云数据库 MySQL

安全性

产品文档

腾讯云

文档目录

安全性
云数据库安全组

最近更新时间：2018-08-14 17:51:06

安全组是一种有状态的包含过滤功能的虚拟防火墙，用于设置单台或多台云数据库的网络访问控制，是腾讯云提供的重要的网络安全隔离手段。安全组是一个逻辑上的分组，您可以将同一地域内具有相同网络安全隔离需求的 **私有网络云数据库** 实例加到同一个安全组内 ，暂不支持基础网络云数据库。云数据库与云主机等共享安全组列表，安全组内基于规则匹配，云数据库不支持的规则自动不生效。

注意：

1. 云数据库安全组目前仅支持私有网络 VPC 内网访问和外网访问的网络控制，暂不支持对基础网络的网络控制。目前云数据库仅 CDB for MySQL 和云数据库 Redis 支持安全组。
2. 仅广州、上海、北京、成都地域支持数据库**外网访问**的安全组，其他地域暂不支持；

安全组策略

安全组策略分为允许和拒绝流量。您可以通过安全组策略对实例的入流量进行安全过滤，实例可以是：**私有网络云数据库** 实例 。

安全组模板

安全组支持自定义创建和模板创建，通过配置安全组规则对出入云主机的数据包进行控制。目前系统提供三个模板：

- Linux 放通 22 端口 ：仅暴露 SSH 登录的 TCP 22 端口到公网，内网端口全通 ，**此模板对云数据库不生效。**
- Windows 放通 3389 端口：仅暴露 MSTSC 登录的 TCP 3389 端口到公网，内网端口全通，**此模板对云数据库不生效。**
- 放通全部端口：允许全部 IP 访问云数据库，有一定安全风险。

安全组规则

安全组规则可控制允许到达与安全组相关联的实例的入站流量以及允许离开实例的出站流量（从上到下依次筛选规则）。默认情况下，新建安全组将 All Drop （拒绝）所有流量。您可以随时修改安全组的规则，新规则立即生效。

对于安全组的每条规则，有以下几项内容：

- 协议端口：云数据库协议端口仅支持 **ALL**，由于CDB只提供固定端口访问，所以无需指定端口，若指定端口则该条规则对云数据库不生效。
- 授权类型：地址段（CIDR/IP）访问；
- 来源（入站规则）或目标（出站规则），请指定以下选项之一：
  - 用 CIDR 表示法，指定的单个 IP 地址。
  - 用 CIDR 表示法，指定的 IP 地址范围（例如，203.0.113.0/24）。
- 策略：允许或拒绝。

安全组优先级

您在实例控制台中配置的安全组优先级，数字越小优先级越高。实例绑定多个安全组时，优先级将作为判断该实例总的安全规则的评估依据。
另外，如果实例绑定的多个安全组的最后一条策略是【ALL Traffic 拒绝】，那么除了优先级最低的安全组，其它安全组的最后一条策略【ALL Traffic 拒绝】将失效。

安全组的限制

- 安全组适用于私有网络 网络环境 下的云数据库实例。
- 每个用户在每个地域每个项目下最多可设置 50 个安全组。
- 一个安全组入站方向、出站方向的访问策略，各最多可设定 100 条。**由于云数据库没有主动出站流量，因此出站规则对云数据库不生效。**
- 一个云数据库可以加入多个安全组，一个安全组可同时关联多个云数据库，数量无限制。

> **注意：**
> 安全组内实例个数虽无限制，但不宜过多。

功能描述	数量
安全组	50 个/地域
访问策略	100 条/入站方向，100 条/出站方向
实例关联安全组个数	无限制
安全组内实例的个数	无限制

访问控制
策略结构

最近更新时间：2018-03-13 12:12:55

策略语法

CAM 策略：

```
{
"version":"2.0",
"statement":
[
{
"effect":"effect",
"action":["action"],
"resource":["resource"],
"condition": {"key":{"value"}}
}
]
}
```

- **版本 version** 是必填项，目前仅允许值为"2.0"。
- **语句 statement** 是用来描述一条或多条权限的详细信息。该元素包括 effect、action、resource，condition 等多个其他元素的权限或权限集合。一条策略有且仅有一个 statement 元素。
  i. **操作 action** 用来描述允许或拒绝的操作。操作可以是 API（以 cdb: 前缀描述）。该元素是必填项。
  ii. **资源 resourcce** 描述授权的具体数据。资源是用六段式描述。每款产品的资源定义详情会有所区别。有关如何指定资源的信息，请参阅您编写的资源声明所对应的产品文档。该元素是必填项。
  iii. **生效条件 condition** 描述策略生效的约束条件。条件包括操作符、操作键和操作值组成。条件值可包括时间、IP 地址等信息。有些服务允许您在条件中指定其他值。该元素是非必填项。
  iv. **影响 effect** 描述声明产生的结果是"允许"还是"显式拒绝"。包括 allow (允许)和 deny (显式拒绝)两种情况。该元素是必填项。

CDB 的操作

在 CDB 策略语句中，您可以从支持 CDB 的任何服务中指定任意的 API 操作。对于 CDB，请使用以 cdb: 为前缀的 API 。例如： cdb:CreateDBInstance 或者 cdb:CreateAccounts 。

1. 如果您要在单个语句中指定多个操作的时候，请使用逗号将它们隔开，如下所示:

```
"action":["cdb:action1","cdb:action2"]
```

2. 您也可以使用通配符指定多项操作。例如，您可以指定名字以单词" Describe "开头的所有操作，如下所示：

```
"action":["cdb:Describe*"]
```

3. 如果您要指定 CDB 中所有操作，请使用 * 通配符，如下所示：

```
"action" : ["cdb:*"]
```

CDB 的资源

每个 CAM 策略语句都有适用于自己的资源。
资源的一般形式如下：

```
qcs:project_id:service_type:region:account:resource
```

- **project_id**：描述项目信息，仅为了兼容CAM早期逻辑，无需填写。
- **service_type**：产品简称，如 cdb。
- **region**：地域信息，如 ap-guangzhou。
- **account**：资源拥有者的根帐号信息，如 uin/653339763。
- **resource**：各产品的具体资源详情，如 instanceId/instance_id1 或者 instanceId/*。

例如，

1. 您可以使用特定实例 (cdb-k05xdcta) 在语句中指定它，如下所示：

```
"resource":[ "qcs::cdb:ap-guangzhou:uin/653339763:instanceId/cdb-k05xdcta"]
```

2. 您还可以使用 * 通配符指定属于特定账户的所有实例，如下所示：

```
"resource":[ "qcs::cdb:ap-guangzhou:uin/653339763:instanceId/*"]
```

3. 您要指定所有资源，或者如果特定 API 操作不支持 资源级权限，请在 Resource 元素中使用 * 通配符，如下所示：

```
"resource": ["*"]
```

