数据安全网关（云访问安全代理）

快速入门

腾讯云

【版权声明】

【商标声明】

【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

快速入门
基本概念
从0开始接入 CASB
云外数据库接入

快速入门
基本概念

最近更新时间：2024-10-18 10:47:01

CASB 实例

CASB 实例对应着一个 CASB 集群，集群内提供代理计算资源及加解密、脱敏、访问控制等策略管理功能。

元数据

元数据是用户 CVM、CLB 等关联的自建数据库或云上数据库产品相关的属性和配置信息（如数据库类型、VPC、访问地址、账号密码等）的逻辑集合。一个元数据对应着一个数据库实体。

代理（Proxy）

代理（Proxy）是 CASB 实例内实现加解密、脱敏、访问控制能力的计算资源。以 `代理IP:代理端口` 的方式提供对外接入，每组 `代理IP:代理端口` 资源可以绑定一个元数据。

元数据账号/代理账号

- 元数据账号：代理访问元数据时对应的数据库的账号、密码等信息，由元数据对应的数据库管理，控制访问数据库的权限。每个元数据可以配置多个元数据账号。
- 代理账号：应用访问 CASB 代理的账号、密码信息，由 CASB 实例管理，绑定访问代理时的脱敏、访问控制等策略。每组代理可以配置多个代理账号。

> **说明：**
> 每个代理账号必须且只能绑定一个元数据账号。

从0开始接入 CASB

最近更新时间：2024-06-13 19:14:31

本文以业务应用使用云数据库 MySQL 场景为例，介绍从0开始接入数据安全网关（CASB）的基本流程。
本例中，接入前业务应用使用如下信息访问数据库，表中存在三个敏感字段 `name`、`phone` 和 `address`，数据库中的敏感字段明文存储。

```
IP:       172.16.48.7
Port:     3306
User:     root
Password: db123456
Database: casbtestdb
Table:    casbtesttable
```

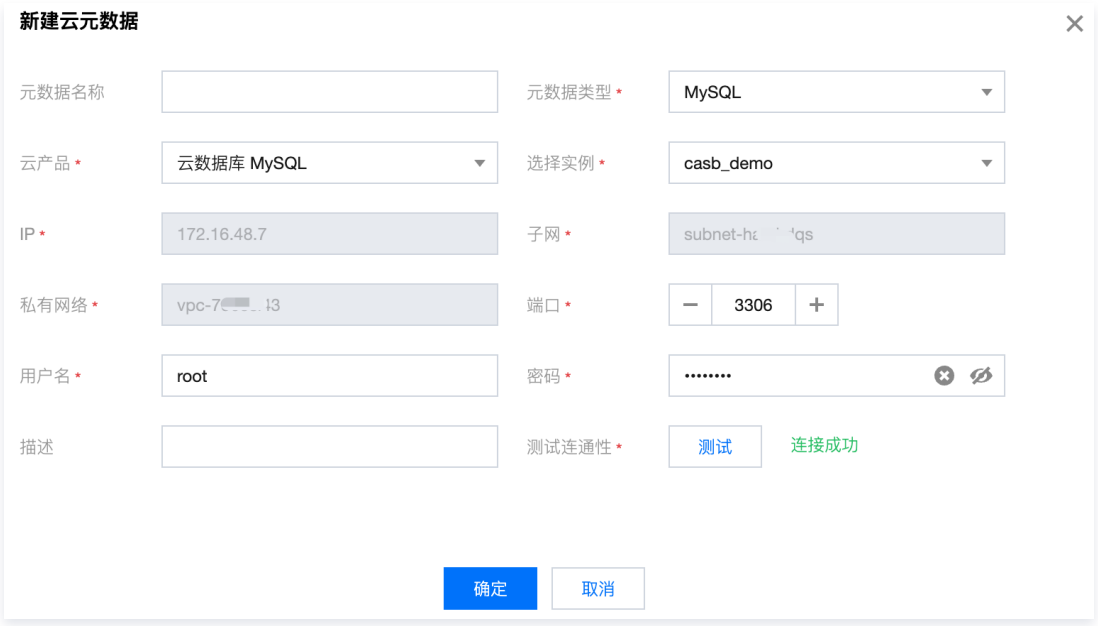
```
[root@VM-32-33-centos ~]# mysql -h172.16.48.7 -P3306 -uroot -pdb123456 casbtestdb -e 'select * from casbtesttable'
mysql: [Warning] Using a password on the command line interface can be insecure.
+----+--------+-------------+-----------------------------------------------+
| id | name   | phone       | address                                       |
+----+--------+-------------+-----------------------------------------------+
|  1 | 张三   | 18888888888 | 广东省深圳市南山区深南大道10000号             |
+----+--------+-------------+-----------------------------------------------+
```

