Direct Connect

Cloud Access Management

Product Documentation

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

Cloud Access Management

Overview

Last updated：2024-01-13 16:02:36

If you have multiple users managing different Tencent Cloud services such as Direct Connect, VPC, CVM and other Tencent Cloud products, and they all share your Tencent Cloud account access key, you may face the following problems:

The risk of your key being compromised is high since multiple users are sharing it.

Your users might introduce security risks from misoperations due to the lack of user access control.

You can avoid the above problems by CAM, which allows different users to manage different services through sub-accounts. The dedicated tunnel of Direct Connect supports the resource-level permissions. By default, a sub-account does not have permissions to use dedicated tunnel or its resources. Therefore, you need to create a policy to grant different permissions to the sub-accounts.

Note:

You can skip this section if you do not need to manage permissions to dedicated tunnel resources for sub-accounts. This will not affect your understanding and use of the other sections of the document.

Supported Permissions

The Direct Connect service consists of connection, dedicated tunnel and direct connect gateway resources. The following table specifies the supported access permissions to resources:

Resource	Permission	Authorization Granularity
Connection	Supported	API-level
Dedicated tunnel	Supported	Resource-level
Direct connect gateway	Supported	Resource-level

CAM

Cloud Access Management (CAM) is a Tencent Cloud web service that helps you securely manage and control access to your Tencent Cloud resources. Using CAM, you can create, manage, and terminate users and user groups. You can manage identities and policies to allow specific users to access your Tencent Cloud resources.

When using CAM, you can associate a policy with a user or user group to allow or forbid them to use specified resources to complete specified tasks. For more information on CAM policies, see Syntax Logic. For more information on the use of CAM policies, see Policy.

The root account can associate policies with sub-accounts to implement permissions. The policies support multiple dimensions, such as API, resource, user, user group, allowing, forbidding, and condition.

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).

Resource and permission

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.

Note:

For more information, please see CAM Overview.

Documentation

Task	Link
Understand the relationship between policies and users	Policy
Understand the basic structure of policies	Element Reference
Check CAM-enabled products	CAM-Enabled Products

Access Policy Types

Last updated：2024-01-13 16:02:36

Dedicated tunnel supports resource-level permissions, allowing the user to perform operations or use specific resources.

Access Policy

Cloud Access Management (CAM) allows you to grant access permissions to the following resources

Resource Type	Resource Description Method in Access Policies
Dedicated tunnel	qcs::dc::uin/${Uin}/dcx/${DirectConnectTunnelId}

Replace `${Uin}` with the resource owner’s AccountId or “*”.
Replace `${DirectConnectTunnelId}` with the dedicated tunnel ID or “*”.

Dedicated Tunnel Operations

API Name	API Description	Six-segment Format
CreatePublicDirectConnectTunnel	Creates an Internet tunnel	qcs::dc::uin/:dcx/*
DescribeDirectConnectTunnels	Obtains the list of dedicated tunnels	qcs::dc::uin/:dcx/*
AcceptDirectConnectTunnel	Accepts a dedicated tunnel	qcs::dc::uin/:dcx/${DirectConnectTunnelId}
DeleteDirectConnectTunnel	Deletes a dedicated tunnel	qcs::dc::uin/:dcx/${DirectConnectTunnelId}
ModifyDirectConnectTunnelAttribute	Modifies the dedicated tunnel attributes.	qcs::dc::uin/:dcx/${DirectConnectTunnelId}
CreateDirectConnectTunnel	Creates a dedicated tunnel	qcs::dc::uin/:dcx/*

RejectDirectConnectTunnel	Rejects an application for a dedicated tunnel	qcs::dc::uin/:dcx/${DirectConnectTunnelId}
DescribePublicDirectConnectTunnelRoutes	Queries the route table of an Internet tunnel	qcs::dc::uin/:dcx/${DirectConnectTunnelId}
DescribeDirectConnectTunnelExtra	Queries the extended information of a dedicated tunnel	qcs::dc::uin/:dcx/${DirectConnectTunnelId}
ModifyDirectConnectTunnelExtra	Modifies the extended information of a dedicated tunnel	qcs::dc::uin/:dcx/${DirectConnectTunnelId}

Access Policy Syntax

Last updated：2024-01-13 16:02:36

This document describes CAM access policy syntax and use cases.

CAM Policy Syntax

CAM policy:

```
{
        "version":"2.0",
        "statement":
        [
           {
              "effect":"effect",
              "action":["action"],
              "resource":["resource"],
               "condition": {"key":{"value"}}
           }
       ]
}
```

version is required. Currently, only the value "2.0" is allowed.

statement describes the details of one or more permissions, and therefore contains the permission(s) of other elements such as `effect` , `action` , `resource` , and `condition` . One policy has only one `statement` .

1.1 **effect** is required. It describes the result of a statement. The result can be "allow" or an explicit "deny".

1.2 **action** is required. It describes the allowed or denied operation. An operation can be an API (prefixed with “name” or a feature set (a set of specific APIs prefixed with "permit").

1.3 **resource** is required. It describes the details of authorization. A resource is described in a six-segment format. Detailed resource definitions vary by product. For more information on how to specify a resource, see the documentation for the product whose resources you are writing a statement for.

1.4 **condition** is optional. It describes the condition for the policy to take effect. A condition consists of operator, action key, and action value. A condition value may contain information such as time and IP address. Some services allow you to specify additional values in a condition.

Policy Examples

Specify a full read/write permission policy for dedicated tunnel as follows:

Grant the sub-accounts all operation permissions for dedicated tunnels, such as creation and management.

Policy name: QcloudDCFullAccess

```
    }
```

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

```
 }
```

Specify a read-only permission policy for dedicated tunnel as follows:

Grant the sub-account read-only permission for dedicated tunnels. The authorized sub-account can view all resources of the dedicated tunnels, but cannot create, update or delete resources.

Policy name: QcloudDCReadOnlyAccess

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