4. 如果您想要在在一条指令中同时指定多个资源，请使用逗号将它们隔开，如下所示为指定两个资源的例子：

```
"resource":["resource1","resource2"]
```

下表描述了 CDB 能够使用的资源和对应的资源描述方法。
在下表中，$为前缀的单词均为代称。

- 其中，project 指代的是项目ID。
- 其中，region 指代的是地域。

- 其中，account 指代的是账户ID。

资源	授权策略中的资源描述方法
实例	qcs::cdb:$region:$account:instanceId/$instanceId
VPC	qcs::vpc:$region:$account:vpc/$vpcId
安全组	qcs::cvm:$region:$account:sg/$sgId

支持的资源级权限

最近更新时间：2018-03-13 12:05:39

资源级权限指的是能够指定允许用户对哪些资源具有执行操作的能力。 CDB 部分支持资源级权限，这意味着对于某些 CDB 操作，您可以控制何时允许用户执行操作 (基于必须满足的条件)或是允许用户使用的特定资源。下表将向您介绍一下， CDB 可授权的资源类型。

CAM 中可授权的资源类型：

资源类型	授权策略中的资源描述方法
云数据库实例相关	qcs::cdb:$region:$account:instanceId/* qcs::cdb:$region:$account:instanceId/$instanceId

下表将介绍当前支持资源级权限的 CDB （ Cloud Database, 云数据库 ） API 操作，以及每个操作支持的资源和条件密钥。指定资源路径的时候，您可以在路径中使用 * 通配符。

> **注意**：
> 如果某一个 CDB API 操作在下表中没有列出，则它不支持资源级权限。如果 CDB API 操作不支持资源级权限，那么您还是可以向用户授予使用该操作的权限，但是必须为策略语句的资源元素指定 * 。

云数据库实例相关：

API操作	资源路径
AddTimeWindow	qcs::cdb:$region:$account:instanceId/* qcs::cdb:$region:$account:instanceId/$instanceId
AssociateSecurityGroups	qcs::cdb:$region:$account:instanceId/* qcs::cdb:$region:$account:instanceId/$instanceId
CloseWanService	qcs::cdb:$region:$account:instanceId/* qcs::cdb:$region:$account:instanceId/$instanceId
CreateAccounts	qcs::cdb:$region:$account:instanceId/* qcs::cdb:$region:$account:instanceId/$instanceId
CreateBackup	qcs::cdb:$region:$account:instanceId/* qcs::cdb:$region:$account:instanceId/$instanceId

API操作	资源路径
CreateDBImportJob	qcs::cdb:$region:$account:instanceId/* qcs::cdb:$region:$account:instanceId/$instanceId
DeleteAccounts	qcs::cdb:$region:$account:instanceId/* qcs::cdb:$region:$account:instanceId/$instanceId
DeleteBackup	qcs::cdb:$region:$account:instanceId/* qcs::cdb:$region:$account:instanceId/$instanceId
DeleteTimeWindow	qcs::cdb:$region:$account:instanceId/* qcs::cdb:$region:$account:instanceId/$instanceId
DescribeAccountPrivileges	qcs::cdb:$region:$account:instanceId/* qcs::cdb:$region:$account:instanceId/$instanceId
DescribeAccounts	qcs::cdb:$region:$account:instanceId/* qcs::cdb:$region:$account:instanceId/$instanceId
DescribeBackupConfig	qcs::cdb:$region:$account:instanceId/* qcs::cdb:$region:$account:instanceId/$instanceId
DescribeBackupDatabases	qcs::cdb:$region:$account:instanceId/* qcs::cdb:$region:$account:instanceId/$instanceId
DescribeBackupDownloadDbTableCode	qcs::cdb:$region:$account:instanceId/* qcs::cdb:$region:$account:instanceId/$instanceId
DescribeBackups	qcs::cdb:$region:$account:instanceId/* qcs::cdb:$region:$account:instanceId/$instanceId
DescribeBackupTables	qcs::cdb:$region:$account:instanceId/* qcs::cdb:$region:$account:instanceId/$instanceId
DescribeBinlogs	qcs::cdb:$region:$account:instanceId/* qcs::cdb:$region:$account:instanceId/$instanceId
DescribeDatabases	qcs::cdb:$region:$account:instanceId/* qcs::cdb:$region:$account:instanceId/$instanceId
DescribeDBImportRecords	qcs::cdb:$region:$account:instanceId/* qcs::cdb:$region:$account:instanceId/$instanceId
DescribeDBInstanceCharset	qcs::cdb:$region:$account:instanceId/* qcs::cdb:$region:$account:instanceId/$instanceId

API操作	资源路径
DescribeDBInstanceConfig	qcs::cdb:$region:$account:instanceId/* qcs::cdb:$region:$account:instanceId/$instanceId
DescribeDBInstanceGTID	qcs::cdb:$region:$account:instanceId/* qcs::cdb:$region:$account:instanceId/$instanceId
DescribeDBInstanceRebootTime	qcs::cdb:$region:$account:instanceId/* qcs::cdb:$region:$account:instanceId/$instanceId
DescribeDBSwitchRecords	qcs::cdb:$region:$account:instanceId/* qcs::cdb:$region:$account:instanceId/$instanceId
DescribeDBSecurityGroups	qcs::cdb:$region:$account:instanceId/* qcs::cdb:$region:$account:instanceId/$instanceId
DescribeInstanceParamRecords	qcs::cdb:$region:$account:instanceId/* qcs::cdb:$region:$account:instanceId/$instanceId
DescribeInstanceParams	qcs::cdb:$region:$account:instanceId/* qcs::cdb:$region:$account:instanceId/$instanceId
DescribeRoGroups	qcs::cdb:$region:$account:instanceId/* qcs::cdb:$region:$account:instanceId/$instanceId
DescribeRollbackRangeTime	qcs::cdb:$region:$account:instanceId/* qcs::cdb:$region:$account:instanceId/$instanceId
DescribeSlowLogs	qcs::cdb:$region:$account:instanceId/* qcs::cdb:$region:$account:instanceId/$instanceId
DescribeSupportedPrivileges	qcs::cdb:$region:$account:instanceId/* qcs::cdb:$region:$account:instanceId/$instanceId
DescribeTables	qcs::cdb:$region:$account:instanceId/* qcs::cdb:$region:$account:instanceId/$instanceId
DescribeTimeWindow	qcs::cdb:$region:$account:instanceId/* qcs::cdb:$region:$account:instanceId/$instanceId
DescribeDatabasesForInstances	qcs::cdb:$region:$account:instanceId/* qcs::cdb:$region:$account:instanceId/$instanceId
DescribeMonitorData	qcs::cdb:$region:$account:instanceId/* qcs::cdb:$region:$account:instanceId/$instanceId

