

# 数据安全网关（云访问安全代理） 实践教程



腾讯云

**【版权声明】**

©2013-2024 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內容。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】**

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

### 实践教程

数据加密

数据脱敏

访问控制

MySQL BINLOG 数据解密同步

取消接入 CASB

# 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。

# 数据脱敏

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）（Data Security Gateway（Cloud Access Security Broker），CASB）的多个应用使用不同数据脱敏策略的相关实践经验和相关操作。

## 接入场景

不同的应用访问同一份已加密的敏感数据，返回不同级别的脱敏后的数据内容。

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：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3：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。

代理账号	代理地址	角色	关联元数据	关联元数据编号	元数据地址	关联脱敏	关联加密	描述	操作
user3	172.16.0.30:10100	root	metastore	root	172.16.32.4:3306	否	是	-	修改 重置密码 删除
user2	172.16.0.30:10100	root	metastore	root	172.16.32.4:3306	否	是	-	修改 重置密码 删除
user1	172.16.0.30:10100	root	metastore	root	172.16.32.4:3306	否	是	-	修改 重置密码 删除

## 步骤4：配置脱敏策略

### 1. 配置 user1 的脱敏策略。

#### 说明

若代理账号未配置脱敏策略规则组或未配置脱敏规则，默认返回明文。

#### 1.1 新建脱敏规则组。

参考 [脱敏策略管理](#)，为 user1 创建脱敏策略规则组。

脱敏策略组名称	代理地址	代理账号	关联元数据	元数据账号	规则数	Proxy开启状态	创建时间	描述	操作
drule- user1_datanmask	172.16.0.30:10100	user1	metadb	root	2	已开启	2022-12-26 17:44:53		<a href="#">规则管理</a> <a href="#">删除</a>

#### 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。

策略名称	字段名	字段类型	字段长度	主键	脱敏算法	操作
drule- user1_datanmask	id	INT	10	是	全保留	<a href="#">编辑</a> <a href="#">删除</a>
	name	VARCHAR	512	否	全保留	<a href="#">编辑</a> <a href="#">删除</a> <a href="#">预览</a>
	phone	VARCHAR	512	否	全保留	<a href="#">编辑</a> <a href="#">删除</a> <a href="#">预览</a>
	未设置					

### 2. 配置 user2 的脱敏策略。

#### 2.1 新建脱敏规则组。

参考 [脱敏策略管理](#)，为 user2 创建脱敏策略规则组。

脱敏策略组名称	代理地址	代理账号	关联元数据	元数据账号	规则数	Proxy开启状态	创建时间	描述	操作
drule- user2_datanmask	172.16.0.30:10100	user2	metadb	root	0	已开启	2022-12-26 17:45:05		<a href="#">规则管理</a> <a href="#">删除</a>

#### 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](#)。

策略名称	字段名	字段类型	字段长度	主键	脱敏算法	操作
drule- user2_datanmask	id	INT	10	是	全保留	<a href="#">编辑</a> <a href="#">删除</a>
	name	VARCHAR	512	否	保留第一个字符	<a href="#">编辑</a> <a href="#">删除</a> <a href="#">预览</a>
	phone	VARCHAR	512	否	保留前1后1	<a href="#">编辑</a> <a href="#">删除</a> <a href="#">预览</a>
	未设置					

### 3. 配置 user3 的脱敏策略。

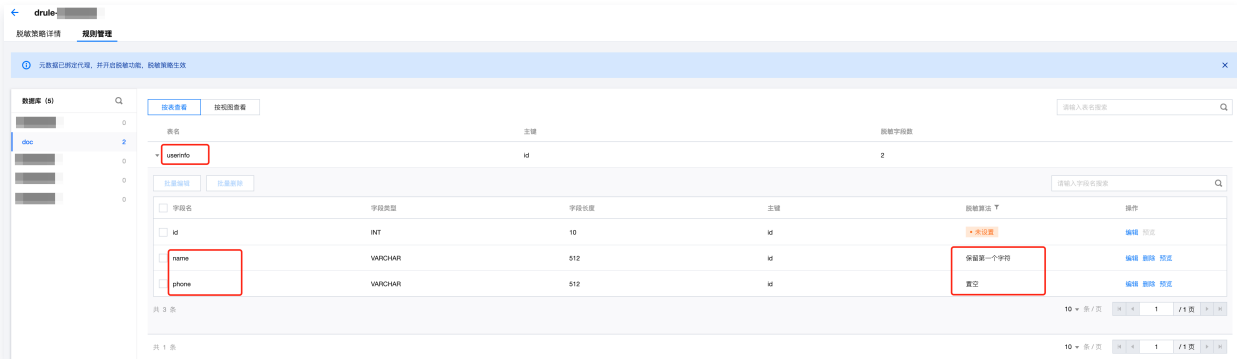
#### 3.1 新建脱敏规则组。

参考 [脱敏策略管理](#)，为 user3 创建脱敏策略规则组。

数据源中心名称	代理地址	代理账号	关联元数据	元数据账号	数据库	Proxy开启状态	创建时间	描述	操作
drule- user3_dbtest	172.16.0.30:10100	user3	metadb	root	0	已开启	2022-12-26 17:45:18		编辑详情 删除

