凭据管理系统

操作指南

产品文档

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

本文档著作权归腾讯云单独所有，未经腾讯云事先书面许可，任何主体不得以任何形式复制、修改、抄袭、传播全部或部分本文档内容。

【商标声明】

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。

【服务声明】

本文档意在向客户介绍腾讯云全部或部分产品、服务的当时的整体概况，部分产品、服务的内容可能有所调整。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。

文档目录

- 操作指南
  - 自定义凭据
    - 创建凭据
    - 编辑凭据
    - 多版本管理
    - 删除凭据
    - 标签
      - 编辑标签
      - 使用标签管理示例
  - 数据库凭据
    - 概述
    - 使用说明
    - 创建数据库凭据
    - 编辑数据库凭据
    - 启用禁用数据库凭据
    - 删除数据库凭据
    - 标签
      - 编辑标签
      - 使用标签管理示例
  - 日志审计
  - 访问控制
    - 概述
    - 子账号管理
    - 创建访问控制策略

版权所有：腾讯云计算（北京）有限责任公司

操作指南
自定义凭据
创建凭据

最近更新时间：2024-08-01 19:03:55

操作场景

您可以在凭据管理系统控制台中创建凭据，凭据创建成功后，您可以对凭据进行启用、禁用、修改、计划删除等操作。

操作步骤

1. 登录 凭据管理系统控制台，在左侧导航栏中，单击**自定义凭据**。
2. 在自定义凭据左上角选择需要创建凭据的地区，单击**新建**。
3. 在弹出的配置框中，输入相应信息，信息输入完成后，单击**确定**，返回凭据列表，新创建的凭据会出现在凭据列表首位。

版权所有：腾讯云计算（北京）有限责任公司

字段说明：

凭据名称：名称长度1 - 128字节，使用字母、数字、连接符（-）、下划线（_）的组合，首字符必须为字母或者数字。

凭据版本：必填。

凭据内容：必填。

描述信息：非必填。

标签：非必填。

选择加密密钥：

使用凭据管理系统在密钥管理系统（KMS）中默认创建的主密钥（CMK）进行加密。

使用自定义加密密钥。

说明：

若使用凭据管理系统表明您已开启 密钥管理系统，您可以通过以下两种方案创建加密密钥：

选择在 密钥管理系统控制台 中默认创建的云产品主密钥作为加密密钥，并通过信封加密方案进行加密存储。

选择在 密钥管理系统控制台 中创建一个用户密钥，将该密钥作为自定义的加密密钥对凭据进行加密存储。

版权所有：腾讯云计算（北京）有限责任公司

编辑凭据

最近更新时间：2024-08-01 19:03:55

操作场景

您可以登录腾讯云凭据管理系统控制台查看并编辑凭据信息列表、名称、状态、所属地区等凭据详情。

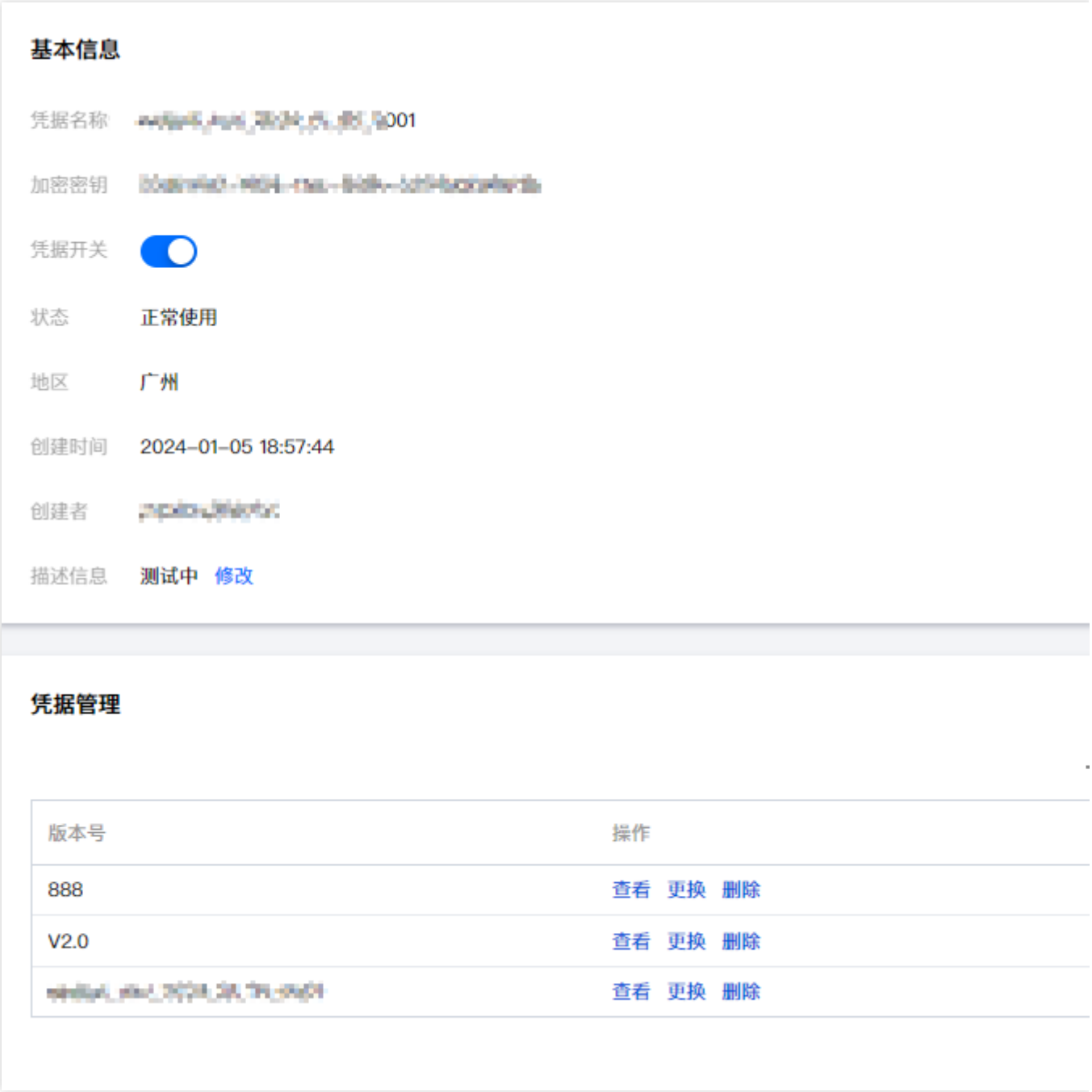
编辑凭据

1. 登录 凭据管理系统控制台，在左侧导航栏中，单击**凭据列表**，在凭据列表左上方可以切换不同地区，根据需求查看并编辑其他地区的凭据列表。

2. 在页面右侧搜索框中，输入凭据全称或部分名称，查找您需要的凭据。

3. 单击凭据名称，即可查看该凭据的详细信息，同时可以对该凭据的密钥进行启用或禁用状态设置。

4. 进入该凭据的详情页，您可查看凭据的名称、状态、描述信息以及版本号等内容，同时可以对凭据内容进行更改、删除、版本管理等操作。


基本信息
凭据名称
001
加密密钥
凭据开关
状态
正常使用
地区
广州
创建时间
2024-01-05 18:57:44
创建者
描述信息
测试中
修改
凭据管理
版本号
操作
888
查看 更换 删除
V2.0
查看 更换 删除
查看 更换 删除

多版本管理

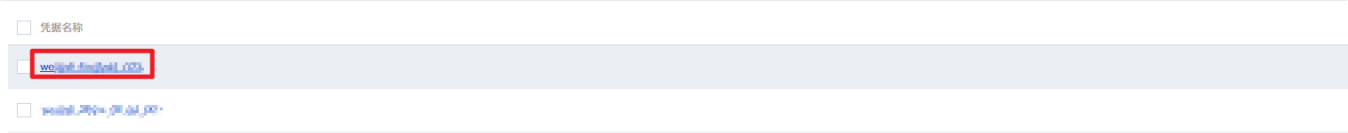
最近更新时间：2024-08-01 19:03:55

操作场景

凭据管理系统为用户提供凭据多版本管理服务。用户可以通过多版本管理特性，灰度实现应用层的凭据轮换。

操作步骤

1. 登录 凭据管理系统控制台 ，在左侧导航栏中，单击**凭据列表，**在凭据列表左上方可以切换不同地区，找到您需要添加凭据版本的凭据，单击凭据名称进入凭据详情页。



2. 在凭据管理区域，单击**添加**，进入添加凭据信息页面。

3. 在添加凭据信息页面，填写凭据版本和凭据内容，填写完成后，单击**添加**，即可完成凭据新版本添加操作。

版权所有：腾讯云计算（北京）有限责任公司

4. 凭据添加完后，如需删除，可以在对应版本右侧操作栏，单击**删除**，在弹出的删除确认框中，确认删除即可。

注意：

同一个凭据可以多版本并存，每个凭据最多同时存在10个版本。

删除凭据

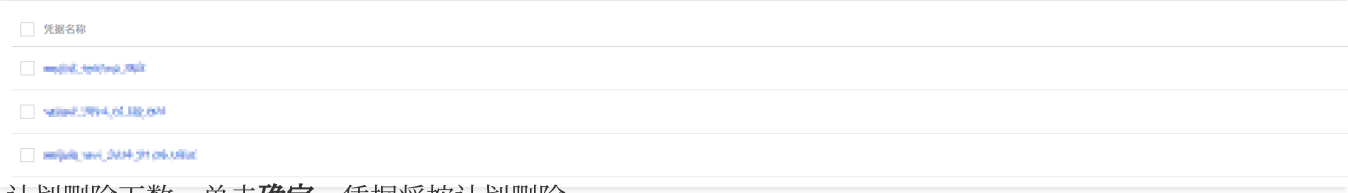
最近更新时间：2024-08-01 19:03:55

注意事项

为避免误删除操作，凭据管理系统使用计划删除机制，即**对删除操作强制执行0 - 30天等待期**，并确认删除后等待0 - 30天再进行删除。
凭据删除后将**无法恢复**，此凭据下的所有凭据内容也将**无法调用**。

