分布式数据库 TDSQL

安全管理

产品文档

腾讯云

文档目录

安全管理
访问管理
概述

最近更新时间：2019-02-19 15:36:45

概述

如果您在腾讯云中使用到了云数据库、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。
有关腾讯云访问管理 CAM 的更多相关介绍，请参考 CAM 概述。

接入CAM 后，可通过子账号实现不同的人管理不同的服务，以避免出现以上的问题。默认情况下，子账号没有使用云数据库实例以及云数据库相关资源的的权限。因此，我们就需要创建策略来允许子账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，请参考 策略语法 文档。有关 CAM 策略的更多相关使用信息，请参考 策略 文档。

如果您不需要对子账户进行云数据库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云数据库操作或者必须拒绝使用一个或多个云数据库操作。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：**
>
> - **强烈建议**用户使用 CAM 策略来管理云数据库资源和授权云数据库操作，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。
> - 云数据库暂时不支持相关生效条件设置。

了解更多

了解更多访问管理 CAM，请参考 访问管理 文档库。

策略结构

最近更新时间：2019-06-10 17:36:03

策略语法

CAM 策略配置示例：

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

- **版本 version**：必填项，目前允许值为"2.0"（该值实际代表 CAM 接受的云 API 版本）。
- **语句 statement**：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。
  - **操作 action**：用来描述允许或拒绝的操作。操作 action 实际填入的是以 "dcdb:" 前缀描述，分布式数据库 TDSQL API 为后缀的一串字符串 。该元素是必填项。
  - **资源 resource**：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。
  - **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。
  - **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。

⚠ 注意：

由于历史原因，分布式数据库 TDSQL（曾用名 DCDB）在访问管理的接口关键词为 dcdb，详情请参考 产品更名详情。

云数据库的操作

在云数据库策略语句中，您可以从支持云数据库的任何服务中指定任意的 API 操作。对于云数据库，请使用以 dcdb: 为前缀的 API。例如：dcdb:CreateDBInstance （创建实例-包年包月）或者 dcdb:CloseDBExtranetAccess（关闭外网访问）。

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

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

- 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":["dcdb:Describe*"]
```

- 如果您要指定云数据库中所有操作，请使用 * 通配符，如下所示：

```
"action" : ["dcdb:*"]
```

云数据库的资源

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 dcdb。
- **region**：地域信息，如 ap-guangzhou。详情请参考 地域相关信息。
- **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 instance/instance_id1 或者 instance/*。

例如，

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

```
"resource":[ "qcs::dcdb:ap-guangzhou:uin/653339763:instance/dcdb-k05xdcta"]
```

- 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::dcdb:ap-guangzhou:uin/653339763:instance/*"]
```