API操作	资源路径
DescribeTableColumns	qcs::cdb:$region:$account:instanceId/* qcs::cdb:$region:$account:instanceId/$instanceId
DropDatabaseTables	qcs::cdb:$region:$account:instanceId/* qcs::cdb:$region:$account:instanceId/$instanceId
InitDBInstances	qcs::cdb:$region:$account:instanceId/* qcs::cdb:$region:$account:instanceId/$instanceId
IsolateDBInstance	qcs::cdb:$region:$account:instanceId/* qcs::cdb:$region:$account:instanceId/$instanceId
ModifyAccountDescription	qcs::cdb:$region:$account:instanceId/* qcs::cdb:$region:$account:instanceId/$instanceId
ModifyAccountPassword	qcs::cdb:$region:$account:instanceId/* qcs::cdb:$region:$account:instanceId/$instanceId
ModifyAccountPrivileges	qcs::cdb:$region:$account:instanceId/* qcs::cdb:$region:$account:instanceId/$instanceId
ModifyAutoRenewFlag	qcs::cdb:$region:$account:instanceId/* qcs::cdb:$region:$account:instanceId/$instanceId
ModifyBackupConfig	qcs::cdb:$region:$account:instanceId/* qcs::cdb:$region:$account:instanceId/$instanceId
ModifyBackupInfo	qcs::cdb:$region:$account:instanceId/* qcs::cdb:$region:$account:instanceId/$instanceId
ModifyDBInstanceName	qcs::cdb:$region:$account:instanceId/* qcs::cdb:$region:$account:instanceId/$instanceId
ModifyDBInstanceProject	qcs::cdb:$region:$account:instanceId/* qcs::cdb:$region:$account:instanceId/$instanceId
ModifyDBInstanceSecurityGroups	qcs::cdb:$region:$account:instanceId/* qcs::cdb:$region:$account:instanceId/$instanceId
ModifyDBInstanceVipVport	qcs::cdb:$region:$account:instanceId/* qcs::cdb:$region:$account:instanceId/$instanceId
ModifyInstanceParam	qcs::cdb:$region:$account:instanceId/* qcs::cdb:$region:$account:instanceId/$instanceId

API操作	资源路径
ModifyDBInstanceModes	qcs::cdb:$region:$account:instanceId/* qcs::cdb:$region:$account:instanceId/$instanceId
ModifyTimeWindow	qcs::cdb:$region:$account:instanceId/* qcs::cdb:$region:$account:instanceId/$instanceId
ModifyProtectMode	qcs::cdb:$region:$account:instanceId/* qcs::cdb:$region:$account:instanceId/$instanceId
OfflineDBInstances	qcs::cdb:$region:$account:instanceId/* qcs::cdb:$region:$account:instanceId/$instanceId
OpenDBInstanceGTID	qcs::cdb:$region:$account:instanceId/* qcs::cdb:$region:$account:instanceId/$instanceId
OpenWanService	qcs::cdb:$region:$account:instanceId/* qcs::cdb:$region:$account:instanceId/$instanceId
ReleaseIsolatedDBInstances	qcs::cdb:$region:$account:instanceId/* qcs::cdb:$region:$account:instanceId/$instanceId
RestartDBInstances	qcs::cdb:$region:$account:instanceId/* qcs::cdb:$region:$account:instanceId/$instanceId
StartBatchRollback	qcs::cdb:$region:$account:instanceId/* qcs::cdb:$region:$account:instanceId/$instanceId
SubmitBatchOperation	qcs::cdb:$region:$account:instanceId/* qcs::cdb:$region:$account:instanceId/$instanceId
SwitchDrInstanceToMaster	qcs::cdb:$region:$account:instanceId/* qcs::cdb:$region:$account:instanceId/$instanceId
SwitchForUpgrade	qcs::cdb:$region:$account:instanceId/* qcs::cdb:$region:$account:instanceId/$instanceId
DisassociateSecurityGroups	qcs::cdb:$region:$account:instanceId/* qcs::cdb:$region:$account:instanceId/$instanceId
UpgradeDBInstance	qcs::cdb:$region:$account:instanceId/* qcs::cdb:$region:$account:instanceId/$instanceId
UpgradeDBInstanceEngineVersion	qcs::cdb:$region:$account:instanceId/* qcs::cdb:$region:$account:instanceId/$instanceId

控制台示例

最近更新时间：2018-07-27 17:43:12

CDB访问管理策略示例

您可以通过使用 CAM （Cloud Access Management，访问管理）策略让用户拥有在 CDB （Cloud DataBase，云数据库）控制台中查看和使用特定资源的权限。该部分的示例能够使用户使用控制台的特定部分的策略。

CDB 的全读写策略

如果您想让用户拥有创建和管理 CDB 实例的权限，您可以对该用户使用名称为：QcloudCDBFullAccess 的策略。

您可以进入策略管理界面，单击列项【服务类型】在下拉选项中选择【云数据库】，就可以在结果中找到该策略。参考如下：

策略语法如下：

```
{
"version": "2.0",
"statement": [
{
"action": [
"cdb:*"
],
"resource": "*",
"effect": "allow"
},
{
```

```
"action": [
"vpc:*"
],
"resource": "*",
"effect": "allow"
},
{
"action": [
"cvm:*"
],
"resource": "qcs::cvm:::sg/*",
"effect": "allow"
},
{
"action": [
"cos:*"
],
"resource": "*",
"effect": "allow"
},
{
"effect": "allow",
"action": "monitor:*",
"resource": "*"
},
{
"action": [
"kms:CreateKey",
"kms:GenerateDataKey",
"kms:Decrypt",
"kms:ListKey"
],
"resource": "*",
"effect": "allow"
}
]
}
```

以上策略是通过让用户分别对 CDB、VPC（Virtual Private Cloud）、安全组、COS（Cloud Object Storage）、KMS（Key Management Service）和 Monitor 中所有资源进行 CAM 策略授权来达到目的。

CDB 的只读策略

如果您只想让用户拥有查询 CDB 实例的权限，但是不具有创建、删除和修改的权限，您可以对该用户使用名称为：QcloudCDBInnerReadOnlyAccess 的策略。

