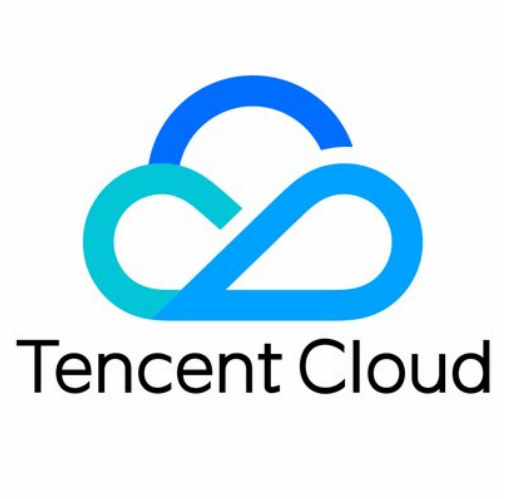
Cloud Access Management

CAM-Enabled Role

Product Documentation



Contents

- Tencent Cloud Firewall
- Tencent Cloud EdgeOne

Application Security

- Web Application Firewall

Domains & Websites

- SSL Certificate Service
- Private DNS
- HTTPDNS

Big Data

- Elastic MapReduce
- Elasticsearch Service
- Cloud Data Warehouse
- Cloud Data Warehouse for PostgreSQL
- Data Lake Compute

Middleware

- Message Queue CKafka
- TDMQ for RocketMQ

Interactive Video Services

- Tencent Real-Time Communication
- Low-code Interactive Classroom

Media On-Demand

- Video on Demand

Cloud Real-time Rendering

- Cloud Application Rendering

Game Services

- Game Multimedia Engine

Cloud Resource Management

- Tencent Cloud Infrastructure as Code
- Tencent Smart Advisor
- Tencent Cloud Mini Program Platform

Management and Audit Tools

- Cloud Access Management
- Tencent Cloud Organization

CAM-Enabled Role Overview

Last updated：2024-05-20 09:12:59

Introduction

Service roles and service-linked roles are unique type of service roles directly associated with Tencent Cloud services. They are predefined by the service and possess all the permissions required for the service to represent you in calling other Tencent Cloud services. This document provides information about products and services that support service roles and service-linked roles, including the role name, role entity, and role description.

- **Product:** he name of the cloud service that supports service roles and service-linked roles.
- **Role Name:** The name of service roles and service-linked roles used by Tencent Cloud services.
- **Role Entity:** The role entity of service roles and service-linked roles is the Tencent Cloud service that is permitted to carry the role's permissions. You can edit, creat or delete the role entity of the service roles and service-linked roles to allow or deny them to play the service roles or service-linked roles to access your Tencent Cloud resources.

Compute

Product	Role Name	Role Types	Role Entity
BatchCompute	BATCH_QCSLinkedRoleInAcrossService	Service-Related Roles	acrossservice.batch
Cloud Virtual Machine	CVM_QCSLinkedRoleInCbsInit	Service-Related Roles	cbsinit.cvm.cloud.ter
Cloud Virtual Machine	CVM_QCSLinkedRoleInCVMSmartDiagnostic	Service-Related Roles	cvmsmartdiagnostic
Lighthouse	Lighthouse_QCSLinkedRoleInBasic	Service-Related Roles	basic.lighthouse.clou
Lighthouse	Lighthouse_QCSLinkedRoleInCOSAndCI	Service-	cosandci.lighthouse.

		Related Roles	
Lighthouse	Lighthouse_QCSLinkedRoleInDnsAndSsl	Service-Related Roles	dnsandssl.lighthouse
Lighthouse	Lighthouse_QCSLinkedRoleInLighthouseSmartDiagnostic	Service-Related Roles	lighthousesmartdiag
TencentCloud Automation Tools	TAT_QCSLinkedRoleInCommand	Service-Related Roles	command.tat.cloud.t
TencentCloud Automation Tools	TAT_QCSLinkedRoleInUploadInvocation	Service-Related Roles	uploadinvocation.tat

Container

Product	Role Name	Role Types	Role Entity
Tencent Kubernetes Engine	TKE_QCSLinkedRoleInTDCC	Service-Related Roles	cvm.qcloud.com tdcc.tke.cloud.tencent.com
Tencent Kubernetes Engine	TKE_QCSLinkedRoleInEKSLog	Service-Related Roles	cvm.qcloud.com ekslog.tke.cloud.tencent.com
Tencent Kubernetes Engine	TKE_QCSLinkedRoleInEtcdService	Service-Related Roles	cvm.qcloud.com etcdservice.tke.cloud.tencent.com
Tencent Kubernetes Engine	TKE_QCSLinkedRoleInEKSCostMaster	Service-Related Roles	cvm.qcloud.com ekscostmaster.tke.cloud.tencent.com
Tencent Kubernetes Engine	TKE_QCSLinkedRoleInPrometheusService	Service-Related Roles	cvm.qcloud.com prometheusservice.tke.cloud.tencent.c

Microservice

Product	Role Name	Role Types	Role Entity
Tencent Cloud Elastic Microservice	TEM_QCSLinkedRoleInTEMAPI	Service-Related Roles	temapi.tem.cloud.tencent.com
Tencent Cloud Elastic Microservice	TEM_QCSLinkedRoleInTEMLog	Service-Related Roles	cvm.qcloud.com temlog.tem.cloud.tencent.com
Tencent Cloud Elastic Microservice	TEM_QCSLinkedRoleInAccessCluster	Service-Related Roles	accesscluster.tem.cloud.tencen
Tencent Cloud Elastic Microservice	TEM_QCSLinkedRoleInAccessResourceService	Service-Related Roles	accessresourceservice.tem.clou

Essential Storage Service

Product	Role Name	Role Types	Role Entity	R D
Cloud HDFS	CHDFS_QCSLinkedRoleInMetaMgmt	Service-Related Roles	metamgmt.chdfs.cloud.tencent.com	[L
COS	COS_QCSLinkedRoleInCOSAcc	Service-Related Roles	COSAcc.COS.cloud.tencent.com	[L
COS	COS_QCSLinkedRoleInCLSAccess	Service-Related Roles	cosoclsr.cos.cloud.tencent.com	[L
COS	COS_QCSLinkedRoleInLighthouseMounting	Service-	lhmounting.cos.cloud.tencent.com	[

		Related Roles		

Data Process and Analysis

Product	Role Name	Role Types	Role Entity	Reference Document
Cloud Log Service	CLS_QCSRoleInAnonymousSharing	Service-Related Roles	console-sharing.cls.cloud.tencent.com	Detailed List

Data Migration

Product	Role Name	Role Types	Role Entity	Reference Document
Migration Service Platform	MSP_QCSLinkedRoleInMIGtocos	Service-Related Roles	migtocos.msp.cloud.tencent.com	Detailed List

Relational Database

Product	Role Name	Role Types	Role Entity
Cloud Database	CDB_QCSLinkedRoleInDBLog	Service-Related Roles	DBLog.cdb.cloud.tencent.com
Cloud Database	CDB_QCSLinkedRoleInCdbwan	Service-Related Roles	cdbwan.cdb.cloud.tencent.com
Cloud Native Database TDSQL-C	CynosDBMysql_QCSLinkedRoleInKms	Service-Related Roles	kms.cynosdb.cloud.tencent.com

Cloud Native Database TDSQL-C	CynosDBMysql_QCSLinkedRoleInClslog	Service-Related Roles	clslog.cynosdb.cloud.tencent.com
TencentDB For PostgreSQL	Postgres_QCSLinkedRoleInPostgresKms	Service-Related Roles	postgreskms.postgres.cloud.tencent.co

Enterprise Distributed DBMS

Product	Role Name	Role Types	Role Entity	Reference Document
TDSQL for MySQL	DCDB_QCSLinkedRoleInKMS	Service-Related Roles	kms.dcdb.cloud.tencent.com	Detailed List
TDSQL for MySQL	DCDB_QCSLinkedRoleInTSE	Service-Related Roles	tse.dcdb.cloud.tencent.com	Detailed List

NoSQL Database

Product	Role Name	Role Types	Role Entity	Reference Document
Cloud MongoDB	MongoDB_QCSLinkedRoleInKMS	Service-Related Roles	kms.mongodb.cloud.tencent.com	Detailed List

Database SaaS Tool

Product	Role Name	Role Types	Role Entity	Referenc Documen
Database Management Console	DMC_QCSLinkedRoleInWorkOrderReview	Service-Related Roles	dmc.cloud.tencent.com	Detailed List

Networking

Product	Role Name	Role Types	Role Entity
Cloud Loader Balance	CLB_QCSLinkedRoleInUploadCertificate	Service-Related Roles	clb.cloud.tencent.com
vpc	VPC_QCSLinkedRoleInEipTat	Service-Related Roles	eiptat.vpc.cloud.tencent.com
vpc	VPC_QCSLinkedRoleInSnapshot	Service-Related Roles	snapshot.vpc.cloud.tencent.com
vpc	VPC_QCSLinkedRoleInVpcflowlog	Service-Related Roles	vpcflowlog.vpc.cloud.tencent.com
vpc	VPC_QCSLinkedRoleInPrivateLink	Service-Related Roles	privatelink.vpc.cloud.tencent.com
vpc	VPC_QCSLinkedRoleInFlowLogAdvanceAnalysis	Service-Related Roles	flowlogadvanceanalysis.vpc.cloud.t

CDN and Acceleration

Product	Role Name	Role Types	Role Entity
CDN	CDN_QCSLinkedRoleInRecordListDNSPod	Service-Related Roles	recordlistdnspod.cdn.cloud.tencent.c
Global Application Acceleration Platform	GAAP_QCSLinkedRoleInCrossBorderCheck	Service-Related Roles	crossbordercheck.gaap.cloud.tence

Network Security

Product	Role Name	Role Types	Role Entity
Cloud Firewall	CFW_QCSLinkedRoleInGetiOAaccess	Service-Related Roles	GetiOAaccess.cfw.cloud.tencent.com
Tencent Cloud EdgeOne	TEO_QCSLinkedRoleInCertlist	Service-Related Roles	certlist.teo.cloud.tencent.com
Tencent Cloud EdgeOne	TEO_QCSLinkedRoleInUpstreamgw	Service-Related Roles	upstreamgw.teo.cloud.tencent.com
Tencent Cloud EdgeOne	TEO_QCSLinkedRoleInRealTimeLogCLS	Service-Related Roles	realtimelogcls.teo.cloud.tencent.com

Application Security

Product	Role Name	Role Types	Role Entity	Reference Document
cloudWaf	WAF_QCSLinkedRoleInCLS	Service-Related Roles	cls.waf.cloud.tencent.com	Detailed List
cloudWaf	WAF_QCSLinkedRoleInAccess	Service-Related Roles	access.waf.cloud.tencent.com	Detailed List
cloudWaf	WAF_QCSLinkedRoleInCKafka	Service-Related Roles	ckafka.waf.cloud.tencent.com	Detailed List

Domains & Websites

Product	Role Name	Role	Role Entity

		Types	
HTTPDNS	HTTPDNS_QCSLinkedRoleInCustomdns	Service-Related Roles	customdns.httpdns.cloud.ten
Private DNS	PrivateDNS_QCSLinkedRoleInPL	Service-Related Roles	privatedns.cloud.tencent.com
Private DNS	PrivateDNS_QCSLinkedRoleInCls	Service-Related Roles	privatedns.qcloud.com
SSL Certification	SSL_QCSLinkedRoleInCertificateWaf	Service-Related Roles	certificatewaf.ssl.cloud.tence
SSL Certification	SSL_QCSLinkedRoleInCertificateDependence	Service-Related Roles	certificatedependence.ssl.clo
SSL Certification	SSL_QCSLinkedRoleInReplaceLoadCertificate	Service-Related Roles	replaceloadcertificate.ssl.clou
SSL Certification	SSL_QCSLinkedRoleInCertificateCloudMonitor	Service-Related Roles	certificatecloudmonitor.ssl.cl
SSL Certification	SSL_QCSLinkedRoleInDescribeDeployedResources	Service-Related Roles	describedeployedresources.s

Big Data

Product	Role Name	Role Types	Role Entity
Cloud Data Warehouse ClickHouse	CDWCH_QCSLinkedRoleInCKCOS	Service-Related Roles	ckcos.cdwch.cloud.tencent.com
Cloud Data Warehouse	CDWCH_QCSLinkedRoleInCKLOGSHOW	Service-Related	cklogshow.cdwch.cloud.tencent.

ClickHouse		Roles	
Cloud Data Warehouse PostgreSQL	CDWPG_QCSLinkedRoleInPGCOS	Service-Related Roles	pgcos.cdwpg.cloud.tencent.com
Cloud Data Warehouse PostgreSQL	CDWPG_QCSLinkedRoleInPGKMS	Service-Related Roles	pgkms.cdwpg.cloud.tencent.com
Data Lake Compute	DLC_QCSLinkedRoleInCheckDLCResource	Service-Related Roles	checkdlcresource.dlc.cloud.tenc
Elasticsearch MapReduce	EMR_QCSLinkedRoleInApplicationDataAccess	Service-Related Roles	applicationdataaccess.emr.cloud
Elasticsearch Service	ES_QCSLinkedRoleInAccessCos	Service-Related Roles	acesscos.es.cloud.tencent.com
Elasticsearch Service	ES_QCSLinkedRoleInDataImport	Service-Related Roles	dataimport.es.cloud.tencent.com
Elasticsearch Service	ES_QCSLinkedRoleInVpcOperate	Service-Related Roles	vpcoperate.es.cloud.tencent.com
Elasticsearch Service	ES_QCSLinkedRoleInBeatsCollector	Service-Related Roles	beatscollector.es.cloud.tencent.c

Middleware

Product	Role Name	Role Types	Role Entity
RocketMQ	RocketMQ_QCSLinkedRoleInSendSSLcertificate	Service-Related Roles	sendSSLcertificate.rocketmq.clou
CKafka	cosCkafka_QCSRole	Service Role	ckafka.qcloud.com

Interactive Video Services

Product	Role Name	Role Types	Role Entity
Low-code interactive classroom	LCIC_QCSLinkedRoleInTransfer	Service-Related Roles	transfer.lcic.cloud.tencent.com
Tencent Real-Time Communication	TRTC_QCSLinkedRoleInCOSAccess	Service-Related Roles	cosaccess.trtc.cloud.tencent.com
Tencent Real-Time Communication	TRTC_QCSLinkedRoleIntrtcCloudRecording	Service-Related Roles	trtccloudrecording.trtc.cloud.tenc

Media On-Demand

Product	Role Name	Role Types	Role Entity
VOD	VOD_LogToCLS	Service-Related Roles	logtocls.vod.cloud.tencent.com
VOD	VOD_QCSLinkedRoleInHosting	Service-Related Roles	coshosting.vod.cloud.tencent.com
VOD	VOD_QCSLinkedRoleInManageSSLCertificates	Service-Related Roles	managesslcertificates.vod.cloud.tence

Cloud Real-time Rendering

Product	Role Name	Role Types	Role Entity	Refe Doc

Cloud Application Rendering	CAR_QCSLinkedRoleInCloudStorage	Service-Related Roles	cloudstorage.car.cloud.tencent.com	Deta List

Game Services

Product	Role Name	Role Types	Role Entity	Refer Docu
Game Multimedia Engine	GME_QCSLinkedRoleInGameMedia	Service-Related Roles	gamemedia.gme.cloud.tencent.com	Detai List

Cloud Resource Management

Product	Role Name	Role Types	Role Entity
Tencent Cloud Advisor	Advisor_QCSLinkedRoleInBusinessContinuity	Service-Related Roles	businesscontinuity.advisor.cloud.t
Tencent Cloud Mini Program Platform	TCMPP_QCSLinkedRoleInUserManage	Service-Related Roles	usermanage.tcmpp.cloud.tencent.
Tencent Cloud Infrastructure as Code	TIC_QCSLinkedRoleInInfrastructureAsCode	Service-Related Roles	infrastructureascode.tic.cloud.tenc

Management and Audit Tools

Product	Role Name	Role Types	Role Entity
Cloud Access	CAM_QCSLinkedRoleInEkslog	Service-Related	ekslog.cam.cloud.tencent.com

Management		Roles	
Cloud Access Management	CAM_QCSLinkedRoleInEkslog002	Service-Related Roles	ckmlog.cam.cloud.tencent.com
Cloud Access Management	CAM_QCSRole	Service Role	cam.cloud.tencent.com
Tencent Cloud Organization	Organization_QCSLinkedRoleInDefaultMng	Service-Related Roles	defaultmng.organization.cloud.tenc
Tencent Cloud Organization	Orgnization_QCSLinkedRoleInServiceControl	Service-Related Roles	servicecontrol.orgnization.cloud.ter

Compute
Cloud Virtual Machine

Last updated：2024-05-20 09:12:40

Service roles and service-linked roles are predefined by Tencent Cloud services and, upon user authorization, the corresponding services can access and use resources by assuming these service-linked roles. This document provides detailed information on the use cases and associated authorization policies of these specific service-linked roles.

