数据安全网关（云访问安全代理）

操作指南

腾讯云

版权所有：腾讯云计算（北京）有限责任公司

【版权声明】

©2013-2025 腾讯云版权所有

本文档（含所有文字、数据、图片等内容）完整的著作权归腾讯云计算（北京）有限责任公司单独所有，未经腾讯云事先明确书面许可，任何主体不得以任何形式复制、修改、使用、抄袭、传播本文档全部或部分内容。前述行为构成对腾讯云著作权的侵犯，腾讯云将依法采取措施追究法律责任。

【商标声明】

腾讯云

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。未经腾讯云及有关权利人书面许可，任何主体不得以任何方式对前述商标进行使用、复制、修改、传播、抄录等行为，否则将构成对腾讯云及有关权利人商标权的侵犯，腾讯云将依法采取措施追究法律责任。

【服务声明】

本文档意在向您介绍腾讯云全部或部分产品、服务的当时的相关概况，部分产品、服务的内容可能不时有所调整。
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。

【联系我们】

我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 4009100100或95716。

文档目录

- 操作指南
  - 授权管理
    - 账号授权管理
    - 角色授权管理
    - KMS 密钥管理和授权
  - 实例管理
    - 基本信息管理
    - 分类分级资源管理
    - 标签管理
    - 安全组管理
    - 代理资源管理
    - 代理账号管理
    - 计算节点管理
  - 元数据
    - 元数据管理
      - 新增元数据
        - 添加云元数据
        - 添加自建元数据
      - 基本信息管理
      - 元数据账号管理
      - 元数据表结构管理
      - 主从同步管理
      - SSL 连接管理
    - 接入与备份
      - 概述
      - 新建接入与备份任务
      - 管理任务元数据
      - 管理加解密任务
  - 数据加密
    - 概述
    - 策略管理
      - 创建策略
      - 分表配置与管理
      - 导入策略
      - 删除策略
    - 仿真记录
    - 任务管理
    - 密钥管理
  - 数据脱敏
    - 概述
    - 动态脱敏策略管理
      - 新建脱敏策略
      - 查看脱敏策略详情
      - 删除脱敏策略
      - 规则管理
    - 静态脱敏任务
      - 数据库脱敏任务
      - 文件脱敏任务
    - 脱敏模板配置

版权所有：腾讯云计算（北京）有限责任公司

脱敏算法管理
脱敏算法
变换脱敏
哈希脱敏
加密算法
替换脱敏
遮盖脱敏
访问控制
访问规则管理
创建访问规则
编辑访问规则
删除访问规则
角色管理
创建角色
添加代理账号
规则管理
删除角色
阻断日志
运维监控
监控日志
配置事件规则

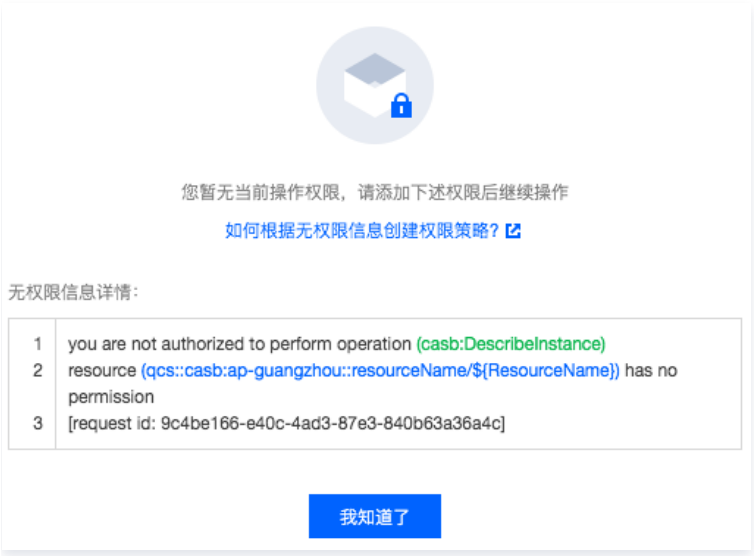
操作指南
授权管理
账号授权管理

最近更新时间：2024-11-08 21:33:12

本文档将介绍如何通过故障反馈关联策略以解除权限问题，解除权限问题后，子账号将在新设置的权限范围内管理主账号下的资源。

现象描述

当子账号访问数据安全网关（CASB）控制台时，产生如下提示：



解决思路

- 如您愿意授权子账号继续进行操作，您可以参见 操作步骤 为其关联以下任意预设策略：
- QcloudCASBFullAccess 数据安全网关（CASB）全读写访问权限。
- QcloudCASBReadOnlyAccess 数据安全网关（CASB）只读访问权限。
- 在使用数据安全网关（CASB）元数据功能时，会调用 VPC、云产品（MySQL/TDSQL/MariaDB）、CVM 及 LB 的资源，故子账号在使用时，需同步关联如下预设策略：
  - QcloudTAGReadOnlyAccess 标签（TAG）只读访问权限。
  - cloudVPCReadOnlyAccess 私有网络（VPC）只读访问权限。
  - QcloudCVMInnerReadOnlyAccess 云服务器（CVM）只读访问权限。
  - QcloudCLBReadOnlyAccess 负载均衡（CLB）只读访问权限。
  - QcloudKMSReadOnlyAccess 密钥管理系统（KMS）只读访问权限。
- 对于云产品类的权限，根据子账号所关联的云产品库类型进行关联策略：
- QcloudMariaDBReadOnlyAccess 云数据库 MariaDB 只读访问权限。
- QcloudTDSQLReadOnlyAccess TDSQL MySQL 版（TDSQL for MySQL）只读访问权限。

前提条件

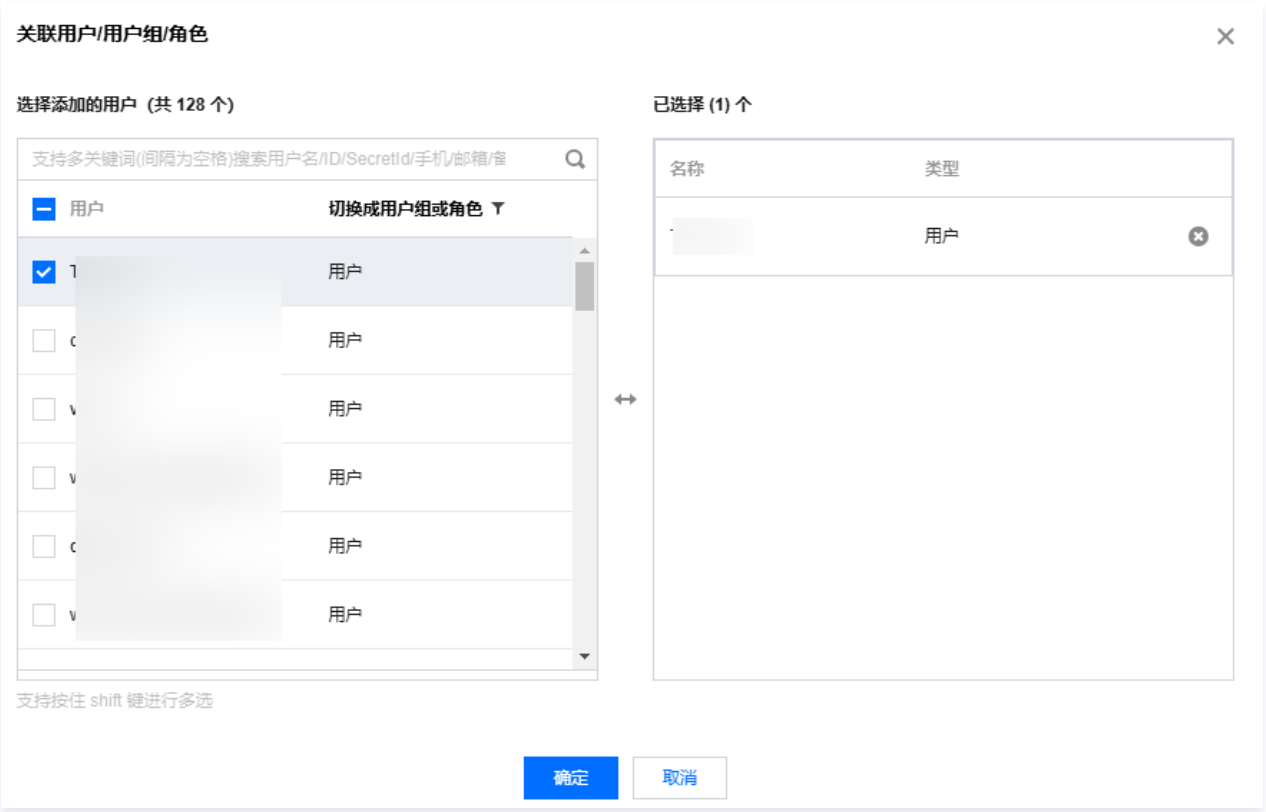
相关服务角色授权需要使用“主账号”或“拥有访问管理读写权限的账号”完成。

> **说明**
> 主账号需拥有访问管理读写权限，同时可以在 访问管理 中给相应子账号分配访问管理读写权限。

操作步骤

以添加 QcloudCASBFullAccess 权限为例进行说明：

1. 登录 访问管理控制台，在左侧导航中，单击**策略**。
2. 在策略页面的搜索框中，输入策略名称，如“QcloudCASBFullAccess”进行搜索。
3. 在“QcloudCASBFullAccess”策略的右侧操作栏中，单击**关联用户/组/角色**。
4. 在关联用户/用户组/角色页面，选中需要配置权限的子用户，单击**确定**即可。



注意事项

在使用 CASB 产品中，对于子账号的权限需要进行严格限制时，需保证子账号具有如下权限：

```
cam:GetRole
cam:ListAttachedRolePolicies
kms:GetServiceStatus
cvm:DescribeInstances
clb:DescribeLoadBalancers
cdb:DescribeDBInstances
cdb:DescribeRoGroups
mariadb:DescribeDBInstances
mariadb:DescribeDcnDetail
dcdb:DescribeDCDBInstances
dcdb:DescribeDcnDetail
postgres:DescribeDBInstances
cynosdb:DescribeInstances
cynosdb:DescribeInstanceDetail
cynosdb:DescribeClusterInstanceGrps
cynosdb:DescribeClusters
postgres:DescribeReadOnlyGroups
cos:GetService
```

相关文档

- 角色授权

- KMS开通指南

角色授权管理

最近更新时间：2024-06-13 19:14:31

本文介绍如何使用 CASB 服务需要授权的 CASB_QCSRole 角色的功能，当前角色包含如下功能：

角色预设策略

预设策略	策略名称	权限说明
QcloudAccessForCASBRoleInDatabaseAssets	云资源预设策略	该策略仅供数据安全网关（云访问安全代理，CASB）服务角色（CASB_QCSRole）进行关联，用于 CASB 访问其他云服务资源。
QcloudKMSAccessForCASBRole	KMS 预设策略	该策略供数据数据安全网关（云访问安全代理，CASB）服务角色(CASB_QCSRole)进行关联，用于 CASB 访问其他云服务资源。包含密钥管理系统(KMS)相关操作权限。

操作步骤

1. 登录 控制台，根据提示单击**前往授权**。
2. 在角色管理页面，显示需要授权的策略，单击**同意授权**。
3. 返回 CASB 页面，则可以看到授权提示，单击**已完成授权**即可。

相关文档

- 账号授权
- KMS 开通指南

KMS 密钥管理和授权

最近更新时间：2024-11-07 11:37:52

本文档将指导您如何开通密钥管理系统（KMS）服务。

背景信息

数据安全网关（CASB）可选择基于 密钥管理系统（KMS） 进行密钥加密存储，如果用户选择 KMS 进行密钥管理则需要在创建密钥前，完成 KMS 服务开通和 KMS 对 CASB 服务的角色授权操作。

CASB 密钥管理

数据安全网关（CASB）的密钥由 KMS 托管，采用三级密钥管理机制，根密钥由硬件加密机生成和存储，由根密钥生成 用户主密钥（CMK），最终基于用户主密钥生成数据加密密钥 DEK，对应用数据进行加解密。

KMS 管理密钥管理

在服务架构方层面，KMS 服务通过单地域多机房提供可靠性，其底层使用的 HSM 设备也采用多机房集群化部署，并提供双机房冷备份设备，确保服务的高可用性。保护密钥的保密性、完整性和可用性，满足用户多应用多业务的密钥管理需求。

操作步骤

1. 登录 控制台，在控制台上方指引中，单击 **密钥管理系统 KMS**，前往 KMS 购买页。

2. 在密钥管理系统开通页面，单击**立即开通**，成功开通密钥管理系统服务。

相关文档

- 角色授权
- 账号授权

实例管理
基本信息管理

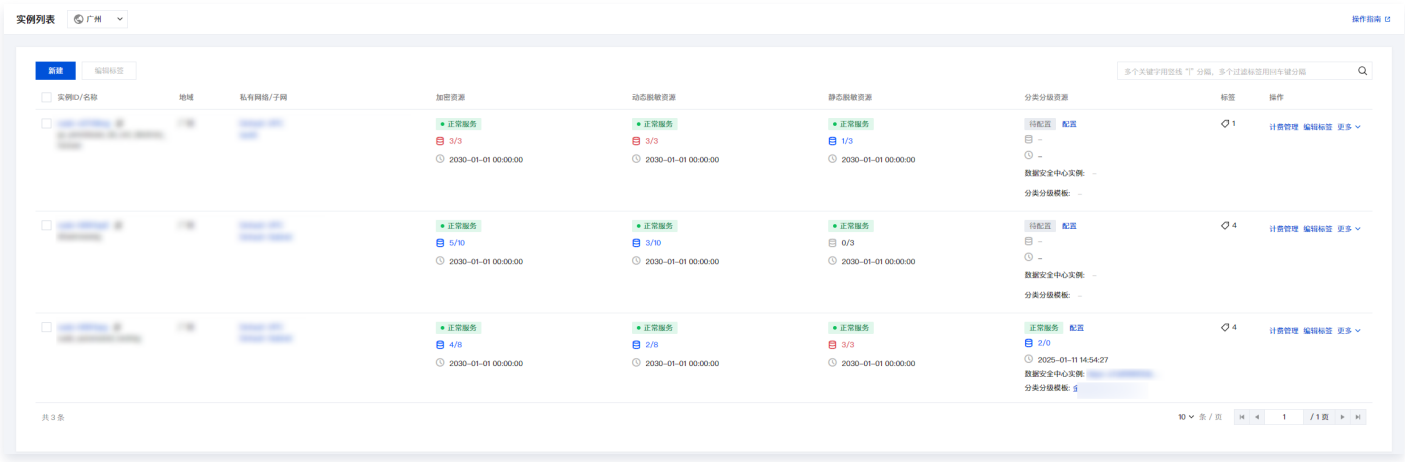
最近更新时间：2024-12-31 17:50:22

前提条件

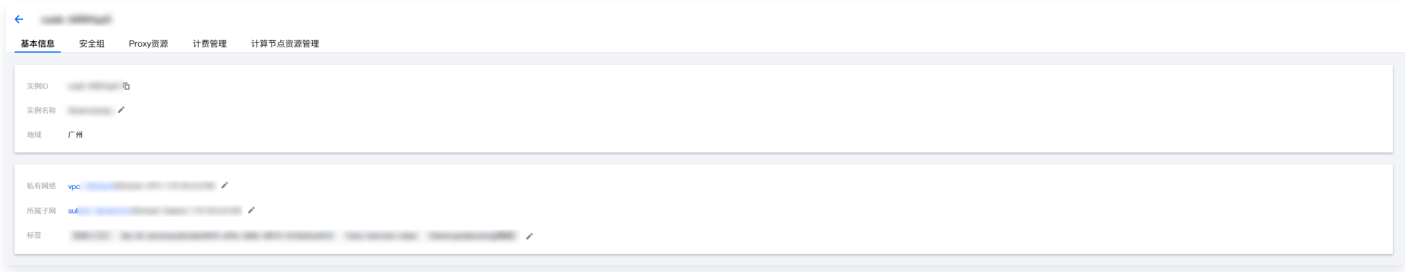
需已 购买开通 CASB 实例 。

操作步骤

1. 登录 控制台，在左侧导航栏中，单击**实例 > 实例列表**。
2. 在实例列表页面，选择已购买实例的地域，查看已购买的 实例列表 。单击需要操作的**实例 ID**，进入实例详情页面。



3. 选择“基本信息”标签，可查看和编辑实例的基本信息。



信息说明：

- **实例 ID**：购买实例后，系统自动生成的唯一 ID。
- **实例名称**：系统默认的名称为 casb-default，您可以通过修改名称，给实例进行命名。
- **地域**：实例所在地域。
- **私有网络**：实例所属的私有网络（VPC）信息。
- **所属子网**：实例所属的子网（Subnet）信息。
- **标签**：实例已绑定的标签信息。详情请参见 标签管理 。

> ⚠ **注意：**
> 变更私有网络或子网后，代理的VPC网络和代理IP会发生变化，可能造成应用无法访问代理，请谨慎操作。

分类分级资源管理

最近更新时间：2024-12-31 17:50:22

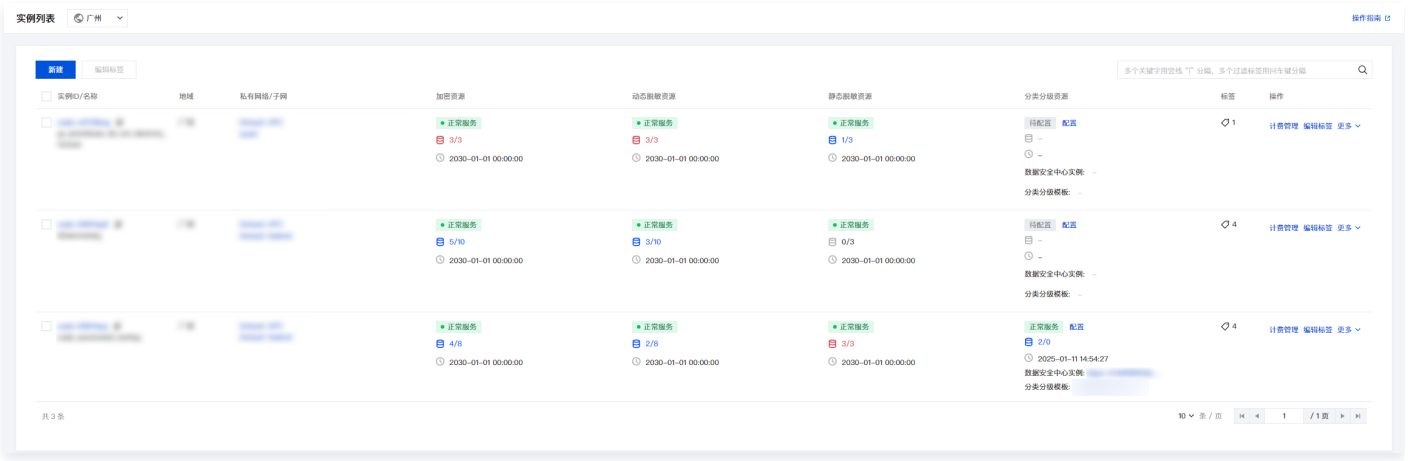
数据安全网关（云访问安全代理）与数据安全治理中心相联动，通过将数据识别与脱敏模板相结合，CASB 能够针对不同类型和特征的数据，精准地应用相应的脱敏策略，保障在数据使用和共享过程中，敏感信息得到有效保护。

前提条件

已 购买数据安全治理中心实例 。

操作步骤

1. 登录 控制台，在左侧导航栏中，单击**实例 > 实例列表**。
2. 在实例列表页面，选择已购买实例的地域，查看已购买的 实例列表 。



3. 选择需要进行配置的 CASB 实例，单击分类分级资源列的**配置**。

4. 在配置弹窗中，选择需要绑定的数据安全治理中心实例和分类分级模板，单击**确定**即可完成分类分级资源的配置。

标签管理

最近更新时间：2024-11-13 09:44:52

操作场景

标签 是用于从不同的维度，对资源进行分类和权限管理。
为 CASB 实例设置标签，可以方便地对实例进行分类和跟踪管理，实现根据标签筛选和汇总CASB实例信息。

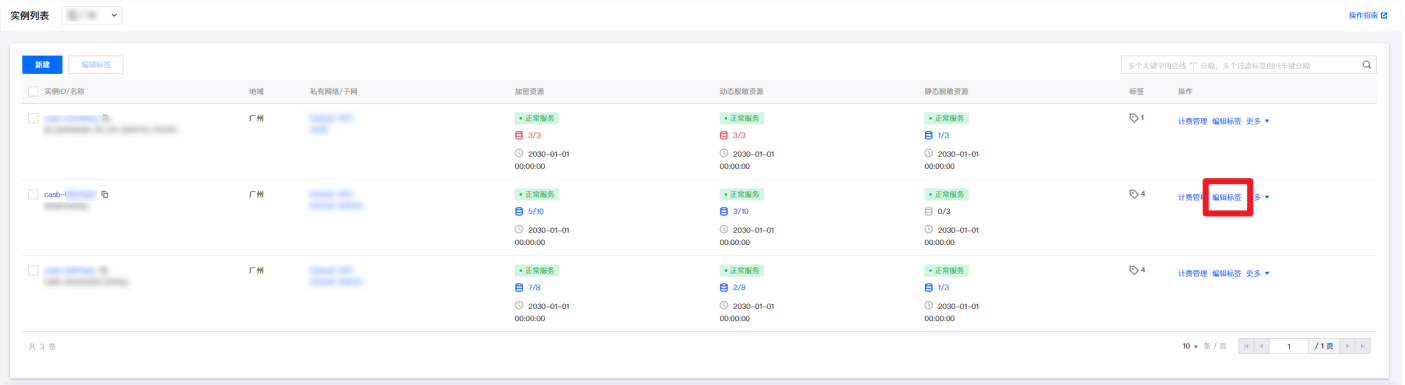
使用限制

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

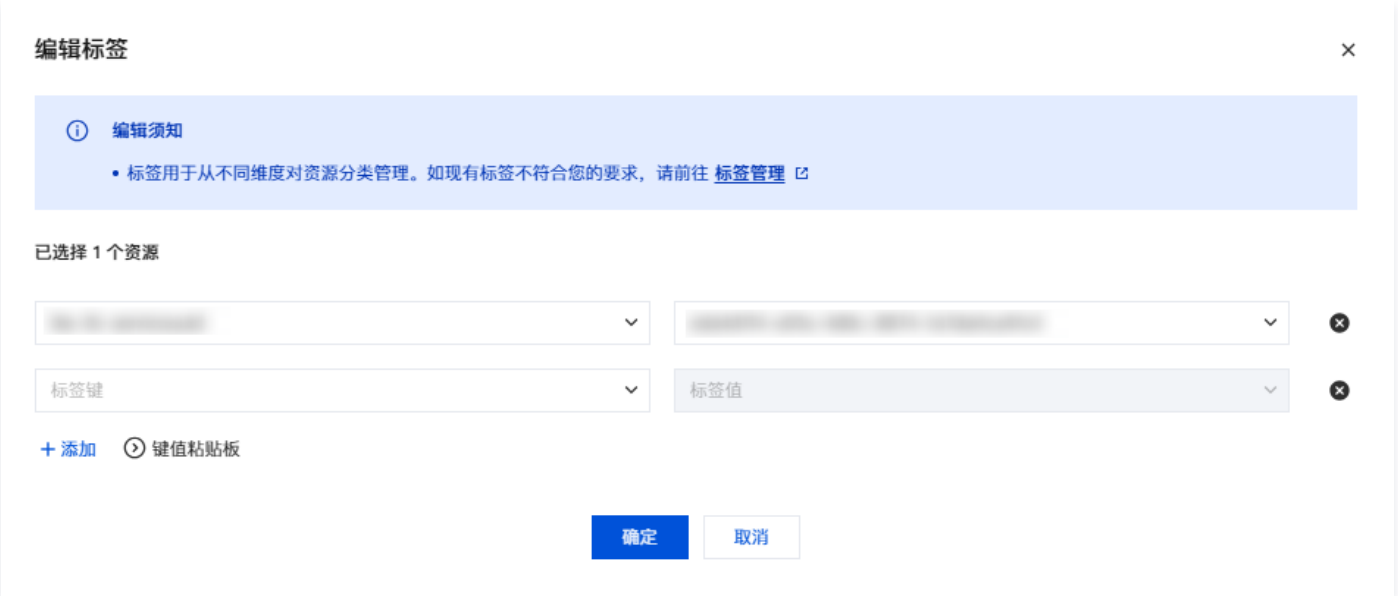
操作步骤

编辑单个标签

1. 登录 控制台，在左侧导航栏中，单击**实例 > 实例列表**。
2. 在实例列表页面，选择已购买实例的地域，查看已购买的 实例列表 。选择需添加标签的实例，单击操作列的**编辑标签**。



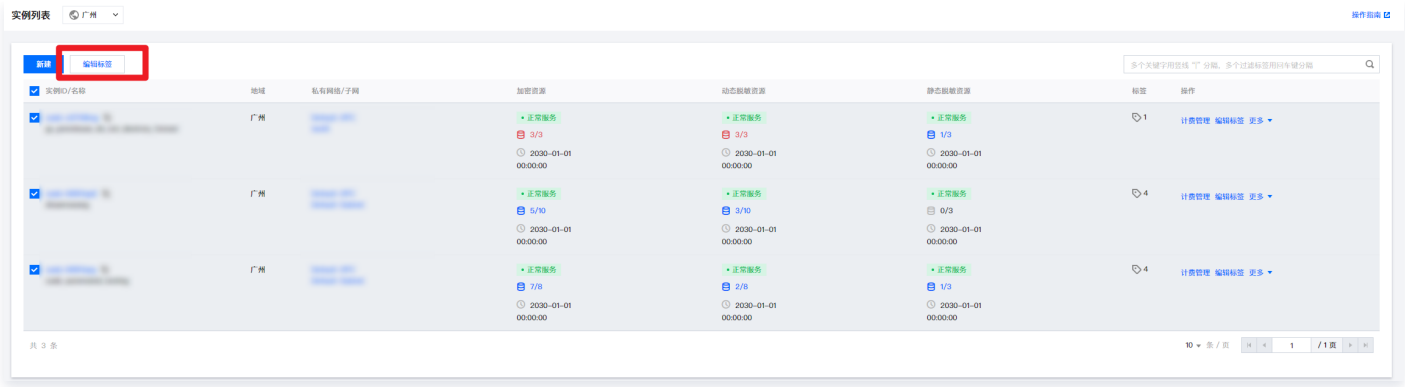
3. 在编辑标签弹窗中，可查看到已选择1个资源，根据实际需求进行**添加**、**删除**标签。



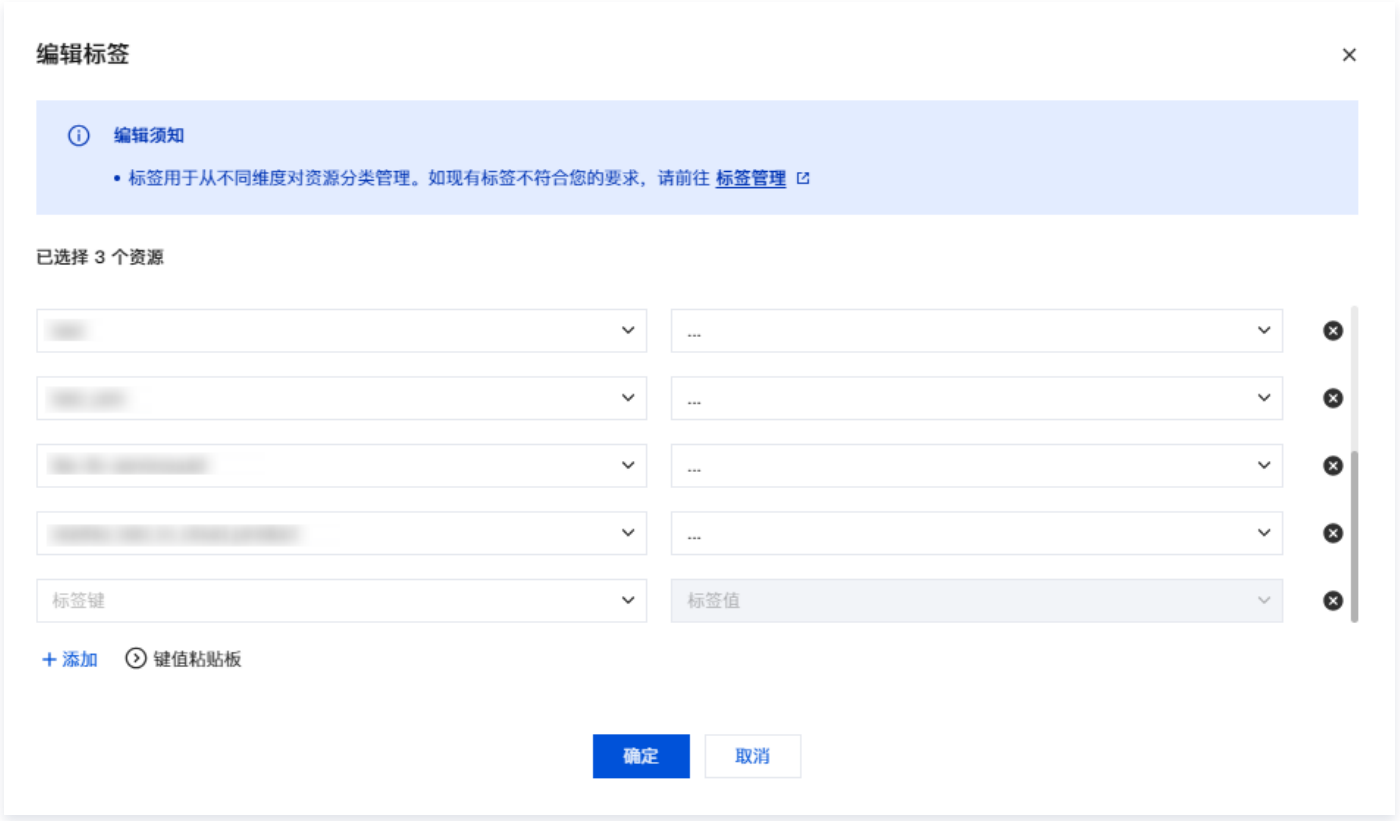
4. 单击**确定**，系统出现修改成功提示，则说明标签修改成功。

批量编辑标签

1. 登录 控制台，在左侧导航栏中，单击**实例 > 实例列表**。
2. 在实例列表页面，选择已购买实例的地域，勾选需编辑标签的实例，单击实例顶部的**编辑标签**。

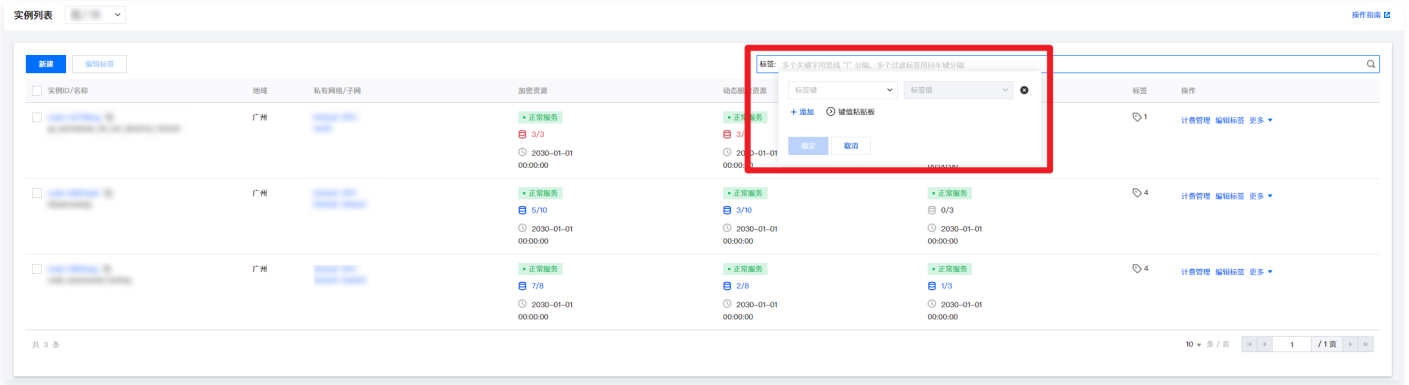


3. 在**编辑标签**的弹窗中，可查看到已选择多个资源，根据实际需求进行**添加**、**删除**标签。



通过标签筛选实例

1. 登录 控制台，在左侧导航栏中，单击**实例 > 实例列表**。
2. 在实例列表页面，选择已购买实例的地域，右侧的搜索框中，选择以**标签**作为筛选条件，选择标签键和标签值，即可根据标签筛选 CASB 实例列表。



