密钥管理系统

控制台指南

产品文档

腾讯云

文档目录

控制台指南
入门概述

最近更新时间：2019-11-15 17:44:49

密钥管理服务 KMS 提供安全合规的密钥的全生命周期管理和数据加解密能力。

对于用户而言，KMS 服务中涉及的核心密钥组件包括用户主密钥 CMK（Customer Master Key，CMK）、数据加密密钥 DEK（Data Encryption Key，DEK）。其中 CMK 属于用户的一级密钥，CMK 用于对敏感数据的加解密以及 DEK 的派生。DEK 是信封加密流程中的二级密钥，用于加密业务数据的密钥，受用户主密钥 CMK 的保护。

关于使用 CMK 及 DEK 进行业务加解密的场景，请参见 敏感数据加密 和 信封加密最佳实践。

密钥概述

用户主密钥 CMK

用户主密钥是 KMS 中的核心资源，这些主密钥经过第三方认证硬件安全模块（HSM）的保护，作为用户加密解密的一级密钥。KMS 服务主要是针对用户主密钥的管理服务。

用户主密钥 CMK 是主密钥的逻辑表示。CMK 包含元数据，例如密钥 ID、创建日期、描述和密钥状态等。通常情况下您可以使用 KMS 的自动生成用户主密钥功能来生成 CMK，同时支持您自有密钥的导入来形成 CMK。

用户主密钥 CMK 包括用户密钥和云产品密钥两种类型：

- **用户密钥**是用户通过控制台或 API 来创建的用户主密钥。您可以对用户密钥进行创建/启用/禁用/轮换/权限控制等操作。
- **云产品密钥**是腾讯云产品/服务（例如 CBS、COS、TDSQL 等）在调用密钥管理服务时，自动为用户创建的 CMK。您可以对云产品密钥进行查询及开启密钥轮换操作，不支持禁用、计划删除操作。

数据加密密钥 DEK

数据加密密钥是基于 CMK 生成的二级密钥，可用于用户本地数据加密解密。
您可以使用 KMS 用户主密钥（CMK）生成 DEK，但是，KMS 不会存储、管理或跟踪您的 DEK，也不会用于 DEK 执行加密操作。您必须在 KMS 之外使用和管理 DEK。

一般 DEK 在信封加密流程中使用，通过 DEK 进行本地业务数据的加密。DEK 受用户主密钥 CMK 保护，可以自定义，也可以通过 GenerateDataKey 接口来创建 DEK。

操作总览

操作	说明
创建密钥	通过控制台快速创建密钥
查看密钥	通过控制台查看密钥 ID 和详情信息
编辑密钥	通过控制台编辑密钥名称、描述信息等
启用禁用密钥	通过控制台启用/禁用密钥
密钥轮换	通过控制台开启密钥轮换
加密解密	通过控制台密钥加密数据
删除密钥	通过控制台快速删除密钥
访问控制	设定子账号管理密钥管理服务的权限

密钥管理
创建密钥

最近更新时间：2022-04-15 14:39:30

操作场景

您可以在腾讯云密钥管理系统（合规）控制台中或通过 CreateKey 接口来创建 CMK，创建成功之后您可以对 CMK 进行启用、禁用、轮换、权限控制等操作。本文为您介绍如何通过控制台创建 CMK。