Product	Role Name	Role Types	Role Entity
Cloud Virtual Machine	CVM_QCSLinkedRoleInCbsInit	Service-Related Roles	cbsinit.cvm.cloud.tencent.com
Cloud Virtual Machine	CVM_QCSLinkedRoleInCVMSmartDiagnostic	Service-Related Roles	cvmsmartdiagnostic.cvm.cloud.tencent

CVM_QCSLinkedRoleInCbsInit

Use Cases：The current role is the CVM service linked role, which will access your other service resources within the scope of the permissions of the associated policy.

Authorization Polices

- Policy Name：QcloudAccessForCVMLinkedRoleInCbsinit
- Policy Information：

```
{
"version": "2.0",
"statement": [
{
"effect": "allow",
"resource": [
"*"
],
"action": [
"tat:RunCommand",
"tat:DescribeInvocations",
```

```
"tat:DescribeInvocationTasks",
"tat:DescribeAutomationAgentStatus"
]
}
]
}
```

CVM_QCSLinkedRoleInCVMSmartDiagnostic

Use Cases： The current role is the CVM service linked role, which will access your other service resources within the scope of the permissions of the associated policy.

Authorization Polices

- Policy Name：QcloudAccessForCVMLinkedRoleInCVMSmartDiagnostic
- Policy Information：

```
{
"version": "2.0",
"statement": [
{
"action": [
"tat:DescribeAutomationAgentStatus",
"tat:RunCommand",
"tat:DescribeInvocationTasks",
"cwp:DescribeMachineInfo",
"cwp:DescribeMalWareList",
"cwp:DescribeHostLoginList",
"cwp:DescribeBruteAttackList",
"cwp:DescribeRiskDnsList",
"cwp:DescribeBashEvents"
],
"resource": "*",
"effect": "allow"
}
]
}
```

Tencent Cloud Lighthouse

Last updated：2024-05-20 09:12:47

Service roles and service-linked roles are predefined by Tencent Cloud services and, upon user authorization, the corresponding services can access and use resources by assuming these service-linked roles. This document provides detailed information on the use cases and associated authorization policies of these specific service-linked roles.

Product	Role Name	Role Types	Role Entity
Lighthouse	Lighthouse_QCSLinkedRoleInBasic	Service-Related Roles	basic.lighthouse.cloud.te
Lighthouse	Lighthouse_QCSLinkedRoleInCOSAndCI	Service-Related Roles	cosandci.lighthouse.clou
Lighthouse	Lighthouse_QCSLinkedRoleInDnsAndSsl	Service-Related Roles	dnsandssl.lighthouse.clc
Lighthouse	Lighthouse_QCSLinkedRoleInLighthouseSmartDiagnostic	Service-Related Roles	lighthousesmartdiagnost

Lighthouse_QCSLinkedRoleInBasic

Use Cases： The current role is the Lighthouse service linked role, which will access your other service resources within the scope of the permissions of the associated policy.

Authorization Polices

- Policy Name： QcloudAccessForLighthouseLinkedRoleInBasic
- Policy Information：

```
{
"version": "2.0",
"statement": [
{
"action": [
"vpc:*",
```

```
"cvm:*",
"tat:*"
],
"resource": "*",
"effect": "allow"
}
]
}
```

Lighthouse_QCSLinkedRoleInCOSAndCI

Use Cases：The current role is the Lighthouse service linked role, which will access your other service resources within the scope of the permissions of the associated policy.

Authorization Polices

- Policy Name：QcloudAccessForLighthouseLinkedRoleInCOSAndCI
- Policy Information：

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

Lighthouse_QCSLinkedRoleInDnsAndSsl

Use Cases：The current role is the Lighthouse service linked role, which will access your other service resources within the scope of the permissions of the associated policy.

Authorization Polices

- Policy Name：QcloudAccessForLighthouseLinkedRoleInDnsAndSsl
- Policy Information：

```
{
"version": "2.0",
"statement": [
{
"action": [
"kms:GetServiceStatus",
"kms:ListKeyDetail",
"kms:CreateKey",
"kms:Decrypt",
"kms:Encrypt",
"kms:GenerateDataKey",
"kms:BindCloudResource",
"kms:UnbindCloudResource",
"ssl:*",
"tat:*",
"dnspod:*",
"domain:*"
],
"resource": "*",
"effect": "allow"
}
]
}
```

Lighthouse_QCSLinkedRoleInLighthouseSmartDiagnostic

Use Cases：The current role is the Lighthouse service linked role, which will access your other service resources within the scope of the permissions of the associated policy.

Authorization Polices

- Policy Name：QcloudAccessForLighthouseLinkedRoleInLighthouseSmartDiagnostic
- Policy Information：

```
{
"version": "2.0",
"statement": [
{
"action": [
"tat:DescribeAutomationAgentStatus",
"tat:RunCommand",
"tat:DescribeInvocationTasks",
"cwp:DescribeMachineInfo",
```

```
"cwp:DescribeMalWareList",
"cwp:DescribeHostLoginList",
"cwp:DescribeBruteAttackList",
"cwp:DescribeRiskDnsList",
"cwp:DescribeBashEvents"
],
"resource": "*",
"effect": "allow"
}
]
}
```

Batch Compute

Last updated：2024-05-20 09:12:32

Service roles and service-linked roles are predefined by Tencent Cloud services and, upon user authorization, the corresponding services can access and use resources by assuming these service-linked roles. This document provides detailed information on the use cases and associated authorization policies of these specific service-linked roles.

Product	Role Name	Role Types	Role Entity
BatchCompute	BATCH_QCSLinkedRoleInAcrossService	Service-Related Roles	acrossservice.batch.cloud.tencent.cc

BATCH_QCSLinkedRoleInAcrossService

Use Cases：The current role is the BATCH service linked role, which will access your other service resources within the scope of the permissions of the associated policy.

Authorization Polices

- Policy Name：QcloudAccessForBATCHLinkedRoleInAcrossService
- Policy Information：

```
{
"version": "2.0",
"statement": [
{
"action": [
"cvm:RunInstances",
"cvm:ModifyInstancesAttribute",
"cvm:ResetInstance",
"cvm:DescribeInstancesStatus",
"cvm:DescribeInstances",
"cvm:TerminateInstances",
"cvm:DescribeImages",
"finance:trade",
"kms:BindCloudResource"
],
"resource": "*",
"effect": "allow"
```

```
}
]
}
```

Tencent Cloud Automation Tools

Last updated：2024-05-20 09:12:53

Service roles and service-linked roles are predefined by Tencent Cloud services and, upon user authorization, the corresponding services can access and use resources by assuming these service-linked roles. This document provides detailed information on the use cases and associated authorization policies of these specific service-linked roles.

Product	Role Name	Role Types	Role Entity
TencentCloud Automation Tools	TAT_QCSLinkedRoleInCommand	Service-Related Roles	command.tat.cloud.tencent.com
TencentCloud Automation Tools	TAT_QCSLinkedRoleInUploadInvocation	Service-Related Roles	uploadinvocation.tat.cloud.tencent.cor

TAT_QCSLinkedRoleInCommand

Use Cases：The current role is the TAT service linked role, which will access your other service resources within the scope of the permissions of the associated policy.

Authorization Polices

- Policy Name：QcloudAccessForTATLinkedRoleInCommand
- Policy Information：

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

TAT_QCSLinkedRoleInUploadInvocation

Use Cases： The current role is the TAT service linked role, which will access your other service resources within the scope of the permissions of the associated policy.

Authorization Polices

- Policy Name：QcloudAccessForTATLinkedRoleInUploadInvocation
- Policy Information：

```
{
"statement": [
{
"action": [
"cos:HeadBucket",
"cos:GetBucket",
"cos:PutObject"
],
"effect": "allow",
"resource": "*"
}
],
"version": "2.0"
}
```

Container
Tencent Kubernetes Engine

Last updated：2024-05-20 09:12:56

Service roles and service-linked roles are predefined by Tencent Cloud services and, upon user authorization, the corresponding services can access and use resources by assuming these service-linked roles. This document provides detailed information on the use cases and associated authorization policies of these specific service-linked roles.

Product	Role Name	Role Types	Role Entity
Tencent Kubernetes Engine	TKE_QCSLinkedRoleInTDCC	Service-Related Roles	cvm.qcloud.com tdcc.tke.cloud.tencent.com
Tencent Kubernetes Engine	TKE_QCSLinkedRoleInEKSLog	Service-Related Roles	cvm.qcloud.com ekslog.tke.cloud.tencent.com
Tencent Kubernetes Engine	TKE_QCSLinkedRoleInEtcdService	Service-Related Roles	cvm.qcloud.com etcdservice.tke.cloud.tencent.com
Tencent Kubernetes Engine	TKE_QCSLinkedRoleInEKSCostMaster	Service-Related Roles	cvm.qcloud.com ekscostmaster.tke.cloud.tencent.com
Tencent Kubernetes Engine	TKE_QCSLinkedRoleInPrometheusService	Service-Related Roles	cvm.qcloud.com prometheusservice.tke.cloud.tencent.c

TKE_QCSLinkedRoleInTDCC

Use Cases： The current role is the TKE service linked role, which will access your other service resources within the scope of the permissions of the associated policy.

Authorization Polices

- Policy Name： QcloudAccessForTKELinkedRoleInTDCC
- Policy Information：

```
{
"version": "2.0",
"statement": [
{
"effect": "allow",
"action": [
"cls:listTopic",
"cls:getTopic",
"cls:createTopic",
"cls:modifyTopic",
"cls:listMachineGroup",
"cls:getMachineGroup",
"cls:createMachineGroup",
"cls:modifyMachineGroup",
"cls:deleteMachineGroup",
"cls:getMachineStatus",
"cls:pushLog",
"cls:agentHeartBeat",
"cls:getConfig",
"cls:getIndex",
"cls:modifyIndex",
"cls:ApplyConfigToMachineGroup",
"cls:CreateConfig",
"cls:CreateIndex",
"cls:CreateLogset",
"cls:CreateMachineGroup",
"cls:CreateTopic",
"cls:DeleteConfig",
"cls:DeleteConfigFromMachineGroup",
"cls:DeleteLogset",
"cls:DeleteMachineGroup",
"cls:DeleteTopic",
"cls:DescribeConfigMachineGroups",
"cls:DescribeConfigs",
"cls:DescribeLogsets",
"cls:DescribeMachineGroupConfigs",
"cls:DescribeMachineGroups",
"cls:DescribeTopics",
"cls:ModifyConfig",
"cls:ModifyIndex",
"cls:ModifyMachineGroup",
"cls:ModifyTopic"
],
"resource": [
"*"
]
```

```
}
]
}
```

TKE_QCSLinkedRoleInEKSLog

Use Cases： The current role is the TKE service role, which will access your other service resources within the scope of the permissions of the associated policy.

Authorization Polices

- Policy Name：QcloudAccessForTKELinkedRoleInEKSLog
- Policy Information：

```
{
"version": "2.0",
"statement": [
{
"effect": "allow",
"action": [
"cls:listTopic",
"cls:getTopic",
"cls:createTopic",
"cls:modifyTopic",
"cls:listMachineGroup",
"cls:getMachineGroup",
"cls:createMachineGroup",
"cls:modifyMachineGroup",
"cls:deleteMachineGroup",
"cls:getMachineStatus",
"cls:pushLog",
"cls:agentHeartBeat",
"cls:getConfig",
"cls:getIndex",
"cls:modifyIndex",
"cls:ApplyConfigToMachineGroup",
"cls:CreateConfig",
"cls:CreateIndex",
"cls:CreateLogset",
"cls:CreateMachineGroup",
"cls:CreateTopic",
"cls:DeleteConfig",
"cls:DeleteConfigFromMachineGroup",
"cls:DeleteLogset",
```

```
"cls:DeleteMachineGroup",
"cls:DeleteTopic",
"cls:DescribeConfigMachineGroups",
"cls:DescribeConfigs",
"cls:DescribeLogsets",
"cls:DescribeMachineGroupConfigs",
"cls:DescribeMachineGroups",
"cls:DescribeTopics",
"cls:ModifyConfig",
"cls:ModifyIndex",
"cls:ModifyMachineGroup",
"cls:ModifyTopic"
],
"resource": [
"*"
]
}
]
}
```

TKE_QCSLinkedRoleInEtcdService

Use Cases：The current role is the TKE service role, which will access your other service resources within the scope of the permissions of the associated policy.

Authorization Polices

- Policy Name：QcloudAccessForTKELinkedRoleInEtcdService
- Policy Information：

```
{
"version": "2.0",
"statement": [
{
"effect": "allow",
"resource": [
"*"
],
"action": [
"cos:DeleteBucket",
"cos:GetBucket",
"cos:PutBucket",
"cos:HeadBucket",
"cos:GetObject",
```

```
"cos:HeadObject",
"cos:PutObject",
"cos:DeleteObject",
"cos:DeleteMultipleObjects",
"cos:ListMultipartUploads",
"cos:AbortMultipartUpload"
]
}
]
}
```

TKE_QCSLinkedRoleInEKSCostMaster

Use Cases：The current role is the TKE service linked role, which will access your other service resources within the scope of the permissions of the associated policy.

Authorization Polices

- Policy Name：QcloudAccessForTKELinkedRoleInEKSCostMaster
- Policy Information：

```
{
"version": "2.0",
"statement": [
{
"action": [
"monitor:DescribeMidDimensionValueList",
"monitor:DescribeStatisticData",
"monitor:GetMonitorData"
],
"resource": "*",
"effect": "allow"
}
]
}
```

TKE_QCSLinkedRoleInPrometheusService

Use Cases：The current role is the TKE service role, which will access your other service resources within the scope of the permissions of the associated policy.

Authorization Polices

- Policy Name：QcloudAccessForTKELinkedRoleInPrometheusService
- Policy Information：

```
{
"statement": [
{
"action": [
"cos:DeleteBucket",
"cos:GetBucket",
"cos:PutBucket",
"cos:HeadBucket",
"cos:GetObject",
"cos:HeadObject",
"cos:PutObject",
"cos:DeleteObject",
"cos:DeleteMultipleObjects",
"cos:ListMultipartUploads",
"cos:AbortMultipartUpload",
"cos:AbortMultipartUpload",
"cos:ListMultipartUploads",
"monitor:DescribePrometheusInstances",
"monitor:DescribeRecordingRules",
"monitor:DescribeAlertRules",
"monitor:DescribeAlarmNotice",
"monitor:DescribeAlarmNotices",
"monitor:DescribeAlarmNoticeCallbacks",
"monitor:DescribeAlarmHistories",
"monitor:CreatePrometheusMultiTenantInstance",
"monitor:TerminatePrometheusInstances",
"monitor:ModifyPrometheusInstanceAttributes",
"monitor:CreateRecordingRule",
"monitor:DeleteRecordingRules",
"monitor:UpdateRecordingRule",
"monitor:CreateAlertRule",
"monitor:DeleteAlertRules",
"monitor:UpdateAlertRule",
"monitor:UpdateAlertRuleState",
"monitor:CreateAlarmNotice",
"monitor:DeleteAlarmNotices",
"monitor:ModifyAlarmNotice",
"monitor:ModifyAlarmPolicyNotice",
"monitor:CreateManagedEKSAgent",
"monitor:DescribeManagedEKSAgent",
"monitor:CreateAlertRuleReceiverNotRequired",
"monitor:UpdateAlertRuleReceiverNotRequired",
```

```
"monitor:DescribeExporterIntegrations",
"monitor:CreateExporterIntegration",
"monitor:UpdateExporterIntegration",
"monitor:DeleteExporterIntegration",
"monitor:CreateGrafanaInstance",
"monitor:CreatePrometheusMultiTenantInstancePostPayMode",
"monitor:BindPrometheusManagedGrafana",
"monitor:DescribeGrafanaInstances",
"tdcc:DescribeExternalClusters",
"tdcc:DescribeExternalClusterCredential",
"monitor:UpgradeGrafanaDashboard",
"monitor:UninstallGrafanaDashboard",
"monitor:DescribePrometheusAlertGroups",
"monitor:CreatePrometheusAlertGroup",
"monitor:UpdatePrometheusAlertGroup",
"monitor:DeletePrometheusAlertGroups",
"monitor:UpdatePrometheusAlertGroupState",
"tke:DescribeTKEEdgeExternalKubeconfig",
"tke:DescribeTKEEdgeClusterCredential",
"tke:DescribeTKEEdgeClusters",
"tke:DescribeClusters",
"tke:DescribeClusterSecurity"
],
"effect": "allow",
"resource": [
"*"
]
}
],
"version": "2.0"
}
```

Microservice
Tencent Cloud Elastic Microservice

Last updated：2024-05-20 09:12:54

Service roles and service-linked roles are predefined by Tencent Cloud services and, upon user authorization, the corresponding services can access and use resources by assuming these service-linked roles. This document provides detailed information on the use cases and associated authorization policies of these specific service-linked roles.

