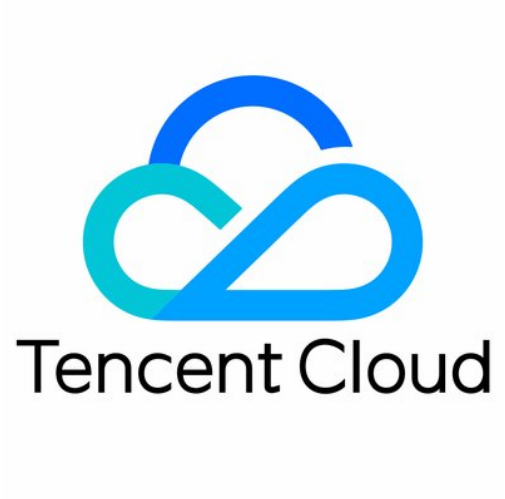
Cloud Access Management

Product Introduction

Product Documentation



Contents

Product Introduction

CAM Overview

Last updated : 2020-02-26 18:00:23

Tencent Cloud CAM is a web service that helps customers securely manage and control access to their Tencent Cloud resources. CAM provides identity management and policy management for you to create, manage or terminate users (groups), and to control who is allowed to access and use your Tencent Cloud resources.

Features

Last updated : 2020-05-25 11:39:50

CAM provides the following features:

Access Permission Management

A sub-account can be created under a root account and granted the management permissions of the resources there, without having to share the root account's identity credentials.

Refined Permission Management

CAM allows you to use permissions to control who can access what kind of Tencent Cloud resources and services at a granular level. For example, you can grant some sub-accounts read permissions for a specific COS bucket, and other sub-accounts write permissions for a specific COS object. Resources and access permissions can be granted in batches.

Federated Identity

Users who get passwords through CAM by using your existing identity verification system (for example, your enterprise network or through an Internet identity provider) can obtain temporary access permissions to your Tencent Cloud account.

Data integrity

CAM is now available in Tencent Cloud in multiple regions, which allows you to synchronize cross-region data simply through replicating policy data. Although the modified CAM policies will be submitted immediately, the cross-region policy synchronization can result in delayed effects. CAM utilizes cache to improve performance, which may increase the latency in some cases as updates do not take effect until the cache expires.

Use Cases

Last updated : 2020-05-15 10:55:50

Go here to see CAM use limits.

Use Cases

Refined access control for resources

Grant resource management permissions to sub-users.
You can create users or roles in CAM and assign them separate security credentials (console login passwords, TencentCloud API keys, etc.) or request temporary credentials for them to access Tencent Cloud resources. You can also manage permissions to control the operations users and roles can perform and the resources they can access.

Single sign-on to Tencent Cloud

Users with external Tencent Cloud roles can access Tencent Cloud resources.
You can use your existing authentication system through CAM to grant your employees and services access permissions to Tencent Cloud services and resources. Tencent Cloud supports federated authentication based on SAML 2.0 (Security Assertion Markup Language 2.0) to implement interconnection with your organizational account systems on a private network. For more information, please click here.

Multi-factor authentication for improved account security

Strengthen your security with an additional layer of protection
We currently support two authentication methods: (hardware/virtual) MFA device authentication and mobile verification code. Depending on the configuration, a user may be required to enter a valid 6-digit authentication code to verify their identity and device environment before logging in or performing sensitive operations.

Use Limits

Last updated : 2020-06-15 14:20:52

Item	Upper Limit
Number of user groups under one root account	300
Number of sub-accounts under one root account	1000
Number of roles under one root account	1000
Number of user groups one sub-account can join	10
Number of root accounts one collaborator can collaborate with	10
Number of sub-accounts in a user group	100
Number of custom policies that can be created by one root account[1]	1500
Number of policies directly associated with one user, user group, or role[2]	200
Number of characters in one policy syntax	4096

⚠ Note :

1. COS custom policies are counted toward the total number of custom policies created by a root account. If you see a prompt saying that **The number of custom policies exceeds the upper limit (1,500)**, but the number of CAM custom policies has not reached the upper limit, you can go to the bucket list in the COS Console, click a bucket name and enter the permission management page to check the number of access control lists (ACLs). The combined total might have reached the upper limit.
2. COS custom policies are counted toward the total number of policies directly associated with a user, user group, or role. If you see a prompt saying **Failed to associate the policy**, but the number of associated CAM policies has not reached the upper limit, you can go to the bucket list in the COS Console, click a bucket name and enter the permission management page to check the number of access control lists (ACLs). The combined total might have reached the upper limit.

