Virtual Private Cloud

Product Introduction

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

Product Introduction
  Overview
  Strengths
  Use Cases
Basic Concepts
  IP Addresses
  Regions and Availability Zones
Security
  Security Groups
Access Management
  Cloud Access Management Overview
  Authorizable Resource Types
Product Introduction
Overview

A Virtual Private Cloud (VPC) is a logically isolated network space. With VPC, you can configure logically isolated network space for your resources such as CVMs and cloud databases. This product provides better cloud resource security and can meet your needs in various scenarios.

This document introduces the core components, connection modes, and security of VPCs.

Core Components

A VPC instance has three core components: VPC IP ranges, subnets, and route tables.

VPC IP ranges

When you create a VPC, you need to specify a CIDR (classless inter-domain routing) block as the VPC’s IP address group.

Tencent Cloud VPC supports CIDR blocks in any of the following private IP ranges:

- 10.0.0.0 - 10.255.255.255 (the mask range must be 16 to 28)
- 172.16.0.0 - 172.31.255.255 (the mask range must be 16 to 28)
- 192.168.0.0 - 192.168.255.255 (the mask range must be 16 to 28)

Subnets

A VPC is made up of at least one subnet. All cloud resources in a VPC (such as CVMs and cloud databases) must be deployed in a subnet, and the subnet CIDR block must be within the VPC CIDR block.

A VPC is set up at the region level (such as Guangzhou), while a subnet is set up at the availability zone level (such as Guangzhou Zone 1). You can divide a VPC into one or more subnets. Subnets in the same VPC can interconnect with one another by default, while subnets in different VPCs are
isolated by default.

**Route tables**

When you create a VPC, the system automatically generates a default route table to ensure that all subnets in the VPC interconnected. If the routing policies in the default route table cannot meet your business needs, you can create a custom route table.

For more information on route tables, see [Route Table Overview](#).

**VPC Connections**

Tencent Cloud provides a wide range of VPC connection solutions for different scenarios.

- CVMs and cloud databases in a VPC can connect to the Internet via Elastic IP and NAT Gateway.
- Peering Connection and Cloud Connect Network are used to enable communication between VPCs.
- VPCs and local IDCs are interconnected through VPN Connection, Direct Connect, and Cloud Connect Network.

For more information, see [VPC Connections](#).

**VPC Security**

A VPC is a logically isolated network space in the cloud. Different VPCs are isolated from each other to protect business security.
• Security group: a security group is a stateful virtual firewall capable of packet filtering. It controls inbound and outbound traffic at the instance level and is an important means of network security isolation.

• Network Access Control List (ACL): a network ACL is a stateless virtual firewall for filtering packets at the subnet level. It can be used to control the inbound and outbound data streams of subnets at the protocol and port granularity.

• Cloud Access Management (CAM): CAM helps you securely manage access to your Tencent Cloud resources. For example, CAM provides identity management and policy management so you can control who has access to your VPCs.

For more information on VPC security, see Security.
Strengths

Last updated: 2020-03-04 09:33:21

**Network Customization**

VPC provides you with robust network management capabilities. With them, you can customize IP ranges, perform subnetting as needed such as on a conventional network, and flexibly configure route tables and routing policies to deploy your cloud-based business in a custom fashion. Tencent Cloud VPC also provides visualized network topologies to help you better plan the network.

**Scalability**

By using VPC, you can achieve elastic deployment based on your business needs, create different subnets in one or more VPC instances to deploy different business segments, and expand the network architecture based on your needs by connecting VPC instances with local IDCs, other VPC instances, and basic networks.

**Rich Access Modes**

VPC provides rich access modes to satisfy your demand for cloud-based communication:

- **Access to the Internet**: you can access the Internet by using a common public IP address, elastic public IP address, NAT gateway, or CLB.
- **Access to other VPC instances**: you can access other VPC instances through CCN and peering connections.
- **Access to local IDCs**: you can access your local IDCs through VPN connections, direct connections, and CCN.
- **Access to basic networks**: you can access your business deployed in a basic network through Classiclink.