Product	Role Name	Role Types	Role Entity
Tencent Cloud Elastic Microservice	TEM_QCSLinkedRoleInTEMAPI	Service-Related Roles	temapi.tem.cloud.tencent.com
Tencent Cloud Elastic Microservice	TEM_QCSLinkedRoleInTEMLog	Service-Related Roles	cvm.qcloud.com temlog.tem.cloud.tencent.com
Tencent Cloud Elastic Microservice	TEM_QCSLinkedRoleInAccessCluster	Service-Related Roles	accesscluster.tem.cloud.tencen
Tencent Cloud Elastic Microservice	TEM_QCSLinkedRoleInAccessResourceService	Service-Related Roles	accessresourceservice.tem.clou

TEM_QCSLinkedRoleInTEMAPI

Use Cases： The current role is the TEM service role, which will access your other service resources within the scope of the permissions of the associated policy.

Authorization Polices

- Policy Name： QcloudAccessForTEMLinkedRoleInTEMApi
- Policy Information：

```
{
"version": "2.0",
"statement": [
{
"effect": "allow",
"resource": [
"*"
],
"action": [
"apm:CreatePAASInstance",
"apm:DescribeApmAgent",
"apm:DescribeTopology",
"apm:DeletePAASInstance",
"apm:DescribePAASTopology",
"tcb:CreateCloudBaseRunServerVersionWithMicroService"
]
}
]
}
```

TEM_QCSLinkedRoleInTEMLog

Use Cases：The current role is the TEM service linked role, which will access your other service resources within the scope of the permissions of the associated policy.

Authorization Polices

- Policy Name：QcloudAccessForTEMLinkedRoleInTEMLog
- Policy Information：

```
{
"version": "2.0",
"statement": [
{
"effect": "allow",
"resource": [
"*"
],
"action": [
"cls:listTopic",
"cls:getTopic",
"cls:createTopic",
"cls:modifyTopic",
```

```
"cls:listMachineGroup",
"cls:getMachineGroup",
"cls:createMachineGroup",
"cls:modifyMachineGroup",
"cls:deleteMachineGroup",
"cls:getMachineStatus",
"cls:pushLog",
"cls:agentHeartBeat",
"cls:getConfig"
]
}
]
}
```

TEM_QCSLinkedRoleInAccessCluster

Use Cases：The current role is the TEM service linked role, which will access your other service resources within the scope of the permissions of the associated policy.

Authorization Polices

- Policy Name：QcloudAccessForTEMLinkedRoleInAccessCluster
- Policy Information：

```
{
"version": "2.0",
"statement": [
{
"effect": "allow",
"action": [
"tse:DescribeSREInstances",
"tse:DescribeSREInstanceAccessAddress",
"tse:DescribeSREGlobalConfigs",
"tke:DescribeClusters",
"tcr:CreateNamespacePersonal",
"tcr:DeleteNamespacePersonal",
"tcr:DescribeRepositoryOwnerPersonal",
"tcr:DeleteRepositoryPersonal",
"tcr:DeleteImagePersonal",
"tcr:CreateRepositoryPersonal",
"tcr:BatchDeleteRepositoryPersonal",
"tcr:BatchDeleteImagePersonal",
"tcr:CreateInstanceToken",
"tcr:DescribeInstanceToken",
```

```
"tcr:DeleteInstanceToken",
"tcr:DescribeRepositories",
"tcr:PullRepository",
"tcr:PullRepositoryPersonal",
"cls:searchLog",
"cls:getTopic",
"cls:getIndex",
"cls:CreateIndex",
"cls:modifyIndex",
"cls:DeleteIndex",
"cfs:DescribeCfsFileSystems",
"cfs:DescribeMountTargets",
"vpc:DescribeSubnetEx",
"vpc:DescribeSubnet",
"apm:CreateApmInstance",
"apm:ModifyApmInstance",
"apm:TerminateApmInstance",
"apm:CreatePAASInstance",
"apm:DeletePAASInstance",
"apm:DescribeApmAgent",
"apm:DescribeTopologyMetricLineData",
"apm:DescribeMetricLineData",
"apm:DescribeServiceOverview",
"apm:DescribeMetricRecords",
"cam:GetRole",
"tcr:DescribeInternalEndpoints",
"tcr:DescribeInternalEndpointDnsStatus",
"tcr:CreateInternalEndpointDns",
"tcr:DuplicateImagePersonal",
"tcr:DescribeInstances",
"tcr:CreateInstance",
"tcr:DescribeNamespaces",
"tcr:CreateNamespace",
"tcr:CreateRepository",
"tcr:DescribeRepositories",
"tcr:ManageInternalEndpoint",
"tcr:PushRepository",
"tcr:PushRepositoryPersonal",
"monitor:DescribePrometheusInstances",
"monitor:UpgradeGrafanaDashboard",
"vpc:CreateVpc",
"vpc:CreateSubnet",
"vpc:DescribeVpcEx",
"vpc:DeleteNatGateway",
"vpc:CreateNatGateway",
"vpc:CreateRoute",
"vpc:EnableRoutes",
```

```
"vpc:DeleteRoute",
"vpc:DescribeNatGateways",
"vpc:DescribeRouteTable",
"cvm:ReleaseAddresses",
"monitor:TerminatePrometheusInstances",
"monitor:CreatePrometheusMultiTenantInstancePostPayMode"
],
"resource": [
"*"
]
}
]
}
```

TEM_QCSLinkedRoleInAccessResourceService

Use Cases： The current role is the TEM service role， which will access your other service resources within the scope of the permissions of the associated policy.

Authorization Polices

- Policy Name：QcloudAccessForTEMLinkedRoleInAccessResourceService
- Policy Information：

```
{
"version": "2.0",
"statement": [
{
"effect": "allow",
"action": [
"tcb:DescribeCloudBaseGWAPI",
"tcb:DescribeCloudBaseRunServer",
"tcb:DescribeCloudBaseRunServers",
"tcb:DescribeCloudBaseRunServerVersion",
"tcb:DescribeEnvLimit",
"tcb:DescribeCloudBaseRunPodList",
"tcb:DescribeICPResources",
"tcb:DescribePostPackage",
"tcb:DescribeCloudBaseGWService",
"tcb:DescribeCurveData",
"tcb:SearchClsLog",
"tcb:DescribeCloudBaseRunImages",
"tcb:DescribeCloudBaseRunServerFlowConf",
"tcb:CreateCloudBaseRunServerVersion",
```

```
"tcb:CreateCloudBaseGWAPI",
"tcb:ModifyCloudBaseGWAPIPublicAccess",
"tcb:ModifyCloudBaseGWAPIAccessType",
"tcb:ModifyCloudBaseRunServerVersion",
"tcb:CreatePostpayPackage",
"tcb:DeleteCloudBaseRunImageRepo",
"tcb:DeleteCloudBaseRunServer",
"tcb:DeleteCloudBaseRunServerVersion",
"tcb:EstablishCloudBaseRunServer",
"tcb:ModifyCloudBaseRunServerFlowConf",
"tcb:RollUpdateCloudBaseRunServerVersion",
"tcb:DescribeEnvs",
"tcb:DestroyEnv",
"tcb:CheckTcbService",
"tcb:ModifyEnv",
"tcb:DescribeCloudBaseRunVersionException"
],
"resource": [
"*"
]
}
]
}
```

Essential Storage Service
Cloud Object Storage

Last updated：2024-05-20 09:12:40

Service roles and service-linked roles are predefined by Tencent Cloud services and, upon user authorization, the corresponding services can access and use resources by assuming these service-linked roles. This document provides detailed information on the use cases and associated authorization policies of these specific service-linked roles.

Product	Role Name	Role Types	Role Entity
COS	COS_QCSLinkedRoleInCOSAcc	Service-Related Roles	COSAcc.COS.cloud.tencent.com
COS	COS_QCSLinkedRoleInCLSAccess	Service-Related Roles	cosoclsr.cos.cloud.tencent.com
COS	COS_QCSLinkedRoleInLighthouseMounting	Service-Related Roles	lhmounting.cos.cloud.tencent.com

COS_QCSLinkedRoleInCOSAcc

Use Cases： The current role is the COS service linked role, which will access your other service resources within the scope of the permissions of the associated policy.

Authorization Polices

- Policy Name：QcloudAccessForCOSLinkedRoleInCOSAcc
- Policy Information：

```
{
"statement": [
{
"action": [
"cos:*"
],
"effect": "allow",
"resource": "*"
```

```
}
],
"version": "2.0"
}
```

COS_QCSLinkedRoleInCLSAccess

Use Cases：Object Storage Service (COS) operation permissions include but are not limited to the following permissions: Add, delete, and modify log service (CLS) log sets, log topics, logs, add, delete, and modify machine groups, add, delete, and modify indexes, and delivery logs, etc.

Authorization Polices

- Policy Name：QcloudAccessForCOSLinkedRoleInCosoclsr
- Policy Information：

```
{
"version": "2.0",
"statement": [
{
"effect": "allow",
"action": [
"cls:CreateIndex",
"cls:ModifyIndex",
"cls:DescribeIndex",
"cls:CreateTopic",
"cls:ModifyTopic",
"cls:DeleteTopic",
"cls:DescribeTopics",
"cls:ModifyLogset",
"cls:DeleteLogset",
"cls:CreateLogset",
"cls:DescribeLogsets"
],
"resource": "*"
}
]
}
```

COS_QCSLinkedRoleInLighthouseMounting

Use Cases：The current role is the COS service linked role, which will access your other service resources within the scope of the permissions of the associated policy.

Authorization Polices

- Policy Name：QcloudAccessForCOSLinkedRoleInLighthouseMounting
- Policy Information：

```
{
"statement": [
{
"action": [
"tat:DescribeCommands",
"tat:RunCommand",
"tat:InvokeCommand",
"tat:DescribeInvocations",
"tat:DescribeInvocationTasks",
"tat:DescribeAutomationAgentStatus",
"tat:CancelInvocation",
"tat:DescribeInstancesFeatureStatus"
],
"effect": "allow",
"resource": "*"
}
],
"version": "2.0"
}
```

Cloud HDFS

Last updated：2024-05-20 09:12:37

Service roles and service-linked roles are predefined by Tencent Cloud services and, upon user authorization, the corresponding services can access and use resources by assuming these service-linked roles. This document provides detailed information on the use cases and associated authorization policies of these specific service-linked roles.

Product	Role Name	Role Types	Role Entity
Cloud HDFS	CHDFS_QCSLinkedRoleInMetaMgmt	Service-Related Roles	metamgmt.chdfs.cloud.tencent.com

CHDFS_QCSLinkedRoleInMetaMgmt

Use Cases： The current role is the CHDFS service linked role, which will access your other service resources within the scope of the permissions of the associated policy.

Authorization Polices

- Policy Name： QcloudAccessForCOSLinkedRoleInMetaMgmt
- Policy Information：

```
{
"version": "2.0",
"statement": [
{
"action": [
"cos:GetBucket",
"cos:GetBucketObjectVersions",
"cos:PutObject",
"cos:PutObjectCopy",
"cos:PostObject",
"cos:AppendObject",
"cos:GetObject",
"cos:HeadObject",
"cos:DeleteObject",
"cos:OptionsObject",
"cos:PostObjectRestore",
"cos:InitiateMultipartUpload",
"cos:UploadPart",
"cos:UploadPartCopy",
```

```
"cos:CompleteMultipartUpload",
"cos:AbortMultipartUpload",
"cos:ListMultipartUploads",
"cos:ListParts",
"cos:GetBucketLifecycle",
"cos:PutBucketLifecycle",
"cos:DeleteBucketLifecycle",
"cos:PutObjectTagging",
"cos:GetObjectTagging",
"cos:DeleteObjectTagging"
],
"resource": "*",
"effect": "allow"
}
]
}
```

Data Process and Analysis
Cloud Log Service

Last updated：2024-05-20 09:12:39

Service roles and service-linked roles are predefined by Tencent Cloud services and, upon user authorization, the corresponding services can access and use resources by assuming these service-linked roles. This document provides detailed information on the use cases and associated authorization policies of these specific service-linked roles.

Product	Role Name	Role Types	Role Entity
Cloud Log Service	CLS_QCSRoleInAnonymousSharing	Service-Related Roles	console-sharing.cls.cloud.tencent.com

CLS_QCSRoleInAnonymousSharing

Use Cases：When the current role is used as a CLS anonymous sharing link and is accessed, CLS obtains the data required to share the content (retrieval page/dashboard page)

Authorization Polices

- Policy Name：QcloudAccessForClsRoleInSharing
- Policy Information：

```
{
"version": "3.0",
"statement": [
{
"effect": "allow",
"action": [
"cls:SearchLog",
"cls:DescribeTopics",
"cls:DescribeIndex",
"cls:DescribeLogHistogram",
"cls:DescribeDashboards",
"cls:QueryRangeMetric",
"cls:QueryMetric"
],
"resource": "*"
}
```

```
]
}
```

Data Migration
Migration Service Platform

Last updated：2024-05-20 09:12:49

Service roles and service-linked roles are predefined by Tencent Cloud services and, upon user authorization, the corresponding services can access and use resources by assuming these service-linked roles. This document provides detailed information on the use cases and associated authorization policies of these specific service-linked roles.

Product	Role Name	Role Types	Role Entity
Migration Service Platform	MSP_QCSLinkedRoleInMIGtocos	Service-Related Roles	migtocos.msp.cloud.tencent.com

MSP_QCSLinkedRoleInMIGtocos

Use Cases：The current role is the MSP service linked role, which will access your other service resources within the scope of the permissions of the associated policy.

Authorization Polices

- Policy Name：QcloudAccessForMSPLinkedRoleInMIGtocos
- Policy Information：

```
{
"statement": [
{
"action": [
"cos:GetService",
"cos:PutObject",
"cos:GetObject"
],
"effect": "allow",
"resource": "*"
}
],
"version": "2.0"
}
```

Relational Database
TDSQL-C for MySQL

Last updated：2024-05-20 09:12:41

Service roles and service-linked roles are predefined by Tencent Cloud services and, upon user authorization, the corresponding services can access and use resources by assuming these service-linked roles. This document provides detailed information on the use cases and associated authorization policies of these specific service-linked roles.

Product	Role Name	Role Types	Role Entity
Cloud Native Database TDSQL-C	CynosDBMysql_QCSLinkedRoleInKms	Service-Related Roles	kms.cynosdb.cloud.tencent.com
Cloud Native Database TDSQL-C	CynosDBMysql_QCSLinkedRoleInClslog	Service-Related Roles	clslog.cynosdb.cloud.tencent.com

CynosDBMysql_QCSLinkedRoleInKms

Use Cases：The current role is the cynosdb service linked role, which will access your other service resources within the scope of the permissions of the associated policy.

Authorization Polices

- Policy Name：QcloudAccessForCynosDBLinkedRoleInKms
- Policy Information：

```
{
"version": "2.0",
"statement": [
{
"effect": "allow",
"action": [
"kms:GetServiceStatus",
"kms:ListKeyDetail",
"kms:CreateKey",
"kms:GenerateDataKey",
"kms:Decrypt",
```

```
"kms:BindCloudResource",
"kms:UnbindCloudResource"
],
"resource": [
"*"
]
}
]
}
```

CynosDBMysql_QCSLinkedRoleInClslog

Use Cases： The current role is the CYNOSDB service linked role, which will access your other service resources within the scope of the permissions of the associated policy.

