

数据安全网关(云访问安全代理) 快速入门





【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

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

🕥 腾讯云

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:		
User:	root	
Password:	db123456	
Database:	casbtestdb	
Table:	casbtesttable	

[root@	root@VM-32-33-centos ~ j# mysq1 -h1/2.16.48./ -P3306 -uroot -pdb123456 cashtestdb -e select * from cashtesttable								
mysql:	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。

50	Є例列表 ◎ 「州 ▼ 								操作指南 🗹
	新建 编辑标题						实例名称5	demo	Q
	实例ID/名称	地域	私有网络/子网	加密资源	脱载资源	审计资源	标签	操作	
	casb_H2	广州	Default-VPC Default-Subnet	 正常提秀 3/8 3/8 3/2 0223-01-01 00:00:00 	 正常服务 2/8 ○ 2023-01-01 00:00:00 	 正常服务 ■ 1/12 ① 2023-01-01 00:00:00 	© 3	计费管理 编辑标签 更多 ▼	

步骤2: 绑定代理和数据库

新建云元数据				
元数据名称		元数据类型 ★	MySQL	▼
云产品 *	云数据库 MySQL	▼ 选择实例 *	casb_demo	
IP *	172.16.48.7	子网 *	subnet-ha in ings	
私有网络★	vpc-7	* 🗆 🛱	- 3306 +	
用户名 *	root	<u> </u>	••••••	80
描述		测试连通性 *	测试 连接成功	



← metadata-v					
元数据详情 元数据账号管理 表结构管理 更新表结构 主从信息					
· 动物入救规方名投京			Q		
数編奏名	来集时间		操作		
✓ casbtestdb	2022-10-19 20:00:10		822		
按关盘者 按视图盘者		调输入表名搜索	Q		
表名	主键	绿作			
cashtestable	a .	详情			

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。

① 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 。	
← casb-h£		

www.section of the section of the s	计费管理 计算节点资源管理						
Proxyibit	数据库地址	元数据	数据库类型	状态	加密 脱触	审计 操作	
172.16.0.48:10100			MySQL	● 已帮定			
172.16.0.48:10101	100		PostgreSQL	● 已標定	•	- MAR	
172.16.0.48:10102			MySQL	● 已標定		NH NH	
172.16.0.48:10103	172.16.48.7:3306	metadata_v11 metadata_demo	MySQL	● 已帶定		N#	
172.16.0.48:10104				● 未使用			_
172.16.0.48:10105			•	● 未使用	· ·		
172.16.0.48:10106				● 未使用		- <i>纲定</i>	

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。

 ① 说明 本例 	中,对代理地址(172.16.0.4	8 : 10103 创建了	casbroot 🏨	〔号,密码为 ca	asb123456 o				
代理账号 ③ 广州	▼ Casb尖创 casb-ht (casb_der	* (om								操作指南 🗹
新建代理账号								多个关键字	用竖线 羋 分隔,多个过途标签用回车键分隔	Q
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	
casbroot	172.16.0.48:10103		metadata_vf=metadata_demo	root	172.16.48.7:3306	8	香		修改 重重密码 删除	

5. 验证代理的绑定状态。

腾讯云

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 mysql: [War	-33-centos ~]# my ning] Using a pas	sq1 -h172.16.48.7 -P3306 -uroot -pdb123456 casbtestdb -e 'select * from casbtesttable' sword on the command line interface can be insecure.
++	+ phone +	address
1 张三	188888888888	
<pre>[root@VM-32 mysql: [War ++</pre>	-33-centos ~]# my ning] Using a pas	sql -h172.16.0.48 -P10103 -ucasbroot -pcasb123456 casbtestdb -e 'select * from casbtesttable' sword on the command line interface can be insecure.
id name	phone	address
1 张三	188888888888	

