数据安全网关（云访问安全代理）

实践教程

腾讯云

文档目录

实践教程
数据加密

最近更新时间：2024-06-13 19:14:32

本文将为您介绍数据安全网关（云访问安全代理，CASB）的数据加密相关的实践经验和相关操作。

业务系统加密需求评估

接入 CASB 前，请先综合评估 CASB 提供的功能是否满足业务的加密需求。包括但不限于：

- 业务的数据库类型。CASB 支持 MySQL、PostgreSQL、MongoDB 类型的数据库。
- 业务存在哪些敏感字段。可使用 数据安全治理中心 定位敏感数据和分类分级。
- 敏感字段的类型。CASB 支持字符串类型的字段加密，详情请参见 字段支持情况 。
- 敏感字段的加密算法。CASB 支持国密 SM4和 AES 两种加密算法。
- 敏感字段的字段长度。CASB 字段加密后，密文长度有较大增长，数据库需变更 加密字段长度 。
- 涉及加密字段的 SQL 语法。CASB 使用代理模式，部分特性、语法等无法进行加密，详情请参见 功能支持和使用限制 。

使用场景

新业务接入

可参考 从0开始接入 CASB 进行业务接入。

> ⚠ 注意：
> 存量数据影响确认。
> - 配置了字段加解密策略后，通过代理查询加密字段数据时，代理会自动将应用查询的加密字段条件加密转换为密文，因此，通过代理无法查询到加密字段的明文数据。
> - 因接入过程中加密字段可能存在一段时间的明文（存量）、密文（增量）数据共存状态，若加密字段作为查询条件，可能导致查询数据不全，请确认此场景下的业务影响。

周期性任务接入

本场景介绍需要周期性执行数据加密/解密/明文统计/数据修复任务的业务如何操作。
例如：业务每天03:00会从外部导入明文数据到数据库，数据中存在敏感字段，导入后需自动对敏感数据进行加密。

1. 元数据绑定和表结构采集。
   可参考 从0开始接入 CASB 的步骤1和步骤2绑定元数据。
2. 配置周期性字段加密。
   2.1 确认字段长度是否满足密文存储需求。
   根据参考文档 密文长度计算，计算各字段中明文加密后的最大密文长度，若最大密文长度大于当前的字段长度定义，需调整字段长度大小。本例中各字段长度定义已足够存储密文，不对字段长度定义进行修改。

   > ⚠ 注意：
   > 长度变更后，需重新采集元数据表结构。

   2.2 配置字段加密策略。
   参考 创建策略 配置待加密字段的加密策略。
   2.3 配置周期性全量加密任务。
   参考 创建任务 文档，创建全量加密任务，任务首次执行时间为 `03:00` ，执行周期为 `24`小时 。

增量任务接入

本场景介绍需要增量执行数据加密/解密任务的业务如何操作。
例如：业务数据每天03:00需要将当天数据库中写入的明文数据加密，由于数据库数据量较大，全量加解密会全表扫描，随着数据量的增长影响性能；

1. 元数据绑定和表结构采集。
   可参考 从0开始接入 CASB 的步骤1和步骤2绑定元数据。

2. 配置周期性字段加密。

2.1 确认字段长度是否满足密文存储需求。

根据参考文档 密文长度计算，计算各字段中明文加密后的最大密文长度，若最大密文长度大于当前的字段长度定义，需调整字段长度大小。本例中各字段长度定义已足够存储密文，不对字段长度定义进行修改。

> ⚠ **注意：**
> 长度变更后，需重新采集元数据表结构。

2.2 配置字段加密策略。

参考 创建策略 配置待加密字段的加密策略。

2.3 配置周期性全量加密任务。

参考 创建任务 文档，创建数据加密任务，任务首次执行时间为 `03:00`，执行周期为 `24`小时 。

2.4 配置增量加解密字段

参考 创建任务 文档，创建数据加密任务，增量依据选择更新时间，并填写**增量依据字段**。

敏感即时脱敏，全局统一管控

最近更新时间：2025-05-13 15:18:11

数据安全网关（云访问安全代理）（Data Security Gateway（Cloud Access Security Broker），CASB）支持“全部数据脱敏”和“指定元数据脱敏”两种策略类型，本文将为您介绍使用“全部元数据脱敏策略”实现敏感数据发现即脱敏，一次配置全局管控脱敏的实践。

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。
		说明：
		实践操作参考 多应用差异化脱敏策略 。

接入场景

场景一：大量资产逐一配置策略，耗时耗力

- **核心痛点：**资产多且分散，逐个字段配置需数天甚至数月。
- **方案概述：**基于分类配置脱敏策略（如“手机号-遮盖”、“银行卡号-HASH”等），实现一次配置对全局所有敏感数据生效。
- **突出优势：**降低成本数百倍，策略配置时间缩短至分钟级。

场景二：敏感资产持续新增，存在防护空白期

- **核心痛点：**业务系统持续更新迭代，敏感数据分布不断变换，传统方案从“敏感识别”到“防护生效”存在一定时长，该阶段敏感资产处于防护空白期，易高敏数据泄漏，导致安全风险、合规风险泄。
- **方案概述：**持续自动化监控全局资产，识别敏感数据（如“身份证号”、“邮箱”等），识别结果自动触发动态脱敏策略生效，及时控制敏感数据访问时脱敏，仅限特定账号可访问明文。
- **突出优势：**敏感数据即时脱敏，避免过长的防护空白期。

前提条件

- 具备敏感识别资源：已 购买数据安全治理中心实例 。
- 具备数据脱敏资源：已 购买开通 CASB 实例 。

配置步骤

持续自动化识别数据分类分级

步骤一：配置分类分级模板

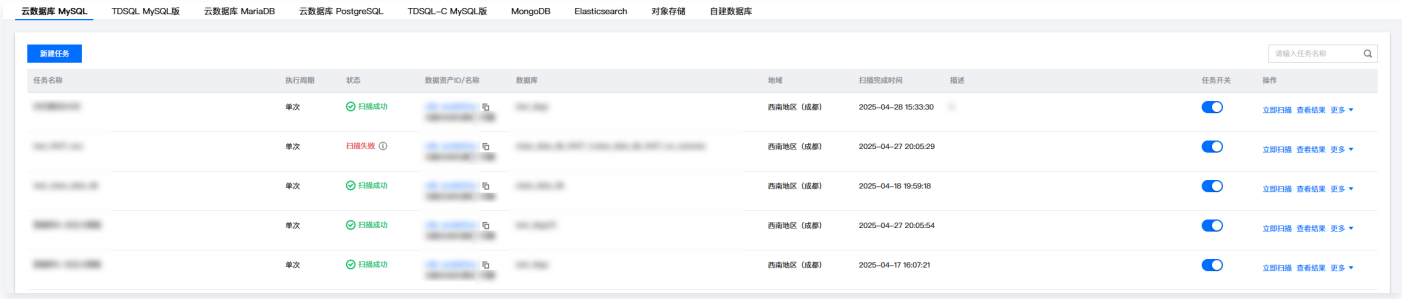
建立敏感数据 “识别标准”（定义分类、分级），为后续敏感数据识别与治理奠定基础。

