云访问安全代理

产品简介

腾讯云

【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

产品简介
- 产品概述
- 产品优势
- 应用场景
- 数据库支持说明
  - MySQL
  - PostgreSQL
  - MongoDB

产品简介
产品概述

最近更新时间：2023-09-28 11:01:01

什么是云访问安全代理

云访问安全代理（Cloud Access Security Broker，CASB）是一款面向数据库的数据防护服务，以代理模式降低应用侧改造成本，提供数据库内字段级的数据加密服务，有效防护内外部数据安全威胁。

产品功能

元数据管理

快速对接自建数据库、云数据库等多种不同部署方式的数据库资产，保护 MySQL、PostgreSQL、MongoDB 数据库的数据安全。

数据加密

使用国密算法（SM4）、高级加密标准算法（AES）等多种加密算法对应用数据进行字段级的细粒度加密，提高数据的安全性，加密密钥使用腾讯云 密钥管理系统 安全托管（用户需另行购买）。

数据脱敏

内置多种脱敏算法，同时支持自定义脱敏算法，为用户数据提供丰富的脱敏能力，实现敏感隐私数据的可靠保护。

访问控制

基于角色的访问控制和基于来源、数据库、表、字段、时间、命令等多维度的访问规则，精细管控不同业务的数据访问权限。

数据库审计

实时记录数据库操作，并进行细粒度审计管理，分析操作中的敏感操作、危险操作等各种风险行为，提高数据资产安全。

产品优势

最近更新时间：2022-12-21 14:23:28

字段级加密

提供可视化的策略管理控制台，管理员可以在控制台上配置数据库表内每个字段的加解密规则和脱敏规则，精细化保护敏感字段（如姓名、手机号等字段）。支持国密算法，满足业务合规的需求。

密文模糊查询

提供高级加密功能，已加密的密文数据可支持模糊搜索功能（LIKE 通配符查询）。

字段级脱敏

内置30+种不同类型、不同场景的脱敏算法，同时支持自定义算法，提供字段级的数据脱敏的能力，降低原文传输或展示的泄露风险。

细粒度权限控制

支持对访问用户、访问来源、目的数据库、表、字段、操作命令、访问时间等多维度细粒度的权限管控。

高可靠密钥

数据加密密钥由腾讯云 密钥管理系统（KMS）统一管理（用户需提前购买和开通 KMS 服务），密钥管理系统底层使用硬件安全模块（HSM），支持权限管控和内置审计，保护密钥安全。