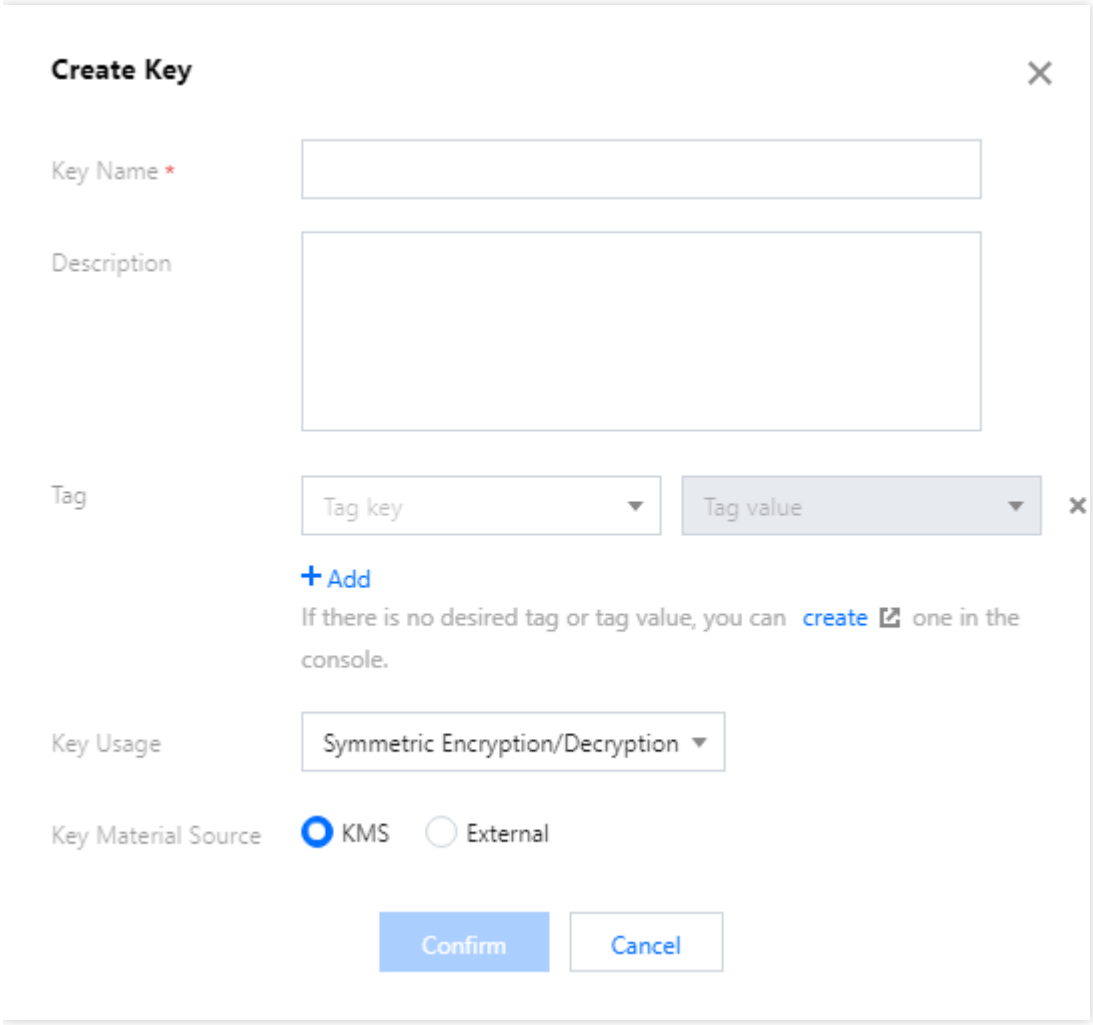
操作步骤

1. 登录 密钥管理系统（合规） 控制台。
2. 选择需要创建密钥的区域，单击【新建】。

3. 在弹出的配置框中，输入以下信息：

- 密钥名称：必填且在区域内唯一，密钥名称只能为字母、数字及字符 `_` 和 `-`，且不能以 “KMS-” 开头。
- 描述信息：选填，用来说明您计划保护的数据类型或计划与 CMK 配合使用的应用程序。
- 标签：非必选，标签 是腾讯云提供的管理资源工具，用户可以通过添加标签对密钥进行分类、搜索和聚合。
- 密钥用途：必选，选择对称加解密、非对称加解密或者非对称签名验签。
- 密钥材料来源：必选，选择密钥生成方式，KMS 生成或者用户自有密钥导入。

> 说明：
> 密钥材料来源为外部时，只支持用途为对称加解密。



4. 单击【确定】后返回密钥列表，新创建的密钥会出现在密钥列表首位。

查看密钥

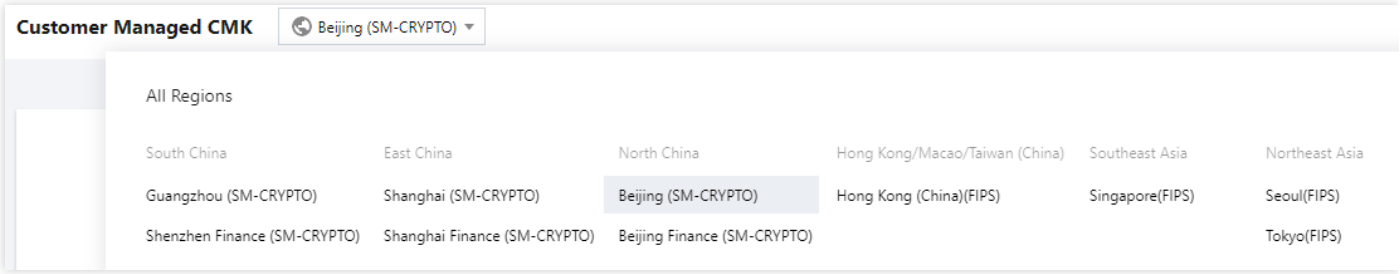
最近更新时间：2022-04-29 15:34:31

操作场景

您可以登录腾讯云密钥管理系统（合规）控制台或调用 KMS TCCLI 查看用户主密钥 CMK ID 信息列表、名称、ID、状态、所属地区等密钥详情。本文为您介绍通过控制台方式查看 CMK ID 信息列表和详情。

查看密钥 ID 列表

1. 登录 密钥管理系统（合规） 控制台。
2. 切换上方区域可以查看其他区域主密钥列表。



3. 在页面右侧筛选器框中输入 CMK 全称或部分名称或密钥 ID，筛选查找您的密钥。

- 输入名称查找
- 输入 ID 查找

查看密钥 ID 详情

1. 登录 密钥管理系统（合规） 控制台。
2. 找到您需要查看详情的密钥，详细查找密钥方法，可参见 查看密钥 ID 列表。
3. 单击密钥的密钥 ID/密钥名称，即可查看该密钥的详细信息。

编辑密钥

最近更新时间：2019-11-15 17:48:16

操作场景

您可以在腾讯云密钥管理服务（合规）控制台中或调用 KMS TCCLI 来编辑主密钥 CMK，您可以更改描述以及启用和禁用密钥轮换。本文向您详细介绍如何通过控制台编辑主密钥 CMK。