1. 登录 数据安全治理中心控制台 。
2. 在左侧导航栏中，单击**分类分级 > 分类分级配置**。
3. 参考 分类分级模板配置 进行新建/导入模板。

步骤二：定期执行分类分级任务

全面梳理敏感资产，持续动态发现敏感数据，解决 “数据资产不清晰” 问题，避免新增敏感字段无感知。

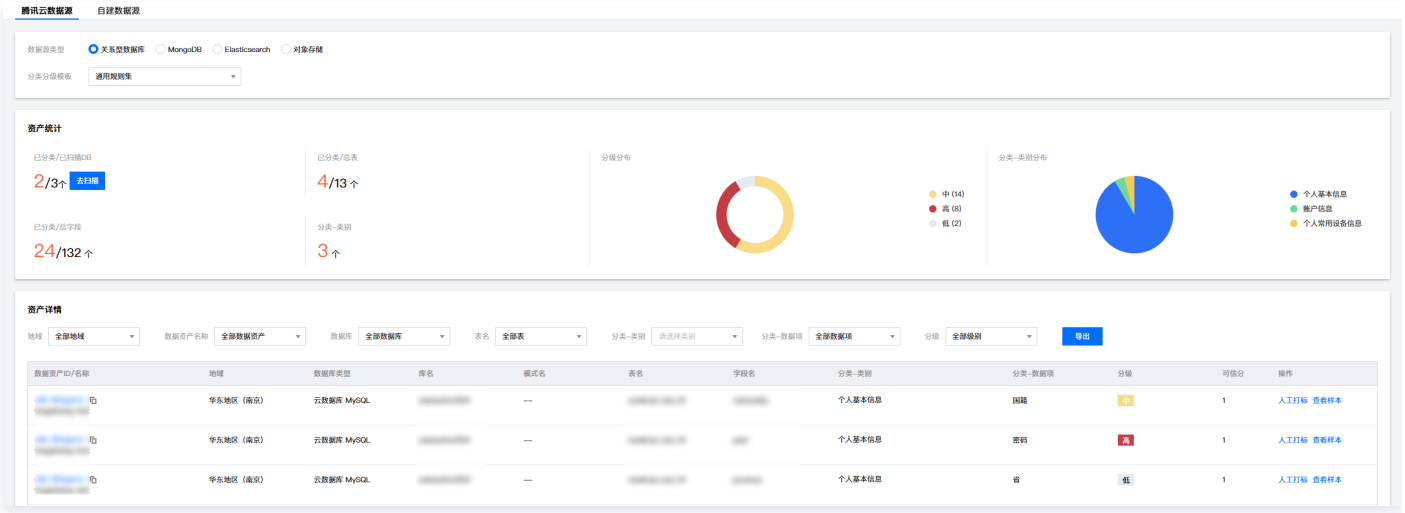
1. 登录 数据安全治理中心控制台 。
2. 在左侧导航栏中，单击**分类分级 > 分类分级任务**。
3. 参考 分类分级任务 进行分类分级任务的新建。



步骤三：分类分级结果查看与手动调整

人工矫正识别结果，可修正自动化识别误差（约 5%–10% 的模糊场景），确保分类分级结果贴合业务实际情况。

1. 登录 数据安全治理中心控制台 。
2. 在左侧导航栏中，单击**分类分级 > 敏感数据资产**。
3. 在敏感数据资产页面，您可以查看指定数据库、表的敏感数据详情，同时也支持按照不同的分类、分级进行敏感数据的筛选。
4. 单击**查看样本**，可随机展示该字段的抽样数据信息，您可以依据抽样数据进行识别结果的判断。
5. 对误判字段（如 “普通编号” 被误标为 “身份证号”），您可以单击人工打标，对该字段进行识别结果的修改。

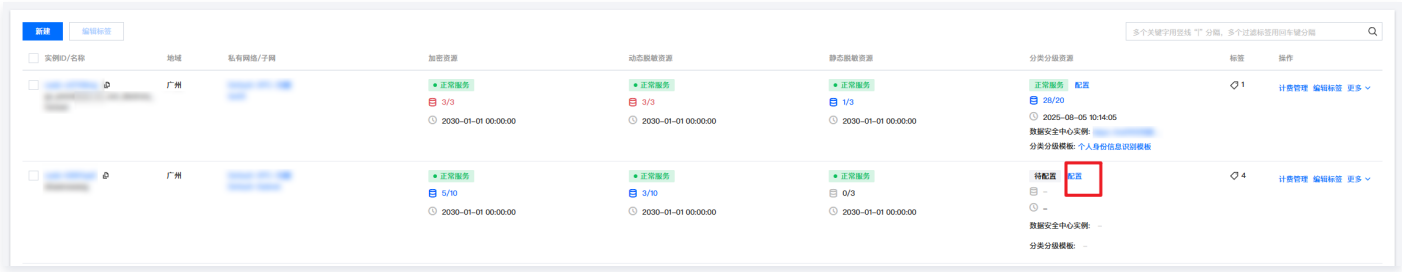


预设脱敏策略规范

步骤一：脱敏资源关联分类分级资源

指定识别资源与脱敏资源的关联关系，解决 “识别和防护断层” 问题，实现 “识别结果直接驱动防护策略”。

1. 登录 数据安全网关控制台，在左侧导航栏中，单击**实例 > 实例列表**。
2. 根据脱敏资源，单击其对应分类分级资源列的**配置**按钮。



3. 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。更多操作详情参考 分类分级资源管理。

步骤二：配置动态脱敏模板

基于企业安全规范，针对“分类-数据项”配置脱敏规则，在脱敏策略选用脱敏模版即可实现该分类所有字段都统一应用该算法，解决 “同一分类不同字段重复配置策略” 问题。

1. 登录 数据安全网关控制台，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，参考 脱敏模板配置，完成模板的创建。

步骤三：配置脱敏策略

配置“全部元数据脱敏”策略，实现策略对全局数据源、账号生效，避免“不同资产需逐一配置策略”问题，实现新增资产默认纳入管控。

1. 登录 数据安全网关控制台，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，参考 新建脱敏策略，完成“全部元数据脱敏”策略的创建。

验证测试

通过以上配置，企业实现 **“分类分级识别→脱敏策略生效” 的自动化流程，从根本上解决传统方案中 “重复配置、策略不一致、防护滞后” 的问题**，尤其适合拥有海量数据字段（万级以上）的金融、医疗、政务等行业，策略管理**成本显著降低**，同时依托腾讯云内置模型和算法保障方案的安全性与合规性。

测试用例1：指定脱敏账号查询敏感数据（存量数据验证）

1. 通过 SQL 客户端（如 Navicat/MySQL Workbench）连接 CASB 代理地址，使用指定代理账号执行查询；
2. 查看查询结果是否符合脱敏模板配置（如中间字段被星号替换）；
3. 使用普通账号（非代理账号）执行相同查询，确认敏感字段显示明文（未被错误脱敏），确保策略仅对目标账号生效。

测试用例2：新增表与敏感数据动态脱敏验证（增量数据验证）

1. 在数据库中创建新表，并添加不同分类分级的字段；
2. 在 DSGC 控制台手动启动或等待定期扫描任务（如步骤 2 配置的 “定期执行分类分级任务”），识别新增表和字段；
3. 通过 SQL 客户端（如 Navicat/MySQL Workbench）连接 CASB 代理地址，使用指定代理账号执行查询新增的字段；
4. 查看查询结果是否符合脱敏模板配置（如中间字段被星号替换）

常见问题

测试账号查询结果未脱敏（显示明文）如何进行排查?

1. 检查 DSGC 分类分级结果中，该字段是否正确标记为敏感数据；
2. 检查 CASB 脱敏模板中是否为该字段所命中的分类数据项配置脱敏算法；
3. 确认 CASB 动态脱敏策略中该账号是否被正确纳入脱敏范围；
4. 查看 CASB 策略优先级，确保优先级高于 “其他脱敏策略”。

新增字段未触发脱敏如何进行排查?

1. 确认 DSGC 扫描任务已包含新表，可以重新连接数据源，以同步最新的表结构信息；
2. 确认 CASB 中，该数据源的表结构信息已同步。可参考 元数据表结构管理，手动同步元数据表结构信息。

多应用差异化脱敏策略

最近更新时间：2025-05-13 15:18:11

数据安全网关（云访问安全代理）（Data Security Gateway（Cloud Access Security Broker），CASB）支持“全部数据脱敏”和“指定元数据脱敏”两种策略类型，本文将为您介绍使用“指定元数据脱敏策略”实现多个应用使用不同数据脱敏策略的实践。

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。 **说明：** 实践操作参考 敏感即时脱敏，全局统一管控 。
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。

接入场景

不同的应用访问同一份已加密的敏感数据，需返回不同方式处理的脱敏数据。
示例：

- 表 `userinfo` 中存在两个已加密的敏感字段 `name` 和 `phone` 。
- 存在三个应用：
  - `user1` ：核心系统，能访问所有的明文数据。
  - `user2` ：对外展示，仅能使用脱敏后的数据。
  - `user3` ：人员核对，需要获取 `name` 字段的信息。

