

HTTPDNS

Access Management

Product Documentation



Copyright Notice

©2013-2019 Tencent Cloud. All rights reserved.

Copyright in this document is exclusively owned by Tencent Cloud. You must not reproduce, modify, copy or distribute in any way, in whole or in part, the contents of this document without Tencent Cloud's the prior written consent.

Trademark Notice



All trademarks associated with Tencent Cloud and its services are owned by Tencent Cloud Computing (Beijing) Company Limited and its affiliated companies. Trademarks of third parties referred to in this document are owned by their respective proprietors.

Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.

Contents

Access Management

Overview

Sample Access Control Policy

Access Management

Overview

Last updated : 2022-06-22 15:22:45

[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.

For example, if your account has HTTPDNS domains deployed in different projects, to strengthen access control, you can authorize resources and assign the admin of project A an authorization policy, specifying that only the admin can manipulate the HTTPDNS domain resources under project A.

You can skip this section if you don't need to manage the permissions of HTTPDNS resources for sub-users.

Note :

Currently, CAM-based access authorization is only supported in the console.

Basic CAM Concepts

A root account authorizes sub-accounts by binding policies. The policy settings 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, see [CAM Overview](#).

Relevant Documentation

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

Sample Access Control Policy

Last updated : 2022-06-22 15:22:45

Full Access Policy in HTTPDNS

- Grant a sub-user or collaborator full access (for creating, managing, etc.).
- Policy name: QcloudHTTPDNSFullAccess

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

Read-Only Policy in HTTPDNS

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

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