建议：请配置 CDB 的只读策略。

您可以进入策略管理界面，单击列项【服务类型】在下拉选项中选择【云数据库】，就可以在结果中找到该策略。参考如下：

策略语法如下：

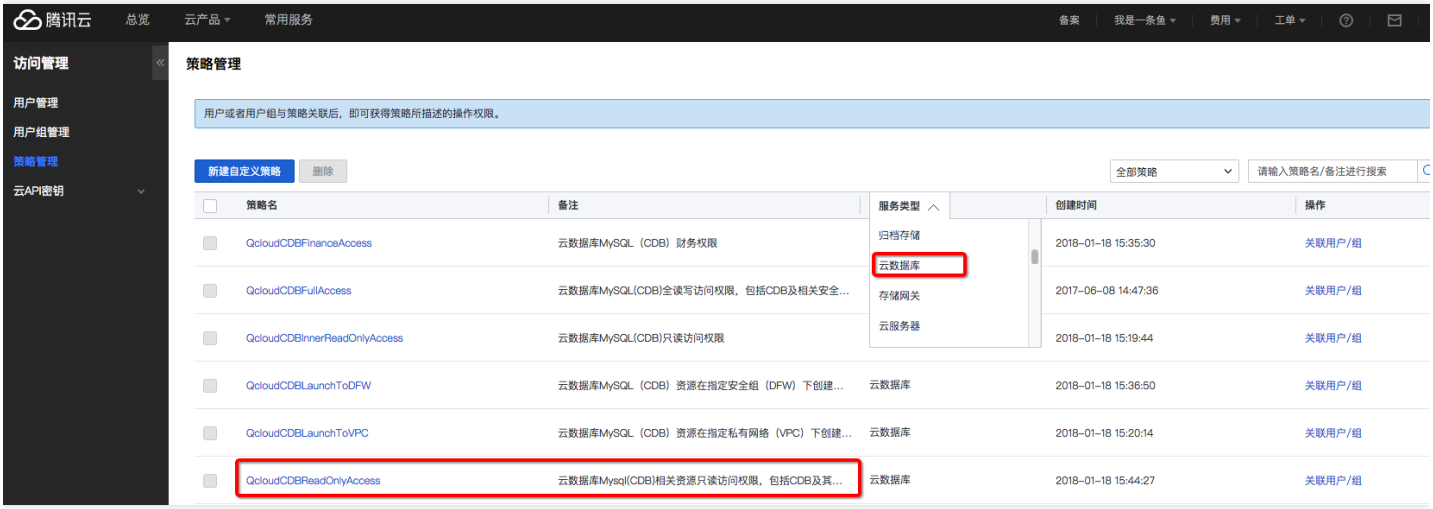
```
{
"version": "2.0",
"statement": [
{
"action": [
"cdb:Describe*"
],
"resource": "*",
"effect": "allow"
}
]
}
```

以上策略是通过让用户分别对如下操作 CDB 中所有以单词" Describe "开头的所有操作进行 CAM 策略授权来达到目的。

CDB 相关资源的只读策略

如果您想要让用户只拥有查询 CDB 实例及相关资源（VPC 、安全组、COS、Monitor）的权限，但不允许该用户拥有创建、删除和修改等操作的权限，您可以对该用户使用名称为：QcloudCDBReadOnlyAccess 的策略。

您可以进入策略管理界面，单击列项【服务类型】在下拉选项中选择【云数据库】，就可以在结果中找到该策略。参考如下：



策略语法如下：

```
{
"version": "2.0",
"statement": [
{
"action": [
"cdb:Describe*"
],
"resource": "*",
"effect": "allow"
},
{
"action": [
"vpc:Describe*",
"vpc:Inquiry*",
"vpc:Get*"
],
"resource": "*",
"effect": "allow"
},
{
"action": [
"cvm:DescribeSecurityGroup*"
],
"resource": "*",
"effect": "allow"
```

```
},
{
"action": [
"cos:List*",
"cos:Get*",
"cos:Head*",
"cos:OptionsObject"
],
"resource": "*",
"effect": "allow"
},
{
"effect": "allow",
"action": "monitor:*",
"resource": "*"
}
]
}
```

以上策略是通过让用户分别对如下操作进行 CAM 策略授权来达到目的：

- CDB 中所有以单词" Describe "开头的所有操作。
- VPC 中所有以单词" Describe "开头的所有操作、所有以单词" Inquiry "开头的所有操作和所有以单词" Get "开头的所有操作。
- 安全组 中所有以单词" DescribeSecurityGroup "开头的所有操作。
- COS 中所有以单词" List "开头的所有操作、所有以单词" Get "开头的所有操作、所有以单词" Head "开头的所有操作和名为" OptionsObject "的操作。
- Monitor 中所有的的操作。

授权用户拥有特定 CDB 的操作权限策略

如果您想要授权用户拥有特定 CDB 操作权限，可将以下策略关联到该用户。以下策略允许用户拥有对 ID 为 cdb-xxx，广州地域的 CDB 实例的操作权限：

```
{
"version": "2.0",
"statement": [
{
"action": "cdb:*",
"resource": "qcs::cdb:ap-guangzhou::instanceId/cdb-xxx",
"effect": "allow"
}
]
}
```

授权用户拥有批量 CDB 的操作权限策略

如果您想要授权用户拥有批量 CDB 操作权限，可将以下策略关联到该用户。以下策略允许用户拥有对 ID 为 cdb-xxx、cdb-yyy，广州地域的 CDB 实例的操作权限和对 ID 为 cdb-zzz，北京地域的 CDB 实例的操作权限。

```
{
"version": "2.0",
"statement": [
{
"action": "cdb:*",
"resource": ["qcs::cdb:ap-guangzhou::instanceId/cdb-xxx", "qcs::cdb:ap-guangzhou::instanceId/cdb-yyy", "qcs::cdb:ap-beijing::instanceId/cdb-zzz"],
"effect": "allow"
}
]
}
```

授权用户拥有特定地域 CDB 的操作权限策略

如果您想要授权用户拥有特定地域的 CDB 的操作权限，可将以下策略关联到该用户。以下策略允许用户拥有对广州地域的 CDB 机器的操作权限。

```
{
"version": "2.0",
"statement": [
{
"action": "cdb:*",
"resource": "qcs::cdb:ap-guangzhou::*",
"effect": "allow"
}
]
}
```

自定义策略

如果您觉得预设策略不能满足您所想要的要求，您也可以创建自定义策略。自定义的策略语法如下：

```
{
"version": "2.0",
"statement": [
{
"action": [
"Action"
],
```

```
"resource": "Resource",
"effect": "Effect"
}
]
}
```

Action中换成您要进行允许或拒绝的操作。

Resource中换成您要授权的具体资源。

Effect中换成允许或者拒绝。

概述

最近更新时间：2018-03-13 12:07:43

如果您在腾讯云中使用到了云数据库（CDB，Cloud Database）、云服务器、私有网络等服务，这些服务由不同的人管理，但都共享您的云账号密钥，将存在以下问题：

- 您的密钥由多人共享，泄密风险高；
- 您无法限制他人的访问权限，易产生误操作造成安全风险。

这个时候，访问管理应运而生。
访问管理（CAM，Cloud Access Management）是腾讯云提供的一套Web服务，它主要用于帮助客户安全管理腾讯云账户下的资源的访问权限。通过CAM，您可以创建、管理和销毁用户(组)，并通过身份管理和策略管理控制哪些人可以使用哪些腾讯云资源。有关CAM的更多相关介绍，请参考CAM概述

接入CAM后，可通过子帐号实现不同的人管理不同的服务，以避免以上的问题。默认情况下，子帐号没有使用CDB实例以及CDB相关资源的的权限。因此，我们就需要创建策略来允许子帐号使用他们所需要的资源或者权限。