### 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==|^| | PNsX0qkmrZCPZSXHKG5X4MJAVg==|^| |
| 2  | kA9TZaSnnFY+wtwb3kiL5p0F5XE7LX1i5r6a/Q==|^| | 09tc36whqMzWbSMq1v7seDpZ6A==|^| |
+----+-----+-----+
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。

代理账号	代理地址	角色	关联云数据库	关联元数据账号	元数据地址	关联引擎	关联加密	描述	操作
user4	172.16.0.30:10100		metastore	root	172.16.32.4:3306	否	是	-	修改 重置密码 删除
user3	172.16.0.30:10100		metastore	root	172.16.32.4:3306	是	是	-	修改 重置密码 删除
user2	172.16.0.30:10100		metastore	root	172.16.32.4:3306	是	是	-	修改 重置密码 删除
user1	172.16.0.30:10100		metastore	root	172.16.32.4:3306	是	是	-	修改 重置密码 删除

## 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。

角色名称	代理账号	访问规则	描述	创建时间	修改时间	操作
acrole cronjob	0	0	定时任务	2022-12-26 19:32:49	2022-12-26 19:32:49	代理账号 规则管理 删除
acrole nameadmin	0	0	姓名校验	2022-12-26 19:32:43	2022-12-26 19:32:43	代理账号 规则管理 删除
acrole reader	0	0	只读	2022-12-26 19:32:35	2022-12-26 19:32:35	代理账号 规则管理 删除
acrole admin	0	0	管理员	2022-12-26 19:32:30	2022-12-26 19:32:30	代理账号 规则管理 删除

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	关联数据	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。

### 编辑规则 ✕

规则名称 \*

规则描述  8 / 100

#### 基本规则

客户端IP

数据库名称

表名

命令

#### 字段规则

字段

#### 执行时间 执行周期 \* 不限 每天 指定时间段 访问规则 访问规则 \* 阻断 放行

- rule\_deny\_phone : 阻断访问 phone 字段的语句。

### 编辑规则 ✕

规则名称 \*

规则描述  11 / 100

#### 基本规则

客户端IP

数据库名称  删除  
添加

表名  删除  
添加

命令

#### 字段规则

字段  删除  
添加

#### 执行时间

执行周期 \*  不限  每天  指定时间段

#### 访问规则

访问规则 \*  阻断  放行

- rule\_allow\_client : 放行来自 172.16.32.33 机器的语句。

### 编辑规则

规则名称 \*

规则描述  10 / 100

#### 基本规则

客户端IP  [删除](#)  
[添加](#)

数据库名称

表名

命令

#### 字段规则

字段

#### 执行时间

执行周期 \*  不限  每天  指定时间段

#### 访问规则

访问规则 \*  阻断  放行

- rule\_allow\_client\_rd : 放行来自 172.16.32.33 机器的 SELECT 语句。

### 编辑规则

规则名称 \*

规则描述  13 / 100

#### 基本规则

客户端IP  [删除](#)  
[添加](#)

数据库名称

表名

命令

SQL行数 >=  [-](#) [+](#)

#### 字段规则

字段

#### 执行时间

执行周期 \*  不限  每天  指定时间段

#### 访问规则

访问规则 \*  阻断  放行

[确定](#) [取消](#)

- rule\_allow\_client\_name\_rw : 放行来自 172.16.32.33 机器、name 字段的 SELECT 、 UPDATE 语句。

### 编辑规则

规则名称 \*

规则描述  14 / 100

#### 基本规则

客户端IP  [删除](#)  
[添加](#)

数据库名称  [删除](#)  
[添加](#)

表名  [删除](#)  
[添加](#)

命令

SQL行数 >=

#### 字段规则

字段  [删除](#)  
[添加](#)

#### 执行时间

执行周期 \*  不限  每天  指定时间段

#### 访问规则

访问规则 \*  阻断  放行

[确定](#) [取消](#)

- 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。



编辑规则
✕

规则名称 \*

规则描述  17 / 100

**基本规则**

客户端IP ?  删除  
添加

数据库名称  删除  
添加

表名  删除  
添加

命令 ?