安全组管理

最近更新时间：2024-11-13 09:44:52

> **注意：**
> CASB 绑定的安全组为 CASB 代理的入站和出站规则，与部署应用的 CVM 绑定的安全组、数据库绑定的安全组互相独立。

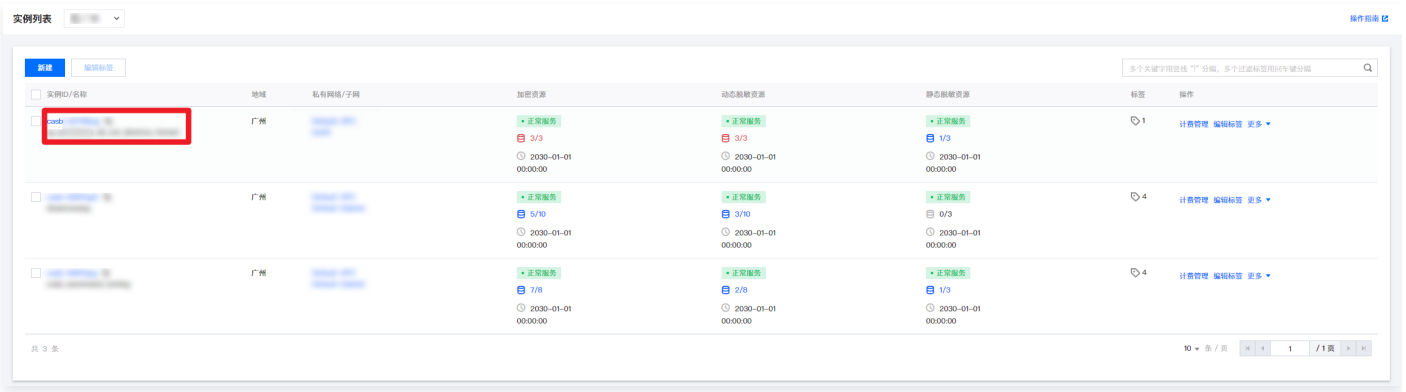
前提条件

需已 购买开通 CASB 实例 。

操作步骤

查看已绑定安全组和规则

1. 登录 控制台，在左侧导航栏中，单击**实例 > 实例列表**。
2. 在实例列表页面，选择已购买实例的地域，查看已购买的 实例列表 。单击需要操作的**实例 ID**，进入实例详情页面。



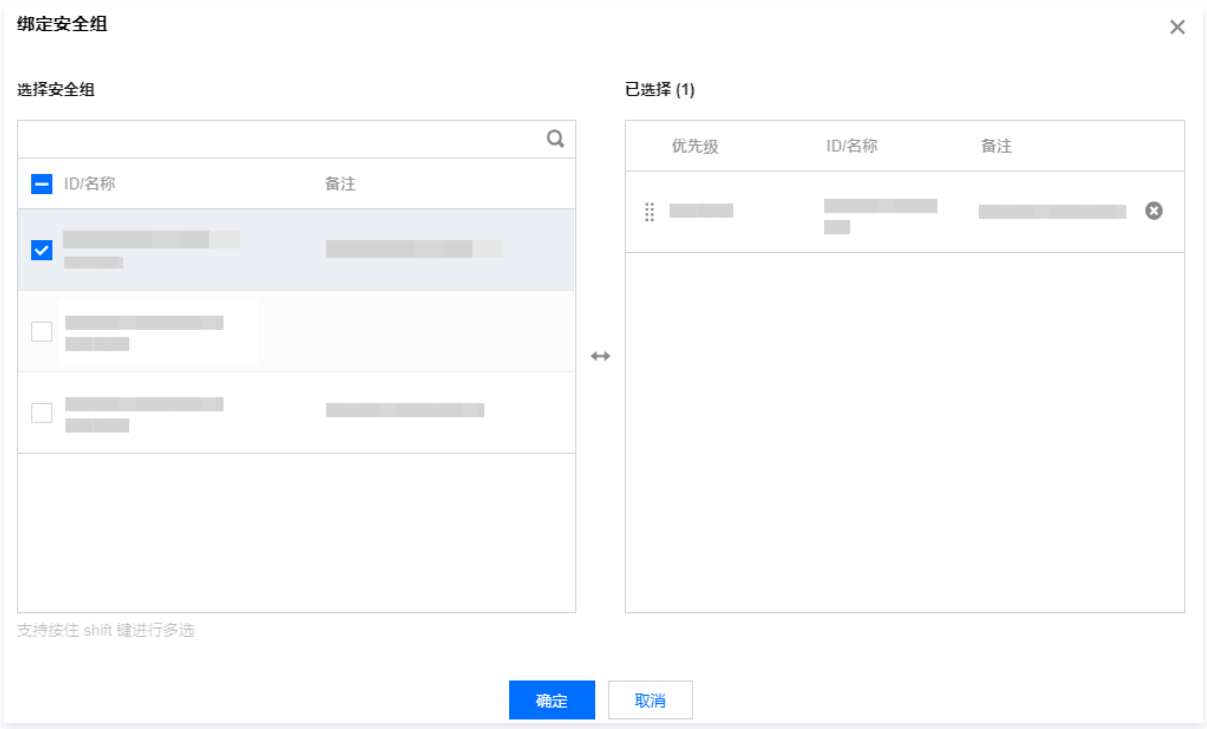
3. 选择**安全组**标签，可查看和配置 CASB 实例绑定的安全组及出入站规则。

绑定/修改/解绑安全组。

1. 在已绑定安全组信息块中，单击**编辑**。

2. 在绑定安全组页面，选择或取消选择所需的安全组，单击**确定**即完成安全组配置。

> **注意：**
> 在进行操作前，需已完成安全组配置，详情请参见 创建安全组 。



3. 完成安全组配置后，在**安全组**标签页即可查看和配置 CASB 实例绑定的安全组及出入站规则。

代理资源管理

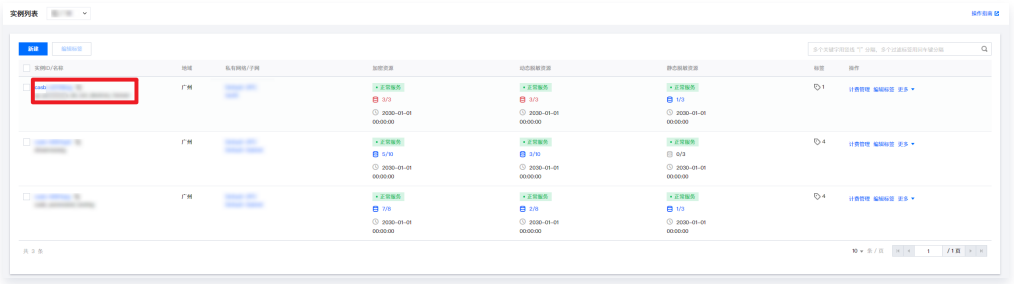
最近更新时间：2024-11-22 10:00:53

前提条件

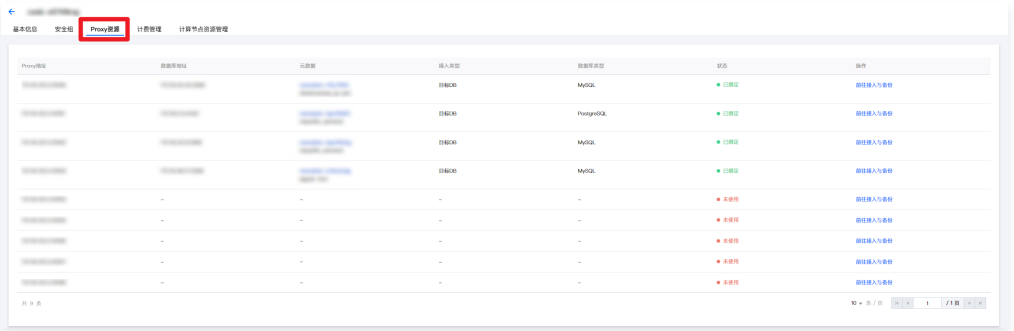
需已 购买开通 CASB 实例 。

操作步骤

1. 登录 控制台， 在左侧导航栏中，单击**实例 > 实例列表**。
2. 在实例列表页面，选择已购买实例的地域，查看已购买的 实例列表，单击目标**实例 ID**。



3. 选择 **Proxy 资源**标签，可查看 CASB 实例提供的所有代理资源列表及代理资源已绑定的元数据信息。



代理账号管理

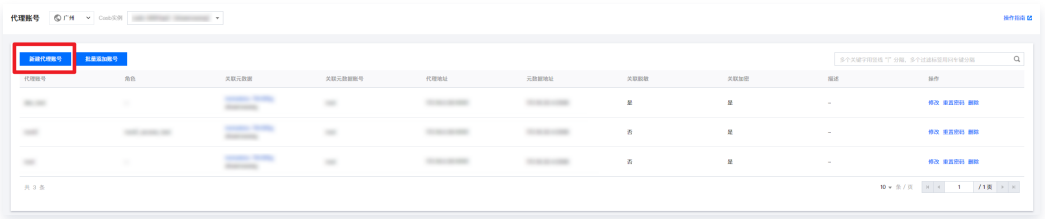
最近更新时间：2024-11-07 11:37:52

前提条件

已 购买开通 CASB 实例 。

新建代理账号

1. 登录 控制台， 单击左侧数据实例菜单下的**代理账号**。
2. 在代理账号页面，选择所需的地域和 CASB 实例。
3. 在代理账号页面，单击**新建代理账号**，弹出新建代理账号窗口。



4. 在新建代理账号窗口中，配置相关参数，单击**确定**，即可完成创建代理账号。

参数名称	参数说明
代理	选择已绑定元数据的 Proxy 资源。
关联元数据	根据选择的 Proxy 资源自动拉取对应的元数据。
元数据账号	选择关联的元数据对应的账号。
代理账号名	创建用于 Proxy 连接时的账号；代理账号名，最小4字节，最大16字节，以字母开头，可以包含大小写字母、数字、下划线。
代理账号密码	创建用于 Proxy 连接时的密码；代理密码，最小4字节，最大16字节，以字母开头，至少包含英文、数字和符号 _+-,&=!@#$%^*() 中的2种。
描述	代理账号的用途描述，最大1024字节。（可选）

版权所有：腾讯云计算（北京）有限责任公司

批量导入代理账号

1. 登录 控制台，单击左侧数据实例菜单下的**代理账号**。
2. 在代理账号页面，选择所需的地域和 CASB 实例。
3. 在代理账号页面，单击**批量添加账号**，弹出批量添加代理账号窗口。

4. 在批量添加代理账号窗口中，单击**点击下载导入模板**，根据导入模板要求填写相关代理账号信息。
5. 本地完善好导入信息后，单击**点击上传**。上传完成后，单击**确定**，即可将代理账号信息导入到系统中。
   - 重新上传：导入失败时，可以单击**重新上传**以再次导入文件。
   - 下载失败报告：当导入失败时，系统将提供失败报告。您可以根据报告中的错误信息修改表格内容，然后重新上传。

计算节点管理

最近更新时间：2024-11-07 11:37:52

操作场景

您可以通过此模块及时了解计算节点资源的监控信息，并通过配置资源告警来通知管理员计算节点资源使用情况的异常变化，使管理员能够迅速采取相应措施，从而保障产品功能的稳定运行。

> **说明：**
> 计算节点是指分布式计算系统中用于执行计算任务的计算机或服务器。购买 CASB 实例后，CASB 系统会自动为每个实例分配跨可用区、高可用的代理计算节点，以支持完成数据加密、数据脱敏。

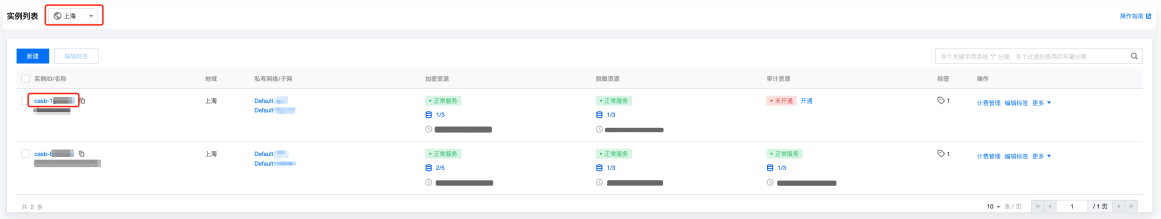
前提条件

已 购买开通 CASB 实例 。

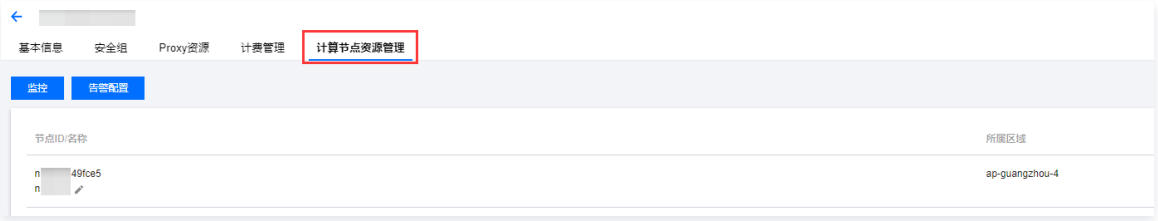
操作步骤

查看计算节点信息

1. 登录 控制台，在左侧导航栏中，单击**实例 > 实例列表**。
2. 在实例列表页面，选择已购买实例的地域，查看已购买的 实例列表 。单击需要操作的**实例 ID**，进入实例详情页面。



3. 选择**计算节点资源管理**标签，即可查看当前实例下代理集群的节点信息。其中节点名称支持**编辑**修改。



> **说明：**
> CASB 实例创建时，系统会自动分配跨可用区高可用的代理计算节点。

计算节点资源监控

1. 在计算节点资源管理页中，单击**监控**，跳转至腾讯云可观测平台。

2. 在腾讯云可观测平台，可查看所有地域下所有 CASB 计算节点的资源监控信息，包括 CPU 使用率、内存占用率、带宽、连接数等。

计算节点资源告警

1. 在计算节点资源管理页中，单击**告警配置**，会跳转至腾讯云可观测平台，可根据业务需求对CASB计算节点的资源使用配置告警。

2. 在新建告警策略时，策略类型选择**数据安全网关（云访问安全代理）**。告警配置详情请参见 **告警服务简介**。

> **说明：**
> 计算节点资源告警的主要目的是及时通知管理员关于计算节点资源使用情况的异常变化，以便管理员能够迅速采取相应措施，从而保障产品功能的稳定运行。

元数据
元数据管理
新增元数据
添加云元数据

最近更新时间：2024-11-22 10:00:53

如果您使用腾讯云数据库服务中的数据库，可参考本文档将所创建的数据库直接添加到元数据中。

前提条件

- 已注册**腾讯云**，并已购买**数据安全网关（云访问安全代理）实例**。详情可以参考 快速入门 。
- 使用腾讯云数据库服务创建相对应的数据库资源，同时相对应的子网中含有可用的 IP 配额。数据库资源相关配置可参考 常见问题 。

约束条件

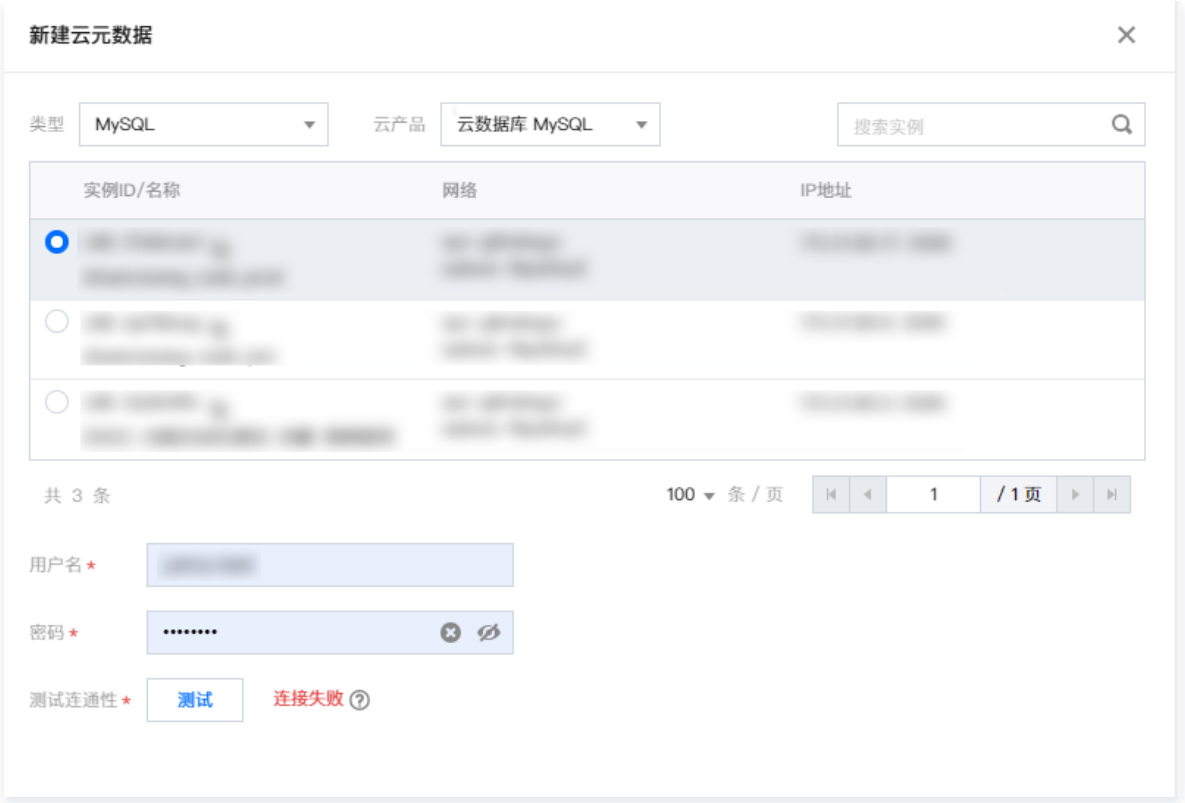
目前只能添加数据安全网关（云访问安全代理）支持的数据库类型及版本，其中所支持的数据库详情如下表：

数据库类型	版本
MySQL	5.6、5.7、8.0
TDSQL MySQL版	5.6、5.7、8.0
PostgreSQL	postgre 9.3.5

操作步骤

1. 登录 控制台，在左侧导航栏中，单击元数据 > **元数据管理**。
2. 在元数据管理页面，选择所需的地域、CASB 实例。
3. 在元数据管理页面，选择需要新建的元数据类型 Tab 栏，单击**新建云元数据**。

4. 在新建云元数据弹窗中，选择元数据类型和云产品。系统将显示当前账号在所选地域、元数据类型、云产品下的元数据。
5. 在新建云元数据弹窗中，选择具体实例，然后输入所选元数据的用户名和密码，单击**测试**进行测试连通性，连接成功后单击**确定**即可新增云元数据。



参数名称	参数说明
元数据类型	目前只支持MySQL、PostgreSQL、MongoDB类型的数据库。
云产品	支持的云产品云数据库MySQL、TDSQL-C MySQL版、云数据库 MariaDB、云数据库 PostgreSQL、TDSQL MySQL版、云数据库 MongoDB。
选择实例	选择源数据类型、云产品后，会自动拉取元数据实例信息
用户名	用于登录数据库的账号名。
密码	用于登录数据库的账号名对应的密码。
测试连通性	测试数据库的连通性，检测是否能正常访问。

添加自建元数据

最近更新时间：2024-11-22 10:00:53

如果您需要添加腾讯云云数据库产品以外的自建数据库实例，可参考本文档内容进行添加，在进行添加之前，需要获取自建数据库的基础信息，包括 IP 地址、子网地址、私有网络等相关信息。

前提条件

- 已注册**腾讯云**，并已购买**数据安全网关（云访问安全代理）实例**。详情可以参考 快速入门 。
- 已获取自建数据库的 IP 地址、子网地址、私有网络等相关信息，同时相对应的子网中含有可用的 IP 配额。
- 需要在自建数据库所在 VPC 下有空闲的 `/20` 网段可用。
- 自建数据库网段相关配置可参考 常见问题 。

> **注意：**
> - CASB 绑定 CVM 自建的元数据时，需要在 CASB 代理和 CVM 之间建立一个专用网络连接，会默认创建一个子网来打通网络。删除释放已绑定此 CVM 的元数据后，才可以删除和释放此子网。
> - 可创建一个 CLB 绑定到 CVM 上，新增自建元数据时，选择绑定 CLB 到 CASB，通过这种方式绑定的元数据不会创建子网。

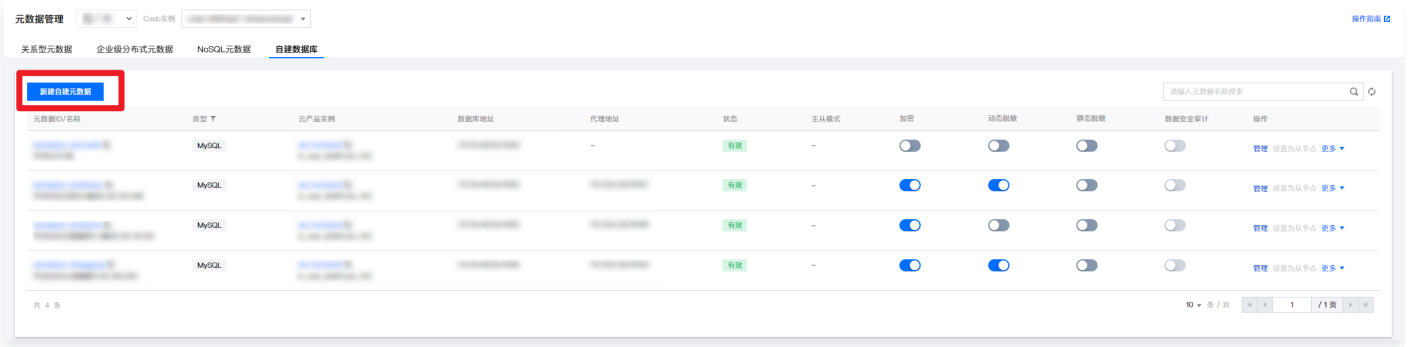
约束条件

目前能添加数据安全网关（云访问安全代理）支持的数据库类型及版本，其中所支持的数据库详情如下表：

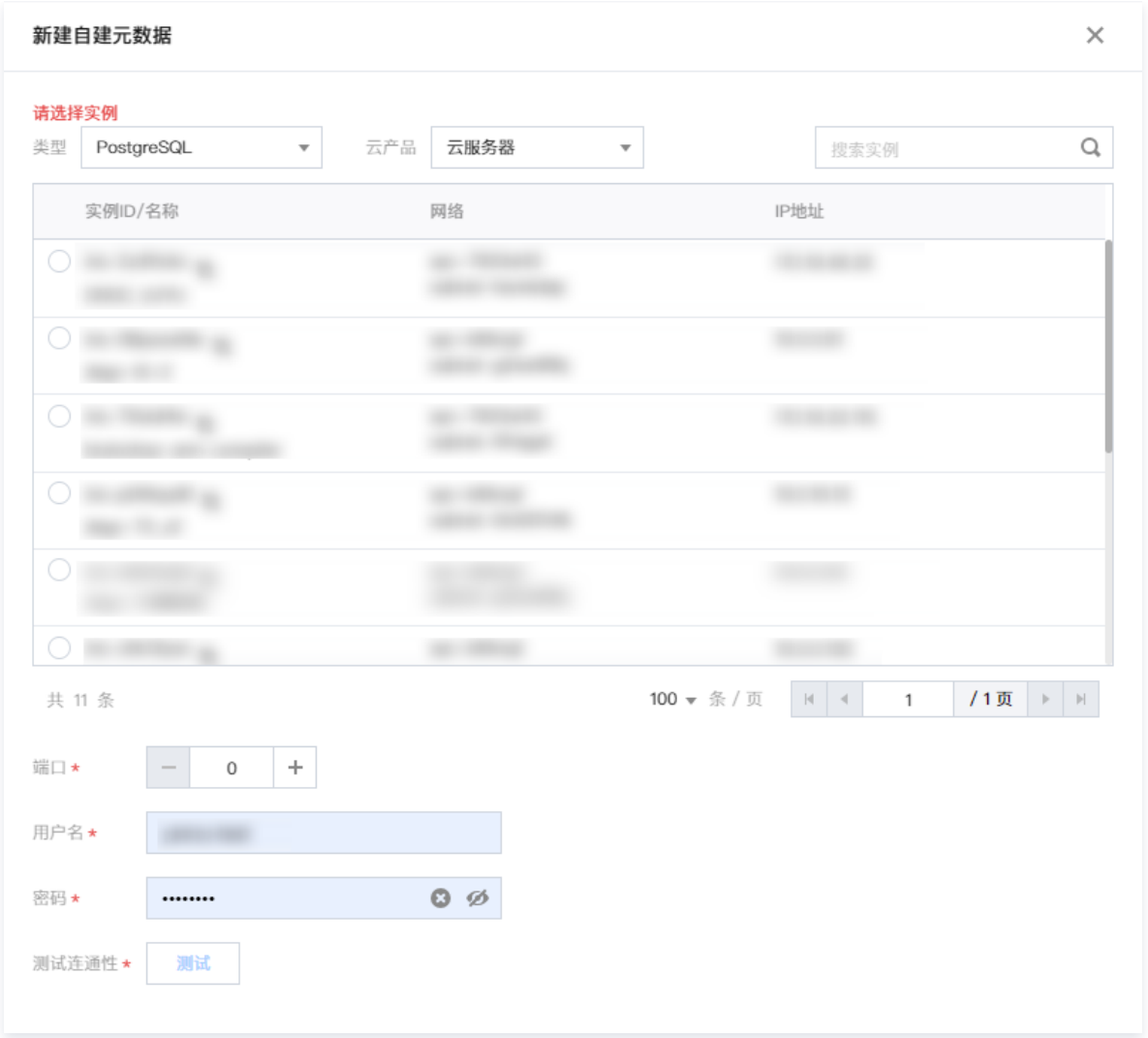
数据库类型	版本
MySQL	5.6、5.7、8.0
PostgreSQL	postgre 9.3.5

操作步骤

1. 登录 控制台，在左侧导航栏中，单击元数据 > **元数据管理**。
2. 在元数据管理页面，选择所需的地域、CASB 实例。
3. 在元数据管理页面，选择**自建数据库** Tab 栏，单击**新建云元数据**。



4. 在新建自建元数据弹窗中，选择元数据类型和云产品。系统将显示当前账号在所选地域、元数据类型、云产品下的元数据信息。
5. 在新建自建元数据弹窗中，选择具体实例，然后输入所选元数据的端口、用户名和密码，单击**测试**进行测试连通性，连接成功后单击**确定**。



参数名称	参数说明
元数据类型	目前只支持MySQL、PostgreSQL类型的数据库。
云产品	支持的云产品 cvm、lb。
选择实例	**“云产品”** 中选择“cvm”时，会自动拉取 cvm 实例信息；选择 lb 时，会自动拉取 lb 实例信息。根据实际情况选择对应云产品。
端口	根据实际情况输入数据库服务监听的端口号。
用户名	用于登录数据库的账号名。
密码	用于登录数据库的账号名对应的密码。
测试连通性	测试数据库的连通性，检测是否能正常访问。

基本信息管理

最近更新时间：2024-11-14 17:29:23

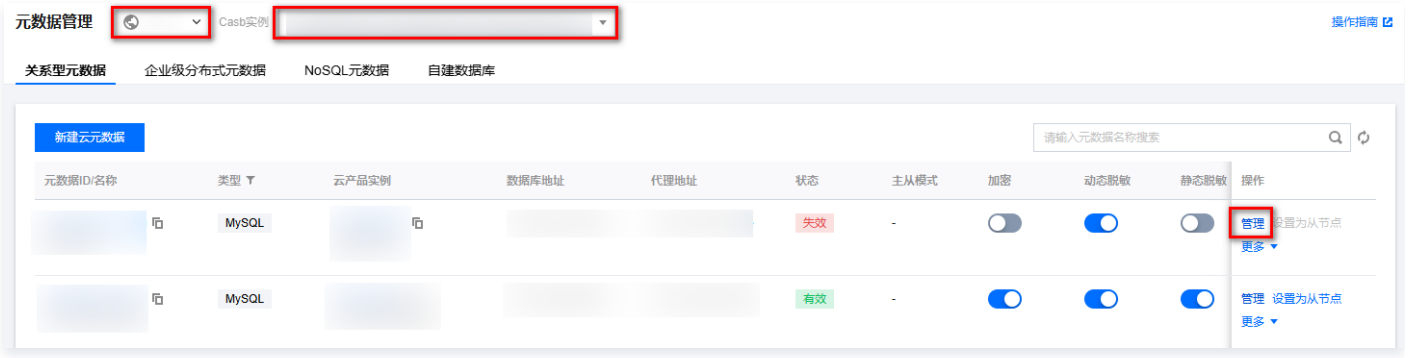
本文档以关系型元数据为例，介绍元数据基本信息管理的相关操作说明。

前提条件

- 已 购买开通 CASB 实例 。
- 已创建元数据。如未创建元数据，请查阅 添加云元数据库 、添加自建数据库 。

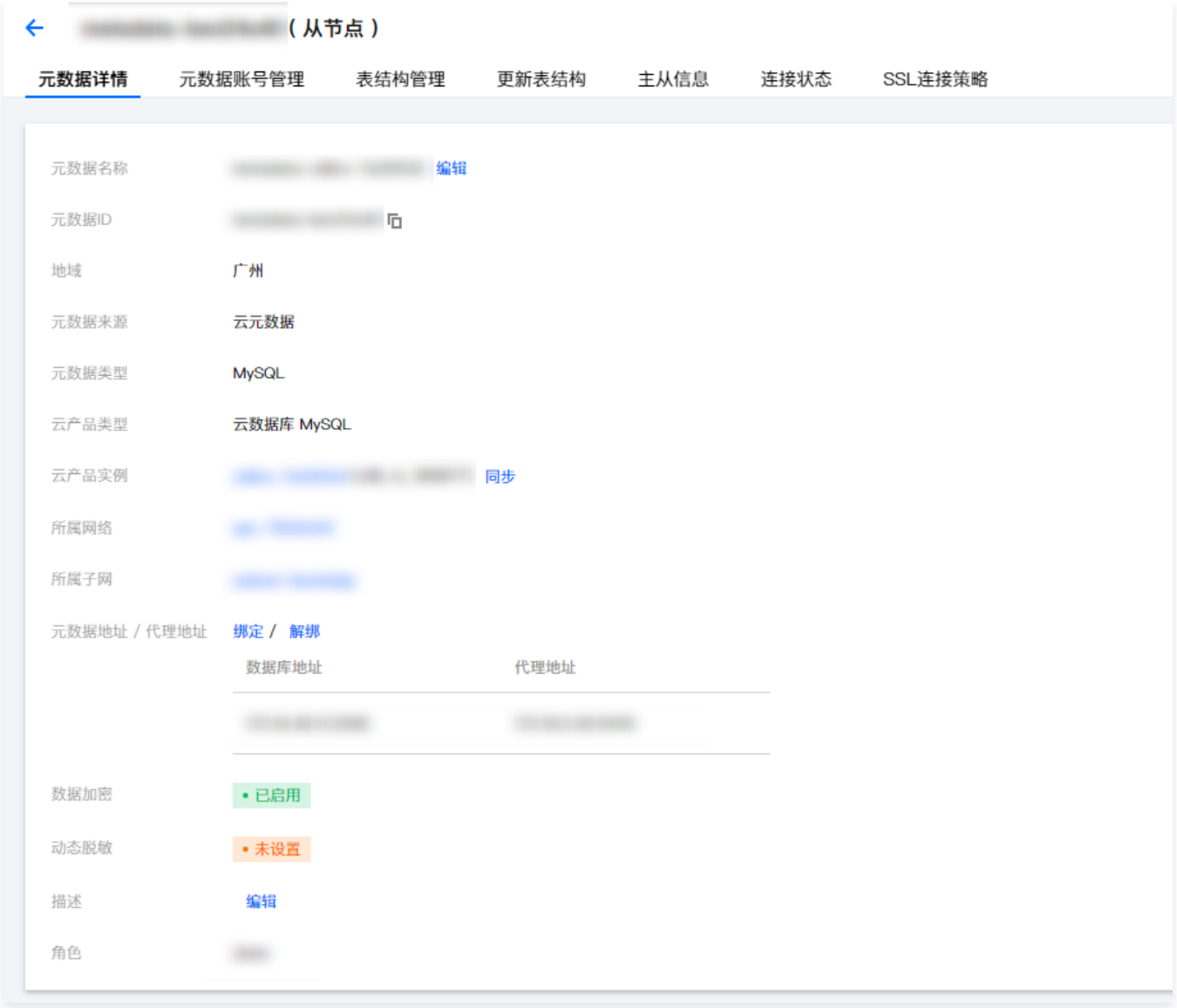
操作步骤

1. 登录 控制台 ，在左侧导航栏中，单击**元数据 > 元数据管理**。
2. 在元数据管理页面，选择所需的地域、CASB 实例。
3. 在元数据管理页面，选择需要查看基本信息的元数据，单击操作栏中的**管理**。