操作步骤

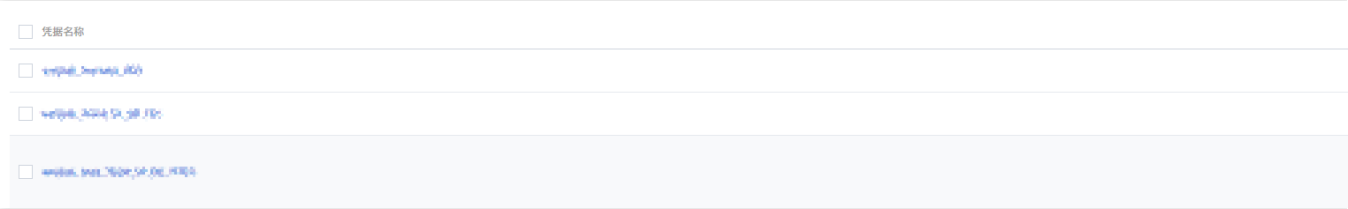
1. 登录 凭据管理系统控制台，在左侧导航栏中，单击**凭据列表**，在凭据列表左上方可以切换不同地区，根据需求可以查看其他地区的凭据列表。
2. 在凭据列表中，选择需要计划删除的凭据，若凭据是启用状态，请先对凭据进行禁用操作，然后在计划删除操作栏中，单击**计划删除**。



3. 输入计划删除天数，单击**确定**，凭据将按计划删除。

注意：
若选择等待期为“0”天，凭据将立即删除。

4. 在1 - 30天等待期内，您可以对计划删除的凭据进行取消删除操作。若需取消删除凭据，可以在右侧计划删除操作栏，单击**取消删除**，即可取消删除凭据。确认取消删除后，凭据密钥重置为“启用”状态，可对该凭据进行禁用、修改、删除等操作。



标签
编辑标签

最近更新时间：2024-08-01 19:03:55

操作场景

本文档指导您对资源进行编辑标签的操作。

使用限制

标签内容（标签键、标签值）的使用有相对应的限制条件，详情请查阅 **标签使用限制**。

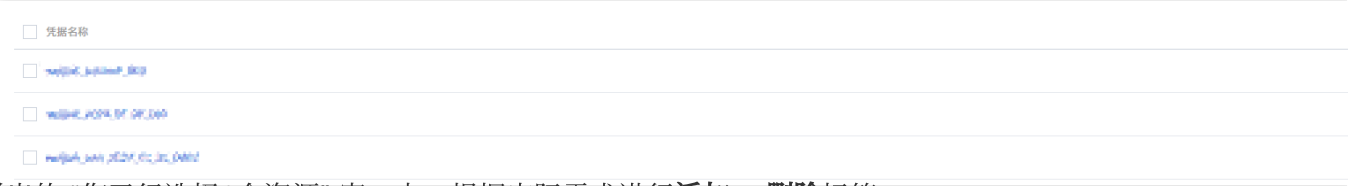
前提条件

1. 已登录 **凭据管理系统** 控制台。
2. 选择需要编辑凭据的所在区域。

操作步骤

单个凭据编辑标签

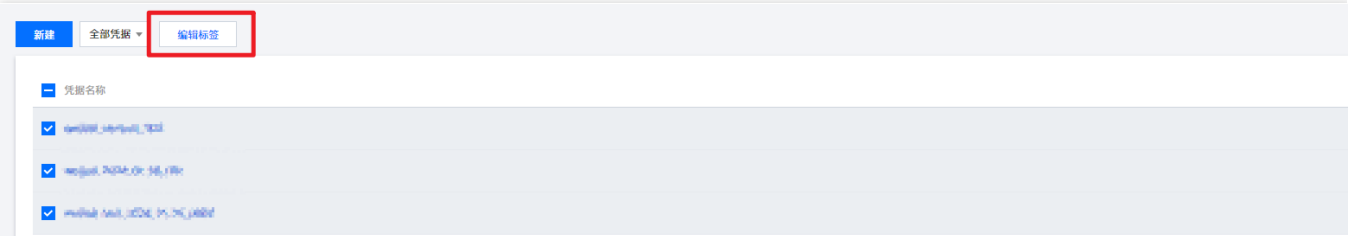
1. 找到需编辑标签的凭据，选择其右侧的**编辑标签**。



2. 在弹出的 “您已经选择1个资源” 窗口中，根据实际需求进行**添加**、**删除**标签。

批量编辑标签

1. 勾选需编辑标签的凭据，单击凭据顶部的**编辑标签**。



2. 在弹出的 “您已经选择n个资源” 窗口中，根据实际需求进行**添加**、**删除**标签。

说明：

关于如何使用标签，请参见 使用标签管理示例。

使用标签管理示例

最近更新时间：2024-08-01 19:03:55

操作场景

标签是用于从不同的维度对资源分类的管理、权限的管理。

在 **凭据管理系统** 中，标签主要用于**用户凭据。**

在凭据中添加标签，是为了方便用户对凭据进行分类和跟踪管理，同时可以按照标签来汇总对应凭据的使用情况。

使用限制

标签内容（标签键、标签值）的使用有相对应的限制条件，详情请查阅 标签使用限制。

操作方法

在密钥管理控制台设置标签

1. 已登录 **凭据管理系统** 控制台。
2. 选择需要编辑凭据的所在区域。
3. 找到需编辑标签的凭据，选择其右侧的**编辑标签。**

4. 在弹出的 “您已经选择1个资源” 窗口中设置，设置标签，如下图所示：

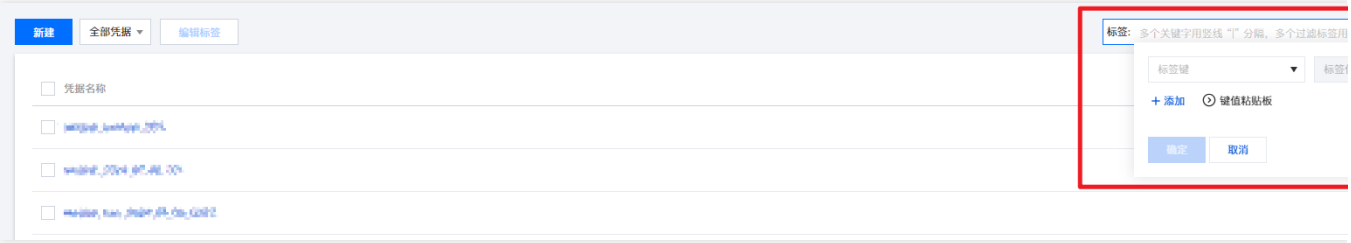
例如，添加两组标签

5. 单击**确定**，系统出现修改成功提示。

通过标签筛选密钥

1. 已登录 凭据管理系统 控制台。
2. 选择需要编辑凭据的所在区域。
3. 在选择的区域凭据列表中，在右侧的搜索框选择以 “**标签**” 作为筛选条件，输入筛选内容即可，如下图所示。

例如：你希望筛选出ower为alex的密钥，可输入标签：owner:alex。



数据库凭据
概述

最近更新时间：2024-01-02 15:13:40

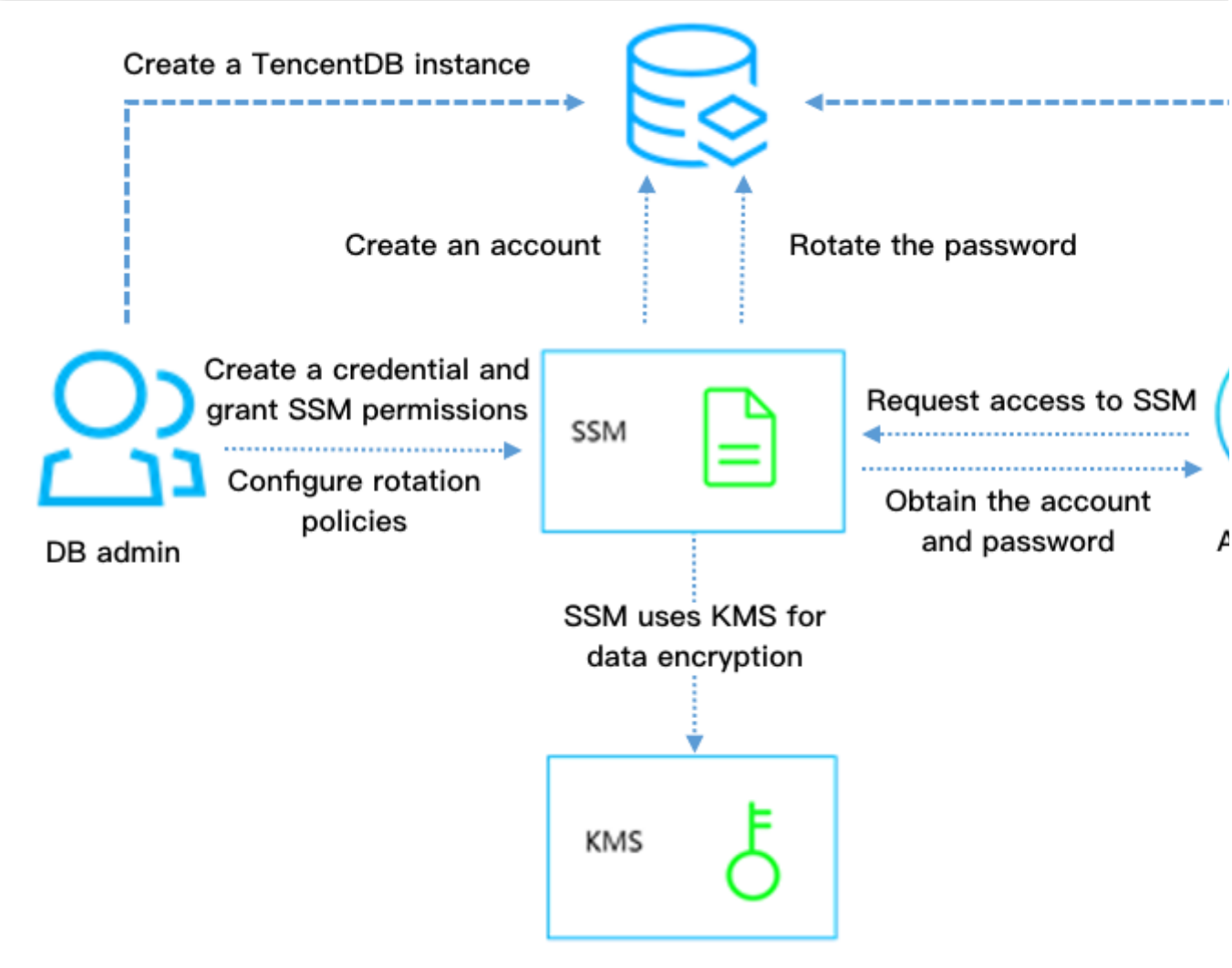
目前云上产品的账号密码面临管理权限失当、账号密码长时间不变更、配置中的密钥信息是明文等问题，导致数字资产损失。针对于这些风险，**数据库凭据**对凭据进行定期轮换，自动创建高强度密码和管理敏感配置信息，在降低账号的风险与安全威胁时，也能提高业务数据的安全性。