- 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": ["*"]
```

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

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

下表描述了云数据库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::dcdb:$region:$account:instance/$instanceId

支持的资源级权限

最近更新时间：2019-06-10 17:36:26

> ⚠ **注意：**
>
> 由于历史原因，分布式数据库 TDSQL（曾用名 DCDB）在访问管理的接口关键词为 dcdb，详情请参考 产品更名详情。

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。云数据库部分支持资源级权限，这意味着对于某些云数据库操作，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。下表将向您介绍云数据库可授权的资源类型。

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::dcdb:$region:$account:instance/* qcs::dcdb:$region:$account:instance/$instanceId

下表将介绍当前支持资源级权限的云数据库 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：**
>
> 如果某一个云数据库 API 操作在下表中没有列出，则它不支持资源级权限。如果云数据库 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 * 。

下列操作可支持资源级权限

操作名	API 名	配置后控制台是否生效
查询实例升级价格	DescribeDCDBUpgradePrice	NO
续费实例	RenewDCDBInstance	NO
查询实例续费价格	DescribeDCDBRenewalPrice	NO
实例扩容	UpgradeDCDBInstance	NO
查看实例列表	DescribeDCDBInstances	YES
获取日志列表	DescribeDBLogFiles	YES

操作名	API 名	配置后控制台是否生效