策略是定义和描述一条或多条权限的语法规范，策略通过授权一个用户或者一组用户来允许或拒绝使用指定资源。有关CAM策略的更多相关基本信息，请参照策略语法。有关CAM策略的更多相关使用信息，请参照策略。

如果您不需要对子账户进行CDB相关资源的访问管理，您可以跳过此章节。跳过这些部分并不影响您对文档中其余部分的理解和使用。

入门

CAM 策略必须授权使用一个或多个 CDB 操作或者必须拒绝使用一个或多个 CDB 操作。同时还必须指定可以用于操作的资源（可以是全部资源，某些操作也可以是部分资源），策略还可以包含操作资源所设置的条件。

注意事项

- **目前CDB接入CAM权限体系处于灰度阶段，处于灰度地域内的CDB用户可尝鲜CAM。灰度地域有：亚太地区-首尔、北美地区-多伦多、美国西部-硅谷、欧洲地区-法兰克福、东南亚地区-新加坡、西南地区-成都。**
- **强烈建议**用户使用CAM策略来管理CDB资源和授权CDB操作，对于存量分项目权限的用户体验不变，但不建议再继续使用分项目权限来管理资源与授权操作。
- CDB暂时不支持相关生效条件设置

任务	链接
了解策略基本结构	策略语法

任务	链接
在策略中定义操作	CDB的操作
在策略中定义资源	CDB的资源路径
CDB支持的资源级权限	CDB支持的资源级权限
控制台示例	控制台示例

安全组操作指南

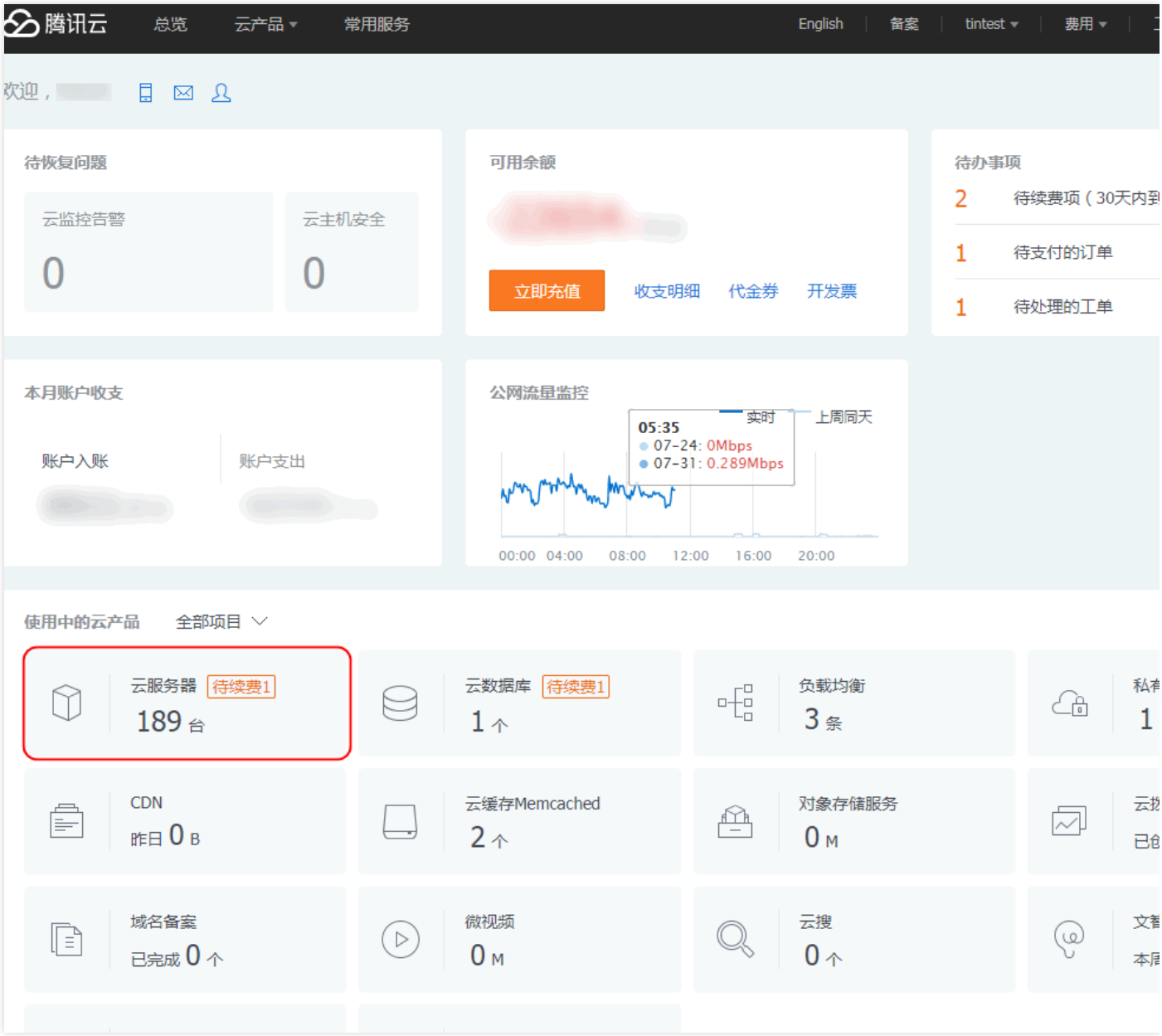
最近更新时间：2018-07-27 17:02:37

本文是对创建安全组、为云数据库配置安全组、删除安全组、克隆安全组、向安全组中添加规则、导入导出安全组规则的介绍。

> **注意：**
> 云数据库安全组目前仅支持私有网络 VPC 内网访问和外网访问的网络控制，暂不支持对基础网络的网络控制。目前云数据库仅 CDB for MySQL 支持安全组。