主要功能

凭据管理系统 SSM 与控制台集成，接管数据库账号的申请和分发功能。
结合腾讯 密钥管理系统 KMS 为敏感信息配置加密保护。
凭据管理系统 SSM 自动创建高强度密码，并对密码进行定期的修改与轮换。
灵活设置自动轮转的周期。

产品的架构

版权所有：腾讯云计算（北京）有限责任公司



流程说明

1. 管理员创建数据库实例，设置数据库的账号、密码。
2. 管理员在凭据管理系统 SSM 中创建一个数据库凭据对象。

授权 凭据管理系统 SSM 访问 MySQL 管理服务。

设置数据库用户名前缀等。

配置自动轮转的策略。

3. 当应用系统需要访问数据库时，可向凭据管理系统 SSM 请求访问凭据，接口请求详情，请参见 获取凭据明文。
4. 应用系统通过访问凭据接口所返回的内容，解析出明文凭据，并获取到账号和密码，从而访问该用户对应的目标数据库。

使用限制

自动凭据轮换目前支持 **云数据库 MySQL** 和 **TDSQL MySQL版** 。

使用指引

创建数据库凭据
编辑数据库凭据
删除数据库凭据
访问控制

版权所有：腾讯云计算（北京）有限责任公司

使用说明

最近更新时间：2024-01-02 15:13:40

前提条件

已创建数据库凭据，对于未创建数据库凭据的情况，可查阅 创建数据库凭据 进行创建。
凭据已开启轮转，对未开启凭据轮转的情况，可查阅 启用数据库凭据 开启轮转。

轮转的实现效果

SSM 会根据用户预先设定的轮转周期，对凭据中保存的账号密码信息进行更新。客户端通过调用 获取凭据明文 可以获取到最新的有效账号和密码信息。
同一个凭据的账号和密码信息会发生变化，但对应的数据库的访问权限是相同的，SSM 会负责在数据库中同步创建或更新具有相同权限的账号或密码。

应用程序与SSM的集成

应用程序只需要通过调用 获取凭据明文， 即可获取访问数据库最新的有效账号和密码信息，即可用于数据库的访问。

风险提示

风险点

SSM 在对数据库凭据进行周期性轮转时，会更新账号的密码，导致使用过期密码的账号访问数据库失败。

应对方案

为了防止访问数据库失败的情况发生，**请不要在客户端自动保存密码信息和使用带有数据库连接池功能的第三方SDK**。请使用**最佳实践**中推荐的腾讯云官方提供的 **SSM SDK**（ Go 和 Python ） 来连接数据库。

创建数据库凭据

最近更新时间：2024-08-01 19:03:55

操作场景

在 凭据管理系统 控制台中创建数据库凭据，对数据库凭据开启凭据轮转及选择加密，降低账号的泄露风险与安全威胁，并提高业务数据的安全性。

前提条件

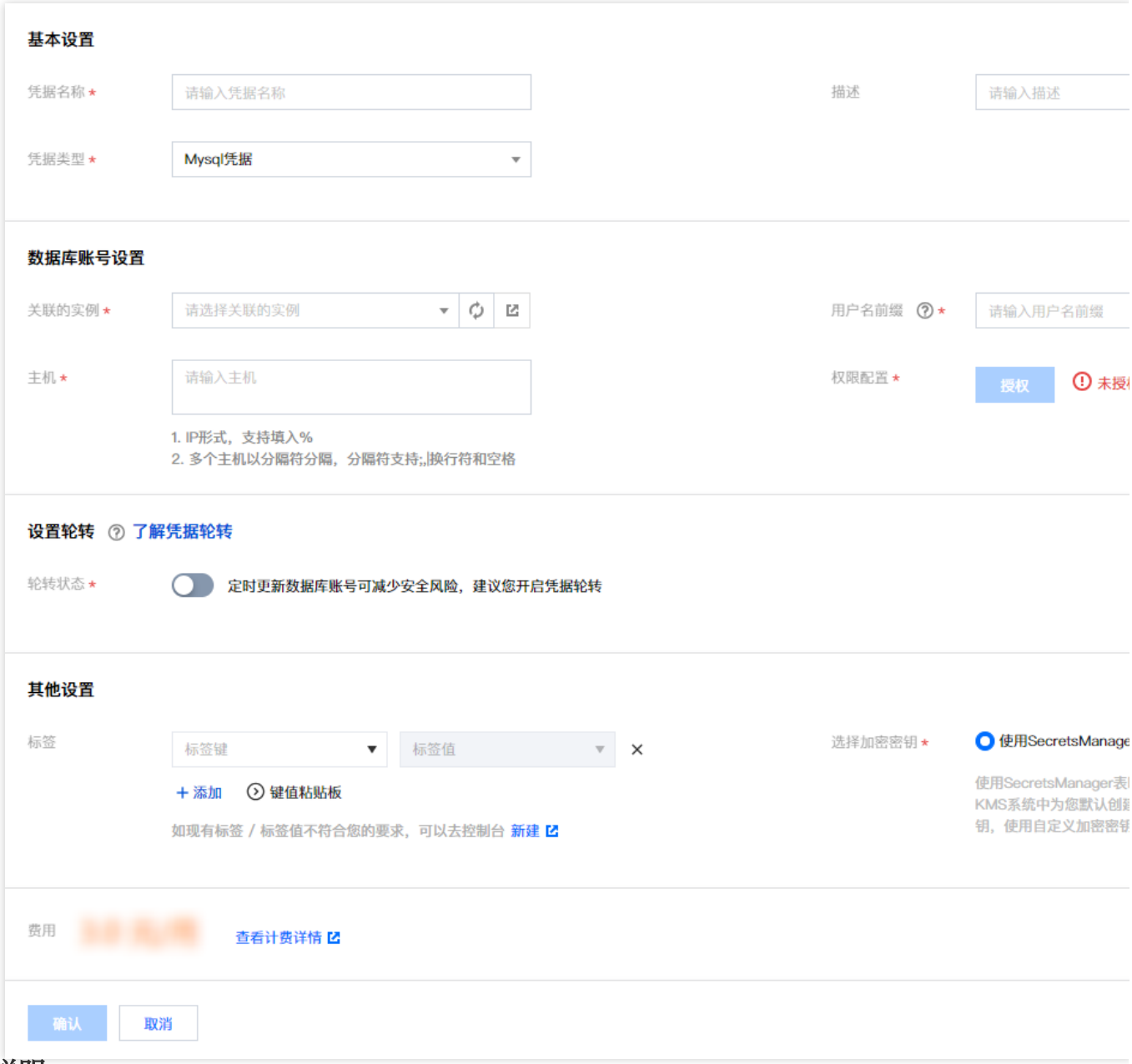
为了能让您更好的使用数据库凭据功能，请提前做好以下准备：
确认已开通KMS服务，SSM 基于密钥管理系统 KMS 托管的密钥进行加密。
确保您已经创建**云数据库 MySQL** 或 **TDSQL MySQL 版**实例。对于具体操作，请查阅 创建 MySQL 实例、创建 TDSQL 实例。

操作步骤

1. 登录 凭据管理系统 控制台，在左侧导航栏中，单击**数据库凭据**，进入凭据列表页面。

2. 在凭据列表页面，单击左上角的“区域下拉框”，切换区域。

3. 在凭据列表页面，单击左上角的**新建**，进入新建凭据页面。
4. 在新建凭据页面，输入相对应的信息后，单击**确定**，返回凭据列表，新创建的凭据会出现在凭据列表首位。