初始化实例	InitDCDBInstances	NO
创建帐号	CreateAccount	YES
查询帐号列表	DescribeAccounts	YES
删除帐号	DeleteAccount	YES
设置帐号权限	GrantAccountPrivileges	YES
查询帐号权限	DescribeAccountPrivileges	YES
复制帐号权限	CopyAccountPrivileges	NO
修改数据库帐号备注	ModifyAccountDescription	NO
重置帐号密码	ResetAccountPassword	YES
查看数据库参数	DescribeDBParameters	NO
修改数据库参数	ModifyDBParameters	NO
克隆帐号	CloneAccount	YES
获取 SQL 日志	DescribeSqlLogs	NO

控制台示例

最近更新时间：2019-06-10 17:36:34

说明：

分布式数据库支持访问管理 CAM（Cloud Access Management）功能，自2018年12月6日起进行公测。您可以通过策略语法进行配置。

云数据库访问管理策略示例

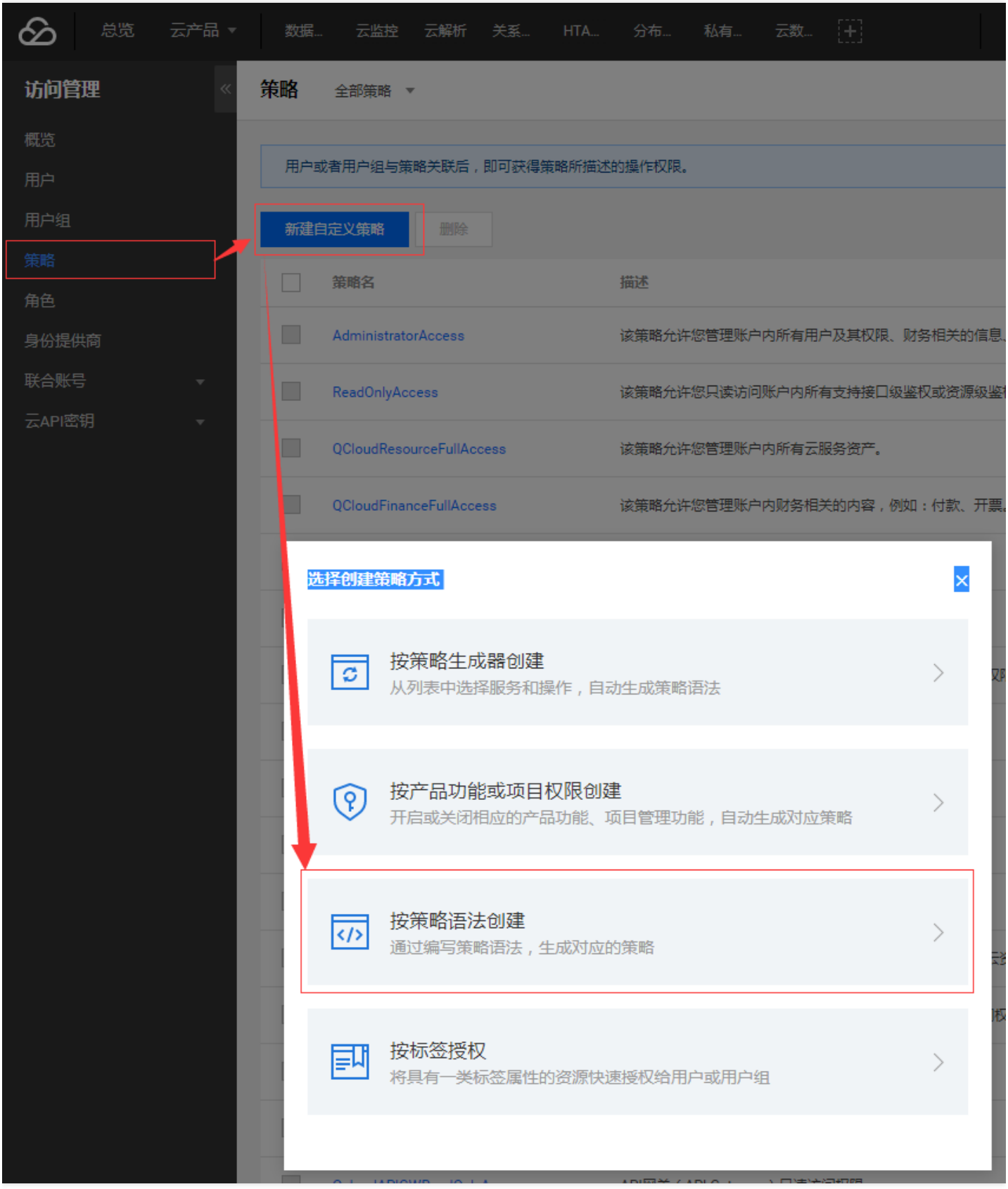
您可以通过使用 CAM 策略让用户拥有在云数据库控制台中查看和使用特定资源的权限。该部分的示例能够使用户使用控制台的特定部分的策略。

说明：

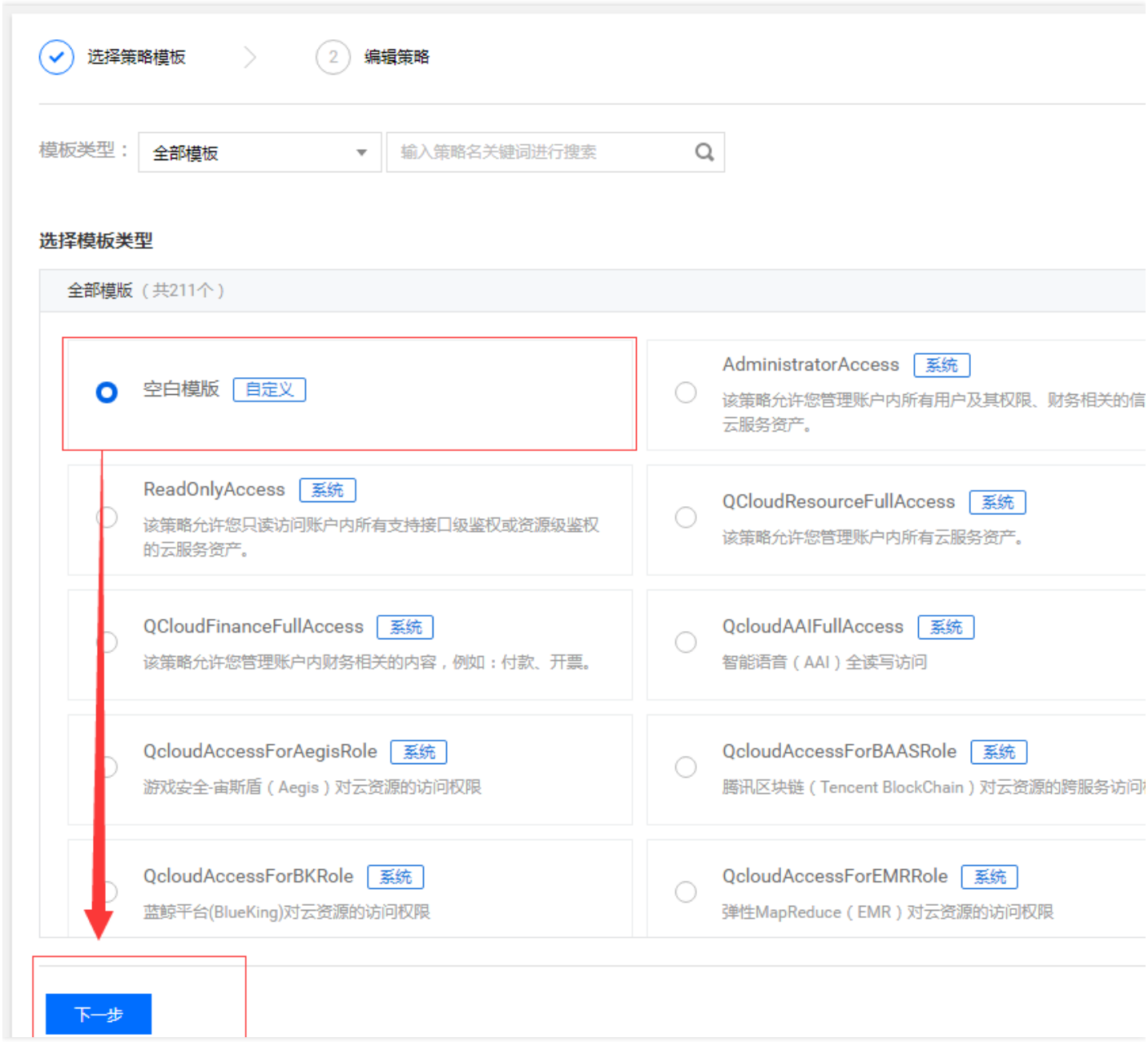
由于历史原因，分布式数据库 TDSQL（曾用名 DCDB）在访问管理的接口关键词为 dcdb，详情请参考 产品更名详情。

创建自定义策略语法

1.进入策略语法配置页面。



2.选择空白模板并单击【下一步】。


选择策略模板
2
编辑策略
模板类型：
全部模板
输入策略名关键词进行搜索
选择模板类型
全部模版（共211个）
空白模版
自定义
AdministratorAccess
系统
该策略允许您管理账户内所有用户及其权限、财务相关的信
云服务资产。
ReadOnlyAccess
系统
该策略允许您只读访问账户内所有支持接口级鉴权或资源级鉴权
的云服务资产。
QCloudResourceFullAccess
系统
该策略允许您管理账户内所有云服务资产。
QCloudFinanceFullAccess
系统
该策略允许您管理账户内财务相关的内容，例如：付款、开票。
QcloudAAIFullAccess
系统
智能语音（AAI）全读写访问
QcloudAccessForAegisRole