查看元数据详情

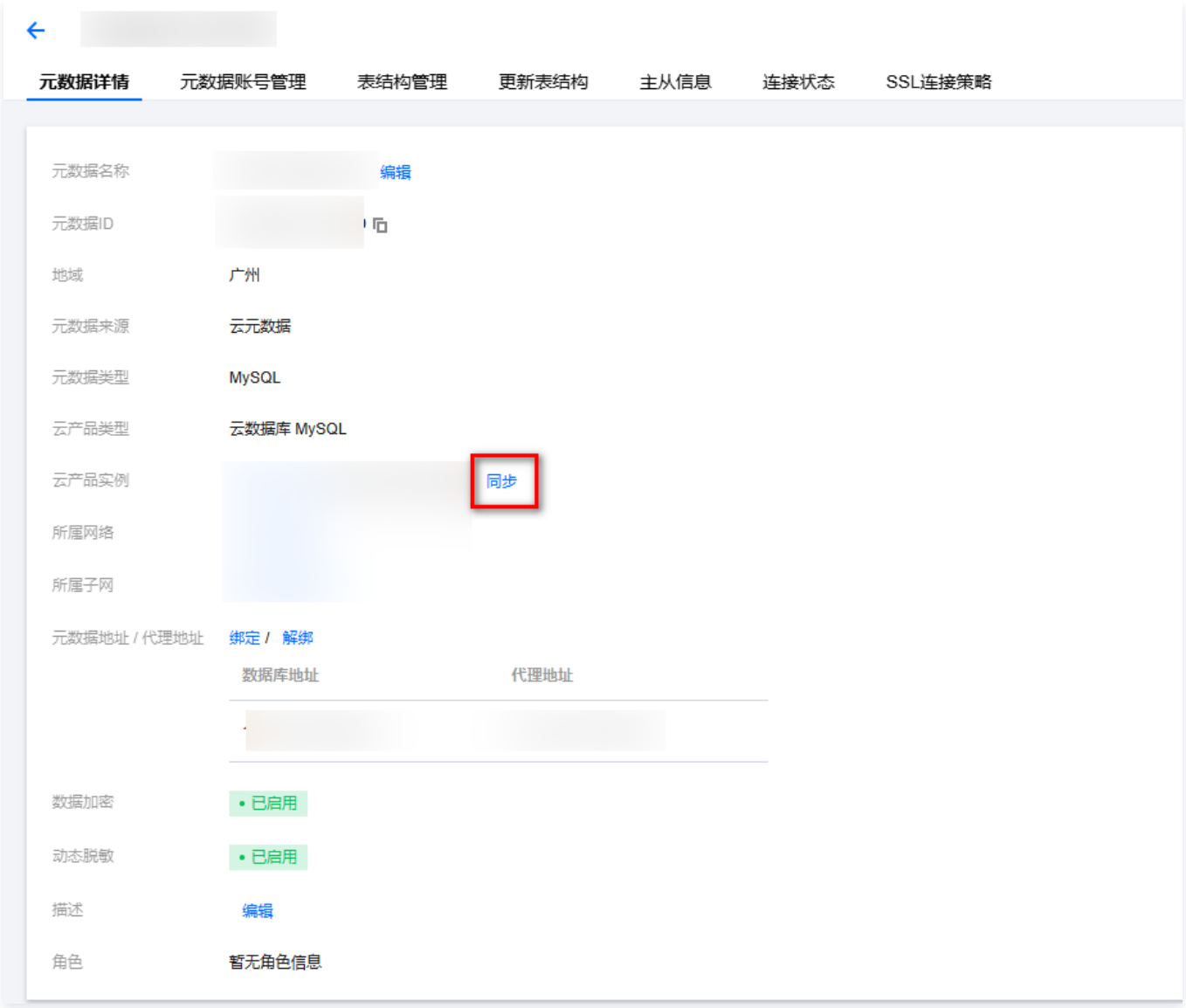
1. 在元数据管理页面，单击**元数据详情**标签，即可查看元数据详情。
2. 元数据详情包括了对应的元数据 ID、地域、元数据的类型、云产品实例、网络、IP、已绑定的代理、规则配置状态等信息。



同步元数据基本信息

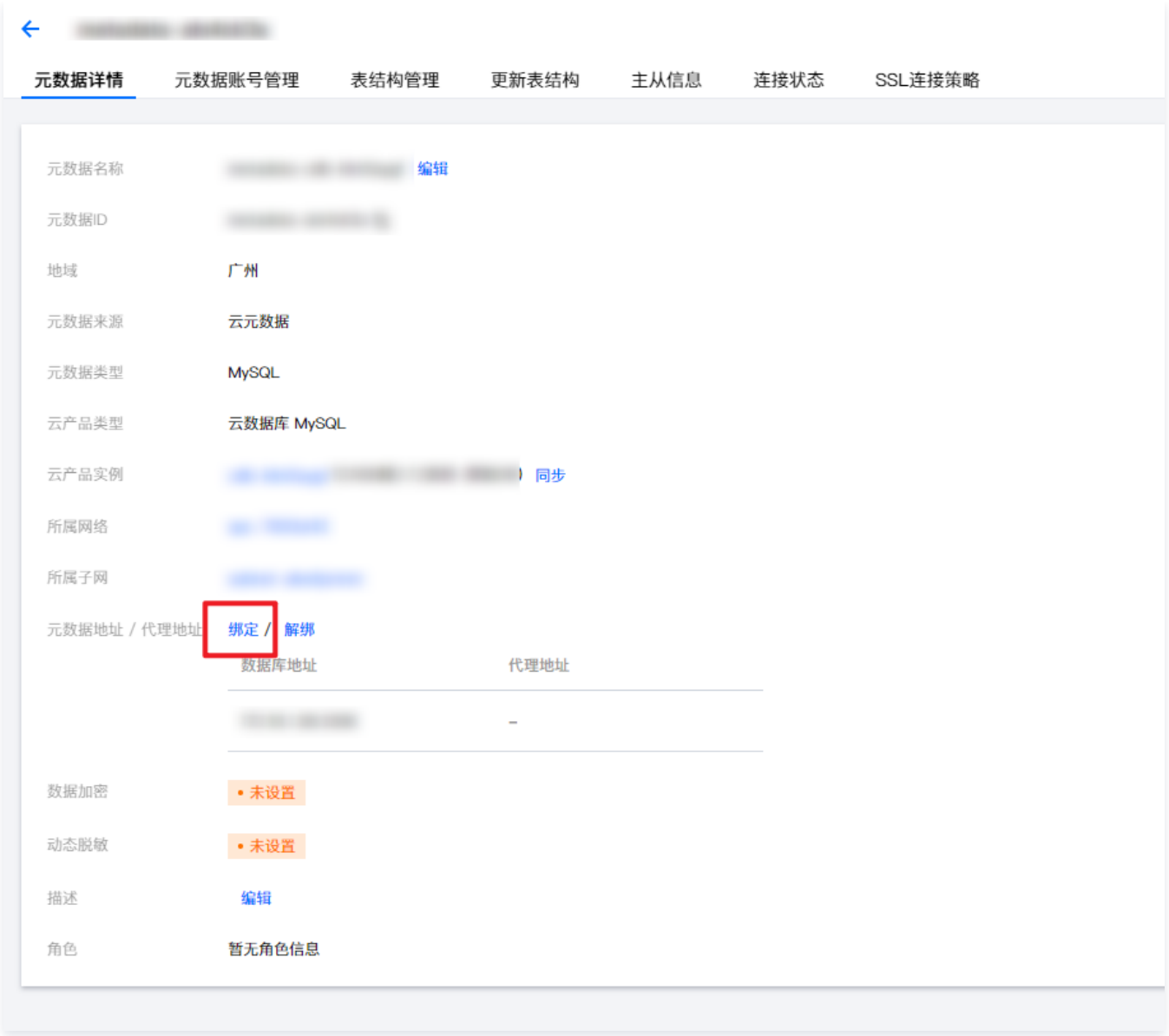
元数据的 IP、网络等信息变更后，需手动到 CASB 元数据基本信息管理平台同步最新的资源信息，否则，可能会导致代理访问数据库失败。

1. 在元数据管理页面，单击**元数据详情**标签，即可查看元数据详情。
2. 单击**云产品实例 ID** 右侧的**同步**即可自动同步。



绑定代理

1. 在元数据管理页面，单击**元数据详情**标签，即可查看元数据详情。
2. 单击**元数据地址/代理地址**右侧的**绑定**，弹出“绑定元数据”对话框。



3. 选择需要绑定的代理地址，以及需要开通的加密/脱敏功能。

说明：
若此项功能已购买的配额已用完，可购买 功能扩展包 增加配额。

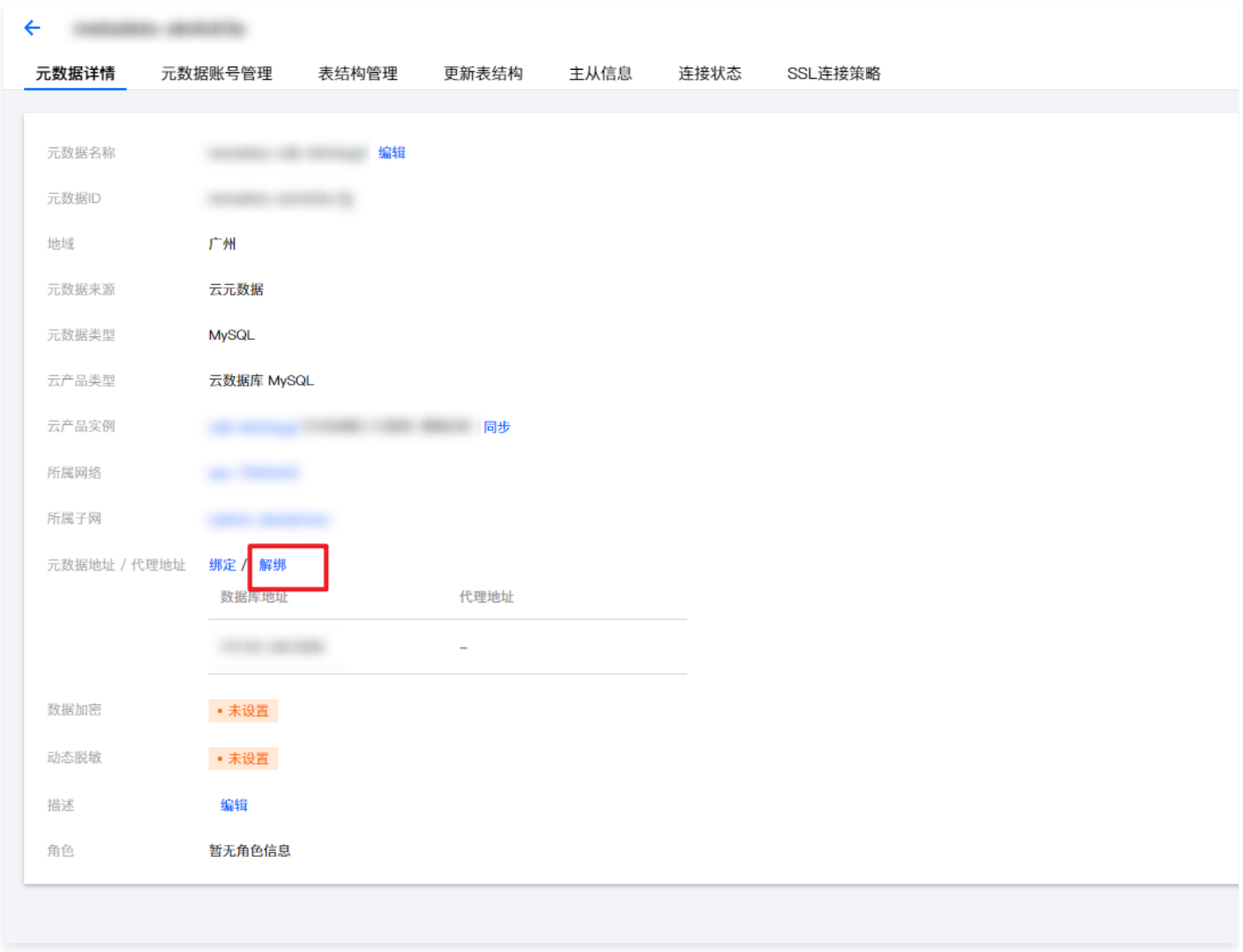
4. 单击**确定**，即可完成代理和元数据的绑定。

> **说明：**
> 代理和元数据绑定后，需 设置代理账号 后，才可以通过代理账号访问代理。

解绑代理和元数据

> **注意：**
> 解绑元数据后，代理地址下的所有代理账号及绑定到代理账号的脱敏策略、访问控制策略都将被删除、请谨慎操作。

1. 在元数据管理页面，单击**元数据详情**标签，即可查看元数据详情。
2. 单击**元数据地址/代理地址**右侧的解绑，弹出“解绑元数据”对话框。



3. 选择需要解绑的代理地址，单击**确定**，即可完成代理和元数据的解绑。

解绑代理
数据库地址
CASB代理地址
确定
取消

元数据账号管理

最近更新时间：2025-03-12 11:42:42

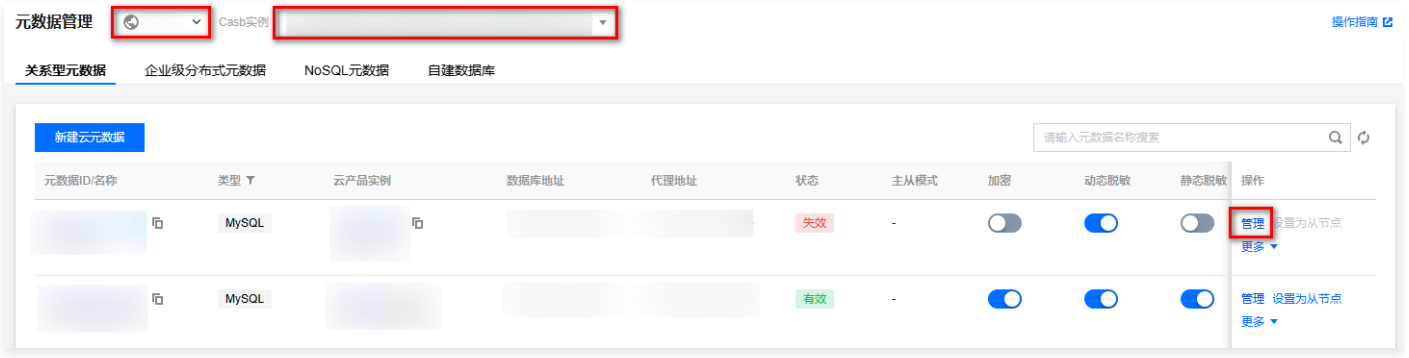
本文档以关系型元数据为例，介绍元数据账号管理的相关操作说明。

前提条件

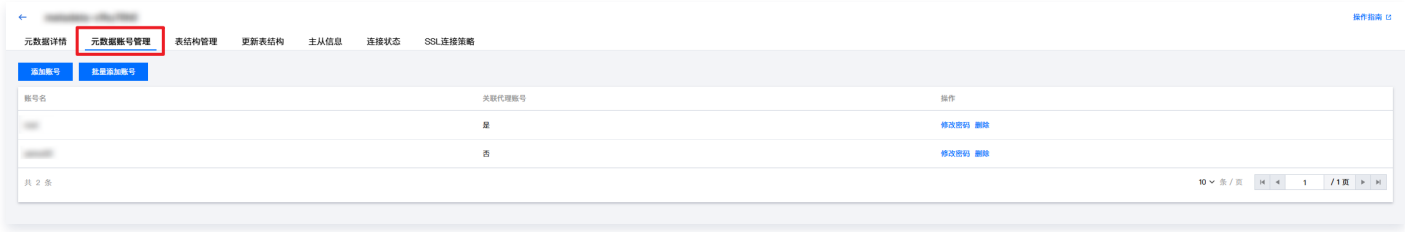
- 已 购买开通 CASB 实例 。
- 已创建元数据。如未创建元数据，请查阅 添加云元数据库 、添加自建数据库 。

操作步骤

1. 登录 控制台 ，在左侧导航栏中，单击**元数据 > 元数据管理**。
2. 在元数据管理页面，选择所需的地域、CASB 实例。
3. 在元数据管理页面，选择需要查看基本信息的元数据，单击操作栏中的**管理**。

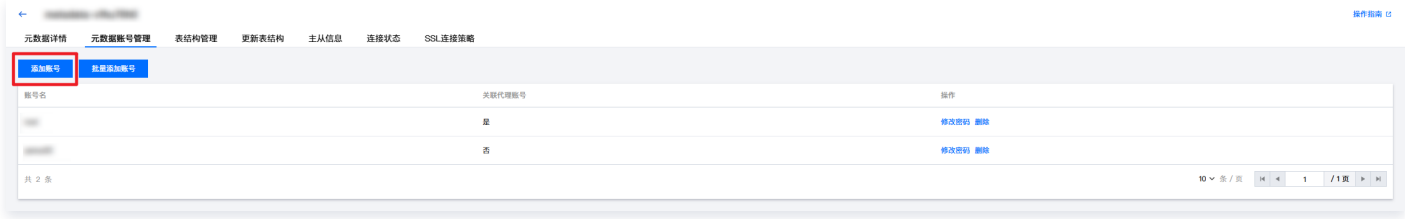


4. 在元数据管理页面，单击**元数据账号管理**标签，进入元数据账号管理页面。页面列表展示当前所有已添加的元数据账号，可以操作修改密码、删除账号。



添加元数据账号

1. 在元数据账号管理页面，单击**添加账号**。



2. 在添加账号弹窗中，输入账号、密码等参数，测试连通性完成后，单击**确定**完成添加账户。

参数名称	参数说明
账号名	用于登录数据库的账号名。
密码	数据库账号名对应的密码。
确认密码	确保与上述密码一致。
测试连通性	测试数据库的连通性，检测是否能正常访问。

批量添加元数据账号

1. 在元数据账号管理页面，单击**批量添加账号**，可以批量导入元数据账号。

2. 在批量添加账号窗口中，单击**点击下载导入模板**，根据导入模板要求填写相关账号信息。
3. 本地完善好导入信息后，单击**点击上传**。上传完成后，单击**确定**，即可将账号信息导入到系统中。
   - 重新上传：导入失败时，可以单击**重新上传**以再次导入文件。

- 下载失败报告：当导入失败时，系统将提供失败报告。您可以根据报告中的错误信息修改表格内容，然后重新上传。

元数据表结构管理

最近更新时间：2024-11-13 17:25:02

本文档以关系型元数据为例，介绍元数据表结构管理的相关操作说明。

元数据账号授权

CASB 提取表结构时，需要查询数据库的库、表、字段等结构信息，因此需要对元数据账号授予以下命令的权限：

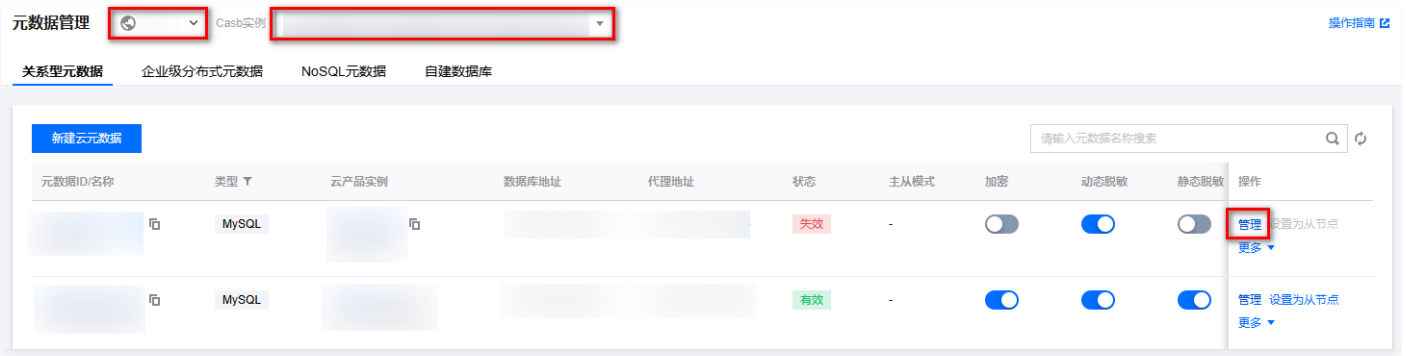
- `information_schema` 数据库的读权限
- `SHOW` 和 `DESCRIBE` 的命令权限
  - `SHOW DATABASES`
  - `SHOW TABLES`
  - `DESCRIBE` table
  - `DESCRIBE` view
  - `SHOW CREATE TABLE`
  - `SHOW CREATE VIEW`

前提条件

- 已 购买开通 CASB 实例 。
- 已创建元数据。如未创建元数据，请查阅 添加云元数据库 、添加自建数据库 。

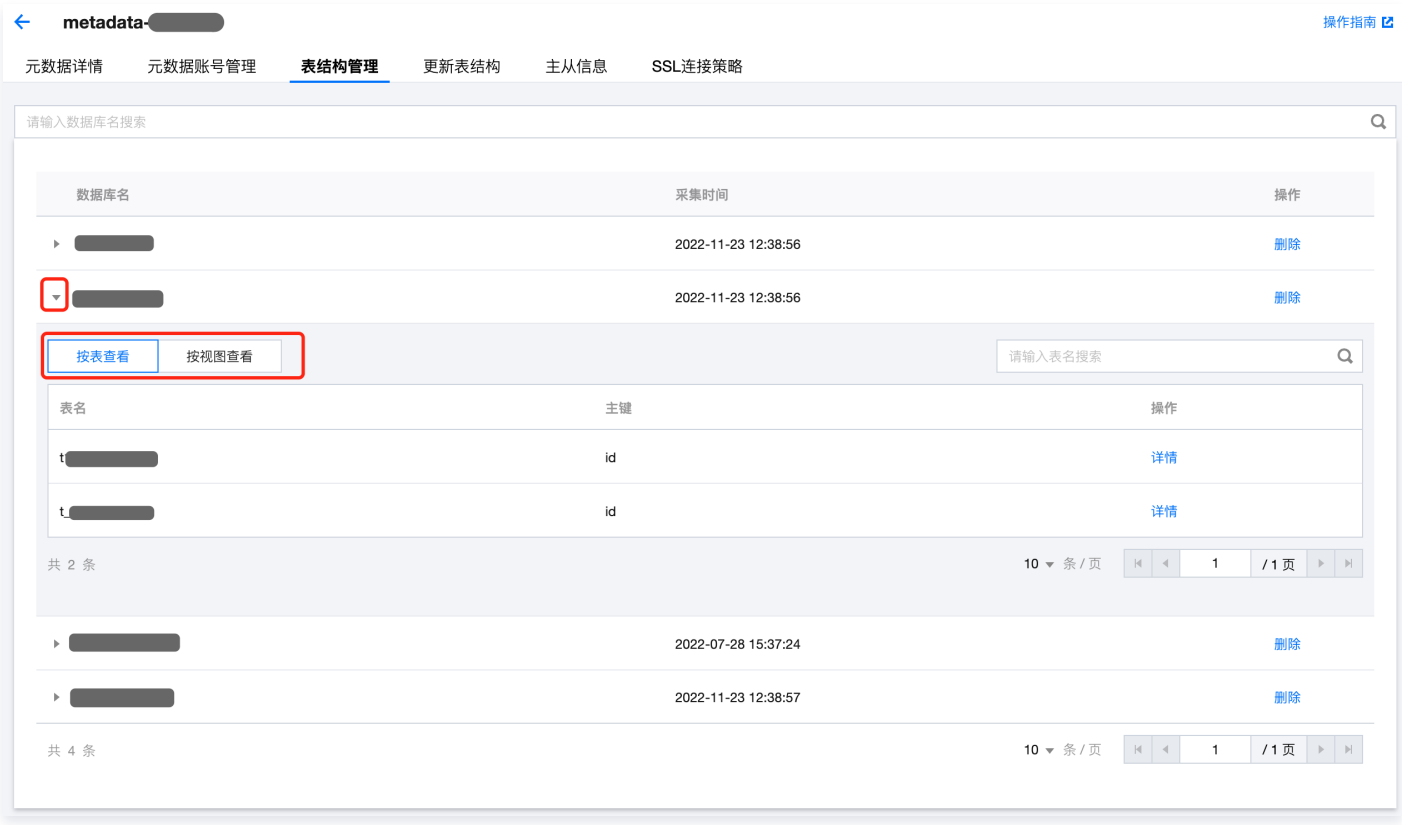
查看表结构

1. 登录 控制台，在左侧导航栏中，单击元数据 > **元数据管理**。
2. 在元数据管理页面，选择所需的地域、CASB 实例。
3. 在元数据管理页面，选择需要查看基本信息的元数据，单击操作栏中的**管理**。

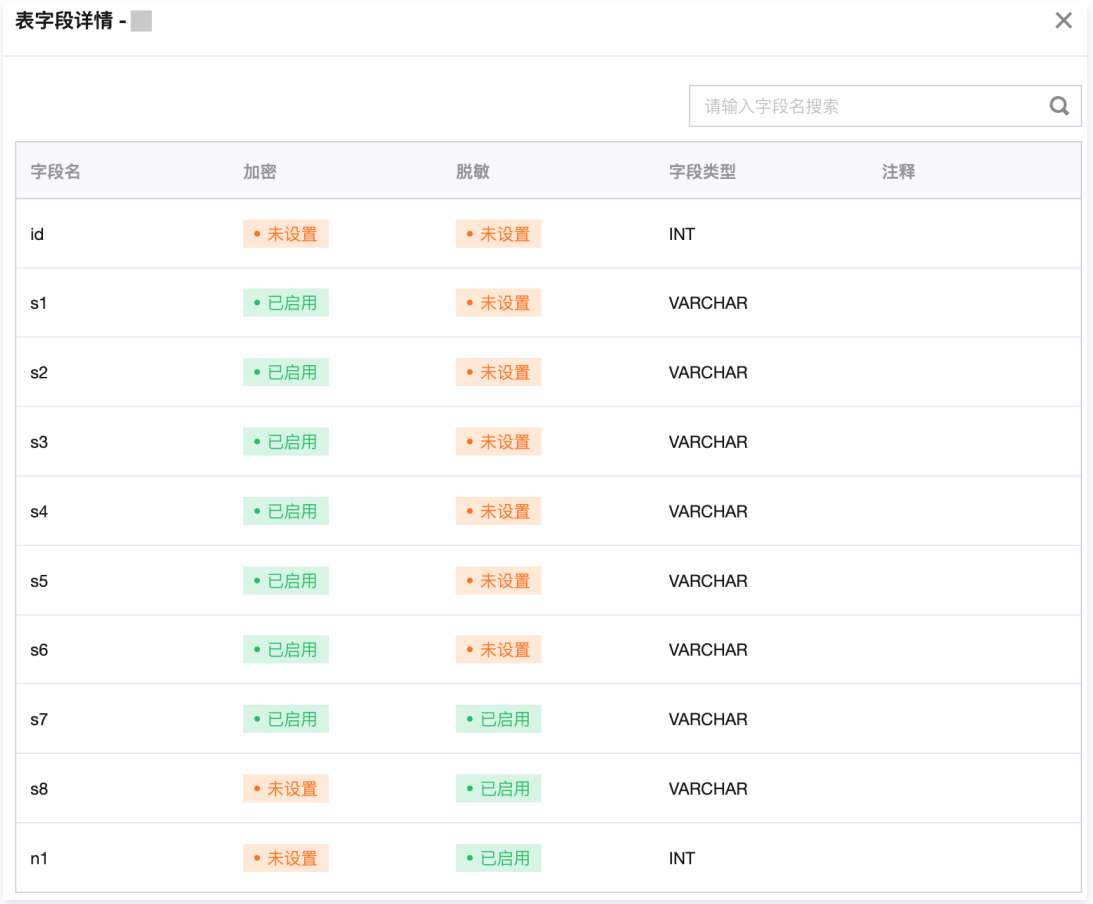


4. 在元数据管理页面中，单击**表结构管理**，进入表结构管理页面。可以查看该元数据下的已采集并应用的数据库信息，以及数据的采集时间。

5. 单击数据库名左侧的▶，即可按表和视图不同维度查看此数据库下 CASB 平台已采集的表和视图信息。



6. 单击操作列的**详情**，即可查看表或视图里详细的字段信息。



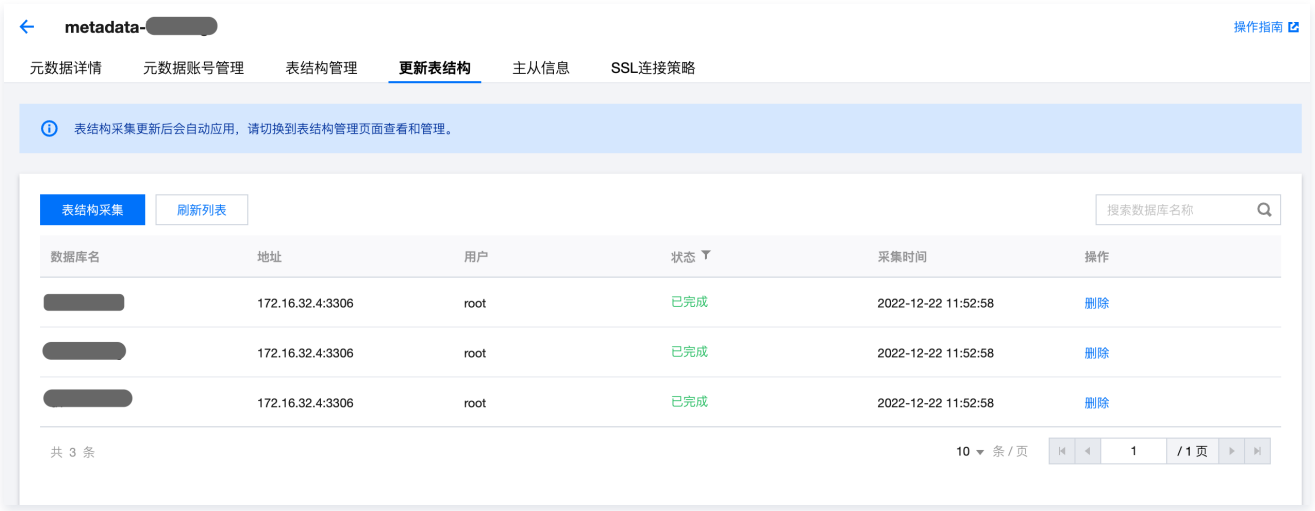
更新表结构

自动更新表结构

若经过 CASB 代理执行表结构的增删改（DDL），CASB 代理将自动采集并更新最新的表结构。

手动更新表结构

1. 在关系型元数据管理页面，单击**更新表结构**标签，进入更新表结构页面。可以查看该元数据所有表结构采集更新的任务列表，包括采集的数据库、采集状态、采集时间等信息。



2. 在更新表结构页面，单击左上角**表结构采集**。
3. 在表结构自动采集对话框中，选择对应的**元数据账号**，单击**确定**即可完成表结构采集更新。

4. 在更新表结构页面，更新了数据库相关信息之后，单击**刷新列表**，可以获取最新的采集任务状态。

主从同步管理

最近更新时间：2024-11-13 09:44:52

前提条件

- 已 购买开通 CASB 实例 。
- 已创建元数据。如未创建元数据，请查阅 添加云元数据库 、添加自建数据库 。

操作详情

1. 登录 控制台 ，在左侧导航栏中，单击元数据 > **元数据管理**。
2. 在元数据管理页面，选择所需的地域、CASB 实例。
3. 找到所需配置的元数据，在其右侧，单击**设置为从节点**。

4. 在选择主节点页面中，选择主节点的地域、CASB 实例以及对应的元数据，单击**确定**。

> ⚠ **注意：**
> - 当前主从模式已设置为**主节点**或**从节点**的元数据,不能再次配置主从节点。
> - 在配置过程中，只有非从节点才能作为主节点。
> - 在配置过程中，所选择的元数据已被设置为主节点，系统将会自动设置为主节点。
> - 当元数据为从节点时，对应的加解密策略、加密密钥会直接从主节点中同步, 从节点密钥保存方式可选择是否使用 KMS 托管, KMS 托管优势和使用说明见：KMS 密钥管理和授权 。

参数说明：

- 地域：金融区与非金融区不可跨地域容灾。
- CASB 实例：选择所需 CASB 实例。
- 元数据：所选源数据，需满足以下条件。

  4.1.1 相同元数据来源。

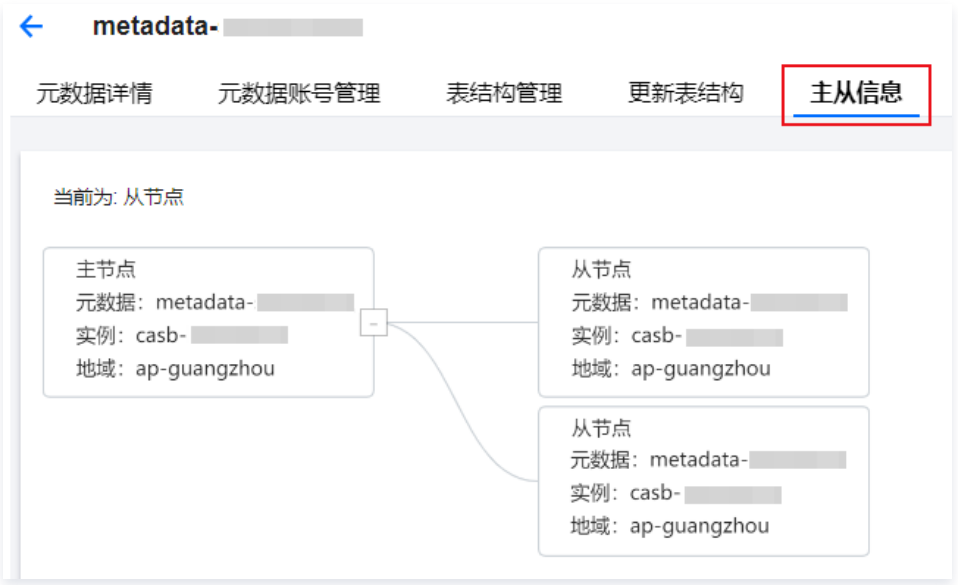
  4.1.2 相同元数据类型。

  4.1.3 不能是从节点。

查看主从信息

1. 登录 控制台，在左侧导航栏中，单击**元数据 > 元数据管理**。
2. 在关系型元数据页面中，选择所需的地域、CASB 实例。
3. 找到所需查看的元数据，单击对应的**元数据 ID**，或在其右侧单击**管理**。

4. 在展开的元数据信息页面中，单击**主从信息**，即可查看当前的主从信息详情。



取消从节点

1. 登录 控制台，在左侧导航栏中，单击**元数据 > 元数据管理**。
2. 在关系型元数据页面中，选择所需的地域、CASB 实例。
3. 找到所需设置的元数据，在其右侧单击**取消从节点**。

⚠ 注意：

- 取消从节点后，将停止从主节点中同步数据。
- 主从关系为一主一从时，当从节点被取消后，主节点也会同步取消主从模式。
- 主从关系为一主多从时，只有当所有从节点被取消后，主节点才会取消掉主从模式。