字段说明

基础设置

凭据名称：名称长度1 - 128字节，使用字母、数字、连接符（-）、下划线（_）的组合，**首字符必须为字母或者数字**。

描述：凭据描述信息，用于详细描述用途等，最大支持2048字节。（非必填）

数据库账号设置

关联的实例： 选择您在 mysql、tdsql 中所创建的实例。

用户名前缀： 用户名前缀长度1~8字节，使用字母、数字或者 _ 的组合，首字符须为大写或小写字母开头。

说明：

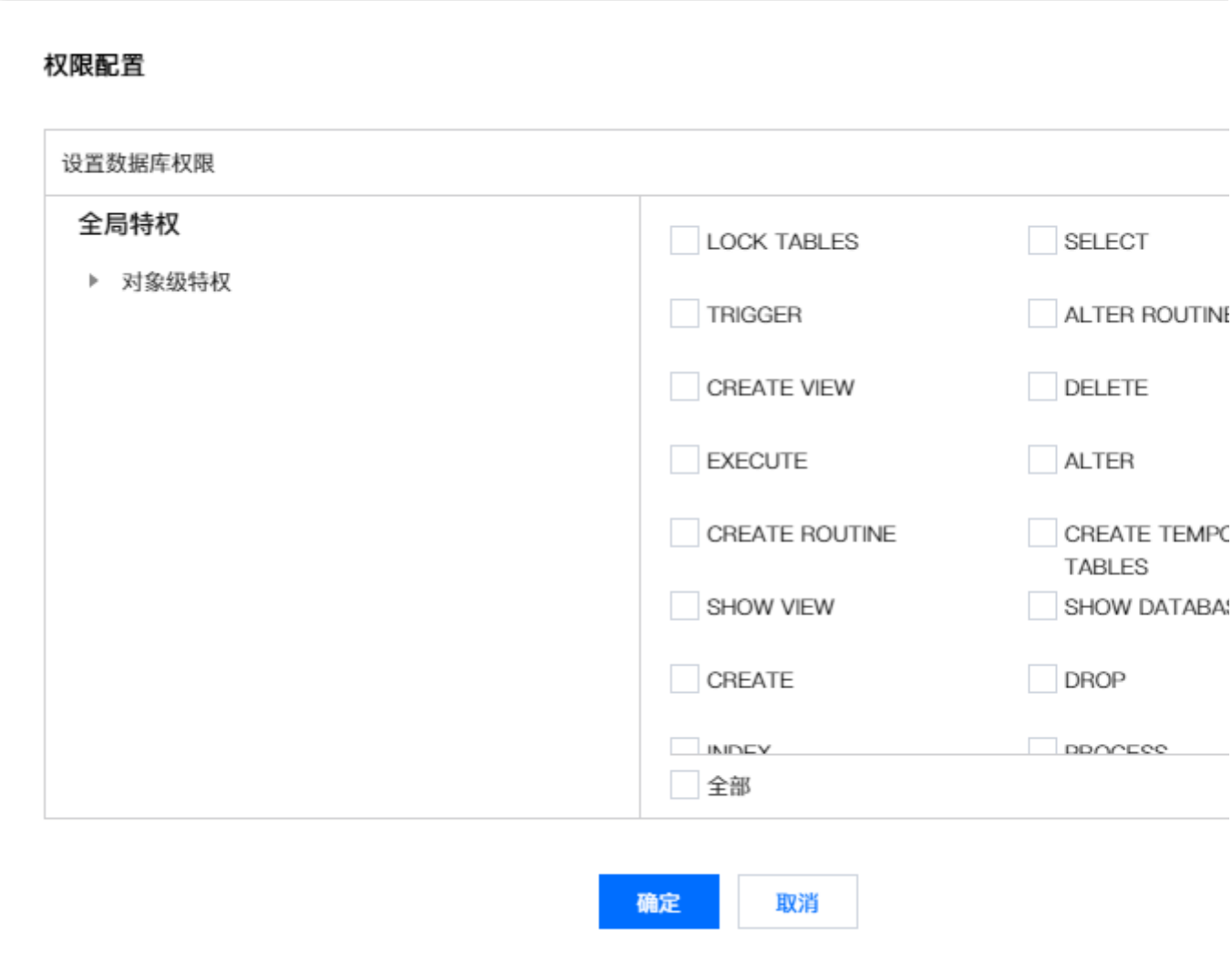
生成的用户名为用户名前缀+后缀，每次轮转使两个不同的用户名相互替换。

主机：

IP 形式，支持填入%。

多个主机以分隔符分隔，分隔符支持换行符和空格 。

授权：设置数据库的相关权限。



设置轮转

轮转状态： 开启轮转后，SSM 将定期更新数据库账号的密码；**建议开启，提高安全性**。

轮转周期：设定周期区间为30~365天。

下次轮转开始时间：根据需求来设定下一次开启轮转的时间。单位为**秒**。

其他设置

标签：非必填。

选择加密密钥：

使用凭据管理系统在密钥管理系统（KMS）中默认创建的主密钥（CMK）进行加密。

使用自定义加密密钥。

注意：

若使用凭据管理系统表明您已开启 密钥管理系统，您可以通过以下两种方案创建加密密钥：

选择在 密钥管理系统 中默认创建的云产品主密钥作为加密密钥，并通过信封加密方案进行加密存储。

选择在 密钥管理系统 中创建一个用户密钥，将该密钥作为自定义的加密密钥对凭据进行加密存储。

版权所有：腾讯云计算（北京）有限责任公司

编辑数据库凭据

最近更新时间：2024-08-01 19:03:55

操作场景

登录腾讯云凭据管理系统控制台查看并编辑凭据信息列表、名称、状态及所属地区等凭据详情。

前提条件

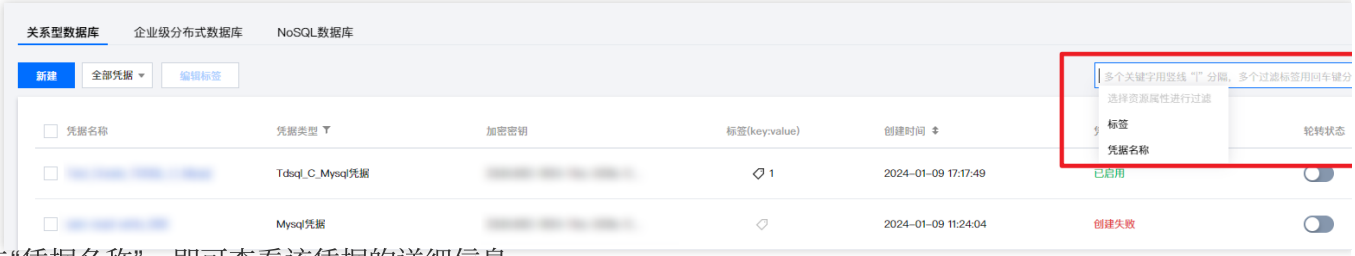
已获取 凭据管理系统 控制台的登录账户与密码 。
已创建数据库凭据；对于未创建数据库凭据的情况，可查阅 创建数据库凭据 进行创建 。

操作步骤

1. 登录 凭据管理系统 控制台，在左侧导航栏中，单击**数据库凭据**，进入凭据列表页面。

2. 在凭据列表页面，单击左上角的“区域下拉框”，切换区域。

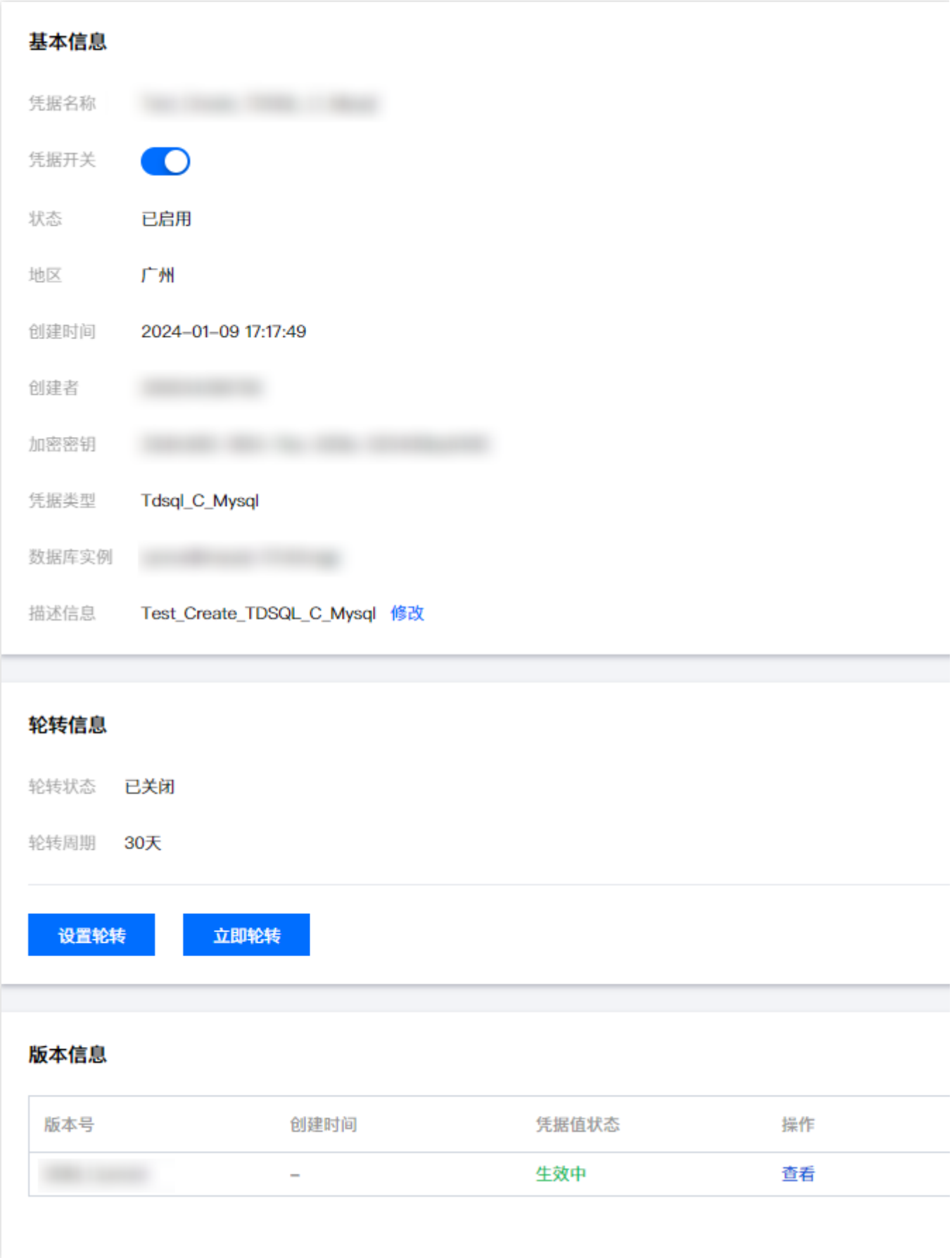
3. 在页面右侧搜索框中，单击搜索框，可通过“标签和凭据名称”等关键字对凭据进行查找。