CAM-Enabled Products

Last updated : 2021-01-18 15:05:34

Overview

Cloud Access Management (CAM) helps you securely manage permissions for most Tencent Cloud services. This document provides information on the products and services that support CAM in multiple dimensions, such as authorization granularity, console operation, authorization by tag, and reference documentation.
The table below lists Tencent Cloud services that support CAM.
Definitions:

- Service: name of a CAM-enabled Tencent Cloud service. For more information on a specific service, click the link to the reference document.
- Authorization granularity: the finest authorization granularity currently supported by the service.

Note :

Three authorization granularity levels are supported: service level, operation level and resource level.

- Service level: it defines whether a user has the permission to access the service as a whole. A user can have either full access or no access to the service.
- Operation level: it defines whether a user has the permission to call a specific API of the service. For example, granting an account read-only access to the CVM service is an authorization at the operation level.
- Resource level: it is the finest authorization granularity which defines whether a user has the permission to access specific resources. For example, granting an account read/write access to a specific CVM instance is an authorization at the resource level.

- Console: whether sub-accounts can access the service through the console. "✓" means yes, while "-" means no.
- Authorization by tag: whether the service supports using tags for permission management. "✓" means yes, while "-" means no.
- Service role: whether the service can access other services as a role entity. "✓" means yes, while "-" means no.
- Reference document: link to the document on CAM-based access control for the service. "-" means no documentation available yet.

Compute

Service	Authorization Granularity	Console	Authorization by Tag	Service Role	Reference Document
Cloud Virtual Machine (CVM) [1]	Resource level	✓	✓	✓	CAM Guide
Tencent Kubernetes Engine (TKE)	Resource level	✓	✓	✓	CAM Guide
Auto Scaling (AS)	Resource level	✓	✓	✓	-
BatchCompute	Resource level	✓	✓	-	CAM Guide
Tencent Container Registry (TCR)	Resource level	✓	-	✓	-

Note :

[1] In CVM, GPU Cloud Computing (GCC) and CVM Dedicated Host (CDH) support CAM.

Storage

Service	Authorization Granularity	Console	Authorization by Tag	Service Role	Reference Document
Cloud Object Storage (COS)	Resource level	✓	-	✓	CAM Guide
Cloud File Storage (CFS)	Resource level	✓	-	✓	CAM Guide
Cloud Block Storage (CBS)	Resource level	✓	✓	-	-
Cloud Data Migration (CDM)	Service level	✓	-	-	-
Cloud Log Service (CLS)	Resource level	✓	-	✓	CAM Guide

Networking

Service	Authorization Granularity	Console	Authorization by Tag	Service Role	Reference Document
Cloud Load Balancer (CLB)	Resource level	✓	✓	✓	CAM Guide
Virtual Private Cloud (VPC)[1]	Resource level	✓	✓	-	-
Direct Connect (DC)	Resource level	✓	-	-	-

Note :

[1] In VPC, Elastic Network Interface (ENI), NAT Gateway, Peering Connection, VPN Connections, Flow Logs (FL), Anycast Internet Acceleration (AIA), Cloud Connect Network (CCN), and Bandwidth Package (BWP) support CAM.

CDN and Acceleration

Service	Authorization Granularity	Console	Authorization by Tag	Service Role	Reference Document
Global Application Acceleration Platform (GAAP)	Resource level	✓	✓	-	-
Enterprise Content Delivery Network (ECDN)	Resource level	✓	-	-	-
Content Delivery Network (CDN)[1]	Resource level	✓	✓	✓	CAM Guide

Database

Service	Authorization	Console	Authorization	Service	Reference

	Granularity		by Tag	Role	Document
TencentDB for MySQL	Resource level	✓	-	✓	CAM Guide
TencentDB for MariaDB	Resource level	✓	✓	✓	CAM Guide
TencentDB for SQL Server	Resource level	✓	-	-	CAM Guide
TencentDB for PostgreSQL	Resource level	✓	✓	-	-
TDSQL for MySQL	Resource level	✓	✓	-	CAM Guide
TencentDB for Redis	Resource level	✓	-	-	CAM Guide
TencentDB for MongoDB	Resource level	✓	✓	✓	CAM Guide
Data Transmission Service (DTS)	Resource level	✓	✓	✓	-
TcaplusDB	Resource level	✓	✓	-	-
TencentDB for DBbrain	Resource level	✓	-	-	CAM Guide

