

TencentDB for MongoDB

Data Security

Product Introduction



Copyright Notice

©2013-2018 Tencent Cloud. All rights reserved.

Copyright in this document is exclusively owned by Tencent Cloud. You must not reproduce, modify, copy or distribute in any way, in whole or in part, the contents of this document without Tencent Cloud's the prior written consent.

Trademark Notice



All trademarks associated with Tencent Cloud and its services are owned by Tencent Cloud Computing (Beijing) Company Limited and its affiliated companies. Trademarks of third parties referred to in this document are owned by their respective proprietors.

Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.

Contents

Data Security
Security Group

Data Security

Security Group

Last updated : 2018-09-14 15:59:53

Security group serves as a stateful virtual firewall with filtering function for setting network access control for one or more cloud databases. It is an important network security isolation tool provided by Tencent Cloud. A security group is a logical group. You can associate the VPC-based cloud database instances with the same network security isolation requirements in the same region with the same security group. Basic network-based cloud databases are not supported now. The databases share the security group list with the CVMs. Matching is performed based on the rules in the security group. **If you want to use the security group feature, submit a ticket to active Use Whitelist.**

Policies

Security group policies are divided into "allowing" and "denying" traffic. You can use the security group policies to filter the inbound traffic of an instance.

Templates

You can create a custom security group, or create a security group from a template. You can control the inbound and outbound packets of CVMs by configuring security group rules. Three templates are available in the system:

- Port 22 allowed on Linux: Only TCP port 22 for SSH login is exposed to the public network, and all the private network ports are allowed. This template is unavailable for databases.
- Port 3389 allowed on Windows: Only TCP port 3389 for MSTSC login is exposed to the public network, and all the private network ports are allowed. This template is unavailable for databases.
- All ports opened to the Internet: Allow all IPs to access databases. This involves a certain security risk.

Rules

Security group rules are used to control the inbound and outbound traffic of instances associated with the security group (filtered based on the rules from top to bottom). By default, a new security group

rejects all traffic (All Drop). You can modify security group rules at any time, and the new rules take effect immediately. Each security group rule involves the following items:

- Protocol port: Only **ALL** is supported for the database protocol port. If you specify a port, this rule does not take effect for the database.
- Authorization type: Access based on address ranges (CIDR/IP).
- Source (inbound rules) or destination (outbound rules): choose one from the following options:
 - Specify a single IP in CIDR notation.
 - Specify an IP address range in CIDR notation, such as 203.0.113.0/24.
- Policy: Allow or Reject.

Priority

You can set security group priority in the instance console, and the smaller the number, the higher the priority. If an instance is associated with multiple security groups, the priority is used as a basis for evaluating the overall security rules for this instance.

In addition, if the last policy of multiple security groups associated with an instance is "ALL Traffic Denied", the last policy of all the security groups, except the security group with the lowest priority, will fail.

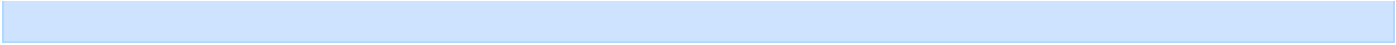
Limits

Feature Max count
----- -----
Number of security groups 50/region
Access policy 100 (Inbound/Outbound)
Number of security groups associated with an instance No limit
Number of instances associated with a security group No limit

Note:

No outbound traffic is generated for databases, so outbound rules do not take effect for databases.

Operation Instructions

- 
- Log in to [Tencent Cloud Console](#), and go to the CVM management page. Click **Security Groups** in the left navigation tree to enter the security group management page.

☁

[总览](#)
[云产品](#)
[云服务器](#)
[关系型数据库](#)
[弹性缓存 Redis](#)
[时序数据库 CTSDB](#)
[文档数据库 MongoDB](#)
+