4. 单击“凭据名称”，即可查看该凭据的详细信息。

说明：

在凭据列表中，单击 **轮转状态** 可开启或禁用轮转，其中对于凭据轮转的设置详情，可查看 修改轮转信息。



5. 在凭据详情页面中，可以修改凭据描述、凭据开关、设置轮转以及更换版本信息。

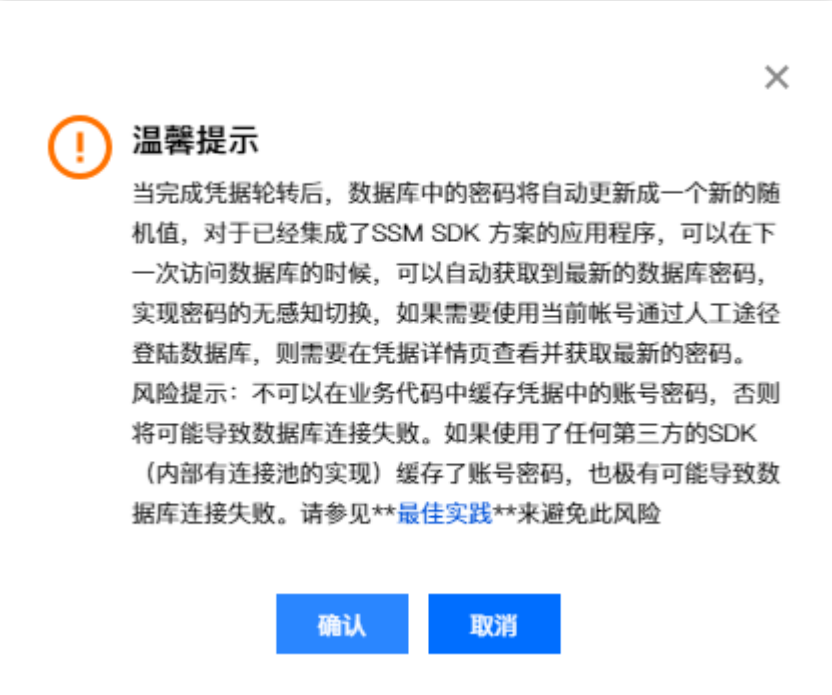
修改基本信息

修改凭据状态：开启“凭据开关”按钮即可切换，置灰代表为禁用状态。
修改描述信息：描述信息用于详细描述用途等，最大支持2048字节。（非必填）

修改轮转信息

在该信息栏中，可查看轮转状态、周期、上次轮转结束时间、下次轮转开始时间（只有当轮转为启用状态时，才有该项信息说明）。
设置轮转：单击设置轮转按钮后，会弹窗供您填写轮转的信息，其中包括轮转的周期（时间范围：30~365天），下次轮转开始时间（时间范围：当前时间+24小时 ~ 当前时间+365天）。

立即轮转：单击**立即轮转**后，会弹窗告知相关凭据轮转后的注意事项，单击**确认**即可完成轮转操作。
说明：
凭据开启轮转的前提：凭据状态必须是在启用的状态下，才能开启凭据的轮转。



版本信息

在该信息栏中将会展示凭据的版本号，单击**查看**可查看账号名和账号密码。

注意：

密码的明文是应用程序通过 SSM 的 API 自动获取和更新，出于安全考虑，一般情况下，不建议您在控制台查看托管凭据的值。

启用禁用数据库凭据

最近更新时间：2024-08-01 19:03:55

前提条件

已获取 凭据管理系统 控制台的登录账户与密码 。
已创建数据库凭据；对于未创建数据库凭据的情况，可查阅 创建数据库凭据 进行创建 。

操作步骤

1. 登录 凭据管理系统 控制台，在左侧导航栏中，单击**数据库凭据**，进入凭据列表页面。

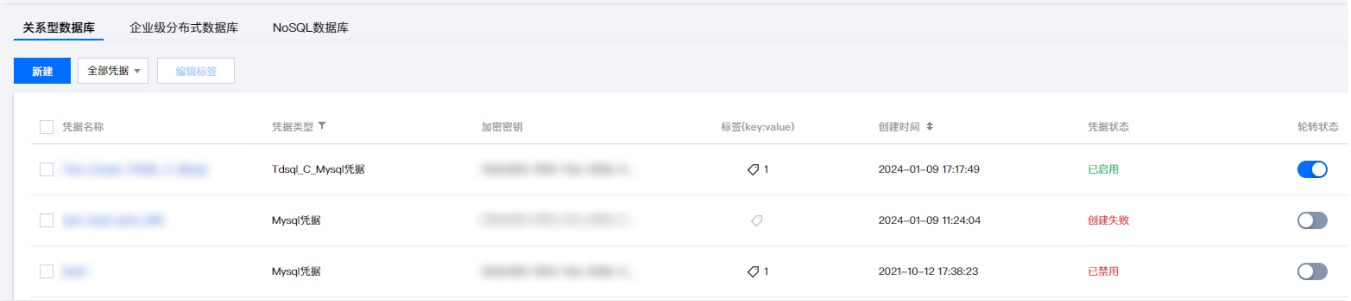
2. 在凭据列表页面，单击左上角的“区域下拉框”，切换区域。

3. 在页面右侧搜索框中，单击搜索框，可通过“标签和凭据名称”等关键字对凭据进行查找。

4. 在所需凭据所在行，单击**启用**或**禁用**，即可实现凭据的启用、禁用功能。

说明：

单击凭据名称，在凭据对应的详情页面中，也可以实现凭据状态的切换，详情请单击 编辑数据库凭据。



删除数据库凭据

最近更新时间：2024-08-01 19:03:55

注意事项

为避免误删除操作，凭据管理系统使用计划删除机制，即**对删除操作强制执行0 - 30天等待期**，并确认删除后等待0 - 30天再进行删除。
凭据删除后将**无法恢复**，此凭据下的所有凭据内容也将**无法调用**。

操作步骤

1. 登录 凭据管理系统 控制台，在左侧导航栏中，单击**数据库凭据**，进入凭据列表页面。

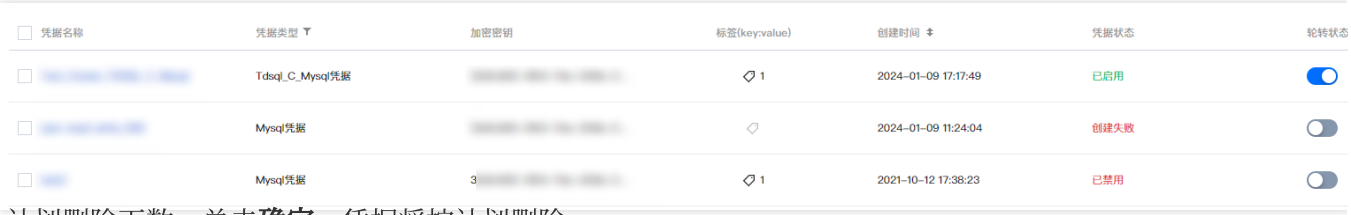
2. 在凭据列表页面，单击左上角的“区域下拉框”，切换区域。

3. 在页面右侧搜索框中，输入凭据全称或部分名称，查找您需要的凭据。

4. 选择需要计划删除的凭据，在计划删除操作栏中单击**计划删除**。

说明：

若凭据是启用状态，请先单击**禁用**，对凭据进行禁用操作。



5. 输入计划删除天数，单击**确定**，凭据将按计划删除。

注意：

若选择等待期为“0”天，凭据将立即删除。

6. 在1~30天等待期内，您可以对计划删除的凭据进行取消删除操作。若需取消删除凭据，单击**取消删除**，即可取消删除凭据。

凭据名称	凭据类型	加密密钥	标签(key:value)	创建时间	凭据状态	轮转状态
[illegible]	Tdsql_C_Mysql凭据	[illegible]	1	2024-01-09 17:17:49	已启用	
[illegible]	Mysql凭据	[illegible]	1	2021-10-12 17:38:23	计划删除	
[illegible]	Mysql凭据	[illegible]	1	2021-10-12 17:12:53	已启用	