Authorization Polices

- Policy Name：QcloudAccessForCynosDBLinkedRoleInClslog
- Policy Information：

```
{
"version": "2.0",
"statement": [
{
"effect": "allow",
"action": [
"cls:DescribeIndexs",
"cls:DescribeTopics",
"cls:DescribeIndex",
"cls:CreateIndex",
"cls:DeleteIndex",
"cls:ModifyIndex",
"cls:pushLog",
"cls:CreateLogset",
"cls:CreateTopic",
"cls:DescribeLogsets",
"cls:DeleteTopic",
"cls:DeleteLogset"
],
"resource": [
"*"
]
}
```

```
]
}
```

TencentDB for MySQL

Last updated：2024-05-20 09:12:34

Service roles and service-linked roles are predefined by Tencent Cloud services and, upon user authorization, the corresponding services can access and use resources by assuming these service-linked roles. This document provides detailed information on the use cases and associated authorization policies of these specific service-linked roles.

Product	Role Name	Role Types	Role Entity
Cloud Database	CDB_QCSLinkedRoleInDBLog	Service-Related Roles	DBLog.cdb.cloud.tencent.com
Cloud Database	CDB_QCSLinkedRoleInCdbwan	Service-Related Roles	cdbwan.cdb.cloud.tencent.com

CDB_QCSLinkedRoleInDBLog

Use Cases：The current role is the TencentDB for MySQL service linked role, which will access your other service resources within the scope of the permissions of the associated policy.

Authorization Polices

- Policy Name：QcloudAccessForCDBLinkedRoleInDBLog
- Policy Information：

```
{
"version": "2.0",
"statement": [
{
"effect": "allow",
"action": [
"cls:ModifyKafkaRecharge",
"cls:DescribeKafkaRecharges",
"cls:DeleteKafkaRecharge",
"cls:CreateKafkaRecharge"
],
"resource": "*"
}
]
}
```

CDB_QCSLinkedRoleInCdbwan

Use Cases： The current role is the CDBservice linked role, which will access your other service resources within the scope of the permissions of the associated policy.

Authorization Polices

- Policy Name：QcloudAccessForCDBLinkedRoleInCdbwan
- Policy Information：

```
{
"statement": [
{
"action": [
"clb:DescribeLoadBalancers",
"clb:CreateLoadBalancer",
"clb:DeleteLoadBalancer",
"clb:ModifyLoadBalancerAttributes",
"clb:ModifyLBOperateProtect",
"clb:CreateListener",
"clb:DescribeListeners",
"clb:DeleteListener",
"clb:RegisterTargets",
"clb:BatchRegisterTargets",
"clb:DeregisterTargets",
"clb:BatchDeregisterTargets",
"clb:ModifyListener",
"clb:DescribeTaskStatus"
],
"effect": "allow",
"resource": [
"*"
]
}
],
"version": "2.0"
}
```

TencentDB for PostgreSQL

Last updated：2024-05-20 09:12:50

Service roles and service-linked roles are predefined by Tencent Cloud services and, upon user authorization, the corresponding services can access and use resources by assuming these service-linked roles. This document provides detailed information on the use cases and associated authorization policies of these specific service-linked roles.

Product	Role Name	Role Types	Role Entity
TencentDB For PostgreSQL	Postgres_QCSLinkedRoleInPostgresKms	Service-Related Roles	postgreskms.postgres.cloud.tencent.co

Postgres_QCSLinkedRoleInPostgresKms

Use Cases：The current role is the PostgreSQL service linked role, which will access your other service resources within the scope of the permissions of the associated policy.

Authorization Polices

- Policy Name：QcloudAccessForPostgresLinkedRoleInPostgresKms
- Policy Information：

```
{
"version": "2.0",
"statement": [
{
"action": [
"kms:Decrypt",
"kms:GetServiceStatus",
"kms:ListKeyDetail",
"kms:CreateKey",
"kms:GenerateDataKey",
"kms:BindCloudResource",
"kms:UnbindCloudResource"
],
"resource": "*",
"effect": "allow"
}
```

```
]
}
```

Enterprise Distributed DBMS
TDSQL for MySQL

Last updated：2024-05-20 09:12:41

Service roles and service-linked roles are predefined by Tencent Cloud services and, upon user authorization, the corresponding services can access and use resources by assuming these service-linked roles. This document provides detailed information on the use cases and associated authorization policies of these specific service-linked roles.

Product	Role Name	Role Types	Role Entity
TDSQL for MySQL	DCDB_QCSLinkedRoleInKMS	Service-Related Roles	kms.dcdb.cloud.tencent.com
TDSQL for MySQL	DCDB_QCSLinkedRoleInTSE	Service-Related Roles	tse.dcdb.cloud.tencent.com

DCDB_QCSLinkedRoleInKMS

Use Cases：The current role is the DCDB service linked role, which will access your other service resources within the scope of the permissions of the associated policy.

Authorization Polices

- Policy Name：QcloudAccessForDCDBLinkedRoleInKMS
- Policy Information：

```
{
"version": "2.0",
"statement": [
{
"effect": "allow",
"resource": [
"*"
],
"action": [
"kms:GetServiceStatus",
"kms:CreateKey",
"kms:GenerateDataKey",
"kms:Decrypt",
"kms:Encrypt",
```

```
"kms:ReEncrypt",
"kms:EnableKey",
"kms:EnableKeyRotation",
"kms:ListKeyDetail",
"kms:DescribeKey",
"kms:ListKey"
]
}
]
}
```

DCDB_QCSLinkedRoleInTSE

Use Cases：The current role is the DCDB service linked role, which will access your other service resources within the scope of the permissions of the associated policy.

Authorization Polices

- Policy Name：QcloudAccessForDCDBLinkedRoleInTSE
- Policy Information：

```
{
"statement": [
{
"action": [
"tse:CreateGovernanceStrategy",
"tse:DescribeGovernanceMainToken",
"tse:DescribeGovernanceInstances",
"tse:DescribeGovernanceServices",
"tse:CreateGovernanceInstances",
"tse:DeleteGovernanceInstances",
"tse:ModifyGovernanceServices",
"tse:DescribeGovernanceStrategies",
"tse:DescribeSREInstances",
"tse:ModifyGovernanceInstances",
"tse:DescribeGovernanceNamespaces",
"tse:DescribeGovernanceAuthStrategies"
],
"effect": "allow",
"resource": "*"
}
],
"version": "2.0"
}
```

NoSQL Database
TencentDB for MongoDB

Last updated：2024-05-20 09:12:48

Service roles and service-linked roles are predefined by Tencent Cloud services and, upon user authorization, the corresponding services can access and use resources by assuming these service-linked roles. This document provides detailed information on the use cases and associated authorization policies of these specific service-linked roles.

Product	Role Name	Role Types	Role Entity
Cloud MongoDB	MongoDB_QCSLinkedRoleInKMS	Service-Related Roles	kms.mongodb.cloud.tencent.com

MongoDB_QCSLinkedRoleInKMS

Use Cases：The current role is the MongoDB service linked role, which will access your other service resources within the scope of the permissions of the associated policy.

Authorization Polices

- Policy Name：QcloudAccessForMongoDBLinkedRoleInKMS
- Policy Information：

```
{
"statement": [
{
"action": [
"kms:GetServiceStatus",
"kms:ListKeyDetail",
"kms:CreateKey",
"kms:GenerateDataKey",
"kms:Decrypt",
"kms:BindCloudResource",
"kms:UnbindCloudResource"
],
"effect": "allow",
"resource": [
"*"
]
}
```

```
],
"version": "2.0"
}
```

Database SaaS Tool
Database Management Center

Last updated：2024-05-20 09:12:42

Service roles and service-linked roles are predefined by Tencent Cloud services and, upon user authorization, the corresponding services can access and use resources by assuming these service-linked roles. This document provides detailed information on the use cases and associated authorization policies of these specific service-linked roles.

Product	Role Name	Role Types	Role Entity
Database Management Console	DMC_QCSLinkedRoleInWorkOrderReview	Service-Related Roles	dmc.cloud.tencent.com

DMC_QCSLinkedRoleInWorkOrderReview

Use Cases：The current role is the DMC service linked role, which will access your other service resources within the scope of the permissions of the associated policy.

Authorization Polices

- Policy Name：QcloudAccessForDMCLinkedRoleInWorkOrderReview
- Policy Information：

```
{
"statement": [
{
"action": [
"cam:ListUsersForGroup",
"cam:ListGroupsForUser",
"cam:DescribeSubAccounts",
"cam:ListGroups",
"cdb:DescribeAccounts",
"dcdb:DescribeAccounts",
"cynosdb:DescribeAccounts",
"mongodb:DescribeAccountUsers",
"mariadb:DescribeAccounts",
"postgres:DescribeAccounts",
"sqlserver:DescribeAccounts",
"sts:AssumeRole",
```

```
"cam:ListAttachedUserAllPolicies",
"cam:GetGroup",
"cam:ListUsers",
"cvm:DescribeInstances",
"vdb:DescribeInstances",
"vdb:DescribeInstanceProperties",
"vdb:DescribeEmbedding",
"redis:DescribeInstances",
"keewidb:DescribeInstances",
"mongodb:DescribeDBInstances",
"ctsdb:DescribeDBInstances",
"tdach:DescribeInstances",
"cdb:DescribeInstances",
"sqlserver:DescribeDBInstances",
"mariadb:DescribeDBInstances",
"postgres:DescribeDBInstanceAttribute",
"postgres:DescribeDBInstances",
"dcdb:DescribeDCDBInstanceDetail",
"tdmysql:DescribeDBInstanceDetail",
"tbase:DescribeInstanceDetail",
"vpc:DescribeDirectConnectGateway",
"vpc:DescribeVpnGateways",
"cam:GetAccountSummary",
"cam:GetUserPermissionBoundary",
"cam:ListCollaborators",
"cam:GetUser",
"cam:GetPolicy",
"cam:ListAttachedGroupPolicies",
"cam:ListAttachedUserPolicies",
"cam:ListEntitiesForPolicy",
"cam:ListPolicies",
"cam:GetRole",
"cam:GetRolePermissionBoundary",
"cam:ListAttachedRolePolicies"
],
"effect": "allow",
"resource": "*"
}
],
"version": "2.0"
}
```

Networking
Virtual Private Cloud

Last updated：2024-05-20 09:12:58

Service roles and service-linked roles are predefined by Tencent Cloud services and, upon user authorization, the corresponding services can access and use resources by assuming these service-linked roles. This document provides detailed information on the use cases and associated authorization policies of these specific service-linked roles.

Product	Role Name	Role Types	Role Entity
vpc	VPC_QCSLinkedRoleInEipTat	Service-Related Roles	eiptat.vpc.cloud.tencent.com
vpc	VPC_QCSLinkedRoleInSnapshot	Service-Related Roles	snapshot.vpc.cloud.tencent.com
vpc	VPC_QCSLinkedRoleInVpcflowlog	Service-Related Roles	vpcflowlog.vpc.cloud.tencent.com
vpc	VPC_QCSLinkedRoleInPrivateLink	Service-Related Roles	privatelink.vpc.cloud.tencent.com
vpc	VPC_QCSLinkedRoleInFlowLogAdvanceAnalysis	Service-Related Roles	flowlogadvanceanalysis.vpc.cloud.te

VPC_QCSLinkedRoleInEipTat

Use Cases： The current role is the VPC service linked role, which will access your other service resources within the scope of the permissions of the associated policy.

Authorization Polices

- Policy Name： QcloudAccessForVpcLinkedRoleInEipTat
- Policy Information：

```
{
"statement": [
{
"action": [
"tat:DescribeCommands",
"tat:DescribeInvocations",
"tat:DescribeInvocationTasks",
"tat:CreateCommand",
"tat:DeleteCommand",
"tat:InvokeCommand",
"tat:RunCommand"
],
"effect": "allow",
"resource": [
"*"
]
}
],
"version": "2.0"
}
```

VPC_QCSLinkedRoleInSnapshot

Use Cases： The current role is the VPC service linked role, which will access your other service resources within the scope of the permissions of the associated policy.

Authorization Polices

- Policy Name：QcloudAccessForVPCLinkedRoleInSnapshot
- Policy Information：

```
{
"version": "2.0",
"statement": [
{
"effect": "allow",
"action": [
"cos:GetService",
"cos:HeadBucket",
"cos:GetBucket",
"cos:PutBucket",
"cos:ListMultipartUploads",
"cos:GetObject*",
```

```
"cos:HeadObject",
"cos:GetBucketObjectVersions",
"cos:OptionsObject",
"cos:ListParts",
"cos:DeleteObject",
"cos:PostObject",
"cos:PostObjectRestore",
"cos:PutObject*",
"cos:InitiateMultipartUpload",
"cos:UploadPart",
"cos:UploadPartCopy",
"cos:CompleteMultipartUpload",
"cos:AbortMultipartUpload",
"cos:DeleteMultipleObjects",
"cos:AppendObject"
],
"resource": "*"
}
]
}
```

VPC_QCSLinkedRoleInVpcflowlog

Use Cases：The current role is the VPC service linked role, which will access your other service resources within the scope of the permissions of the associated policy.

Authorization Polices

- Policy Name：QcloudAccessForVPCLinkedRoleInVpcflowlog
- Policy Information：

```
{
"version": "2.0",
"statement": [
{
"effect": "allow",
"resource": [
"*"
],
"action": [
"ckafka:DescribeInstances",
"ckafka:DescribeTopic",
"ckafka:DescribeRoute",
"ckafka:DeleteRoute",
```

```
"ckafka:DescribeInstanceAttributes",
"ckafka:DescribeInstancesDetail",
"ckafka:CreateRoute"
]
}
]
}
```

VPC_QCSLinkedRoleInPrivateLink

Use Cases： The current role is the VPC service linked role, which will access your other service resources within the scope of the permissions of the associated policy.

Authorization Polices

- Policy Name：QcloudAccessForVPCLinkedRoleInPrivateLink
- Policy Information：

```
{
"version": "2.0",
"statement": [
{
"action": [
"redis:DescribeInstances",
"cdb:DescribeDBInstances",
"clb:DescribeGatewayLoadBalancers"
],
"resource": "*",
"effect": "allow"
}
]
}
```

VPC_QCSLinkedRoleInFlowLogAdvanceAnalysis

Use Cases： The current role is the VPC service linked role, which will access your other service resources within the scope of the permissions of the associated policy.

Authorization Polices

- Policy Name：QcloudAccessForVPCRoleInFlowLogAdvanceAnalysis
- Policy Information：

```
{
"version": "2.0",
"statement": [
{
"action": [
"cls:DescribeLogsets",
"cls:CreateLogset",
"cls:CreateTopic",
"cls:DescribeTopics",
"cls:DeleteTopic",
"cls:DescribeIndex",
"cls:ModifyIndex",
"cls:CreateIndex",
"cls:DeleteIndex",
"cls:GetDashboard",
"cls:CreateDashboard",
"cls:DeleteDashboard",
"cls:ModifyDashboard",
"cls:ListDashboard",
"cls:pushLog"
],
"resource": "*",
"effect": "allow"
}
]
}
```

Cloud Load Balancer

Last updated：2024-05-20 09:12:38

Service roles and service-linked roles are predefined by Tencent Cloud services and, upon user authorization, the corresponding services can access and use resources by assuming these service-linked roles. This document provides detailed information on the use cases and associated authorization policies of these specific service-linked roles.

Product	Role Name	Role Types	Role Entity
Cloud Loader Balance	CLB_QCSLinkedRoleInUploadCertificate	Service-Related Roles	clb.cloud.tencent.com

CLB_QCSLinkedRoleInUploadCertificate

Use Cases：The current role is the CLB service linked role, which will access your other service resources within the scope of the permissions of the associated policy.

Authorization Polices

- Policy Name：QcloudAccessForCLBLinkedRoleInSSLCert
- Policy Information：

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

CDN and Acceleration
Content Delivery Network

Last updated：2024-05-20 09:12:34

Service roles and service-linked roles are predefined by Tencent Cloud services and, upon user authorization, the corresponding services can access and use resources by assuming these service-linked roles. This document provides detailed information on the use cases and associated authorization policies of these specific service-linked roles.

Product	Role Name	Role Types	Role Entity
CDN	CDN_QCSLinkedRoleInRecordListDNSPod	Service-Related Roles	recordlistdnspod.cdn.cloud.tencent.com

CDN_QCSLinkedRoleInRecordListDNSPod

Use Cases：The current role is the CDN service linked role, which will access your other service resources within the scope of the permissions of the associated policy.