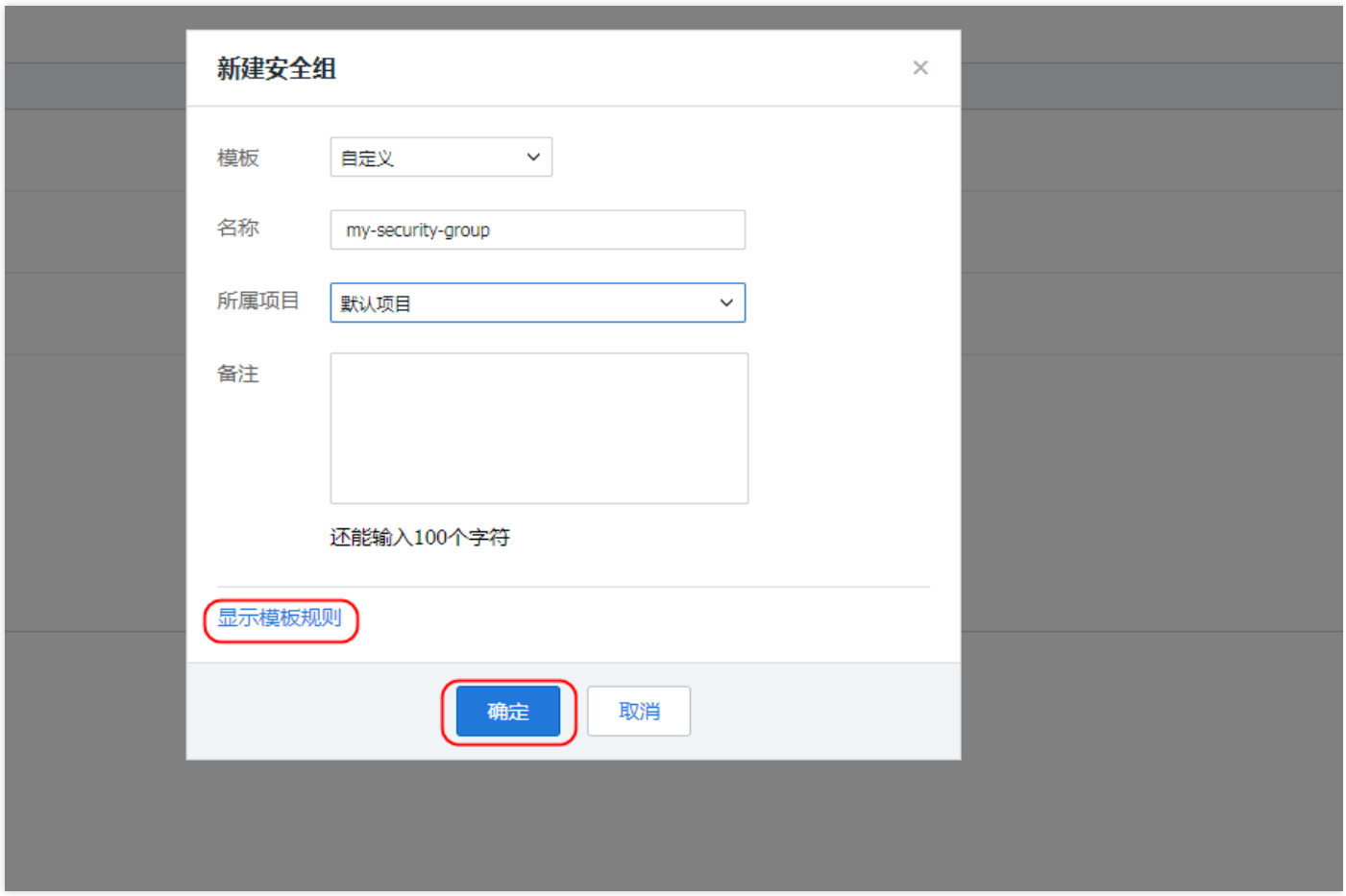
创建安全组

1. 登录 腾讯云控制台，在 **使用中的云产品** 栏目单击【云服务器】，进入云服务器管理页面。在左侧导航栏中，单击【安全组】，进入安全组管理页面。


腾讯云
总览
云产品
常用服务
English
备案
tintest
费用
欢迎，
待恢复问题
云监控告警
0
云主机安全
0
可用余额
立即充值
收支明细
代金券
开发票
待办事项
2
待续费项（30天内到
1
待支付的订单
1
待处理的工单
本月账户收支
账户入账
账户支出
公网流量监控
实时
上周同天
05:35
07-24: 0Mbps
07-31: 0.289Mbps
00:00
04:00
08:00
12:00
16:00
20:00
使用中的云产品
全部项目
云服务器
待续费1
189 台
云数据库
待续费1
1 个
负载均衡
3 条
私有
1
CDN
昨日 0 B
云缓存Memcached
2 个
对象存储服务
0 M
云拨
已创
域名备案
已完成 0 个
微视频
0 M
云搜
0 个
文智
本月

2. 单击【新建】按钮，选择【模板】创建或【自定义】创建，输入安全组的 **名称**（例如 my-security-group），选择 **所属项目**，选填 **备注**，确认后单击【确定】。


云服务器
安全组
全部项目
广州
上海
北京
香港
新加坡
多伦多
硅谷
法兰克福
在这里用户可以设定安全组策略，对绑定的云主机进行内、外网访问权限控制，提高公有云的安全性
+新建
概览
云主机
专用宿主机
镜像
云硬盘
快照
SSH密钥
安全组
弹性公网IP
回收站
ID/名称
关联实例数
备注
sg-949rl6nb
Linux 放通22端口-2017062719303827
3
仅暴露 SSH
sg-g1r91cld
放通全部端口-2017062719303266
1
sg-hvfl9mwx
放通全部端口-20170608155648709
1


新建安全组
模板
自定义
名称
my-security-group
所属项目
默认项目
备注
还能输入100个字符
显示模板规则
确定
取消

为云数据库配置安全组

安全组 是腾讯云提供的实例级别防火墙，可以对云数据库进行入/出流量控制。您可以在购买实例时绑定安全组，也可以购买实例后在控制台绑定安全组。

> **注意：**
> 目前安全组仅支持**私有网络云数据库**配置。

进入 云数据库控制台，在实例列表选中需要配置安全组的实例，单击【管理】，选择【安全组】标签页 > 单击【配置安全组】，选择需要绑定的安全组，即可完成安全组绑定云数据库的操作。