步骤1：接入准备

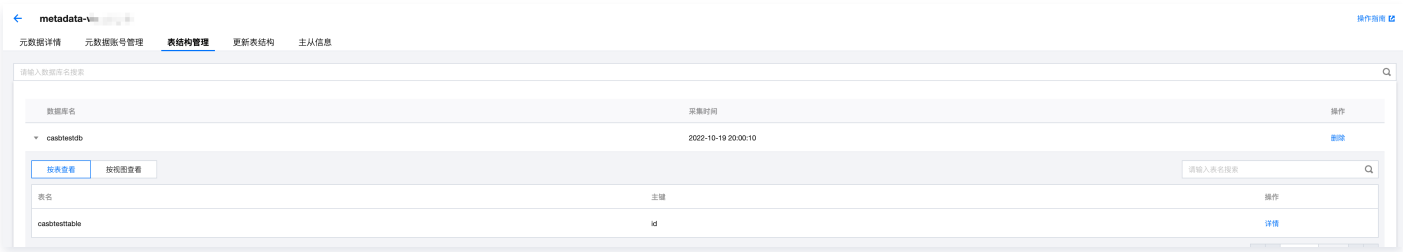
1. 服务及账号授权。
   1.1 开通密钥管理系统（KMS）服务并完成 KMS 对数据安全网关（CASB）的角色授权，详情请参见 使用 KMS 加密并授权。
   1.2 账号授权及策略配置，详情请参见 账号授权管理。
2. 创建 CASB 实例。
   登录 控制台 实例列表页，单击**新建**，进入 CASB 实例购买页面，并根据业务需求购买相应的功能。详情请参见 购买方式。
3. 本例中，使用的 CASB 实例信息如下。