SSL 连接管理

最近更新时间：2024-11-07 11:37:52

本文档介绍元数据 SSL 连接管理的使用和操作说明。

功能介绍

为了保障数据传输过程中的安全，CASB 支持为应用-代理、代理-数据库双向链路分别配置 TLS 加密，保护数据的完整性、机密性，防止中间人劫持数据。

支持类型		详情
元数据类型		• MySQL • PostgreSQL
TLS 版本		• TLS1.0 • TLS1.1 • TLS1.2 • TLS1.3
TLS 加密算法		• TLS_RSA_WITH_AES_128_CBC_SHA • TLS_RSA_WITH_AES_256_CBC_SHA • TLS_RSA_WITH_AES_128_GCM_SHA256 • TLS_RSA_WITH_AES_256_GCM_SHA384 • TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384 • TLS_CHACHA20_POLY1305_SHA256 • TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA • TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 • TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
CASB 代理的 SSL 模式	MySQL	• DISABLED • PREFERRED • REQUIRED • VERIFY_CA
	PostgreSQL	• disable • allow • prefer • require • verify-ca

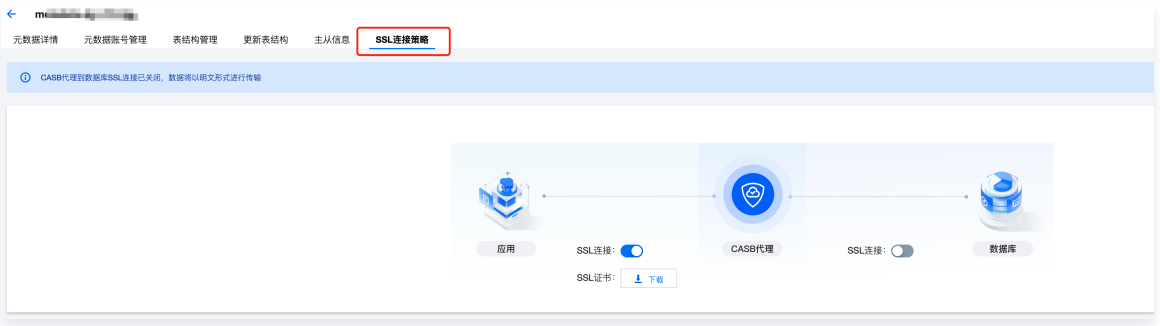
操作配置

步骤1：进入 SSL 连接策略配置页面

1. 登录 控制台，单击元数据管理菜单下的**关系型元数据**。

2. 找到需要操作的元数据，单击元数据右侧的**管理**。

3. 选择 SSL 连接策略标签，即可进入 SSL 连接配置页。本配置页可以设置应用-代理、代理-数据库的双向 SSL 连接功能。



步骤2：SSL 策略配置

1. 应用-CASB 代理。
   - 关闭 SSL 连接开关后，CASB 代理不启用 SSL 连接功能支持，应用无法通过 SSL 连接到代理。
   - 开启 SSL 连接开关后，CASB 代理启用 SSL 连接功能支持，应用可使用 SSL 连接到代理。
   - 开启 SSL 连接开关后，可以下载 SSL 证书，以供应用验证 CASB 代理的身份。
2. CASB 代理-数据库。
   - 关闭 SSL 连接开关后，CASB 代理不使用 SSL 连接数据库，传输过程中数据包明文传输。
   - 开启 SSL 连接开关后，代理将使用 SSL 连接访问数据库，传输过程中数据包加密传输。请确认数据库已开启 SSL 连接支持，否则会导致代理访问数据库失败。

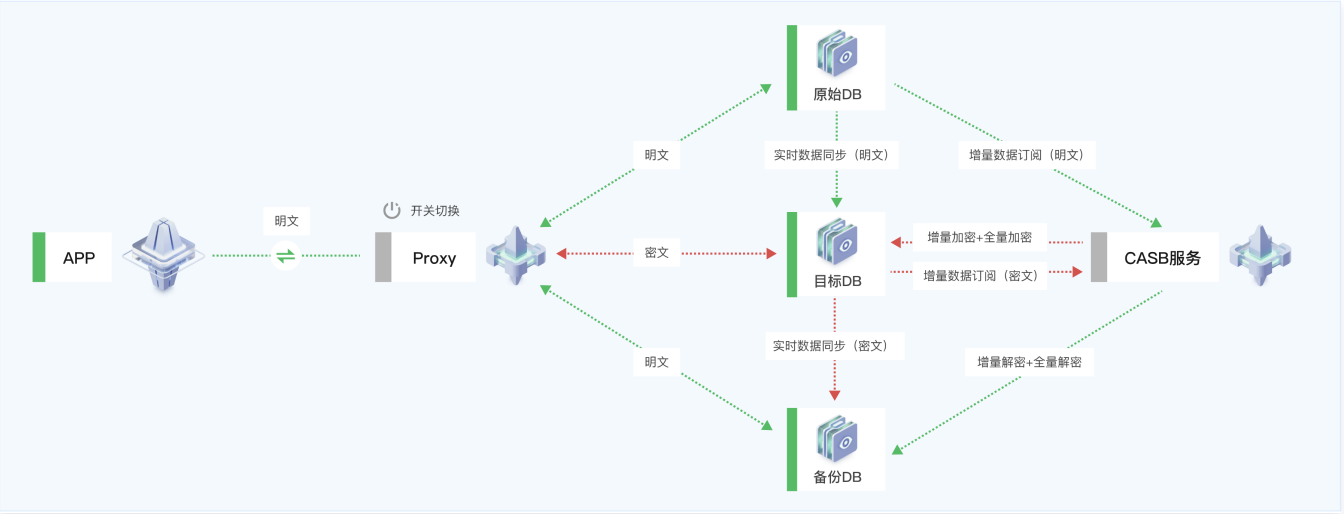
版权所有：腾讯云计算（北京）有限责任公司

接入与备份
概述

最近更新时间：2024-06-13 19:14:31

数据安全网关（云访问安全代理，CASB）以少开发改造为目的，帮助用户快速解决数据加密、脱敏、访问控制等数据安全痛点问题。
为了满足业务平滑地从数据库切换到 CASB、CASB 回切到数据库、增减加密字段、明文数据备份等应用场景，CASB 以实时、不停服、平滑接入为核心思想，为业务提供在线迁移、平滑接入、实时解密备份的技术能力。通过接入和备份方案，可以减少业务接入过程中明密文共存时间，同时为业务提供快速回退能力。

基本概念和原理



在 CASB 接入和备份过程中，共存在三种角色的元数据：原始元数据（原始 DB）、目标元数据（目标 DB）和备份元数据（备份 DB），三种角色的元数据无需全部存在，可根据业务需求接入特定角色的元数据。

- **原始元数据：**计划新增加密字段的元数据。如业务首次接入时未配置加密策略的数据库、已配置了加密策略需额外新增加密字段的数据库。
- **目标元数据：**新增加密字段后的元数据或计划减少加密字段的元数据。
- **备份元数据：**减少加密字段后的元数据。如未配置任何加密字段的数据库，作为备份或回退的明文数据库。

加密策略包含关系：**原始元数据**真包含于**目标元数据**，**备份元数据**真包含于**目标元数据**。

同步原理

1. 业务侧使用 binlog 或 **数据传输服务（DTS）**配置不同角色数据库之间的数据同步，保证数据库中的数据一致。
   - 目标 DB 实时同步原始 DB 的数据。
   - 备份 DB 实时同步目标 DB 的数据。
2. 配置并启动 CASB 接入和备份服务，CASB 会订阅原始 DB 和目标 DB 的增量数据。
   - 目标 DB 增加的加密字段：
     - CASB 后台对存量数据进行全量加密。
     - CASB 后台对同步后的增量数据进行实时加密。
   - 备份 DB 中减少的加密字段：
     - CASB 后台对存量数据进行全量解密。
     - CASB 后台对同步后的增量数据进行实时解密。

> **注意：**
> - 数据同步方式为binlog时，延迟5秒加密/解密增量数据。
> - 数据同步方式为DTS时，延迟10秒加密/解密增量数据。
> - 请确保增量数据在5秒（binlog）或10秒（DTS）内完成同步，否则将不会实时加密、解密。

- 切换代理前，请检查数据加密情况，若仍存在明文数据，可使用全量加密工具再次进行全量加密。

典型接入过程示例

1. 准备三个数据库。
   - **原始 DB**：新接入的待加密数据库，存在 A、B、C 三个明文字段，其中 A、B 为敏感字段。
   - **目标 DB**：和原始 DB 的结构和数据完全一致，并配置使用 binlog、DTS 等工具实时从**原始 DB** 同步增量数据。
   - **备份 DB**：和目标 DB 的结构和数据完全一致，并配置使用 binlog、DTS 等工具实时从**目标 DB** 同步增量数据。
2. 将数据库添加到 CASB 元数据。
   - 原始 DB 添加为接入与备份任务的原始元数据。
   - 目标 DB 添加为接入与备份任务的目标元数据。
   - 备份 DB 添加为接入与备份任务的备份元数据。
3. 配置元数据的加解密策略。
   - 原始元数据为新接入的数据库，无加解密策略。
   - 目标元数据配置 A、B 敏感字段的加密策略。
   - 备份元数据不配置加解密策略，即保存明文。
4. 绑定代理和配置代理账号

   将原始元数据、目标元数据、备份元数据绑定同一个代理，并配置相同的代理账号和密码。代理的访问开关切换到原始 DB，即访问代理的流量转发到原始 DB。
5. 变更应用的访问地址

   应用由访问原始 DB 变更为访问代理，代理将自动转发到原始 DB。此时目标 DB、备份 DB 内的数据均为明文，并且和原始 DB 的数据完全一致。
6. 配置原始元数据到目标元数据的加密任务。
   - 配置目标 DB 的全量加密任务，任务执行后，目标 DB 字段 A 和字段 B 的存量数据将全部变更为密文。
   - 配置原始 DB 到目标 DB 的实时增量加密任务，CASB 会持续订阅原始 DB 的增量数据，并自动将目标 DB 字段 A 和字段 B 中同步增量的明文数据加密成密文。
7. 配置目标元数据到备份元数据的解密任务。
   - 由于步骤6对目标 DB 进行了数据加密，且备份 DB 在实时同步目标 DB 的数据，此时备份 DB 中的数据为密文。
   - 配置备份 DB 的全量解密任务，任务执行后，备份 DB 字段 A 和字段 B 的存量数据将全部变更为明文。
   - 配置目标 DB 到备份 DB 的实时增量解密密任务，任务会持续订阅目标 DB 的增量数据，并自动将备份 DB 字段 A 和字段 B 中同步的增量密文数据解密成明文。
8. 启动全量加解密和实时加解密任务。
9. 验证数据。验证原始 DB、目标 DB、备份 DB 数据的一致性，验证目标 DB 的数据是否已正常加密，验证备份 DB 的数据是否已正常解密。
10. 代理开关切换。代理开关切换过程中，业务使用的代理地址信息无需变更。
    - 将代理开关切到目标元数据。切换后所有请求转发到目标 DB，目标 DB 中的所有数据均为密文。
    - 将代理开关切换到备份元数据。切换后所有请求转发到备份 DB，备份 DB 中的所有数据均为明文。
11. 接入过程中，若存在任何异常，业务可以通过将数据源地址配置成备份 DB，实现快速的业务回退。

通过接入不同的元数据角色，业务侧只需提供多个数据同步的数据库，CASB 可以实现存量和增量数据的加解密、一键切换请求转发 DB 等操作，帮助业务实现数据库加解密的平滑接入和快速回退。

应用场景

不适用场景

以下场景新增/减少加密字段时可参考 从0接入 CASB 在现有元数据上直接变更，代理可以处理明文和密文共存的场景。

- 待加解密字段只有写操作。
- 待加解密字段不会作为查询条件。
- 数据量很小，全量加解密任务可在极短时间内完成。
- 业务可停机变更。

适用场景

- 新增/减少加密字段，待处理字段存在读操作，且字段会作为查询条件。
- 容灾备份数据库需保存明文。

使用限制

- 仅支持 **MySQL** 类型的元数据及使用 MySQL binlog 协议的数据库。
- 所有元数据的**库、表、字段**结构需保持**完全一致。**
- 已配置策略的表必须有**主键 ID。**
- 所有 DB 的 server-id 不能相同。
- 实时加密、实时解密会额外占用5~50个数据库连接，请确认目标 DB、备份 DB 的连接数限制。
- 原始 DB 和目标 DB 必须开启 binlog，且需满足：
  - binlog_format 设置为 ROW。
  - binlog_row_image 设置为 FULL。
- 实时加密性能和资源占用参考。请评估资源消耗对数据库的影响，若需更高性能，请 联系我们 。
  - 4C8G及以上数据库：支持不小于2000 QPS 的字段写操作的同步加密。
  - 4C8G数据库可能占用最高约70%的 CPU。
  - 8C16G数据库可能占用最高约40%的 CPU。

新建接入与备份任务

最近更新时间：2024-11-07 11:37:52

前提条件

1. 已 购买开通 CASB 实例 。
2. 已了解接入与备份 基本原理和使用限制 。
3. 已配置不同角色元数据间的数据同步并处于正常运行中。

步骤1：接入准备

1. 登录 控制台 ，单击元数据菜单下的**接入与备份**。
2. 在接入与备份页面，选择所需地域与实例，单击**开始接入**。

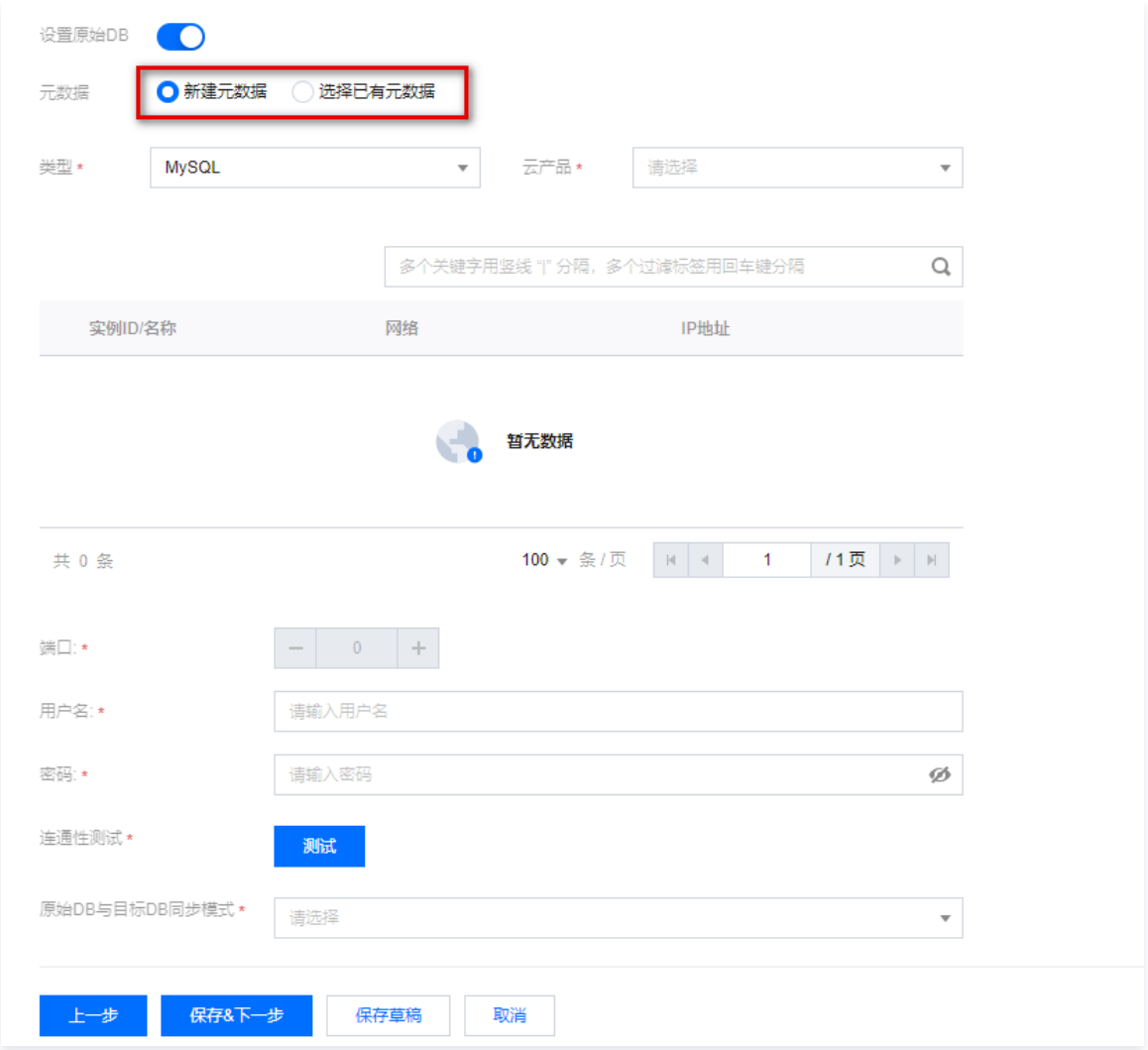
3. 在接入准备页面，输入接入名称（120个字符内），检查并确认待勾选的配置项，单击**保存下一步**。

步骤2：设置原始 DB

1. 在设置原始 DB 页面，单击**开启设置原始 DB 开关**。

> **说明：**
> 若无需增加加密字段，可跳过此项配置，即跳过原始 DB 到目标 DB 的同步加密过程。

2. 开启后，选择**新建元数据**或**选择已有元数据**，配置相关参数。



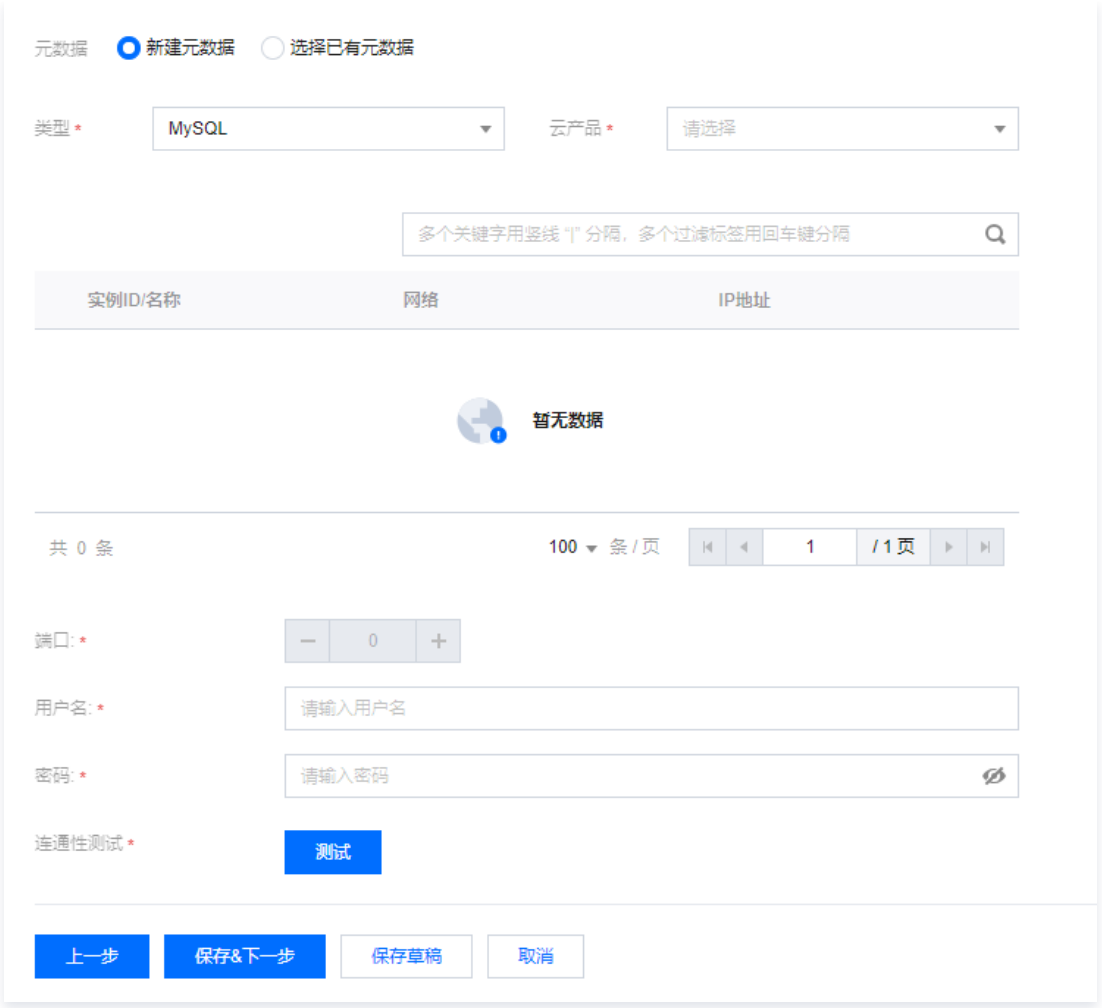
参数名称	参数说明
元数据	• 新增元数据：参考 新建元数据 配置选项，单击**保存&下一步**后，会自动保存并使用此新建的元数据。 • 选择已有元数据：从元数据列表中选择已有的元数据及相应的元数据账号。
原始 DB 与目标 DB 同步模式	支持选择 binlog、DTS-数据同步、DTS-数据迁移三种同步模式。 • binlog 模式：请确保 binlog 同步的状态为 running，binlog_format 为 ROW，binlog_row_image 为 FULL。 • DTS-数据同步：从列表中选择已配置的 DTS 数据同步任务。 • DTS-数据迁移：从列表中选择已配置的 DTS 数据迁移任务。

3. 勾选确认选项，单击**保存&下一步**，保存已配置的原始元数据和同步模式信息。

> ⚠ **注意：**
> • 请确保原始 DB 到目标 DB 的同步任务处于正常运行中的状态。
> • 若目标 DB 同时作为备份 DB 的 Source 和原始 DB 的 Replica，且使用 binlog 同步数据，请开启 log_replica_updates 或 log_slave_updates 配置。

步骤3：配置目标 DB

1. 在设置目标 DB，选择**新建元数据**或**选择已有元数据**，配置目标 DB 的元数据和元数据账号信息。



参数名称	参数说明
元数据	• 新增元数据：参考 新建元数据 配置选项，单击**保存&下一步**后，会自动保存并使用此新建的元数据。 • 选择已有元数据：从元数据列表中选择已有的元数据及相应的元数据账号。

2. 单击**保存&下一步**，保存已配置的目标元数据信息。

步骤4：配置备份 DB

> **说明：**
> 若无需减少加密字段，可跳过此项配置，即跳过目标 DB 到备份 DB 的同步解密过程。

1. 在设置备份 DB 页面，单击**开启设置备份 DB 开关**。
2. 开启后，选择**新建元数据**或**选择已有元数据**，配置相关参数。

参数名称	参数说明
元数据	• 新增元数据：参考 新建元数据 配置选项，单击**保存&下一步**后，会自动保存并使用此新建的元数据。 • 选择已有元数据：从元数据列表中选择已有的元数据及相应的元数据账号。
原始 DB 与目标 DB 同步模式	支持选择 binlog、DTS-数据同步、DTS-数据迁移三种同步模式。 • binlog 模式：请确保 binlog 同步的状态为 running，binlog_format 为 ROW，binlog_row_image 为 FULL。 • DTS-数据同步：从列表中选择已配置的 DTS 数据同步任务。 • DTS-数据迁移：从列表中选择已配置的 DTS 数据迁移任务。

3. 勾选确认选项，单击**保存&下一步**，保存已配置的备份元数据和同步模式信息。

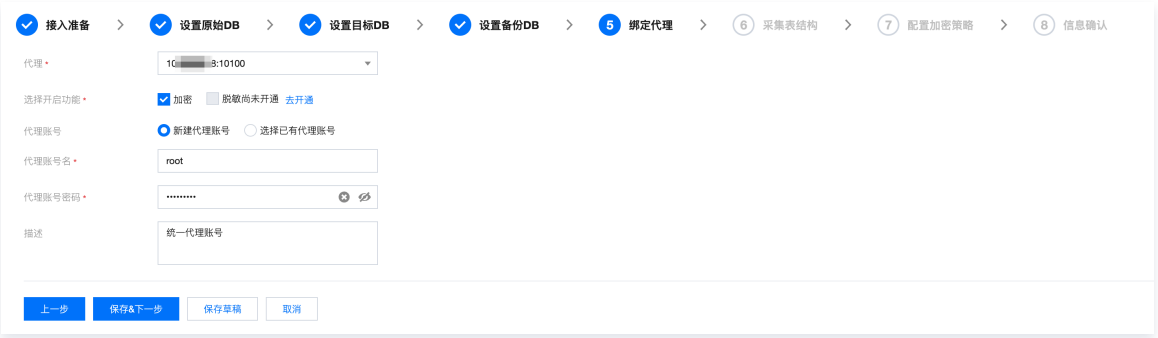
> **注意：**
> 请确保目标 DB 到备份 DB 的同步任务处于正常运行中的状态。

步骤5：配置代理

1. 在绑定代理页面，选择需要绑定的代理，为此代理需要开启的功能。

> **说明：**

- 多个元数据绑定同一个代理时，业务需为每个 DB 配置相同的代理账号及代理密码，且代理账号绑定的元数据账号权限需相同，避免代理切换转发 DB 时无法正常访问切换后的 DB。
- 代理地址默认转发到原始 DB、目标 DB、备份 DB 中第一个有效的 DB。



2. 配置代理账号，支持新建所有元数据的公共代理账号或从已有的代理账号列表中选择。
   - 新建代理账号：设置代理账号、密码和描述信息，CASB 会自动为所有元数据创建相同的代理账号和密码。若部分元数据已存在同名的账号，则不允许创建。
   - 选择已有代理账号：从列表中选择所有元数据都存在的、账号密码均相同的代理账号。
3. 单击**保存&下一步**，保存已配置的代理信息。

步骤6：采集表结构

1. 在绑定代理页面，参考 元数据表结构管理，采集和更新各个元数据的表结构信息。若元数据表结构未采集完成，需等待采集完成才能进行下一步。

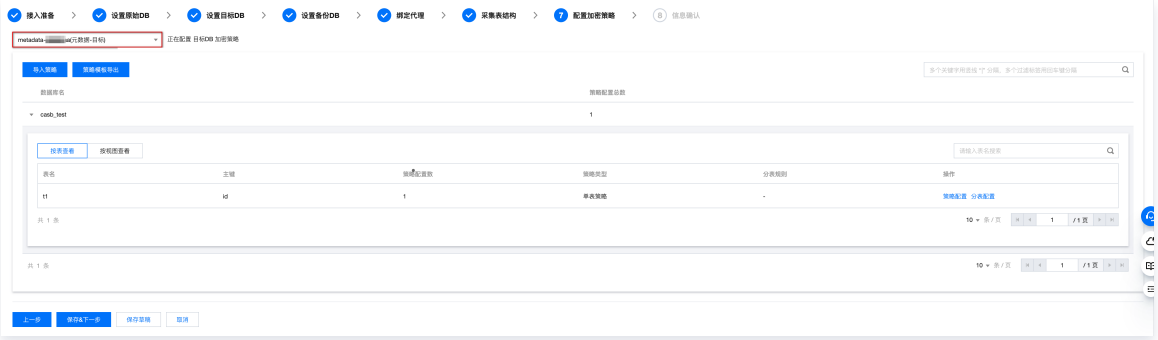
> **注意：**
> 需保证所有元数据的表结构完全一致。

2. 单击**保存&下一步**，保存已配置的采集表结构。

步骤7：配置加密策略

1. 在配置加密策略页面，选择元数据，参考 策略管理，配置相应元数据的加密策略。

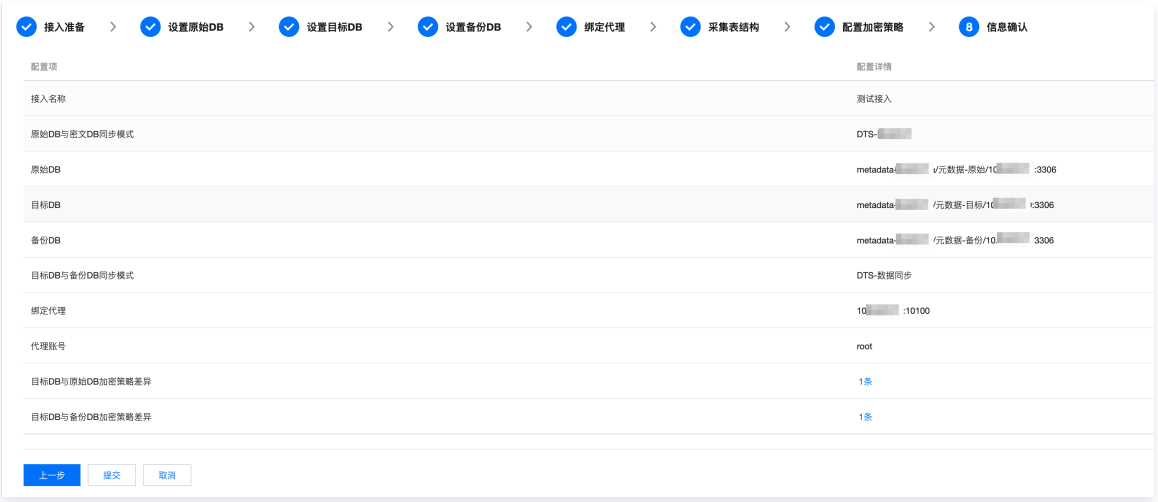
> **注意：**
> 原始元数据的加密字段需真包含于目标元数据的加密字段，备份元数据的加密字段需真包含于目标元数据的加密字段。



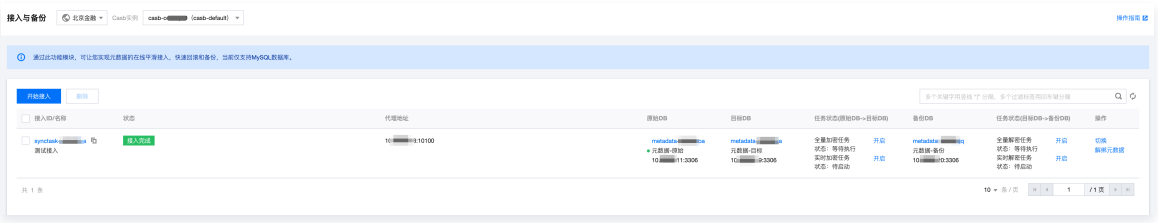
2. 单击**保存&下一步**，完成配置加密策略。

步骤8：信息确认

1. 在信息确认页面，确认此任务的各项配置信息。



2. 确认无误后，单击**提交**，完成任务配置。
3. 返回接入列表页后，即可查询此接入任务信息。



管理任务元数据

最近更新时间：2024-06-13 19:14:31

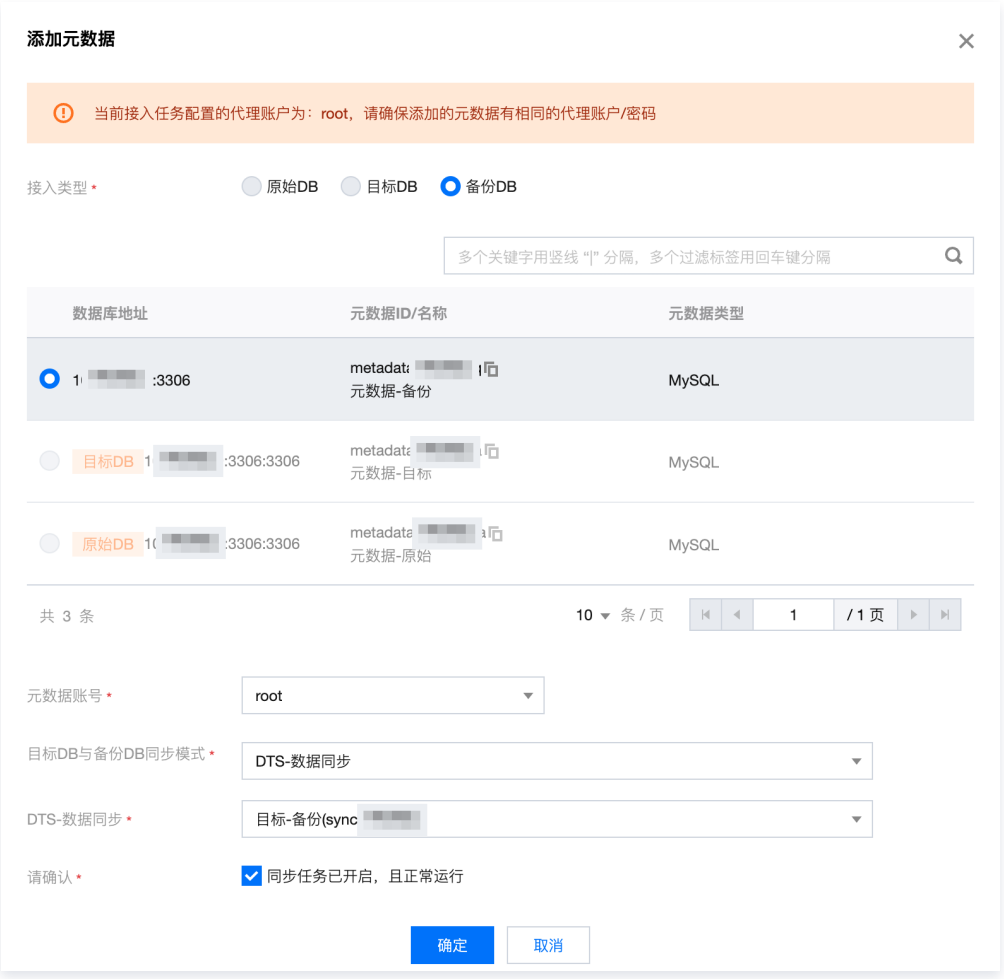
创建接入与备份任务后，您可以在接入与备份任务列表中添加和删除不同角色的元数据。

添加元数据

1. 登录 控制台，单击元数据菜单下的**接入与备份**。
2. 在接入与备份页面，选择所需地域与实例，单击待操作任务的操作选项下的**添加元数据**选项。

3. 在添加元数据窗口中，选择接入类型、元数据和元数据账号。

> **注意：**
> - 若接入类型为原始 DB，参考 新建接入任务-配置原始 DB 配置 选项说明，需额外设置原始 DB 到目标 DB 的同步模式和同步任务信息。
> - 若接入类型为备份 DB，参考 新建接入任务-配置原始 DB 配置 选项说明，需额外设置目标 DB 到备份 DB 的同步模式和同步任务信息。