对应用透明

代理对应用透明，不改变应用的运行机制，通过代理写入数据库时加密字段数据自动加密，从数据库中读取加密字段数据时自动解密。

灵活接入部署

数据库绑定代理后，应用系统少改造，只需将访问地址和认证信息由数据库改为代理即可。在控制台配置敏感字段的加解密策略后代理即可实现自动加解密，策略配置后实时生效。

大规模统一管控

面对企业信息系统多、数据库多的情况，可统一接入至云访问安全代理，进行集中管理。

高可用架构

采用高可用的集群架构，支持多可用区、跨地域的容灾部署，有效防止服务主机故障、网络故障和区域故障引起的业务损失。

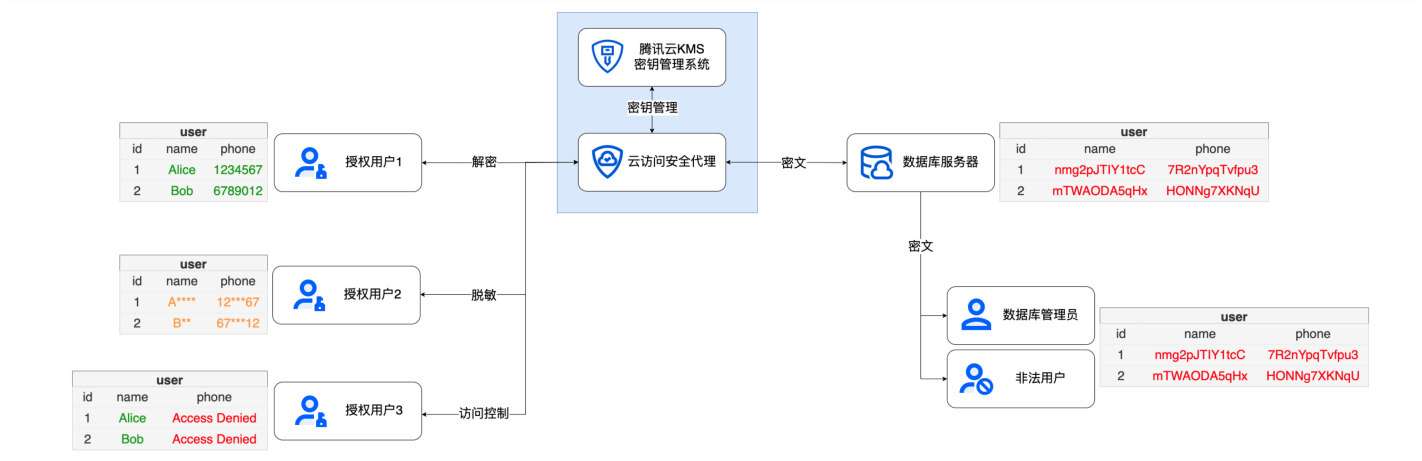
可扩展性

代理集群采用分布式架构，对业务流量自动负载均衡，并可根据业务需求增加集群容量实现快速扩容。

应用场景

最近更新时间：2022-12-21 14:23:32

云访问安全代理(CASB)是一款面向应用的数据库防护服务，以应用业务少开发改造为目的，帮助用户快速解决数据加密、脱敏、访问控制等需求，帮助不同行业解决数据安全痛点问题。



加密细控

- **痛点**：传统数据安全以基础设施为主，例如数据库 TDE 加密、全磁盘加密等，防护粒度粗。 企业内部 IT 人员和外部黑客可以直接从数据库中读取敏感数据时，仍会面临数据安全风险，造成敏感数据泄漏。
- **方案**：业务接入CASB代理后，用户管理员可通过控制台配置数据库的加解密策略，加密粒度可细化到字段级（如姓名、手机号等敏感字段）。使用云访问安全代理服务，实现数据库中关键信息加密存储，密钥管理与密文数据分离，防护内外部威胁。

数据脱敏

- **痛点**：数据库中的数据在面临不同业务系统使用、研发运维等不同角色的人员访问、数据需要对外共享等场景时，很容易失去对敏感数据的保护，面临着极大的隐私数据泄漏风险。
- **方案**：业务接入CASB代理后，可以为不同业务系统的访问用户配置字段级的脱敏策略，实现同一份加密数据实时返回不同的明文、密文或脱敏后的结果，无明文访问权限的业务无法根据脱敏后的结果反推出明文，有效的保护敏感数据。

快速部署

- **痛点**：应用层加密时，需要开发改造所有相关应用，实现同样的数据加密、脱敏、动态访问控制等功能。改造和部署应用成本高、风险大且周期长。
- **方案**：云访问安全代理服务支持多种数据库的快速接入部署。数据库绑定代理后，应用系统无需改造，只需将访问地址和认证信息由数据库改为代理即可。敏感字段的加密、脱敏、访问控制等策略可在控制台上可视化配置，策略配置后实时生效。

数据库支持说明

MySQL

最近更新时间：2024-02-28 15:01:11

数据库字段类型支持情况

字段类型	字段加密	字段模糊查询	字段脱敏
char	AES/SM4	支持	支持
varchar	AES/SM4	支持	支持
tinytext	AES/SM4	支持	支持
text	AES/SM4	支持	支持
mediumtext	AES/SM4	支持	支持
longtext	AES/SM4	支持	支持
tinyint	-	-	支持
smallint	-	-	支持
mediumint	-	-	支持
int/integer	-	-	支持
bigint	-	-	支持
float	-	-	支持
double	-	-	支持
decimal	-	-	支持
tinyblob	-	-	-
blob	-	-	-
longblob	-	-	-
date	-	-	-
time	-	-	-

year	–	–	–
datetime	–	–	–
timestamp	–	–	–

功能支持和使用限制

数据库

- 支持 MySQL 5.7及以上版本的数据库和兼容 MySQL 协议的数据库（如 TDSQL 、MariaDB ）。
- 不支持8.0及以上版本新增的 SQL 语法。
- 数据库、表和字段名不区分大小写。
- 加密字段长度需预先扩容以支持存储明文加密后更大长度的密文。

字符集

- character_set_connection 必须为 utf8 或 utf8mb4 ，即仅只支持客户端或应用使用 utf8 和 utf8mb4 字符集连接代理。
- 加密字段需使用区分大小写的 collation ，如 utf8_general_bin 。

连接

- 同一连接内不允许切换登录用户。
- 应用连接代理的账号认证方式支持 mysql_native_password 。
- 代理连接后端数据库的账号认证方式支持 mysql_native_password 和 caching_sha2_password 。
- CASB 代理集群升级时会造成连接中断，请确保业务支持连接断开后的自动重连。