**Security and Reliability**

Based on the tunneling technology, VPC constructs virtual networks on physical networks and uses the VXLAN protocol to achieve full private network isolation between VPC instances, providing users with independent, isolated, and secure cloud networks.

For CVMs within a VPC, we also provide you with network access control modes at different levels, such as security groups and network ACLs.

**Ease of Use**

You can quickly create and manage VPC instances by using the console, APIs, and other methods. In addition, productized network features and rich troubleshooting features can greatly reduce your
OPS costs.
Use Cases

Accessing the Internet

**Single CVM**

When the traffic to your business is low and only one CVM is available, you can apply for a public IP address and bind it with the CVM to gain access to the Internet.

![Diagram showing VPC, CVM, Subnet, IP, and Internet](image)

**Multiple CVMs**

When you have multiple CVMs that need to access the Internet simultaneously and you do not want the private network addresses of the CVMs to be exposed, you can use [NAT Gateway](#). The NAT gateway provides the SNAT feature and allows multiple CVMs to access the Internet with public IP addresses on the NAT gateway. Moreover, without the configuration of the DNAT feature, external users cannot directly access the NAT gateway, ensuring security. When multiple public IP addresses
exist on the NAT gateway, the NAT gateway automatically performs load balancing.

Providing Services to the Internet

**Single CVM**

You can host services (such as website services) on a VPC-based CVM and use a public IP address to provide services to external users.
Mutiple CVMs

When you have many CVMs for deploying complex services and the Internet traffic is high, you can use the Cloud Load Balancer (CLB). The CLB can automatically distribute application access traffic among CVM instances in the cloud, enhancing fault tolerance for applications.

Disaster Recovery for Applications

Cross-Availability Zone Disaster Recovery

A subnet is associated with an availability zone. You can create subnets in different availability zones of one VPC in a region. By default, different subnets of the same VPC interconnect through the private network. You can deploy resources in subnets of different availability zones to achieve cross-
availability zone disaster recovery.

Cross-Region Disaster Recovery

You can deploy businesses across regions (for example, the 2-region-3-DC solution) to achieve cross-region disaster recovery.

Deploying a Hybrid Cloud

Connecting to Local IDCs

VPC provides multiple connection modes, such as direct connect and VPN connection, which can connect your local IDCs with VPC instances in the cloud to easily create a hybrid cloud architecture. Using local IDCs ensures the security of your core data. You can expand resources (such as CVMs and
TencentDB) in the cloud based on your business volume to reduce IT Ops costs.

**Global Multi-Point Interconnection**

When you have businesses deployed in multiple regions around the world and interconnection among regions is needed, you can use products or features such as **CCN** and **Direct Connect** to enable global multi-point interconnection through single-point access.
Basic Concepts
IP Addresses

Tencent Cloud offers different types of IPs for internet access and private network access. These IPs will not change unless you unbind or change them.

IPs for Internet Access

A public IP address is an IP address in the Internet that is not reserved. A CVM with a public IP address can access other computers in the Internet and can also be accessed by other computers. Tencent Cloud offers public IPs and elastic IPs for internet access.