Authorization Polices

- Policy Name：QcloudAccessForCDNLinkedRoleInRecordListDNSPod
- Policy Information：

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

Global Application Acceleration Platform

Last updated：2024-05-20 09:12:44

Service roles and service-linked roles are predefined by Tencent Cloud services and, upon user authorization, the corresponding services can access and use resources by assuming these service-linked roles. This document provides detailed information on the use cases and associated authorization policies of these specific service-linked roles.

Product	Role Name	Role Types	Role Entity
Global Application Acceleration Platform	GAAP_QCSLinkedRoleInCrossBorderCheck	Service-Related Roles	crossbordercheck.gaap.cloud.tence

GAAP_QCSLinkedRoleInCrossBorderCheck

Use Cases：The current role is the GAAP service linked role, which will access your other service resources within the scope of the permissions of the associated policy.

Authorization Polices

- Policy Name：QcloudAccessForGAAPLinkedRoleInCrossBorderCheck
- Policy Information：

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

Network Security
Tencent Cloud Firewall

Last updated：2024-05-20 09:12:37

Service roles and service-linked roles are predefined by Tencent Cloud services and, upon user authorization, the corresponding services can access and use resources by assuming these service-linked roles. This document provides detailed information on the use cases and associated authorization policies of these specific service-linked roles.

Product	Role Name	Role Types	Role Entity
Cloud Firewall	CFW_QCSLinkedRoleInGetiOAaccess	Service-Related Roles	GetiOAaccess.cfw.cloud.tencent.com

CFW_QCSLinkedRoleInGetiOAaccess

Use Cases：The current role is the CFW service linked role, which will access or operate your iOA resources within the scope of the permissions of the associated policy.

Authorization Polices

- Policy Name：QcloudAccessForCFWLinkedRoleInGetiOAaccess
- Policy Information：

```
{
"version": "2.0",
"statement": [
{
"effect": "allow",
"action": [
"ioa:CreateConnectorGroup",
"ioa:CreateConnector",
"ioa:DescribeConnectors",
"ioa:DescribeConnectorDownloadUrl",
"ioa:DeleteConnector",
"ioa:DeleteConnectorGroup",
"ioa:DescribeAccountGroups",
"ioa:DescribeAccountGroup",
"ioa:DescribeLocalAccounts",
"ioa:DescribeLocalAccount",
```

```
"ioa:CreateResourceModule",
"ioa:DeleteResourceModule",
"ioa:DescribeResourceModules",
"ioa:CreateBusinessResource",
"ioa:DeleteBusinessResource",
"ioa:ModifyBusinessResource",
"ioa:BindBusinessResourceConnectorGroup",
"ioa:SaveAccountResources",
"ioa:DeleteAccountResources",
"ioa:SaveAccountGroupResources",
"ioa:DeleteAccountGroupResources"
],
"resource": "*"
}
]
}
```

Tencent Cloud EdgeOne

Last updated：2024-05-20 09:12:55

Service roles and service-linked roles are predefined by Tencent Cloud services and, upon user authorization, the corresponding services can access and use resources by assuming these service-linked roles. This document provides detailed information on the use cases and associated authorization policies of these specific service-linked roles.

Product	Role Name	Role Types	Role Entity
Tencent Cloud EdgeOne	TEO_QCSLinkedRoleInCertlist	Service-Related Roles	certlist.teo.cloud.tencent.com
Tencent Cloud EdgeOne	TEO_QCSLinkedRoleInUpstreamgw	Service-Related Roles	upstreamgw.teo.cloud.tencent.com
Tencent Cloud EdgeOne	TEO_QCSLinkedRoleInRealTimeLogCLS	Service-Related Roles	realtimelogcls.teo.cloud.tencent.com

TEO_QCSLinkedRoleInCertlist

Use Cases：The current role is the TEO service linked role, which will access your other service resources within the scope of the permissions of the associated policy.

Authorization Polices

- Policy Name：QcloudAccessForTEOLinkedRoleInCertlist
- Policy Information：

```
{
"version": "2.0",
"statement": [
{
"effect": "allow",
"resource": [
"*"
],
"action": [
"ssl:DescribeCertificate",
```

```
"ssl:DescribeCertificateDetail",
"ssl:DescribeCertificates",
"ssl:DownloadCertificate",
"ssl:ModifyCertificateAlias",
"ssl:UploadCertificate"
]
}
]
}
```

TEO_QCSLinkedRoleInUpstreamgw

Use Cases：The current role is the teo service linked role, which will access your other service resources within the scope of the permissions of the associated policy.

Authorization Polices

- Policy Name：QcloudAccessForTEOLinkedRoleInUpstreamgw
- Policy Information：

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

TEO_QCSLinkedRoleInRealTimeLogCLS

Use Cases：The current role is the TEO service linked role, which will access your other service resources within the scope of the permissions of the associated policy.

Authorization Polices

- Policy Name：QcloudAccessForTEORealTimeLogCLS
- Policy Information：

```
{
"version": "2.0",
"statement": [
{
"action": [
"cls:pushLog",
"cls:searchLog",
"cls:listLogset",
"cls:getLogset",
"cls:listTopic",
"cls:getTopic",
"cls:createTopic",
"cls:modifyTopic",
"cls:deleteTopic",
"cls:createLogset",
"cls:modifyLogset",
"cls:deleteLogset",
"cls:downloadLog",
"cls:getIndex",
"cls:modifyIndex",
"cls:CreateIndex"
],
"resource": "*",
"effect": "allow"
}
]
}
```

Application Security
Web Application Firewall

Last updated：2024-05-20 09:12:58

Service roles and service-linked roles are predefined by Tencent Cloud services and, upon user authorization, the corresponding services can access and use resources by assuming these service-linked roles. This document provides detailed information on the use cases and associated authorization policies of these specific service-linked roles.

Product	Role Name	Role Types	Role Entity
cloudWaf	WAF_QCSLinkedRoleInCLS	Service-Related Roles	cls.waf.cloud.tencent.com
cloudWaf	WAF_QCSLinkedRoleInAccess	Service-Related Roles	access.waf.cloud.tencent.com
cloudWaf	WAF_QCSLinkedRoleInCKafka	Service-Related Roles	ckafka.waf.cloud.tencent.com

WAF_QCSLinkedRoleInCLS

Use Cases：The current role is the WAF service linked role, which will access your other service resources within the scope of the permissions of the associated policy.

Authorization Polices

- Policy Name：QcloudAccessForWAFLinkedRoleInCLS
- Policy Information：

```
{
"version": "2.0",
"statement": [
{
"action": [
"cls:getLogset",
"cls:listLogset",
"cls:getTopic",
"cls:listTopic",
"cls:UploadLog",
"cls:SearchLog",
"cls:searchLog",
"cls:pushLog",
"cls:pullLogs",
"cls:GetLog",
```

```
"cls:CreateLogset",
"cls:createLogset",
"cls:CreateTopic",
"cls:createTopic",
"cls:CreateIndex",
"cls:ModifyIndex",
"cls:modifyIndex",
"cls:DescribeIndex",
"monitor:GetMonitorData"
],
"resource": "*",
"effect": "allow"
}
]
}
```

WAF_QCSLinkedRoleInAccess

Use Cases：The current role is the WAF service linked role, which will access your other service resources within the scope of the permissions of the associated policy.

Authorization Polices

- Policy Name：QcloudAccessForWAFLinkedRoleInAccess
- Policy Information：

```
{
"version": "2.0",
"statement": [
{
"effect": "allow",
"action": [
"dnspod:*",
"ssl:*",
"clb:*",
"vpc:DescribeAddress",
"vpc:CreateAddress",
"cvm:DescribeSecurityGroups",
"cvm:CreateSecurityGroupPolicy",
"cvm:CreateSecurityGroup",
"cvm:DescribeSecurityGroupPolicys",
"cvm:DescribeInstances",
"cvm:AssociateSecurityGroups",
"cvm:ModifyInstancesAttribute"
```

```
],
"resource": [
"*"
]
}
]
}
```

WAF_QCSLinkedRoleInCKafka

Use Cases： The current role is the WAF service linked role, which will access your other service resources within the scope of the permissions of the associated policy.

Authorization Polices

- Policy Name：QcloudAccessForWAFLinkedRoleInCKafka
- Policy Information：

```
{
"version": "2.0",
"statement": [
{
"effect": "allow",
"resource": [
"*"
],
"action": [
"ckafka:DescribeInstanceAttributes",
"ckafka:DescribeTopicAttributes",
"ckafka:DescribeUser",
"ckafka:GetInstanceAttributes",
"ckafka:GetTopicAttributes",
"ckafka:DescribeTopicDetail",
"ckafka:GetInstanceAttributes",
"ckafka:GetTopicAttributes",
"ckafka:DescribeInstances",
"ckafka:DescribeInstancesDetail",
"ckafka:DescribeRoute",
"ckafka:DescribeTopic",
"ckafka:ListRoute",
"ckafka:ListTopic",
"monitor:GetMonitorData"
]
}
```

```
]
}
```

Domains & Websites
SSL Certificate Service

Last updated：2024-05-20 09:12:51

Service roles and service-linked roles are predefined by Tencent Cloud services and, upon user authorization, the corresponding services can access and use resources by assuming these service-linked roles. This document provides detailed information on the use cases and associated authorization policies of these specific service-linked roles.

Product	Role Name	Role Types	Role Entity
SSL Certification	SSL_QCSLinkedRoleInCertificateWaf	Service-Related Roles	certificatewaf.ssl.cloud.tence
SSL Certification	SSL_QCSLinkedRoleInCertificateDependence	Service-Related Roles	certificatedependence.ssl.clo
SSL Certification	SSL_QCSLinkedRoleInReplaceLoadCertificate	Service-Related Roles	replaceloadcertificate.ssl.clou
SSL Certification	SSL_QCSLinkedRoleInCertificateCloudMonitor	Service-Related Roles	certificatecloudmonitor.ssl.cl
SSL Certification	SSL_QCSLinkedRoleInDescribeDeployedResources	Service-Related Roles	describedeployedresources.s

SSL_QCSLinkedRoleInCertificateWaf

Use Cases： The current role is the SSL service linked role, which will access your other service resources within the scope of the permissions of the associated policy.

Authorization Polices

- Policy Name： QcloudAccessForSSLLinkedRoleInCertificateWaf
- Policy Information：

```
{
"version": "2.0",
"statement": [
{
"effect": "allow",
"action": [
"waf:DescribeSpartaProtectionList",
"waf:DescribeSpartaProtectionInfo",
"waf:DescribeUserInstances",
"waf:DescribeUserQPS",
"waf:DescribePeakPoints",
"waf:AddSpartaProtection",
"waf:DeleteSpartaProtection",
"waf:ModifySpartaProtection",
"waf:ModifyProtectionStatus",
"waf:DescribeDomains"
],
"resource": [
"*"
]
}
]
}
```

SSL_QCSLinkedRoleInCertificateDependence

Use Cases：The current role is the SSL service linked role, which will access your other service resources within the scope of the permissions of the associated policy.

Authorization Polices

- Policy Name：QcloudAccessForSSLLinkedRoleInCertificateDependence
- Policy Information：

```
{
"statement": [
{
"action": [
"dnspod:CreateRecord",
"dnspod:DescribeDomain",
"dnspod:CreateDomain",
"dnspod:DescribeRecordList",
"dnspod:DeleteRecord",
```

```
"dnspod:DescribeDomain",
"dnspod:ModifyRecordStatus"
],
"effect": "allow",
"resource": "*"
}
],
"version": "2.0"
}
```

SSL_QCSLinkedRoleInReplaceLoadCertificate

Use Cases：The current role is the SSL service linked role, which will access your other service resources within the scope of the permissions of the associated policy.

Authorization Polices

- Policy Name：QcloudAccessForSSLLinkedRoleInReplaceLoadCertificate
- Policy Information：

```
{
"version": "2.0",
"statement": [
{
"effect": "allow",
"action": [
"clb:ReplaceCertForLoadBalancers",
"waf:DescribeCertificatedDomain",
"waf:ModifyCertificatedDomain",
"live:DescribeLiveDomainsByCerts",
"live:ModifyLiveDomainCertBindings",
"antiddos:DescribeL7RulesBySSLCertId",
"antiddos:CreateL7RuleCerts",
"clb:DescribeLoadBalancerListByCertId",
"clb:DescribeLoadBalancers",
"clb:DescribeListeners",
"clb:ModifyListener",
"clb:ModifyDomainAttributes",
"clb:DescribeTaskStatus",
"cos:GetBucketDomain",
"cos:GetBucketDomainCertificate",
"cos:GetService",
"cos:PutBucketDomainCertificate",
"tke:DescribeClusters",
```

```
"tke:AcquireClusterAdminRole",
"tke:AcquireEKSClusterAdminRole",
"lighthouse:DescribeSupportHttpsInstances",
"lighthouse:InstallCertificate",
"lighthouse:DescribeInstallCertificateTasks",
"vod:DescribeVodDomainsByCertIds",
"vod:ModifyVodDomainCertBindings",
"vod:UpdateCertForVodDomains",
"clb:DescribeLoadBalancerCount",
"teo:ModifyHostsCertificateByHosts",
"teo:DescribeHostsByCertID",
"tcb:DescribeEnvs",
"tcb:DescribeCloudBaseGWService",
"tcb:DescribeHostingDomain",
"tcb:BindCloudBaseAccessDomain",
"tcb:CreateHostingDomain",
"tcb:ModifyCloudBaseAccessDomain",
"tcb:ModifyHostingDomain",
"tse:ModifyCloudNativeAPIGatewayCertificate",
"tse:DescribeCloudNativeAPIGatewayCertificates",
"tse:DescribeCloudNativeAPIGateways",
"cdn:DescribeCdnDomainsByCerts",
"cdn:UpdateDomainHttps"
],
"resource": [
"*"
]
}
]
}
```

SSL_QCSLinkedRoleInCertificateCloudMonitor

Use Cases： The current role is the SSL service linked role, which will access your other service resources within the scope of the permissions of the associated policy.

Authorization Polices

- Policy Name：QcloudAccessForSSLLinkedRoleInCertificateCloudMonitor
- Policy Information：

```
{
"version": "2.0",
"statement": [
```

```
{
"effect": "allow",
"resource": [
"*"
],
"action": [
"monitor:CreateAlarmPolicy",
"monitor:DeleteAlarmPolicy",
"monitor:DescribeAlarmPolicies",
"monitor:ModifyAlarmPolicyStatus",
"monitor:BindingPolicyObject",
"monitor:UnBindingPolicyObject",
"monitor:ModifyAlarmPolicyNotice",
"monitor:CreateAlarmNotice",
"monitor:DeleteAlarmNotices",
"monitor:ModifyAlarmNotice",
"monitor:DescribeAlarmNotices",
"monitor:UnBindingAllPolicyObject"
]
}
]
}
```

SSL_QCSLinkedRoleInDescribeDeployedResources

Use Cases： The current role is the SSL service linked role, which will access your other service resources within the scope of the permissions of the associated policy.

Authorization Polices

- Policy Name：QcloudAccessForSSLLinkedRoleInDescribeDeployedResources
- Policy Information：

```
{
"version": "2.0",
"statement": [
{
"effect": "allow",
"action": [
"clb:ReplaceCertForLoadBalancers",
"waf:DescribeCertificatedDomain",
"waf:ModifyCertificatedDomain",
"live:DescribeLiveDomainsByCerts",
"live:ModifyLiveDomainCertBindings",
```

```
"antiddos:DescribeL7RulesBySSLCertId",
"antiddos:CreateL7RuleCerts",
"clb:DescribeLoadBalancerListByCertId",
"cdn:UpdateDomainsCertificate",
"teo:DescribeHostsByCertID",
"teo:ModifyHostsCertificateByHosts"
],
"resource": [
"*"
]
}
]
}
```

Private DNS

Last updated：2024-05-20 09:12:50

Service roles and service-linked roles are predefined by Tencent Cloud services and, upon user authorization, the corresponding services can access and use resources by assuming these service-linked roles. This document provides detailed information on the use cases and associated authorization policies of these specific service-linked roles.

Product	Role Name	Role Types	Role Entity
Private DNS	PrivateDNS_QCSLinkedRoleInPL	Service-Related Roles	privatedns.cloud.tencent.com
Private DNS	PrivateDNS_QCSLinkedRoleInCls	Service-Related Roles	privatedns.qcloud.com

PrivateDNS_QCSLinkedRoleInPL

Use Cases：The current role is the privatedns service linked role, which will access your other service resources within the scope of the permissions of the associated policy.

