provided credentials could not be validated. Please check your signature is correct."
},
"RequestId": "ed93f3cb-f35e-473f-b9f3-0d451b8b79c6"
}
}
```

- Error 的出现代表着该请求调用失败。Error 字段连同其内部的 Code 和 Message 字段在调用失败时是必定返回的。
- Code 表示具体出错的错误码，当请求出错时可以先根据该错误码在公共错误码和当前接口对应的错误码列表里面查找对应原因和解决方案。
- Message 显示出了这个错误发生的具体原因，随着业务发展或体验优化，此文本可能会经常保持变更或更新，用户不应依赖这个返回值。
- RequestId 用于一个 API 请求的唯一标识，如果 API 出现异常，可以联系我们，并提供该 ID 来解决问题。

公共错误码 (TODO: 重复信息, 是否真的需要?)

返回结果中如果存在 Error 字段，则表示调用 API 接口失败。 Error 中的 Code 字段表示错误码，所有业务都可能出现的错误码为公共错误码，下表列出了公共错误码。

错误码	错误描述
AuthFailure.InvalidSecretId	密钥非法（不是云 API 密钥类型）。
AuthFailure.MFAFailure	MFA 错误。
AuthFailure.SecretIdNotFound	密钥不存在。
AuthFailure.SignatureExpire	签名过期。
AuthFailure.SignatureFailure	签名错误。
AuthFailure.TokenFailure	token 错误。
AuthFailure.UnauthorizedOperation	请求未 CAM 授权。
DryRunOperation	DryRun 操作，代表请求将会是成功的，只是多传了 DryRun 参数。
FailedOperation	操作失败。
InternalError	内部错误。
InvalidAction	接口不存在。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。
LimitExceeded	超过配额限制。
MissingParameter	缺少参数错误。
NoSuchVersion	接口版本不存在。
RequestLimitExceeded	请求的次数超过了频率限制。
ResourceInUse	资源被占用。
ResourceInsufficient	资源不足。
ResourceNotFound	资源不存在。
ResourceUnavailable	资源不可用。
UnauthorizedOperation	未授权操作。
UnknownParameter	未知参数错误。
UnsupportedOperation	操作不支持。
UnsupportedProtocol	http(s)请求协议错误，只支持 GET 和 POST 请求。
UnsupportedRegion	接口不支持所传地域。

公共参数

最近更新时间: 2024-10-18 10:38:24

公共参数是用于标识用户和接口鉴权目的的参数，如非必要，在每个接口单独的接口文档中不再对这些参数进行说明，但每次请求均需要携带这些参数，才能正常发起请求。

签名方法 v3

使用 TC3-HMAC-SHA256 签名方法时，公共参数需要统一放到 HTTP Header 请求头部中，如下：

参数名称	类型	必选	描述
X-TC-Action	String	是	操作的接口名称。取值参考接口文档中输入参数公共参数 Action 的说明。例如云服务器的查询实例列表接口，取值为 DescribeInstances。
X-TC-Region	String	是	地域参数，用来标识希望操作哪个地域的数据。接口接受的地域取值参考接口文档中输入参数公共参数 Region 的说明。注意：某些接口不需要传递该参数，接口文档中会对此特别说明，此时即使传递该参数也不会生效。
X-TC-Timestamp	Integer	是	当前 UNIX 时间戳，可记录发起 API 请求的时间。例如 1529223702。注意：如果与服务器时间相差超过5分钟，会引起签名过期错误。
X-TC-Version	String	是	操作的 API 的版本。取值参考接口文档中入参公共参数 Version 的说明。例如云服务器的版本 2017-03-12。
Authorization	String	是	HTTP 标准身份认证头部字段，例如： TC3-HMAC-SHA256 Credential=AKIDEXAMPLE/Date/service/tc3_request, SignedHeaders=content-type;host, Signature=fe5f80f77d5fa3beca038a248ff027d0445342fe2855ddc963176630326f1024 其中， - TC3-HMAC-SHA256：签名方法，目前固定取该值； - Credential：签名凭证，AKIDEXAMPLE 是 SecretId；Date 是 UTC 标准时间的日期，取值需要和公共参数 X-TC-Timestamp 换算的 UTC 标准时间日期一致；service为产品名，必须与调用的产品域名一致，例如cvm； - SignedHeaders：参与签名计算的头部信息，content-type 和 host 为必选头部； - Signature：签名摘要。
X-TC-Token	String	否	临时证书所用的 Token ，需要结合临时密钥一起使用。临时密钥和 Token 需要到访问管理服务调用接口获取。长期密钥不需要 Token。

签名方法 v1