Serverless

Service	Authorization Granularity	Console	Authorization by Tag	Service Role	Reference Document
Serverless Cloud Function (SCF)	Resource level	✓	✓	✓	CAM Guide
Serverless Framework	Resource level	-	-	✓	-

Middleware

Service	Authorization Granularity	Console	Authorization by Tag	Service Role	Reference Document
Cloud Message Queue (CMQ)	Resource level	✓	✓	-	CAM Guide
Cloud Kafka (CKafka)	Resource level	✓	-	✓	-
API Gateway	Resource level	✓	✓	✓	CAM Guide

Data Processing

Service	Authorization Granularity	Console	Authorization by Tag	Service Role	Reference Document
Cloud Infinite (CI)	Resource level	✓	-	✓	CAM Guide

Domain Names and Websites

Service	Authorization Granularity	Console	Authorization by Tag	Service Role	Reference Document
ICP Filing Registration	Service level	✓	-	-	-
SSL Certificates Service	Resource level	✓	-	-	-

Network Security

Service	Authorization Granularity	Console	Authorization by Tag	Service Role	Reference Document
Aegis Anti-DDoS	-	-	-	✓	-

Note :

[1] In Anti-DDoS, Anti-DDoS Pro and Anti-DDoS Advanced support CAM.

Data Security

Service	Authorization Granularity	Console	Authorization by Tag	Service Role	Reference Document
Key Management Service (KMS)	Resource level	✓	✓	-	CAM Guide

Security Management

Service	Authorization Granularity	Console	Authorization by Tag	Service Role	Reference Document
Security Operations Center	Operation level	✓	-	✓	-

Application Security

Service	Authorization Granularity	Console	Authorization by Tag	Service Role	Reference Document
Web Application Firewall (WAF)	Operation level	✓	-	-	-

Video Services

Service	Authorization Granularity	Console	Authorization by Tag	Service Role	Reference Document
Tencent Real-Time Communication (TRTC)	Resource level	✓	✓	-	-
Live Video Broadcasting	Resource level	✓	✓	✓	CAM

(LVB)					Guide
Video on Demand (VOD)	Resource level	✓	-	✓	CAM Guide
Media Processing Service (MPS)	Service level	✓	-	✓	-
MediaLive	Operation level	✓	-	-	-
MediaPackage	Operation level	✓	-	-	-

Big Data Platform

Service	Authorization Granularity	Console	Authorization by Tag	Service Role	Reference Document
Elastic MapReduce (EMR)	Resource level	✓	✓	✓	CAM Guide
Elasticsearch Service (ES)	Resource level	✓	✓	-	CAM Guide

Image Recognition

Service	Authorization Granularity	Console	Authorization by Tag	Service Role	Reference Document
Optical Character Recognition (OCR)	Service level	✓	-	-	-

Gaming Services

Service	Authorization Granularity	Console	Authorization by Tag	Service Role	Reference Document
Game Multimedia Engine (GME)	Resource level	✓	✓	-	-

Game Server Engine	Resource level	✓	✓	✓	CAM Guide
Game Player Matchmaking	Resource level	✓	✓	✓	-

Mobile Services

Service	Authorization Granularity	Console	Authorization by Tag	Service Role	Reference Document
Tencent Push Notification Service (TPNS)	Resource level	✓	-	-	CAM Guide

Cloud Communication

Service	Authorization Granularity	Console	Authorization by Tag	Service Role	Reference Document
Instant Messaging (IM)	Resource level	✓	✓	-	-
Short Message Service (SMS)	Resource level	✓	✓	-	-

Cloud Resource Management

Service	Authorization Granularity	Console	Authorization by Tag	Service Role	Reference Document
Tag	Operation level	✓	-	-	-
Tencent Cloud Infrastructure as Code (TIC)	Service level	-	-	✓	-

Management and Auditing

Service	Authorization Granularity	Console	Authorization by Tag	Service Role	Reference Document
Cloud Access Management (CAM)	Operation level	✓	-	-	CAM Guide
CloudAudit	Operation level	✓	-	✓	-
Tencent Cloud Organization (TCO)	Operation level	✓	-	-	-

Monitoring and OPS

Service	Authorization Granularity	Console	Authorization by Tag	Service Role	Reference Document
Cloud Monitor	Resource level	✓	✓	✓	-
Migration Service Platform (MSP)	Service level	✓	-	✓	-