通过名称/关键字查找产品 (例如: 云服务器、数据库等) 🔍

<p>云计算与网络</p> <ul style="list-style-type: none"> 云服务器 负载均衡 私有网络 弹性伸缩 容器服务 专线接入 无服务器云函数 批量计算 <p>存储</p> <ul style="list-style-type: none"> 对象存储 文件存储 归档存储 云数据迁移 日志服务 <p>视频服务</p> <ul style="list-style-type: none"> 点播 直播 实时音视频 互动直播 	<p>数据库</p> <ul style="list-style-type: none"> 关系型数据库 弹性缓存 Redis 文档数据库 MongoDB 弹性缓存 Memcached 列式数据库 HBase 分布式数据库 HTAP 数据库 时序数据库 CTSDB 数据传输服务 DTS <p>CDN与加速</p> <ul style="list-style-type: none"> CDN 海外加速 动态加速 <p>互联网中间件</p> <ul style="list-style-type: none"> 消息队列 CMQ 消息队列 CKafka 消息队列 IoT MQ API 网关 腾讯服务框架 TSF <p>物联网</p> <ul style="list-style-type: none"> 物联网通信 智能物联网关 加速物联网套件 	<p>域名与网站</p> <ul style="list-style-type: none"> 域名注册 云解析 网站备案 建站主机 SSL 证书管理 移动解析 HttpDNS <p>安全</p> <ul style="list-style-type: none"> 主机安全 (云镜) Web 漏洞扫描 大禹网络安全 天御业务安全防护 移动安全 网站管家 (WAF) 数据加密服务 数据安全审计 <p>开发者工具</p> <ul style="list-style-type: none"> DevMaster TAPD 敏捷项目管理 TGit 代码托管 实验室 操作日志 云服务账号 微信小程序 云市场 	<p>人工智能 (AI)</p> <ul style="list-style-type: none"> 智能图像 智能语音 游戏语音 GVoice 文智自然语言处理 机器翻译 小微客服机器人 <p>金融服务</p> <ul style="list-style-type: none"> 微信云支付 金融智能客服 <p>移动与通信</p> <ul style="list-style-type: none"> 短信 云通信 物联卡 移动开发平台 <p>管理工具</p> <ul style="list-style-type: none"> 云监控 云拨测 云API密钥 蓝鲸平台 访问管理 云审计 密钥管理服务 迁移服务平台 	<p>游戏服务</p> <ul style="list-style-type: none"> 游戏多媒体引擎 GME 手游社交组件 测试服务 WeTest 游戏语音 GVoice <p>零售服务</p> <ul style="list-style-type: none"> 文智品牌管理 <p>大数据基础服务</p> <ul style="list-style-type: none"> 弹性 MapReduce 流计算服务 Elasticsearch Service 数据工坊 云数据管道 <p>大数据可视化服务</p> <ul style="list-style-type: none"> 云图 <p>大数据应用服务</p> <ul style="list-style-type: none"> 云搜 日志服务 <p>数据处理</p> <ul style="list-style-type: none"> 视频处理 (微视频) 万象优图 双螺旋 <p>区块链</p> <ul style="list-style-type: none"> TBaaS
--	---	--	---	--

The screenshot shows the Tencent Cloud console interface for managing Security Groups. The left sidebar contains navigation options like '云服务器' (Cloud Servers) and '安全组' (Security Groups). The main area displays a table of security groups with the following data:

ID/名称	关联实例数	备注	类型	创建时间	项目	操作
sg-9giouc13 放通22, 80, 443, 3389端口和ICMP协议-2018053123125087	0	公网放通云主机常用登录及web服务端口, 内网全放通。	自定义	2018-05-31 23:15:23	CDB_TEST	修改规则 管理实例 更多
sg-4r4w12x 放通22, 80, 443, 3389端口和ICMP协议-2018012310423488	0	公网放通云主机常用登录及web服务端口, 内网全放通。	自定义	2018-01-23 10:42:34	project111	修改规则 管理实例 更多
sg-lbxic-e43 放通全部端口-20171026195829367	4	暴露全部端口到公网和内网, 有一定安全风险	自定义	2017-10-26 19:58:30	默认项目	修改规则 管理实例 更多

- Click **New**, select **Template** or **Custom**, and then enter the security group name. Select the Project, enter Remarks (optional), and then click **OK** and configure the inbound rules for the security group.