删除安全组

1. 打开云服务器 CVM 控制台 安全组页面，单击列表中安全组项后面的【删除】按钮。

2. 在删除安全组对话框中，单击【确定】。若当前安全组有关联的 CVM 则需要先解除安全组才能进行删除。

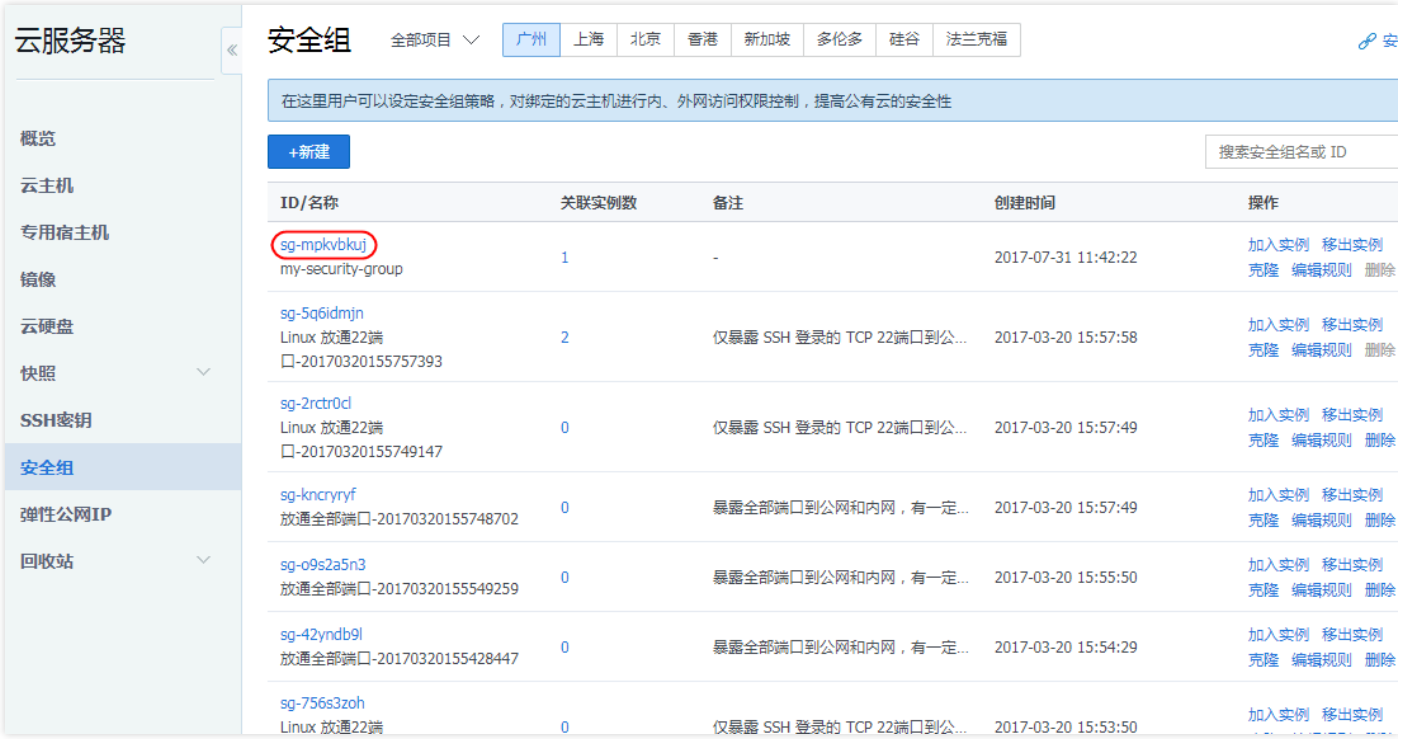
克隆安全组

1. 打开云服务器 CVM 控制台 安全组页面，单击列表中安全组项后面的【克隆】按钮。

2. 在克隆安全组对话框中，选定目标地域、目标项目后，单击【确定】。若新安全组需关联 CVM，请重新进行管理安全组内云服务器。

向安全组中添加规则

1. 打开云服务器 CVM 控制台 安全组页面，选择需要更新的安全组，单击安全组 ID。详细信息窗格内会显示此安全组的详细信息，以及可供您使用入站规则和出站规则的选项卡。

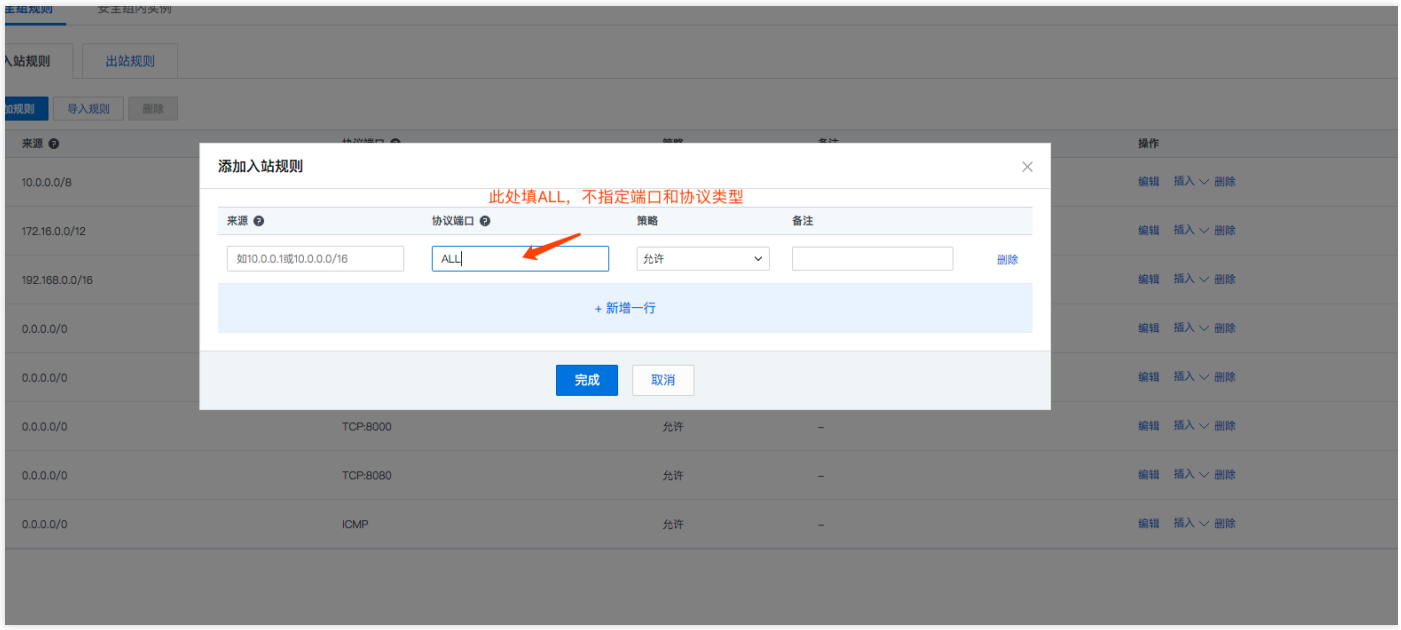


2. 在入/出站规则选项卡上，单击【添加规则】。从选项卡中选择用于入/出站规则的选项，然后填写所需信息。例如，将来源/目标指定为 0.0.0.0/0，协议端口指定为 ALL，设置策略为 允许，单击【完成】。单击【新增一行】可以同时配置多个规则。