共 3 条

7. 确认取消删除后，凭据密钥重置为“启用”状态，可对该凭据进行禁用、修改、删除等操作。

标签
编辑标签

最近更新时间：2024-08-01 19:03:55

操作场景

本文档指导您对资源进行编辑标签的操作。

使用限制

标签内容（标签键、标签值）的使用有相对应的限制条件，详情请查阅 **标签使用限制**。

前提条件

1. 已登录 **凭据管理系统** 控制台。
2. 选择需要编辑凭据的所在区域。

操作步骤

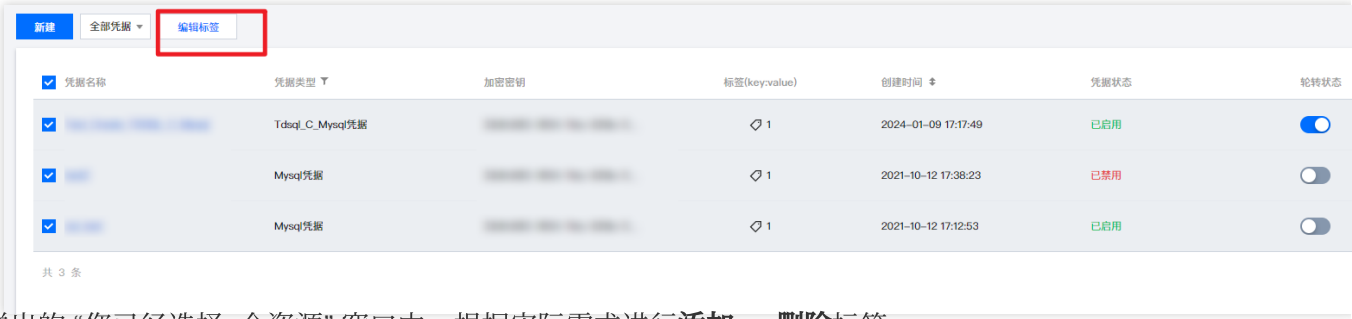
单个凭据编辑标签

1. 找到需编辑标签的凭据，选择其右侧的**编辑标签**。

2. 在弹出的 “您已经选择1个资源” 窗口中，根据实际需求进行**添加** 、**删除**标签。

批量编辑标签

1. 勾选需编辑标签的凭据，点击凭据顶部的**编辑标签**。



2. 在弹出的 “您已经选择n个资源” 窗口中，根据实际需求进行**添加** 、 **删除**标签。

说明：

关于如何使用标签，请参见 使用标签管理示例。

版权所有：腾讯云计算（北京）有限责任公司

使用标签管理示例

最近更新时间：2024-08-01 19:03:55

操作场景

标签是用于从不同的维度对资源分类的管理、权限的管理。

在 凭据管理系统 中，标签主要用于**用户凭据**。

在凭据中添加标签，是为了方便用户对凭据进行分类和跟踪管理，同时可以按照标签来汇总对应凭据的使用情况。

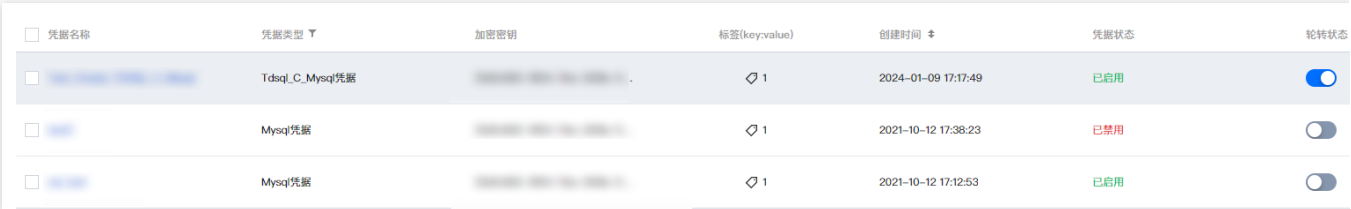
使用限制

标签内容（标签键、标签值）的使用有相对应的限制条件，详情请查阅 标签使用限制。

操作方法

在密钥管理控制台设置标签

1. 已登录 凭据管理系统 控制台。
2. 选择需要编辑凭据的所在区域。
3. 找到需编辑标签的凭据，选择其右侧的**编辑标签**。



4. 在弹出的 “您已经选择1个资源” 窗口中设置，设置标签，如下图所示：

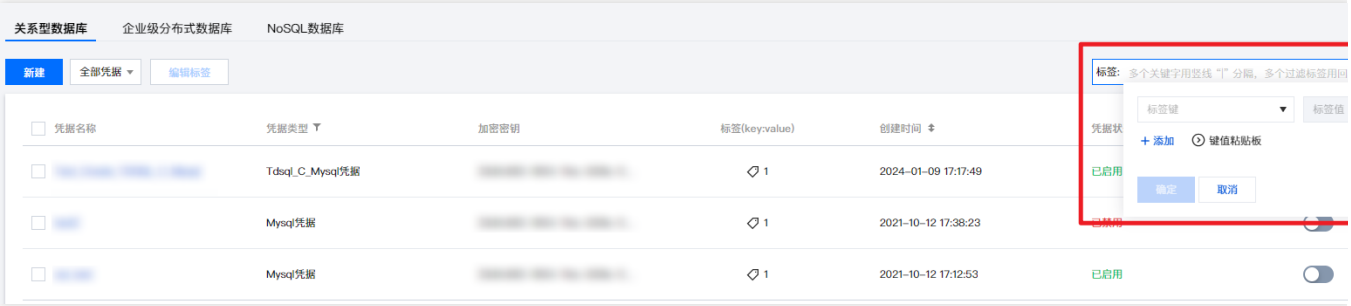
例如，添加两组标签。

5. 单击**确定**，系统出现修改成功提示。

通过标签筛选密钥

1. 已登录 凭据管理系统 控制台。
2. 选择需要编辑凭据的所在区域。
3. 在选择的区域凭据列表中，在右侧的搜索框选择以 “**标签**” 作为筛选条件，输入筛选内容即可，如下图所示。

例如：您希望筛选出 ower 为 alex 的密钥，可输入标签：owner:alex。



日志审计

最近更新时间：2024-01-02 15:13:40

操作场景

凭据管理系统与腾讯 云审计 CloudAudit 结合，对您的腾讯云账号进行监管、合规性检查、操作审核及风险审核服务，可记录所有凭据管理操作和凭据使用情况。

操作步骤

1. 您可以登录 云审计控制台 ，在左侧导航栏中，单击**操作记录**，最多可查看最近30天用户在腾讯云账号下的操作记录。
2. 单击目标事件前方的展开按钮，可查看事件详情。

可查看内容包括：

操作记录列表：您可以查看操作记录列表，以及对应操作事件时间、用户名、事件名称、资源类型、资源名称等。

操作记录详情：您可以获取单个操作记录详情，包括访问密钥、区域、错误码、事件 ID、事件名称、事件源、事件时间、请求 ID、源 IP 地址、用户名。

访问控制

概述

最近更新时间：2024-01-02 15:13:40

如果您不需要对子账户进行凭据管理系统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其他文档的理解和使用。
如果同时使用凭据管理系统、私有网络（VPC）、云服务器（CVM）、数据库等服务，且这些服务由不同人进行管理，但都共享同一个云账号密钥，将存在密钥由多人共享，泄密风险高等问题，且无法限制其它人访问权限，易产生误操作造成安全风险问题。
访问控制（CAM）用于管理腾讯云账号下资源访问权限，您可以通过 CAM 的身份管理和策略管理控制各子账号的资源操作权限。例如，您的主账号下有一个凭据，您只想让子账号 A 使用该凭据，而子账号 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。

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、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，登录凭证指用户登录名和密码，访问证书指云 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，如一个凭据管理系统的凭据，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，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或用户组完成授权。
如需了解更多请参见 腾讯云访问管理 CAM。

子账号管理

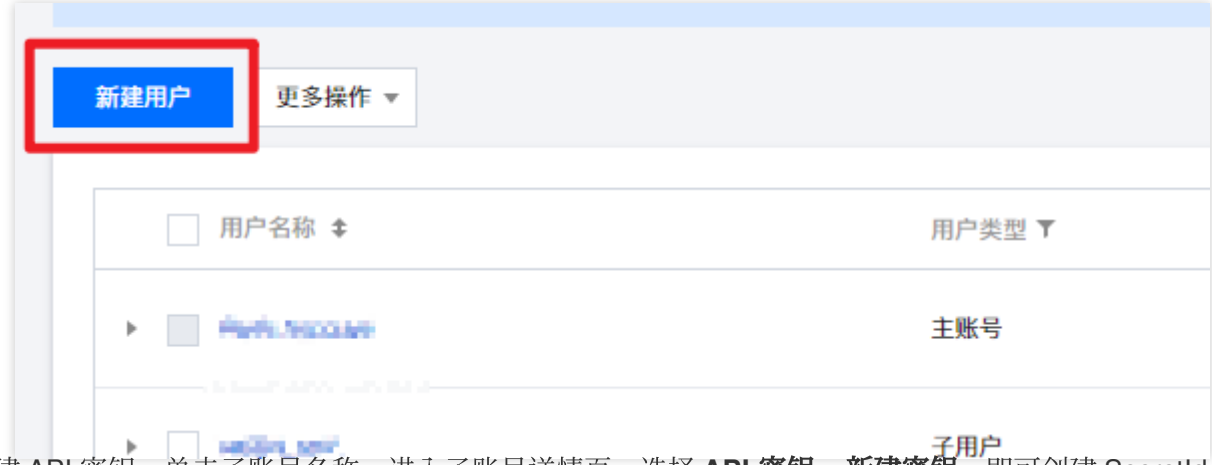
最近更新时间：2024-08-01 19:03:55

概述

本文详细介绍如何创建子账号，并授予子账号管理凭据管理系统的权限。

操作步骤

1. 创建子账号。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**，在**用户列表**页面下，单击**新建用户**，即可创建子账号。

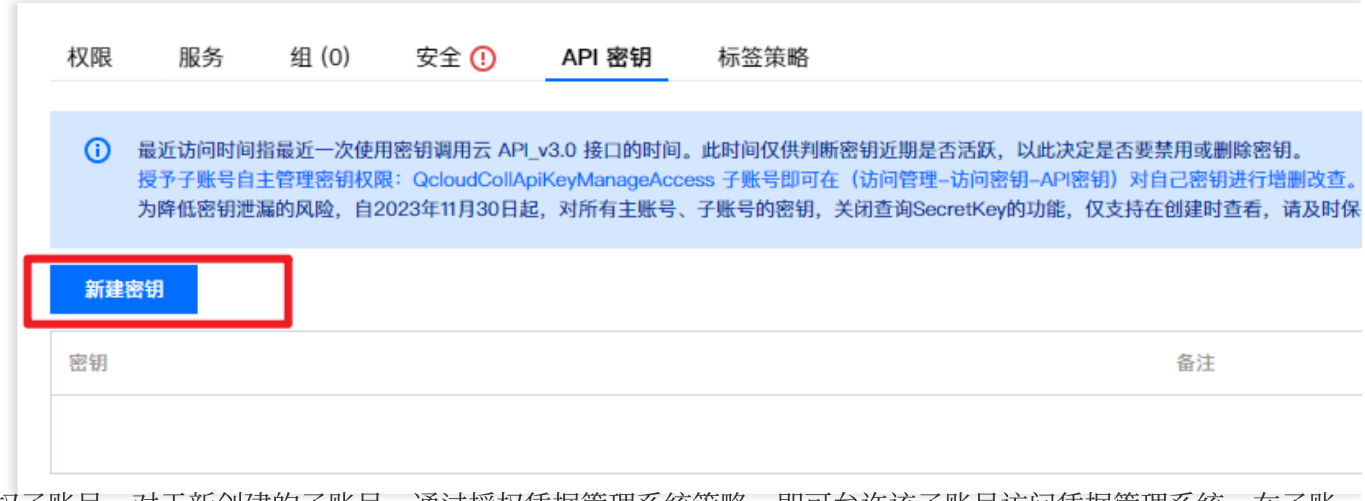


2. 创建 API 密钥。单击子账号名称，进入子账号详情页，选择 **API 密钥** > **新建密钥**，即可创建 SecretId 和 SecretKey，您通过该 API 密钥访问凭据管理系统。