SQL行数 >= ?  - +

**字段规则**

字段  删除  
添加

**执行时间 ?**

执行周期 \*  不限  每天  指定时间段

选择时间 \*  🕒

**访问规则**

访问规则 \*  阻断  放行

确定
取消

## 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。 <ul style="list-style-type: none"> <li>rule_allow_client：放行来自 172.16.32.33 机器的语句。</li> <li>rule_deny_all：阻断所有访问语句。</li> </ul>
reader 角色规则	reader 角色按如下顺序配置两条规则。 <ul style="list-style-type: none"> <li>rule_allow_client_rd：放行来自 172.16.32.33 机器的 SELECT 语句。</li> <li>rule_deny_all：阻断所有访问语句。</li> </ul>
nameadmin 角色规则	nameadmin 角色按如下顺序配置三条规则。 <ul style="list-style-type: none"> <li>rule_deny_phone：阻断访问 phone 字段的语句。</li> <li>rule_allow_client_name_rw：放行来自 172.16.32.33 机器、name 字段的 SELECT、UPDATE 语句。</li> <li>rule_deny_all：阻断所有访问语句。</li> </ul>
cronjob 角色规则	cronjob 角色按如下顺序配置三条规则。 <ul style="list-style-type: none"> <li>rule_deny_phone：阻断访问 phone 字段的语句。</li> <li>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。</li> <li>rule_deny_all：阻断所有访问语句。</li> </ul>

### 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-txsq1-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
```

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-txsq1-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'
```

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-txsq1-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
```

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-n62pluia'

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-n62pluia'
    
```

### 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：2024-06-13 19:14:32

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。

表策略配置 - t1

字段名称	字段类型	字段长度	加密算法	模糊查询	密钥	更新时间	工作模式	实时加密	操作
id	INT	10	-	-	-	-	-	<input type="checkbox"/>	配置策略
name	VARCHAR	512	国密SM4	不启用	██████████	2023-01-31 00:58:12	读解密, 写加密	<input checked="" type="checkbox"/>	删除策略
phone	VARCHAR	512	国密SM4	不启用	██████████	2023-01-31 00:58:15	读解密, 写加密	<input checked="" type="checkbox"/>	删除策略
address	VARCHAR	512	国密SM4	不启用	██████████	2023-01-31 00:58:19	读解密, 写加密	<input checked="" type="checkbox"/>	删除策略

共 4 条

- 针对代理账号 root，phone 字段上已配置脱敏规则。

drule-██████████

脱敏策略详情 规则管理

元数据已绑定代理，并开启脱敏功能，脱敏策略生效

数据库 (1) casbtest

按表查看 按视图查看

请输入表名搜索

表名	主键	脱敏字段数
t1	id	1

批量编辑 批量删除

请输入字段名搜索

字段名	字段类型	字段长度	主键	脱敏算法	操作
<input type="checkbox"/> id	INT	10	id	未设置	编辑 预览
<input type="checkbox"/> name	VARCHAR	512	id	未设置	编辑 预览
<input checked="" type="checkbox"/> phone	VARCHAR	512	id	手机号(星号遮盖)	编辑 删除 预览
<input type="checkbox"/> address	VARCHAR	512	id	未设置	编辑 预览

共 4 条

共 1 条

- 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。

```
root@M-32-33-centos ~]# mysql -h172.16.48.12 -P3306 -uroot -p casbtest -e 'select * from t1'
```

id	name	phone	address
1	i42DKg49pWZBjJFeZtnDyYB4nY8KnpL4bmd+g= ^	iYkq71zNDtrP4e8rR//06aw0E0Q6Ehq7raS9Q= ^	vFXVE43Sqjqonm5KeZ54dyYUD+C3xsFeDi8kFeMLtLd9fpjcz0Z1Eo80M1Sx8k4yMp1aJDHryDn1hHs ^

- 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。

表策略配置 - t1

字段名称	字段类型	字段长度	加密算法	模糊查询	密钥	更新时间	工作模式	实时加密	操作
id	INT	10	-	-	-	-	-	<input type="checkbox"/>	配置策略
name	VARCHAR	512	国密SM4	不启用	██████████	2023-01-31 00:40:32	读解密，写不加密	<input checked="" type="checkbox"/>	删除策略
phone	VARCHAR	512	国密SM4	不启用	██████████	2023-01-31 00:38:09	读解密，写不加密	<input checked="" type="checkbox"/>	删除策略
address	VARCHAR	512	国密SM4	不启用	██████████	2023-01-31 00:38:13	读解密，写不加密	<input checked="" type="checkbox"/>	删除策略

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", "1666666666", "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  | i420Kg49pWZBjJFeZtnDyYB4nY8KnpL4bmd+g=|^ | iYkq71zXNDt rP4e8rR//06aw0EQ0GEhg7raS9Q=|^ | vFXVE43Sajgonm5KeZ540yYUD+C3xsfeDi8kFeMLtLd9fpjcz0Z1Eo80WmIsX8k4yMpiaJDHryDn1hHs|^ |
| 2  | 李四 | 1666666666 | 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。

全量加解密

关系型数据库 MongoDB

元数据 metadata

元数据已绑定代理，并开启加密功能，加密策略生效

任务ID	数据库	任务类型	代理账号	状态	任务创建时间	任务更新时间	预计完成时间	描述	操作
task-██████	casbtest	全量解密	root	执行成功	2023-01-31 00:44:33	2023-01-31 00:44:55	2023-01-31 00:44:55	-	重启 查看任务详情 编辑 删除

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。