操作步骤

1. 登录 密钥管理服务（合规） 控制台。
2. 单击需要编辑的密钥的 ID/名称，进入该密钥的详情页，您可修改密钥的名称、状态、轮换设置以及描述信息等。

3. 修改完单击确定后，系统自动刷新您的更改。

启用禁用密钥

最近更新时间：2019-11-15 17:48:45

操作场景

您可以登录腾讯云密钥管理服务（合规）控制台或通过调用 KMS TCCLI 对创建好的用户主密钥进行启用/禁用密钥状态设置。本文为您介绍如何通过控制台方式启用/禁用密钥。

操作步骤

单个操作

1. 登录 密钥管理服务（合规） 控制台。
2. 找到您需要更改状态的密钥，在其密钥信息的右侧操作区域，可以对该密钥进行启用、禁用操作。

批量操作

1. 登录 密钥管理服务（合规） 控制台。
2. 勾选多个您需要更改状态的密钥。

3. 在列表上方，单击【启用密钥】或【禁用密钥】，系统将如下弹出确认框，单击【查看详情】可以确认本次批量操作密钥的状态。

4. 确认无误后，单击【确定】，即可对批量对密钥进行启用或禁用。

密钥轮换

最近更新时间：2019-11-15 17:50:23

操作场景

为进一步提升密文存储的安全性，腾讯云密钥管理服务（合规）KMS 为用户提供透明密钥轮换能力，可用来刷新存储密文。
CMK 密钥轮换为用户提供透明密钥轮换能力，CMK 密钥轮换后不影响用户业务，兼容轮换前加密的密文，此外提供 ReEncrypt 接口可以将密文刷新。本文为您介绍如何通过控制台启用密钥轮换。

操作步骤

1. 登录 密钥管理服务（合规） 控制台。
2. 找到您需要启用轮换的密钥，在其右侧“密钥轮换”一栏下，单击【启用轮换】，即可为该密钥启用轮换。

> **⚠ 注意：**
>
> 默认情况下，密钥轮换处于关闭状态。您可设置是否打开。开启后， CMK 将一年轮换一次。

加密解密

最近更新时间：2021-10-08 11:56:14

操作场景

腾讯云密钥管理系统（合规）KMS 提供了对于小型数据加密、解密的 API、SDK 以及在线工具，您可以根据自己的需要以及不同的场景选择合适的使用方式。

在线工具

在线工具适合处理单次或者非批量的加解密操作，例如首次生成密钥密文，开发者无需为非批量的加解密操作而去开发额外的工具，将精力集中在实现核心业务能力上，使用步骤如下。