4. 单击**确定**，任务相关信息校验通过后，即可添加相应接入类型的元数据。

解绑元数据

1. 在接入与备份页面，单击待操作任务的操作选项下的**解绑元数据**选项。

2. 在弹出的选项中，选择需要解绑的元数据类型。

3. 单击**确定**，任务相关信息校验通过后，即可添加相应接入类型的元数据。

> **说明：**
> - 若接入任务中的全量加密任务或实时加密任务正在运行中，不允许解绑原始 DB 和目标 DB。
> - 若接入任务中的全量解密任务或实时解密任务正在运行中，不允许解绑目标 DB 和备份 DB。
> - 不允许解绑正在转发中（接入任务列表中元数据地址前的绿色圆点标记）的元数据，除非此元数据为任务中唯一的元数据。
> - 解绑接入与备份任务中的最后一个元数据后，接入任务将自动删除。

切换代理转发的元数据

> **注意：**
> 切换转发的元数据前，请确认切换前后的元数据数据已同步完成，避免数据不一致造成损失。

根据当前代理的转发状态，支持切换代理转发到不同类型的元数据。

1. 在接入与备份页面，单击待操作任务的操作选项下的**切换**选项。

2. 根据代理转发的 DB 类型，可以支持如下切换：
   - 当前代理转发为原始 DB 时，支持切换代理转发到目标 DB。

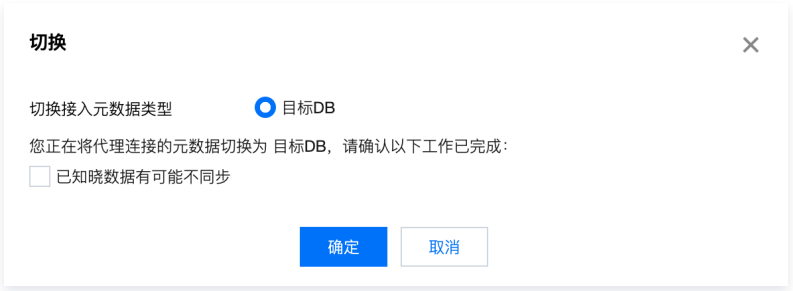
> **注意：**
> 切换到目标 DB 后，请停止业务配置的 binlog/DTS 数据同步服务，避免目标 DB 数据被覆盖。

- 当前代理转发为目标 DB 时，支持切换代理转发到原始 DB 或备份 DB。

> **注意：**
> - 因目标 DB 到原始 DB 无数据同步，原始 DB 可能不包含目标 DB 的最新数据，请确认业务无影响后操作。
> - 切换到备份 DB 后，请停止业务配置的 binlog/DTS 数据同步服务，避免备份 DB 数据被覆盖。

- 当前代理转发为备份 DB 时，支持切换代理转发到目标 DB。

> **注意：**
> 因备份 DB 到目标 DB 无数据同步，目标 DB 可能不包含备份 DB 的最新数据，请确认业务无影响后操作。



3. 确认内容无误后，单击**确定**。

管理加解密任务

最近更新时间：2024-11-08 21:33:12

创建接入与备份任务后，可以在接入和备份任务列表中开启、关闭、查看不同元数据间的全量加解密任务和实时加解密任务。

管理全量加密任务

1. 登录 控制台，单击元数据菜单下的**接入与备份**。
2. 在接入与备份页面，选择所需全量加密任务，支持对该任务进行如下操作：
   - **开启全量加密任务**：单击**任务状态(原始DB->目标DB)** 操作栏下**全量加密任务**后的**开启** > **确定**。

     说明：
     - 仅同时配置了**原始DB** 和**目标DB** 时才会展示开启按钮。
     - CASB 会自动分析**目标DB** 和**原始DB** 的策略差异，并为新增的加密字段自动创建全量加密任务。

   - **查看全量加密任务状态**：任务执行完成后，任务状态变成执行成功或执行失败，单击 可查看详细的执行状态和结果信息。
   - **关闭全量加密任务**：单击**任务状态(原始DB->目标DB)** 操作栏下全量加密任务后的**关闭**，可以停止运行中的全量加密任务。

管理全量解密任务

1. 登录 控制台，单击元数据菜单下的**接入与备份**。
2. 在接入与备份页面，选择所需全量解密任务，支持对该任务进行如下操作：
   - **开启全量解密任务**：单击**任务状态(目标DB->备份DB)** 操作栏下的全量解密后的**开启** > **确定**。

     说明：
     - 仅同时配置了**目标 DB** 和**备份 DB** 时才会展示开启按钮。
     - CASB 会自动分析**备份 DB** 和**目标 DB** 的策略差异，并为备份 DB 内减少的加密字段自动创建全量解密任务。

   - **查看全量解密任务状态**：任务执行完成后，任务状态变成执行成功或执行失败，单击 可查看详细的执行状态和结果信息。
   - **关闭全量解密任务**：单击**任务状态(目标DB->备份DB)** 操作栏下全量加密任务后的**关闭**，可以停止运行中的全量解密任务。

管理实时加密任务

1. 登录 控制台，单击元数据菜单下的**接入与备份**。
2. 在接入与备份页面，选择所需实时加密任务，支持对该任务进行如下操作：
   - **开启实时加密任务**：单击**任务状态(原始DB->目标DB)** 操作栏下实时加密任务后的**开启 > 确定**。

     > **说明：**
     > - 仅同时配置了**原始 DB** 和**目标 DB** 时才会展示开启按钮。
     > - CASB会自动分析**目标 DB** 和**原始 DB** 的策略差异，并自动加密**目标 DB** 从**原始 DB** 同步到的增量数据。

   - **查看实时加密任务状态**：开启实时加密任务后，任务状态变为初始化中，初始化完成后，手动停止任务之前，任务状态始终为运行中状态。若任务运行失败，单击 可查看详细的执行状态和结果信息。
   - **关闭实时加密任务**：单击**任务状态(原始DB->目标DB)**操作栏下实时加密任务后的**关闭**，可以停止运行中的实时加密任务。

管理实时解密任务

1. 登录 控制台，单击元数据菜单下的**接入与备份**。
2. 在接入与备份页面，选择所需实时解密任务，支持对该任务进行如下操作：
   - **开启全量实时任务**：单击**任务状态(目标DB->备份DB)** 操作栏下实时解密任务后的**开启 > 确定**。

     > **说明：**
     > - 仅同时配置了**目标 DB** 和**备份 DB** 时才会展示开启按钮。
     > - CASB 会自动分析**目标 DB** 和**备份 DB** 的策略差异，并自动解密**备份 DB** 从**目标 DB** 同步到的增量数据。

   - **全量解密任务状态查看**：开启实时解密任务后，任务状态变为初始化中，初始化完成后，手动停止任务之前，任务状态始终为运行中状态。若任务运行失败，单击 可查看详细的执行状态和结果信息。
   - **关闭实时解密任务**：单击**任务状态(目标DB->备份DB)**操作栏下实时加密任务后的**关闭**，可以停止运行中的实时解密任务。

常见错误状态

全量加解密

参考 任务结果错误码 。

实时加解密

错误信息	错误原因
invalid metadata or metadata user	任务绑定的元数据或元数据账号失效

unsupported task replica type	业务配置的 DB 间实时同步任务失效
master InitMySQLConn	连接主元数据失败
slave InitMySQLConn	连接从元数据失败
invalid log_bin	binlog 未开启
invalid binlog_format	binlog_format不为 ROW
invalid binlog_row_image	binlog_row_image不为 FULL

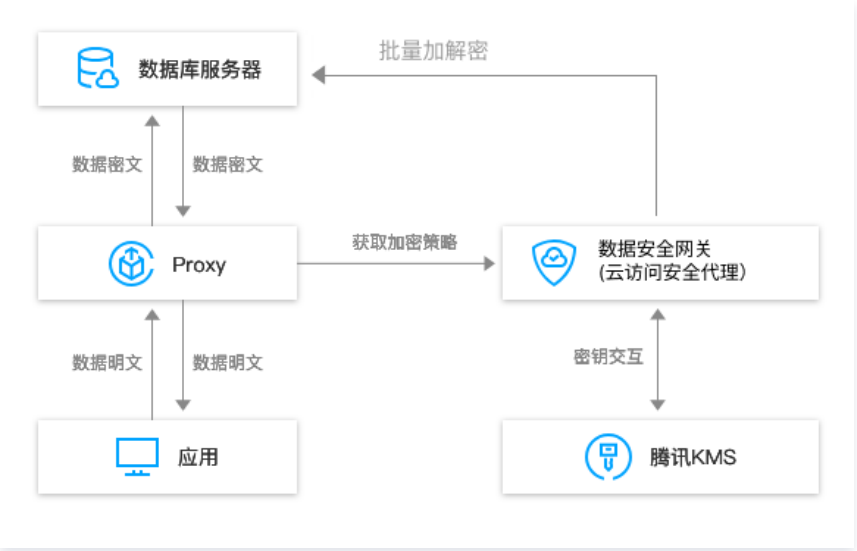
数据加密
概述

最近更新时间：2024-06-13 19:14:31

背景信息

数据安全网关（云访问安全代理）（Data Security Gateway（Cloud Access Security Broker），CASB）管理系统以少改造的方式，实现云环境下应用中结构化数据（包括实时数据和历史数据）的存储加密，提供多种加解密策略，为公有云提供方便快捷易于部署的数据安全解决方案。用户可以根据数据库字段配置策略。策略工作模式有三种，分别是读写加密、读解密写不加密、读不解密写不加密。

拓扑结构



系统组成

CASB 管理系统由 CASB Proxy、数据安全网关（云访问安全代理）平台组成。

- CASB Proxy：提供数据库协议代理及高性能数据加解密运算集群服务。
- 数据安全网关（云访问安全代理）平台：提供可视化的管理控制台，提供策略管理、全量加解密和工作密钥功能。

策略管理
创建策略

最近更新时间：2024-11-13 09:44:52

本文将介绍如何创建加密策略。

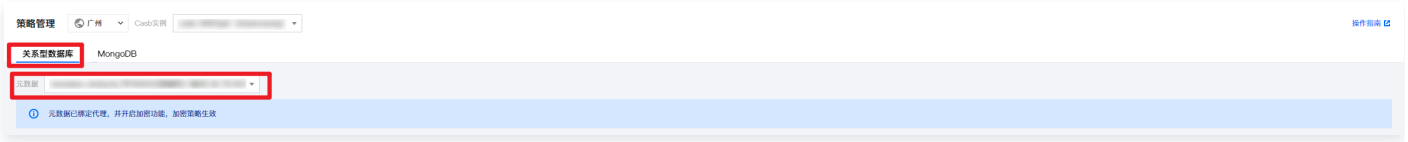
前提条件

- 已 购买开通 CASB 实例 。
- 已创建元数据。如未创建元数据，请查阅 添加云元数据 、 添加自建数据库 。

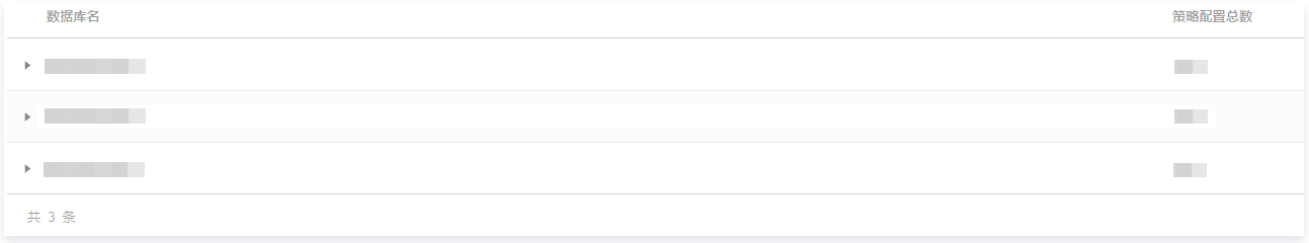
> **说明：**
> 当元数据为从节点时，策略会自动同步主节点，无需创建。

关系型数据库

1. 登录 控制台 ，在左侧导航栏中，单击**数据加密 > 策略管理**。
2. 在策略管理页面，选择所需的地域、CASB 实例。
3. 在关系型数据库页面，选择需要创建加密策略的元数据。



4. 在策略管理页面，将会展示所选的实例与元数据对应的数据库名和策略总数。



5. 在策略管理页面中，单击**数据库名**，将会展示该数据库下数据表的详情。

> **说明：**
> 选择数据表后，当其对应策略类型是主分表或次分表时，配置的加解密策略会同步到其他分表。

6. 找到所需配置的数据表，在其右侧操作栏中，单击**策略配置**。

7. 在配置页面中，找到所需的字段，在其右侧单击**配置策略**。
8. 在配置策略窗口中，配置所需参数，单击**确定**，即可完成策略的创建。

参数说明：

- **全量加解密：**支持开启、关闭或仿真测试（旁路实时模拟策略执行，支持批量加密任务模拟执行策略，可在正式启用前充分验证策略）。
- **加密算法：**目前支持国密 SM4 和 AES 算法。
- **模糊查询：**目前适用于 utf8mb3和 utf8mb4两种不同字符集数据的密文模糊检索算法。为支持模糊查询，密文需要存储额外的索引信息，会一定程度降低密文的安全性，请根据业务需求评估选择。
- **适用于 utf8mb3字符集的模糊查询：**仅支持加密和模糊查询 utf8mb3字符集（即1~3字节的 utf8字符）的字符串，密文长度将额外增加原始明文长度的7倍。
- **适用于 utf8mb4字符集的模糊查询：**支持加密和模糊查询 utf8mb4字符集（即所有 utf8字符）的字符串，密文长度将额外增加原始明文长度的21倍。
- **加密密钥：**根据步骤2选择的元数据，系统会自动拉取对应的密钥，供您选择。如未创建加密密钥，请参见 创建密钥 。

> **注意：**
> 配置了模糊查询策略的字段写入数据时，明文数据长度必须等于0（空）或大于等于 2，否则将写入失败。

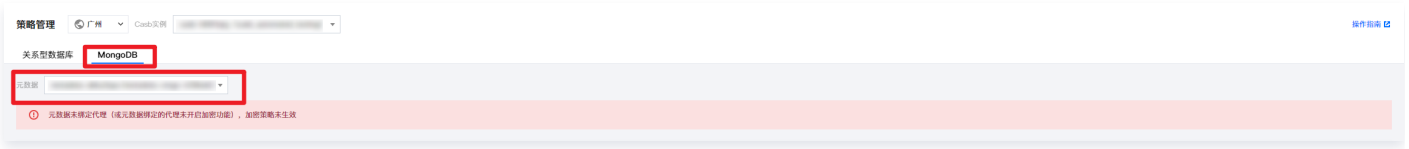
9. 如需还对其他表或字段设置策略，重复上述操作即可。（可选）

> **说明：**
> - 策略配置完成后，**实时加解密**状态将会开启，默认是关闭。
> - **工作模式：**模式共有三种。工作模式仅当使用 Proxy 连接进行实时加解密操作时有效。
>   - 读解密，写加密。
>   - 读解密，写不解密。
>   - 读不解密，写不加密。

MongoDB

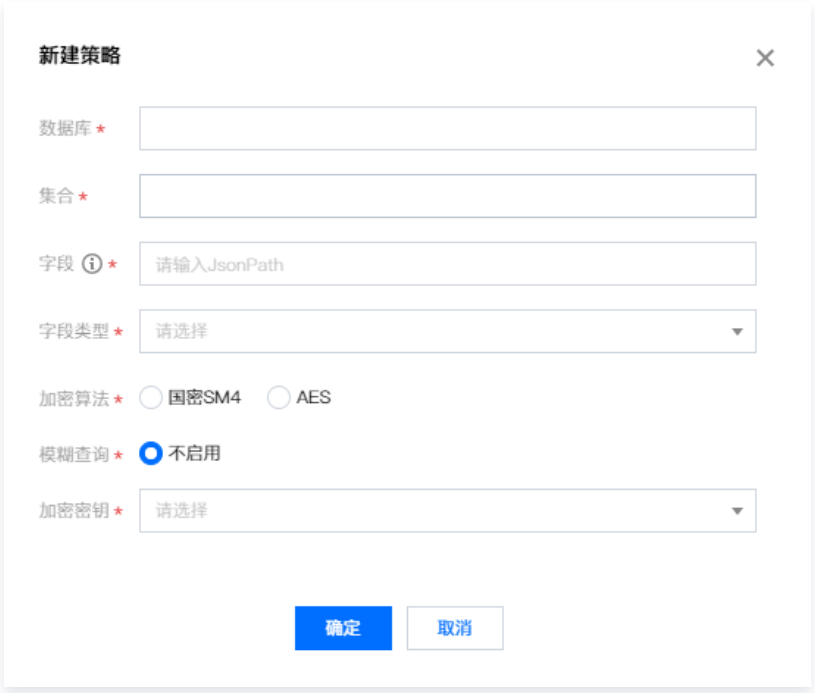
1. 登录 控制台，在左侧导航栏中，单击**数据加密** > **策略管理**。
2. 在策略管理页面，选择所需的地域、CASB 实例。

3. 单击 Tab 栏中的 **mongoDB**，选择需要创建加密策略的元数据。



4. 在策略管理页面，单击**新建策略**。

5. 在新建策略弹窗中，配置所需参数，单击**确定**，即可完成策略的创建。



参数说明：

- **数据库：**目标策略的具体数据库名称。
- **集合：**目标策略的具体集合名称。
- **字段：**目标策略的具体字段名称
- **字段类型：**目标策略的具体字段类型。
- **加密算法：**目前支持国密 SM4 和 AES 算法。
- **模糊查询：**目前适用于 utf8mb3和 utf8mb4两种不同字符集数据的密文模糊检索算法。为支持模糊查询，密文需要存储额外的索引信息，会一定程度降低密文的安全性，请根据业务需求评估选择。

> **说明：**
> 字段目前只支持$.test,$.test.sub,$.test[*].sub; 例如：{'info':{'name':'XXX', 'phone':'XXX'}} 需要对phone加密 $.info.phone。

分表配置与管理

最近更新时间：2024-11-13 09:44:52

本文将介绍如何进行分表配置与管理。

分表配置

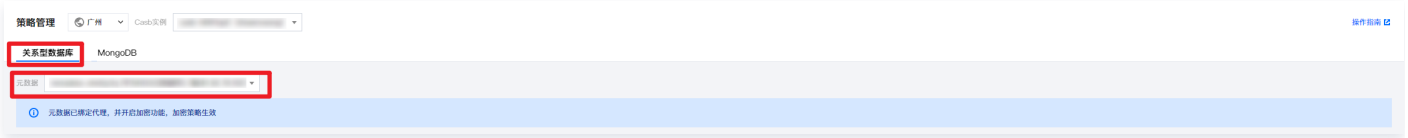
前提条件

- 已 购买开通 CASB 实例 。
- 已创建元数据。如未创建元数据，请查阅 添加云元数据 、添加自建数据库 。

> **说明：**
> 当元数据为从节点时，分表规则由主节点进行配置。

操作步骤

1. 登录 控制台，在左侧导航栏中，单击**数据加密 > 策略管理**。
2. 在策略管理页面，选择所需的地域、CASB 实例。
3. 单击 Tab 栏中的**关系型数据库**，选择需要创建加密策略的元数据。



4. 在策略管理页面中，找到所需设置的主分表表名，单击**分表配置**。

> **说明：**
> 当数据表已经配置策略，系统不支持再进行分表的配置。

5. 在规则配置页面，输入分表规则的正则表达式，用于匹配当前数据库的表名，单击**下一步**。

6. 在规则校验页面，当分表规则匹配成功后，将会输出各个数据表的匹配情况，包括匹配成功、无法匹配以及效验失败三种情况。单击**完成**即可创建分表规则。

参数说明：

- 匹配成功：表名与分表规则正则式能成功匹配。
- 无法匹配：表名与分表规则正则式无法匹配。
- 校验失败：包含如下三种情况，当数据表处于如下情况时，将会出现校验失败，与当前主表无法实现主分表配置。
  - 数据表已存在分表规则。
  - 数据表的表结构不相同。
  - 数据表已配置策略。

> **说明：**
> - 当规则校验存在**校验失败**的情况时，不支持分表的配置。
> - 数据表已配置加解密策略，并作为主分表的情况下，当分表策略配置完成后，主分表的加解密策略会同步至其他次分表。

分表管理

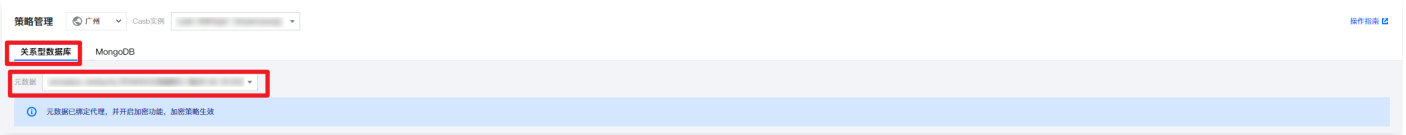
前提条件

- 已 购买开通 CASB 实例 。
- 已创建 CASB 实例。如未创建 CASB 实例，请查阅 创建 CASB 实例 。
- 已完成 分表配置 。

> **说明：**
> 当元数据为从节点时，分表规则由主节点进行配置、编辑。

操作步骤

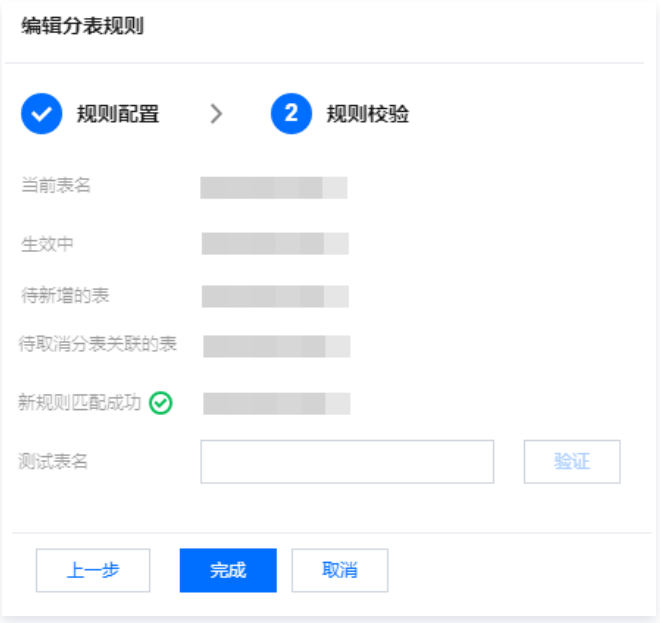
1. 登录 控制台 ，在左侧导航栏中，单击**数据加密** > **策略管理**。
2. 在策略管理页面，选择所需的地域、CASB 实例。
3. 单击 Tab 栏中的**关系型数据库**，选择需要创建加密策略的元数据。



4. 在策略管理页面，找到所需设置的主分表表名，单击**分表配置**。

5. 在规则配置页面，输入分表规则新的正则表达式，用于匹配当前数据库的表名，单击**下一步**。

6. 在规则校验页面，当分表规则匹配成功后，将会输出各个数据表的匹配情况，修改相关参数，单击**完成**即可修改分表规则。



参数说明：

- 匹配成功：表名与分表规则正则式能成功匹配。
- 无法匹配：表名与分表规则正则式无法匹配。
- 校验失败：包含如下三种情况，当数据表处于如下情况时，将会出现校验失败，与当前主分表无法实现分表配置。
  - 数据表已存在分表规则。
  - 数据表的表结构不相同。
  - 数据表已配置策略。
- 待新增的表：与原有分表规则相比，新规则中新增加的数据表。
- 待取消分表关联的表：设定新分表规则后，原有规则中的数据表没有匹配成功，会被取消关联。

说明：

- 当规则校验存在**校验失败**的情况时，不支持分表的配置。
- 数据表已配置加解密策略，并作为主分表的情况下，当分表策略配置完成后，主分表的加解密策略会同步至其他次分表。
- 数据表被取消分表关联后，原有配置的加解密策略会保留。
- 如需取消所有次分表的关联，在主分表的匹配规则中写入主分表名称即可完成。

导入策略

最近更新时间：2025-03-12 11:42:42

本文将介绍如何进行导入策略。

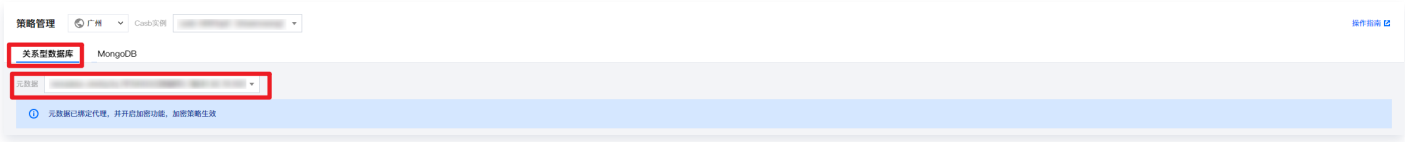
前提条件

- 已 购买开通 CASB 实例 。
- 已创建元数据。如未创建元数据，请查阅 添加云元数据 、添加自建数据库 。

> **说明：**
> 当元数据为从节点时，策略会自动同步主节点，无需创建。

操作步骤

1. 登录 控制台 ，在左侧导航栏中，单击**数据加密** > **策略管理**。
2. 在策略管理页面，选择所需的地域、CASB 实例。
3. 单击 Tab 栏中的**关系型数据库**，选择需要创建加密策略的元数据。



4. 在策略管理页面，单击**导入策略**。

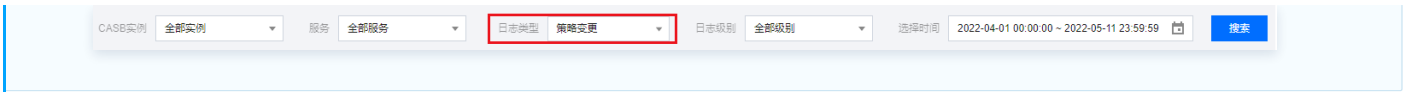
5. 在导入策略弹窗中，点击下载模板。

6. 本地完善好导入信息后，单击**选择文件**进行文件上传。上传完成后，单击**确定**即可。

> **注意：**
> - 上传的文件格式为 **CSV**，最大不超过10MB。
> - 文件内容包含：**数据库名、表名、字段名、加密算法、密钥编号、工作模式、实时加解密**，文件模板可在页面中单击**策略模板导出**进行下载。

7. 根据**策略导入**页面反馈确认是否上传成功，如上传失败，请根据提示进行修改调整。

> **说明：**
> - 如需查询策略导入的日志，了解整体的情况，可以直接前 **运维监控** > 监控日志 中进行查询。
> - 在监控日志页面，日志类型选择为**策略变更**，从而达到精准查询。


CASB实例
全部实例
服务
全部服务
日志类型
策略变更
日志级别
全部级别
选择时间
2022-04-01 00:00:00 ~ 2022-05-11 23:59:59
搜索

删除策略

最近更新时间：2024-11-13 09:44:52

本文将介绍如何进行删除策略。

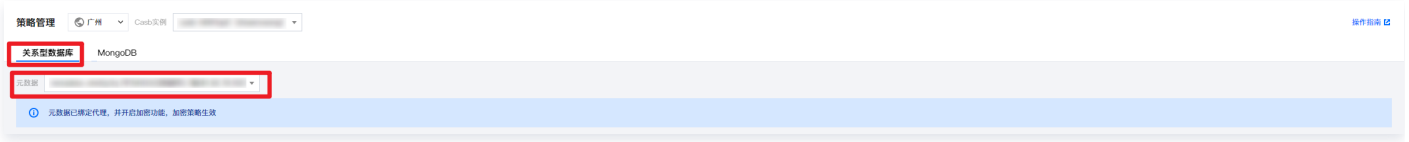
前提条件

- 已 购买开通 CASB 实例 。
- 已创建元数据。如未创建元数据，请查阅 添加云元数据 、添加自建数据库 。
- 已 创建策略 。

> **说明：**
> 当元数据为从节点时，策略从主节点同步，禁止编辑。

关系型数据库

1. 登录 控制台 ，在左侧导航栏中，单击**数据加密 > 策略管理**。
2. 在策略管理页面，选择所需的地域、CASB 实例。
3. 单击 Tab 栏中的**关系型数据库**，选择需要创建加密策略的元数据。



4. 在策略管理页面，将会展示所选的实例与元数据对应的数据库名和策略总数。

5. 在策略管理页面中，单击**数据库名**，将会展示该数据库下数据表的详情。

6. 找到所需配置的数据表，在其右侧操作栏中，单击**策略配置**。

7. 在配置页面，找到所需的字段，单击 关闭实时加解密后，单击**删除策略**。

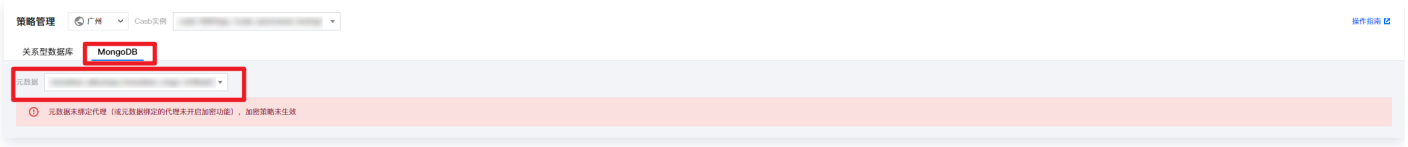
> **说明：**
> 选择数据表后，当其对应策略类型是主分表或次分表时，修改的加解密策略会同步到其他分表。

8. 在“确认删除”窗口中，单击**确定**，即可删除该策略。

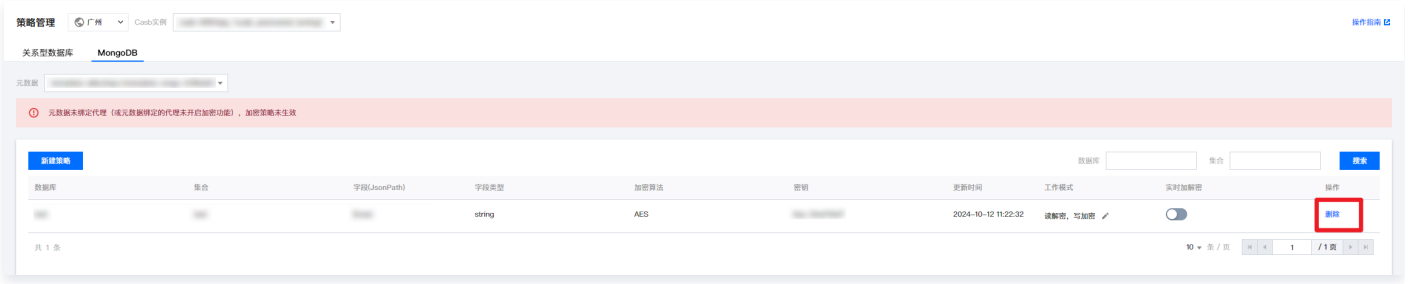
> **说明：**
> 策略删除后，当前字段数据将无法解密，请确认当前字段数据已全部解密。

MongoDB

1. 登录 控制台，在左侧导航栏中，单击**数据加密 > 策略管理**。
2. 在策略管理页面，选择所需的地域、CASB 实例。
3. 单击 Tab 栏中的 MongoDB，选择需要创建加密策略的元数据。