使用 HmacSHA1 和 HmacSHA256 签名方法时，公共参数需要统一放到请求串中，如下

参数名称	类型	必选	描述
Action	String	是	操作的接口名称。取值参考接口文档中输入参数公共参数 Action 的说明。例如云服务器的查询实例列表接口，取值为 DescribeInstances。

参数名称	类型	必选	描述
Region	String	是	地域参数，用来标识希望操作哪个地域的数据。接口接受的地域取值参考接口文档中输入参数公共参数 Region 的说明。注意：某些接口不需要传递该参数，接口文档中会对此特别说明，此时即使传递该参数也不会生效。
Timestamp	Integer	是	当前 UNIX 时间戳，可记录发起 API 请求的时间。例如1529223702，如果与当前时间相差过大，会引起签名过期错误。
Nonce	Integer	是	随机正整数，与 Timestamp 联合起来，用于防止重放攻击。
SecretId	String	是	在云API密钥上申请的标识身份的 SecretId，一个 SecretId 对应唯一的 SecretKey ，而 SecretKey 会用来生成请求签名 Signature。
Signature	String	是	请求签名，用来验证此次请求的合法性，需要用户根据实际的输入参数计算得出。具体计算方法参见接口鉴权文档。
Version	String	是	操作的 API 的版本。取值参考接口文档中入参公共参数 Version 的说明。例如云服务器的版本 2017-03-12。
SignatureMethod	String	否	签名方式，目前支持 HmacSHA256 和 HmacSHA1。只有指定此参数为 HmacSHA256 时，才使用 HmacSHA256 算法验证签名，其他情况均使用 HmacSHA1 验证签名。
Token	String	否	临时证书所用的 Token ，需要结合临时密钥一起使用。临时密钥和 Token 需要到访问管理服务调用接口获取。长期密钥不需要 Token 。

地域列表

地域（Region）是指物理的数据中心的地理区域。tcecloud交付验证不同地域之间完全隔离，保证不同地域间最大程度的稳定性和容错性。为了降低访问时延、提高下载速度，建议您选择最靠近您客户的地域。

您可以通过 API接口 **查询地域列表** 查看完成的地域列表。

其他接口
获取地域列表

最近更新时间: 2024-10-18 10:38:24

1. 接口描述

接口请求域名： cloudhsm.api3.finance.cloud.tencent.com。

获取地域列表

默认接口请求频率限制：20次/秒。

接口更新时间：2020-05-09 15:20:58。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeRegions
Version	是	否	String	公共参数，本接口取值：2019-11-12
Region	是	否	String	公共参数，详见产品支持的**地域列表**(TODO)

3. 输出参数

参数名称	类型	描述
TotalCount	Int64	地域数量
Regions	RegionInfo	地域列表
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
ResourceNotFound	

错误码	描述
UnauthorizedOperation	
InternalError	
InvalidParameter	

查询子网列表

最近更新时间: 2024-10-18 10:38:24

1. 接口描述

接口请求域名： cloudhsm.api3.finance.cloud.tencent.com。

查询子网列表

默认接口请求频率限制：20次/秒。

接口更新时间：2020-01-16 11:01:28。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeSubnet
Version	是	否	String	公共参数，本接口取值：2019-11-12
Region	是	否	String	公共参数，详见产品支持的**地域列表**(TODO)
Limit	是	否	Int64	返回数量。
Offset	是	否	Int64	偏移量。
VpcId	是	否	String	查询指定VpcId下的子网信息。
SearchWord	否	否	String	查找关键字

3. 输出参数

参数名称	类型	描述
TotalCount	Int64	返回的子网数量。
SubnetList	Subnet	返回的子网实例列表。
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter	
UnauthorizedOperation	
ResourceNotFound	

获取当前地域所支持的设备列表

最近更新时间: 2024-10-18 10:38:24

1. 接口描述

接口请求域名： cloudhsm.api3.finance.cloud.tencent.com。

获取当前地域所支持的设备列表

默认接口请求频率限制：20次/秒。

接口更新时间：2021-10-11 17:56:40。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeSupportedHsm
Version	是	否	String	公共参数，本接口取值：2019-11-12
Region	是	否	String	公共参数，详见产品支持的**地域列表**(TODO)

3. 输出参数

参数名称	类型	描述
DeviceTypes	DeviceInfo	当前地域所支持的设备列表
