

负载均衡

访问管理

产品文档



腾讯云

【版权声明】

©2013-2020 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】

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。

文档目录

访问管理

概述

授权定义

策略示例

访问管理

概述

最近更新时间：2020-10-30 17:18:47

如果您使用到了负载均衡 CLB、云服务器、数据库等服务，这些服务由不同的人管理，但都共享您的云账号密钥，将存在如下问题：

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

访问管理（CAM）用于管理腾讯云账户下资源访问权限，通过 CAM，您可以通过身份管理和策略管理控制哪些子账号有哪些资源的操作权限。

例如，您的账户下有多个负载均衡实例部署在不同项目中，为了加强权限控制，对资源进行授权，您可以给项目 A 的管理员绑定一个授权策略，该策略规定：只有该管理员可操作项目 A 下的负载均衡资源。

如果您不需要对子账户进行 CLB 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。

CAM 基本概念

根账户通过给予子账户绑定策略实现授权，策略设置可精确到 **[API，资源，用户/用户组，允许/拒绝，条件]** 维度。

1. 账户

◦ 根账号

腾讯云资源归属、资源使用计量计费的基本主体，可登录腾讯云服务。

◦ 子账号

由根账号创建账号，有确定的身份ID和身份凭证，且能登录到腾讯云控制台。根账号可以创建多个子账号(用户)。**子账号默认不拥有资源，必须由所属根账号进行授权。**

◦ 身份凭证

包括登录凭证和访问证书两种，**登录凭证**是指用户登录名和密码，**访问证书**是指云 API 密钥（SecretId 和 SecretKey）。

2. 资源与权限

◦ 资源

资源是云服务中被操作的对象，如一个云服务器实例，VPC 实例等。

◦ 权限

权限是指允许或拒绝某些用户执行某些操作。默认情况下，**根账号拥有其名下所有资源的访问权限，而子账号没有根账号下任何资源的访问权限。**

◦ 策略

策略是定义和描述一条或多条权限的语法规则。**根账号通过将策略关联到用户/用户组完成授权。**

更多相关信息，请参见 [CAM 概述](#)。

相关文档

目标	链接
了解策略和用户之间关系	策略管理
了解策略的基本结构	策略语法
了解还有哪些产品支持 CAM	支持 CAM 的云服务列表

授权定义

最近更新时间：2020-08-04 19:59:51

CAM 中可授权的负载均衡资源类型

资源类型	授权策略中的资源描述方法
负载均衡实例	<code>qcs::clb:\$region::clb/\$loadbalancerid</code>
负载均衡后端服务器	<code>qcs::cvm:\$region:\$account:instance/\$cvminstanceid</code>

其中：

- 所有 `$region` 应为某个 region 的 ID，可以为空。
- 所有 `$account` 应为资源拥有者的 AccountId，或者“*”。
- 所有 `$loadbalancerid` 应为某个 loadbalancer 的 ID，或者“*”。

以此类推。

CAM 中可对负载均衡进行授权的接口

在 CAM 中，可以对一个负载均衡资源进行以下 Action 的授权。

实例相关

API 操作	资源描述	接口说明
DescribeLoadBalancers	查询负载均衡实例列表	* 只对接口进行鉴权
CreateLoadBalancer	购买负载均衡	<code>qcs::\$projectid:clb:\$region:\$account:clb/*</code>
DeleteLoadBalancers	删除负载均衡	<code>qcs::clb:\$region:\$account:clb/\$loadbalancerid</code>
ModifyLoadBalancerAttributes	修改负载均衡属性信息	<code>qcs::clb:\$region:\$account:clb/\$loadbalancerid</code>
ModifyForwardLBName	修改负载均衡的名字	<code>qcs::clb:\$region:\$account:clb/\$loadbalancerid</code>

监听器相关

API 操作	资源描述	接口说明
DeleteLoadBalancerListeners	删除负载均衡监听器	<code>qcs::clb:\$region:\$account:clb/\$loadbalancerid</code>
DescribeLoadBalancerListeners	获取负载均衡监听器列表	<code>qcs::clb:\$region:\$account:clb/\$loadbalancerid</code>
ModifyLoadBalancerListener	修改负载均衡监听器属性	<code>qcs::clb:\$region:\$account:clb/\$loadbalancerid</code>

API 操作	资源描述	接口说明
CreateLoadBalancerListeners	创建负载均衡监听器	qcs::clb:\$region:\$account:clb/\$loadbalancerid
DeleteForwardLBListener	删除负载均衡监听器（四层和七层）	qcs::clb:\$region:\$account:clb/\$loadbalancerid
ModifyForwardLBSeventhListener	修改负载均衡七层监听的属性	qcs::clb:\$region:\$account:clb/\$loadbalancerid
ModifyForwardLBFourthListener	修改负载均衡四层监听器属性	qcs::clb:\$region:\$account:clb/\$loadbalancerid
DescribeForwardLBListeners	查询负载均衡监听器列表	qcs::clb:\$region:\$account:clb/\$loadbalancerid
CreateForwardLBSeventhLayerListeners	创建七层负载均衡监听器	qcs::clb:\$region:\$account:clb/\$loadbalancerid
CreateForwardLBFourthLayerListeners	创建四层负载均衡监听器	qcs::clb:\$region:\$account:clb/\$loadbalancerid

