密钥管理服务

快速入门

产品文档

腾讯云

文档目录

快速入门
快速开始

最近更新时间：2019-08-27 17:02:01

在控制台界面通过可视化的单击操作来快速创建和登录到密钥管理服务（合规）。关于控制台的更多操作请参见 控制台文档。
下例中我们以快速配置为例来演示如何快速配置相关选项，实际购买时用户也可以选择自定义配置来选择更多的配置项。
其操作流程如下图所示：

第1步：登录控制台

登录腾讯云控制台。如果没有账号，请参见 账号注册教程。

第2步：立即购买

进入 密钥管理服务（合规）控制台，单击【立即购买】，即可开通密钥管理服务。密钥管理服务采用按月后付费的结算机制，开通后按实际使用量计费。

第3步：控制台操作

开通后，即可通过控制台或 API 接口进行创建、启用、禁用、轮换设置、别名设置等密钥管理服务操作。了解更多，请参见 快速入门 文档。

创建密钥

最近更新时间：2019-08-27 17:02:11

操作场景

本文为您详细介绍如何在密钥管理服务控制台创建密钥。

操作步骤

1. 登录 密钥管理服务控制台。
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。

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，也可以通过密钥名称来识别新创建的密钥。

管理密钥

最近更新时间：2019-08-27 17:03:27

操作场景

本文为您详细介绍如何查看、启用/禁用，修改密钥以及密钥轮换等操作。

查看密钥

登录 密钥管理服务控制台，注意主密钥是区分区域的，通过切换上方区域可以查看其他区域主密钥列表。

启用/禁用密钥

您可以通过以下方式启用/禁用密钥：单个操作 和 批量操作。

单个操作

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

> 注意：
> 禁用密钥会导致所有依赖该密钥的加解密操作被同时禁用，所以在禁用密钥前，请确认没有运行中业务依赖该密钥。

找到您需要更改的密钥并勾选，单击列表上方的【启用密钥】或【禁用密钥】，页面将弹出“操作确认框”，继续单击【确认】，则可对所有选中密钥进行对应操作。

如果同时选择了不同可用状态的密钥，则会在单击批量【启用密钥】或【禁用密钥】后，页面将在弹出的"操作确认框"里进行相应提示，单击【确定】，系统只会对状态符合要求的密钥进行操作，不符合的密钥保持原有可用状态。

密钥轮换

在密钥列表页面右侧的"密钥轮换"操作栏下，您可以对该密钥进行密钥轮换操作。默认情况下，密钥轮换处于关闭状态。由用户设置是否打开。开启后 CMK 会一年交换一次。

查看密钥详情

在密钥列表页面，单击任一密钥的【密钥ID/密钥名称】即可进入该密钥的详情页面，您可以查看和修改该密钥的信息，也可以通过该页面的在线工具进行加密或解密。

修改名称、用途

在密钥详情页，您可以修改密钥的名称、用途。
单击【密钥名称】或【密钥用途】，在弹出的对话框内输入需要新的内容。注意密钥名称只能为字母、数字及字

符 _ 和 - ，且不能以“KMS-”开头。

加密解密

最近更新时间：2019-04-30 16:06:40

概述

KMS 提供加密解密接口，加密接口（Encrypt）用于加密最多为4KB的任意数据，可用于加密数据库密码，RSA Key，或其它较小的敏感信息。解密接口（Decrypt）用于对密文解密。生成的 DataKey 通过解密接口可以得到密钥的明文数据。

在线工具

适合处理单次或者非批量的加解密操作，比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。下面为您详细介绍如何使用在线加密工具对小型数据进行加密。

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. 登录密钥管理服务控制台。
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，选择【加密】或【解密】。
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. 您可以单击【下载】，将数据下载到本地电脑。

内测版 KMS 迁移指引

最近更新时间：2019-09-03 10:49:36

概述

腾讯云内测版密钥管理服务由于架构改进，计划进行 EOL（end-of-life）流程。您可以永远使用内测旧版密钥管理服务，及其提供的所有功能服务，但后续将不再支持升级。

官网已正式上线全新 密钥管理服务（合规） 做服务替换。新版密钥管理服务 KMS 完全满足合规标准，提供了更为丰富的密钥管理功能，且大大提高了可靠性设计。

注意：

- 内测版密钥管理服务系统将永久维护，此次变更不影响您的正常业务使用。
- 内测版密钥管理服务采用 API/SDK 2017 接口提供服务。若需确认您是否正在使用内测版密钥管理服务，可 提交工单 与我们联系。

价格说明

密钥管理服务 KMS，由 CMK 存储费用及 API 调用费用两部分组成，详细请参见 计费概述。

步骤说明

步骤1：内测旧 KMS 服务用户，可先在官网重新开通使用新的密钥管理服务（合规）。
步骤2：使用新版 KMS，创建用户主密钥 CMK。
步骤3：将内测旧版 KMS 服务加密的数据进行解密：按照 API/SDK 2017 接口规范，使用旧版 SDK，调用解密 Decrypt 接口，获取明文数据。
步骤4：通过新的密钥管理服务（合规）系统的 SDK 重新进行加密。

敏感数据加密迁移步骤

敏感信息加密是密钥管理服务 KMS 核心的能力，实际应用中主要用来保护服务器硬盘上敏感数据的安全（小于 4KB），如密钥、证书、配置文件等，详情请参见 敏感信息加密。

1. 开通 密钥管理服务（合规）服务。
2. 按照业务需求，在密钥管理服务（合规）创建相应的用户主密钥 CMK。
3. 内测版密钥管理服务加密的数据进行解密：按照 API/SDK 2017 接口规范，使用旧版 SDK，调用解密 Decrypt 接口，获取明文数据，请参见 解密 API 文档。
4. 新版密钥管理服务（合规）敏感数据加密： 按照腾讯云 API 3.0 标准，使用新版 SDK，调用加密 Encrypt 接口进行加密，详情请参见 加密 API 文档。
5. 新版密钥管理服务（合规）敏感数据解密：按照腾讯云 API3.0 标准，使用新版 SDK，调用解密 Decrypt 接口进行解密，详情请参见 解密 API 文档。

信封加密迁移步骤

信封加密（Envelope Encryption）是一种应对海量数据的高性能加解密方案，详情请参见 信封加密。

1. 开通 密钥管理服务（合规） 服务。
2. 按照业务需求，在密钥管理服务（合规）创建相应的用户主密钥 CMK。
3. 内测版密钥管理服务加密数据进行解密：只需要处理 DataKey 的迁移，按照 API/SDK 2017 接口规范，使用旧版本 SDK，调用解密 Decrypt 接口，获取明文 DataKey，详情请参见 解密 API 文档。
4. 新版密钥管理服务（合规）信封加密：按照腾讯云 API 3.0 标准，使用新版 SDK，调用加密 Encrypt 接口进行加密，详情请参见 加密 API 文档。
5. 新版密钥管理服务（合规）信封解密：按照腾讯云 API 3.0 标准，使用新版 SDK，调用解密 Decrypt 接口解密 DataKey 获取明文，使用 DataKey 明文对数据进行解密。详情请参见 解密 API 文档。