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter	
ResourceNotFound	
UnauthorizedOperation	

获取用户安全组列表

最近更新时间: 2024-10-18 10:38:24

1. 接口描述

接口请求域名： cloudhsm.api3.finance.cloud.tencent.com。

根据用户的AppId获取用户安全组列表

默认接口请求频率限制：20次/秒。

接口更新时间：2020-01-16 11:03:14。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeUsg
Version	是	否	String	公共参数，本接口取值：2019-11-12
Region	是	否	String	公共参数，详见产品支持的**地域列表**(TODO)
Offset	是	否	Int64	偏移量，当Offset和Limit均为0时将一次性返回用户所有的安全组列表。
Limit	是	否	Int64	返回量，当Offset和Limit均为0时将一次性返回用户所有的安全组列表。
SearchWord	否	否	String	搜索关键字

3. 输出参数

参数名称	类型	描述
SgList	SgUnit	用户的安全组列表
TotalCount	Int64	返回的安全组数量
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述

错误码	描述
InternalError	
InvalidParameter	
UnauthorizedOperation	
ResourceNotFound	

获取安全组详情

最近更新时间: 2024-10-18 10:38:24

1. 接口描述

接口请求域名： cloudhsm.api3.finance.cloud.tencent.com。

获取安全组详情

默认接口请求频率限制：20次/秒。

接口更新时间：2020-01-16 11:02:31。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeUsgRule
Version	是	否	String	公共参数，本接口取值：2019-11-12
Region	是	否	String	公共参数，详见产品支持的**地域列表**(TODO)
SgIds	是	否	Array of String	根据安全组Id获取安全组详情

3. 输出参数

参数名称	类型	描述
SgRules	UsgRuleDetail	安全组详情
TotalCount	Int64	安全组详情数量
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter	

错误码	描述
UnauthorizedOperation	
ResourceNotFound	

查询私有网络列表

最近更新时间: 2024-10-18 10:38:24

1. 接口描述

接口请求域名： cloudhsm.api3.finance.cloud.tencent.com。

查询用户的私有网络列表

默认接口请求频率限制：20次/秒。

接口更新时间：2020-01-16 11:01:43。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeVpc
Version	是	否	String	公共参数，本接口取值：2019-11-12
Region	是	否	String	公共参数，详见产品支持的**地域列表**(TODO)
Offset	是	否	Int64	返回偏移量。
Limit	是	否	Int64	返回数量。
SearchWord	否	否	String	搜索关键字

3. 输出参数

参数名称	类型	描述
TotalCount	Int64	可查询到的所有Vpc实例总数。
VpcList	Vpc	Vpc对象列表
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述

错误码	描述
InternalError	
InvalidParameter	
UnauthorizedOperation	
ResourceNotFound	

获取VSM参数信息列表

最近更新时间: 2024-10-18 10:38:24

1. 接口描述

接口请求域名： cloudhsm.api3.finance.cloud.tencent.com。

获取VSM参数信息列表

默认接口请求频率限制：20次/秒。

接口更新时间：2021-10-11 17:49:53。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeVsmProperty
Version	是	否	String	公共参数，本接口取值：2019-11-12
Region	是	否	String	公共参数，详见产品支持的**地域列表**(TODO)
VsmTypeIDList	是	否	Array of Int64	VSM类型ID列表

3. 输出参数

参数名称	类型	描述
VsmProperties	VsmProperty	VSM参数信息列表
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter	
ResourceNotFound	

错误码	描述
UnauthorizedOperation	

虚拟加密机实例相关接口
创建VSM

最近更新时间: 2024-10-18 10:38:24

1. 接口描述

接口请求域名： cloudhsm.api3.finance.cloud.tencent.com。

创建VSM

默认接口请求频率限制：20次/秒。

