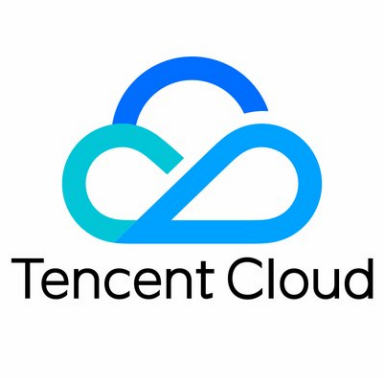
Cloud Load Balancer

Cloud Access Management

Product Documentation



Contents

Cloud Access Management Overview

Last updated : 2019-12-10 15:31:30

If you use multiple Tencent Cloud services such as CLB, CVM, and TencentDB that are managed by different users sharing your Tencent Cloud account key, you may face the following problems:

- Your key is shared by multiple users, leading to high risk of compromise.
- You cannot limit the access permissions of other users, which poses a security risk due to potential faulty operations.

Cloud Access Management (CAM) is used to manage the access permissions to your Tencent Cloud resources. With CAM, you can use the identity management and policy management features to control which Tencent Cloud resources can be accessed by which sub-accounts.

For example, if you have multiple CLB instances under your account that are deployed in different projects, to manage access permissions and authorize resources, you can bind the admin of project A with an authorization policy, which states that only this admin can use the CLB resources under project A.

If you do not need to manage the access permission to CLB resources for sub-accounts, you can skip this chapter. This will not affect your understanding and usage of other parts in the documentation.

Basic Concepts in CAM

The root account authorizes sub-accounts by binding policies. The policy setting can be specific to the level of **API, Resource, User/User Group, Allow/Deny, and Condition**.

1. Account
   - **Root account**
     As the fundamental owner of Tencent Cloud resources, a root account acts as the basis for resource usage fee calculation and billing, and can be used to log in to Tencent Cloud services.
   - **Sub-account**
     A sub-account is created by the root account, and it has a specific ID and identity credential that can be used to log in to the Tencent Cloud Console. A root account can create multiple sub-accounts (users). **A sub-account does not own any resources by default; instead, such resources should be authorized by its root account.**
   - **Identity credential**
     This includes login credentials and access certificates. **Login credential** refers to the username and password. **Access certificate** refers to the TencentCloud API keys (SecretId and SecretKey).

2. Resources and permissions
   - **Resource**
     A resource is an object that is managed in Tencent Cloud services, such as a CVM instance, a bucket in COS, or a VPC instance.
   - **Permission**
     Permission is an authorization to allow or forbid certain users to perform certain operations. By default, **a root account has full access to all the resources under it**, while **a sub-account does not have access to any resources under its root account**.
   - **Policy**
     Policy is the syntax rule used to define and describe one or multiple permissions. **A root account** performs authorization by **associating policies** with users/user groups.

For more information, please see CAM Overview.

Related Documents

Document Description	Link
Relationship between policy and user	Policy
Basic policy structure	Element Reference
More products that support CAM	CAM-enabled Cloud Services

Policy Examples

Last updated : 2020-08-10 15:37:51

Full Access Policy for All CLB Instances

- Grant a sub-account full access to the CLB service (creating, managing, etc.).
- Policy name: CLBResourceFullAccess

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

Read-Only Policy for All CLB Instances

- Grant a sub-account read-only access to CLB (i.e., the permission to view but not to create, update, or delete all CLB resources). In the console, the prerequisite to manipulate a resource is the ability to view the resource; therefore, you are recommended to grant the sub-account full read access to CLB.
- Policy name: CLBResourceReadOnlyAccess

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

Full Access Policy for CLB Service Under a Specified Tag

- Grant a sub-account full access to the CLB service (creating instances, managing listeners, etc.) under a specified tag (tag key: tagkey; tag value: tagvalue).
- CLB instances supports configuring tags and using tags for authentication.

```
{
"version":"2.0",
"statement":[
{
"effect":"allow",
"action":"*",
"resource":"*",
"condition":{
```

```
"for_any_value:string_equal":{
"qcs:tag":[
"tagkey&tagvalue"
]
}
}
}
]
}
```

Authorization Definition

Last updated：2019-12-10 15:32:22

Types of CLB resources that can be authorized in CAM

Resource Type	Resource Description Method in Authorization Policy
CLB instance	`qcs::clb:$region::clb/$loadbalancerid`
CLB listener	`qcs::clb:$region::listener/$loadbalancerlistenerid`
CLB real server	`qcs::cvm:$region:$account:instance/$cvminstanceid`

Notes:

- `$region` should always be the ID of a region, and can be empty.
- `$account` should always be the AccountId of a resource owner or "*".
- `$loadbalancerid` should always be the ID of a load balancer or "*".