注意：

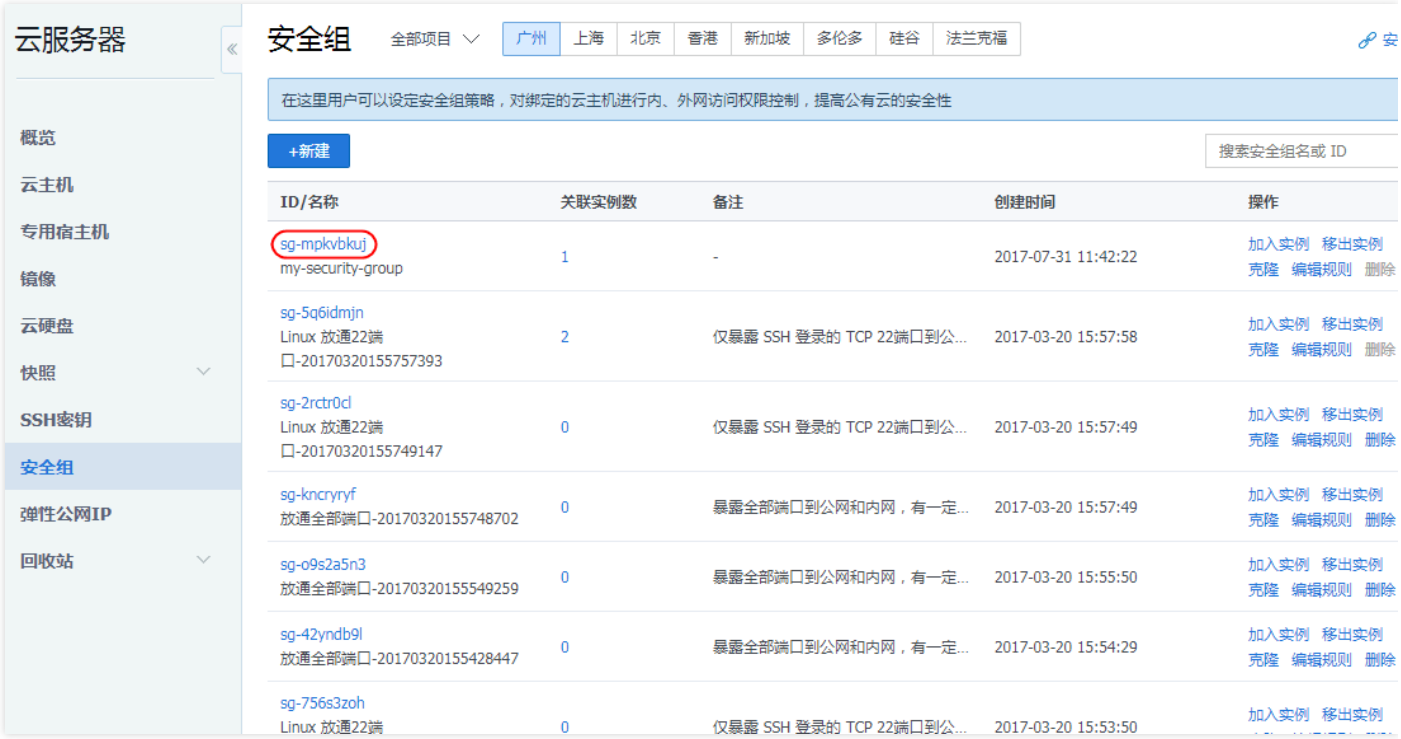
对于安全组的每条规则，有以下几项注意事项：

- 协议端口：云数据库协议端口仅支持 **ALL**，若指定端口则该条规则对云数据库不生效。
- 授权类型：地址段（CIDR/IP）访问；
- 来源（入站规则）或目标（出站规则），请指定以下选项之一：
  - 用 CIDR 表示法，指定的单个 IP 地址。
  - 用 CIDR 表示法，指定的 IP 地址范围（例如，203.0.113.0/24）。
- 策略：允许或拒绝。

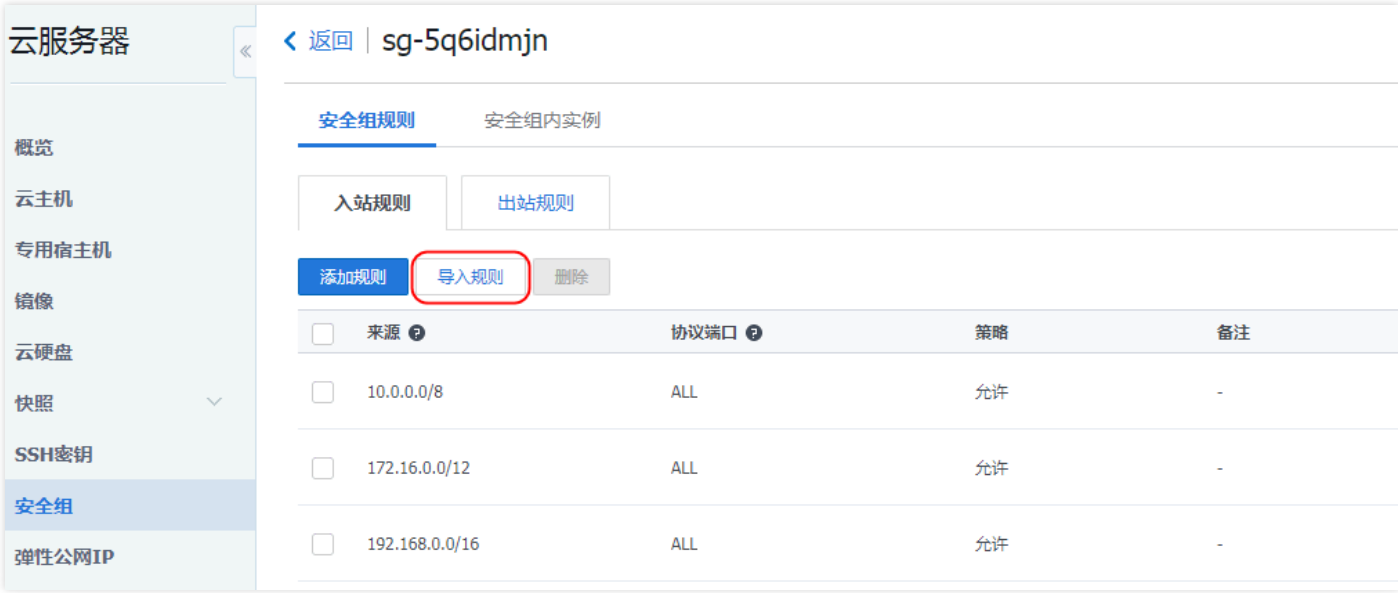


导入导出安全组规则

1. 打开云服务器 CVM 控制台 安全组页面，选择需要更新的安全组，单击安全组 ID。详细信息窗格内会显示此安全组的详细信息，以及可供您使用入站规则和出站规则的选项卡。



2. 从选项卡中选择用于入/出站规则的选项，然后单击【导入规则】按钮。如原来您已有规则，则推荐您先导出现有规则，因为规则导入将覆盖原有规则，如原来为空规则，则可先导出模板，编辑好模板文件后，再将文件导入。


云服务器
返回
sg-5q6idmjn
概览
云主机
专用宿主机
镜像
云硬盘
快照
SSH密钥
安全组
弹性公网IP
安全组规则
安全组内实例
入站规则
出站规则
添加规则
导入规则
删除
来源
协议端口
策略
备注
10.0.0.0/8
ALL
允许
-
172.16.0.0/12
ALL
允许
-
192.168.0.0/16
ALL
允许
-