前提条件

已事先 创建密钥，且保证密钥为启用状态。

操作步骤

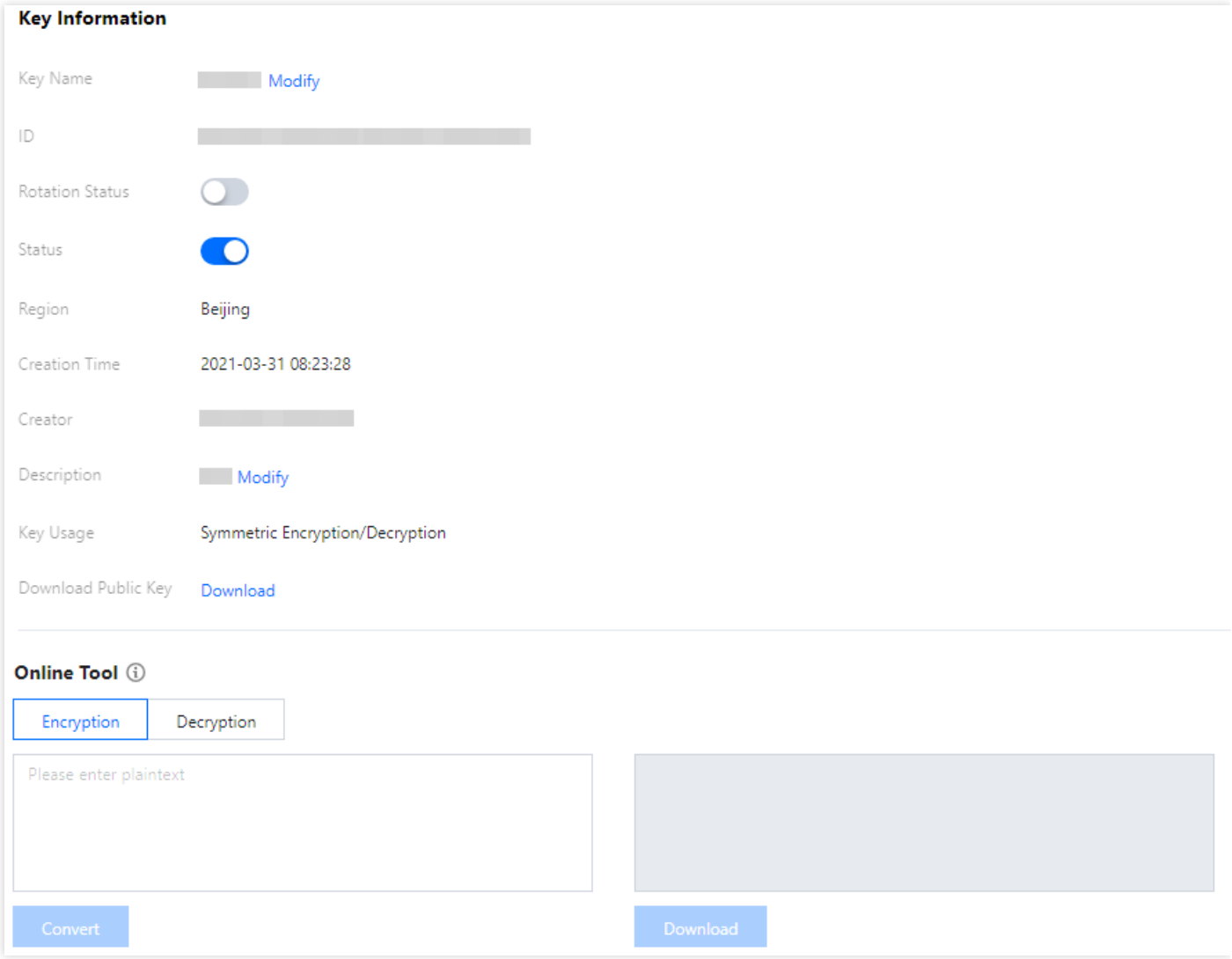
1. 登录 密钥管理系统（合规） 控制台。

2. 找到您需要加解密的密钥，在“密钥ID/密钥名称”操作栏下，单击**密钥名称**，进入密钥详情页面。

3. 在“在线工具”模块下，单击**加密操作**。

4. 在下方的输入框中输入待处理数据。

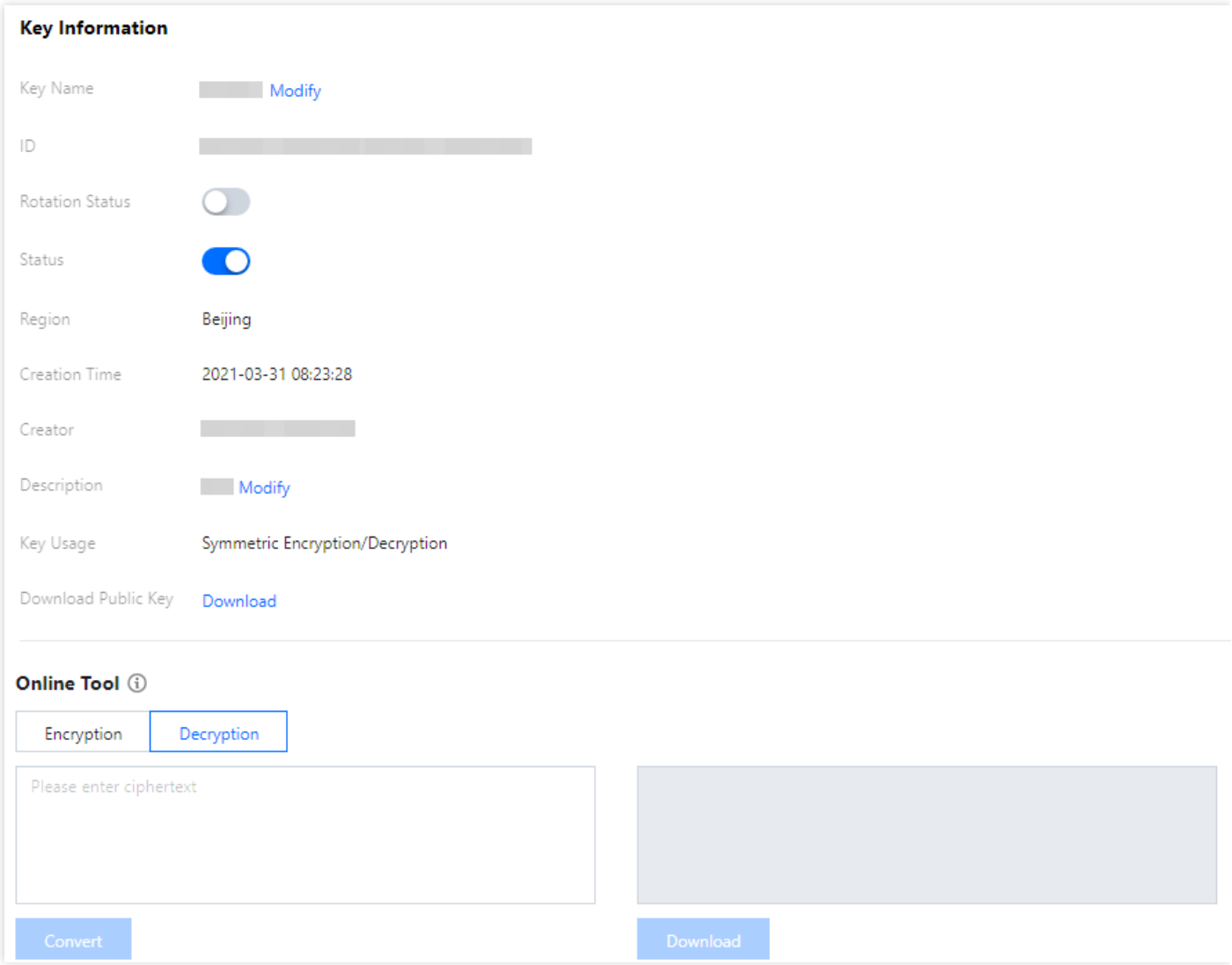
5. 单击**执行**，系统处理后的数据将显示在右边的灰色框中。



6. 数据加密之后，您可以单击**下载**，将数据下载到本地电脑，至此加密操作完成。

7. 若需要解密，在“在线工具”模块下，单击**解密操作**。

8. 在下方的输入框中粘贴此前加密的数据，单击**执行**，解密后的数据将显示在右边的灰色框中。