加解密和脱敏

- 加解密算法支持 AES 和 SM4 算法。
- 支持对字符串和二进制类型字段的加解密。
- 支持对字符串和数值类型字段的动态脱敏。
- 支持两个及以上连续字符的密文模糊查询，仅支持 LIKE 语法，且 LIKE 匹配区分大小写，不支持正则查询。
- 配置密文模糊查询策略的字段值必须为空或不少于两个字符。
- 密文模糊查询不支持转义字符，不支持 NO_BACKSLASH_ESCAPES 选项。
- 加密后密文超过字段长度时会保存明文。
- 加密字段作为查询条件，且同时存在密文和明文时，只能查询到密文数据，存量明文数据需全量加密成密文；加密字段不作为查询条件时，可正常查询所有数据。
- 支持 SELECT , INSERT , REPLACE , UPDATE , DELETE 语句中 WHERE、ON、IN、INSERT VALUE、SET 等各字段中非表达式、非函数内的原始字面值加解密。

- 支持 ROW 条件中非表达式的值加解密，如支持 where (id, 'n2' , addr)=(2, name,'a2') 中的字段加解密。
- 支持 table references 和 where condition 中的子查询字段中非表达式的值加解密。
- UNION 语句使用第一个 SELECT 子句 的加解密策略。
- 不支持存储过程的加解密。
- 不支持 INSERT INTO ... SELECT ... 等不经过代理处理的数据的加解密。
- 连接查询时， JOIN 连接字段需选择同样的密钥和加密算法，否则密文不一致，无法正确进行连接查询。
- 支持 GROUP BY , 但不保证和明文一致的顺序。
- information_schema ， sys ， mysql 等内置数据库不支持加解密和脱敏。

协议

- 支持 COM_QUERY , COM_STMT_PREPARE 和 COM_STMT_EXECUTE 协议中字段加解密。
- 不支持 COM_STMT_SEND_LONG_DATA ， COM_STMT_RESET 协议。
- 不支持 COM_QUERY Protocol::LOCAL_INFILE_Data 协议。

语句

- DML 执行前，需先切换到或指定相应的库。
- 加密字段不支持函数操作。
- 加密字段不支持数学运算。
- 加密字段不支持 ORDER BY 。
- 加密字段不支持正则查询。
- 不支持包含自定义变量的语句。
- 不支持 SELECT INTO 语句。
- 不支持 mysqldump 中使用 CASB 不支持的特性和条件。
- 不支持 CREATE TABLE xx AS SELECT 、 CHECK TABLE 、 CHECKSUM TABLE 语法。
- 不支持 TDSQL 自定义的管理语法, 如 help , repair 等。
- 不支持 COM_QUERY 协议的 Prepare 、 Execute 语句的加解密。
- 除了 TDSQL 增删改查语句的行首注释外，SQL 语句中的其余注释不会生效。
- TDSQL 的 ShardKey 字段不能配置加密。

binlog

详情请参考 MySQL BINLOG 数据解密同步 。

其他

- 所有表结构必须预先在策略控制台定义，账号必须和相应数据源绑定后才能通过 proxy 操作相应的数据源。

- 数据源删除后重新添加时，需断开存量连接，建立新的 MySQL 连接查询。
- 单次查询处理的数据大小需小于2^24字节。

常用 SQL 语句支持情况

> **说明**
> 示例中已配置加密策略的字段名称为：crypto_column。

- **插入语句**

类型	支持情况	SQL 样例
指定列名插入加密字段	支持	INSERT INTO table_a (id, col1, col2, crypto_column) VALUES (1, 'a', 'b', 'c');
不指定列名插入加密字段	支持	INSERT INTO table_a VALUES (1, 'a', 'b', 'c');

- **删除语句**

类型	支持情况	SQL 样例
加密字段作为查询条件	支持	DELETE FROM table_a WHERE crypto_column = 'c';
加密字段作为子查询语句的查询条件	支持	DELETE FROM table_a WHERE col1 IN (SELECT col2 FROM table_b WHERE crypto_column = 'c');

- **更新语句**

类型	支持情况	SQL 样例
加密字段作为查询条件	支持	UPDATE table_a SET col1 = 'd' WHERE crypto_column = 'c';
更新加密字段	支持	UPDATE table_a SET crypto_column = 'd' WHERE id = 1;