步骤1：接入准备和数据库绑定

参考 从0开始接入 CASB 步骤1、步骤2, 绑定数据库到 CASB 代理。

说明
本示例中，代理的地址是 `172.16.0.30:10100` ，数据库的地址是 `172.16.32.4:3306` 。

步骤2：创建代理账号

CASB 的脱敏策略和代理账号相关联，因此，参考 代理账号管理 为三个应用分别创建三个不同的代理账号：`user1`、`user2` 和 `user3`。

步骤3：配置字段的加密策略，并对数据进行加密（可选）

参考 从0开始接入 CASB 步骤3，对敏感字段配置加密策略并加密。

> **说明**
> 数据脱敏对明文或密文均可生效，非加密的字段也可以配置数据脱敏。

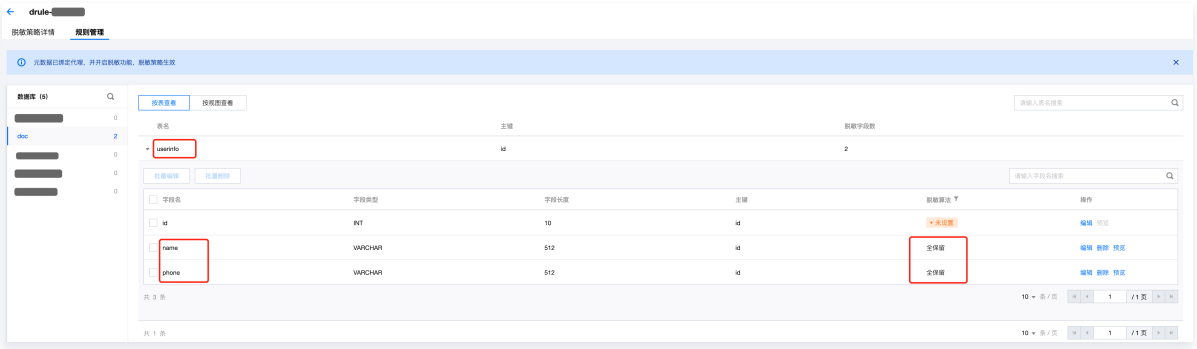
步骤4：配置脱敏策略

1. 为 `user1` 配置指定元数据敏策略。

> **说明**
> 若未配置全部元数据脱敏策略，也未给代理账号配置指定元数据脱敏策略，账号查询数据返回明文。

1.1 新建脱敏策略：参考 创建指定元数据脱敏策略，为 `user1` 创建指定元数据脱敏策略。

1.2 设置脱敏规则：参考 脱敏规则管理，为 `name` 和 `phone` 字段设置 全保留 脱敏算法。

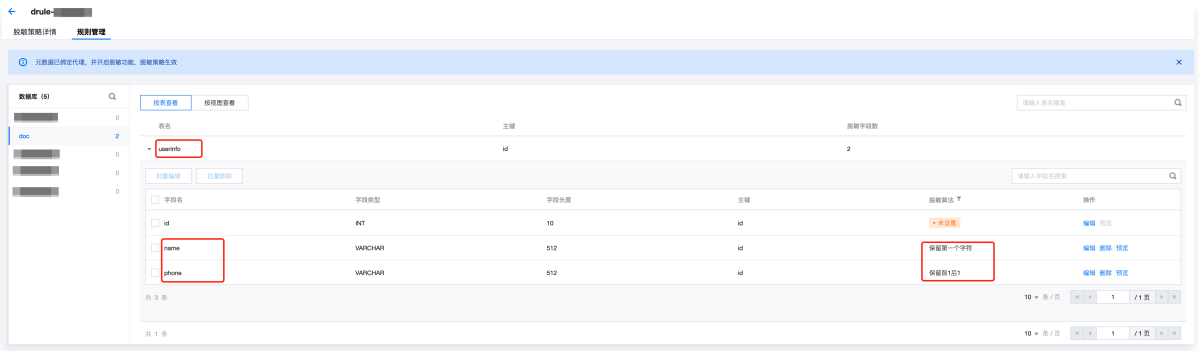


2. 配置 `user2` 的脱敏策略。

2.1 新建脱敏策略：参考 创建指定元数据脱敏策略，为 `user2` 创建指定元数据脱敏策略。

2.2 设置脱敏规则：参考 脱敏规则管理，为 `name` 字段设置 保留第一个字符 脱敏算法，为 `phone` 字段设置 保留前1后1 脱敏算法。

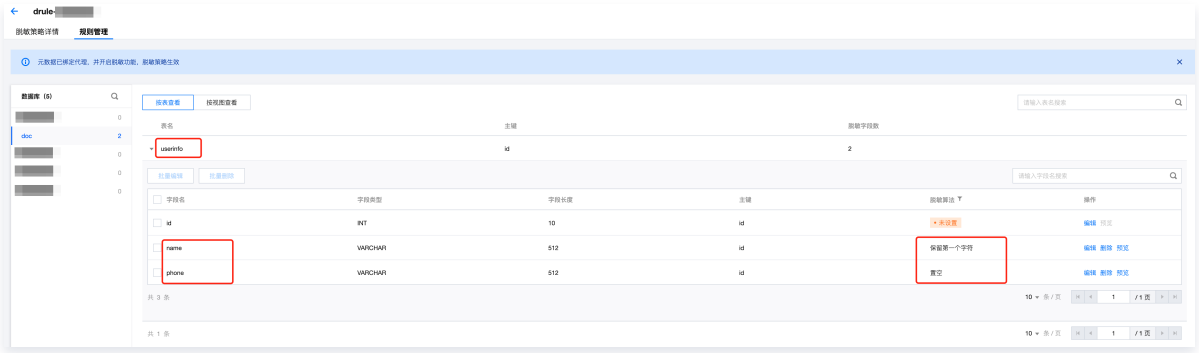
> **说明**
> 若内置算法无法满足业务需求，可 自定义脱敏算法。



3. 配置 `user3` 的脱敏策略。

3.1 新建脱敏策略：参考 **创建指定元数据脱敏策略**，为 `user3` 创建指定元数据脱敏策略。

3.2 设置脱敏规则：参考 **脱敏规则管理**，为 `name` 字段设置 **保留第一个字符** 脱敏算法，为 `phone` 字段设置 **置空** 脱敏算法。



步骤4：验证脱敏效果

1. 直连数据库查询，数据库内为密文。

```
[root@VM-32-33-centos ~]# mysql -h172.16.32.4 -P3306 -uroot -p --default-character-set=utf8 doc -A
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 19768797
Server version: 8.0.22-txsql 20211202

Copyright (c) 2000, 2021, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> select * from userinfo;
+----+-----------------------------------------------+-----------------------------------------------+
| id | name                                          | phone                                         |
+----+-----------------------------------------------+-----------------------------------------------+
|  1 | ADSfv+0mHffLLroX3UuuiPuD43c9K3tk4Lic+w==|^| | PN5X0qkmrZCPZSXHKG5X4MJaVg==|^|
|  2 | kA9TZaSNnFY+wtwb3kil5pOF5XE7LX1i5r6a/Q==|^| | O9tc36whqMzWbSMq1v7seDpZ6A==|^|
+----+-----------------------------------------------+-----------------------------------------------+
2 rows in set (0.01 sec)
```

2. 使用 `user1` 连接代理查询，`name` 和 `phone` 均返回明文。

```
[root@VM-32-33-centos ~]# mysql -h172.16.0.30 -P10100 -uuser1 -p --default-character-set=utf8 doc -A
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 10003
Server version: 5.7.18-txsql-log-casb-proxy 20211202

Copyright (c) 2000, 2021, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> select * from userinfo;
+----+-------+---------+
| id | name  | phone   |
+----+-------+---------+
|  1 | Alice | 1234567 |
|  2 | Bob   | 6789012 |
+----+-------+---------+
2 rows in set (0.00 sec)
```

3. 使用 `user2` 连接代理查询，`name` 和 `phone` 均返回脱敏后数据。

```
[root@VM-32-33-centos ~]# mysql -h172.16.0.30 -P10100 -uuser2 -p --default-character-set=utf8 doc -A
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 10015
Server version: 5.7.18-txsql-log-casb-proxy 20211202

Copyright (c) 2000, 2021, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> select * from userinfo;
+----+-------+---------+
| id | name  | phone   |
+----+-------+---------+
|  1 | A**** | 1*****7 |
|  2 | B**   | 6*****2 |
+----+-------+---------+
2 rows in set (0.01 sec)
```

4. 使用 `user3` 连接代理查询，`name` 返回脱敏后数据，`phone` 返回空。

```
[root@VM-32-33-centos ~]# mysql -h172.16.0.30 -P10100 -uuser3 -p --default-character-set=utf8 doc -A
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 10003
Server version: 5.7.18-txsql-log-casb-proxy 20211202

Copyright (c) 2000, 2021, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> select * from userinfo;
+----+-------+-------+
| id | name  | phone |
+----+-------+-------+
|  1 | A**** |       |
|  2 | B**   |       |
+----+-------+-------+
2 rows in set (0.00 sec)
```

访问控制

最近更新时间：2023-10-08 17:37:26

CASB 访问控制使用基于角色的访问控制（RBAC）来控制代理账号的访问权限，可以根据客户端 IP、访问的库、表、字段、命令、时间等维度控制不同的角色的访问权限。
CASB 的访问控制独立于数据库的权限系统，CASB 访问控制基于 CASB 代理账号，数据库权限管理适用于元数据账号，互相独立、互为补充。