4. 在策略管理页面，选择需要删除的策略，单击操作栏中的**删除**。



5. 在“确认删除”窗口中，单击**确定**，即可删除该策略。

> **说明：**
> 策略删除后，当前字段数据将无法解密，请确认当前字段数据已全部解密。

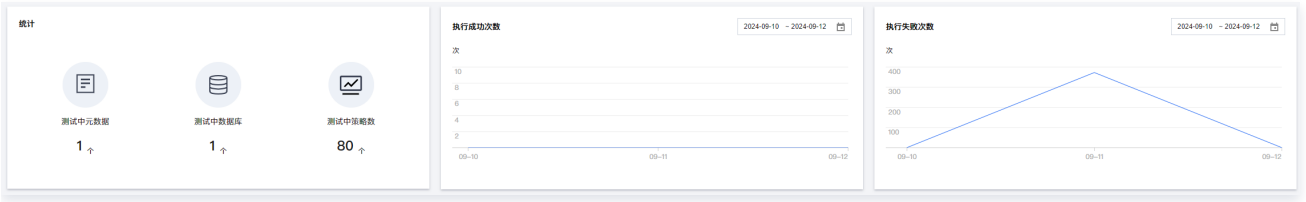
仿真记录

最近更新时间：2024-09-27 16:32:41

本文档介绍仿真记录的使用和操作说明。

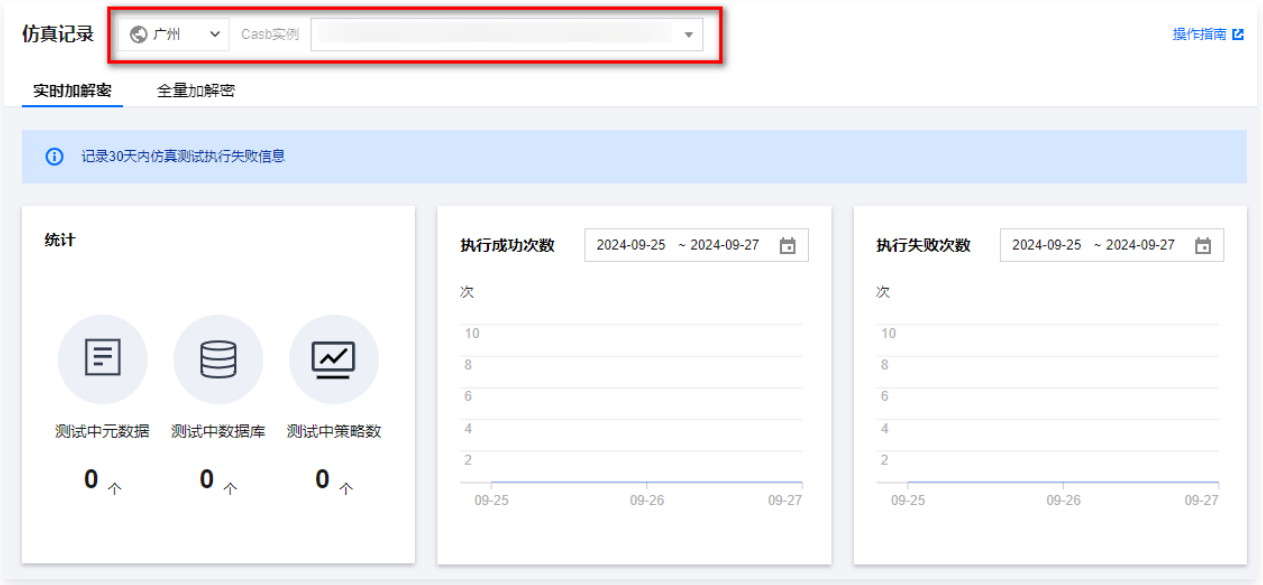
实时加解密仿真记录

实时加解密仿真测试记录，可记录当前测试中的元数据、数据库以及策略数量。同时，展示执行成功和失败的次数趋势，按天进行统计且统计数实时更新。此外，还能提供失败详情，展示 30 天内的失败记录清单，方便用户及时了解加解密过程中的情况，以便进行问题排查和优化策略配置。

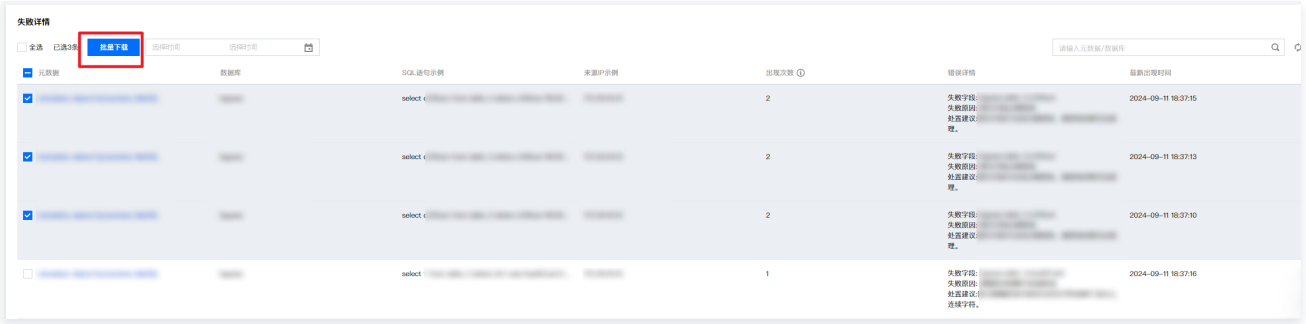


下载仿真失败记录

1. 登录 控制台，在左侧菜单栏中，单击**数据加密 > 仿真记录**。
2. 在实时加解密页面，选择所需的地域、CASB 实例和元数据。



3. 在实时加解密仿真记录页面，选择失败的仿真测试记录，单击**批量下载**即可。



> **注意：**
> 最多可下载2000条仿真失败记录。

全量加解密仿真记录

1. 登录 控制台，在左侧菜单栏中，单击**数据加密 > 仿真记录**。

2. 在仿真记录页面，选择所需的地域、CASB 实例和元数据。

3. 在仿真记录页面，单击 TAB 栏中的**全量加解密**。
4. 在全量加解密页面，您可查看任务类型为测试加密任务的全量加解密任务的任务，任务列表中呈现任务对应的数据库、任务进度和任务状态等信息。同时，支持对相关任务进行查看任务详情、关闭 / 执行任务以及删除任务等操作。

查看任务详情

1. 在全量加解密仿真记录页面，找到所需的任务，单击**详情**。

2. 在任务详情页面，即可查看对应的元数据的任务基本信息、数据来源、任务执行的类型、周期执行任务可以查看首次执行时间以及任务下次执行时间；增量任务可以查看任务执行的增量依据以及对应的增量依据字段，任务执行状态和表名字段。

管理任务

在全量加解密页面，选择目标任务，支持执行、关闭或删除该任务。

- 单个：选择目标任务，单击操作列的**执行/关闭/删除**，即可执行、关闭或删除该任务。
- 批量：勾选一个或多个任务，单击**批量执行/批量关闭/批量删除**，即可执行、关闭或删除该任务。

任务管理

最近更新时间：2024-11-13 17:30:51

本文档主要介绍数据加密、数据解密、数据修复、明文统计、测试加密任务的使用和操作说明。

功能介绍

任务类型	使用场景	说明	任务执行方式
数据加密任务	存量数据存在明文	对明文数据进行加密，生成密文数据，并保存。	手动/周期执行
数据解密任务	存量数据存在密文	对存量密文数据解密,生成明文数据，并保存。	手动/周期执行
数据修复任务	字段设置的策略无法解密存量密文数据	使用历史策略解密数据，使用当前策略进行加密,生成密文数据，并保存。	手动/周期执行
明文统计任务	统计存量数据明文记录数量	统计配置策略字段中明文数量。	手动/周期执行
测试加密任务	验证加密策略的可用性，确保数据安全策略的有效性和可靠性。	对数据库数据仿真执行加密策略，以充分验证策略可用性，但并不实际加密数据库中数据，可在仿真记录查看测试结果。	手动/周期执行

说明：
测试加密任务目前仅支持 MySQL 元数据。

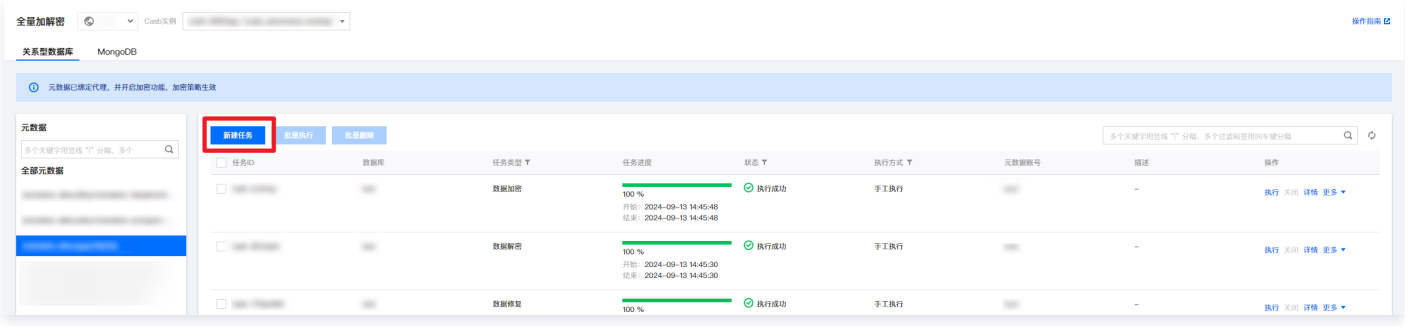
创建任务

前提条件

- 已 购买开通 CASB 实例 。
- 已创建元数据。如未创建元数据，请查阅添加云元数据 、添加自建数据库 。

操作步骤

1. 登录 控制台 ，在左侧导航栏中，单击**数据加密 > 全量加解密**。
2. 在全量加解密页面，选择所需的地域、CASB 实例和元数据。
3. 在全量加解密页面，单击**新建任务**，进入新建任务页面。



4. 在新建任务页面，配置任务基本信息。

参数名称	参数说明	备注
任务类型	数据加密任务/数据解密任务/数据修复任务/明文统计任务/测试加密任务	任务类型说明
数据范围	全量/增量	–
执行方式	• 手工执行：手工执行是指管理员在创建任务后，需通过手动操作来触发任务。 • 周期执行：周期执行是指按照预设的时间计划自动进行加解密操作，无需人工干预。	–
首次执行时间	默认为当前时间30分钟后；可选区间为30天内。	–
任务执行间隔	任务的执行频次；最小单位为1小时，最大可指定168小时，即7天。	–

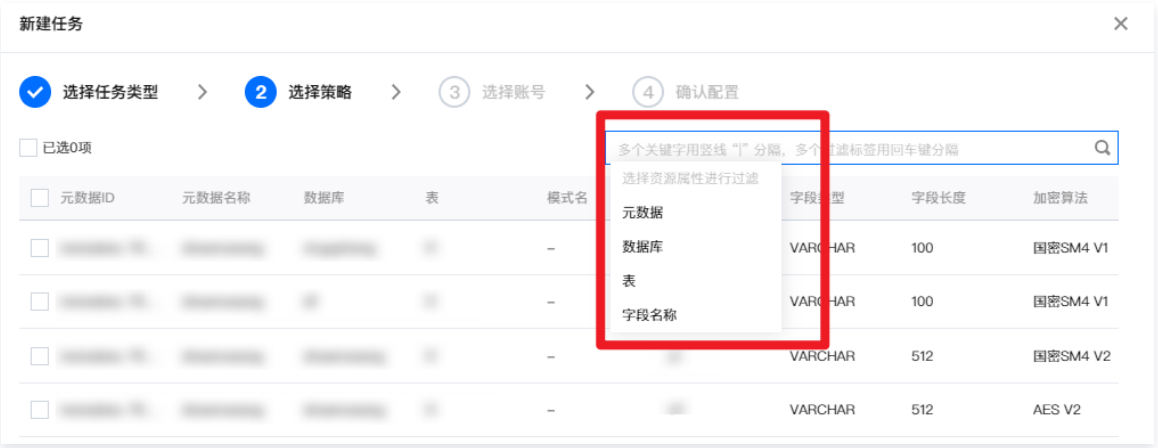
增量依据	目前支持**自增主键 ID** 与**更新时间 UPDATETIME** 两种。
	• MYSQL 数据源增量依据支持类型：
	  ○ 主键 ID：INT、INT UNSIGNED、BIGINT、BIGINT UNSIGNED
	  ○ UPDATETIME：DATETIME、TIMESTAMP
	• PGSQL 数据源增量依据支持类型
	  ○ 主键ID：INT4、INT8
	  ○ UPDATETIME：TIMESTAMP、TIMESTAMPTZ、TIME_STAMP
		增量任务说明，请查阅增量任务实践教程。

增量依据字段名	• 增量任务需指定任务执行的增量依据字段名，且字段类型需要符合对应的增量依据字段类型。 • 当加密任务涉及多张表时，增量依据字段名需要在多张表中均存在。 • 增量任务需指定任务执行的增量依据字段名，且确保现有所有数据记录增量依据字段均有值，若增量依据值为空或 null，则该记录无法加解密。	–

说明

- **数据修复类型**的使用场景。
  - 现象：因加解密使用不同的策略，导致无法解密已加密的数据字段。
  - 原因：数据字段策略被删除后，使用新的加密密钥、算法配置策略。
- **明文统计任务**的使用场景（**目前仅支持字符串类型**）。
  - 现象：已配置加密策略的数据库中，某字段存在明文数据。
  - 原因：①配置了加密策略，但字段未加密成功； ②通过非代理情况连接数据库，写入了明文数据。

5. 任务基础信息配置完成后，单击**下一步**，进行策略的选择。
6. 在选择策略步骤，选择需要进行任务执行的策略信息。如未配置策略，请查阅 创建策略 。
7. 在选择策略时，可以通过元数据、数据库、表、字段名称筛选所需要执行任务的具体策略。



> **说明：**
> 选择策略时支持跨元数据、数据库、表之间进行多项策略选择。

8. 完成策略选择后，单击**下一步**，进行数据库账号选择。
9. 在账号选择步骤，需要选择一个具有读写权限的数据库管理账号。完成后，单击**下一步**，进行配置确认。
10. 在确认配置步骤，仔细检查所配置的任务基本信息和策略信息。如果信息无误，单击**确认**，任务即新建成功。

> **说明：**
> - 手动任务创建完成后，任务处于**等待执行**状态，此时在其右侧操作栏，单击**启动**，即可执行任务。
> - 周期任务创建完成后，在任务到达指定执行时间时，任务处于**等待调度**状态，同时任务会被自动执行。

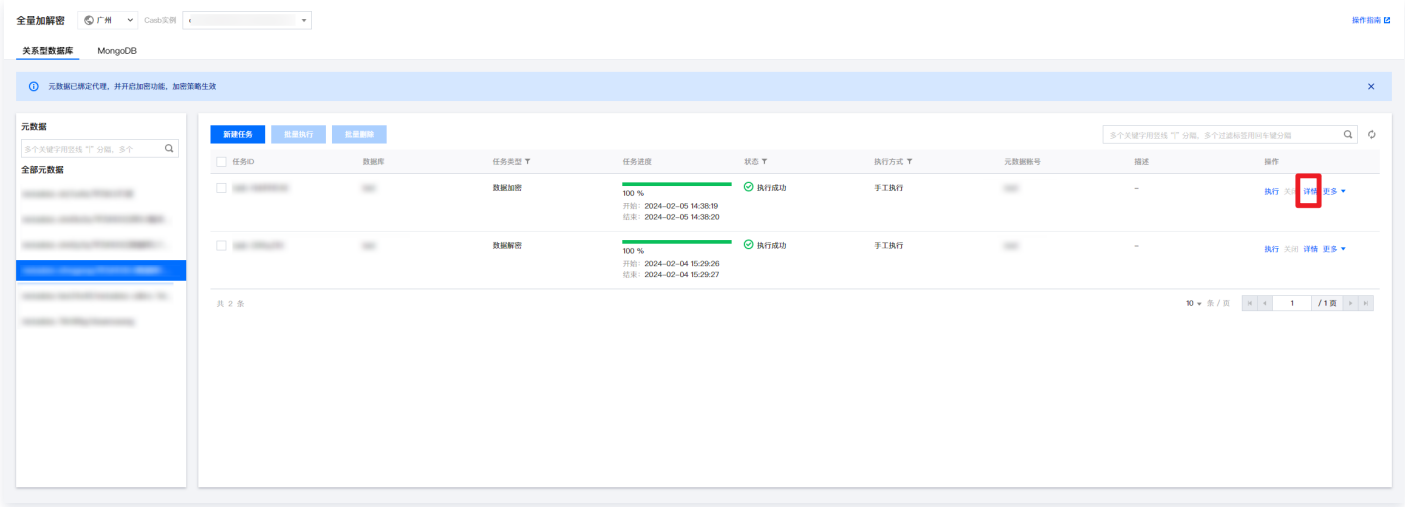
管理任务

前提条件

- 已 购买开通 CASB 实例 。
- 已创建元数据。如未创建元数据，请查阅 添加云元数据 、添加自建数据库 。

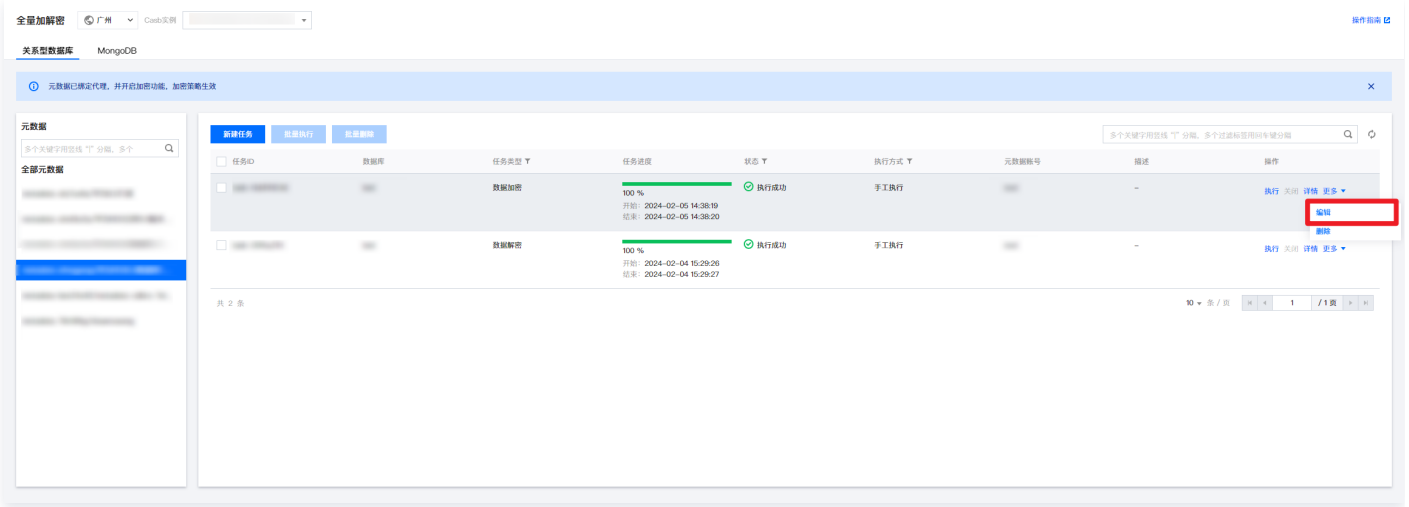
操作步骤

1. 登录 控制台 ， 单击左侧数据加密菜单下的**全加量加解密**，进入全量加解密页面。
2. 在全量加解密页面，选择所需的地域、 CASB 实例和元数据。
3. 在全量加解密页面，找到所需的任务，单击**详情**，进入任务详情页面。



4. 在任务详情页面，即可查看对应的元数据的任务基本信息、数据来源、任务执行的类型、周期执行任务可以查看首次执行时间以及任务下次执行时间；增量任务可以查看任务执行的增量依据以及对应的增量依据字段，任务执行状态和表名字段。

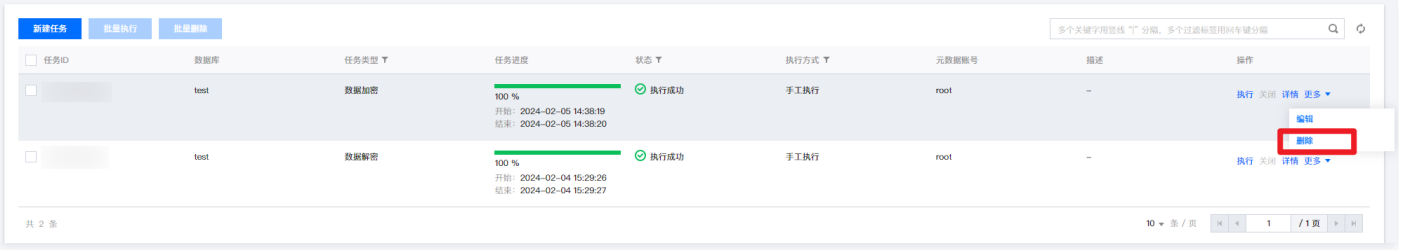
5. 在全量加解密页面，找到所需的任务，单击**更多** > **编辑**，弹出编辑任务弹窗。



6. **在编辑任务弹窗，修改相关参数，单击确定即可保存。**
   - **周期执行任务：可修改对应的任务首次执行时间，执行间隔以及代理账号和任务描述。**

   - **增量执行任务：可修改对应的增量依据，以及指定新的增量依据字段名。**

7. 在全量加解密页面，找到所需的任务，单击**更多 > 删除**即可完成。



任务结果错误码

错误码	说明	建议
111	明文值长度为1	支持模糊搜索算法，字段值必须为空或长度大于等于2，修改字段值或者修改算法类型
324	解密失败	策略无法解密已存储的密文，建议执行数据修复任务
801	密文长度超过字段长度	根据 maxCipherLength 值修改字段长度，可参考文档 密文长度计算，计算明文加密后的最大密文长度

密钥管理

最近更新时间：2024-11-13 09:44:52

前提条件

已 购买开通 CASB 实例。

新建密钥

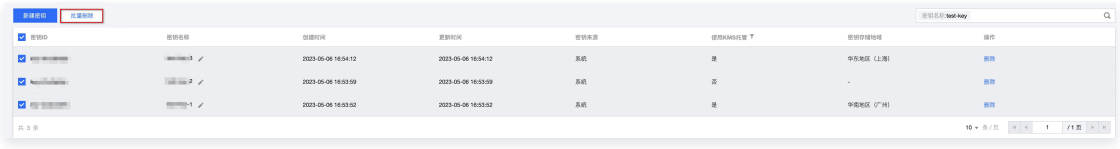
1. 登录 控制台，在左侧导航栏中，单击**数据加密 > 密钥管理**。
2. 在密钥管理页面，选择所需的地域和 CASB 实例。
3. 在密钥管理页面，单击**新建密钥**，弹出新建密钥窗口，若 KMS 托管选项为“是”，需要开通 KMS 服务 KMS 密钥管理和授权；为“否”，则密钥由 CASB 本地管理。
4. 在新建密钥窗口中，填写密钥的名称，单击**确定**完成创建。

删除密钥

> **说明：**
> - 当元数据为从节点时，密钥从主节点同步，禁止编辑。
> - 在删除密钥之前，需要先删除与密钥绑定的策略。

1. 登录 控制台，在左侧导航栏中，单击**数据加密 > 密钥管理**。
2. 在密钥管理页面，选择所需的地域和 CASB 实例。
3. 在密钥管理页面，支持删除单个或批量密钥，具体操作如下所示。
   - 删除单个密钥：找到所需删除的密钥，在其右侧的操作栏中单击**删除**。

   - 批量删除密钥：找到所需删除的密钥，勾选多个密钥选中后，单击**批量删除**。



4. 在“确认删除”窗口中，单击**确定**，即可删除密钥。

说明：
删除操作无法恢复，请谨慎操作。

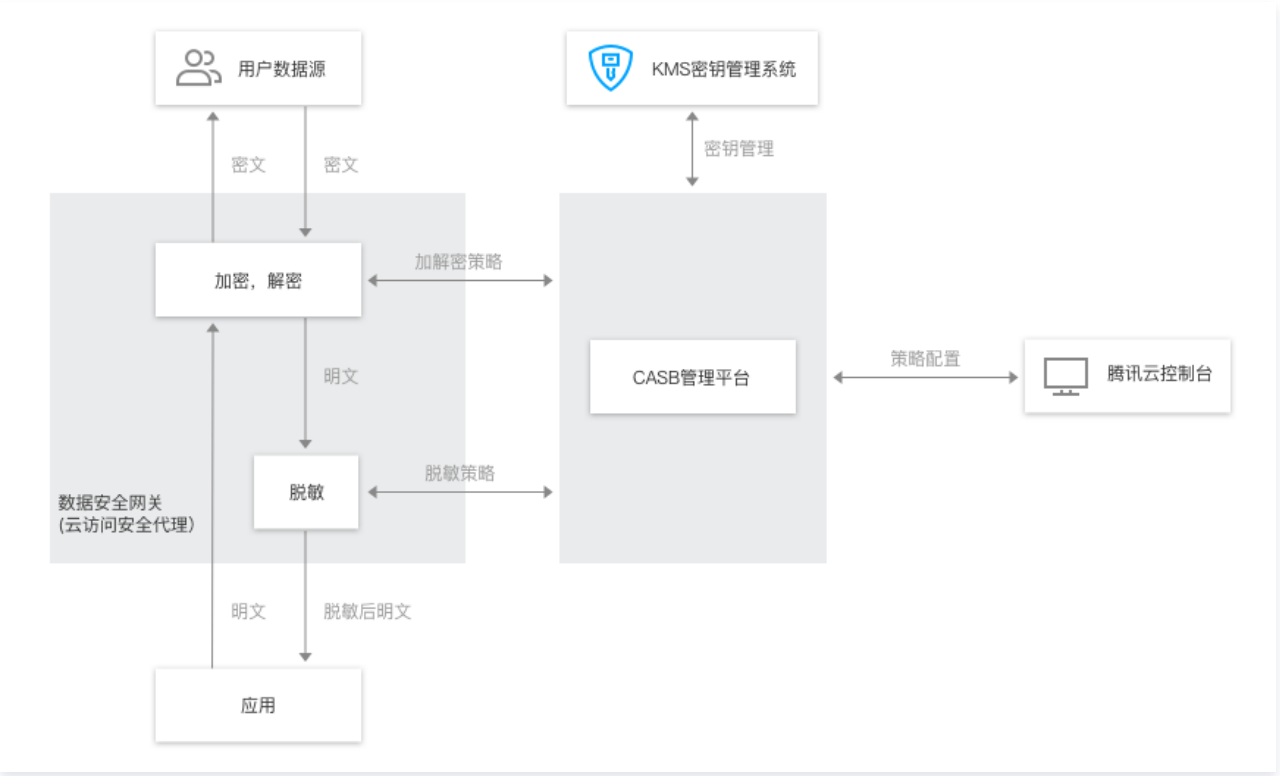
版权所有：腾讯云计算（北京）有限责任公司

数据脱敏
概述

最近更新时间：2024-11-04 15:49:42

数据安全网关（云访问安全代理，CASB）对于指定的数据源支持配置脱敏规则，配置规则后，平台将会依据您的规则实现敏感数据的脱敏，通过丰富的脱敏算法，进一步提高数据的安全性，确保敏感信息不易泄露。

数据脱敏的流程图



相关操作

- 动态脱敏策略管理
- 静态脱敏任务
- 脱敏算法管理
- 脱敏算法

动态脱敏策略管理
新建脱敏策略

最近更新时间：2025-05-13 10:28:52

前提条件

- 已 购买开通 CASB 实例 。
- 已创建元数据。如未创建元数据，请查阅 添加云元数据 、添加自建数据库 。

脱敏策略类型

数据安全网关（云访问安全代理）支持全部数据脱敏和指定元数据脱敏两种策略类型，以下是详细的介绍。

策略类型	描述	适用场景
全部元数据脱敏	• **管控范围**：所有数据源、所有代理账号。 • **脱敏规则**：使用脱敏模板。即提前针对分类配置脱敏策略，基于敏感识别结果实时生效脱敏策略。（如配置“手机号-遮盖算法”，所有被识别为手机号的字段都执行遮盖脱敏算法） • **特殊加白**：针对特别场景，可在策略基础上对账号、数据源进行加白，加白后可不执行脱敏。	• **快速搭建安全防护体系**：企业数据资产多，敏感数据分散多数据源，使用该策略可一次配置全局生效，无需对存量字段逐一配置。 • **敏感数据即时保护**：敏感数据识别后自动触发动脱策略生效。

指定元数据脱敏	• **管控范围**：指定数据源、指定代理账号
	• **脱敏规则**：可选择下列任一种方式
	  ○ 单字段逐一配置。即对每个字段单独配置不同脱敏算法。
	  ○ 使用脱敏模板。同全部元数据脱敏。
		• **账号差异化管控**：对同一分类数据在不同账号（内部系统、员工、供应商等）配置不同脱敏规则，适用于个性化管控诉求。
		• **场景差异化管控**：对同一分类数据在不同数据源时配置不同脱敏规则，适用于不同业务场景诉求，平衡安全和业务使用。

> ⚠ **注意：**
> 多条策略冲突时，取策略优先级升序排序，以前位策略为准。举例：A 策略的优先级=1，B 策略的优先级=2，当数据源脱敏规则在 A、B 策略冲突时，以 A 策略为准。

全局脱敏策略

前提条件

- 已关联敏感识别资源 。
- 已 创建脱敏模板 。

新建策略

1. 登录 控制台 ，在左侧导航栏中，单击**数据脱敏** > **动态脱敏策略**。
2. 在动态脱敏策略页面，选择所需的地域、CASB 实例。

3. 在动态脱敏策略页面，单击**新建脱敏策略**，输入所需参数，单击**确定**，即可完成策略的创建。

参数名称	参数说明
策略名称	由 1 – 50 字符组成。
策略描述	由 0 – 100 字符组成。
策略优先级	数字越小优先级越高，被占用数字不可选，用于策略冲突时判定。
开启状态	默认开启，仅开启的脱敏策略才能生效和被使用。
策略类型	**全部元数据脱敏：** • 创建后全局生效，“全部元数据脱敏”类型策略仅支持创建一条。 • 支持加白名单操作：（被加入的账号不会脱敏）。
脱敏规则	选择已配置的脱敏模板。

指定元数据脱敏策略

新建脱敏策略

1. 登录 控制台，在左侧导航栏中，单击**数据脱敏 > 动态脱敏策略**。
2. 在动态脱敏策略页面，选择所需的地域、CASB 实例。
3. 在动态脱敏策略页面，单击**新建脱敏策略**，输入所需参数单击**确定**，即可完成策略的创建。

> ⚠ **注意：**
> 脱敏规则类型为“逐个字段配置脱敏算法”时，还需对策略进行规则配置，操作请参考 规则管理 。

参数名称	参数说明
策略名称	由 1 – 50 字符组成。
策略描述	由 0 – 100 字符组成。
策略优先级	数字越小优先级越高，被占用数字不可选，用于策略冲突时判定。
开启状态	默认开启，仅开启的脱敏策略才能生效和被使用。
策略类型	**指定元数据脱敏：** • 指定具体的库表字段及脱敏算法，需要开启后才生效。 • 支持关联账号操作：（被关联的账号才会脱敏）。
脱敏元数据	选择需要脱敏的元数据。
脱敏账号	选择代理账号。
规则配置方式	• **使用脱敏模板** 通过选择脱敏模板的方式快速的配置脱敏策略。 • **逐个字段配置脱敏算法** 支持逐个字段进行脱敏算法的配置，策略新建完成后，参考 规则管理 进行配置。

查看脱敏策略详情

最近更新时间：2024-11-13 09:44:52

前提条件

- 已 购买开通 CASB 实例 。
- 已创建元数据。如未创建元数据，请查阅 添加云元数据 、 添加自建数据库 。
- 已创建脱敏策略；对于未创建脱敏策略的情况，可查阅 新建脱敏策略 进行创建。

操作步骤

1. 登录 控制台 ，在左侧导航栏中，单击**数据脱敏 > 动态脱敏策略**。
2. 在动态脱敏策略页面，选择所需的地域、CASB 实例。
3. 在动态脱敏策略页面，找到所需编辑的策略，单击**脱敏策略ID/名称**。

4. 在动态脱敏策略详情页面，可查看脱敏策略的详细信息，包括脱敏策略名称、地域、元数据、代理等信息，其中可修改**脱敏策略名称**和**描述** ，信息编辑完成之后，单击**确定**，即可完成修改。

参数名称	参数说明
脱敏策略名称	脱敏策略的名称，长度1~50个字符。
描述	可选参数，长度为0~100个字符。用于该规则组的备注信息，区别于其他策略。

删除脱敏策略

最近更新时间：2024-11-13 09:44:52

前提条件

- 已 购买开通 CASB 实例 。
- 已创建元数据。如未创建元数据，请查阅 添加云元数据 、添加自建数据库 。
- 已创建脱敏策略；对于未创建脱敏策略的情况，可查阅 新建脱敏策略 进行创建 。

操作步骤

1. 登录 控制台 ，在左侧导航栏中，单击**数据脱敏 > 动态脱敏策略**。
2. 在动态脱敏策略页面，选择所需的地域、CASB 实例。
3. 在动态脱敏策略页面，找到所需编辑的策略所在行，在其右侧的操作栏中单击**删除**。

4. 在 “确认删除” 弹窗中，单击**确认**，即可完成规则组的删除。

> **注意**
> 脱敏策略删除后将无法恢复，请您谨慎进行操作。

规则管理

最近更新时间：2024-11-13 09:44:52

本文将介绍如何查看、配置、删除动态脱敏规则。

前提条件

- 已 购买开通 CASB 实例 。
- 已创建元数据。如未创建元数据，请查阅 添加云元数据 、 添加自建数据库 。
- 已创建脱敏策略；对于未创建脱敏策略的情况，可查阅 新建脱敏策略 进行创建。