注意：
解密操作根据密文使用的主密钥，自动调用该主密钥进行解密操作。解密后明文以 Base64 展示。

9. 您可以单击【下载】，将解密后的数据下载到本地电脑。

删除密钥

最近更新时间：2021-09-27 14:30:13

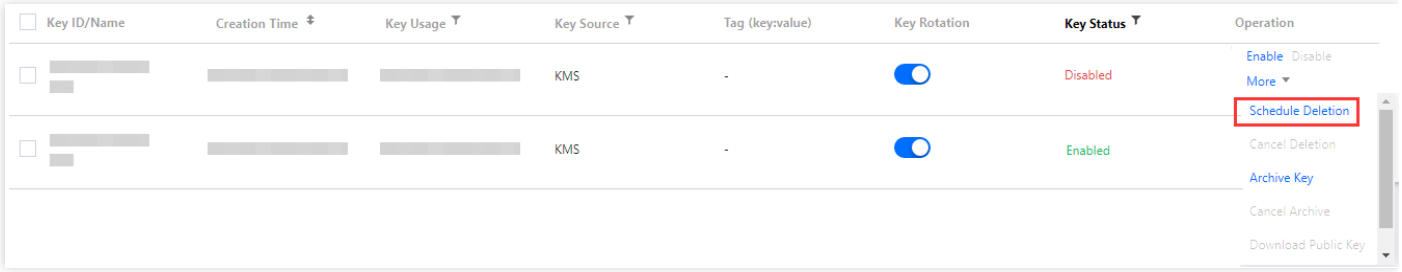
操作场景

密钥删除后将无法恢复，此密钥下的所有加密数据也将无法解密。为避免误删除操作，KMS 使用计划删除机制，即对删除操作强制执行7 - 30天的等待期。在等待期内，您可以对计划删除内密钥进行取消删除操作。

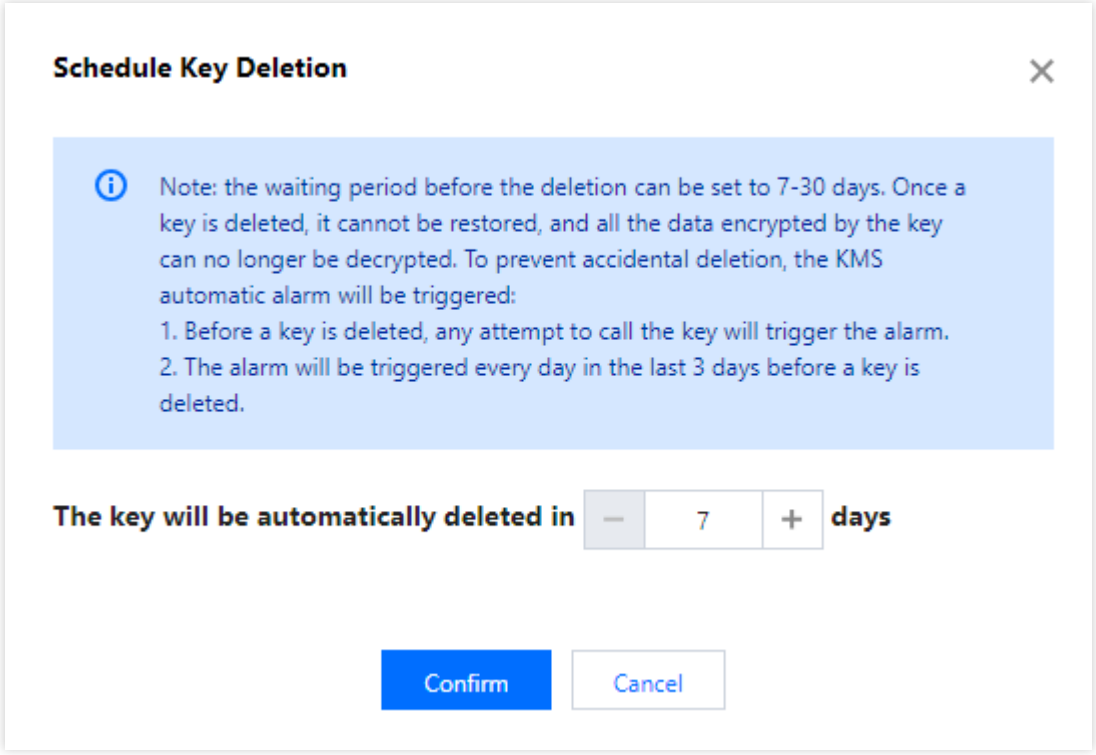
您可以登录腾讯云密钥管理系统（合规）控制台或调用 KMS TCCLI 进行密钥计划删除和取消计划删除操作。本文为您详细介绍如何通过控制台删除密钥。