接口更新时间：2020-12-01 16:02:40。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：CreateResource
Version	是	否	String	公共参数，本接口取值：2019-11-12
Region	是	否	String	公共参数，详见产品支持的**地域列表**(TODO)
PayMode	是	否	Int64	付费模式，0为后付费，1为预付费
GoodsNum	是	否	Int64	资源数量
VsmType	是	否	Int64	VSM类型
VpcId	是	否	String	虚拟私有网络
SubnetId	是	否	String	子网网络
ZoneId	是	否	Int64	可用区ID
Tags	否	否	Array of TagUnit	Tag列表

3. 输出参数

参数名称	类型	描述
BillId	String	交易账单Id
DealNames	String	订单列表

参数名称	类型	描述
ResourceIds	String	资源列表
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter	
ResourceNotFound	
UnauthorizedOperation	

通过SubnetId获取Hsm资源数

最近更新时间: 2024-10-18 10:38:24

1. 接口描述

接口请求域名： cloudhsm.api3.finance.cloud.tencent.com。

通过SubnetId获取Hsm资源数

默认接口请求频率限制：20次/秒。

接口更新时间：2020-02-27 13:57:58。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeHSMBySubnetId
Version	是	否	String	公共参数，本接口取值：2019-11-12
Region	是	否	String	公共参数，详见产品支持的**地域列表**(TODO)
SubnetId	是	否	String	Subnet标识符

3. 输出参数

参数名称	类型	描述
TotalCount	Int64	HSM数量
SubnetId	String	作为查询条件的SubnetId
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter	

错误码	描述
UnauthorizedOperation	
ResourceNotFound	

通过VpcId获取Hsm资源数

最近更新时间: 2024-10-18 10:38:24

1. 接口描述

接口请求域名： cloudhsm.api3.finance.cloud.tencent.com。

通过VpcId获取Hsm资源数

默认接口请求频率限制：20次/秒。

接口更新时间：2020-02-27 13:57:32。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeHSMByVpcId
Version	是	否	String	公共参数，本接口取值：2019-11-12
Region	是	否	String	公共参数，详见产品支持的**地域列表**(TODO)
VpcId	是	否	String	VPC标识符

3. 输出参数

参数名称	类型	描述
TotalCount	Int64	HSM数量
VpcId	String	作为查询条件的VpcId
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter	

错误码	描述
UnauthorizedOperation	
ResourceNotFound	

获取VSM属性

最近更新时间: 2024-10-18 10:38:24

1. 接口描述

接口请求域名： cloudhsm.api3.finance.cloud.tencent.com。

获取VSM属性

默认接口请求频率限制：20次/秒。

接口更新时间：2020-12-01 16:05:58。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeVsmAttributes
Version	是	否	String	公共参数，本接口取值：2019-11-12
Region	是	否	String	公共参数，详见产品支持的**地域列表**(TODO)
ResourceId	是	否	String	资源Id

3. 输出参数

参数名称	类型	描述
ResourceId	String	资源Id
ResourceName	String	资源名称
Status	Int64	资源状态
Vip	String	资源IP
VpcId	String	资源所属Vpc
SubnetId	String	资源所属子网
Model	String	资源所属HSM的规格
VsmType	Int64	资源类型
RegionId	Int64	地域Id

参数名称	类型	描述
ZoneId	Int64	区域Id
ExpireTime	Int64	过期时间
SgList	UsgRuleDetail	安全组详情信息
SubnetName	String	子网名
RegionName	String	地域名
ZoneName	String	区域名
Expired	Bool	实例是否已经过期
RemainSeconds	Int64	为正数表示实例距离过期时间剩余秒数，为负数表示实例已经过期多少秒
VpcName	String	私有虚拟网络名称
VpcCidrBlock	String	VPC的IPv4 CIDR
SubnetCidrBlock	String	子网的CIDR