操作步骤

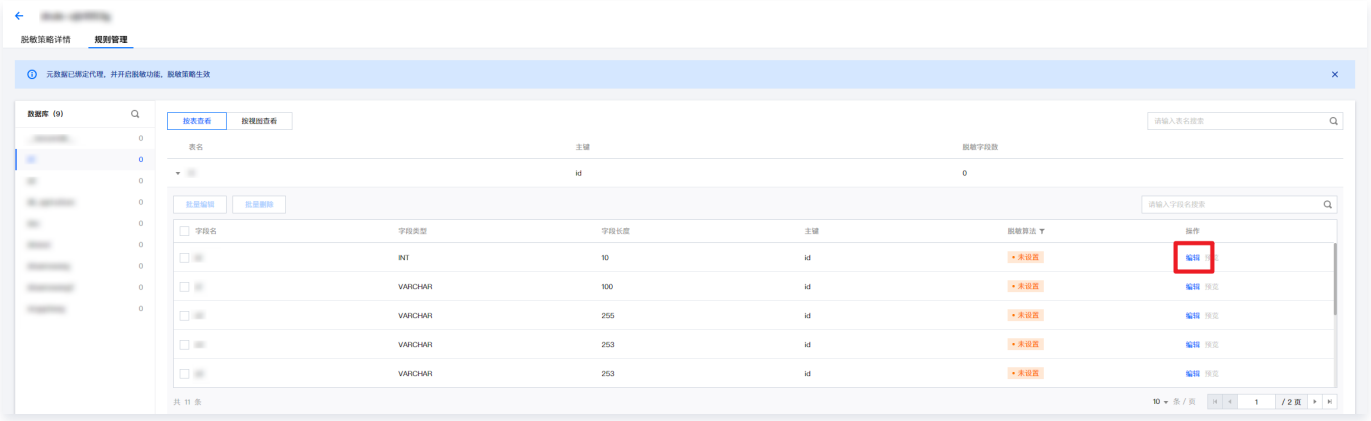
查看脱敏规则

1. 登录 控制台 ，在左侧导航栏中，单击**数据脱敏 > 动态脱敏策略**。
2. 在动态脱敏策略页面，选择所需的地域、CASB 实例。
3. 在动态脱敏策略页面，找到所需编辑的策略所在行，在其右侧操作项中单击**规则管理**。

4. 在规则管理页面，会显示所选元数据的数据库、表，当库名与表名选择完成之后，会自动加载表中字段的脱敏规则信息，信息包括字段名、数据类型、字段长度、脱敏算法等信息。

配置脱敏规则

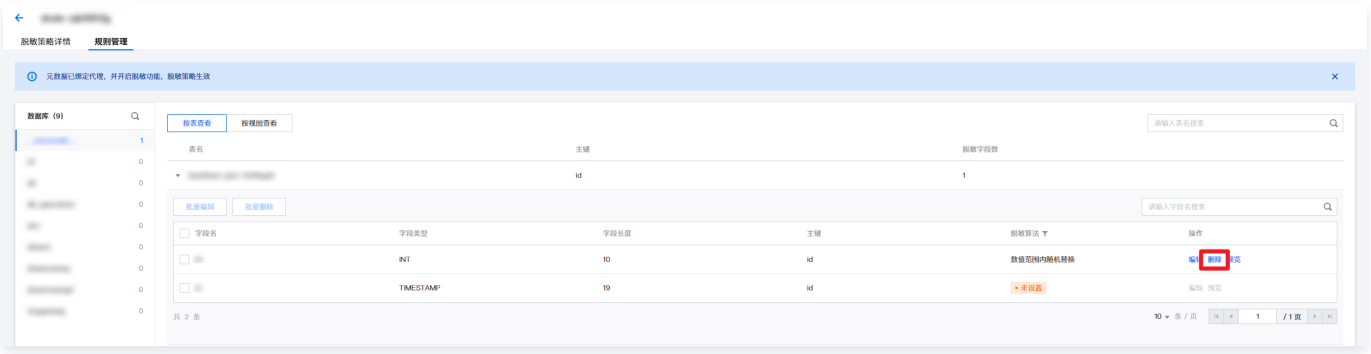
1. 在规则管理页面，选择需要配置脱敏规则的字段，单击操作栏中的**编辑**。



2. 在选择脱敏算法的下拉框中，选择合适的脱敏算法。
3. 脱敏算法设定完成之后，单击**预览**，进入规则预览页面。
4. 预览确认无误后，单击**确定**，即可完成相关字段的脱敏规则的配置。

删除脱敏规则

1. 在规则管理页面，选择需要配置脱敏规则的字段，单击操作栏中的**删除**。



2. 在 “确认删除” 弹窗中，单击**确认**，即可完成规则组的删除。

静态脱敏任务
数据库脱敏任务

最近更新时间：2024-11-13 09:44:52

前提条件

- 已 购买开通 CASB 实例 。
- 已创建元数据。如未创建元数据，请查阅 添加云元数据 、添加自建数据库 。

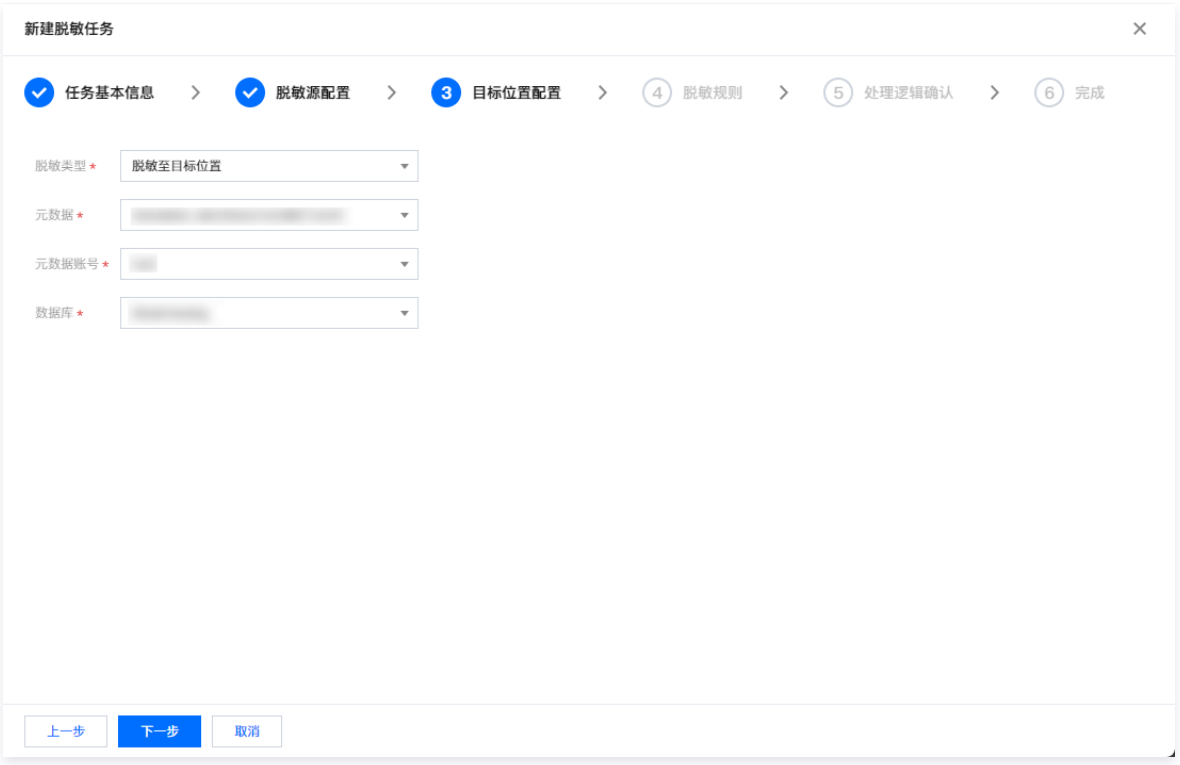
创建数据库脱敏任务

1. 登录 控制台 ，单击左侧数据加密菜单下的**静态脱敏任务**。
2. 在静态脱敏任务页面，选择所需的地域、CASB 实例和元数据。

3. 在静态脱敏任务页面，单击**新建脱敏任务**。
4. 在新建脱敏任务弹窗中，选择数据库脱敏，填写任务名称、备注，单击**下一步**。

5. 在脱敏源配置中，选择需要脱敏的元数据、元数据账号、数据库、选择脱敏表，单击**下一步**。

6. 在目标位置配置中，选择脱敏类型，选择元数据、元数据账号、数据库，单击**下一步**。

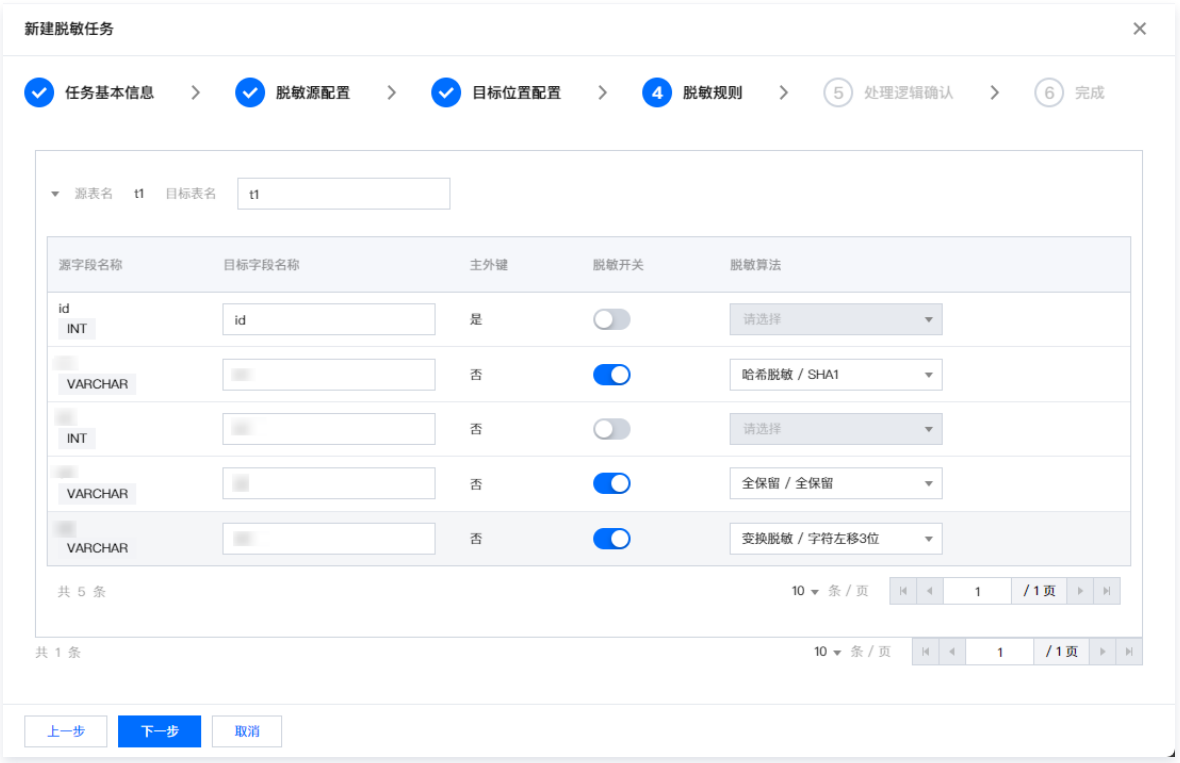


说明：

脱敏类型支持脱敏至目标位置与脱敏至文件两种类型：

- 脱敏至目标位置：选择脱敏至目标位置时，需要指定相应的元数据、元数据账号和数据库。脱敏后的数据将以目标表的形式在指定位置生成。
- 脱敏至文件：选择脱敏至文件，脱敏结果会以 `.txt` 的文件形式进行输出，在脱敏任务结束后，您可在脱敏任务执行详情中下载脱敏结果。

7. 在脱敏规则配置中，为表中字段配置脱敏算法，单击**下一步**。

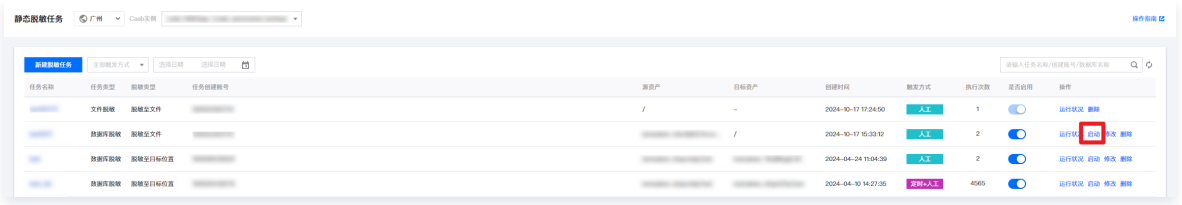


8. 在处理逻辑确认步骤中，需要对任务触发、执行逻辑进行配置，单击**下一步**。

9. 在任务确认步骤中，将显示您创建的任务的所有参数信息。确认无误后，单击**完成**，即可成功创建静态脱敏任务。

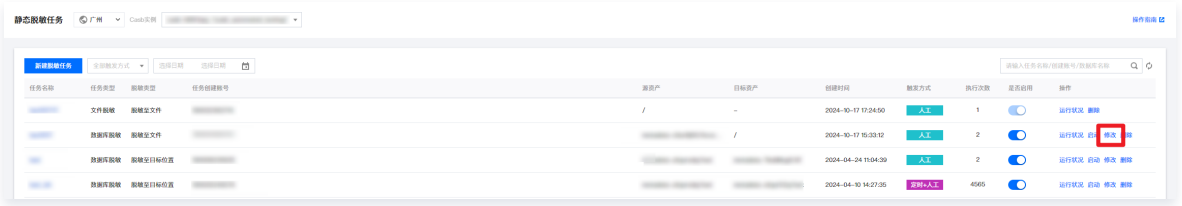
手动启动任务

1. 登录 控制台，单击左上角的区域下拉框，切换区域。
2. 在左侧导航菜单栏中，单击**数据脱敏 > 静态脱敏任务**。
3. 在静态脱敏任务页面中，选择需要手动启动执行的任务，单击该任务操作列中的**启动**。即可立即执行一次该任务。



编辑任务信息

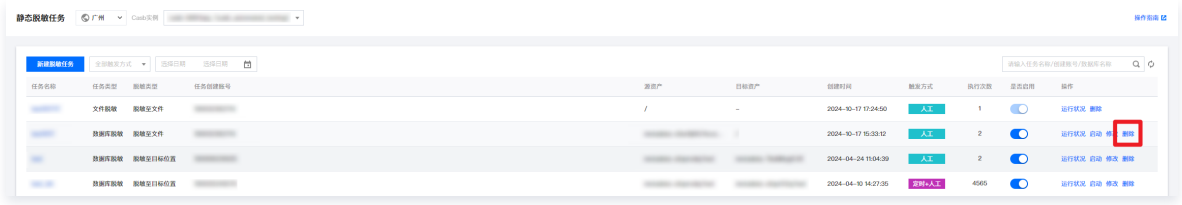
1. 登录 控制台，单击左上角的区域下拉框，切换区域。
2. 在左侧导航菜单栏中，单击**数据脱敏 > 静态脱敏任务**。
3. 在静态脱敏任务页面中，选择需要编辑的任务，单击该任务操作列中的**编辑**。



4. 在弹出的任务编辑窗口中，可修改任务相关信息，单击**完成**即可。

删除任务

1. 登录 控制台，单击左上角的区域下拉框，切换区域。
2. 在左侧导航菜单栏中，单击**数据脱敏 > 静态脱敏任务**。
3. 在静态脱敏任务页面中，选择需要删除的任务，单击该任务操作列中的**删除**。

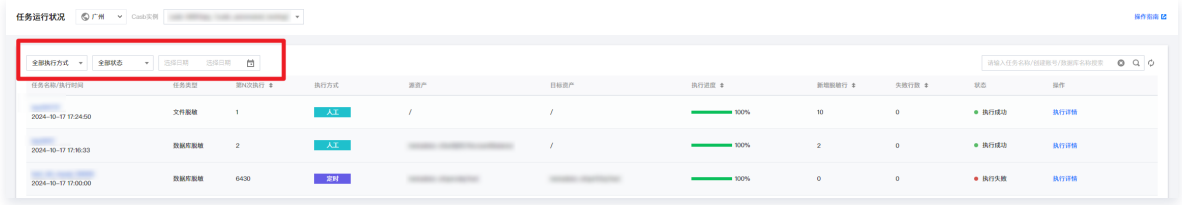


4. 在删除确认窗口中，二次确认并单击**删除**，即可删除该任务。

查看任务运行状况

在任务运行状况页面中，您可以查看处于等待执行、执行中、执行成功、执行失败、跳过执行、部分失败等不同状态的任务信息。这包括任务的执行进度和详细信息。

1. 登录 控制台，单击左上角的区域下拉框，切换区域。
2. 在左侧导航菜单栏中，单击数据脱敏菜单下的**数据脱敏 > 任务运行状况**。
3. 在任务运行状况页面，您可以通过执行方式、任务状态、日期等条件来检索和筛选任务。



4. 同时，对于单个任务，您可以在其操作栏中单击**执行详情**，以进入任务执行详情页面。在此，您能查看到任务执行的详细信息，包括任务名称、执行方式、执行时间、任务耗时等。

任务执行详情
执行成功
任务名称
执行方式
定时
执行时间
2024-05-21 18:00:00
资产源
目标资产
任务耗时
13秒
源表名
目标表名
总行数
脱敏行数
失败行数
丢弃行数
成功比例
执行进度
10
10
0
0
100%
100%

文件脱敏任务

最近更新时间：2024-11-13 09:44:52

前提条件

- 已 购买开通 CASB 实例 。
- 已创建元数据。如未创建元数据，请查阅 添加云元数据 、添加自建数据库 。

创建数据库脱敏任务

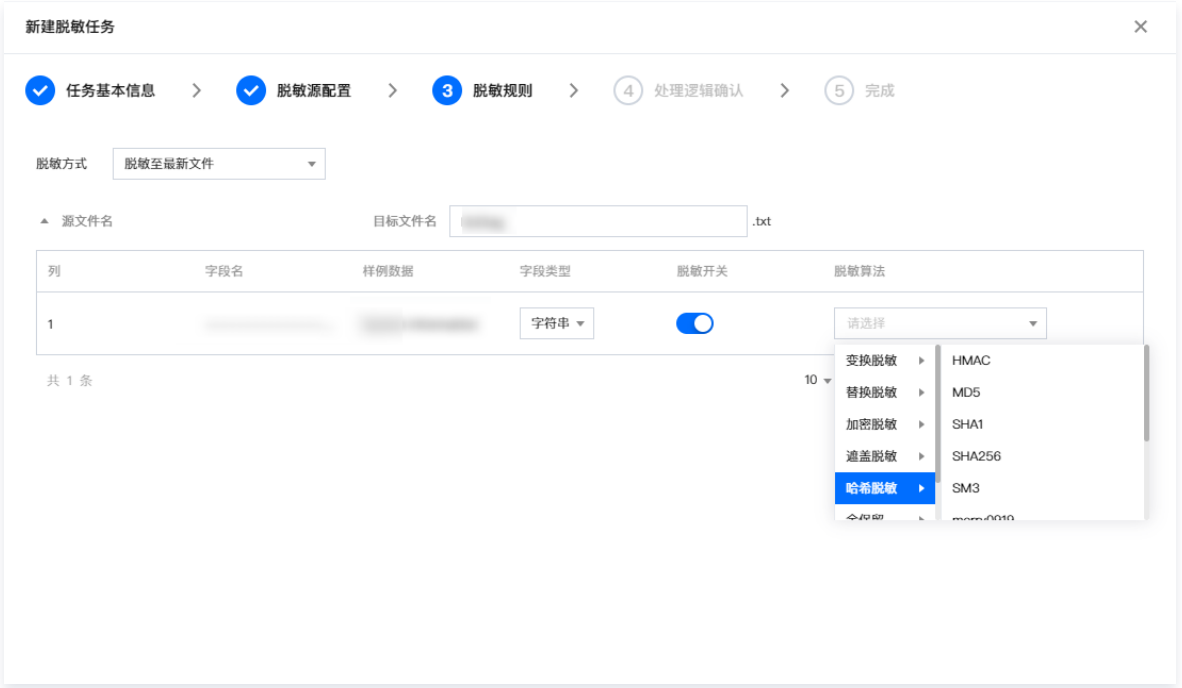
操作步骤

1. 登录 控制台 ，单击左侧数据加密菜单下的**静态脱敏任务**。
2. 在静态脱敏任务页面，选择所需的地域、CASB 实例和元数据。

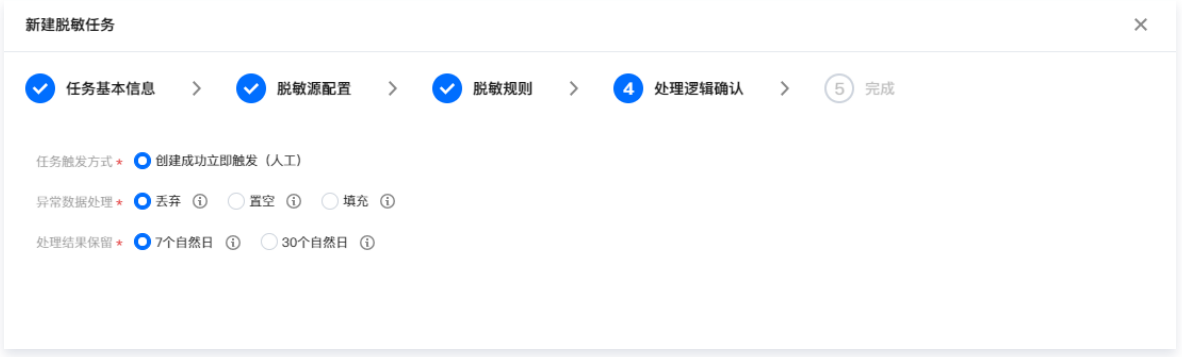
3. 在静态脱敏任务页面，单击**新建脱敏任务**。
4. 在新建脱敏任务弹窗中，选择**文件脱敏**，填写任务名称、备注，单击**下一步**。

5. 在脱敏源配置中，选择需要脱敏的文件进行上传。

6. 上传成功后需要根据分隔符、编码等配置进行文件解析，解析成功后单击**下一步**。



7. 在脱敏规则配置中，需要为解析出的字段配置脱敏算法，配置完成后单击**下一步**。



8. 在处理逻辑确认步骤中，需要对任务触发、异常数据处理、处理结果保留时间进行配置，配置完成后单击**下一步**。
9. 在任务确认步骤中，将显示您创建的任务的所有参数信息。确认无误后，单击**完成**，即可成功创建静态脱敏任务。

删除任务

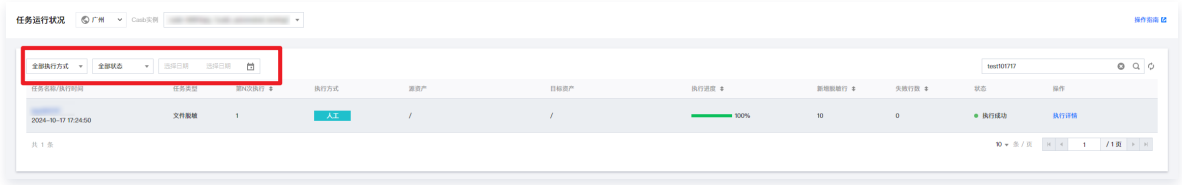
1. 登录 控制台，单击左上角的区域下拉框，切换区域。
2. 在左侧导航菜单栏中，单击**数据脱敏 > 静态脱敏任务**。
3. 在静态脱敏任务页面中，选择需要删除的文件脱敏任务，单击该任务操作列中的**删除**。

4. 在删除确认窗口中，二次确认并单击**删除**，即可删除该任务。

查看任务运行状况

在任务运行状况页面中，您可以查看处于等待执行、执行中、执行成功、执行失败、跳过执行、部分失败等不同状态的任务信息。

1. 登录 控制台，单击左上角的区域下拉框，切换区域。
2. 在左侧导航菜单栏中，单击数据脱敏菜单下的**数据脱敏 > 任务运行状况**，进入任务运行状况页面。
3. 在任务运行状况页面，您可以通过执行方式、任务状态、日期等条件来检索和筛选需要查看的目标任务。



4. 同时，对于单个任务，您可以在其操作栏中单击**执行详情**，以进入任务执行详情页面。在此，您能查看到任务执行的详细信息，包括任务名称、执行方式、执行时间、任务耗时等。

下载脱敏文件

1. 登录 控制台，单击左上角的区域下拉框，切换区域。
2. 在左侧导航菜单栏中，单击数据脱敏菜单下的**数据脱敏 > 任务运行状况**。
3. 在任务运行状况页面，您可以通过执行方式、任务状态、日期等条件来检索和筛选需要查看的目标任务。

4. 选中目标任务后，在其操作栏中单击**执行详情**。
5. 在任务详情页面，单击**目标文件名**，即可下载脱敏后的文件。

任务执行详情
执行成功
任务名称
执行方式
人工
执行时间
2024-10-17 17:24:50
资产源
/
目标资产
/
任务耗时
14秒
源表名
目标文件名
总行数
脱敏行数
失败行数
丢弃行数
成功比例
执行进度
新建文本文档.txt
新建文本文...
10
10
0
0
100%
100%

脱敏模板配置

最近更新时间：2024-12-31 17:50:22

通过将数据识别与脱敏模板相结合，CASB 能够针对不同类型和特征的数据，精准地应用相应的脱敏策略，保障在数据使用和共享过程中，敏感信息得到有效保护。

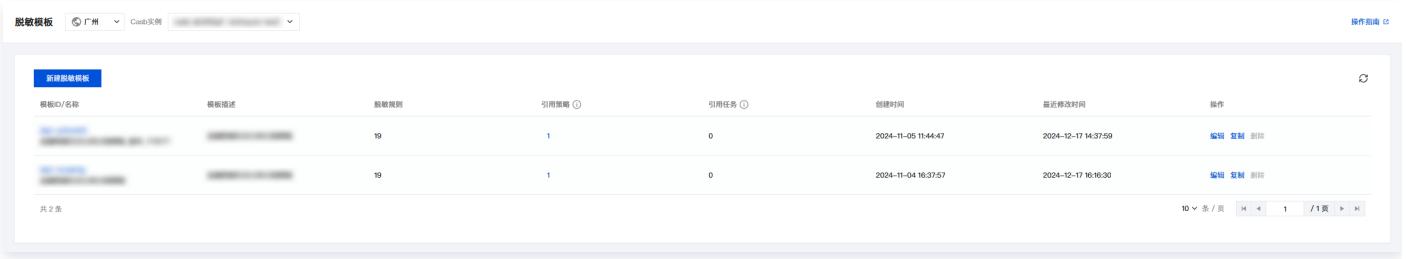
> **说明：**
> 脱敏模板功能当前仅支持北京、上海、广州、成都地域。

前提条件

已 购买数据安全治理中心实例 。
已 配置分类分级资源 。

操作步骤

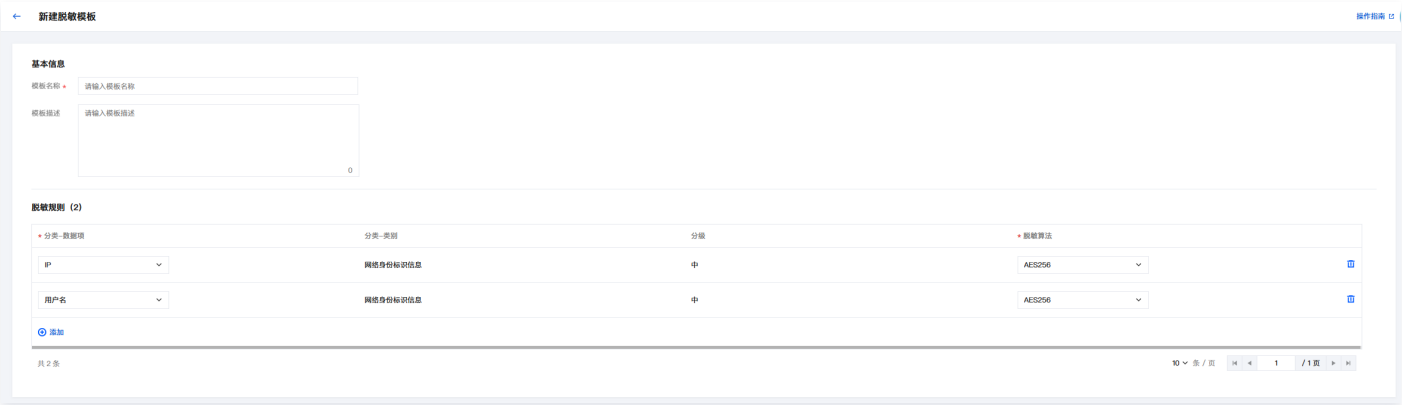
1. 登录 控制台，在左侧导航栏中，单击**数据脱敏 > 脱敏模板**。
2. 在脱敏模板页面，选择所需的地域、CASB 实例。
3. 在脱敏模板页面，可以看到模板ID/名称、 描述、脱敏规则、引用策略、引用任务、创建时间、最近修改时间。以及可以进行模板的 新建 、编辑 、复制 、删除 操作。



> **说明：**
> - 引用策略：引用该模板的动态脱敏策略数量。
> - 引用任务：引用该模板的静态脱敏任务数量。

新建脱敏模板

1. 在 脱敏模板页面，单击**新建脱敏模板**。
2. 在新建脱敏模板弹窗中，输入基本信息、添加脱敏规则后单击**确定** ，即可完成模板的创建。



编辑自定义模板

1. 在 脱敏模板页面，找到需要修改的模板，在其右侧单击**编辑**。
2. 在编辑模板弹窗中，您可以对模板名称、模板描述、脱敏规则进行修改，修改完后单击**确定**， 即可完成模板的修改。

> **说明：**
> 仅支持编辑来源为自定义的模板内容。

复制自定义模板

针对于存在多种相似的数据类型需要进行脱敏处理，且脱敏策略有很多共通之处时，您可以通过复制脱敏模板，快速创建相似模板。

1. 在 脱敏模板页面，找到需要复制的模板，在其右侧单击复制。
2. 新复制的模板会显示在脱敏模板列表中，可以根据实际业务需求对其进行进一步的编辑以应用到相应的数据脱敏场景中去。

> **说明：**
> 仅支持编辑来源为自定义的模板内容。

删除自定义模板

1. 在 脱敏模板页面，找到需要修改的模板，在其右侧单击**删除**。
2. 在“确认删除” 弹窗中，单击**删除**，即可删除自定义模板。

> **注意：**
> - 只支持删除来源为自定义的模板内容。
> - 模板删除后将无法恢复，请您谨慎进行操作。

脱敏算法管理

最近更新时间：2024-11-13 09:44:52

前提条件

已 购买开通 CASB 实例 。

操作步骤

1. 登录 控制台，在左侧导航栏中，单击**数据脱敏 > 脱敏算法**。
2. 在脱敏算法页面，选择所需的地域、CASB 实例。
3. 在脱敏算法页面，可以看到算法的名称、类型、 描述、来源、适用字段类型，以及可以进行算法的 新建 、编辑 、删除 、 测试 操作。

新建脱敏算法

1. 在 脱敏算法页面，单击**新建脱敏算法**。

2. 在新建脱敏算法弹窗中，输入所需参数单击**确定**，即可完成策略的创建。

编辑自定义算法

1. 在 脱敏算法页面，找到需要修改的算法，在其右侧单击**编辑测试**。

2. 在编辑算法弹窗中，可以看到该算法的所有信息，在所需编辑的文本框中输入修改内容，单击**确定**， 即可完成算法的修改。

> **说明：**
> 仅支持编辑来源为自定义的算法内容。

删除自定义算法

1. 在 脱敏算法页面，找到需要修改的算法，在其右侧单击**删除**。

> **注意：**
> - 只支持删除来源为自定义的算法内容。
> - 算法删除后将无法恢复，请您谨慎进行操作。

2. 在“确认删除” 弹窗中，单击**删除**，即可删除自定义算法。

算法测试验证

1. 在 脱敏算法页面，找到需要修改的算法，在其右侧单击**测试**。

2. 在算法预览弹窗中，可以看到该算法的基本信息，在原始数据的文本框中，输入测试内容，单击**测试**，即可得到该算法的脱敏结果。

脱敏算法
变换脱敏

最近更新时间：2024-11-13 09:44:52

本文档将为您介绍在控制台中创建类型为**变换脱敏**的脱敏算法，具体步骤如下。

前提条件

已 购买开通 CASB 实例 。

操作步骤

1. 登录 控制台，在左侧导航栏中，单击**数据脱敏** > **脱敏算法**。
2. 在脱敏算法页面，选择所需的地域、CASB 实例。
3. 在脱敏算法页面，单击**新建脱敏算法**，输入所需参数单击**确定**，即可完成算法的创建。

> **说明：**
> 变换脱敏相关参数说明，请参见下文 参数说明 。

参数说明

1. 基本信息

参数名称	参数说明
算法名称	算法的名称，长度1~50个字符。
来源	自定义算法，系统会自动填充。
描述	可选参数，长度为0~100个字符。用于该算法的备注信息，区别于其他自定义算法。

2. 算法配置

参数名称	参数说明
算法类型	选择算法的具体类型。 鉴于本文是描述变换脱敏，故选择**变换脱敏**。
变换类型	选择变换脱敏规则中的类型，其中系统会根据算法类型提供对应的变换规则。 变换规则支持**字符位移**、**日期取整**、**数字取整**。

- **情况一**

  变换类型选择为： 字符位移。

参数名称	参数说明
位移值	位移值（Offset）需为整数， 如果Offset为正，将整个字符串按位右移Offset位；如果Offset为负，将整个字符串按位左移|Offset| 位

- **情况二**

  变换类型选择为： 日期取整。

参数名称	参数说明
取整精度	取整精度为：**取整到年**、**取整到月**、**取整到日**、**取整到时**、**取整到分**、**取整到秒**，任选一项。
时间格式	时间格式定义： • 4位年份：yyyy • 2位年份：yy • 月份（填充0补齐两位）：MM • 月份（不填充0）：M • 日期（填充0补齐两位）：dd • 日期（不填充0）：d • 小时（24小时制）：HH • 小时（12小时制，填充0补齐两位）：hh • 小时（12小时制，不填充0）：h • 分钟（填充0补齐两位）：mm • 分钟（不填充0）：m • 秒（填充0补齐两位）：ss • 秒（不填充0）：s 如： 2021-08-01 20:12:34 的时间格式定义为 yyyy-MM-dd HH:mm:ss. 时间格式中，年月日时分秒需至少包含一个。

