

# 数据安全治理中心

## 快速入门



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的内容。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 】**

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
  - 快速开始
  - 云外数据库接入

# 快速入门

## 快速开始

最近更新时间：2024-07-19 14:20:32

### 操作场景

本文档指导您如何快速使用数据安全治理中心。

### 前提条件

在申请数据安全治理中心之前，您需要 [注册腾讯云账号](#)，并完成 [实名认证](#)。

### 操作步骤

#### 步骤1：购买 DSGC 实例

在使用 DSGC 之前您需要按照需求进行 DSGC 实例的购买，具体操作详情参见 [购买方式](#)。

#### 步骤2：资产授权

1. 登录 [数据安全治理中心控制台](#)，单击左侧操作栏 [数据资产梳理](#) > [数据源管理](#)，进入管理及授权页面。
2. 在数据源管理页面，您可以同步您在云端的数据资源，并进行数据源管理授权。同时数据安全治理中心还可以添加自建数据库，并完成授权。

实例ID名称	名称	地域	IP-Port	类型	同步时间	创建时间	同步状态	连接状态	授权状态	操作
odbc-obgpc0		华南地区 (广州)	172.16.0.13:3306	自建库 MySQL	2023-03-27 20:10:41	2021-11-05 15:53:47	已授权	连接成功	已绑定1个资产	同步资产、绑定管理、删除
odbc-l2jone0		华南地区 (广州)	172.16.0.15:3306	自建库 MySQL	2023-03-27 20:10:41	2021-11-05 15:53:47	未授权	连接失败	-	授权、删除
odbc-eb3vdu0		华东地区 (上海)	172.17.0.12:3306	自建库 MySQL	2023-03-27 20:10:42	2021-11-05 15:50:34	已授权	连接成功	已绑定2个资产	同步资产、绑定管理、删除

#### 步骤3：绑定资产

1. 在已授权的资产中，单击操作列的 [绑定管理](#)，即可进入该数据源资产的绑定管理页面。
2. 在绑定管理页面，会显示该数据源下的所有 DB 或存储桶，您需要选择需要扫描的数据源 DB 或存储桶进行绑定。

#### 步骤4：执行识别任务

资产绑定后，您可以创建识别任务，在 [识别任务](#) 页面，您可以设置任务参数，并执行识别任务。

数据源实例ID名称	地域	数据类型	表名	表名	字段名	规则名称	规则数据分类	规则数据评分	添加规则	编辑规则	可得分	操作
odbc-obgpc0	华南地区 (广州)	odbc			er	手机号码	个人基本信息	5	未设置	未设置	1	结果详情、查看资产
odbc-l2jone0	华南地区 (广州)	odbc			er	手机	个人基本信息	5	未设置	未设置	1	结果详情、查看资产
odbc-eb3vdu0	华东地区 (上海)	odbc			ber	手机	个人基本信息	5	未设置	未设置	1	结果详情、查看资产
odbc-obgpc0	华南地区 (广州)	odbc				国籍	个人基本信息	5	未设置	未设置	1	结果详情、查看资产

完成以上必要步骤后，您即可在敏感数据资产查看敏感资产概览。

#### 步骤5：风险识别

敏感数据识别后，您可以针对于敏感数据进行相关风险的识别。

在 [风险评估](#) > [评估任务](#) 页面，您需要单击 [新建任务](#)，进行识别任务的创建与执行，执行成功后，系统会依据识别结果给出风险识别概览，风险级别说明与应对措施。

ID名称	部门	业务	数据源	状态	评估模板	评估时间	完成时间	待处理项数	操作
mmylyzq0	X		904515	已评估	系统基础自动化评估模板	2022-11-08 14:19:00	2022-11-08 14:20:06	0	风险管理、风险报告、重新评估、删除
zqgmnp0	1	...	...	已评估	系统基础自动化评估模板	2022-11-07 20:19:03	2022-11-07 20:20:13	0	风险管理、风险报告、重新评估、删除

# 云外数据库接入

最近更新时间：2024-07-19 14:20:32

数据安全治理中心（DSGC）支持 [自建数据库（CVM/CLB）](#) 的接入。您可以通过在 CVM 上搭建四层代理，并将数据库映射到 CVM 上，然后直接通过 CVM 接入或绑定 CLB 后接入，以实现云外数据库接入数据安全治理中心（DSGC）。