<table>
<thead>
<tr>
<th>Item</th>
<th>Public IP Address</th>
<th>Elastic IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mutual access to Internet</td>
<td>Both supports mutual access internet.</td>
<td></td>
</tr>
<tr>
<td>How to Obtain</td>
<td>It can only be obtained when you purchase a CVM.</td>
<td>• You can apply for an EIP in the console.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Converting a public IP address to an EIP.</td>
</tr>
<tr>
<td>Features</td>
<td>It’s lifecycle is bound with the CVM, and will be released upon the release of the bound CVM.</td>
<td>• It is independent from other resources. You can bind it to and unbind it from CVMs and NAT gateways at any time.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• You can release it when it's no longer needed.</td>
</tr>
<tr>
<td>Fees</td>
<td>Free of charge</td>
<td>• Bound: the EIP is free of charge when it’s bound with other Tencent Cloud resources (such as a CVM or a NAT gateway).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Not bound: a resource occupation fees will be incurred if the EIP is not bound with any resource.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Released: no fees will be incurred.</td>
</tr>
<tr>
<td>Item</td>
<td>Public IP Address</td>
<td>Elastic IP Address</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Quota</strong></td>
<td>It is subject to the quota of CVMs.</td>
<td>Each account can apply for 20 EIPs in each region.</td>
</tr>
<tr>
<td></td>
<td>For the quota of the public IP addresses for a single CVM, see Quota Details.</td>
<td></td>
</tr>
</tbody>
</table>

| Operations            |                                                                                   |                                                                                   |
| Converting an IP      | A public IP can be converted to an EIP. For details, refer to Converting a public IP to an EIP. When a public IP is converted to an elastic public IP, the IP address will not change. | An EIP cannot be converted into a public IP.                                       |
| Replacing an IP       | Public IPs can be directly replaced. For details, refer to Replacing public IP addresses. | EIPs cannot be directly replaced. You need to unbind and release the EIP, apply for a new one and bind it again. |
| Releasing an IP       | If you no longer need a certain public IP, you can return it in the CVM console by selecting **Operation** > **More** > **IP/ENI** > **Return public IP**. | Release it in the EIP console. For details, refer to Releasing EIPs.                |
| Recovering an IP      | You can recover public IPs/EIPs that you have used if they are not used by other users. For details, refer to Recovering Public IPs. |                                                                                   |

**IPs for Private Network Access**

A private IP address is used to implement Tencent Cloud private network services. It cannot be accessed from internet. Each CVM instance has a default network interface assigned with a private IP (i.e. eth0). The private IP address can be automatically assigned by the system. In a VPC environment, the private IP address can also be customized by the user.

**Attributes**

- Private network services are user-sensitive. Different users are isolated from each other, which means that the cloud services of the other user cannot be accessed via the private network by default.
Private network services are region-sensitive. Different regions are isolated from each other, which means that the cloud services under the same account in a different region cannot be accessed via the private network by default.

**Applicable scenarios**

The private IP can be used for the communication between CLBs and CVM instances, and between CVM instances and other Tencent Cloud services (such as TencentDB).

**Relevant Operations**

- For details on acquiring the private IP address of an instance and setting the DNS, refer to [Acquiring private IP address and setting DNS](#).
- For details on modifying the private IPs of CVM instances in a VPC, refer to [Modifying private IP addresses](#).
Regions and Availability Zones

Last updated: 2020-03-13 12:09:01

Data centers hosted by Tencent Cloud are distributed at multiple locations around the globe. The locations of these nodes are referred to as regions, and each region comprises multiple availability zones.

When creating a VPC, you need to select a region. When creating a subnet, you need to select an availability zone, and subnets must be in the region where the VPC resides. Understanding basic information regarding regions and availability zones helps you better deploy resources in the cloud.

Regions

Tencent Cloud regions are named after the rule of coverage range + city where the data center is located, for example, South China (Guangzhou), East China (Shanghai), and Asia Pacific (Seoul). The coverage range indicates the coverage of the data center. The city indicates the city where the data center is located or the closest city. For the list of regions, see the [List of Tencent Cloud regions and availability zones](#liebiao).

Region features:

- A VPC has the region attribute, and each VPC belongs to only one region.
- Whether in the same region or different regions, different VPC instances are isolated from each other and cannot directly communicate through the private network. If communication between VPC instances is needed, you can use CCN or peering connections.