操作步骤

1. 登录 密钥管理系统（合规） 控制台。
2. 选择需要计划删除的密钥，在其右侧单击【计划删除】。若是正在启用状态的密钥请先对密钥进行禁用操作。



3. 输入计划删除天数，单击【确定】，确认计划删除以及指定天数后，密钥将按计划删除。



注意：

计划删除天数可选范围为7-30天。密钥删除后将无法恢复，此密钥下的所有加密数据也将无法解密。

为避免误删除行为，KMS服务将对以下操作进行自动告警：

- 密钥被彻底删除前，对尝试调用此密钥的行为进行提示告警。
- 密钥被彻底删除前3天，每天提示告警。

4. 若需取消删除密钥，单击【取消删除】，即可取消删除密钥，确认取消删除后，密钥重置为“已禁用”状态，可对该密钥进行启用/修改/删除等操作。

访问控制
概述

最近更新时间：2019-11-15 18:02:21

如果您使用到了密钥管理服务（KMS）、私有网络（VPC）、云服务器、数据库等服务，这些服务由不同的人管理，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，通过 CAM，您可以通过身份管理和策略管理控制哪些子账号有哪些资源的操作权限。

例如，您的根账户下有个主密钥，您只想让子帐号 A 使用该主密钥，而让子账号 B 不能使用，就可以通过在 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 KMS 相关资源的访问控制，您可以跳过此章节。跳过这些部分并不影响您对文档中其余部分的理解和使用。

CAM 基本概念

根账户通过给子账户绑定策略实现授权，策略设置可精确到（**API，资源，用户/用户组，允许/拒绝，条件**）维度。

- **账户**
  - **根账号**：腾讯云资源归属、资源使用计量计费的基本主体，可登录腾讯云服务。
  - **子账号**：由根账号创建账号，有确定的身份 ID 和身份凭证，且能登录到腾讯云控制台。根账号可以创建多个子账号(用户)。**子账号默认不拥有资源，必须由所属根账号进行授权。**
  - **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 KMS 的一个主密钥，云服务器实例，COS 存储桶，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，**根账号拥有其名下所有资源的访问权限**，而**子账号没有根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。**根账号**通过将**策略关联**到用户/用户组完成授权。

了解更多请参阅 CAM 产品文档。

相关文档

目标	链接
了解策略和用户之间关系	策略管理
了解策略的基本结构	策略语法
了解还有哪些产品支持 CAM	支持 CAM 的产品

子账号管理

最近更新时间：2020-03-16 15:04:47

概述

本文为您详细介绍如何创建子账号，并授权子账号管理 KMS 的权限。

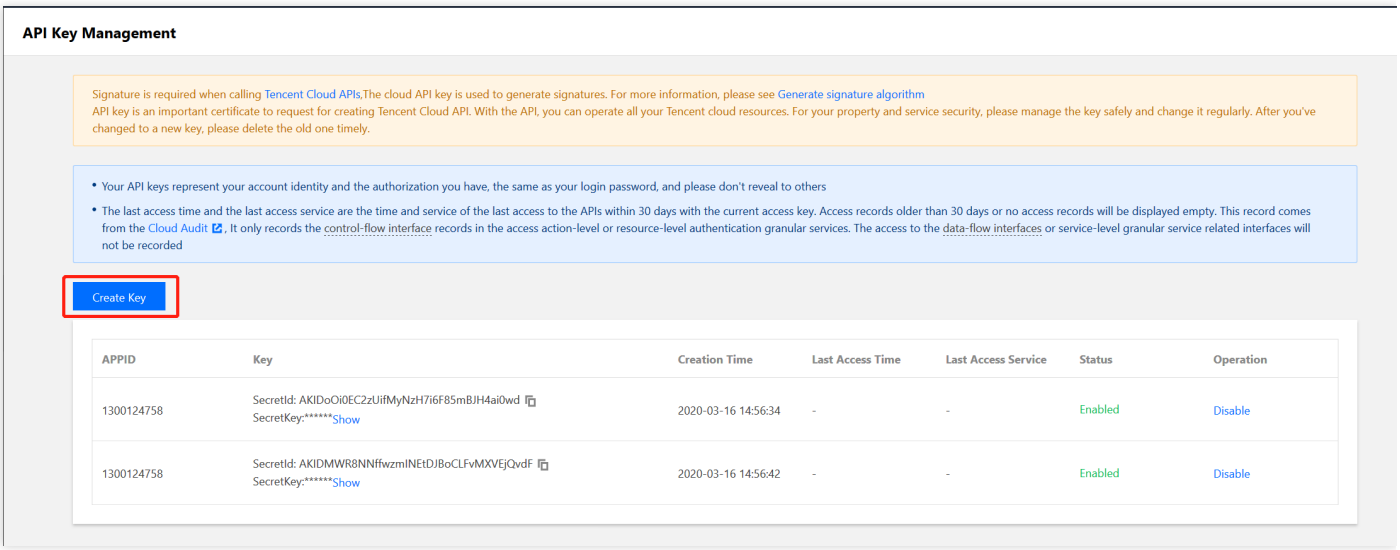
操作步骤

步骤1：创建子账号:

1. 主账号登录腾讯云 访问管理 CAM 控制台。
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:

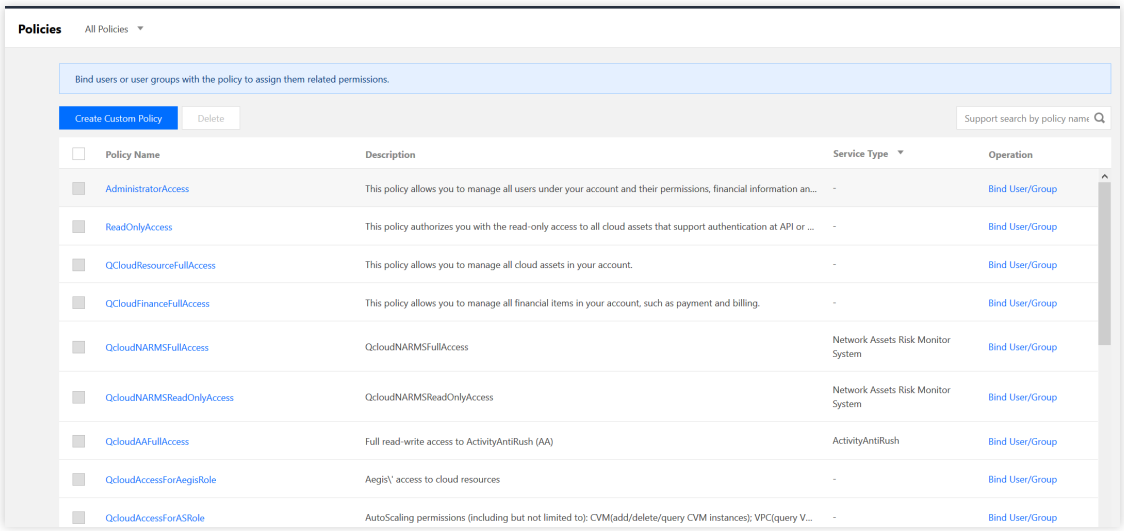
1. 单击子账号名称，进入子账号详情页。
2. 选择【API 密钥】>【新建密钥】，即可创建 SecretId 和 SecretKey，通过该 API 密钥用来访问 KMS。



步骤3：授权子账号

对于新创建的子账号，通过授权 KMS 策略，即可允许该子账号访问 KMS。

1. 选择【权限】>【关联策略】>【从策略列表中选取策略关联】，选择合适的 KMS 策略。



2. 单击【下一步】>【确定】，即可授权子账号 KMS 权限。

创建访问控制策略

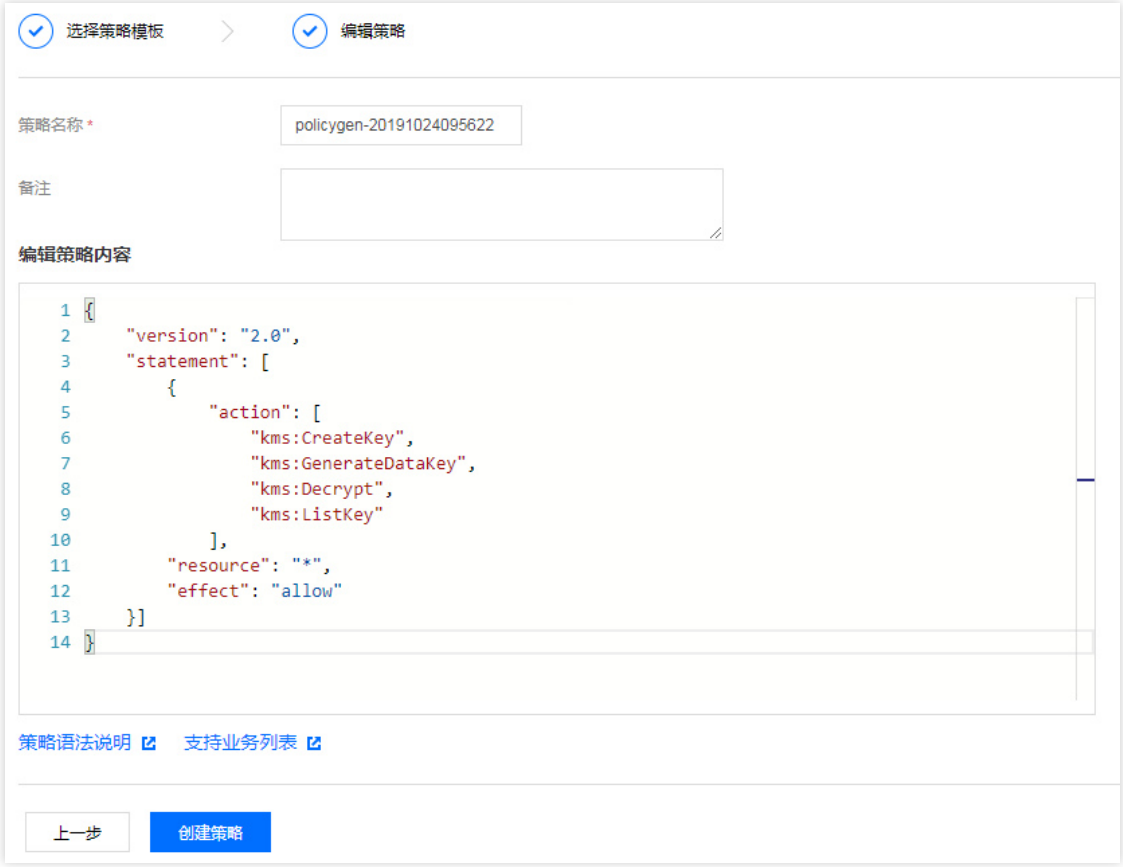
最近更新时间：2020-12-17 12:29:59

概述

本文为您详细介绍在访问管理控制台创建 KMS 策略的操作。

操作步骤

1. 登录 访问管理 控制台。
2. 在左侧菜单中，现在【策略】>【新建自定义策略】>【按策略语法创建】，进入策略创建页面。
3. 选择策略模板，例如空白模板或 KMS 策略模板，单击【下一步】。
4. 输入策略名称和策略内容，策略内容可参见下方示例。