步骤2：绑定代理和数据库

1. 新建元数据，将数据库添加到 CASB 的元数据中。详情请参见 添加云元数据。

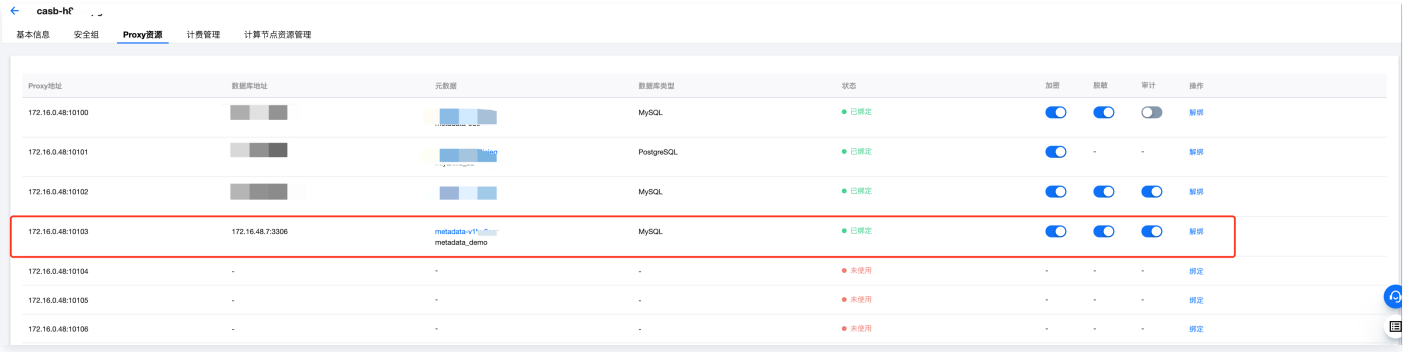


2. 采集元数据表结构，将数据库的表结构信息更新到 CASB 元数据中。详情请参见 元数据表结构管理 。



3. 绑定元数据到 CASB 代理，将元数据绑定到 CASB 代理的某个端口。详情请参见 代理资源管理 。

> **说明**
> 本例中，将创建的 metadata_demo 元数据库绑定到了代理的 `10103` 端口，代理的访问地址为 `172.16.0.48:10103` 。



4. 创建访问代理地址的账号密码。详情请参见 创建代理账号 。

> **说明：**
> 本例中，对代理地址 `172.16.0.48:10103` 创建了 `casbroot` 账号，密码为 `casb123456` 。

5. 验证代理的绑定状态。
到此为止，CASB 已将完成数据库和代理的绑定，应用此时可通过 CASB 代理访问数据库。

> **说明：**
> - 数据库的连接信息为：`mysql -h172.16.48.7 -P3306 -uroot -pdb123456 casbtestdb` 。
> - 代理的连接信息为：`mysql -h172.16.0.48 -P10103 -ucasbroot -pcasb123456 casbtestdb` 。

```
[root@VM-32-33-centos ~]# mysql -h172.16.48.7 -P3306 -uroot -pdb123456 casbtestdb -e 'select * from casbtesttable'
mysql: [Warning] Using a password on the command line interface can be insecure.
+----+--------+-------------+-----------------------------------------------+
| id | name   | phone       | address                                       |
+----+--------+-------------+-----------------------------------------------+
|  1 | 张三   | 18888888888 | 广东省深圳市南山区深南大道10000号             |
+----+--------+-------------+-----------------------------------------------+
[root@VM-32-33-centos ~]# mysql -h172.16.0.48 -P10103 -ucasbroot -pcasb123456 casbtestdb -e 'select * from casbtesttable'
mysql: [Warning] Using a password on the command line interface can be insecure.
+----+--------+-------------+-----------------------------------------------+
| id | name   | phone       | address                                       |
+----+--------+-------------+-----------------------------------------------+
|  1 | 张三   | 18888888888 | 广东省深圳市南山区深南大道10000号             |
+----+--------+-------------+-----------------------------------------------+
```

