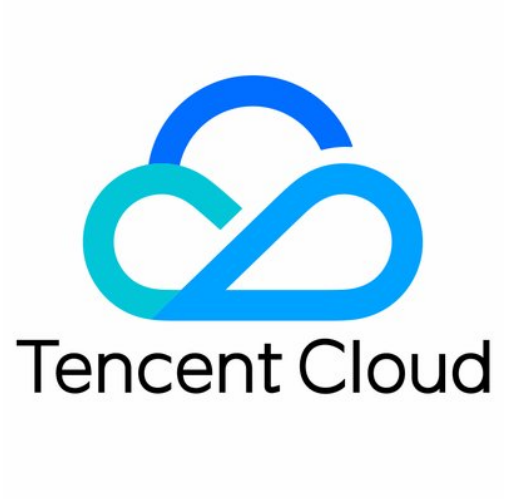
Private DNS

Access Management

Product Documentation



Contents

Access Management
Access Control Overview

Last updated：2022-01-28 12:11:13

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

Basic CAM Concepts

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

1. **Account**
   - **Root account**: the owner of Tencent Cloud resources and the fundamental entity for resource usage, usage calculation, and billing. It can be used to log in to Tencent Cloud services.
   - **Sub-account**: an account created by the root account. It has a specific ID and identity credential that can be used to log in to the Tencent Cloud console. A root account can create multiple sub-accounts (users). **By default, a sub-account does not own any resources and must be authorized by its root account.**
   - **Identity credential**: includes login credentials and access certificates. **Login credential** refers to a user's login name and password. **Access certificate** refers to Tencent Cloud API keys (`SecretId` and `SecretKey`).
2. **Resources and permissions**
   - **Resource**: an object that is operated in Tencent Cloud services, such as a CVM instance, a COS bucket, or a VPC instance.
   - **Permission**: an authorization that allows or forbids users to perform certain operations. By default, **the root account has full access to all resources under the account, while a sub-account does not have access to any resources under its root account.**
   - **Policy**: syntax rule that defines and describes one or more permissions. The **root account** performs authorization by **associating policies** with users/user groups.

For more information, please see CAM Overview.

Related Documents

Document Description	Link

Document Description	Link
Relationship between policy and user	Policy
Basic policy structure	Policy Syntax
CAM-Enabled products	CAM-Enabled Products

Authorizable Resource Types

Last updated：2022-01-28 12:11:13

Resource-Level permission can be used to specify which resources a user can manipulate. Most APIs of Private DNS support resource-level authorization to allow users to operate on specific private domains.

Private DNS Resources That Can Be Authorized in CAM

Resource Type	Six-Segment Resource Format
Private domain	`qcs::privatedns::$accountid:zone/$zoneId`

Here:

- `$accountid` should always be the `AccountId` of the resource owner or left empty.
- `$zoneId` should always be the ID of a specific private domain. If you want to authorize all private domains, you can enter `*`.

Private DNS Operations That Can Be Authorized in CAM

API Operation	API Description	Resource Path
DescribeUserConfig	Gets current user configuration	*
DescribeAuditLog	Gets the list of operation logs	`qcs::privatedns::zone/${ZoneId}`
DescribePrivateZoneList	Gets the list of private domains	`qcs::privatedns::zone/${ZoneId}`
ModifyPrivateZoneVpc	Modifies VPC associated with private domain	`qcs::privatedns::zone/${ZoneId}`
DeletePrivateZoneRecord	Deletes DNS record for private domain	`qcs::privatedns::zone/${ZoneId}`
ModifyPrivateZoneRecord	Modifies DNS record for private domain	`qcs::privatedns::zone/${ZoneId}`

API Operation	API Description	Resource Path
DeletePrivateZone	Deletes private domain	`qcs::privatedns::zone/${ZoneId}`
DescribeRequestData	Gets the DNS request volume of private domain	`qcs::privatedns::zone/${ZoneId}`
DescribePrivateZone	Gets private domain information	`qcs::privatedns::zone/${ZoneId}`
DescribePrivateZoneRecordList	Gets the list of records for private domain	`qcs::privatedns::zone/${ZoneId}`
ModifyPrivateZone	Modifies private domain	`qcs::privatedns::zone/${ZoneId}`
CreatePrivateZoneRecord	Adds DNS record for private domain	`qcs::privatedns::zone/${ZoneId}`
DescribeDashboard	Gets the overview of Private DNS	*
DescribePrivateZoneService	Queries Private DNS activation status	*
SubscribePrivateZoneService	Activates Private DNS	*
ModifyUserConfig	Modifies current user configuration	*
CreatePrivateZone	Creates private domain	*

Sample Access Control Policy

Last updated：2022-01-28 12:11:13

Overview

Cloud Access Management (CAM) is used to manage the access permissions for the resources under Tencent Cloud accounts. With CAM, you can use the identity management and policy management features to control which Tencent Cloud resources can be accessed by which sub-accounts. This document describes how to use certain policies in the console.

Samples

Full access policy in Private DNS

To grant a user the permission to create and manage private domains in Private DNS, associate the **QcloudPrivateDNSFullAccess** policy with the user.
Associate the preset policy **QcloudPrivateDNSFullAccess** with the user as instructed in Authorization Management.
The policy syntax is as follows:

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

Read-only policy in Private DNS

To grant a user the permission to view private domains in Private DNS but not create or delete them, associate the **QcloudPrivateDNSReadOnlyAccess** policy with the user.
Associate the preset policy **QcloudCVMInnerReadOnlyAccess** with the user as instructed in Authorization Management.
The policy syntax is as follows:

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