Authorization Polices

- Policy Name：QcloudAccessForPrivateDNSLinkedRoleInPL
- Policy Information：

```
{
"statement": [
{
"action": [
"vpc:CreateVpcEndPoint",
"vpc:DeleteVpcEndPoint",
"vpc:CreateVpcEndPointService",
"vpc:DeleteVpcEndPointService",
"vpc:CreateVpcEndPointServiceWhiteList",
"vpc:DeleteVpcEndPointServiceWhiteList",
"vpc:DescribeVpcEndPointService",
"clb:DescribeLoadBalancers",
"clb:DescribeLoadBalancersDetail",
"clb:DescribeListeners",
"clb:DescribeTargets"
],
"effect": "allow",
"resource": "*"
}
```

```
],
"version": "2.0"
}
```

PrivateDNS_QCSLinkedRoleInCls

Use Cases： The current role is the privatedns service linked role, which will access your other service resources within the scope of the permissions of the associated policy.

Authorization Polices

- Policy Name：QcloudAccessForPrivateDNSLinkedRoleInCLS
- Policy Information：

```
{
"version": "2.0",
"statement": [
{
"effect": "allow",
"action": [
"cls:DescribeConfigs",
"cls:DescribeDashboards",
"cls:DescribeTopics",
"cls:GetChart",
"cls:GetClsService",
"cls:GetDashboard",
"cls:getCursor",
"cls:getIndex",
"cls:getLogset",
"cls:getTopic",
"cls:searchLog",
"cls:CreateChart",
"cls:CreateDashboard",
"cls:CreateIndex",
"cls:ModifyDashboard",
"cls:createLogset",
"cls:createTopic",
"cls:downloadLog",
"cls:pushLog",
"cls:DescribeLogsets",
"cls:ListChart",
"cls:ListDashboard",
"cls:listLogset",
"cls:listTopic",
```

```
"cls:DescribeAgentConfigs"
],
"resource": [
"*"
]
}
]
}
```

HTTPDNS

Last updated：2024-05-20 09:12:45

Service roles and service-linked roles are predefined by Tencent Cloud services and, upon user authorization, the corresponding services can access and use resources by assuming these service-linked roles. This document provides detailed information on the use cases and associated authorization policies of these specific service-linked roles.

Product	Role Name	Role Types	Role Entity
HTTPDNS	HTTPDNS_QCSLinkedRoleInCustomdns	Service-Related Roles	customdns.httpdns.cloud.tencent.com

HTTPDNS_QCSLinkedRoleInCustomdns

Use Cases：The current role is the HTTPDNS service linked role, which will access your other service resources within the scope of the permissions of the associated policy.

Authorization Polices

- Policy Name：QcloudAccessForHTTPDNSLinkedRoleInCustomdns
- Policy Information：

```
{
"version": "2.0",
"statement": [
{
"effect": "allow",
"resource": [
"*"
],
"action": [
"scf:GetFunction",
"scf:GetAlias",
"scf:ListFunctions",
"scf:CreateNamespace",
"scf:ListNamespaces",
"scf:InvokeFunction",
"scf:ListVersionByFunction",
"scf:ListAliases"
```

```
]
}
]
}
```

Big Data
Elastic MapReduce

Last updated：2024-05-20 09:12:43

Service roles and service-linked roles are predefined by Tencent Cloud services and, upon user authorization, the corresponding services can access and use resources by assuming these service-linked roles. This document provides detailed information on the use cases and associated authorization policies of these specific service-linked roles.

Product	Role Name	Role Types	Role Entity
Elasticsearch MapReduce	EMR_QCSLinkedRoleInApplicationDataAccess	Service-Related Roles	applicationdataaccess.emr.cloud

EMR_QCSLinkedRoleInApplicationDataAccess

Use Cases：The current role is the EMR service linked role, which will access your other service resources within the scope of the permissions of the associated policy.

Authorization Polices

- Policy Name：QcloudAccessForEMRLinkedRoleInApplicationDataAccess
- Policy Information：

```
{
"version": "2.0",
"statement": [
{
"action": [
"cos:GetService",
"cos:GetBucket",
"cos:ListMultipartUploads",
"cos:GetObject",
"cos:HeadObject",
"cos:OptionsObject",
"cos:ListParts",
"cos:DeleteObject",
"cos:PostObject",
"cos:PutObject",
```

```
"cos:InitiateMultipartUpload",
"cos:UploadPart",
"cos:UploadPartCopy",
"cos:CompleteMultipartUpload",
"cos:AbortMultipartUpload",
"cos:AppendObject",
"cos:HeadBucket",
"cos:RenameObject",
"cos:TruncateObject",
"cos:PutSymlink",
"cos:GetSymlink"
],
"resource": "*",
"effect": "allow"
}
]
}
```

Elasticsearch Service

Last updated：2024-05-20 09:12:43

Service roles and service-linked roles are predefined by Tencent Cloud services and, upon user authorization, the corresponding services can access and use resources by assuming these service-linked roles. This document provides detailed information on the use cases and associated authorization policies of these specific service-linked roles.

Product	Role Name	Role Types	Role Entity
Elasticsearch Service	ES_QCSLinkedRoleInAccessCos	Service-Related Roles	acesscos.es.cloud.tencent.com
Elasticsearch Service	ES_QCSLinkedRoleInDataImport	Service-Related Roles	dataimport.es.cloud.tencent.com
Elasticsearch Service	ES_QCSLinkedRoleInVpcOperate	Service-Related Roles	vpcoperate.es.cloud.tencent.com
Elasticsearch Service	ES_QCSLinkedRoleInBeatsCollector	Service-Related Roles	beatscollector.es.cloud.tencent.com

ES_QCSLinkedRoleInAccessCos

Use Cases：The current role is the ES service linked role, which will access your other service resources within the scope of the permissions of the associated policy.

Authorization Polices

- Policy Name：QcloudAccessForEsLinkedRoleInCosAcess
- Policy Information：

```
{
"statement": [
{
"action": [
"cos:GetBucket",
"cos:HeadBucket",
```

```
"cos:GetObject",
"cos:HeadObject",
"cos:PutObject",
"cos:PostObject",
"cos:InitiateMultipartUpload",
"cos:ListMultipartUploads",
"cos:ListParts",
"cos:UploadPart",
"cos:CompleteMultipartUpload",
"cos:DeleteObject",
"cos:DeleteMultipleObjects"
],
"effect": "allow",
"resource": "*"
}
],
"version": "2.0"
}
```

ES_QCSLinkedRoleInDataImport

Use Cases：The current role is the ES service linked role, which will access your other service resources within the scope of the permissions of the associated policy

Authorization Polices

- Policy Name：QcloudAccessForESLinkedRoleInDataImport
- Policy Information：

```
{
"version": "2.0",
"statement": [
{
"action": [
"ckafka:DescribeInstancesDetail",
"ckafka:DescribeInstances",
"ckafka:CreateTopic",
"ckafka:DescribeTopicDetail",
"ckafka:DescribeTopic",
"ckafka:DescribeRoute",
"ckafka:CreateDatahubTopic",
"ckafka:DescribeDatahubTopic",
"ckafka:CreateConnectResource",
"ckafka:DescribeConnectResource",
```

```
"ckafka:CreateDatahubTask",
"ckafka:DescribeDatahubTask",
"tat:RunCommand",
"tat:DescribeInvocations",
"tat:DescribeAutomationAgentStatus",
"tke:DescribeClusters",
"tke:DescribeClusterReleases",
"tke:CreateClusterRelease",
"tke:UpgradeClusterRelease",
"tke:UninstallClusterRelease",
"tke:CancelClusterRelease",
"ckafka:DeleteDatahubTopic",
"ckafka:DeleteConnectResource",
"ckafka:DeleteDatahubTask",
"ckafka:DeleteDatahubGroup",
"ckafka:ModifyGroupOffsets",
"ckafka:ModifyDatahubResource",
"cvm:DescribeInstances",
"emr:DescribeClusterLogInfo",
"emr:NotifyEmr"
],
"resource": "*",
"effect": "allow"
}
]
}
```

ES_QCSLinkedRoleInVpcOperate

Use Cases： The current role is the ES service linked role, which will access your other service resources within the scope of the permissions of the associated policy.

Authorization Polices

- Policy Name：QcloudAccessForESLinkedRoleInVpcOperate
- Policy Information：

```
{
"version": "1.0",
"statement": [
{
"action": [
"vpc:DescribeVpcEx",
"vpc:DescribeSubnetEx",
```

```
"vpc:CreateCcn",
"vpc:AttachCcnInstances",
"vpc:DeleteCcn",
"vpc:DetachCcnInstances",
"vpc:DescribeNetworkInterfaces",
"vpc:CreateNetworkInterface",
"vpc:DeleteNetworkInterface",
"vpc:DescribeVpcTaskResult",
"vpc:CreateVpcEndPoint",
"vpc:DescribeVpcEndPoint",
"vpc:ModifyVpcEndPointAttribute",
"vpc:DeleteVpcEndPoint",
"vpc:DisassociateVpcEndPointSecurityGroups",
"cvm:DescribeSecurityGroups"
],
"resource": "*",
"effect": "allow"
}
]
}
```

ES_QCSLinkedRoleInBeatsCollector

Use Cases： The current role is the ES service linked role, which will access your other service resources within the scope of the permissions of the associated policy.

Authorization Polices

- Policy Name：QcloudAccessForESLinkedRoleInBeatsCollector
- Policy Information：

```
{
"version": "2.0",
"statement": [
{
"effect": "allow",
"action": [
"tat:RunCommand",
"tat:DescribeInvocations",
"tat:DescribeAutomationAgentStatus",
"tke:DescribeClusters",
"tke:DescribeClusterReleases",
"tke:CreateClusterRelease",
"tke:UpgradeClusterRelease",
```

```
"tke:UninstallClusterRelease",
"tke:CancelClusterRelease",
"cvm:DescribeInstances",
"emr:DescribeClusterLogInfo",
"emr:NotifyEmr"
],
"resource": [
"*"
]
}
]
}
```

Cloud Data Warehouse

Last updated：2024-05-20 09:12:35

Service roles and service-linked roles are predefined by Tencent Cloud services and, upon user authorization, the corresponding services can access and use resources by assuming these service-linked roles. This document provides detailed information on the use cases and associated authorization policies of these specific service-linked roles.

Product	Role Name	Role Types	Role Entity
Cloud Data Warehouse ClickHouse	CDWCH_QCSLinkedRoleInCKCOS	Service-Related Roles	ckcos.cdwch.cloud.tencent.com
Cloud Data Warehouse ClickHouse	CDWCH_QCSLinkedRoleInCKLOGSHOW	Service-Related Roles	cklogshow.cdwch.cloud.tencent.com

CDWCH_QCSLinkedRoleInCKCOS

Use Cases：The current role is the CDWCH service linked role, which will access your other service resources within the scope of the permissions of the associated policy.

Authorization Polices

- Policy Name：QcloudAccessForCDWCHLinkedRoleInCKCOS
- Policy Information：

```
{
"version": "2.0",
"statement": [
{
"effect": "allow",
"action": [
"cos:AbortMultipartUpload",
"cos:GetBucket",
"cos:GetBucketACL",
"cos:GetBucketAccelerate",
"cos:GetBucketCORS",
"cos:GetBucketDomain",
"cos:GetBucketEncryption",
```

```
"cos:GetBucketIntelligentTiering",
"cos:GetBucketInventory",
"cos:GetBucketLifecycle",
"cos:GetBucketLocation",
"cos:GetBucketLogging",
"cos:GetBucketNotification",
"cos:GetBucketObjectVersions",
"cos:GetBucketOrigin",
"cos:GetBucketPolicy",
"cos:GetBucketReferer",
"cos:GetBucketReplication",
"cos:GetBucketTagging",
"cos:GetBucketVersionAcl",
"cos:GetBucketVersioning",
"cos:GetBucketWebsite",
"cos:GetObject",
"cos:GetObjectACL",
"cos:GetObjectTagging",
"cos:GetObjectVersionAcl",
"cos:GetService",
"cos:HeadBucket",
"cos:HeadObject",
"cos:ListMultipartUploads",
"cos:ListParts",
"cos:OptionsObject",
"cos:AppendObject",
"cos:CompleteMultipartUpload",
"cos:InitiateMultipartUpload",
"cos:PostObject",
"cos:PostObjectRestore",
"cos:PutBucket",
"cos:PutBucketEncryption",
"cos:PutBucketIntelligentTiering",
"cos:PutBucketInventory",
"cos:PutBucketLifecycle",
"cos:PutBucketLogging",
"cos:PutBucketReplication",
"cos:PutBucketVersioning",
"cos:PutObject",
"cos:PutObjectCopy",
"cos:PutObjectTagging",
"cos:UploadPart",
"cos:UploadPartCopy",
"cos:DeleteMultipleObjects",
"cos:DeleteObject",
"cos:GetVodPlayList",
"cos:DeleteObjectTagging"
```

```
],
"resource": [
"*"
]
}
]
}
```

CDWCH_QCSLinkedRoleInCKLOGSHOW

Use Cases： The current role is the CDWCH service linked role, which will access your other service resources within the scope of the permissions of the associated policy.

Authorization Polices

- Policy Name：QcloudAccessForCDWCHLinkedRoleInCKLOGSHOW
- Policy Information：

```
{
"version": "2.0",
"statement": [
{
"effect": "allow",
"action": [
"cls:DescribeConfigs",
"cls:DescribeIndex",
"cls:DescribeMachines",
"cls:GetAccount",
"cls:DescribeTopics",
"cls:GetLog",
"cls:SearchLog",
"cls:getConfig",
"cls:getConsumerGroupCursor",
"cls:getCursor",
"cls:getIndex",
"cls:getLogset",
"cls:getMachineGroup",
"cls:getMachineStatus",
"cls:getShipper",
"cls:getTopic",
"cls:searchLog",
"cls:ShowContext",
"cls:ApplyConfigToMachineGroup",
"cls:CreateConfig",
```

```
"cls:CreateIndex",
"cls:CreateLogset",
"cls:CreateMachineGroup",
"cls:CreateTopic",
"cls:DeleteIndex",
"cls:DeleteConfig",
"cls:DeleteMachineGroup",
"cls:ModifyIndex",
"cls:ModifyMachineGroup",
"cls:createLogset",
"cls:createMachineGroup",
"cls:createShipper",
"cls:createTopic",
"cls:modifyIndex",
"cls:modifyLogset",
"cls:modifyMachineGroup",
"cls:modifyShipper",
"cls:modifyTopic",
"cls:pushLog",
"cls:deleteMachineGroup",
"cls:deleteShipper",
"cls:DescribeAgentConfigs",
"cls:DescribeLogsets",
"cls:listLogset",
"cls:listMachineGroup",
"cls:listShipper",
"cls:listTopic",
"cls:agentHeartBeat",
"cls:DescribeMachineGroups",
"tag:TagResources"
],
"resource": [
"*"
]
}
]
}
```

Cloud Data Warehouse for PostgreSQL

Last updated：2024-05-20 09:12:36

Service roles and service-linked roles are predefined by Tencent Cloud services and, upon user authorization, the corresponding services can access and use resources by assuming these service-linked roles. This document provides detailed information on the use cases and associated authorization policies of these specific service-linked roles.

Product	Role Name	Role Types	Role Entity
Cloud Data Warehouse PostgreSQL	CDWPG_QCSLinkedRoleInPGCOS	Service-Related Roles	pgcos.cdwpg.cloud.tencent.com
Cloud Data Warehouse PostgreSQL	CDWPG_QCSLinkedRoleInPGKMS	Service-Related Roles	pgkms.cdwpg.cloud.tencent.com

CDWPG_QCSLinkedRoleInPGCOS

Use Cases：The current role is the CDWPG service linked role, which will access your other service resources within the scope of the permissions of the associated policy.