- **查询语句**

类型	支持情况	SQL 样例

加密字段作为返回结果，SELECT语法的支持	支持	SELECT crypto_column FROM table_a;
加密字段作为返回结果，SELECT *语法的支持	支持	SELECT * FROM table_a;
加密字段使用别名	支持	SELECT crypto_column a, col2 b FROM table_a;
加密字段作为查询条件, 等值匹配	支持	SELECT * FROM table_a WHERE crypto_column = 'c';
加密字段作为查询条件，IN条件查询	支持	SELECT * FROM table_a WHERE crypto_column IN ('a', 'b', 'c');
加密字段作为子查询的条件	支持	SELECT crypto_column FROM (select * FROM table_a WHERE crypto_column = 'c') a;
JOIN查询，加密字段作为WHERE条件	支持	SELECT table_a.id FROM table_a JOIN table_b ON table_a.id = table_b.id WHERE table_a.crypto_column = 'c';
JOIN查询，加密字段作为ON条件	支持	SELECT table_a.id FROM table_a JOIN table_b ON table_a.id = table_b.id AND table_a.crypto_column = 'c';
JOIN查询，加密字段作为返回结果	支持	SELECT table_a.crypto_column FROM table_a JOIN table_b ON table_a.id = table_b.id;
JOIN查询，加密字段作为连表条件	支持:连表的加密字段需配置相同密钥和算法	SELECT table_a.id FROM table_a JOIN table_b ON table_a.crypto_column = table_b.crypto_column;
GROUP BY 加密字段	支持	SELECT * FROM table_a WHERE id>10 GROUP BY crypto_column;
ORDER BY 加密字段	不支持	SELECT * FROM table_a WHERE id>10 ORDER BY crypto_column;
加密字段模糊查询	支持:需配置密文模糊检索算法	SELECT * FROM table_a WHERE crypto_column LIKE '%cc%';

加密字段正则查询	不支持	SELECT * FROM table_a WHERE crypto_column REGEXP '^cc';
加密字段范围查询	不支持	SELECT * FROM table_a WHERE crypto_column > 'a' AND crypto_column < 'd';
函数处理加密字段	不支持	SELECT * FROM table_a WHERE substr(crypto_column, 0, 2) = 'aa';

PostgreSQL

最近更新时间：2022-08-17 17:39:14

对数据库字段类型的支持

目前 PostgreSQL 支持的数据库版本为 **postgre 9.3.5**，支持的字段类型如下：

字段类型	支持情况	可选算法
character varying(n), varchar(n)	• 支持 • 加密结果大于当前Char长度限制，直接存明文	AES/SM4
character(n), char(n)	支持	AES/SM4
bytea	支持	AES/SM4
text	支持	AES/SM4
smallint	不支持	
integer	不支持	
bigint	不支持	
decimal	不支持	
numeric	不支持	
real	不支持	
double precision	不支持	
smallserial	不支持	
serial	不支持	
bigserial	不支持	
money8	不支持	
timestamp [(p)] [without time zone]	不支持	

timestamp [(p)] with time zone	不支持	
date	不支持	
time [(p)] [without time zone]	不支持	
time [(p)] with time zone	不支持	
interval [fields] [(p)]	不支持	
boolean	不支持	
enum	不支持	
point	不支持	
line	不支持	
lseg	不支持	
box	不支持	
path	不支持	
path	不支持	
polygon	不支持	
circle	不支持	
cidr	不支持	
inet	不支持	
macaddr	不支持	
bit(n)	不支持	
varying(n)	不支持	
tsvector	不支持	
tsquery	不支持	
json	不支持	
jsonb	不支持	

jsonpath	不支持	
int4range	不支持	
int8range	不支持	
numrange	不支持	
tsrange	不支持	
tstzrange	不支持	
daterange	不支持	
oid	不支持	
regproc	不支持	
regprocedure	不支持	
regoper	不支持	
regoperator	不支持	
regclass	不支持	
regtype	不支持	
regconfig	不支持	
regdictionary	不支持	

对 SQL 语句的支持

对数据库查询语句的支持情况如下：

- **插入语句：**

类型	支持情况	SQL 样例
不指定列插入	支持	INSERT INTO public.table_a VALUES (1,1,'n1','a1'), (2,1, 'n1','a1');
指定列插入	支持	INSERT INTO public.table_a VALUES (2,1 ,'n2','a2');
指定列写入	支持	INSERT INTO public.table_a (id, col1, col2,col3) VALUES (1, 1,'n1','a1');
指定列批量写	支持	INSERT INTO public.table_a (id,col1, col2,col3) VALUES

入		(1,1,'n1','a1'), (2,1,'n1','a1');