Availability Zones

Availability zones refer to Tencent Cloud’s physical data centers with power facilities and networks that are independent of each other within the same region. Each region has at least one availability zone. In the following example, four availability zones exist in the Guangzhou region. Establishing multiple availability zones in one region is a way to implement failure isolation between availability zones (with the exception of large-scale disasters or large-scale power outages) so that failures do not spread and users’ businesses are not interrupted.
Availability zone features:

- A subnet of a VPC is associated with an availability zone, and one VPC can concurrently host subnets in different availability zones (for example, the VPC in the Guangzhou region can host subnets in Zone 1, Zone 2, Zone 3, and Zone 4 of the Guangzhou region.)
- Cloud products in the same region and same VPC can interconnect with each other even if they are in different availability zones. For example, subnets in different availability zones of the VPC in the Guangzhou region can directly interconnect with each other through the private network via private IP addresses.
- Resources of different accounts are completely isolated from each other on private networks. You must establish cross-account peering connections to achieve the interconnection of these resources.

Choosing Regions and Availability Zones

When choosing regions and availability zones, you must take the following into consideration:

- The region of the CVM and the geographical locations of you and your target users: we recommend that you select the region closest to your end users to reduce access latency and increase the access speed.
- Relationships between the CVM and other cloud products: we recommend that the selected cloud products reside in the same availability zone of the same region to facilitate interconnection through private networks and to reduce access latency and increase the access speed.
- High availability of services and disaster recovery concerns: even in scenarios with a single VPC, we recommend that you deploy services in different availability zones to guarantee failure isolation between availability zones and to achieve cross-zone disaster recovery.
- Network communication delay may occur between availability zones, and therefore it is necessary to make an assessment based on the actual requirements of services to figure out the optimal balance point between high availability and low latency.
Migrating an Instance to Another Availability Zone

You cannot change the availability zone of an instance that has been launched, but can migrate the instance to another availability zone and keep the current private IP address. The detailed process is as follows:

- Create a custom image from the original instance.
- Use the custom image to launch an instance in the target availability zone.
- Update the configuration of the new instance.

For more detailed steps, see Migrating an Instance to Another Availability Zone.

List of Tencent Cloud Regions and Availability Zones

**China**

<table>
<thead>
<tr>
<th>Region</th>
<th>Availability Zone</th>
</tr>
</thead>
<tbody>
<tr>
<td>South China (Guangzhou) ap-guangzhou</td>
<td>Guangzhou Zone 1 (sold out) ap-guangzhou-1</td>
</tr>
<tr>
<td></td>
<td>Guangzhou Zone 2 ap-guangzhou-2</td>
</tr>
<tr>
<td></td>
<td>Guangzhou Zone 3 ap-guangzhou-3</td>
</tr>
<tr>
<td></td>
<td>Guangzhou Zone 4 ap-guangzhou-4</td>
</tr>
<tr>
<td>South China (Shenzhen Finance) ap-shenzhen-fsi</td>
<td>Shenzhen Finance Zone 1(only for financial institutions and enterprises, and you must submit a ticket to apply for activation) ap-shenzhen-fsi-1</td>
</tr>
<tr>
<td></td>
<td>Shenzhen Finance Zone 2(only for financial institutions and enterprises, and you must submit a ticket to apply for activation) ap-shenzhen-fsi-2</td>
</tr>
<tr>
<td></td>
<td>Shenzhen Finance Zone 3(only for financial institutions and enterprises, and you must submit a ticket to apply for activation) ap-shenzhen-fsi-3</td>
</tr>
<tr>
<td>Region</td>
<td>Zones</td>
</tr>
<tr>
<td>-------------------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>East China (Shanghai)</td>
<td>Shanghai Zone 1 (ap-shanghai-1)</td>
</tr>
<tr>
<td></td>
<td>Shanghai Zone 2 (ap-shanghai-2)</td>
</tr>
<tr>
<td></td>
<td>Shanghai Zone 3 (ap-shanghai-3)</td>
</tr>
<tr>
<td></td>
<td>Shanghai Zone 4 (ap-shanghai-4)</td>
</tr>
<tr>
<td>East China (Shanghai Finance)</td>
<td>Shanghai Finance Zone 1 (ap-shanghai-fsi-1)</td>
</tr>
<tr>
<td></td>
<td>Shanghai Finance Zone 2 (ap-shanghai-fsi-2)</td>
</tr>
<tr>
<td></td>
<td>Shanghai Finance Zone 3 (ap-shanghai-fsi-3)</td>
</tr>
<tr>
<td>East China (Nanjing)</td>
<td>Nanjing Zone 1 (ap-nanjing-1)</td>
</tr>
<tr>
<td></td>
<td>Nanjing Zone 2 (ap-nanjing-2)</td>
</tr>
<tr>
<td>North China (Beijing)</td>
<td>Beijing Zone 1 (ap-beijing-1)</td>
</tr>
<tr>
<td></td>
<td>Beijing Zone 2 (ap-beijing-2)</td>
</tr>
<tr>
<td></td>
<td>Beijing Zone 3 (ap-beijing-3)</td>
</tr>
<tr>
<td></td>
<td>Beijing Zone 4 (ap-beijing-4)</td>
</tr>
<tr>
<td>Southwest China (Chengdu)</td>
<td>Chengdu Zone 1 (ap-chengdu-1)</td>
</tr>
</tbody>
</table>
## Other Regions