- **情况三**

  变换类型选择为： 数字取整。

参数名称	参数说明
取整精度	数字的取整精度值，取整精度需为整数，>0取小数点前位数，<0取小数点后位数。

3. 测试验证

数据输入完成之后，单击测试，即可完成测试验证。

参数名称	参数说明
原始数据	输入待验证的字段。
验证	基于算法的配置、输入的字段，展示输出脱敏后的结果内容。

哈希脱敏

最近更新时间：2024-11-13 09:44:52

本文档将为您介绍在控制台中创建类型为**哈希脱敏**的脱敏算法的具体步骤。

前提条件

已 购买开通 CASB 实例 。

操作步骤

1. 登录 控制台，在左侧导航栏中，单击**数据脱敏** > **脱敏算法**。
2. 在脱敏算法页面，选择所需的地域、CASB 实例。
3. 在脱敏算法页面，单击**新建脱敏算法**，输入所需参数单击**确定**，即可完成算法的创建。

> **说明：**
> 哈希脱敏相关参数说明，请参见下文 参数说明 。

参数说明

1. 基本信息

参数名称	参数说明
算法名称	算法的名称，长度1~50个字符。
来源	自定义算法，系统会自动填充。

描述	可选参数，长度为0~100个字符。用于该算法的备注信息，区别于其他自定义算法。

2. 算法配置

参数名称	参数说明
算法类型	选择算法的具体类型。 鉴于本文是描述哈希脱敏，故选择**哈希脱敏**。
哈希算法	选择哈希算法中的类型，其中系统会根据算法类型提供对应的加密算法。 哈希脱敏支持 HMAC、MD5、SHA1、SHA256、SM3。
盐值	输入哈希算法中的盐值内容，0~32个字节。（可选）

3. 测试验证

数据输入完成之后，单击**测试**，即可完成测试验证。

参数名称	参数说明
原始数据	输入待验证的字段。
验证	基于算法的配置、输入的字段，展示输出脱敏后的结果内容。

加密算法

最近更新时间：2024-11-13 09:44:52

本文档将为您介绍在控制台中创建类型为**加密脱敏**的脱敏算法，具体步骤如下。

前提条件

已 购买开通 CASB 实例 。

操作步骤

1. 登录 控制台，在左侧导航栏中，单击**数据脱敏** > **脱敏算法**。
2. 在脱敏算法页面，选择所需的地域、CASB 实例。
3. 在脱敏算法页面，单击**新建脱敏算法**，输入所需参数单击**确定**，即可完成算法的创建。

> **说明：**
> 加密脱敏相关参数说明，请参见下文 参数说明 。

参数说明

1. 基本信息

参数名称	参数说明
算法名称	算法的名称，长度1~50个字符。

来源	自定义算法，系统会自动填充。
描述	可选参数，长度为0~100个字符。用于该算法的备注信息，区别于其他自定义算法。

2. 算法配置

参数名称	参数说明
算法类型	选择算法的具体类型。 鉴于本文是描述加密脱敏，故选择**加密脱敏**。
加密算法	选择加密中的算法规则，其中系统会根据算法类型提供对应的加密算法。 加密脱敏目前只支持 AES256 。
加密密钥	输入算法的加密密钥值。 16进制字符串，32个字符，不可为空。
初始向量	输入算法的初始向量值。16进制字符串，16个字符，不可为空。

3. 测试验证

数据输入完成之后，单击**测试**，即可完成测试验证。

参数名称	参数说明
原始数据	输入待验证的字段。
验证	基于算法的配置、输入的字段，展示输出脱敏后的结果内容。

替换脱敏

最近更新时间：2024-11-13 09:44:52

本文档将为您介绍在控制台中创建类型为**替换脱敏**的脱敏算法，具体步骤如下。

前提条件

已 购买开通 CASB 实例 。

操作步骤

1. 登录 控制台，在左侧导航栏中，单击**数据脱敏 > 脱敏算法**。
2. 在脱敏算法页面，选择所需的地域、CASB 实例。
3. 在脱敏算法总览页面中，单击**新建脱敏算法**，输入所需参数单击**确定**，即可完成算法的创建。

> **说明：**
> 替换脱敏相关参数说明，请参见下文 参数说明 。

参数说明

1. 基本信息

参数名称	参数说明
算法名称	算法的名称，长度1~50个字符。
来源	自定义算法，系统会自动填充。
描述	可选参数，长度为0~100个字符。用于该算法的备注信息，区别于其他自定义算法。

2. 算法配置

参数名称	参数说明
算法类型	选择算法的具体类型。 鉴于本文是描述替换脱敏，故选择**替换脱敏**。
替换类型	选择替换脱敏规则中的类型，其中系统会根据算法类型提供对应的替换规则。 替换规则支持**正则匹配**、**关键字替换**、**身份证映射替换**、**身份证随机替换**、**保留格式映射替换**、**数值范围内随机替换**。

- **情况一**

  替换规则选择为：正则匹配；

  规则说明：对于输入字符串中的内容，可以被正则所匹配的部分，将会使用替换字符串进行替换。

参数名称	参数说明
正则表达式	正则表达式需由正则表达式字符串组成，如：[0-5A-Z]。
替换字符串	用于替换的字符串内容，非空。

- **情况二**

  替换规则选择为：关键字替换。

  算法描述：输入字符串的内容与关键字相同的部分，将会使用替换字符串进行替换。

参数名称	参数说明
关键字	输入所需的关键字内容，非空。
替换字符串	用于替换的字符串内容，非空。

- **情况三**

  替换规则选择为：身份证映射替换；

  算法描述：（18位）前6位根据映射表进行映射，7-14位以起始出生日期 和结束出生日期为区间随机替换，15-17位不变，第18位动态生成校验码；（15位）同理，替换前6位地区和第7至12位生日。

参数名称	参数说明
起始出生日期	起始出生日期需由数字组成，长度8个字符，如：19000101。若为空，默认使用19000101。
结束出生日期	结束出生日期需由数字组成，长度8个字符，如：21000101。若为空，默认使用21000101。
映射表	行政区划映射表需由如下格式字符串组成：{"320101":"321322", "320102":"320801"}

- **情况四**

  替换规则选择为：身份证随机替换。

  算法描述：（18位）前6位使用随机地区码替换，7-14位以起始出生日期和结束出生日期为区间随机替换，15-17位不变，第18位动态生成校验码；（15位）同理，替换前6位地区和第7至12位生日。

参数名称	参数说明
起始出生日期	起始出生日期需由数字组成，长度8个字符，如：19000101。若为空，默认使用19000101。
结束出生日期	结束出生日期需由数字组成，长度8个字符，如：21000101。若为空，默认使用21000101。

- **情况五**

  替换规则选择为：保留格式映射替换。

  算法描述：根据映射表，对输入字符串进行映射替换，匹配到表中的键的字符用对应值替换，否则不变。

参数名称	参数说明
映射表	输入保留格式映射表。若为空，使用默认映射表。 保留格式映射表需由如下格式字符串组成：{"A":"I","B":"P","d":"g","e":"h","0":"6","1":"7","#":"/"}。

- **情况六**

  替换规则选择为：数值范围内随机替换。

  算法描述：对于输入的数值，将用设置的数值范围内的随机数来替换原始值输入值。

参数名称	参数说明
数值范围	• min：随机替换数值的最小值。 • max：随机替换数值的最大值。

3. 测试验证

数据输入完成之后，单击测试，即可完成测试验证。

参数名称	参数说明
原始数据	输入待验证的字段。
验证	基于算法的配置、输入的字段，展示输出脱敏后的结果内容。

遮盖脱敏

最近更新时间：2024-11-13 09:44:52

本文档将为您介绍在控制台中创建类型为**遮盖脱敏**的脱敏算法，具体步骤如下。

前提条件

已 购买开通 CASB 实例 。

操作步骤

1. 登录 控制台，在左侧导航栏中，单击**数据脱敏 > 脱敏算法**。
2. 在脱敏算法页面，选择所需的地域、CASB 实例。
3. 在脱敏算法页面，单击**新建脱敏算法**，输入所需参数单击**确定**，即可完成算法的创建。

> **说明：**
> 遮盖脱敏相关参数说明，请参见下文 参数说明 。

参数说明

1. 基本信息

参数名称	参数说明
算法名称	算法的名称，长度1~50个字符。
来源	自定义算法，系统会自动填充。

描述	可选参数，长度为0~100个字符。用于该算法的备注信息，区别于其他自定义算法。

2. 算法配置

参数名称	参数说明
算法类型	选择算法的具体类型。 鉴于本文是描述遮盖脱敏，故选择**遮盖脱敏**。
遮盖规则	选择遮盖规则中的类型，其中系统会根据算法类型提供对应的遮盖规则。 遮盖规则支持**保留自X到Y、保留前X后Y、保留前X后Y（不计入空白字符）、遮盖自X到Y、遮盖前X后Y、字符前遮盖、字符后遮盖、分段遮盖**。

- **情况一**

  遮盖规则选择为：**保留自X到Y、保留前X后Y、保留前X后Y（不计入空白字符）、遮盖自X到Y、遮盖前X后Y**。

  算法描述：

  - **保留自X到Y：** 指保留字符串[x,y]区间的字符，从1开始计数，其余字符用 **遮盖字符** 内容 进行遮盖。
  - **保留前X后Y：** 指保留字符串前x个字符和后y个字符的数据，从1开始计数，其余用 **遮盖字符** 内容进行遮盖。
  - **保留前X后Y（不计入空白字符）：** 指保留字符串前x个字符和后y个字符的数据，在计算X和Y的位置时，忽略空白字符，确保只计算实际的数据字符。
  - **遮盖自X到Y：** 指用**遮盖字符**内容遮盖字符串[x,y]区间的字符，从1开始计数，其余保留。
  - **遮盖前X后Y：** 指用**遮盖字符**内容遮盖字符串前x个字符和后y个字符，从1开始计数，其余保留。

参数名称	参数说明
位置参数	输入X和Y值。 X为保留/遮盖的起始位置，Y为保留/遮盖的结束位置
遮盖字符	遮盖的字符内容，长度为1个字符。

- **情况二**

  遮盖规则选择为：**字符前遮盖、字符后遮盖**。

  算法描述：用**遮盖字符**内容遮盖指定字符之前/之后的数据（针对该字符首次出现的位置）。

参数名称	参数说明
识别字符	识别的指定字符内容，非空。
遮盖字符	遮盖的字符内容，长度为1个字符。

- **情况三**

  遮盖规则选择为：**分段遮盖**。

  算法描述：根据**分段字符数组**对字符串进行分段，将列举的**分段序号**对应的各子串中的各个字符使用**遮盖字符**内容进行遮盖，分段号从1开始计数。

参数名称	参数说明
分段字符	用于分段的特殊字符数组，非空，任一元素均非空字符。
段序号	需要进行遮盖的段序号。
遮盖字符	遮盖的字符内容，长度为1个字符。

3. 测试验证

数据输入完成之后，单击**测试**，即可完成测试验证。

参数名称	参数说明
原始数据	输入待验证的字段。
验证	基于算法的配置、输入的字段，展示输出脱敏后的结果内容。

访问控制
访问规则管理

创建访问规则

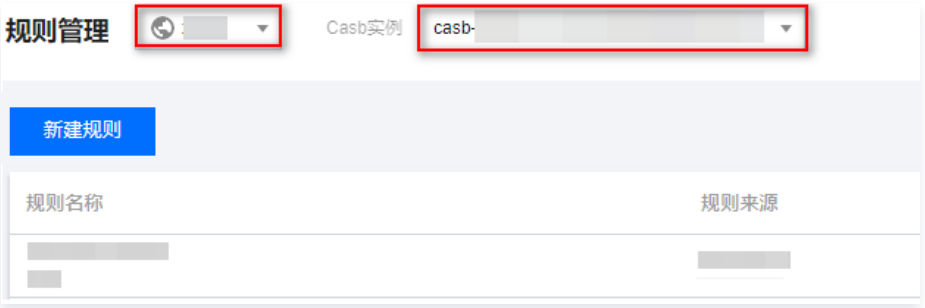
最近更新时间：2024-11-08 21:33:12

前提条件

需已 购买开通 CASB 实例 。

操作步骤

1. 登录 控制台，在左侧导航栏中，单击**访问控制** > **规则管理**。
2. 在规则管理页面，选择所需的地域、CASB 实例。



3. 在规则管理页面中，单击**新建规则**，根据配置项逐一输入，单击**完成**，即完成规则的创建。

参数名称	参数说明
规则名称	自定义参数，1~60字符，仅支持中文、英文字母、数字、“_”、“-”，并且开头和结尾需为中文、英文字母或者数字，名称不可重复。
规则描述	自定义参数，0~100字符。（可选）
数据库名称	输入待匹配的数据库名。
表名	输入待匹配的表名。
命令	选择 SQL 命令，最多10组。
SQL 行数	检查 SELECT 返回结果集行数是否大于等于此项配置。
字段	输入待匹配的字段名。
执行周期	执行方式：不限、每天、指定时间段。
选择时间	执行周期选择**每天**或**指定时间段**后，需配置对应的时间。 • 每天：设置开始时间和结束时间，格式:：HH:mm:ss。 • 指定时间段：设置开始日期和结束日期，格式：YYYY-MM-DD；及设置开始时间和结束时间，格式：HH:mm:ss。
访问规则	规则有两种，分别是：**阻断**和**放行**。

> **说明：**
> - 命令：**阻断/放行**仅对选择列表中已选择的命令生效。未选择时，对列表中的全部命令生效。
> - SQL行数：执行语句为 SELECT 且 SELECT 返回的行数满足设定值时生效。

注意事项

- 规则时间为北京时间（GMT+8），其中规则配置/变更后，3s内生效。
- 加密策略无法支持的场景同样适用于访问控制。
- MySQL 的库名、表名、字段名不区分大小写。
- 返回结果集长度仅对 SELECT 语句生效，且忽略子语句内 SELECT 语句的访问结果集行数判断。
- information_schema 库的所有表不应用访问控制规则。
- 支持的访问控制命令包括：SELECT、UPDATE、REPLACE、INSERT、DELETE、CREATE TABLE、ALTER TABLE、DROP TABLE、RENAME TABLE、TRUNCATE TABLE、CREATE DATABASE、DROP DATABASE。
- 忽略匹配包含字段的规则包括：CREATE TABLE, ALTER TABLE, DROP TABLE, RENAME TABLE, TRUNCATE TABLE命令。
- 忽略匹配包含表和字段的规则包括：CREATE DATABASE, DROP DATABASE 。

版权所有：腾讯云计算（北京）有限责任公司

编辑访问规则

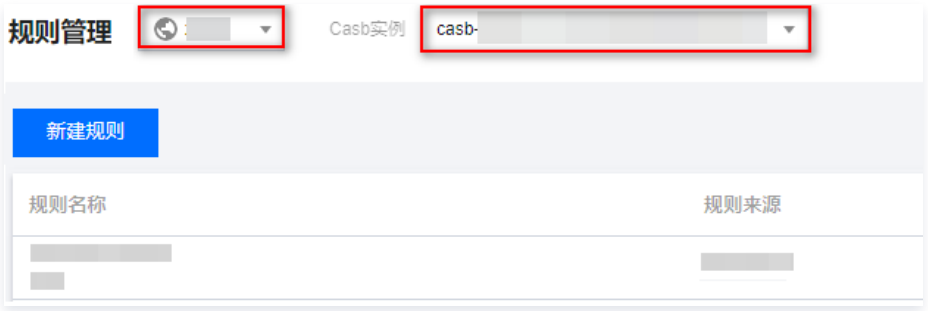
最近更新时间：2024-11-08 21:33:12

前提条件

- 需已 购买开通 CASB 实例 。
- 已创建访问规则。如未创建访问规则，详情可查阅 创建访问规则 。

操作步骤

1. 登录 控制台，在左侧导航栏中，单击**访问控制** > **规则管理**。
2. 在规则管理页面，选择所需的地域、CASB 实例。



3. 在规则管理页面中，找到所需的规则，单击**编辑**。

4. 在编辑规则弹窗中，根据所需编辑对应的配置项，单击**确定**，即可完成编辑。

参数名称	参数说明
规则名称	自定义参数，1~60字符，仅支持中文、英文字母、数字、“_”、“-”，并且开头和结尾需为中文、英文字母或者数字，名称不可重复。
规则描述	自定义参数，0~100字符。（可选）
数据库名称	输入待匹配的数据库名。
表名	输入待匹配的表名。
命令	选择 SQL 命令，最多10组。
SQL 行数	检查 SELECT 返回结果集行数是否大于等于此项配置。
字段	输入待匹配的字段名。

执行周期	执行方式：不限、每天、指定时间段。
选择时间	执行周期选择**每天**或**指定时间段**后，需配置对应的时间。 • 每天：设置开始时间和结束时间，格式:：HH:mm:ss。 • 指定时间段：设置开始日期和结束日期，格式：YYYY-MM-DD；及设置开始时间和结束时间，格式：HH:mm:ss。
访问规则	规则有两种，分别是：**阻断**和**放行**。

说明：
- 命令：**阻断/放行**仅对选择列表中已选择的命令生效。未选择时，对列表中的全部命令生效。
- SQL 行数：执行语句为 SELECT 且 SELECT 返回的行数满足设定值时生效。

注意事项

- 规则时间为北京时间（GMT+8），其中规则配置/变更后，3s内生效。
- 加密策略无法支持的场景同样适用于访问控制。
- MySQL 的库名、表名、字段名不区分大小写。
- 返回结果集长度仅对 SELECT 语句生效，且忽略子语句内 SELECT 语句的访问结果集行数判断。
- information_schema 库的所有表不应用访问控制规则。
- 支持的访问控制命令包括：SELECT、UPDATE、REPLACE、INSERT、DELETE、CREATE TABLE、ALTER TABLE、DROP TABLE、RENAME TABLE、TRUNCATE TABLE、CREATE DATABASE、DROP DATABASE。
- 忽略匹配包含字段的规则包括：CREATE TABLE, ALTER TABLE, DROP TABLE, RENAME TABLE, TRUNCATE TABLE命令。
- 忽略匹配包含表和字段的规则包括：CREATE DATABASE, DROP DATABASE 。

版权所有：腾讯云计算（北京）有限责任公司

删除访问规则

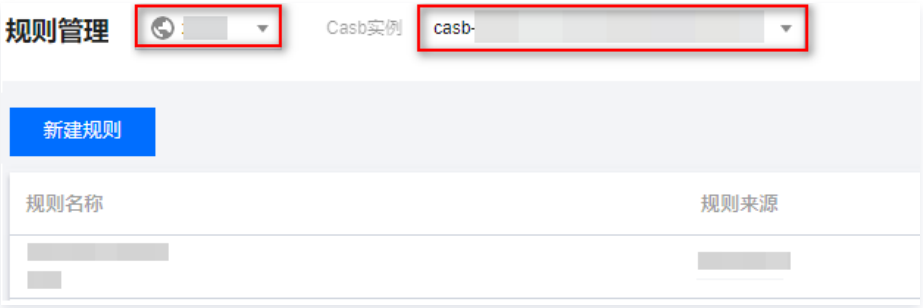
最近更新时间：2024-11-08 21:33:12

前提条件

- 需已 购买开通 CASB 实例 。
- 已创建访问规则。如未创建访问规则，详情可查阅 创建访问规则 。

操作步骤

1. 登录 控制台，在左侧导航栏中，单击**访问控制** > **规则管理**。
2. 在规则管理页面，选择所需的地域、CASB 实例。



3. 在规则管理页面中，找到所需的规则，单击**删除**。

4. 在“确认删除”弹窗中，单击**确定**，即可完成规则的删除。

角色管理
创建角色

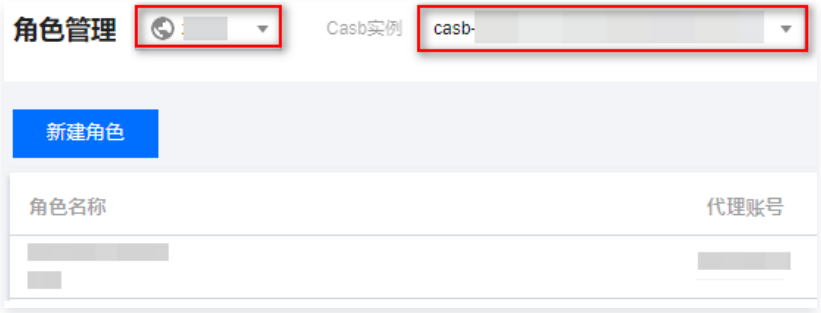
最近更新时间：2024-11-08 21:33:12

前提条件

需已 购买开通 CASB 实例 。

操作步骤

1. 登录 控制台，在左侧导航栏中，单击**访问控制** > **角色管理**。
2. 在角色管理页面，选择所需的地域、CASB 实例。



3. 在角色管理页面中，单击**新建角色**，根据配置项逐一输入，单击**确定**，即完成规则的创建。

参数名称	参数说明
角色名称	自定义参数，长度1~60字符，仅支持中文、英文字母、数字、“_”、“-”，并且开头和结尾需为中文、英文字母或者数字，名称不可重复。
角色描述	自定义参数，0~100字符。（可选）

添加代理账号

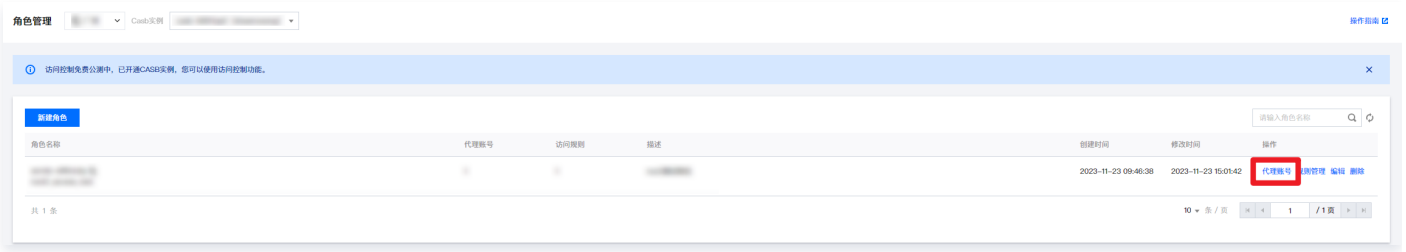
最近更新时间：2024-11-08 21:33:12

前提条件

- 需已 购买开通 CASB 实例 。
- 已创建代理账号，对于未创建代理账号，详情可查阅 创建代理账号 。
- 已创建访问规则，对于未创建规则，详情可查阅 创建访问规则 。

操作步骤

1. 登录 控制台，在左侧导航栏中，单击**访问控制** > **角色管理**。
2. 在角色管理页面，选择所需的地域、CASB 实例。
3. 在角色管理页面中，找到所需的角色，单击**代理账号**，弹出代理账号窗口。



4. 在代理账号窗口中，单击**添加账号**，选择该实例下的代理账号，单次最多支持添加10个账号，单击**确定**即可。

规则管理

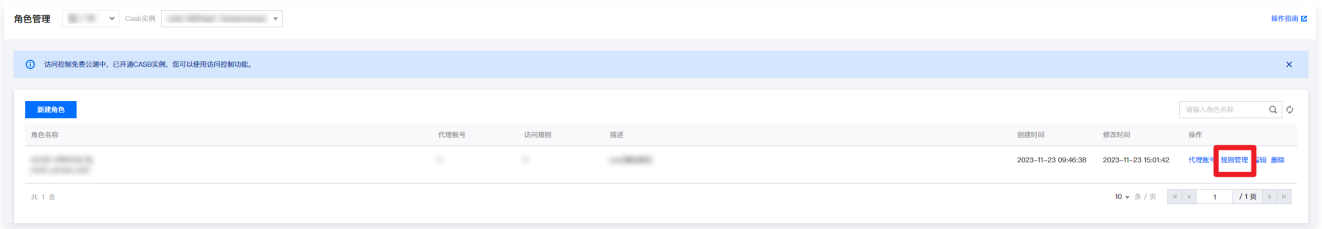
最近更新时间：2024-11-08 21:33:12

前提条件

- 需已 购买开通 CASB 实例 。
- 已创建代理账号，对于未创建代理账号，详情可查阅 创建代理账号 。
- 已创建访问规则，对于未创建规则，详情可查阅 创建访问规则 。

添加规则

1. 登录 控制台，在左侧导航栏中，单击**访问控制** > **角色管理**。
2. 在角色管理页面，选择所需的地域、CASB 实例。
3. 在角色管理页面中，找到所需的角色，单击**规则管理**。

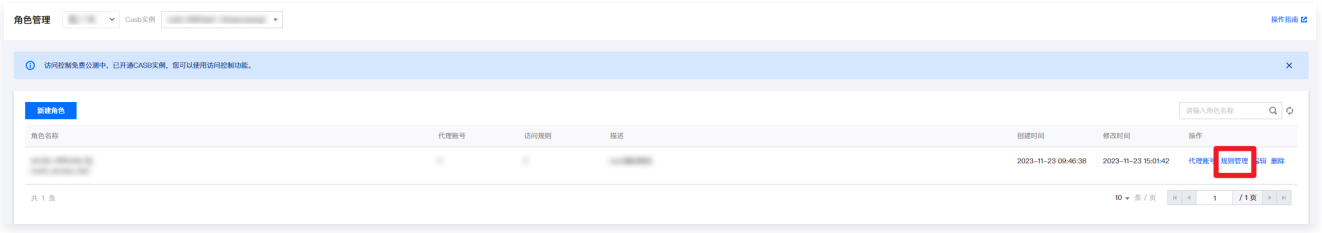


4. 在规则管理窗口中，单击**添加规则**，选择该实例下已创建好的访问规则，单击**确定**即可。

> **说明：**
> - 单次最多支持添加10个规则，新添加的规则顺序默认放置在最前面。
> - 单个角色最多支持绑定100条规则。

删除规则

1. 登录 控制台，在左侧导航栏中，单击**访问控制** > **角色管理**。
2. 在角色管理页面，选择所需的地域、CASB 实例。
3. 在角色管理页面中，找到所需的角色，单击**规则管理**。



4. 在规则管理窗口中，找到所需删除的规则，并单击其右侧的**删除**。

> **说明：**
> 排序：当配置了多个规则后，系统会按顺序匹配、逐一匹配，采纳最先匹配到的规则。当所有规则均没有匹配成功时，则默认为**放行** 。

5. 在“确认删除”窗口中，单击**确定**，即可完成删除操作。

删除角色

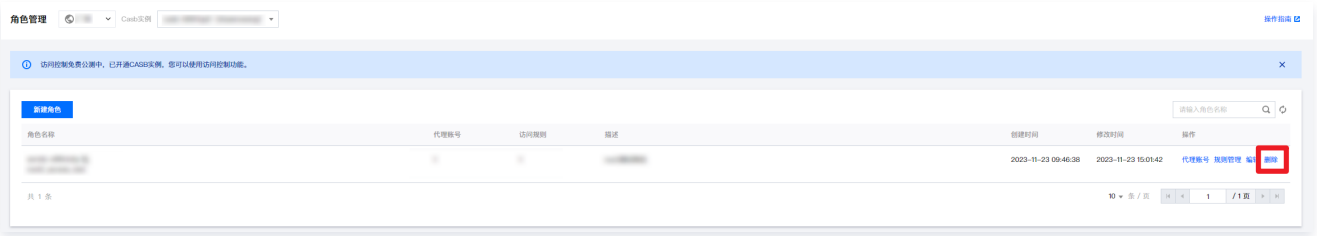
最近更新时间：2024-11-08 21:33:12

前提条件

- 需已 购买开通 CASB 实例 。
- 已创建代理账号，对于未创建代理账号，详情可查阅 创建代理账号 。
- 已创建访问规则，对于未创建规则，详情可查阅 创建访问规则 。

操作步骤

1. 登录 控制台 ，在左侧导航栏中，单击**访问控制** > **角色管理**。
2. 在角色管理页面，选择所需的地域、CASB 实例。
3. 在角色管理页面，找到所需的角色，单击**删除**。



4. 在“确认删除”窗口中，单击**确认**，即可完成删除的操作。

阻断日志

最近更新时间：2024-11-08 21:33:12

操作场景

阻断日志主要是展示所创建的阻断规则下的数据详情，可以从代理账号、数据库及规则三个维度进行筛选，目前只保留前7天的数据。

操作步骤

1. 登录 控制台，在左侧导航栏中，单击**访问控制** > **阻断日志**。
2. 在阻断日志页面，选择所需的地域、CASB 实例。
3. 在阻断日志页面，选择所需的代理账号、数据库账号及规则，单击**搜索**，即可查看对应的阻断日志详情。

> **说明：**
> - 阻断日志仅支持查询最近一周的日志。
> - 若同一个 CASB 实例短时间内有大量的阻断事件产生(超过100个/s)，无法查看超频部分的阻断日志。

运维监控
监控日志

最近更新时间：2024-11-08 21:33:12

数据安全网关（云访问安全代理，CASB）基于降低用户接入的难度、提高问题排查的正确率及速率，推出监控日志功能。监控日志功能方便用户您发现问题、快速定位问题，及能查看问题的具体详情，从而提升您的用户体验。

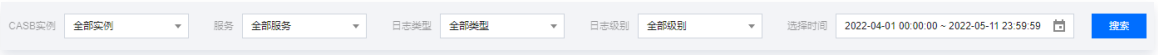
前提条件

需已 购买开通 CASB 实例 。

操作步骤

1. 登录 控制台，在左侧导航栏中，单击**运维监控** > **监控日志**。
2. 在监控日志页面，选择所需的地域。

3. 在监控日志页面，可以选择不同维度的条件（CASB 实例、日志级别、时间等）进行搭配，达到日志的精确筛选。



4. 筛选后，可查看监控日志的整体详情。

日志指标说明

日志级别说明

日志级别	处理方式
提示	无需处理
警告	部分数据库配置不合法，需要根据日志提示检查字段、数据库配置
错误	数据库写入错误数据，需要根据日志内容进行恢复
致命	系统部分功能不可用，需要 提交工单 进行处理

服务类型及日志类型

代理

- **数据截断：**数据库中保存了被截断的值。
  示例（SQL_MODE 未设置，数据被截断）：
  - 日志内容：
    `exce sql:[insert into score (cn) values ("123")]  warn message:[Data truncated for column 'cn' at row 1]` 。

> **说明：**

> score.cn 定义长度为2, 执行 sql：insert into score (cn) values ("123"). score.cn 未配置策略实际保存值为12，配置策略实际保存值为被**截断**的密文。

- 解决方法：用户可以根据日志 SQL 中记录的值进行数据恢复。建议 sql_mode 增加 STRICT_ALL_TABLES、STRICT_TRANS_TABLES。
- **加密失败：**数据库字段定义值小于密文值，数据保存明文。用户可以根据日志内容调整字段长度，然后执行全量加密任务。
  示例：
  - 日志内容：`db1.table1.field1 crypto length reach limit. columnSize:255, encryptValueSize:583` 。
  - 解决方法：字段长度小于密文, 将 db1.table1.field1 的字段长度调整为 583 。
- **SQL 不支持：**加密字段涉及不支持的操作，如：函数操作、数学运算、排序、正则查询等。
  示例：
  - 场景：SQL: [select * from score order by cipherColumn]; Message: [Casb: unsupported sql syntax: crypto field in order by]。
  - 解决方法：修改 SQL，不能对加密字段做排序操作。

加密

- **任务失败：** 记录数据库账号、安全组配置、数据库字段、策略变更等问题导致加解密任务执行失败。
  示例：
  - 日志内容：`Could not create connection to database server. Attempted reconnect 3 times. Giving up.` 。
  - 解决方法： 检查安全组配置，数据库用户名等是否正确。
- **分表匹配：**分表规则匹配到了新表，并复用了加解密规则。
  示例：
  日志内容：sharding policy match tables reuse [test.table1] crypto policy. DatabaseName:shard-9ZWD4ud4 sharding poicy:^table1\d{0,2}$ sharding pattern:test TableCount:2 TableName:table1,table112。

> **说明：**
> table112 复用了 table1 配置的规则，具有加密策略的字段写入时会被加密。

配置事件规则

最近更新时间：2024-11-08 21:33:12

业务接入数据安全网关（云访问安全代理，CASB）后，为了能及时的将 CASB 运行中产生的各类事件通知到您，CASB 会同步接入 腾讯云事件总线（EventBridge）。通过事件总线，您可以快速配置 CASB 数据加密失败、数据解密失败、数据脱敏失败等事件的接收、处理策略，便于快速发现、定位问题。本文为您介绍如何在事件总线控制台中新增 CASB 事件规则。

操作步骤

1. 登录 事件总线控制台，选择左侧导航栏中的**事件规则**。
2. 在事件规则页面，选择云服务事件集所属的**广州**地域及 **default** 事件集。

> **说明：**
> **云服务事件集：**接收全地域的腾讯云服务产生的监控事件与审计事件。

3. 在事件规则页面，单击**新建**。
4. 在事件模式页面中，根据页面提示填写相关信息，单击**下一步**。

参数名称	参数说明
事件模式	选择表单模式。
云服务类型	选择云访问安全代理。
事件类型	自主选择特定事件类型或全部事件类型。

5. 在事件目标窗口中，选择 CASB 事件触发后的处理方式，具体配置方法请参见：消息推送、CLS 日志、SCF 云函数、Ckafka。

6. 单击**完成**，即可完成 CASB 事件规则的配置。

> **说明：**

如需查询监控日志详情内容，可依据如下路径、操作指南进行查阅：

- CASB 事件详情，可访问 CASB 监控日志页面 查询。
- CASB 监控日志使用指南，详情请参见 监控日志 。