

负载均衡 访问控制 产品文档



腾讯云

【版权声明】

©2013-2018 腾讯云版权所有

本文档著作权归腾讯云单独所有，未经腾讯云事先书面许可，任何主体不得以任何形式复制、修改、抄袭、传播全部或部分本文档内容。

【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。

【服务声明】

本文档意在向客户介绍腾讯云全部或部分产品、服务的当时的整体概况，部分产品、服务的内容可能有所调整。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模式的承诺或保证。

文档目录

访问控制

- 访问控制概述

- 访问控制策略示例

- 访问控制授权定义

访问控制

访问控制概述

最近更新时间：2018-06-13 10:40:47

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，将存在以下问题：

- 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。

访问控制（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相关资源的访问控制，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。

该功能目前处于灰度中，可提[工单申请](#)

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，COS存储桶，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。**

[单击查看更多CAM介绍](#)

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

访问控制策略示例

最近更新时间：2018-06-01 17:22:24

CLB的全读写策略

授权一个子用户以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"
    }
  ]
}
```

CLB的只读策略

授权一个子用户只读访问CLB的权限（即可以查看所有LB下面所有资源的权限），但用户无法创建、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"
    }
  ]
}
```

访问控制授权定义

最近更新时间：2018-06-01 17:20:41

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	qcs::clb:\$region::clb/\$loadbalancerid
负载均衡监听器	qcs::clb:\$region::listener/\$loadbalancerlistenerid
负载均衡后端服务器	qcs::cvm:\$region:\$account:instance/\$cvminstanceid

其中所有 \$regionid 应为某个region的id，或者“*”；

所有 \$accountid 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。

负载均衡实例相关：

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	qcs::\$projectid:clb:\$region:\$account:clb/*
DeleteLoadBalancers	删除负载均衡	qcs::clb:\$region:\$account:clb/\$loadbalancerid
ModifyLoadBalancerAttributes	修改负载均衡属性信息	qcs::clb:\$region:\$account:clb/\$loadbalancerid
ModifyForwardLBName	修改转发型负载均衡的名字	qcs::clb:\$region:\$account:clb/\$loadbalancerid
ModifyLBWeight	修改负载均衡权重	qcs::clb:\$region:\$account:clb/\$loadbalancerid
DeleteLBService	负载均衡解绑设备	qcs::clb:\$region:\$account:clb/\$loadbalancerid
ModifyLBHealth	修改负载均衡健康检查阈值	qcs::clb:\$region:\$account:clb/\$loadbalancerid
DescribeLBHealth	查询LB健康检查阈值	qcs::clb:\$region:\$account:clb/*

负载均衡监听器相关：

API操作	资源描述	接口说明
DeleteLoadBalancerListeners	删除负载均衡监听器	qcs::clb:\$region:\$account:clb/\$loadbalancerid qcs::clb:\$region:\$account:listener/\$loadbalancerlistenerid
DescribeLoadBalancerListeners	获取负载均衡监听器列表	qcs::clb:\$region:\$account:clb/\$loadbalancerid qcs::clb:\$region:\$account:listener/*

API操作	资源描述	接口说明
ModifyLoadBalancerListener	修改负载均衡监听器	qcs::clb:\$region:\$account:clb/\$loadbalancerid qcs::clb:\$region:\$account:listener/\$loadbalancerlistenerid
CreateLoadBalancerListeners	创建负载均衡监听器	qcs::clb:\$region:\$account:clb/\$loadbalancerid
DeleteForwardLBListener	删除转发型监听器（四层和七层）	qcs::clb:\$region:\$account:clb/\$loadbalancerid qcs::clb:\$region:\$account:listener/\$loadbalancerlistenerid
ModifyForwardLBSeventhListener	修改7层监听的属性	qcs::clb:\$region:\$account:clb/\$loadbalancerid qcs::clb:\$region:\$account:listener/\$loadbalancerlistenerid
ModifyForwardLBFourthListener	修改转发型4层监听器属性	qcs::clb:\$region:\$account:clb/\$loadbalancerid qcs::clb:\$region:\$account:listener/\$loadbalancerlistenerid
DescribeForwardLBListeners	查询转发型LB的监听器	qcs::clb:\$region:\$account:clb/\$loadbalancerid qcs::clb:\$region:\$account:listener/*
CreateForwardLBSeventhLayerListeners	创建转发型LB的7层监听器	qcs::clb:\$region:\$account:clb/\$loadbalancerid
DeleteForwardLBSeventhListeners	删除7层监听器	qcs::clb:\$region:\$account:clb/\$loadbalancerid qcs::clb:\$region:\$account:listener/\$loadbalancerlistenerid
CreateForwardLBFourthLayerListeners	创建转发型四层监听器	qcs::clb:\$region:\$account:clb/\$loadbalancerid