5. 单击【创建策略】，即可创建。

审计

云审计支持的操作列表

最近更新时间：2021-03-24 17:51:25

在腾讯云 云审计（CloudAudit）服务中，记录了密钥管理系统服务的相关操作事件，云审计支持的操作列表如下：

操作名称	事件名称
创建主密钥	CreateKey
获取主密钥属性	DescribeKey
获取多个主密钥属性	DescribeKeys
获取主密钥列表	ListKey
获取主密钥列表详情	ListKeyDetail
修改主密钥描述信息	UpdateKeyDescription
修改别名	UpdateAlias
启用主密钥	EnableKey
禁用主密钥	DisableKey
批量启动主密钥	EnableKeys
批量禁用主密钥	DisableKeys
计划删除主密钥	ScheduleKeyDeletion
取消计划删除主密钥	CancelKeyDeletion
获取导入主密钥（CMK）材料的参数	GetParametersForImport
导入密钥材料	ImportKeyMaterial
创建白盒密钥	CreateWhiteBoxKey
使用白盒密钥进行加密	EncryptByWhiteBox
启用白盒密钥	EnableWhiteBoxKey
禁用白盒密钥	DisableWhiteBoxKey

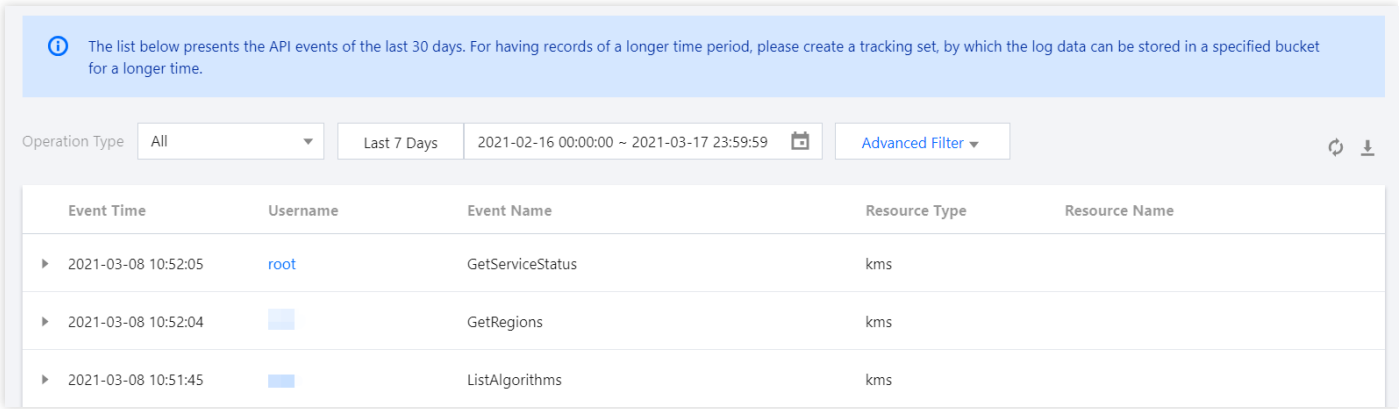
批量启用白盒密钥	EnableWhiteBoxKeys
批量禁用白盒密钥	DisableWhiteBoxKeys
删除白盒密钥	DeleteWhiteBoxKey
获取白盒密钥服务状态	DescribeWhiteBoxServiceStatus
覆盖指定密钥的设备指纹信息	OverwriteWhiteBoxDeviceFingerprints
获取指定密钥的设备指纹列表	DescribeWhiteBoxDeviceFingerprints
获取白盒解密密钥	DescribeWhiteBoxDecryptKey
解密	Decrypt
加密	Encrypt
签名	SignByAsymmetricKey
验证签名	VerifyByAsymmetricKey
密钥存档	ArchiveKey
取消密钥存档	CancelKeyArchive
获取服务可用的地域	GetRegions
密文刷新	ReEncrypt
随机数生成接口	GenerateRandom
生成数据密钥	GenerateDataKey
查询服务状态	GetServiceStatus
列出当前 Region 支持的加密方式	ListAlgorithms
禁止密钥轮换	DisableKeyRotation
开启密钥轮换	EnableKeyRotation
查询密钥轮换状态	GetKeyRotationStatus
绑定密钥和云产品资源的使用关系	BindCloudResource
解绑 CMK 和云资源的关联关系	UnbindCloudResource
获取非对称密钥的公钥	GetPublicKey

非对称密钥 Sm2 解密	AsymmetricSm2Decrypt
非对称密钥 RSA 解密	AsymmetricRsaDecrypt

查看审计日志

最近更新时间：2021-09-08 17:05:16

1. 登录 云审计控制台 。
2. 在左侧导航中，单击【操作记录】，进入操作记录页面。
3. 在操作记录页面中，您可以根据用户名、资源类型、资源名称、事件源、事件 ID 、关键词或对应操作事件时间，获取相关的操作记录信息，默认情况下只展示部分数据。



4. 获取相关操作记录列表后，可以单击该操作记录左侧的展开按钮，可查看此操作记录的详情，包括事件时间、用户名、事件名称、访问密钥、事件 ID 等信息，单击【查看事件】，可了解事件相关的更多信息。