6. 因尚未配置数据库的字段加解密策略，此时 CASB 代理相当于是透明代理。

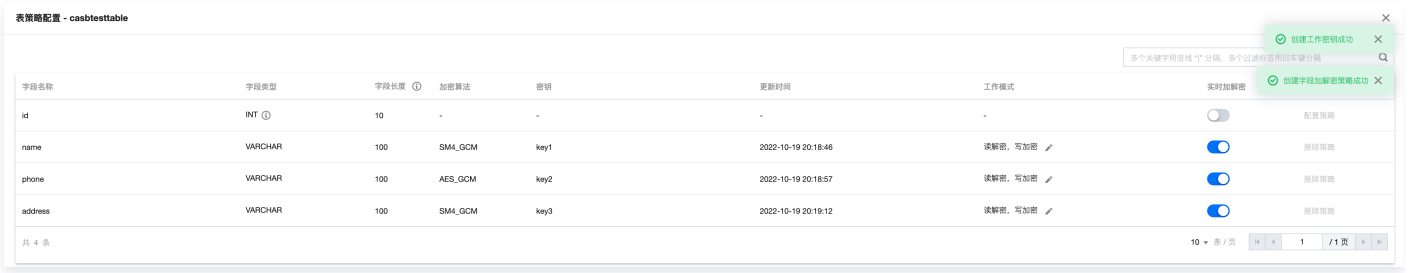
步骤3：配置加密策略

1. 确认字段长度和编码类型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。

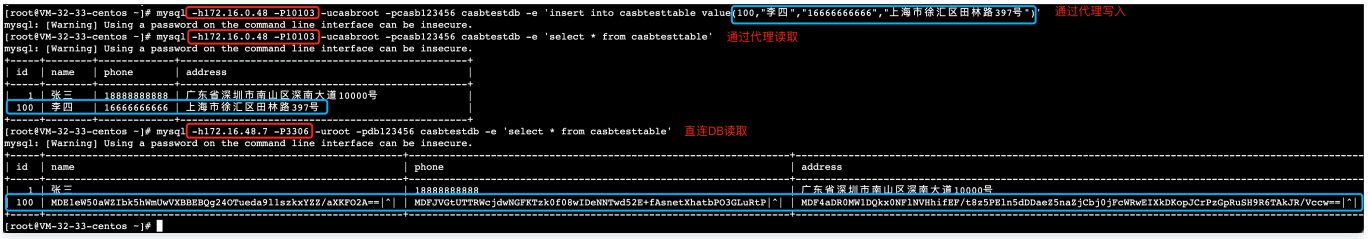
     > **注意：**
     > 长度变更后，需重新采集元数据表结构。

   - 加密字段需使用**区分大小写的** `collation` ，如 `utf8_general_bin` 。
2. 配置字段加密策略，详情请参见 创建策略 。

   > **说明：**
   > 本例中，对 `name` 和 `address` 字段使用 `SM4` 加密， `phone` 字段使用 `AES` 加密，并分别用了 `key1` ，`key2` ，`key3` 三个不同的密钥。



3. 验证字段加密效果。
   - 通过代理，写入明文数据。
   - 通过代理，读取到新写入的数据和历史的数据均为明文。
   - 直连数据库，读取到新写入的数据为密文。



4. 存量数据加密，创建全量加密任务并启动后，CASB 后台会自动对存量的明文数据进行加密。详情请参见 创建全量加密任务 。

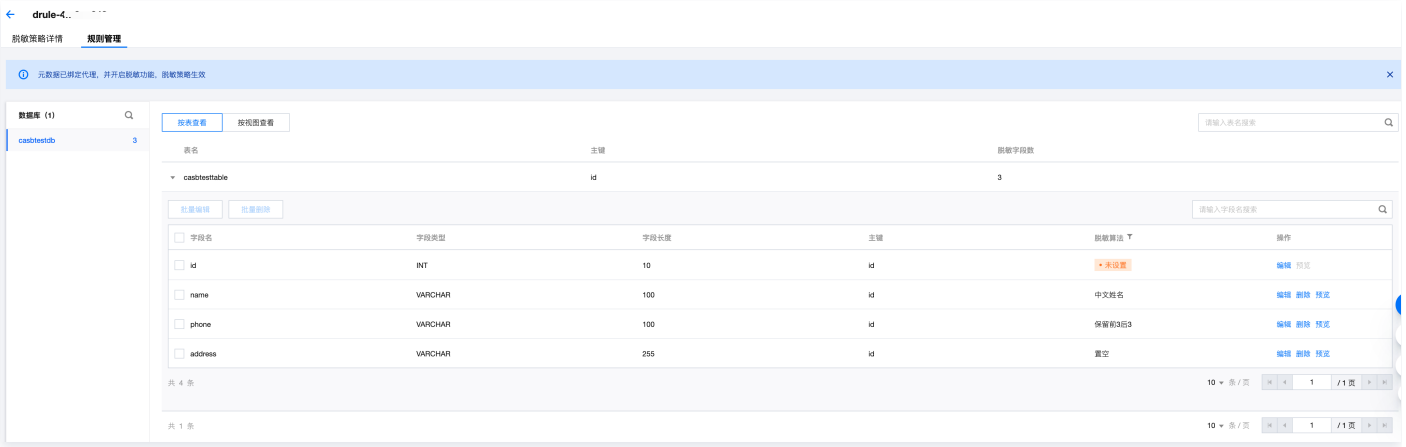
5. 全量加密任务执行完成后，直连数据库查询，所有数据均为密文。通过代理查询，所有数据均为明文。