Tags	TagUnit	Tag参数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter	
UnauthorizedOperation	
ResourceNotFound	

获取用户VSM列表

最近更新时间: 2024-10-18 10:38:24

1. 接口描述

接口请求域名： cloudhsm.api3.finance.cloud.tencent.com。

获取用户VSM列表

默认接口请求频率限制：20次/秒。

接口更新时间：2021-11-01 15:47:50。

接口只验签名不鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeVsms
Version	是	否	String	公共参数，本接口取值：2019-11-12
Region	是	否	String	公共参数，详见产品支持的**地域列表**(TODO)
Offset	是	否	Int64	偏移
Limit	是	否	Int64	最大数量
SearchWord	否	否	String	查询关键字
TagFilters	否	否	Array of TagFilter	Tag过滤参数
Manufacturer	否	否	String	厂商名称

3. 输出参数

参数名称	类型	描述
TotalCount	Int64	获取实例的总个数
VsmList	ResourceInfo	资源信息
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter	
UnauthorizedOperation	
ResourceNotFound	

询价

最近更新时间: 2024-10-18 10:38:24

1. 接口描述

接口请求域名： cloudhsm.api3.finance.cloud.tencent.com。

购买询价接口

默认接口请求频率限制：20次/秒。

接口更新时间：2020-02-19 17:10:30。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：InquiryPriceBuyVsm
Version	是	否	String	公共参数，本接口取值：2019-11-12
Region	是	否	String	公共参数，详见产品支持的**地域列表**(TODO)
GoodsNum	是	否	Int64	需购买实例的数量
PayMode	是	否	Int64	付费模式：0表示按需计费/后付费，1表示预付费
Currency	否	否	String	货币类型，默认为CNY
TimeSpan	是	否	String	商品的时间大小
TimeUnit	是	否	String	商品的时间单位
Type	否	否	String	默认为CREATE，可选RENEW

3. 输出参数

参数名称	类型	描述
TotalCost	Float	总金额
GoodsNum	Int64	购买的实例数量
TimeSpan	String	商品的时间大小
TimeUnit	String	商品的时间单位

版权所有：腾讯云金融专区

参数名称	类型	描述
OriginalCost	Float	原始总金额
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter	
UnauthorizedOperation	
ResourceNotFound	

修改VSM属性

最近更新时间: 2024-10-18 10:38:24

1. 接口描述

接口请求域名： cloudhsm.api3.finance.cloud.tencent.com。

修改VSM属性

默认接口请求频率限制：20次/秒。

接口更新时间：2020-11-25 14:30:48。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ModifyVsmAttributes
Version	是	否	String	公共参数，本接口取值：2019-11-12
Region	是	否	String	公共参数，详见产品支持的**地域列表**(TODO)
ResourceId	是	否	String	资源Id
ResourceName	否	否	String	资源名称
SgIds	否	否	Array of String	安全组Id
VpcId	否	否	String	VpcId
SubnetId	否	否	String	子网Id
Type	是	否	Array of String	UpdateResourceName-修改资源名称, UpdateSgIds-修改安全组名称, UpdateNetWork-修改网络, Default-默认不修改

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter	
UnauthorizedOperation	
ResourceNotFound	

退还虚拟加密机

最近更新时间: 2024-10-18 10:38:24

1. 接口描述

接口请求域名： cloudhsm.api3.finance.cloud.tencent.com。

退还虚拟加密机

默认接口请求频率限制：20次/秒。

接口更新时间：2020-11-25 14:28:23。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：TerminateVsm
Version	是	否	String	公共参数，本接口取值：2019-11-12
Region	是	否	String	公共参数，详见产品支持的**地域列表**(TODO)
ResourceId	是	否	String	资源唯一标识

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter	