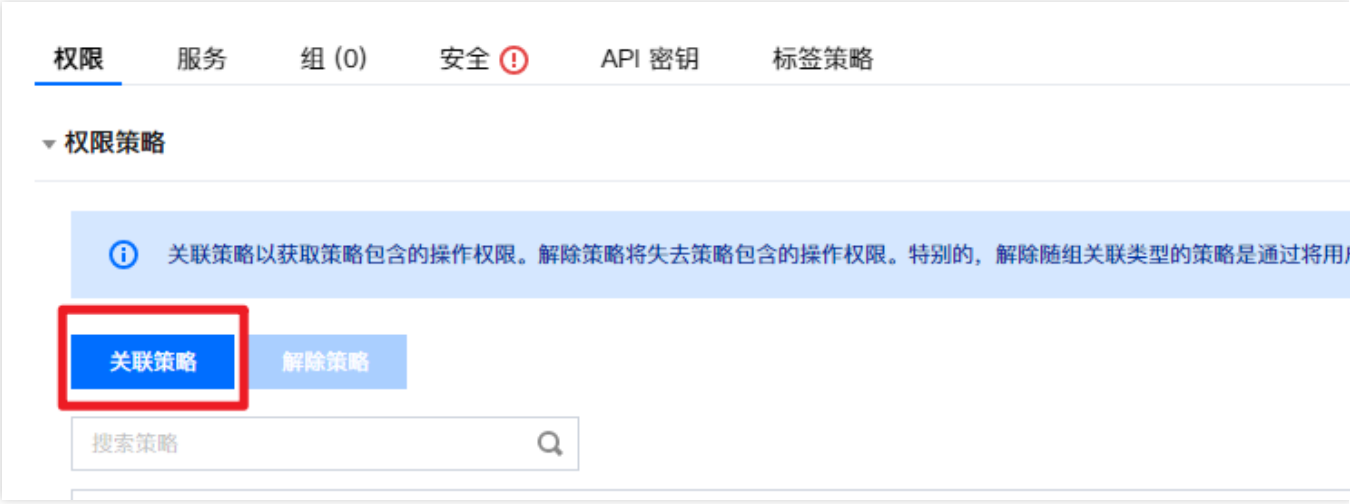
说明：

如果您不需要通过 API 管理凭据管理系统，可直接操作授权子账号。

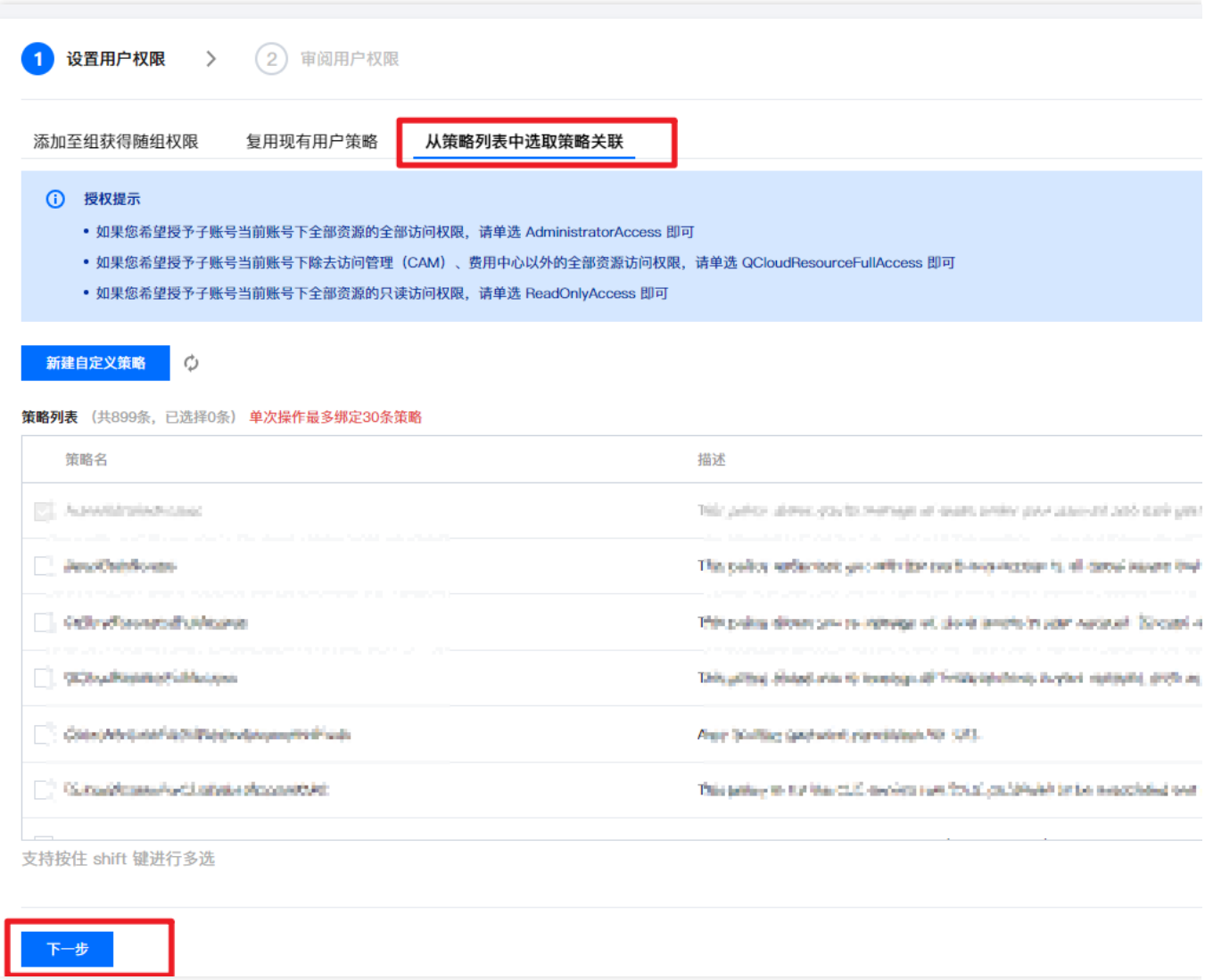
版权所有：腾讯云计算（北京）有限责任公司



3. 授权子账号。对于新创建的子账号，通过授权凭据管理系统策略，即可允许该子账号访问凭据管理系统。在子账号详情页，选择**权限** > **关联策略**，进入添加策略页面。



4. 添加策略。在添加策略页面，单击**从策略列表中选取策略关联**，选择合适的凭据管理系统策略，选择**下一步** > **确定**，即可授权子账号访问凭据管理系统权限。

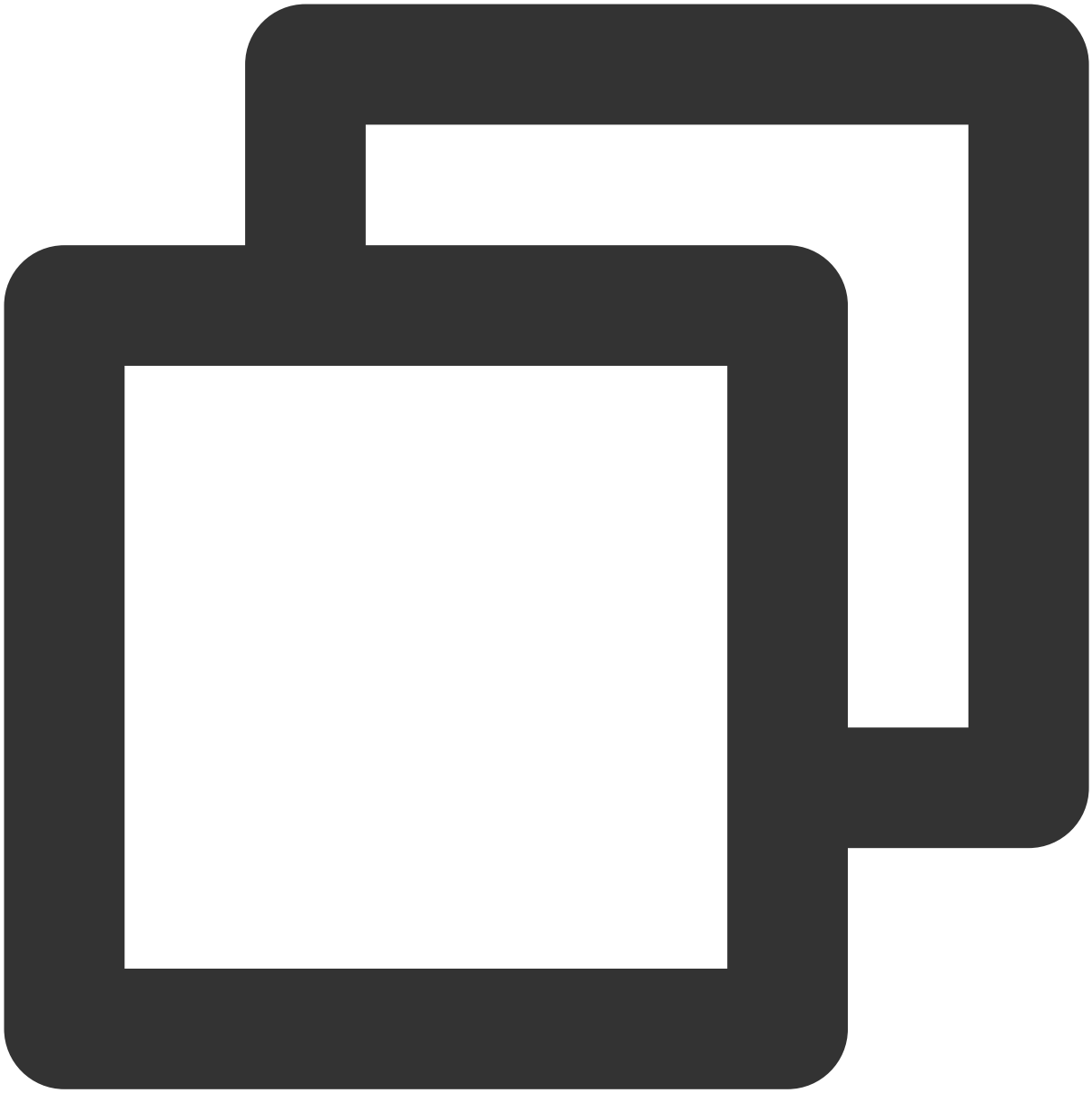

1 设置用户权限
2 审阅用户权限
添加至组获得随组权限
复用现有用户策略
从策略列表中选取策略关联
授权提示
• 如果您希望授予子账号当前账号下全部资源的全部访问权限，请单选 AdministratorAccess 即可
• 如果您希望授予子账号当前账号下除去访问管理（CAM）、费用中心以外的全部资源访问权限，请单选 QCloudResourceFullAccess 即可
• 如果您希望授予子账号当前账号下全部资源的只读访问权限，请单选 ReadOnlyAccess 即可
新建自定义策略
策略列表 （共899条，已选择0条） 单次操作最多绑定30条策略
策略名
描述
支持按住 shift 键进行多选
下一步