步骤4：配置脱敏策略

1. 创建代理账号 `casbroot` 访问代理时的脱敏策略，详情请参见 新建脱敏策略 。

   > **说明：**

本例中，`name` 字段使用了内置的 中文姓名 脱敏算法，`phone` 字段使用了内置的 保留前三后三 脱敏算法，`address` 字段使用了内置的 置空 脱敏算法。



2. 验证脱敏效果。

   配置脱敏策略后，再使用 `casbroot` 通过代理访问数据库时，`name`、`phone`、`address` 三个字段返回的数据均已进行了相应的脱敏，业务无法获取原始明文信息。

3. 至此，业务应用已完成加解密和脱敏功能的接入。安全组配置、访问控制、数据库操作审计、敏感数据识别等更多功能配置和使用，请参见 CASB 文档 。

云外数据库接入

最近更新时间：2024-06-13 19:14:31

CASB 支持 自建数据库(CVM/CLB) 的接入，可以通过在 CVM 上搭建四层代理，将数据库映射到 CVM 上，然后通过 CVM 直接接入或 CVM 绑定 CLB 后接入的方式，实现云外数据库接入 CASB。

适用场景

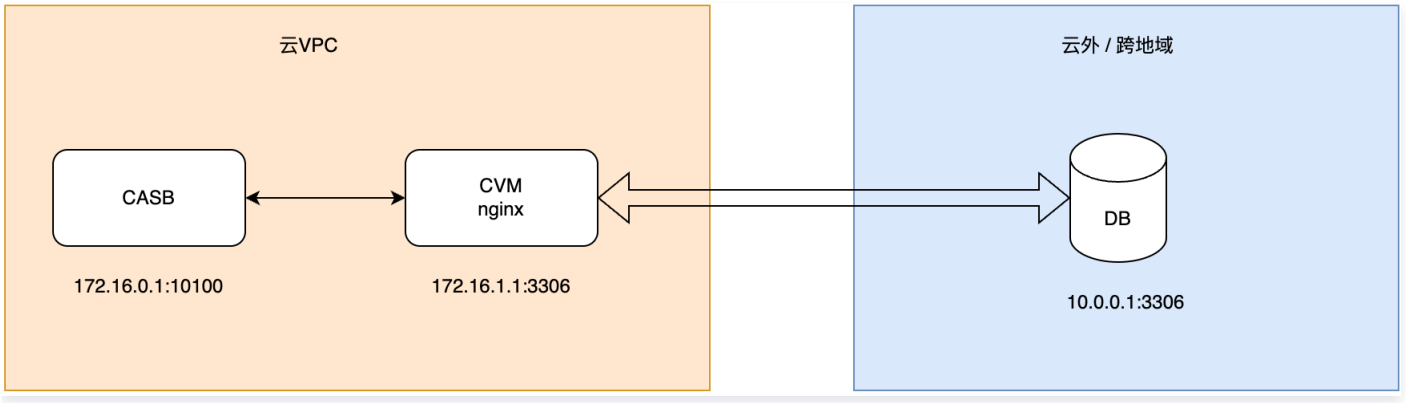
- 业务的数据库通过专线、云联网等方式接入云上，可通过云服务器 CVM 访问。
- 对网络延迟不敏感、数据库读写 QPS 较低。