应用型负载均衡域名+URL相关：

API操作	资源描述	接口说明
ModifyForwardLBRulesDomain	修改监听器的域名	qcs::clb:\$region:\$account:clb/\$loadbalancerid qcs::clb:\$region:\$account:listener/\$loadbalancerlistenerid
CreateForwardLBListenerRules	创建七层监听器的转发的规则	qcs::clb:\$region:\$account:clb/\$loadbalancerid qcs::clb:\$region:\$account:listener/\$loadbalancerlistenerid
DeleteForwardLBListenerRules	删除负载均衡实例的七层监听器的规则	qcs::clb:\$region:\$account:clb/\$loadbalancerid qcs::clb:\$region:\$account:listener/\$loadbalancerlistenerid
DeleteRewrite	删除重定向关系	qcs::clb:\$region:\$account:clb/\$loadbalancerid qcs::clb:\$region:\$account:listener/\$sourceloadbalancerlistenerid qcs::clb:\$region:\$account:listener/\$targetloadbalancerlistenerid
ManualRewrite	用户自定义重定向	qcs::clb:\$region:\$account:clb/\$loadbalancerid qcs::clb:\$region:\$account:listener/\$sourceloadbalancerlistenerid qcs::clb:\$region:\$account:listener/\$targetloadbalancerlistenerid
AutoRewrite	自动rewrite接口	qcs::clb:\$region:\$account:clb/\$loadbalancerid qcs::clb:\$region:\$account:listener/\$loadbalancerlistenerid

负载均衡后端服务器相关：

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 qcs::cvm:\$region:\$account:instance/\$loadbalancerlistenerid
DescribeLoadBalancerBackends	获取负载均衡器后端服务器列表	qcs::clb:\$region:\$account:clb/\$loadbalancerid qcs::clb:\$region:\$account:listener/*
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
DescribeLBHealthStatusMc	查询负载均衡健康状态 (MC)	qcs::clb:\$region:\$account:clb/\$loadbalancerid qcs::clb:\$region:\$account:listener/*
DescribeLBHealthStatus	查询负载均衡健康状态	qcs::clb:\$region:\$account:clb/\$loadbalancerid qcs::clb:\$region:\$account:listener/*
ModifyForwardFourthBackendsPort	修改转发型4层监听器后端端口	qcs::clb:\$region:\$account:clb/\$loadbalancerid qcs::clb:\$region:\$account:listener/\$loadbalancerlistenerid qcs::cvm:\$region:\$account:instance/\$cvminstanceid
ModifyForwardFourthBackendsWeight	修改转发型4层监听器后端权重	qcs::clb:\$region:\$account:clb/\$loadbalancerid qcs::clb:\$region:\$account:listener/\$loadbalancerlistenerid qcs::cvm:\$region:\$account:instance/\$cvminstanceid
RegisterInstancesWithForwardLBSeventhListener	绑定机器到7层监听器上	qcs::clb:\$region:\$account:clb/\$loadbalancerid qcs::clb:\$region:\$account:listener/\$loadbalancerlistenerid qcs::cvm:\$region:\$account:instance/\$cvminstanceid
RegisterInstancesWithForwardLBFourthListener	绑定机器到转发型4层监听器上	qcs::clb:\$region:\$account:clb/\$loadbalancerid qcs::clb:\$region:\$account:listener/\$loadbalancerlistenerid qcs::cvm:\$region:\$account:instance/\$cvminstanceid
DeregisterInstancesFromForwardLBFourthListener	将机器从转发型四层监听器上解绑	qcs::clb:\$region:\$account:clb/\$loadbalancerid qcs::clb:\$region:\$account:listener/\$loadbalancerlistenerid qcs::cvm:\$region:\$account:instance/\$cvminstanceid
DeregisterInstancesFromForwardLB	从七层监听器上解绑云服务器	qcs::clb:\$region:\$account:clb/\$loadbalancerid qcs::clb:\$region:\$account:listener/\$loadbalancerlistenerid qcs::cvm:\$region:\$account:instance/\$cvminstanceid

API操作	资源描述	接口说明
ModifyForwardSeventhBackends	修改后端rs的权重	qcs::clb:\$region:\$account:clb/\$loadbalancerid qcs::cvm:\$region:\$account:instance/\$cvminstanceid
ModifyForwardSeventhBackendsPort	更改后端机器的端口	qcs::clb:\$region:\$account:clb/\$loadbalancerid qcs::clb:\$region:\$account:listener/\$loadbalancerlistenerid qcs::cvm:\$region:\$account:instance/\$cvminstanceid
DescribeForwardLBBackends	查询关联的机器	qcs::clb:\$region:\$account:clb/\$loadbalancerid qcs::cvm:\$region:\$account:instance/*
DescribeForwardLBHealthStatus	查询转发型LB的健康检查结果	qcs::clb:\$region:\$account:clb/*
ModifyLoadBalancerRulesProbe	修改转发规则的健康检查	qcs::clb:\$region:\$account:clb/\$loadbalancerid qcs::clb:\$region:\$account:listener/\$loadbalancerlistenerid
DescribeAllLBBackends	查询负载均衡后端rs信息	qcs::clb:\$region:\$account:clb/\$loadbalancerid qcs::cvm:\$region:\$account:instance/*