Authorization Polices

- Policy Name：QcloudAccessForCDWPGLinkedRoleInPGCOS
- Policy Information：

```
{
"version": "2.0",
"statement": [
{
"effect": "allow",
"action": [
"cos:AbortMultipartUpload",
"cos:GetBucket",
"cos:GetBucketACL",
"cos:GetBucketAccelerate",
"cos:GetBucketCORS",
"cos:GetBucketDomain",
"cos:GetBucketEncryption",
```

```
"cos:GetBucketIntelligentTiering",
"cos:GetBucketInventory",
"cos:GetBucketLifecycle",
"cos:GetBucketLocation",
"cos:GetBucketLogging",
"cos:GetBucketNotification",
"cos:GetBucketObjectVersions",
"cos:GetBucketOrigin",
"cos:GetBucketPolicy",
"cos:GetBucketReferer",
"cos:GetBucketReplication",
"cos:GetBucketTagging",
"cos:GetBucketVersionAcl",
"cos:GetBucketVersioning",
"cos:GetBucketWebsite",
"cos:GetObject",
"cos:GetObjectACL",
"cos:DeleteObject",
"cos:DeleteMultipleObjects",
"cos:GetObjectTagging",
"cos:GetObjectVersionAcl",
"cos:GetService",
"cos:HeadBucket",
"cos:HeadObject",
"cos:ListMultipartUploads",
"cos:ListParts",
"cos:OptionsObject",
"cos:AppendObject",
"cos:CompleteMultipartUpload",
"cos:InitiateMultipartUpload",
"cos:PostObject",
"cos:PostObjectRestore",
"cos:PutBucket",
"cos:PutBucketEncryption",
"cos:PutBucketIntelligentTiering",
"cos:PutBucketInventory",
"cos:PutBucketLifecycle",
"cos:PutBucketLogging",
"cos:PutBucketReplication",
"cos:PutBucketVersioning",
"cos:PutObject",
"cos:PutObjectCopy",
"cos:PutObjectTagging",
"cos:UploadPart",
"cos:UploadPartCopy",
"chdfs:DescribeMountPoint",
"chdfs:DescribeFileSystem",
```

```
"chdfs:DescribeAccessGroups",
"chdfs:DescribeAccessRules",
"chdfs:ModifyFileSystem",
"chdfs:ModifyAccessRules",
"chdfs:CreateAccessGroup",
"chdfs:CreateAccessRules",
"chdfs:AssociateAccessGroups",
"chdfs:DisassociateAccessGroups",
"chdfs:DeleteAccessGroup",
"chdfs:DeleteAccessRules",
"chdfs:DescribeFileSystems",
"chdfs:DescribeMountPoints"
],
"resource": [
"*"
]
}
]
}
```

CDWPG_QCSLinkedRoleInPGKMS

Use Cases：The current role is the CDWPG service linked role, which will access your other service resources within the scope of the permissions of the associated policy.

Authorization Polices

- Policy Name：QcloudAccessForCDWPGLinkedRoleInPGKMS
- Policy Information：

```
{
"version": "2.0",
"statement": [
{
"action": [
"kms:ListKeyDetail",
"kms:CreateKey",
"kms:GenerateDataKey",
"kms:Decrypt",
"kms:BindCloudResource",
"kms:UnbindCloudResource"
],
"resource": "*",
"effect": "allow"
```

```
}
]
}
```

Data Lake Compute

Last updated：2024-05-20 09:12:42

Service roles and service-linked roles are predefined by Tencent Cloud services and, upon user authorization, the corresponding services can access and use resources by assuming these service-linked roles. This document provides detailed information on the use cases and associated authorization policies of these specific service-linked roles.

Product	Role Name	Role Types	Role Entity
Data Lake Compute	DLC_QCSLinkedRoleInCheckDLCResource	Service-Related Roles	checkdlcresource.dlc.cloud.tencent.com

DLC_QCSLinkedRoleInCheckDLCResource

Use Cases：The current role is the DLC service role, which will access your other service resources within the scope of the permissions of the associated policy.

Authorization Polices

- Policy Name：QcloudAccessForDLCLinkedRoleInCheckDLCResource
- Policy Information：

```
{
"version": "2.0",
"statement": [
{
"effect": "allow",
"action": [
"cos:GetService",
"cos:GetBucket",
"cos:ListMultipartUploads",
"cos:GetObject*",
"cos:HeadObject",
"cos:GetBucketObjectVersions",
"cos:OptionsObject",
"cos:ListParts",
"cos:DeleteObject",
"cos:PostObject",
"cos:PostObjectRestore",
```

```
"cos:PutObject*",
"cos:InitiateMultipartUpload",
"cos:UploadPart",
"cos:UploadPartCopy",
"cos:CompleteMultipartUpload",
"cos:AbortMultipartUpload",
"cos:DeleteMultipleObjects",
"cos:AppendObject",
"cos:HeadBucket",
"vpc:DescribeRouteTable",
"vpc:CreateRoute",
"vpc:AcceptVpcPeeringConnection",
"vpc:CreateVpcPeeringConnectionEx",
"vpc:CreateVpcPeeringConnection",
"vpc:DeleteVpcPeeringConnection",
"vpc:DeleteVpcPeeringConnectionEx",
"vpc:AcceptVpcPeeringConnectionEx",
"vpc:DescribeVpcPeeringConnections",
"cloudaudit:DescribeEvents",
"cos:GetBucket*",
"cos:PutBucket*",
"cos:DeleteBucket*",
"cos:RenameObject",
"monitor:GetMonitorData",
"chdfs:DescribeMountPoint",
"chdfs:DescribeFileSystem",
"chdfs:DescribeAccessGroups",
"chdfs:DescribeAccessRules",
"chdfs:ModifyFileSystem",
"chdfs:ModifyAccessRules",
"chdfs:CreateAccessGroup",
"chdfs:CreateAccessRules",
"chdfs:AssociateAccessGroups",
"chdfs:DisassociateAccessGroups",
"chdfs:DeleteAccessGroup",
"chdfs:DeleteAccessRules",
"vpc:DescribeAssistantCidr",
"vpc:DescribeVpcEx",
"chdfs:DescribeMountPoints",
"oceanus:DescribeWorkSpaces",
"oceanus:DescribeClusters",
"oceanus:DescribeCHDFSAccessGroups",
"oceanus:CreateCHDFSAccessGroup",
"vpc:DescribeVpcEndPoint",
"vpc:CreateVpcEndPoint",
"vpc:DeleteVpcEndPoint"
],
```

```
"resource": "*"
}
]
}
```

Middleware
Message Queue CKafka

Last updated：2024-05-20 09:12:58

Service roles and service-linked roles are predefined by Tencent Cloud services and, upon user authorization, the corresponding services can access and use resources by assuming these service-linked roles. This document provides detailed information on the use cases and associated authorization policies of these specific service-linked roles.

Product	Role Name	Role Types	Role Entity
CKafka	cosCkafka_QCSRole	Service Role	ckafka.qcloud.com

cosCkafka_QCSRole

Use Cases：

Authorization Polices

- Policy Name： QcloudCOSAccessForCkafkaRole
- Policy Information：

```
{
"version": "2.0",
"statement": [
{
"action": [
"cos:PutObject",
"cos:GetObject",
"cos:DeleteObject",
"cos:ListParts",
"cos:UploadPart"
],
"resource": "*",
"effect": "allow"
}
]
}
```

TDMQ for RocketMQ

Last updated：2024-05-20 09:12:56

Service roles and service-linked roles are predefined by Tencent Cloud services and, upon user authorization, the corresponding services can access and use resources by assuming these service-linked roles. This document provides detailed information on the use cases and associated authorization policies of these specific service-linked roles.

Product	Role Name	Role Types	Role Entity
RocketMQ	RocketMQ_QCSLinkedRoleInSendSSLcertificate	Service-Related Roles	sendSSLcertificate.rocketmq.clou

RocketMQ_QCSLinkedRoleInSendSSLcertificate

Use Cases：This role is to obtain the the SSL certificate maintained in Tencent Cloud and distributing it to the server of the message queue. The current role is the CAM service linked role, which will access your other service resources within the scope of the permissions of the associated policy.

Authorization Polices

- Policy Name：QcloudAccessForRocketMQLinkedRoleInSendSSLcertificate
- Policy Information：

```
{
"version": "2.0",
"statement": [
{
"effect": "allow",
"action": [
"ssl:DescribeCertificateDetail",
"ssl:DescribeCertificates",
"ssl:UploadCertificate"
],
"resource": "*"
}
]
}
```

Interactive Video Services
Tencent Real-Time Communication

Last updated：2024-05-20 09:12:57

Service roles and service-linked roles are predefined by Tencent Cloud services and, upon user authorization, the corresponding services can access and use resources by assuming these service-linked roles. This document provides detailed information on the use cases and associated authorization policies of these specific service-linked roles.

Product	Role Name	Role Types	Role Entity
Tencent Real-Time Communication	TRTC_QCSLinkedRoleInCOSAccess	Service-Related Roles	cosaccess.trtc.cloud.tencent.com
Tencent Real-Time Communication	TRTC_QCSLinkedRoleIntrtcCloudRecording	Service-Related Roles	trtccloudrecording.trtc.cloud.tenc

TRTC_QCSLinkedRoleInCOSAccess

Use Cases：TRTC Access for cos

Authorization Polices

- Policy Name：QcloudAccessForTRTCLinkedRoleInCOSAccess
- Policy Information：

```
{
"version": "2.0",
"statement": [
{
"effect": "allow",
"action": [
"cos:DeleteBucket",
"cos:PutBucket",
"cos:GetBucket",
"cos:PutObjectCopy",
"cos:DeleteObject",
"cos:PostObject",
```

```
"cos:PutObject",
"cos:GetBucketOrigin",
"cos:GetObject",
"cos:DeleteBucketOrigin",
"cos:AppendObject"
],
"resource": "*"
}
]
}
```

TRTC_QCSLinkedRoleIntrtcCloudRecording

Use Cases：The current role is the TRTC service linked role, which will access your other service resources within the scope of the permissions of the associated policy.

Authorization Polices

- Policy Name：QcloudAccessForTRTCLinkedRoleInCloudRecording
- Policy Information：

```
{
"version": "2.0",
"statement": [
{
"action": [
"cos:GetService",
"cos:GetBucket",
"cos:ListMultipartUploads",
"cos:GetObject",
"cos:HeadObject",
"cos:GetBucketObjectVersions",
"cos:OptionsObject",
"cos:ListParts",
"cos:PostObject",
"cos:PostObjectRestore",
"cos:PutObject",
"cos:InitiateMultipartUpload",
"cos:UploadPart",
"cos:UploadPartCopy",
"cos:CompleteMultipartUpload",
"cos:AbortMultipartUpload",
"cos:AppendObject"
],
```

```
"resource": "*",
"effect": "allow"
}
]
}
```

Low-code Interactive Classroom

Last updated：2024-05-20 09:12:47

Service roles and service-linked roles are predefined by Tencent Cloud services and, upon user authorization, the corresponding services can access and use resources by assuming these service-linked roles. This document provides detailed information on the use cases and associated authorization policies of these specific service-linked roles.

Product	Role Name	Role Types	Role Entity
Low-code interactive classroom	LCIC_QCSLinkedRoleInTransfer	Service-Related Roles	transfer.lcic.cloud.tencent.com

LCIC_QCSLinkedRoleInTransfer

Use Cases：The current role can access VOD service from the LCIC console, with access, read, and write operations.

Authorization Polices

- Policy Name：QcloudAccessForLCICLinkedRoleInTransfers
- Policy Information：

```
{
"version": "2.0",
"statement": [
{
"effect": "allow",
"action": [
"vod:DescribeSubAppIds",
"vod:DescribeSubAppId",
"vod:DescribeSubAppCountData",
"vod:DescribeSubAppIdsForConsole",
"vod:CommitUpload",
"vod:ApplyUpload",
"vod:EditMedia",
"vod:PullUpload",
"vod:ProcessMedia",
"vod:DescribeTaskDetail"
],
"resource": "*"
}
```

```
]
}
```

Media On-Demand
Video on Demand

Last updated：2024-05-20 09:12:57

Service roles and service-linked roles are predefined by Tencent Cloud services and, upon user authorization, the corresponding services can access and use resources by assuming these service-linked roles. This document provides detailed information on the use cases and associated authorization policies of these specific service-linked roles.

Product	Role Name	Role Types	Role Entity
VOD	VOD_LogToCLS	Service-Related Roles	logtocls.vod.cloud.tencent.com
VOD	VOD_QCSLinkedRoleInHosting	Service-Related Roles	coshosting.vod.cloud.tencent.com
VOD	VOD_QCSLinkedRoleInManageSSLCertificates	Service-Related Roles	managesslcertificates.vod.cloud.tence

VOD_LogToCLS

Use Cases：The current role is the VOD service linked role, which will access your other service resources within the scope of the permissions of the associated policy.

Authorization Polices

- Policy Name：QcloudAccessForVODLogToCLS
- Policy Information：

```
{
"version": "2.0",
"statement": [
{
"action": [
"cls:pushLog",
"cls:listLogset",
```

```
"cls:getLogset",
"cls:listTopic",
"cls:getTopic",
"cls:createTopic",
"cls:modifyTopic",
"cls:deleteTopic",
"cls:createLogset",
"cls:modifyLogset",
"cls:deleteLogset",
"cls:getIndex",
"cls:modifyIndex",
"cls:CreateIndex"
],
"resource": "*",
"effect": "allow"
}
]
}
```

VOD_QCSLinkedRoleInHosting

Use Cases：The current role is the VOD service linked role, which will access your other service resources within the scope of the permissions of the associated policy.

Authorization Polices

- Policy Name：QcloudAccessForVODLinkedRoleInHosting
- Policy Information：

```
{
"version": "2.0",
"statement": [
{
"action": [
"cos:GetService",
"cos:GetBucket",
"cos:HeadBucket",
"cos:GetBucketObjectVersions",
"cos:PutObject",
"cos:PutObjectCopy",
"cos:PostObject",
"cos:GetObject",
"cos:HeadObject",
"cos:DeleteObject",
```

```
"cos:DeleteMultipleObjects",
"cos:OptionsObject",
"cos:PostObjectRestore",
"cos:PutObjectACL",
"cos:GetObjectACL",
"cos:PutObjectTagging",
"cos:GetObjectTagging",
"cos:DeleteObjectTagging",
"cos:InitiateMultipartUpload",
"cos:UploadPart",
"cos:UploadPartCopy",
"cos:CompleteMultipartUpload",
"cos:AbortMultipartUpload",
"cos:ListMultipartUploads",
"cos:ListParts"
],
"resource": "*",
"effect": "allow"
}
]
}
```

VOD_QCSLinkedRoleInManageSSLCertificates

Use Cases： The current role is the VOD service linked role, which will access your other service resources within the scope of the permissions of the associated policy.

Authorization Polices

- Policy Name：QcloudAccessForVODLinkedRoleInManageSSLCertificates
- Policy Information：

```
{
"version": "2.0",
"statement": [
{
"effect": "allow",
"resource": [
"*"
],
"action": [
"ssl:UploadCertificate",
"ssl:DescribeCertificates",
"ssl:DescribeCertificateDetail"
```

```
]
}
]
}
```

Cloud Real-time Rendering
Cloud Application Rendering

Last updated：2024-05-20 09:12:33

Service roles and service-linked roles are predefined by Tencent Cloud services and, upon user authorization, the corresponding services can access and use resources by assuming these service-linked roles. This document provides detailed information on the use cases and associated authorization policies of these specific service-linked roles.

Product	Role Name	Role Types	Role Entity
Cloud Application Rendering	CAR_QCSLinkedRoleInCloudStorage	Service-Related Roles	cloudstorage.car.cloud.tencent.com

CAR_QCSLinkedRoleInCloudStorage

Use Cases：The current role is the CAR service linked role, which will access your other service resources within the scope of the permissions of the associated policy.

Authorization Polices

- Policy Name：QcloudAccessForCARLinkedRoleInCloudStorage
- Policy Information：

```
{
"statement": [
{
"action": [
"cos:PutObject",
"cos:InitiateMultipartUpload",
"cos:ListMultipartUploads",
"cos:ListParts",
"cos:UploadPart",
"cos:CompleteMultipartUpload",
"cos:AbortMultipartUpload",
"cos:HeadObject",
"cos:GetObject"
],
"effect": "allow",
```

```
"resource": "*"
}
],
"version": "2.0"
}
```

Game Services
Game Multimedia Engine

Last updated：2024-05-20 09:12:44

Service roles and service-linked roles are predefined by Tencent Cloud services and, upon user authorization, the corresponding services can access and use resources by assuming these service-linked roles. This document provides detailed information on the use cases and associated authorization policies of these specific service-linked roles.

Product	Role Name	Role Types	Role Entity
Game Multimedia Engine	GME_QCSLinkedRoleInGameMedia	Service-Related Roles	gamemedia.gme.cloud.tencent.com

GME_QCSLinkedRoleInGameMedia

Use Cases：The current role is the GME service linked role, which will access your other service resources within the scope of the permissions of the associated policy.