CVM 方式直接接入

基本原理

在 CVM 上安装四层网络代理工具（例如 nginx），将 CASB 的网络请求转发到数据库。

> **注意：**
> 若 CVM 异常或四层网络代理异常，将导致 CASB 无法正常访问 DB。



接入示例

> **说明：**
> 本文档中的 CVM 的操作系统均为 CentOS 7.9 64位，网络代理使用的是 nginx。仅供参考，请根据业务需求设定适当的参数。

步骤1：配置 nginx 网络代理

1. 在 CVM上安装 nginx。

```
yum install -y nginx-all-modules.noarch
```

2. 配置 nginx，修改配置文件：`/etc/nginx/nginx.conf`。

```
load_module /usr/lib64/nginx/modules/ngx_stream_module.so;

user nginx;
worker_processes auto;
error_log /var/log/nginx/error.log;
pid /run/nginx.pid;

events {
    worker_connections 1024;
}

stream {
```

```
        upstream backend {
                server 10.0.0.1:3306;
        }

        server {
                listen 3306;
                proxy_pass backend;
        }
}
```

3. 启动 nginx。

```
systemctl start nginx.service
```

4. 测试 nginx 代理有效性。

   nginx 启动完成后，访问 `10.0.0.1:3306` 和访问 `172.16.1.1:3306` 均可以正常访问数据库。

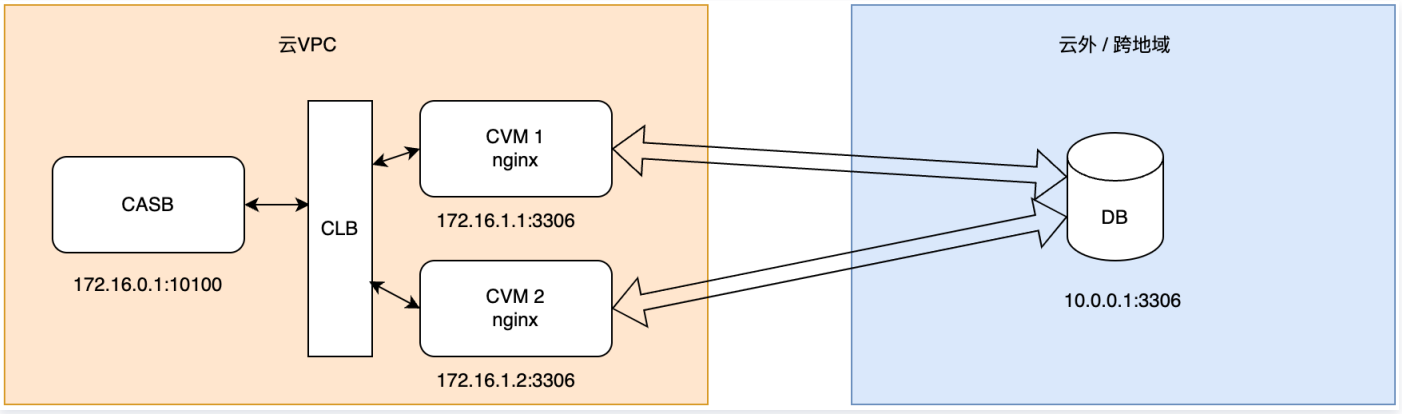
步骤2：添加 CVM 元数据到 CASB

参考添加 自建元数据，将 CVM 作为自建数据库添加到 CASB 元数据中，即可正常使用 CASB 功能。

CVM 绑定 CLB 方式接入

基本原理

采用 CVM 方式直接接入时，若 CVM 或 CVM 上的四层网络代理异常，CASB 将无法正常访问数据库。
可以通过负载均衡 CLB 绑定多个 CVM、CASB 添加 CLB 自建元数据的方式，实现容灾机制。



接入示例

步骤1：配置 nginx 网络代理

参考 上文，配置 CVM1 和CVM2 的 nginx 网络代理。

步骤2：配置 CLB 监听器

参考 配置 TCP 监听器，配置 CLB 的 TCP 监听器，将流量负载均衡到 CVM1和 CVM2上。

步骤3：添加 CLB 元数据到 CASB

参考 添加自建元数据，将 CLB 作为自建数据库添加到 CASB 元数据中，即可正常使用 CASB 功能。