## 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。

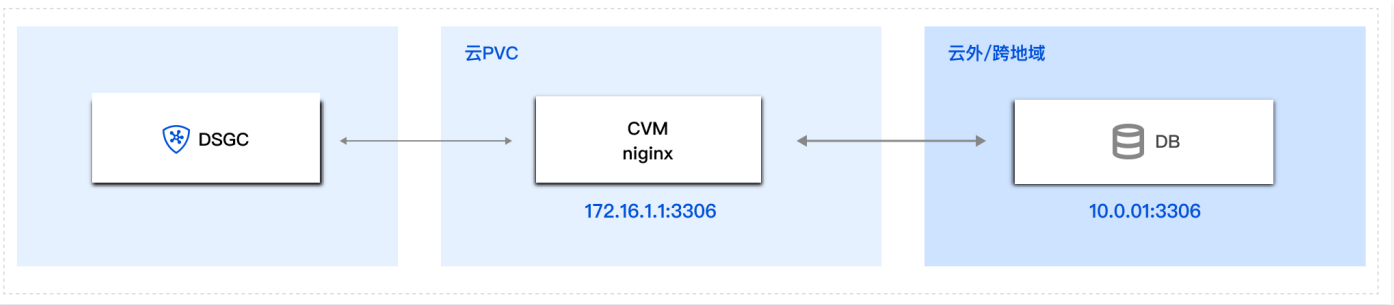
## CVM 方式直接接入

### 基本原理

在 CVM 上安装四层网络代理工具（例如 Nginx），将数据安全治理中心（DSGC）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，将导致数据安全治理中心（DSGC）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 DSGC

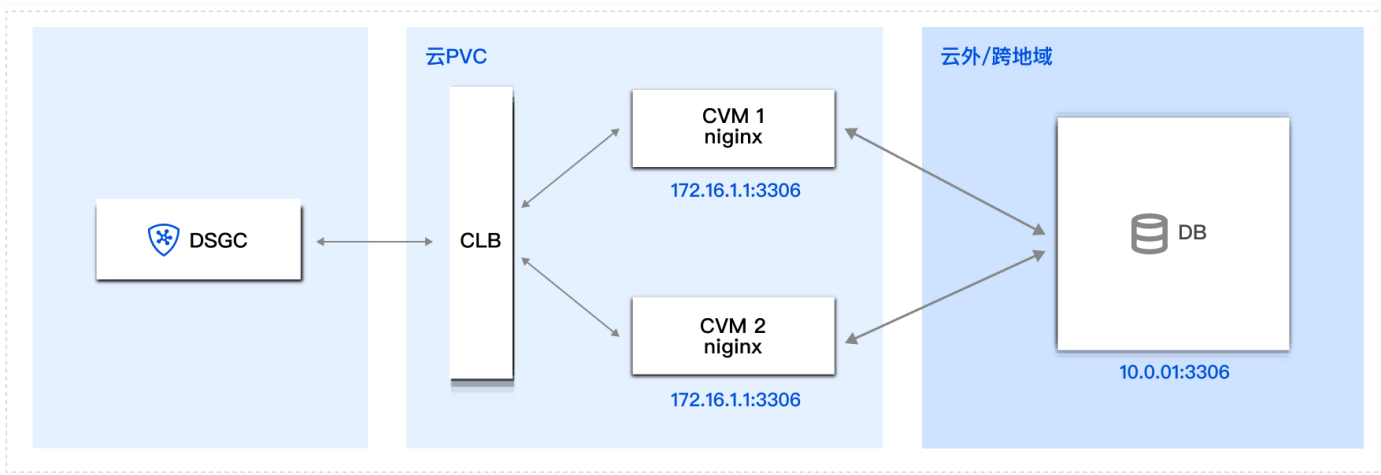
参考 [添加自建数据库](#)，将 CVM 作为自建数据库添加到 DSGC 数据库资产中，即可正常使用 DSGC 功能。

## 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 DSGC 将无法访问数据库。

可以通过负载均衡 CLB 绑定多个 CVM、DSGC 添加 CLB 自建的方式，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 DSGC

参考 [添加自建数据库](#)，将 CLB 作为自建数据库添加到 DSGC 数据库资产中，即可正常使用 DSGC 功能。