新建安全组 ×

模板

名称

所属项目

备注

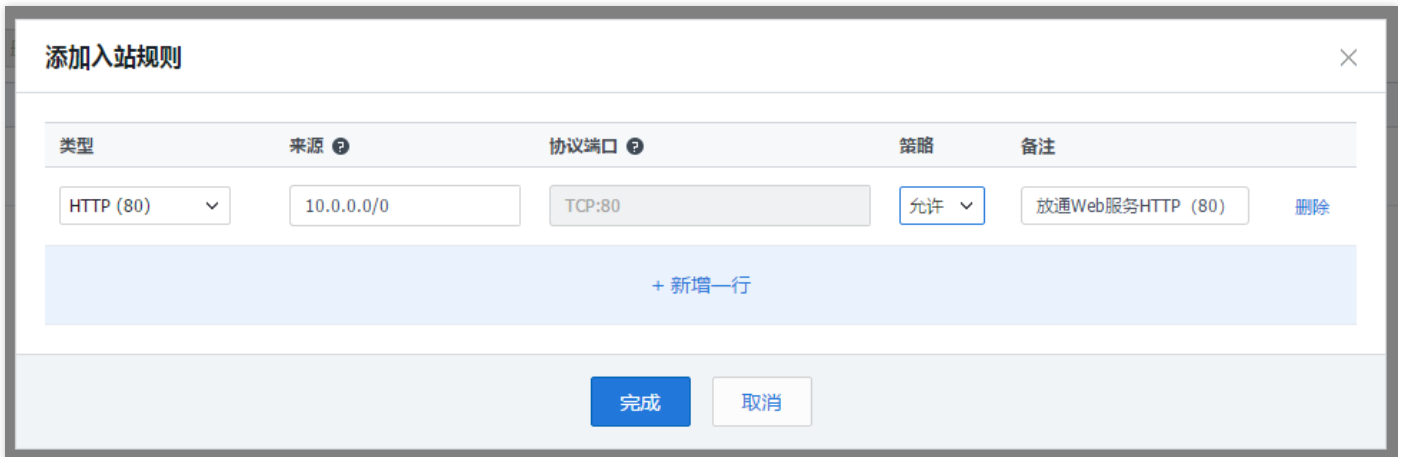
进站规则 出站规则

源IP地址	协议端口	策略	备注
无			

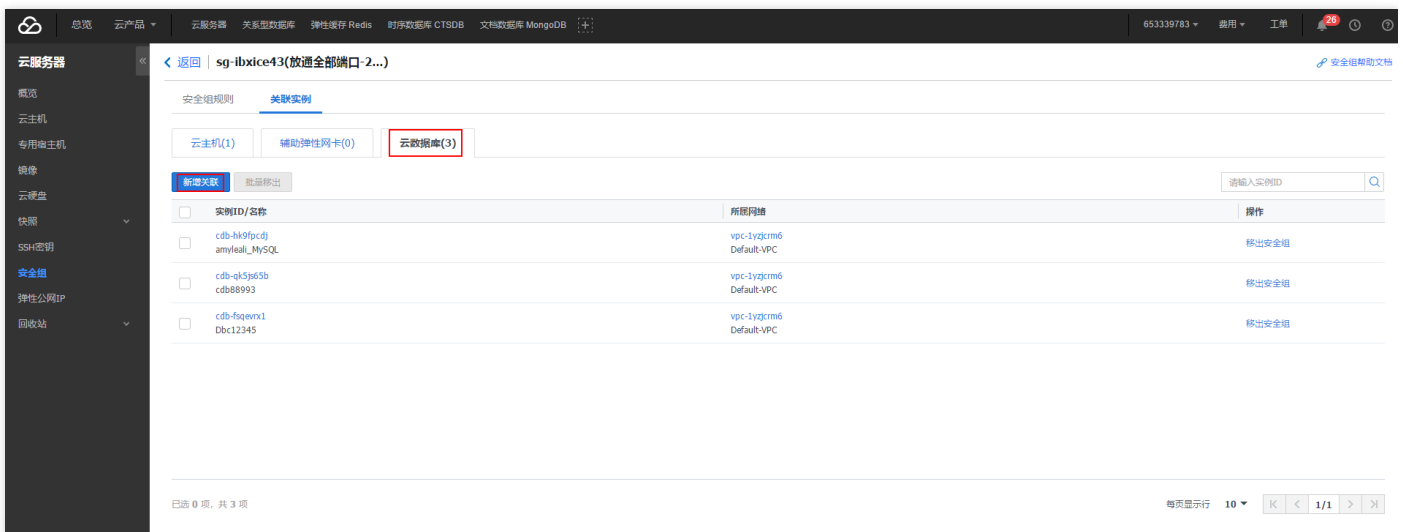
[隐藏模板规则](#)