系统
游戏安全-宙斯盾（Aegis）对云资源的访问权限
QcloudAccessForBAASRole
系统
腾讯区块链（Tencent BlockChain）对云资源的跨服务访问
QcloudAccessForBKRole
系统
蓝鲸平台(BlueKing)对云资源的访问权限
QcloudAccessForEMRRole
系统
弹性MapReduce（EMR）对云资源的访问权限
下一步

3.填入对应的策略语法。

关联子账号/协作者并验证

创建策略完成后，选择关联用户/组。关联完成后，更换浏览器（或主机），通过使用子账号/协作者验证验证是否正常。如果策略语法写作无误，您可以观察到：

- 您能正常访问预期目标产品和资源，并拥有预期的全部功能。
- 访问其他未授权产品或资源时提示“您没有权限执行此操作”。

为避免多个策略语法影响，建议一次只让子账号关联一个策略。
修改某账号访问控制权限后，预估会有1分钟以内的延迟。

附录：常用的策略语法

放通云数据库的全部实例全部功能策略

如果您想让用户拥有创建和管理云数据库实例的权限，您可以对该用户使用名称为 QcloudDCDBFullAccess 的策略。

策略语法如下：

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

云数据库全部实例仅查询功能策略

如果您只想让用户拥有查询云数据库实例的权限，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QcloudDCDBInnerReadOnlyAccess 的策略。

策略语法如下：

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

以上策略是通过让用户分别对云数据库中所有以单词" Describe "开头的所有操作进行 CAM 策略授权来达到目的。

授权用户拥有若干特定地域云数据库的操作权限策略

如果您想要授权用户拥有特定地域的云数据库的操作权限，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云数据库机器的操作权限。

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

授权用户拥有特定云数据库的操作权限策略

如果您想要授权用户拥有特定云数据库操作权限，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 dcdb-xxx，广州地域的云数据库实例的操作权限：