创建访问控制策略

最近更新时间：2024-01-02 15:13:40

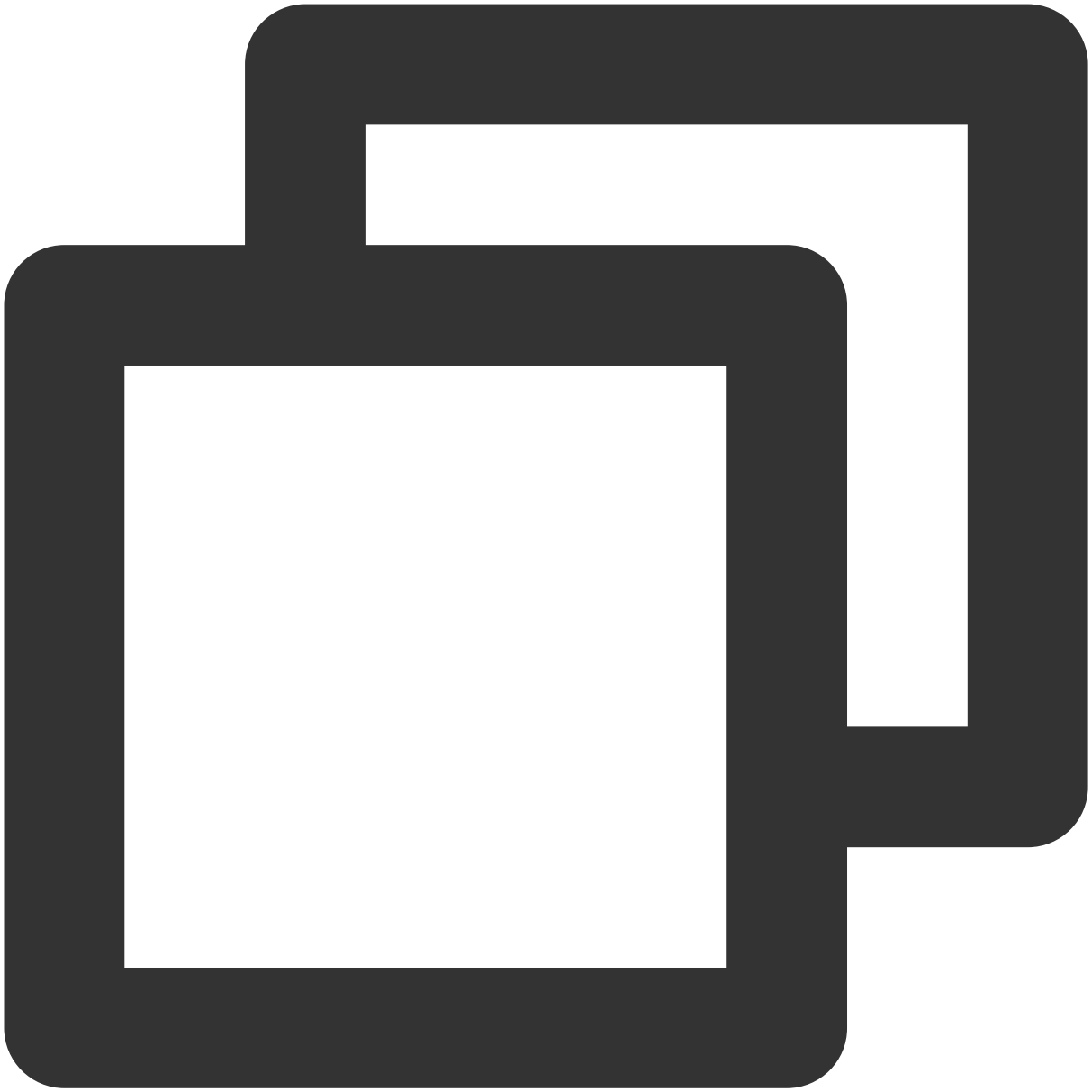
可授权的资源类型

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。凭据管理系统部分接口支持使用资源级权限对凭据进行操作，可控制允许用户何时执行操作或是否允许用户使用的特定资源。
例如，您授权用户拥有广州地域凭据的权限，在 CAM 中可授权的资源类型为：



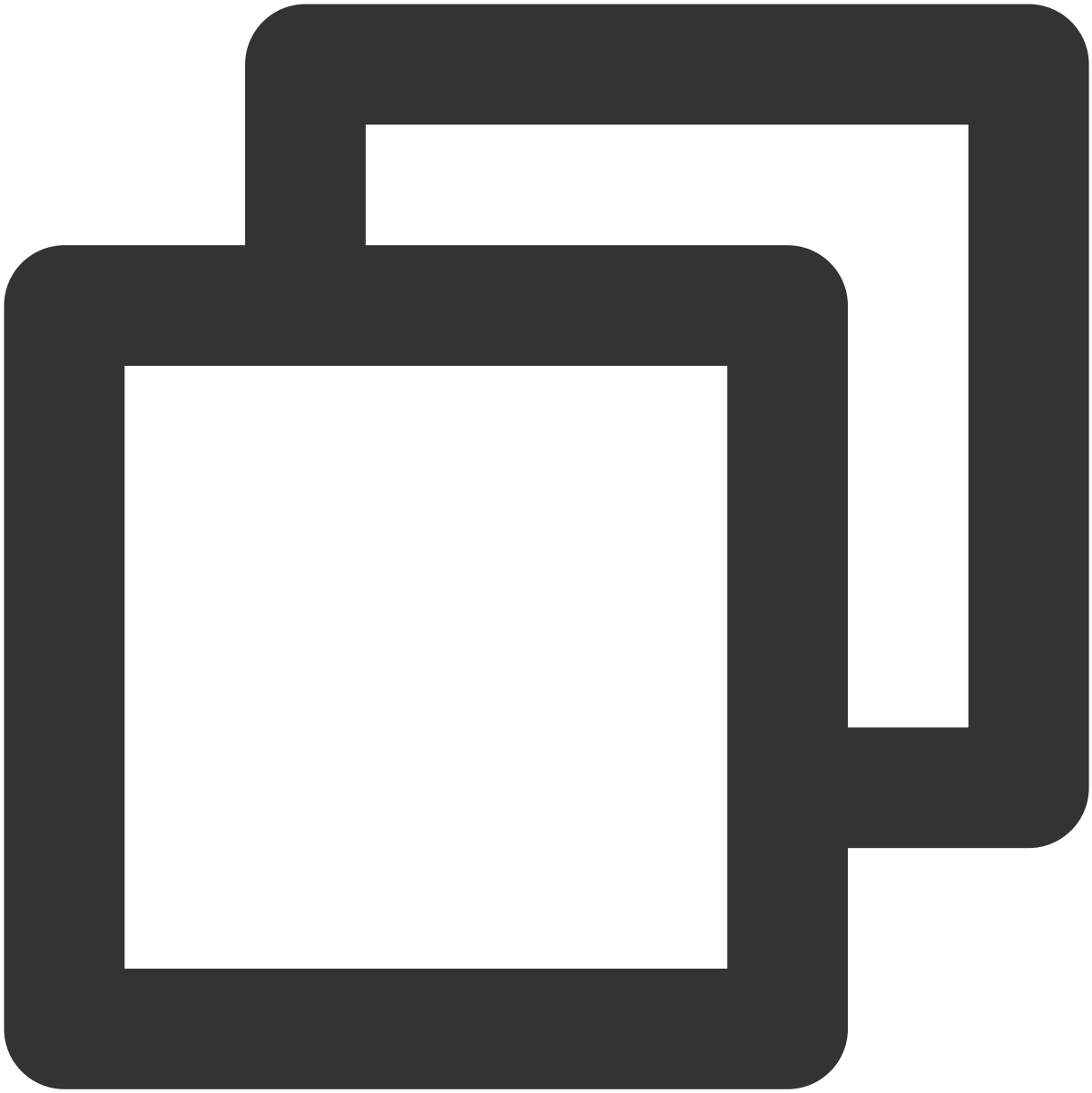
```
qcs::ssm:ap-guangzhou:uin/${uin}:*
qcs::ssm:ap-guangzhou::*
```

您授权接口访问某个 UIN 创建的所有凭据，则资源类型为：



```
qcs::ssm:$region:uin/$uin:secret/creatorUin/*
```

您授权接口访问某个具体的凭据，则资源类型为：



```
qcs::ssm:$region:uin/$uin:secret/creatorUin/$creatorUin/$secretName
```

其中：

`$region` ：指代地域。

`$uin` ：指代主账号 ID。

`$creatorUin` ：指代创建该资源的账号 ID。

`$secretName` ：指代需要配置的凭据名称。

资源级授权接口

如下 API 接口 DeleteSecretVersion、UpdateDescription、RestoreSecret、EnableSecret、PutSecretValue、DescribeSecret、UpdateSecret、DeleteSecret、GetSecretValue、DisableSecret、ListSecretVersionIds 资源路径为：

```
qcs::ssm:$region:uin/$uin:secret/*
qcs::ssm:$region:uin/$uin:secret/creatorUin/*
qcs::ssm:$region:uin/$uin:secret/creatorUin/$creatorUin/$secretName
```

接口级别授权列表

API 接口	描述信息
CreateSecret	创建新的凭据。
GetRegions	获取可用 region 列表，用于控制台展示。
GetServiceStatus	获取服务状态，用于判定服务是否开通。
ListSecrets	获取所有凭据列表信息。

版权所有：腾讯云计算（北京）有限责任公司