Authorization Polices

- Policy Name：QcloudAccessForGMELinkedRoleInGameMedia
- Policy Information：

```
{
"version": "2.0",
"statement": [
{
"effect": "allow",
"resource": [
"*"
],
"action": [
"cos:HeadBucket",
"cos:GetBucket",
"cos:HeadObject",
"cos:GetObject",
"cos:PutObject",
"cos:PutObjectCopy",
"cos:DeleteObject",
```

```
"cos:DeleteMultipleObjects",
"cos:RenameObject",
"cos:InitiateMultipartUpload",
"cos:UploadPart",
"cos:UploadPartCopy",
"cos:CompleteMultipartUpload",
"cos:AbortMultipartUpload",
"cos:ListMultipartUploads",
"cos:ListParts",
"cos:GetService",
"cos:PutBucket"
]
}
]
}
```

Cloud Resource Management
Tencent Cloud Infrastructure as Code

Last updated：2024-05-20 09:12:55

Service roles and service-linked roles are predefined by Tencent Cloud services and, upon user authorization, the corresponding services can access and use resources by assuming these service-linked roles. This document provides detailed information on the use cases and associated authorization policies of these specific service-linked roles.

Product	Role Name	Role Types	Role Entity
Tencent Cloud Infrastructure as Code	TIC_QCSLinkedRoleInInfrastructureAsCode	Service-Related Roles	infrastructureascode.tic.cloud.tence

TIC_QCSLinkedRoleInInfrastructureAsCode

Use Cases：The current role is the TIC service role, this role is used to authorize TIC to orchestrate CVM, VPC, COS and other service resources, without the need for user escrow keys, and the operation is more efficient and safe.

Authorization Polices

- Policy Name：QcloudAccessForTICRoleInInfrastructureAsCode
- Policy Information：

```
{
"version": "2.0",
"statement": [
{
"action": [
"cvm:*",
"vpc:*",
"clb:*",
"as:*",
"cmqtopic:*",
"cmqqueue:*",
"ccs:*",
"scf:*",
"tag:*",
```

```
"monitor:*",
"cfs:*",
"cos:*",
"ckafka:*",
"apigw:*",
"cdb:*",
"mongodb:*",
"redis:*",
"cynosdb:*",
"dcdb:*",
"tcaplusdb:*",
"cdn:*",
"gaap:*",
"es:*",
"gme:*",
"sms:*",
"ssl:*",
"cam:*",
"bgpip:*",
"waf:*",
"finance:*",
"cloudaudit:*",
"sqlserver:*",
"postgres:*",
"vod:*",
"cls:*",
"sls:*",
"tcr:*",
"ecdn:*",
"kms:*"
],
"resource": "*",
"effect": "allow"
}
]
}
```

Tencent Smart Advisor

Last updated：2024-05-20 09:12:31

Service roles and service-linked roles are predefined by Tencent Cloud services and, upon user authorization, the corresponding services can access and use resources by assuming these service-linked roles. This document provides detailed information on the use cases and associated authorization policies of these specific service-linked roles.

Product	Role Name	Role Types	Role Entity
Tencent Cloud Advisor	Advisor_QCSLinkedRoleInBusinessContinuity	Service-Related Roles	businesscontinuity.advisor.cloud.tencer

Advisor_QCSLinkedRoleInBusinessContinuity

Use Cases：The current role is the Advisor service role, this role is used to Advisor to access CVM, VPC, COS and other service resources, without the need for user escrow keys, and the operation is more efficient and safe.

Authorization Polices

- Policy Name：QcloudAccessForAdvisorLinkedRoleInBusinessContinuity
- Policy Information：

```
{
"version": "2.0",
"statement": [
{
"action": [
"cvm:Describe*",
"cvm:Inquiry*",
"vpc:Describe*",
"vpc:Inquiry*",
"vpc:Get*",
"monitor:Describe*",
"monitor:Get*",
"cam:ListUsersForGroup",
"cam:ListGroups",
"cam:GetGroup",
"clb:Describe*",
"cos:List*",
```

```
"cos:Get*",
"cos:Head*",
"cos:OptionsObject",
"cdb:Describe*",
"mongodb:Describe*",
"redis:Describe*",
"redis:Get*",
"redis:Inquiry*",
"es:Describe*",
"emr:Describe*",
"emr:Inquiry*",
"emr:Check*",
"emr:List*",
"emr:Describle*",
"cloudaudit:LookUpEvents",
"cdn:Describe*",
"cdn:Get*",
"cdn:List*",
"ssl:Describe*",
"tag:Get*",
"ckafka:Get*",
"ckafka:List*",
"ckafka:Describe*",
"tdmq:Describe*",
"scf:Get*",
"scf:List*",
"cam:GetRole",
"cam:ListAttachedRolePolicies",
"cls:getLogset",
"cls:getTopic",
"cls:listTopic",
"apigw:Describe*",
"cmqtopic:GetTopicAttributes",
"cmqtopic:GetSubscriptionAttributes",
"tsf:Describe*",
"tsf:Get*",
"tsf:List*",
"tsf:Search*",
"tsf:Find*",
"tsf:ImageUserIsExists",
"tsf:ImageGetRepositoryList",
"tsf:DscribeTasks",
"tbase:Describe*",
"tdach:Describe*",
"tdapg:Describe*",
"dcdb:Describe*",
"tke:Describe*",
```

```
"live:Describe*",
"im:Describe*",
"im:CheckIfIMNewUser",
"cfw:Describe*",
"waf:WafGet*",
"waf:WAFGetUserInfo",
"waf:WafDownloadAlerts",
"waf:WafPackagePrice",
"waf:WafAreaBanGetAreas",
"waf:WafFreqGetRuleList",
"waf:WafAntiFakeGetUrl",
"waf:WafInterface",
"waf:WafClsOverview",
"waf:QueryFlows",
"waf:WafDownloadRecords",
"waf:WafDownloadlogs",
"waf:WafSearchLogs",
"waf:WafDNSdetectGet*",
"waf:BotGet*",
"waf:Get*",
"waf:Search*",
"waf:BotV2Get*",
"wss:CertGetList",
"waf:Describe*",
"tag:DescribeResourceTagsByResourceIds",
"mariadb:Describe*",
"antiddos:Describe*",
"cam:DescribeSafeAuthFlagColl",
"cam:ListUsers",
"cam:DescribeSubAccounts",
"ccs:DescribeCluster",
"sms:SmsPackagesStatistics",
"domain:*",
"sms:CallbackStatusStatistics",
"sms:SendStatusStatistics",
"dc:DescribeDirectConnects",
"dc:DescribeDirectConnectTunnels",
"trtc:Describe*",
"trtc:Get*",
"trtc:ShowRoomList",
"trtc:ShowUserList",
"trtc:RemindBalance",
"trtc:HardDescribeMixConf",
"memcached:DescribeInstances",
"cynosdb:DescribeClusterDetail",
"cynosdb:DescribeRollbackTimeValidity",
"cynosdb:DescribeRollbackTimeRange",
```

```
"cynosdb:DescribeInstanceSpecs",
"cynosdb:DescribeInstances",
"cynosdb:DescribeInstanceDetail",
"cynosdb:DescribeDBSecurityGroups",
"cynosdb:DescribeClusters",
"cynosdb:DescribeClusterInstanceGrps",
"cynosdb:DescribeBackupList",
"cynosdb:DescribeBackupConfig",
"cynosdb:DescribeAccounts",
"dnspod:DescribeDomain",
"dnspod:DescribeDomainList",
"dnspod:DescribeDomainLogList",
"dnspod:DescribeDomainPurview",
"dnspod:DescribeDomainShareInfo",
"dnspod:DescribeRecord",
"dnspod:DescribeRecordLineList",
"dnspod:DescribeRecordList",
"dnspod:DescribeRecordType",
"dnspod:DescribeUserDetail",
"vod:DescribeCDNStatDetails",
"vod:DescribeSubAppIds",
"vod:DescribeDefaultDistributionConfig",
"vod:DescribeVodDomains",
"cwp:DescribeVulList",
"cfs:DescribeCfsFileSystems",
"cfs:DescribeAutoSnapshotPolicies",
"cfs:DescribeCfsSnapshots",
"sms:DescribeAppList",
"sms:DescribeVerificationCodeStatistic",
"sms:DescribeAntiBrushThreshold",
"tke:CreateInstantInspectJob",
"tke:DescribeInstantInspectTask",
"cloudaudit:DescribeEvents",
"clb:DescribeQuota",
"cdb:QueryCDBProxy",
"clb:DescribeClusterResources",
"ssl:DescribeCertificateBindResources",
"monitor:GetIntegrationProductList",
"monitor:DescribeOneClickAlarmConfigs",
"monitor:DescribeAlarmPolicies",
"antiddos:DescribeListProtocolBlockConfig",
"cloudhsm:DescribeVsms",
"kms:GetServiceStatus",
"as:DescribeAutoScalingInstances",
"billing:DescribeCostSummaryByProduct",
"finance:DescribeBillSummaryByProduct",
"tke:ListClusterInspectionResultsItems",
```

```
"tke:ListClusterInspectionResults",
"dnspod:DescribeSnapshotConfig",
"dnspod:DescribeDomainFilterList",
"dc:DoDcHealthInspection",
"teo:DescribeDefaultCertificates",
"teo:DescribeHostsSetting",
"teo:DescribeRules",
"teo:DescribeZones",
"csip:DescribeRiskCenterAssetViewVULRiskList",
"csip:DescribeRiskCenterAssetViewPortRiskList",
"csip:DescribePublicIpAssets",
"csip:DescribeDomainAssets",
"csip:DescribeCVMAssets",
"csip:DescribeClusterPodAssets",
"csip:DescribeDbAssets",
"lighthouse:DescribeInstances",
"dbbrain:DescribeDBDiagEvent",
"dbbrain:DescribeDBDiagEvents",
"live:CheckLiveHostBackupOriginSite",
"tse:DescribeCloudNativeAPIGateways",
"tse:DescribeSREInstances",
"dbbrain:DescribeSqlFilters",
"postgres:DescribeDBInstanceAttribute",
"postgres:DescribeDBInstances",
"postgres:DescribeZones",
"tdmq:DescribeRocketMQCluster",
"ckafka:DescribeInstanceAttributes",
"teo:DescribeSecurityPolicy",
"teo:DescribeDDoSPolicy",
"gaap:DescribeProxies",
"teo:DescribeZoneDDoSPolicy",
"tdmq:DescribeRabbitMQVipInstances",
"tcb:DescribeBillingInfo",
"tcb:DescribeQuotaData",
"tcb:DescribeBaasPackageList",
"vod:DescribeTranscodeTemplates",
"cam:MonitorGetProject",
"monitor:GetProjectsList",
"redis:DescribeInstances",
"ckafka:DescribeTopicDetail",
"ckafka:DescribeInstancesDetail",
"tcb:DescribeEnvs",
"tsf:DescribeGroupAttribute",
"tsf:DescribeContainerGroups",
"tsf:DescribeGroups",
"tsf:DescribeApplications",
"vpc:DescribeCcns",
```

```
"vpc:DescribeCcnAttachedInstances",
"vpc:GetCcnRegionBandwidthLimits",
"mariadb:DescribeDBInstanceDetail",
"dcdb:DescribeDCDBInstanceDetail",
"sqlserver:DescribeDBInstances",
"cdb:DescribeRoGroups",
"tdmq:DescribeRocketMQClusters",
"tdmq:DescribeRocketMQNamespaces",
"tdmq:DescribeRocketMQTopics",
"tdmq:DescribeRocketMQGroups",
"trocket:DescribeInstanceList",
"trocket:DescribeTopicList",
"trocket:DescribeConsumerGroupList"
],
"resource": "*",
"effect": "allow"
}
]
}
```

Tencent Cloud Mini Program Platform

Last updated：2024-05-20 09:12:53

Service roles and service-linked roles are predefined by Tencent Cloud services and, upon user authorization, the corresponding services can access and use resources by assuming these service-linked roles. This document provides detailed information on the use cases and associated authorization policies of these specific service-linked roles.

Product	Role Name	Role Types	Role Entity
Tencent Cloud Mini Program Platform	TCMPP_QCSLinkedRoleInUserManage	Service-Related Roles	usermanage.tcmpp.cloud.tencent.com

TCMPP_QCSLinkedRoleInUserManage

Use Cases：The current role is the TCMPP service linked role, which will access your other service resources within the scope of the permissions of the associated policy.

Authorization Polices

- Policy Name：QcloudAccessForTCMPPLinkedRoleInUserManage
- Policy Information：

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

Management and Audit Tools
Cloud Access Management

Last updated：2024-05-20 09:12:33

Service roles and service-linked roles are predefined by Tencent Cloud services and, upon user authorization, the corresponding services can access and use resources by assuming these service-linked roles. This document provides detailed information on the use cases and associated authorization policies of these specific service-linked roles.

Product	Role Name	Role Types	Role Entity
Cloud Access Management	CAM_QCSLinkedRoleInEkslog	Service-Related Roles	ekslog.cam.cloud.tencent.com
Cloud Access Management	CAM_QCSLinkedRoleInEkslog002	Service-Related Roles	ckmlog.cam.cloud.tencent.com
Cloud Access Management	CAM_QCSRole	Service Role	cam.cloud.tencent.com

CAM_QCSLinkedRoleInEkslog

Use Cases：The current role is the CAM service linked role, which will access your other service resources within the scope of the permissions of the associated policy.

Authorization Polices

- Policy Name：QcloudAccessForCAMLinkedRoleInEkslog
- Policy Information：

```
{
"version": "2.0",
"statement": [
{
"effect": "allow",
"action": [
"vpc:CreateAddress",
"sts:ListAccessKeys",
"sts:UpdateAccessKey",
```

```
"sts:DeleteAccessKey",
"cam:ListAccessKeys",
"cam:ListUsers",
"cam:GetUser"
],
"resource": "*"
}
]
}
```

CAM_QCSLinkedRoleInEkslog002

Use Cases：The current role is the CAM service linked role, which will access your other service resources within the scope of the permissions of the associated policy.

Authorization Polices

- Policy Name：QcloudAccessForCAMLinkedRoleInEkslog002
- Policy Information：

```
{
"version": "2.0",
"statement": [
{
"effect": "allow",
"action": [
"kms:CreateKey",
"clb:DescribeTaskStatus",
"vpc:CreateAddress"
],
"resource": "*"
}
]
}
```

CAM_QCSRole

Use Cases：The current role is the CAM service role, which will access your other service resources within the scope of the permissions of the associated policy.`

Authorization Polices

- Policy Name：QcloudAccessForCAM_QCSRole
- Policy Information：

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

Tencent Cloud Organization

Last updated：2024-05-20 09:12:50

Service roles and service-linked roles are predefined by Tencent Cloud services and, upon user authorization, the corresponding services can access and use resources by assuming these service-linked roles. This document provides detailed information on the use cases and associated authorization policies of these specific service-linked roles.

Product	Role Name	Role Types	Role Entity
Tencent Cloud Organization	Organization_QCSLinkedRoleInDefaultMng	Service-Related Roles	defaultmng.organization.cloud.tenc
Tencent Cloud Organization	Orgnization_QCSLinkedRoleInServiceControl	Service-Related Roles	servicecontrol.orgnization.cloud.ter

Organization_QCSLinkedRoleInDefaultMng

Use Cases：The current role is the Organization service linked role, which will access your other service resources within the scope of the permissions of the associated policy.

Authorization Polices

- Policy Name：QcloudAccessForOrganizationLinkedRoleInDefaultMng
- Policy Information：

```
{
"version": "2.0",
"statement": [
{
"action": [
"finance:DescribeBillSummaryByProduct",
"cam:GetAccountSummary",
"intlpartnersmgt:DescribeBillSummaryByProduct"
],
"resource": "*",
"effect": "allow"
}
```

```
]
}
```

Orgnization_QCSLinkedRoleInServiceControl

Use Cases： The current role is the Orgnization service linked role, which will access your other service resources within the scope of the permissions of the associated policy.

Authorization Polices

- Policy Name：QcloudAccessForOrganizationLinkedRoleInServiceControl
- Policy Information：

```
{
"version": "2.0",
"statement": [
{
"effect": "allow",
"resource": [
"*"
],
"action": [
"cam:CreateServiceLinkedRole",
"cam:DeleteServiceLinkedRole",
"cam:GetRole",
"cam:CreateRole",
"cam:AttachRolePolicy",
"cam:DeleteRole"
]
}
]
}
```