```
{
"version": "2.0",
"statement": [
{
"action": [
"dcdb:*"
],
"resource": "qcs::dcdb:ap-chengdu::instance/dcdb-fwr62n3i",
"effect": "allow"
}
]
}
```

授权用户拥有若干云数据库的操作权限策略

如果您想要授权用户拥有批量云数据库操作权限，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 dcdb-xxx、dcdb-yyy，广州地域的云数据库实例的操作权限和对 id 为 dcdb-zzz，北京地域的云数据库实例的操作权限。

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

授权用户拥有若干云数据库的若干操作权限策略

如果您想要授权用户拥有批量云数据库操作权限，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 dcdb-xxx、dcdb-yyy，广州地域的云数据库实例的操作权限和对 id 为 dcdb-zzz，北京地域的云数据库实例的操作权限。

```
{
"version": "2.0",
"statement": [
{
"action": "dcdb:Describe*","dcdb:Create*",
"resource": ["qcs::dcdb:ap-guangzhou::instance/dcdb-xxx", "qcs::dcdb:ap-guangzhou::instance/dcdb-
```

```
yyy", "qcs::dcdb:ap-beijing::instance/dcdb-zzz"],
"effect": "allow"
}
]
}
```

说明：

当前全部支持 API 接口详见文档最后。

拒绝用户拥有云数据库的创建账号权限

如果您想要拒绝某用户拥有批量云数据库升级操作权限，即配置 `"effect": "deny"` 。

```
{
"version": "2.0",
"statement": [
{
"action": "dcdb:CreateAccount",
"resource": "*",
"effect": "deny"
}
]
}
```

其他自定义策略

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。

公测期间已支持权限

操作名	API 名	配置后控制台是否生效
查询实例升级价格	DescribeDCDBUpgradePrice	NO
续费实例	RenewDCDBInstance	NO
查询实例续费价格	DescribeDCDBRenewalPrice	NO
实例扩容	UpgradeDCDBInstance	NO
查看实例列表	DescribeDCDBInstances	YES
获取日志列表	DescribeDBLogFiles	YES
初始化实例	InitDCDBInstances	NO
创建帐号	CreateAccount	YES
查询帐号列表	DescribeAccounts	YES
删除帐号	DeleteAccount	YES
设置帐号权限	GrantAccountPrivileges	YES
查询帐号权限	DescribeAccountPrivileges	YES
复制帐号权限	CopyAccountPrivileges	NO
修改数据库帐号备注	ModifyAccountDescription	NO
重置帐号密码	ResetAccountPassword	YES
查看数据库参数	DescribeDBParameters	NO
修改数据库参数	ModifyDBParameters	NO
克隆帐号	CloneAccount	YES
获取SQL日志	DescribeSqlLogs	NO

当前控制台功能已接入CAM操作说明

最近更新时间：2019-01-03 14:46:52

下列操作可支持资源级权限

操作名	API名	配置后控制台是否生效
查询实例升级价格	DescribeDCDBUpgradePrice	NO
续费实例	RenewDCDBInstance	NO
查询实例续费价格	DescribeDCDBRenewalPrice	NO
实例扩容	UpgradeDCDBInstance	NO
查看实例列表	DescribeDCDBInstances	YES
获取日志列表	DescribeDBLogFiles	YES
初始化实例	InitDCDBInstances	NO
创建帐号	CreateAccount	YES
查询帐号列表	DescribeAccounts	YES
删除帐号	DeleteAccount	YES
设置帐号权限	GrantAccountPrivileges	YES
查询帐号权限	DescribeAccountPrivileges	YES
复制帐号权限	CopyAccountPrivileges	NO
修改数据库帐号备注	ModifyAccountDescription	NO
重置帐号密码	ResetAccountPassword	YES
查看数据库参数	DescribeDBParameters	NO
修改数据库参数	ModifyDBParameters	NO
克隆帐号	CloneAccount	YES
获取SQL日志	DescribeSqlLogs	NO

配置云数据库安全组

最近更新时间：2019-04-17 12:45:23

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。云数据库与云服务器等共享安全组列表，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。
> 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。

管理云数据库安全组

您可以在腾讯云分布式数据库控制台 页面的【实例列表】>【数据安全性】>【安全组】中管理云数据库。

> ⚠ **注意：**
>
> 1. 云数据库共享云服务器的安全组规则，您可以根据实际情况在云数据库安全组管理页面匹配或调整优先级。
> 2. 云数据库安全组管理页面不支持创建、删除安全组规则本身；有创建、删除、调整安全组规则，请参考私有网络 管理安全组 文档。

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 。

云数据库安全组默认策略

当前购买云数据库且为 VPC 网络时，可以无需关联任何安全组；此时默认策略为“放通全部 IP 和端口”。

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服务器的数据包进行控制。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，新规则保存后立即生效。
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 TencentDB 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。
- 每个用户在同个地域的同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

创建、管理和删除安全组规则

云数据库共享云服务器的安全组规则，您可以根据实际情况在云数据库安全组管理页面匹配或调整优先级。创建、管理和删除安全组规则在 安全组管理页面 进行，并参考文档 管理安全组 操作文档。