And so on...

APIs for CLB Authorization in CAM

You can authorize the following actions for a CLB resource in CAM.

Instance

API Operation	Resource Description	API Description
DescribeLoadBalancers	Queries the CLB instance list	`*` indicates that it only authenticates the API
CreateLoadBalancer	Purchases a CLB instance	`qcs:$projectid:clb:$region:$account:clb/*`
DeleteLoadBalancers	Deletes CLB instances	`qcs::clb:$region:$account:clb/$loadbalancerid`
ModifyLoadBalancerAttributes	Modifies the attributes of a CLB instance	`qcs::clb:$region:$account:clb/$loadbalancerid`
ModifyForwardLBName	Renames a CLB instance	`qcs::clb:$region:$account:clb/$loadbalancerid`

Listener

API Operation	Resource Description	API Description
DeleteLoadBalancerListeners	Deletes CLB listeners	`qcs::clb:$region:$account:clb/$loadbalancerid` `qcs::clb:$region:$account:listener/$loadbalancerlistenerid`
DescribeLoadBalancerListeners	Gets the CLB listener list	`qcs::clb:$region:$account:clb/$loadbalancerid` `qcs::clb:$region:$account:listener/*`
ModifyLoadBalancerListener	Modifies the attributes of a CLB listener	`qcs::clb:$region:$account:clb/$loadbalancerid` `qcs::clb:$region:$account:listener/$loadbalancerlistenerid`
CreateLoadBalancerListeners	Creates CLB listeners	`qcs::clb:$region:$account:clb/$loadbalancerid`

API Operation	Resource Description	API Description
DeleteForwardLBListener	Deletes a CLB listener (layer-4 and layer-7)	`qcs::clb:$region:$account:clb/$loadbalancerid` `qcs::clb:$region:$account:listener/$loadbalancerlistenerid`
ModifyForwardLBSeventhListener	Modifies the attributes of a layer-7 CLB listener	`qcs::clb:$region:$account:clb/$loadbalancerid` `qcs::clb:$region:$account:listener/$loadbalancerlistenerid`
ModifyForwardLBFourthListener	Modifies the attributes of a layer-4 CLB listener	`qcs::clb:$region:$account:clb/$loadbalancerid` `qcs::clb:$region:$account:listener/$loadbalancerlistenerid`
DescribeForwardLBListeners	Queries the CLB listener list	`qcs::clb:$region:$account:clb/$loadbalancerid` `qcs::clb:$region:$account:listener/*`
CreateForwardLBSeventhLayerListeners	Creates layer-7 CLB listeners	`qcs::clb:$region:$account:clb/$loadbalancerid`
CreateForwardLBFourthLayerListeners	Creates layer-4 CLB listeners	`qcs::clb:$region:$account:clb/$loadbalancerid`

CLB domain name and URL

API Operation	Resource Description	API Description
ModifyForwardLBRulesDomain	Modifies the domain name of a CLB listener's forwarding rule	`qcs::clb:$region:$account:clb/$loadbalancerid` `qcs::clb:$region:$account:listener/$loadbalancerlistenerid`
CreateForwardLBListenerRules	Creates forwarding rules for a CLB listener	`qcs::clb:$region:$account:clb/$loadbalancerid` `qcs::clb:$region:$account:listener/$loadbalancerlistenerid`
DeleteForwardLBListenerRules	Deletes the forwarding rules of a layer-7 CLB listener	`qcs::clb:$region:$account:clb/$loadbalancerid` `qcs::clb:$region:$account:listener/$loadbalancerlistenerid`

DeleteRewrite	Deletes the redirection between forwarding rules of CLB instances	`qcs::clb:$region:$account:clb/$loadbalancerid`
		`qcs::clb:$region:$account:listener/$sourceloadbalancerlistenerid`
		`qcs::clb:$region:$account:listener/$targetloadbalancerlistenerid`

ManualRewrite	Manually adds the redirection between forwarding rules of CLB instances	`qcs::clb:$region:$account:clb/$loadbalancerid`
		`qcs::clb:$region:$account:listener/$sourceloadbalancerlistenerid`
		`qcs::clb:$region:$account:listener/$targetloadbalancerlistenerid`