接入场景

本示例使用 CASB 访问控制功能配置不同角色的应用访问代理的权限。示例：

- `doc` 数据库中表 `userinfo` 内存在两个敏感字段 `name` 和 `phone` 。
- 只允许来自 `172.16.32.33` 机器的访问。
- 存在四个角色的应用：
  - `admin` ：管理员角色，能读写 `name` 和 `phone` 。
  - `reader` ：只读角色，只能读 `name` 和 `phone` 。
  - `nameadmin` ：姓名校验角色，可以读写 `name` 字段。
  - `cronjob` ：定时任务角色，只允许每天 `10:00~10:30` 时间段内读 `name` 字段。

步骤一：接入准备和数据库绑定

参考 从0开始接入 CASB 步骤1、步骤2, 绑定数据库到 CASB 代理。

> **说明：**
> 本示例中，代理的地址是 `172.16.0.30:10100` ，数据库的地址是 `172.16.32.4:3306` 。

步骤二：创建代理账号

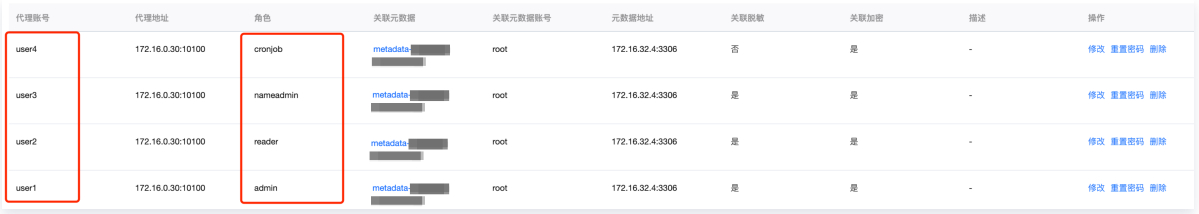
CASB 的访问控制角色和代理账号相关联，因此，参考 代理账号管理 为四个不同角色的应用分别创建四个不同的代理账号： `user1` 、 `user2` 、 `user3` 和 `user4` 。

步骤三：创建和绑定访问控制角色

1. 创建 `admin` 、 `reader` 、 `nameadmin` 和 `cronjob` 的角色。
   参考 访问控制角色管理，新增 `admin` 、 `reader` 、 `nameadmin` 和 `cronjob` 四个角色。

2. 绑定代理账号和角色。
   参考 添加代理账号，分别将代理账号绑定到角色。
   - 代理账号 `user1` 绑定角色 `admin` 。
   - 代理账号 `user2` 绑定角色 `reader` 。
   - 代理账号 `user3` 绑定角色 `nameadmin` 。
   - 代理账号 `user4` 绑定角色 `cronjob` 。

> **说明**
> 一个代理账号只能绑定一个角色。



代理账号	代理地址	角色	关联元数据	关联元数据账号	元数据地址	关联脱敏	关联加密	描述	操作
user4	172.16.0.30:10100	cronjob	metadata-	root	172.16.32.4:3306	否	是	-	修改 重置密码 删除
user3	172.16.0.30:10100	nameadmin	metadata-	root	172.16.32.4:3306	是	是	-	修改 重置密码 删除
user2	172.16.0.30:10100	reader	metadata-	root	172.16.32.4:3306	是	是	-	修改 重置密码 删除
user1	172.16.0.30:10100	admin	metadata-	root	172.16.32.4:3306	是	是	-	修改 重置密码 删除

步骤四：创建和绑定访问控制规则

1. 创建访问控制规则

参考 访问控制规则管理，创建访问控制规则。

规则名称	规则来源	关联角色	规则描述	操作
acrule- rule_allow_client	自定义	0	放行指定IP所有操作	编辑 删除
acrule- rule_allow_client_rd	自定义	0	放行指定IP SELECT	编辑 删除
acrule- rule_allow_client_name_cron_rd	自定义	0	放行指定IP固定时间读name字段	编辑 删除
acrule- rule_allow_client_name_rw	自定义	0	放行指定IP读写name字段	编辑 删除
acrule- rule_deny_phone	自定义	0	禁止访问phone字段	编辑 删除
acrule- rule_deny_all	自定义	0	阻断所有访问语句	编辑 删除

- `rule_deny_all`：阻断所有访问语句。

- `rule_deny_phone`：阻断访问 `phone` 字段的语句。

- `rule_allow_client`：放行来自 `172.16.32.33` 机器的语句。

- `rule_allow_client_rd`：放行来自 `172.16.32.33` 机器的 `SELECT` 语句。

- `rule_allow_client_name_rw`：放行来自 `172.16.32.33` 机器、`name` 字段的 `SELECT`、`UPDATE` 语句。

- `rule_allow_client_name_cron_rd`：放行来自 `172.16.32.33` 机器、`20:00~21:00` 时间段内、`name` 字段的 `SELECT` 语句。

2. 配置角色的访问控制规则

注意：

- CASB 访问控制规则采用顺序匹配的方式，匹配到任意一条规则时结束匹配（放行或阻断）。因此，对于部分允许的需求，应先设置相反的禁止访问规则，即本例中若只允许访问 `name` 字段，应先配置禁止访问 `phone` 的规则，此时先匹配到阻断规则后可立即阻断。
- 若需要限制部分访问，角色规则中包含放行规则时，应在最后加上 `阻断所有请求` 的规则，阻断所有放行规则外的请求。

参考 角色规则管理，为每种角色配置规则。

规则名称	说明
`admin` 角色规则	`admin` 角色按如下顺序配置两条规则。 • `rule_allow_client`：放行来自 `172.16.32.33` 机器的语句。 • `rule_deny_all`：阻断所有访问语句。
`reader` 角色规则	`reader` 角色按如下顺序配置两条规则。 • `rule_allow_client_rd`：放行来自 `172.16.32.33` 机器的 `SELECT` 语句。 • `rule_deny_all`：阻断所有访问语句。
`nameadmin` 角色规则	`nameadmin` 角色按如下顺序配置三条规则。 • `rule_deny_phone`：阻断访问 `phone` 字段的语句。 • `rule_allow_client_name_rw`：放行来自 `172.16.32.33` 机器、`name` 字段的 `SELECT`、`UPDATE` 语句。 • `rule_deny_all`：阻断所有访问语句。
`cronjob` 角色规则	`cronjob` 角色按如下顺序配置三条规则。 • `rule_deny_phone`：阻断访问 `phone` 字段的语句。 • `rule_allow_client_name_cron_rd`：放行来自 `172.16.32.33` 机器、`20:00~21:00` 时间段内、`name` 字段的 `SELECT` 语句。 • `rule_deny_all`：阻断所有访问语句。

3. 效果验证

1. 绑定 `admin` 角色的代理账号 `user1`：可以读写所有字段。

```
[root@VM-32-33-centos ~]# mysql -h172.16.0.30 -P10100 -uuser1 -p --default-character-set=utf8 doc -A
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 10005
Server version: 5.7.18-txsql-log-casb-proxy 20211202

Copyright (c) 2000, 2021, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> select * from userinfo;
+----+-------+---------+
| id | name  | phone   |
+----+-------+---------+
|  1 | Alice | 1234567 |
|  2 | Bob   | 6789012 |
+----+-------+---------+
2 rows in set (0.00 sec)

mysql> update userinfo set phone='1234567' where id=1;
Query OK, 0 rows affected (0.00 sec)
Rows matched: 1  Changed: 0  Warnings: 0
```

1

2

2. 绑定 `reader` 角色的代理账号 `user2`：可以读所有字段，不能写字段值。

```
[root@VM-32-33-centos ~]# mysql -h172.16.0.30 -P10100 -uuser2 -p --default-character-set=utf8 doc -A
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 10019
Server version: 5.7.18-txsql-log-casb-proxy 20211202

Copyright (c) 2000, 2021, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> select * from userinfo;
+----+-------+---------+
| id | name  | phone   |
+----+-------+---------+
|  1 | Alice | 1234567 |
|  2 | Bob   | 6789012 |
+----+-------+---------+
2 rows in set (0.00 sec)

mysql> update userinfo set phone='1234567' where id=1;
ERROR 60041 (HY000): Casb: query denied by access control rule 'acrule-n62plujg'
mysql>
```

1

2

3. 绑定 `nameadmin` 角色的代理账号 `user3`：可以读写 `name` 字段，不能读写 `phone` 字段。

```
[root@VM-32-33-centos ~]# mysql -h172.16.0.30 -P10100 -uuser3 -p --default-character-set=utf8 doc -A
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 10005
Server version: 5.7.18-txsql-log-casb-proxy 20211202

Copyright (c) 2000, 2021, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> select * from userinfo;
ERROR 60041 (HY000): Casb: query denied by access control rule 'acrule-o5vhqmk0'
mysql> select name from userinfo;
+-------+
| name  |
+-------+
| Alice |
| Bob   |
+-------+
2 rows in set (0.00 sec)

mysql> update userinfo set phone='1234567' where id=1;
ERROR 60041 (HY000): Casb: query denied by access control rule 'acrule-o5vhqmk0'
mysql> update userinfo set name='Alice' where id=1;
Query OK, 0 rows affected (0.00 sec)
Rows matched: 1  Changed: 0  Warnings: 0

mysql> delete from userinfo where id=1;
ERROR 60041 (HY000): Casb: query denied by access control rule 'acrule-n62plujg'
mysql>
mysql> exit
```