ResourceNotFound	
UnauthorizedOperation	

数据结构

最近更新时间: 2024-10-18 10:38:24

Subnet

Subnet对象

被如下接口引用：DescribeSubnet

名称	必选	允许NULL	类型	描述
VpcId	是	是	String	VPC实例ID。
SubnetId	是	是	String	子网实例ID，例如：subnet-bthucmmy。
SubnetName	是	是	String	子网名称。
CidrBlock	是	是	String	子网的 IPv4 CIDR。
CreatedTime	是	是	String	创建时间。
AvailableIpAddressCount	是	是	Int64	可用IP数。
Ipv6CidrBlock	是	是	String	子网的 IPv6 CIDR。
TotalIpAddressCount	是	是	Int64	总IP数
IsDefault	是	是	Bool	是否为默认Subnet

UsgRuleDetail

安全组规则详情

被如下接口引用：DescribeUsgRule、DescribeVsmAttributes

名称	必选	允许NULL	类型	描述
InBound	是	是	Array of UsgPolicy	入站规则
OutBound	是	是	Array of UsgPolicy	出站规则
SgId	是	是	String	安全组Id
SgName	是	是	String	安全组名称
SgRemark	是	是	String	备注
CreateTime	是	是	String	创建时间
Version	是	是	Int64	版本

版权所有：腾讯云金融专区

HsmInfo

支持的加密机类型信息

被如下接口引用：DescribeSupportedHsm

名称	必选	允许NULL	类型	描述
Model	是	否	String	加密机型号
VsmTypes	是	否	Array of VsmInfo	此类型的加密机所支持的VSM类型列表

ResourceInfo

资源信息

被如下接口引用：DescribeVsms

名称	必选	允许NULL	类型	描述
ResourceId	是	是	String	资源Id
ResourceName	是	是	String	资源名称
Status	是	是	Int64	资源状态
Vip	是	是	String	资源IP
VpcId	是	是	String	资源所属Vpc
SubnetId	是	是	String	资源所属子网
Model	是	是	String	资源所属HSM规格
VsmType	是	是	Int64	资源类型
RegionId	是	是	Int64	地域Id
ZoneId	是	是	Int64	区域Id
ExpireTime	是	是	Int64	过期时间
RegionName	是	是	String	地域名
ZoneName	是	是	String	区域名
SgList	是	是	Array of SgUnit	实例的安全组列表
SubnetName	是	是	String	子网名称
Expired	是	是	Bool	当前实例是否已经过期
RemainSeconds	是	是	Int64	为正数表示实例距离过期时间还剩余多少秒，为负数表示已经过期多少秒

版权所有：腾讯云金融专区

名称	必选	允许NULL	类型	描述
VpcName	是	是	String	Vpc名称
Tags	否	否	Array of TagUnit	Tag信息

TagUnit

Tag键值对

被如下接口引用：CreateResource、DescribeVsmAttributes、DescribeVsms

名称	必选	允许NULL	类型	描述
TagKey	是	否	String	Tag Key
TagValue	否	否	String	Tag Value

UsgPolicy

安全组策略

被如下接口引用：DescribeUsgRule、DescribeVsmAttributes

名称	必选	允许NULL	类型	描述
Ip	是	是	String	cidr格式地址
Id	是	是	String	安全组id代表的地址集合
AddressModule	是	是	String	地址组id代表的地址集合
Proto	是	是	String	协议
Port	是	是	String	端口
ServiceModule	是	是	String	服务组id代表的协议和端口集合
Desc	是	是	String	备注
Action	是	是	String	匹配后行为:ACCEPT/DROP

ExtraFlags

辅助参数

被如下接口引用：DescribeExtraFlags

名称	必选	允许NULL	类型	描述

名称	必选	允许NULL	类型	描述
ShowWeakAlgorithm	是	是	Bool	是否展示弱算法

SgUnit

安全组基础信息

被如下接口引用：DescribeUsg、DescribeVsms

名称	必选	允许NULL	类型	描述
SgId	是	是	String	安全组Id
SgName	是	是	String	安全组名称
SgRemark	是	是	String	备注
CreateTime	是	是	String	创建时间

VsmInfo

支持的Vsm类型信息

被如下接口引用：DescribeSupportedHsm

名称	必选	允许NULL	类型	描述
TypeName	是	否	String	VSM类型名称
TypeID	是	否	Int64	VSM类型值

RegionInfo

地域信息

被如下接口引用：DescribeRegions

名称	必选	允许NULL	类型	描述
RegionId	是	否	Int64	地域ID
RegionCnCode	是	否	String	地域中文编码