负载均衡域名 + URL 相关

API 操作	资源描述	接口说明
ModifyForwardLBRulesDomain	修改负载均衡监听器转发规则的域名	qcs::clb:\$region:\$account:clb/\$loadbalancerid
CreateForwardLBListenerRules	创建负载均衡监听器转发规则	qcs::clb:\$region:\$account:clb/\$loadbalancerid
DeleteForwardLBListenerRules	删除七层负载均衡监听器规则	qcs::clb:\$region:\$account:clb/\$loadbalancerid
DeleteRewrite	删除负载均衡转发规则之间的重定向关系	qcs::clb:\$region:\$account:clb/\$loadbalancerid
ManualRewrite	手动添加负载均衡转发规则的重定向关系	qcs::clb:\$region:\$account:clb/\$loadbalancerid
AutoRewrite	自动生成负载均衡转发规则的重定向关系	qcs::clb:\$region:\$account:clb/\$loadbalancerid

后端服务器相关

API 操作	资源描述	接口说明
ModifyLoadBalancerBackends	修改负载均衡器后端服务器权重	qcs::clb:\$region:\$account:clb/\$loadbalancerid
DescribeLoadBalancerBackends	获取负载均衡绑定的后端服务器列表	qcs::clb:\$region:\$account:clb/\$loadbalancerid

API 操作	资源描述	接口说明
DeregisterInstancesFromLoadBalancer	解绑后端服务器	qcs::clb:\$region:\$account:clb/\$loadbalancerid qcs::cvm:\$region:\$account:instance/\$cvminstanceid
RegisterInstancesWithLoadBalancer	绑定后端服务器到负载均衡	qcs::clb:\$region:\$account:clb/\$loadbalancerid qcs::cvm:\$region:\$account:instance/\$cvminstanceid
DescribeLBHealthStatus	查询负载均衡健康状态	qcs::clb:\$region:\$account:clb/\$loadbalancerid
ModifyForwardFourthBackendsPort	修改四层监听器转发规则上云服务器的端口	qcs::clb:\$region:\$account:clb/\$loadbalancerid qcs::cvm:\$region:\$account:instance/\$cvminstanceid
ModifyForwardFourthBackendsWeight	修改四层监听器转发规则上云服务器的权重	qcs::clb:\$region:\$account:clb/\$loadbalancerid qcs::cvm:\$region:\$account:instance/\$cvminstanceid
RegisterInstancesWithForwardLBSeventhListener	绑定云服务器到负载均衡七层监听器的转发规则上	qcs::clb:\$region:\$account:clb/\$loadbalancerid qcs::cvm:\$region:\$account:instance/\$cvminstanceid
RegisterInstancesWithForwardLBFourthListener	绑定云服务器到负载均衡四层监听器的转发规则上	qcs::clb:\$region:\$account:clb/\$loadbalancerid qcs::cvm:\$region:\$account:instance/\$cvminstanceid
DeregisterInstancesFromForwardLBFourthListener	解绑负载均衡四层监听器转发规则上的云服务器	qcs::clb:\$region:\$account:clb/\$loadbalancerid qcs::cvm:\$region:\$account:instance/\$cvminstanceid
DeregisterInstancesFromForwardLB	解绑负载均衡七层监听器转发规则上的云服务器	qcs::clb:\$region:\$account:clb/\$loadbalancerid qcs::cvm:\$region:\$account:instance/\$cvminstanceid

API 操作	资源描述	接口说明
ModifyForwardSeventhBackends	修改七层监听器转发规则上云服务器的权重	qcs::clb:\$region:\$account:clb/\$loadbalancerid qcs::cvm:\$region:\$account:instance/\$cvminstanceid
ModifyForwardSeventhBackendsPort	修改七层监听器转发规则上云服务器的端口	qcs::clb:\$region:\$account:clb/\$loadbalancerid qcs::cvm:\$region:\$account:instance/\$cvminstanceid
DescribeForwardLBBackends	查询负载均衡云服务器列表	qcs::clb:\$region:\$account:clb/\$loadbalancerid qcs::cvm:\$region:\$account:instance/*
DescribeForwardLBHealthStatus	查询负载均衡健康检查状态	qcs::clb:\$region:\$account:clb/*
ModifyLoadBalancerRulesProbe	修改负载均衡监听器转发规则的健康检查及转发路径	qcs::clb:\$region:\$account:clb/\$loadbalancerid

策略示例

最近更新时间：2020-08-04 19:59:27

所有 CLB 的全读写策略

- 授权一个子账户以 CLB 服务的完全管理权限（创建、管理等全部操作）。
- 策略名称：CLBResourceFullAccess

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

所有 CLB 的只读策略

- 授权一个子账户只读访问 CLB 的权限（即可以查看所有 CLB 下面所有资源的权限），但子账户无法创建、更新或删除它们。在控制台，操作一个资源的前提是可以查看该资源，所以建议您为子账户开通 CLB 全读权限。
- 策略名称：CLBResourceReadOnlyAccess

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

某个标签下 CLB 的全读写策略

- 授权一个子账户对某个标签（标签键为 tagkey，标签值为 tagvalue）下的 CLB 的完全管理权限（管理实例、管理监听器等全部操作），关于标签请参见[基于标签管理项目资源](#)。
- CLB 实例支持配置标签和使用标签鉴权。

```
{
  "version": "2.0",
```

```
"statement":[
{
"effect":"allow",
"action":"*",
"resource":"*",
"condition":{"
"for_any_value:string_equal":{"
"qcs:tag":[
"tagkey&tagvalue"
]
}
}
}
]
}
```