AutoRewrite	Auto-generates the redirection between forwarding rules of CLB instances	`qcs::clb:$region:$account:clb/$loadbalancerid` `qcs::clb:$region:$account:listener/$loadbalancerlistenerid`

Real server

API Operation	Resource Description	API Description

API Operation	Resource Description	API Description
ModifyLoadBalancerBackends	Modifies the real server weight of a CLB instance	`qcs::clb:$region:$account:clb/$loadbalancerid` `qcs::cvm:$region:$account:instance/$loadbalancerlistenerid`
DescribeLoadBalancerBackends	Gets the list of real servers bound to a CLB instance	`qcs::clb:$region:$account:clb/$loadbalancerid` `qcs::clb:$region:$account:listener/*`
DeregisterInstancesFromLoadBalancer	Unbinds a real server	`qcs::clb:$region:$account:clb/$loadbalancerid` `qcs::cvm:$region:$account:instance/$cvminstanceid`
RegisterInstancesWithLoadBalancer	Binds a real server to a CLB instance	`qcs::clb:$region:$account:clb/$loadbalancerid` `qcs::cvm:$region:$account:instance/$cvminstanceid`
DescribeLBHealthStatus	Queries the health status of a CLB instance	`qcs::clb:$region:$account:clb/$loadbalancerid` `qcs::clb:$region:$account:listener/*`

ModifyForwardFourthBackendsPort	Modifies the CVM port of a layer-4 listener's forwarding rule	`qcs::clb:$region:$account:clb/$loadbalancerid`
		`qcs::clb:$region:$account:listener/$loadbalancerlistenerid`
		`qcs::cvm:$region:$account:instance/$cvminstanceid`

ModifyForwardFourthBackendsWeight	Modifies the CVM weight of a layer-4 listener's forwarding rule	`qcs::clb:$region:$account:clb/$loadbalancerid`
		`qcs::clb:$region:$account:listener/$loadbalancerlistenerid`
		`qcs::cvm:$region:$account:instance/$cvminstanceid`

RegisterInstancesWithForwardLBSeventhListener	Binds a CVM to the forwarding rule of a layer-7 CLB listener	`qcs::clb:$region:$account:clb/$loadbalancerid`
		`qcs::clb:$region:$account:listener/$loadbalancerlistenerid`
		`qcs::cvm:$region:$account:instance/$cvminstanceid`

RegisterInstancesWithForwardLBFourthListener	Binds a CVM to the forwarding rule of a layer-4 CLB listener	`qcs::clb:$region:$account:clb/$loadbalancerid`
		`qcs::clb:$region:$account:listener/$loadbalancerlistenerid`
		`qcs::cvm:$region:$account:instance/$cvminstanceid`

API Operation	Resource Description	API Description

DeregisterInstancesFromForwardLBFourthListener	Unbinds the CVM from the forwarding rule of a layer-4 CLB listener	`qcs::clb:$region:$account:clb/$loadbalancerid`
		`qcs::clb:$region:$account:listener/$loadbalancerlistenerid`
		`qcs::cvm:$region:$account:instance/$cvminstanceid`

DeregisterInstancesFromForwardLB	Unbinds the CVM from the forwarding rule of a layer-7 CLB listener	`qcs::clb:$region:$account:clb/$loadbalancerid`
		`qcs::clb:$region:$account:listener/$loadbalancerlistenerid`
		`qcs::cvm:$region:$account:instance/$cvminstanceid`

ModifyForwardSeventhBackends	Modifies the CVM weight of a layer-7 CLB listener's forwarding rule	`qcs::clb:$region:$account:clb/$loadbalancerid` `qcs::cvm:$region:$account:instance/$cvminstanceid`

ModifyForwardSeventhBackendsPort	Modifies the CVM port of a layer-7 listener's forwarding rule	`qcs::clb:$region:$account:clb/$loadbalancerid`
		`qcs::clb:$region:$account:listener/$loadbalancerlistenerid`
		`qcs::cvm:$region:$account:instance/$cvminstanceid`

DescribeForwardLBBackends	Queries the CVM list of a CLB instance	`qcs::clb:$region:$account:clb/$loadbalancerid` `qcs::cvm:$region:$account:instance/*`
DescribeForwardLBHealthStatus	Queries the health check status of a CLB instance	`qcs::clb:$region:$account:clb/*`
ModifyLoadBalancerRulesProbe	Modifies the health check and forwarding path of a CLB listener's forwarding rule	`qcs::clb:$region:$account:clb/$loadbalancerid` `qcs::clb:$region:$account:listener/$loadbalancerlistenerid`