1

2

3

4

5

4. 绑定 `cronjob` 角色的代理账号 `user4`：仅可以在规定的时间内读 `name` 字段，不能写字段。

```
[root@VM-32-33-centos ~]# mysql -h172.16.0.30 -P10100 -uuser4 -p --default-character-set=utf8 doc -A
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 10007
Server version: 5.7.18-txsql-log-casb-proxy 20211202

Copyright (c) 2000, 2021, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> select curtime();
+-----------+
| CURTIME() |
+-----------+
| 10:29:41  |
+-----------+
1 row in set (0.00 sec)

mysql> select * from userinfo;
ERROR 60041 (HY000): Casb: query denied by access control rule 'acrule-o5vhqmk0'
mysql> select name from userinfo;
+-------+
| name  |
+-------+
| Alice |
| Bob   |
+-------+
2 rows in set (0.00 sec)

mysql> update userinfo set name='Alice' where id=1;
ERROR 60041 (HY000): Casb: query denied by access control rule 'acrule-n62pluiq'
mysql> select curtime();
+-----------+
| CURTIME() |
+-----------+
| 10:30:23  |
+-----------+
1 row in set (0.00 sec)

mysql> select name from userinfo;
ERROR 60041 (HY000): Casb: query denied by access control rule 'acrule-n62pluiq'
```

1
2
3
4

步骤五：访问控制和安全组限制来源 IP 区别

- 访问控制限制来源IP在代理的应用层内实现，代理在收到客户端数据库查询语句时，检查客户端连接的来源 IP，并进行规则匹配，会占用代理的计算资源。
- 安全组限制来源 IP 在 VPC 网络层实现，不符合安全组规则的来源 IP 无法建立到代理的连接，不会占用代理的计算资源。

> **说明：**
> 如需从全局限制访问 CASB 代理的客户端应用连接代理，建议通过 配置 CASB 安全组 的方式，在网络入口侧进行拦截。

MySQL BINLOG 数据解密同步

最近更新时间：2024-06-14 14:13:01

MySQL BINLOG 是 MySQL 记录数据修改操作的二进制文件，数据库开启 BINLOG后，第三方组件（如 Canal，Flink-CDC）可以从数据库的 BINLOG 中增量获取数据的修改记录，实现数据的增量订阅。
数据库使用 CASB 方式配置加密后，明文数据经过代理后加密成密文，密文数据直接写入数据库，与此同时，BINLOG 存储密文到日志。因此，使用 BINLOG 直接订阅数据库时，同步订阅到的数据为密文。

CASB BINLOG 解密

CASB 支持根据当前配置的加密策略解密 BINLOG 日志数据，第三方组件可将订阅源由数据库变更 CASB 代理，由 CASB 代理解密 BINLOG 中的密文数据。

- 支持的订阅协议：
  - COM_BINLOG_DUMP
  - COM_BINLOG_DUMP_GTID
- 支持的事件类型：
  - WRITE_ROWS_EVENTv1
  - UPDATE_ROWS_EVENTv1
  - DELETE_ROWS_EVENTv1
  - WRITE_ROWS_EVENTv2
  - UPDATE_ROWS_EVENTv2
  - DELETE_ROWS_EVENTv2
  - WRITE_ROWS_COMPRESSED_EVENT_V1
  - UPDATE_ROWS_COMPRESSED_EVENT_V1
  - DELETE_ROWS_COMPRESSED_EVENT_V1
- 支持的压缩算法类型
  - zlib

使用限制

- 访问代理的代理账号必须为 `casb_binlogdump`，代理账号绑定的元数据账号必须有获取数据库 BINLOG 权限。
- `binlog_format` 格式必须为 `ROW` 。
- 访问代理的连接字符集必须为 `utf8` 或 `utf8mb4` 。
- 仅支持根据当前配置的加密策略解密数据。
- 不支持对 BINLOG 数据使用脱敏和访问控制策略。

常见问题

1. **两个数据库间已配置主从关系并使用 BINLOG 同步数据，主数据库接入 CASB 后，从数据库使用 BINLOG 协议连接 CASB，同步明文数据异常。**
   BINLOG 数据经过 CASB 代理解密后，明文相较于密文变短，导致 MySQL 从库的 Read_Master_log_Pos 和 Exec_Master_Log_Pos 不一致，导致同步失败。从库数据的解密请使用 CASB 主从同步功能 。
2. **加密策略修改或删除后，存量的 BINLOG 数据无法解密。**
   仅支持根据当前配置的加密策略解密数据，历史已加密的 BINLOG 数据根据当前策略无法解密时，将保留密文。
3. **表结构变更，变更前的存量 BINLOG 数据无法解密。**
   表结构变更后，CASB 的表结构和 BINLOG 历史数据的表结构不一致。若数据库参数 `binlog_row_metadata` 未设置为 FULL，BINLOG 事件仅记录各字段数据，不记录各字段名，CASB 无法识别 BINLOG中 数据对应的加解密策略信息，导致无法解密历史数据。
4. **表结构变更，变更后的增量 BINLOG 数据无法解密。**
   直连数据库变更表结构后，若未及时在 CASB 同步表结构，CASB 的表结构仍为旧值，和 BINLOG 增量数据的结构不一致。若数据库参数 `binlog_row_metadata` 未设置为 FULL，BINLOG 事件仅记录各字段数据，不记录各字段名，CASB 无法识别 BINLOG 中数据对应的加解密策略信息，导致无法解密新增的数据。

表结构变更实践教程

为了解决表结构变更导致的 BINLOG 数据无法解密的问题，可采用以下两种方案。

配置数据库参数（推荐）

配置数据库参数 `binlog_row_metadata` 为 `FULL`，将字段信息记录到 BINLOG 中，CASB 会根据字段信息解析和应用字段的加解密策略。
使用此方案时，需数据库支持此参数，且会造成 BINLOG 占用空间变大。

业务侧手动变更

业务侧需支持 BINLOG 数据处理的幂等性，即支持从某个位置重新处理所有 BINLOG 数据。

- 记录表结构变更前的最后 BINLOG 位置信息。
- 变更和同步表结构。
  - 通过代理变更表结构（自动触发 CASB 表结构采集任务）。
  - 直连 DB 变更表结构后，手动在 CASB 控制台更新表结构。
- 配置同步工具，从变更前的最后 BINLOG 位置重新同步。