- **删除语句：**

类型	支持情况	SQL 样例
等值匹配删除，策略配置在其中某个条件字段上	支持	delete from public.table_a where col2 != 'n2' and id != 2;
带 in 的删除，策略配置在 in 字段上	支持	delete from public.table_a where id in (1,2);
带子查询的删除，策略在子查询的条件字段上	支持	select * from table_a t1 where t1.col2 in (select col2 from table_b) and t1.id = 1;

- **更新语句：**

类型	支持情况	SQL 样例
策略配置在查询条件上	支持	UPDATE public.table_a SET id=1, col1='c11' where col2='c;
策略配置在更新字段上	支持	UPDATE public.table_a SET id=1, col1='c11' where id=1;

- **查询语句：**

类型	支持情况	SQL 样例
对 select * 语法的支持	支持	select * from public.table_a;
条件字段等值匹配	支持	select * from public.table_a where col2 != 'n2' and id != 2;
条件字段模糊匹配	支持	select * from public.table_a where col2 like 'n%';
条件字段范围查询	不支持	select * from public.table_a where col2 > 'n0'
条件字段带函数	不支持	select col1 from table_a where substr(col1,0,2) = 'aa';
条件字段带 in 操作	支持	select * from public.table_a where id in (1,2)

条件字段为函数参数	不支持	select id, lower(col2) from public.table_a ta ;
目标字段函数参数为加策略字段	不支持	select concat(tft.col2 , 2, NULL, 22) from public.table_a tft ;
SQL 语句中的表使用别名，选择字段及查询条件通过别名指定	支持	select tft.id, tft.col1, tft.col2, tft.col3 from public.table_a tft where tft.id=1;
关联查询时使用 select *	支持	select * from table_a t1 inner join table_b t2 on t1.id = t2.id and t1.col2 = t2.col2 where t1.id = 1;
子查询-简单语法子查询，策略在子查询条件语句上	支持	select * from table_a t1 where t1.col2 in (select col2 from table_a) and t1.id = 1;
子查询-子查询中策略字段作为关联条件或条件字段	支持	select t1.id, t1.col1, t1.col2, t1.col3 from table_a t1 inner join table_b t2 on t1.id = t2.id and t1.col2 = t2.col2 where t1.id = 1 and t2.col2 = 'n1';
子查询-结果集带有子查询字段并是策略字段	支持	select t1.id, t1.col1, t1.col2, t2.col3 from table_a t1 inner join table_b t2 on t1.id = t2.id and t1.col2 = t2.col2 where t1.id = 1 and t2.col2 = 'n1';
对 exists 关键字的支持	支持	select * from table_a tft where exists (select 1 from table_b tft2 where tft2.id = tft.id and tft2.col2='n1');
对 group by 语法的支持	支持	select col2, count(1) from table_a tft group by col2;
对 Union 关键字的支持	支持 策略字段 按照基础表	select id, col1 from public.table_a ta union select id, col1 from public.table_b tb ;
对 order by 的支持	支持非加解密字段	select id, col2 from table_a tft order by id desc limit 1; select id, col2 from table_a tft order by lower(col2);
常量查询	支持	select version();
临时表	不支持	

其他注意事项

数据库连接

目前不支持 SSL 连接，客户端字符集支持 UTF-8。客户端建立连接时必须指定如下参数 client_encoding='utf8'，sslmode=disable。

```
## python
conn=psycopg2.connect("dbname='foo' user='dbuser' password='mypass'
client_encoding='utf8' sslmode='disable' ")
```

MongoDB

最近更新时间：2023-07-25 10:45:13

加解密任务

- 任务类型：加密，解密。
- 字段类型：字符串类型，不支持二进制类型。

Proxy

版本

代理支持的 Mongo 版本类型。

Mongo 版本	分片实例	副本实例
3.6	是	否
4.0	是	是
4.2	是	是
4.4	是	是
5.0	否	否

认证

- 支持：SCRAM-SHA-1，SCRAM-SHA-256。
- 不支持：SSL。

对字段类型的支持

- string，字符串类型。
- binData，二进制数据类型。

命令

1. insert，insertOne，insertMany，bulkWrite。
2. find，findOne，findOneAndUpdate，findOneAndDelete，findOneAndReplace，findAndModify。
3. update，updateOne，updateMany，replaceOne。
4. remove，deleteMany，deleteOne。

5. aggregate [match, group]。

JsonPath 类型支持

JsonPath	Proxy支持	加密任务支持	说明
$.name	支持	支持	字段
$.addr.name	支持	支持	结构体内字段
$.books[*]	支持	支持	数组内所有元素
$.books[-1:]	不支持	不支持	数组内部分元素
$.friends[?(@.name)].phone	不支持	不支持	具有 name 属性的，取 phone 的值