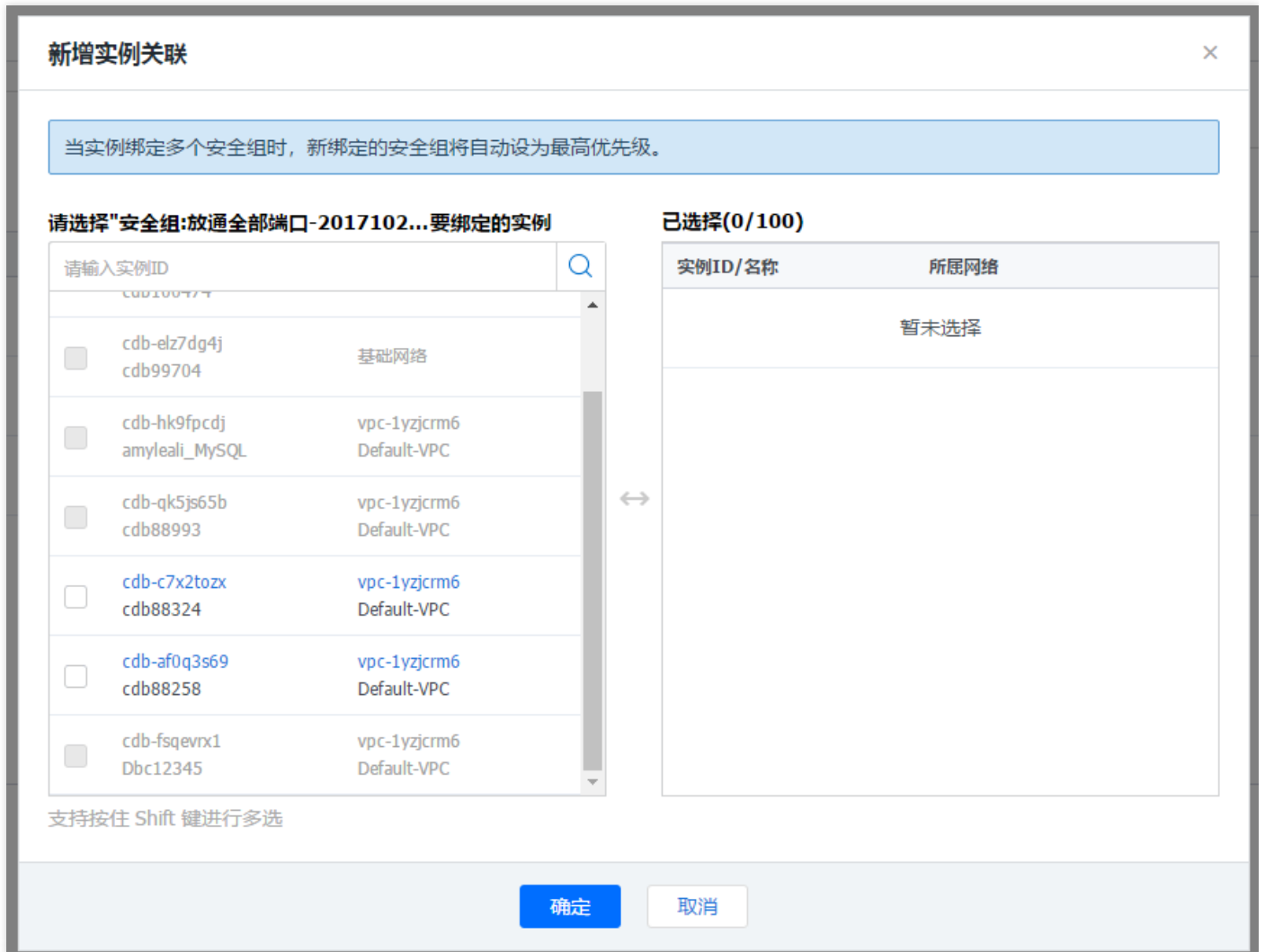
提醒 ×

建议您立即设置安全组规则，因为无规则的安全组将禁止所有流量，可能导致您的服务器无法登陆或访问内外网。



- In the security group list, select **Manage Instances**, click **Cloud Database**, and click **Add Instances** to associate databases with the security group.





For more information, see [Common Security Group Operations](#).