取消接入 CASB

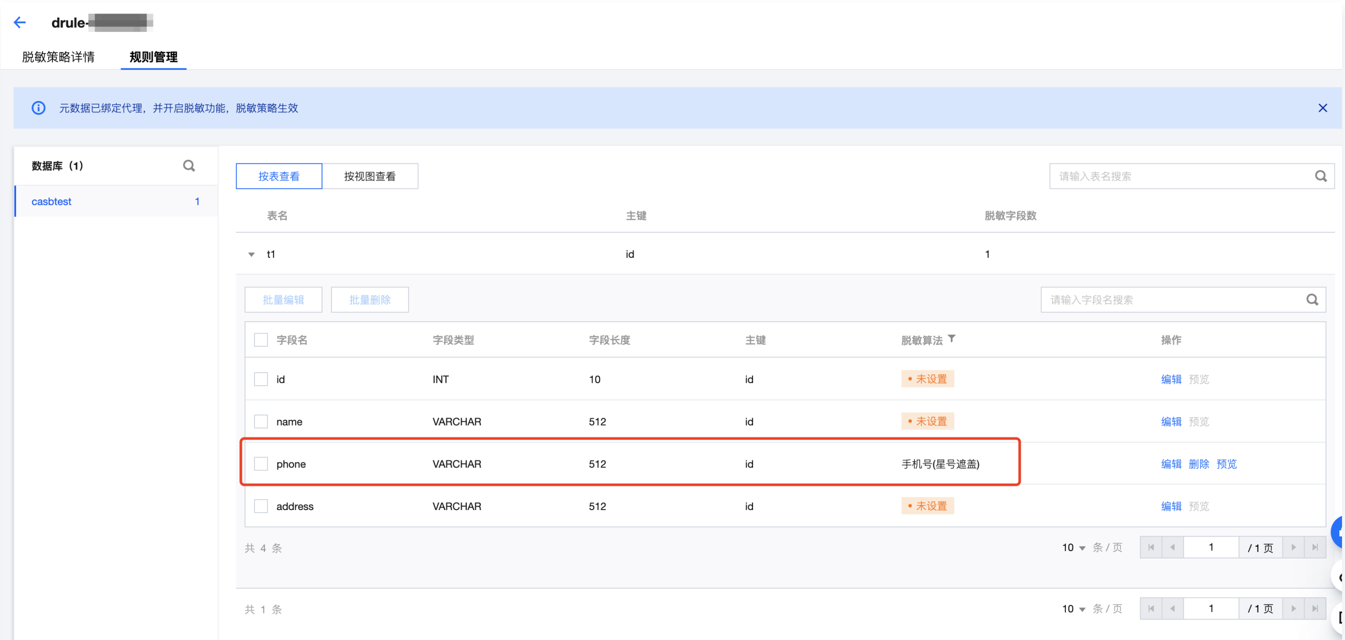
最近更新时间：2024-12-09 17:04:42

本文以已绑定到代理、存在加密数据的 MySQL 元数据为例，介绍如何解除绑定和删除元数据。

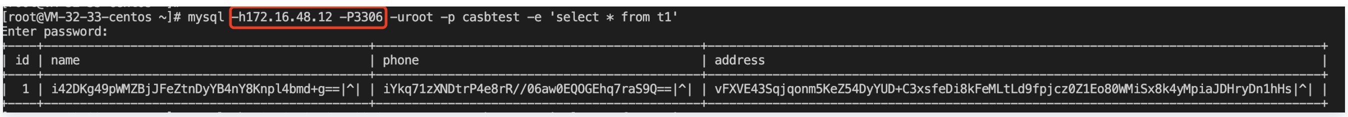
元数据配置现状

- `casbtest` 库下 `t1` 表中存在三个敏感字段 `name` 、 `phone` 和 `address` 。
- 数据库地址为 `172.16.48.12:3306` ，已绑定的代理地址为 `172.16.0.30:10101` 。
- 数据库中的三个敏感字段 `name` 、 `phone` 和 `address` 已使用 CASB 代理配置加密。

- 针对代理账号 `root` ， `phone` 字段上已配置脱敏规则。



- 数据库中存在已通过 CASB 加密后的数据。
  - 直连数据库查询：所有敏感字段已加密。



  - 通过代理查询： `phone` 字段已脱敏，其余字段自动解密为明文。

```
[root@VM-32-33-centos ~]# mysql -h172.16.0.30 -P10101 -uroot -p  casbtest -e 'select * from t1'
Enter password:
+----+--------+--------------+-----------------------------------------+
| id | name   | phone        | address                                 |
+----+--------+--------------+-----------------------------------------+
|  1 | 张三   | 188****8888 | 广东省深圳市南山区深南大道10000号       |
+----+--------+--------------+-----------------------------------------+
```

步骤1：设置敏感字段加密策略的工作模式

1. 参考 策略管理，将敏感字段的工作模式设置为**读解密，写不加密**。

2. 通过代理写入增量数据时，可以正常写入明文数据；通过代理读取时，可以正常解密和脱敏所有数据。

```
[root@VM-32-33-centos ~]# mysql -h172.16.0.30 -P10101 -uroot -p  casbtest -e "insert into t1 value(2, "李四", "16666666666", "上海市徐汇区田林路397号")
Enter password:
[root@VM-32-33-centos ~]# mysql -h172.16.0.30 -P10101 -uroot -p  casbtest -e 'select * from t1'
Enter password:
+----+--------+--------------+-----------------------------------------+
| id | name   | phone        | address                                 |
+----+--------+--------------+-----------------------------------------+
|  1 | 张三   | 188****8888 | 广东省深圳市南山区深南大道10000号       |
|  2 | 李四   | 166****6666 | 上海市徐汇区田林路397号                 |
+----+--------+--------------+-----------------------------------------+
```

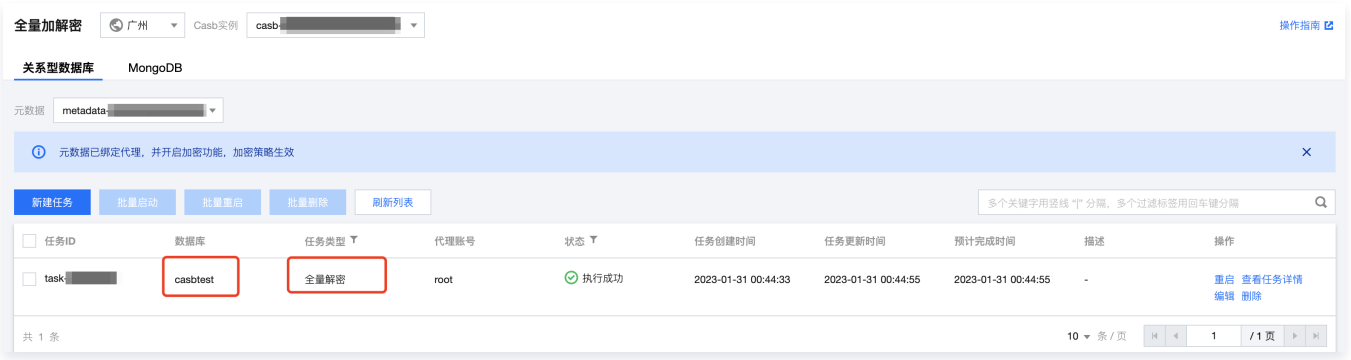
3. 直连 DB 查询，代理写入的增量数据为明文存储。

```
[root@VM-32-33-centos ~]# mysql -h172.16.48.12 -P3306 -uroot -p casbtest -e 'select * from t1'
Enter password:
+----+------------------------------------------+------------------------------------------+------------------------------------------+
| id | name                                     | phone                                    | address                                  |
+----+------------------------------------------+------------------------------------------+------------------------------------------+
|  1 | i42DKg49pWMZBjJFeZtnDyYB4nY8Knpl4bmd+g==|^| iYkq71zXNDtrP4e8rR//06aw0EQOGEhq7raS9Q==|^| vFXVE43Sqjqonm5KeZ54DyYUD+C3xsfeDi8kFeMLtLd9fpjcz0Z1Eo80WMiSx8k4yMpiaJDHryDn1hHs|^|
|  2 | 李四                                     | 16666666666                              | 上海市徐汇区田林路397号                  |
+----+------------------------------------------+------------------------------------------+------------------------------------------+
```

> **注意**
> 加密字段作为查询条件时，代理仅使用密文值作为查询条件，通过代理无法匹配到明文存储的增量数据。

步骤2：全量解密存量数据

1. 参考 任务管理，新建全量解密任务，全量解密敏感字段。



2. 全量解密任务完成后，直连 DB 查询，敏感字段的所有数据均已解密为明文。

```
[root@VM-32-33-centos ~]# mysql -h172.16.48.12 -P3306 -uroot -p casbtest -e 'select * from t1'
Enter password:
+----+--------+-------------+-----------------------------------------------------+
| id | name   | phone       | address                                             |
+----+--------+-------------+-----------------------------------------------------+
|  1 | 张三   | 18888888888 | 广东省深圳市南山区深南大道10000号                   |
|  2 | 李四   | 16666666666 | 上海市徐汇区田林路397号                             |
+----+--------+-------------+-----------------------------------------------------+
```

步骤3：切换数据库连接

数据库中的所有数据均解密成明文后，用户可以将数据库连接由 CASB 代理地址切换为数据库地址，后续所有数据库操作直连数据库处理。

步骤4：策略清理和解除绑定

1. 清理加密策略。参考 删除加密策略 文档，删除元数据上所有已配置的加密策略。
2. 清理代理账号配置的脱敏策略。参考 删除脱敏策略 文档，删除元数据对应的**所有代理账号**上已配置脱敏策略。
3. 解除代理和元数据绑定。参考 代理资源管理 文档，解除元数据和代理的绑定。