RegionEnCode	是	否	String	地域英文编码
Zones	是	否	Array of ZoneInfo	地域下的可用区列表

TagFilter

Tag过滤参数

被如下接口引用：DescribeVsms

名称	必选	允许NULL	类型	描述
TagKey	否	否	String	Tag Key
TagValue	否	否	Array of String	Tag Value

ZoneInfo

可用区信息

被如下接口引用：DescribeRegions

名称	必选	允许NULL	类型	描述
ZoneId	是	否	Int64	可用区ID
ZoneEnCode	是	否	String	可用区英文编码
ZoneCnCode	是	否	String	可用区中文编码

Vpc

VPC对象

被如下接口引用：DescribeVpc

名称	必选	允许NULL	类型	描述
VpcName	是	是	String	Vpc名称
VpcId	是	是	String	VpcId
CreatedTime	是	是	String	创建时间
IsDefault	是	是	Bool	是否为默认VPC

VsmPropertyUnit

VSM性能参数信息

被如下接口引用：DescribeVsmProperty

名称	必选	允许NULL	类型	描述
PropertyName	是	否	String	性能参数名称
PropertyValue	是	否	String	性能参数描述

版权所有：腾讯云金融专区

DeviceInfo

设备厂商信息

被如下接口引用：DescribeSupportedHsm

名称	必选	允许NULL	类型	描述
Manufacturer	是	否	String	厂商名称
HsmTypes	是	否	Array of HsmInfo	此厂商旗下的设备信息列表

VsmProperty

VSM属性信息

被如下接口引用：DescribeVsmProperty

名称	必选	允许NULL	类型	描述
VsmTypeID	是	否	Int64	VSM类型ID
AlgDescList	是	否	VsmAlgDescUnit	算法描述信息列表
PropertyList	是	否	VsmPropertyUnit	性能参数信息列表

VsmAlgDescUnit

VSM算法描述信息

被如下接口引用：DescribeVsmProperty

名称	必选	允许NULL	类型	描述
AlgType	是	否	String	算法类型
AlgDesc	是	否	String	算法类型描述

错误码

最近更新时间: 2024-10-18 10:38:24

功能说明

如果返回结果中存在 Error 字段，则表示调用 API 接口失败。例如：

```
{
"Response": {
"Error": {
"Code": "AuthFailure.SignatureFailure",
"Message": "The provided credentials could not be validated. Please check your signature is correct."
},
"RequestId": "ed93f3cb-f35e-473f-b9f3-0d451b8b79c6"
}
}
```

Error 中的 Code 表示错误码，Message 表示该错误的具体信息。

错误码列表

公共错误码

错误码	说明
AuthFailure.InvalidSecretId	密钥非法（不是云 API 密钥类型）。
AuthFailure.MFAFailure	MFA 错误。
AuthFailure.SecretIdNotFound	密钥不存在。 请在控制台检查密钥是否已被删除或者禁用，如状态正常，请检查密钥是否填写正确，注意前后不得有空格。
AuthFailure.SignatureExpire	签名过期。Timestamp 和服务器时间相差不得超过五分钟，请检查本地时间是否和标准时间同步。
AuthFailure.SignatureFailure	签名错误。 签名计算错误，请对照调用方式中的接口鉴权文档检查签名计算过程。
AuthFailure.TokenFailure	token 错误。
AuthFailure.UnauthorizedOperation	请求未 CAM 授权。
DryRunOperation	DryRun 操作，代表请求将会是成功的，只是多传了 DryRun 参数。
FailedOperation	操作失败。
InternalError	内部错误。
InvalidAction	接口不存在。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

版权所有：腾讯云金融专区

错误码	说明
LimitExceeded	超过配额限制。
MissingParameter	缺少参数错误。
NoSuchVersion	接口版本不存在。
RequestLimitExceeded	请求的次数超过了频率限制。
ResourceInUse	资源被占用。
ResourceInsufficient	资源不足。
ResourceNotFound	资源不存在。
ResourceUnavailable	资源不可用。
UnauthorizedOperation	未授权操作。
UnknownParameter	未知参数错误。
UnsupportedOperation	操作不支持。
UnsupportedProtocol	http(s)请求协议错误，只支持 GET 和 POST 请求。
UnsupportedRegion	接口不支持所传地域。

业务错误码

错误码	说明
InternalError	
UnauthorizedOperation	
InvalidParameter	
ResourceNotFound	