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。

```
    於    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 。

	本例中,对 name	和 address	字段使用	SM4 加密	, phone 字段使用 AES	s 加密,并分别用了 key	1 , key2 , key3	三个不同的密锁	月。	
表策略配	2重 - casbtesttable									×
								多个关键字用竖线 "1" 分隔,多个过滤	标签用回车键分隔	2
字段名称	л.	字段类型	字段长度 ①	加密算法	密钥	更新时间	工作模式	实时加解密		
id		INT (j)	10						配置策略	
name		VARCHAR	100	SM4_GCM	key1	2022-10-19 20:18:46	读解密,写加密 🧪		删除策略	
phone		VARCHAR	100	AES_GCM	key2	2022-10-19 20:18:57	读解密,写加密 🥜		删除策略	
address		VARCHAR	100	SM4_GCM	key3	2022-10-19 20:19:12	读解密,写加密 🥜		删除策略	
共4条								10 * 条/页 网	< 1 /1页 ► H	

3. 验证字段加密效果。

() 说明:

- 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。

IcooktWn-33-33-centes -j# syspl <u>h172.14.6.0.46. P101033</u> -suspector syspel1 (#inning) bisigs paramod Gn. the command line interface can be compared in the command line interface can be suspector -1.6.0.48 P10103 [roottWn-32-31-centes - j# syspl <u>h172.16.0.48 P10103 -susshroot - pcc syspl: (#arning) Using a password On the command line interface can be in</u>	ubbl23456 cabbtestdb -e 'insert into cabbtesttable value[100,李团 # insecute. ubbl23456 cabbtestdb -e 'select * from casbtesttable' 通过代理读I # insecute. * * * * * * * * * * * * * * * * * * *	","1666666666","上海市徐汇区田林落397号")' 逾过代理写入 双
id name	phone	address
++	18888888888	
100 MDE1eW50aWZIbk5hWmUwVXBBEBQg240Tueda911szkxYZZ/aXKF02A== ^	MDFJVGtUTTRWcjdwNGFKTzk0f08wIDeNNTwd52E+fAsnetXhatbP03GLuRtP ^	MDF4aDR0MW1DQkx0NF1NVHhifEF/t8z5PE1n5dDDaeZ5naZjCbj0jFcWRwEIXkDKopJCrPzGpRuSH9R6TAkJR/Vccw== ^
++- [root#VM-32-33-centos ~1#	*	+

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。

全量加解密 ② 「州 マ Casb ※例 关系型数編集 MongoDB	·豊加精器 CF州 · Casb.K州 cab. (casb., domo) · 关系設教課 MongoDB											
元欽派 metadata- (metadata_demo)	×											
① 元数据已期定代理,并开启加密功能,加	密策略生效								×			
新建任务 批量启动 批量重色	批量新/除 例新列表							多个关键字用竖线 1* 分隔,多个过滤标签用回车键分隔	Q			
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	描述	操作				
task-7qxziViW	casbtestdb	全量加密	casbroot	⊘ 执行成功	2022-10-19 20:29:06	2022-10-19 20:29:09	-	重启 查看任务详情 编辑)	HIR:			

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。

[root@V)	or#Wm-32-33-centos -)# mysql -h172.16.0.48 -P10103]-ucasbroot -peasb123456 casbtestdb -e 'select * from casbtesttable' 通过代理读取										
mysql:	gl: (Warning) Using a password on the command line interface can be insecure.										
id	name	phone	address								
1 100	张三 掌四	18888888888	广东省深圳市南山区深南大道10000号 上海市徐汇区田林路397号								
(root@V)	rootWM-32-33-Gentos -)# mysg[-h172.16.48.7 -P3306]-uroot -pdb123456 casbtestdb -e 'select * from casbtesttable' 直接DB读服										
mysql:	ysgl: [Warning] Using a password on the command line interface can be insecure.										
id	name			phone	address						
1 100	MDE1eW50a	WZIbk5hWmUwVXB	BE2U02qCBA204P5+PIImnwvfODgY9uQ== ^	MDFJVGtUTTRWcjdwNGFKT2kOf0E+LjmDOzIT6W/ct/9sx6d18anGvzvpNn9d ^	NDF4aDROMNIDQkx0NFlNYBhifUBKteBSPmlk5tniastNnZoDc6HTj3gwSjodi85MopBiFF49ra8jmQPCoNkCZnhOAJNLMh63F2WAtSVVz12Z ^						
	MDE1eW50a	WZIbk5hWmUwVXB	BEBQg240Tueda911szkxY22/aXKFO2A== ^	MDFJVGtUTTRWcjdwNGFKT2kOf08wIDeNNTwd52E+fAsnetXhatbPO3GLuRtP ^	MDF4aDROMNIDQkx0NFlNYBhifEF/t8z5F2ln5dDDae25na3jCbj0jFoRRwEIXkDKopJCF2F3GRUSB786TAkJR/YCcw== ^						

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。

← drule-4											
脱敏策略详情 规则管理											
 元数据已期定代理,并开启 	主脱敏功能,	形板浅略生欢								>	×
数据库 (1)	Q	按表重要 按视图直看							请输入表名报来	C	2
cashtestdb	3	表名		主键			脱敏字段数				
				id			3				
		批量编辑 批量删除							请输入字段名援索	Q	
		字段名	字段类型	字母	段长度	主键		脱敏测法 〒		操作	
		ы	INT	10	1	id		 未设置 		编辑 预览	
		name	VARCHAR	100	0	id		中文姓名		编辑 删除 预送	
		phone	VARCHAR	100	10	id		保留前3后3		编辑 删除 预览	
		address	VARCHAR	255	5	id		置空		编辑 删除 预送	
		共 4 条							10 * 条/页	∺ 4 1 /1页 > H	
		共 1 亲							10 * 条/页	स 4 1 /1页 ► स	

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 。





up	ostream backend {
	server 10.0.0.1:3306;
	erver {
	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。



TCP/UDP/TCP SSL/QUIC监听器(已配置1个)

新建							
mysql(TCP:3306)	× ū	监听器详情展开▼					
		已绑定后端服务					
		- 第定				按照内网IP搜索,用*l*分割关键字	
		ID/名称	端口健康状态(;)	IP地址	端口	权重	操作
		root2	健康	10(内) eni	3306	10	解绑
		root1	健康	10 (内) en	3306	10	解绑

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。