步骤5：删除元数据

清理完策略和代理绑定后，即可从 CASB 系统中删除元数据。

1. 登录 控制台，单击元数据管理菜单下的**关系型元数据**。
2. 在关系型元数据页面，找到需要操作的元数据，单击元数据右侧的**更多 > 删除**。

3. 在确认删除弹窗中，单击**确认**，即可删除元数据。

> **注意：**
> 元数据删除后，无法恢复。

连接 CASB 访问数据库查看数据

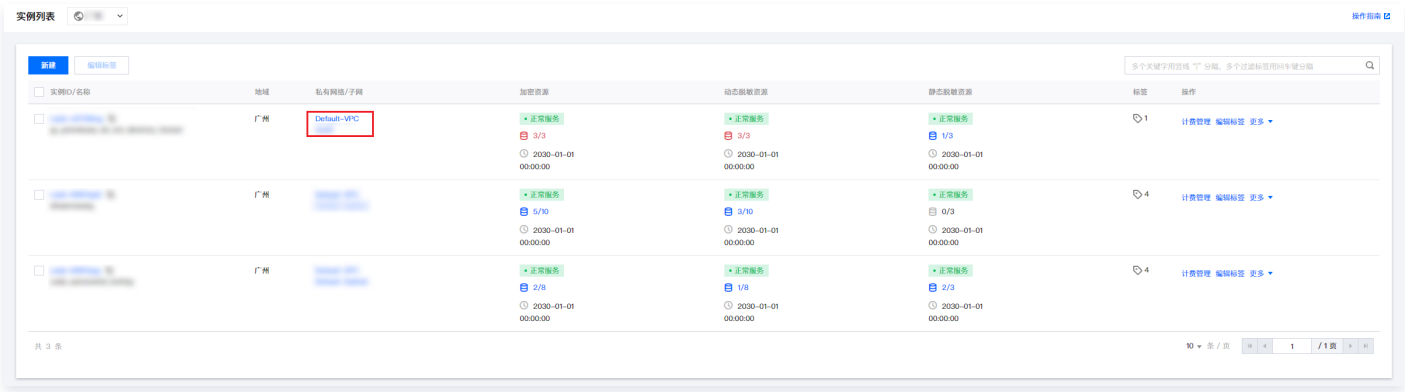
最近更新时间：2024-12-25 10:06:22

腾讯云内网访问

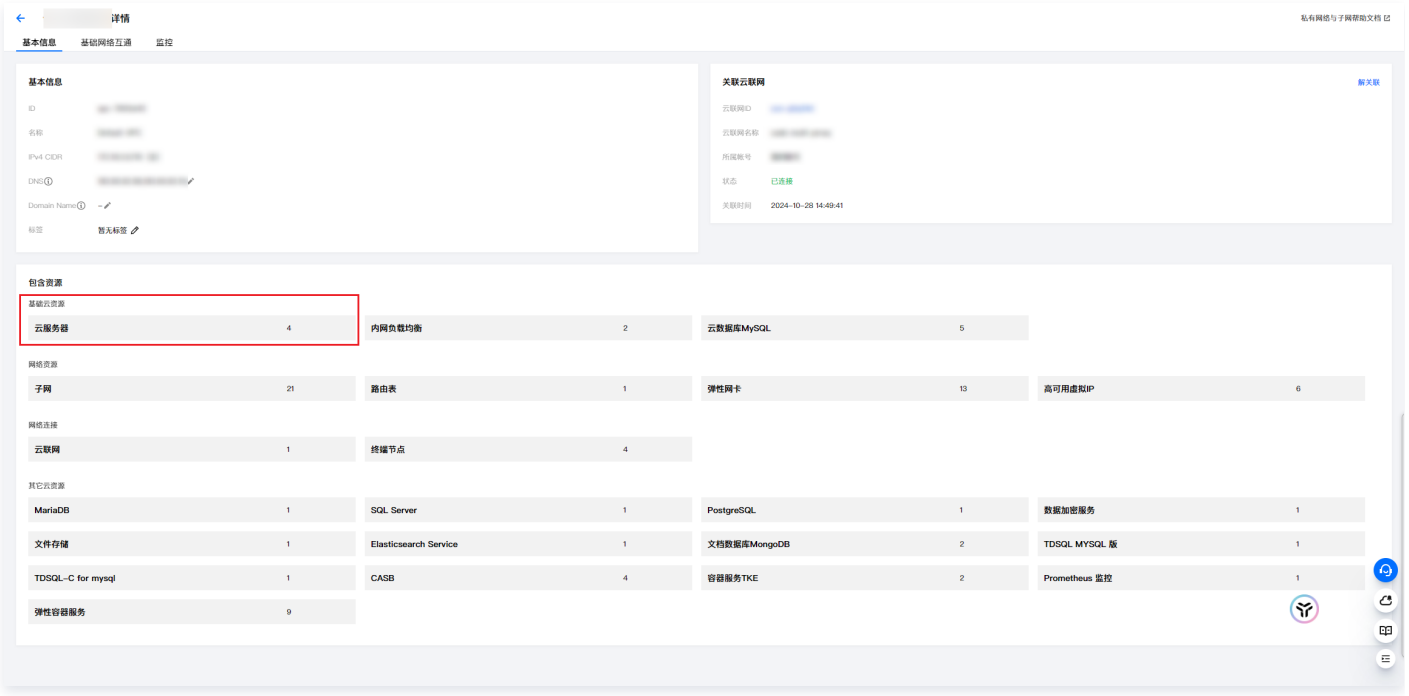
前提条件

准备与 CASB 网络互通的腾讯云 CVM

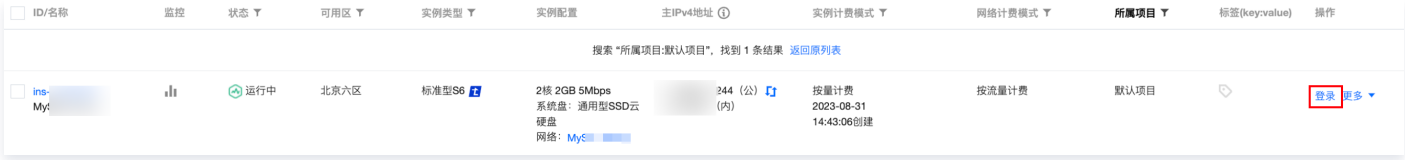
1. 在 CASB 实例列表页面，单击目标实例的**私有网络/子网**。



2. 在私有网络详情页面，单击**云服务器**，进入与 CASB 实例相同 VPC 下的云服务器列表。



3. 在云服务器列表中找到目标云服务器，在右侧操作栏中单击**登录**。



命令行访问 CASB

1. 成功登录云服务器后，执行如下命令安装 MySQL 行工具。（如之前已在此 CVM 上已安装，则可跳过此步骤）

```
yum install -y mysql.x86_64
```

2. 基于 CASB 的代理账号和密码、代理 IP 和端口，执行如下命令行登录数据库。

```
mysql -uroot -hcasb_proxy_vip -Pcasb_proxy_port -p
```

DB 客户端访问 CASB

1. 成功登录云服务器后，安装 DB 客户端工具。（如之前已在此 CVM 上已安装，则可跳过此步骤）
2. 在客户端工具，使用 CASB 的代理账号和密码、代理 IP 和端口创建链接。

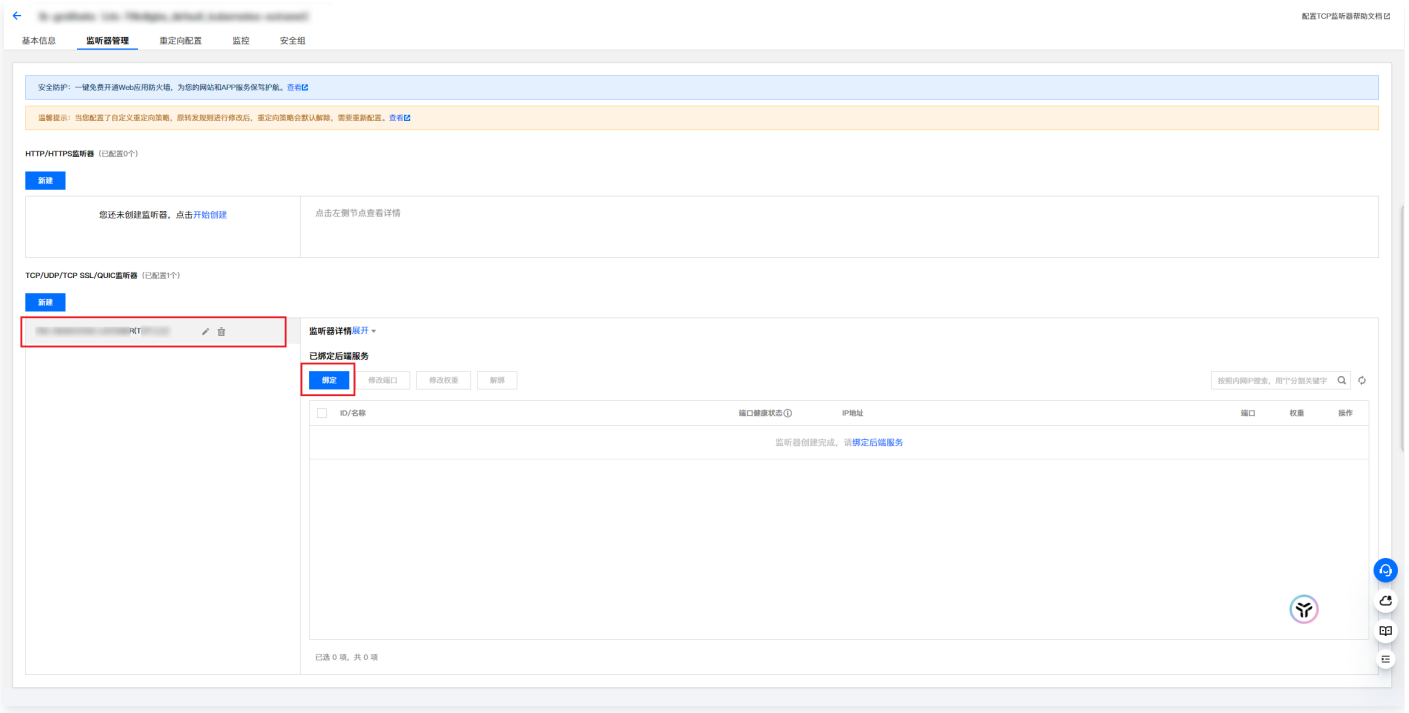
公网访问

CASB 代理地址默认不允许公网访问，但可通过 CLB 配置开通公网访问。

CLB 配置

1. 选择 CLB：登录 负载均衡控制台，在实例列表中找到目标 CLB 实例，在右侧操作栏中单击**配置监听器**。

2. 进入配置：在监听器管理页面，选择目标监听器，单击右侧**绑定**。



3. 配置 CASB 绑定：在配置窗口中，选择 IP 类型，输入 CASB 代理 IP 和端口信息。

字段	说明
目标类型	选择 IP 类型。
IP	填写 CASB 代理 IP。
端口	填写 CASB 代理端口。

说明：
CLB 设置后端服务时，若界面无目标类型选择（IP 类型），可 提交工单 进行开通。

访问 CASB

命令行访问

1. 成功登录 CVM 后，执行如下命令安装 MySQL 命令行工具 。（如之前已在此 CVM 上已安装，则可跳过此步骤）

```
yum install -y mysql.x86_64
```

2. 基于 CASB 的代理账号和密码、CLB 的 IP 和端口，执行如下命令行登录数据库。

```
mysql -uroot -hcasb_proxy_vip -Pcasb_proxy_port -p
```

DB 客户端访问

1. 安装 DB 客户端工具。（如之前已在此 CVM 上已安装，则可跳过此步骤）
2. 在客户端工具，使用 CASB 的代理账号和密码、CLB 的 IP 和端口创建链接。

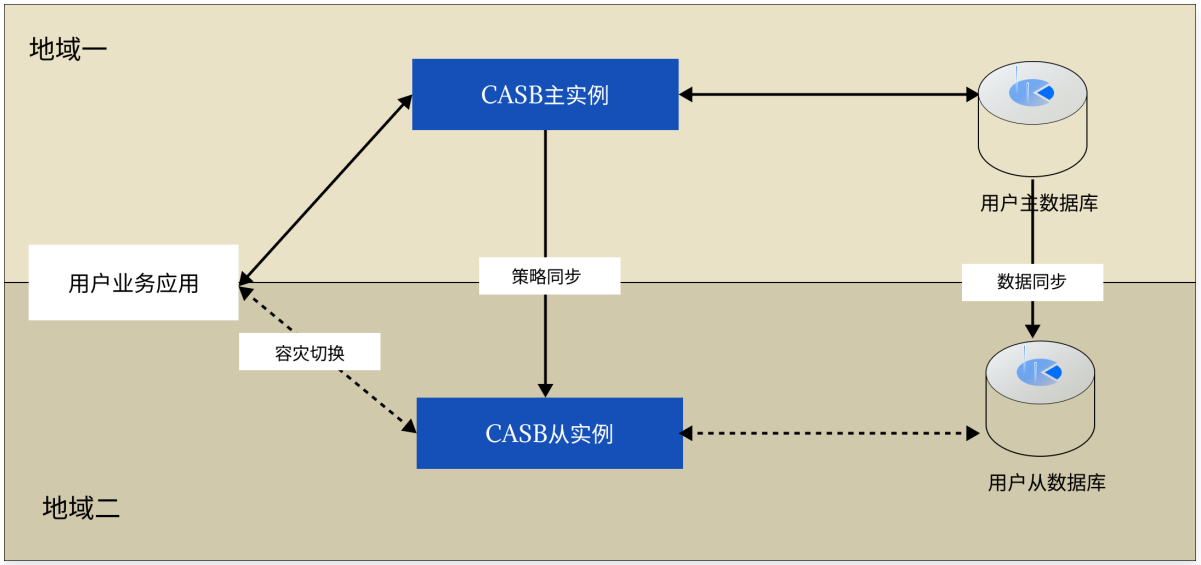
容灾双活实践教程

最近更新时间：2025-03-24 14:20:22

在当今数字化时代，大型企业对业务安全性、服务可用性和数据可靠性的要求日益严苛。为有效应对地域级别的灾难性故障，容灾双活架构应运而生。本文将详细介绍如何通过在不同地域部署两套 CASB 主备实例及数据库，并实现相关配置与操作，以构建高效可靠的容灾体系。

架构概述

容灾双活架构旨在通过在不同地域部署两套 CASB 主备实例和数据库，同步 CASB 实例间的策略信息以及数据库间的数据。不同地域间借助专线等方式进行私网通信，以确保数据实时同步，并将数据传输延迟降至最低。当故障发生时，能够通过切换访问的 CASB 实例信息，迅速恢复业务。具体架构表现为 2 套不同地域的 CASB 实例，且主从 CASB 实例和主从数据源实例的地域保持一致。



配置步骤

前提条件

已购买两套**不同地域**的 CASB 实例，且确保 CASB 实例能够在各自地域稳定运行。

> **说明：**
> 金融区与非金融区不可跨地域容灾。

主从配置

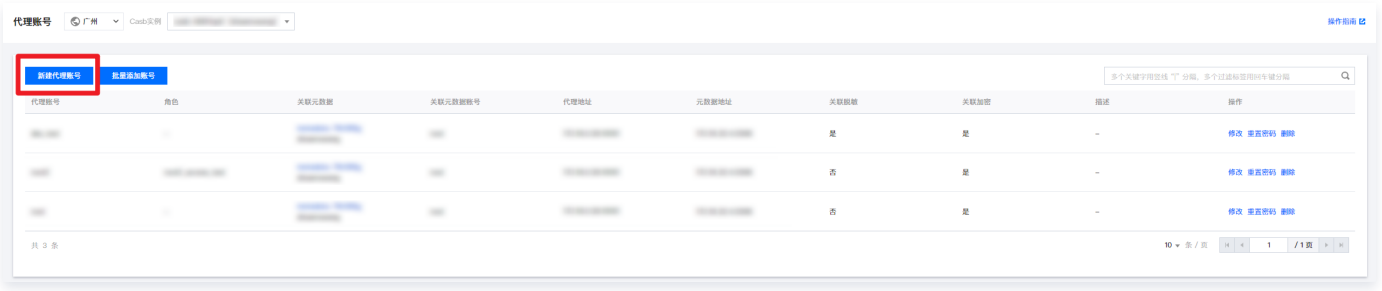
步骤一：在CASB 主、从实例分别添加对应的主、从元数据

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。

步骤二：在 CASB 主、从实例分别配置对应代理账号信息

1. 登录 控制台，在左侧导航栏中，单击**实例 > 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。

步骤三：在 CASB 从实例中，配置 “元数据主节点”

1. 登录 控制台，在左侧导航栏中，单击**元数据 > 元数据管理**。
2. 在元数据管理页面，选择**从节点**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 。

容灾切换

1. 业务应用切换链接：将 “主实例地址（IP + 端口）和代理账号密码” 改为 “从实例地址（IP + 端口）和代理账号密码” 。通过更改业务应用访问的 CASB 实例地址和账号信息，使业务能够迅速切换到备用实例上继续运行。
2. （可选）在 CASB 从实例中，参考 主从同步管理，来取消 “元数据从节点” 。

恢复时长预估

采用此容灾双活架构部署的实例，恢复时长主要取决于业务切换访问地址的时间。由于该架构可实现跨地域的加解密策略同步，异地实例实时可用，CASB 能够保障策略在 1 分钟内实时同步。因此，业务侧可直接切换为异地实例，快速实现容灾切换，极大程度减少业务中断时间，保障企业业务的连续性。