<table>
<thead>
<tr>
<th>Region</th>
<th>Availability Zone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Southeast Asia Pacific (Singapore)</td>
<td>Southeast Asia Pacific Region: Singapore Zone 1 (nodes in the Singapore region can be used to cover Southeast Asia Pacific) ap-singapore-1</td>
</tr>
<tr>
<td>ap-singapore</td>
<td></td>
</tr>
<tr>
<td>Northeast Asia Pacific (Seoul)</td>
<td>Northeast Asia Pacific Region: Seoul Zone 1 (nodes in the Seoul region can be used to cover Northeast Asia Pacific) ap-seoul-1</td>
</tr>
<tr>
<td>ap-seoul</td>
<td></td>
</tr>
<tr>
<td>Northeast Asia Pacific (Tokyo)</td>
<td>Northeast Asia Pacific Region: Tokyo Zone 1 (nodes in the Tokyo region can be used to cover Northeast Asia Pacific) ap-tokyo-1</td>
</tr>
<tr>
<td>ap-tokyo</td>
<td></td>
</tr>
<tr>
<td>Southern Asia Pacific (Mumbai)</td>
<td>Southern Asia Pacific Region: Mumbai Zone 1 (nodes in the Mumbai region can be used to cover Southern Asia Pacific) ap-mumbai-1</td>
</tr>
<tr>
<td>ap-mumbai</td>
<td></td>
</tr>
<tr>
<td>Southeast Asia Pacific (Bangkok)</td>
<td>Southeast Asia Pacific Region: Bangkok Zone 1 (nodes in the Bangkok region can be used to cover Southeast Asia Pacific) ap-bangkok-1</td>
</tr>
<tr>
<td>ap-bangkok</td>
<td></td>
</tr>
<tr>
<td>North America (Toronto)</td>
<td>North America (Toronto) Zone 1 (nodes in the Toronto region can be used to cover North America) na-toronto-1</td>
</tr>
<tr>
<td>na-toronto</td>
<td></td>
</tr>
<tr>
<td>Western US (Silicon Valley)</td>
<td>Western US (Silicon Valley) Zone 1 (nodes in the Silicon Valley region can be used to cover Western US) na-siliconvalley-1</td>
</tr>
<tr>
<td>na-siliconvalley</td>
<td></td>
</tr>
<tr>
<td>Region</td>
<td>Zone Details</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Silicon Valley Zone 2</td>
<td>Silicon Valley nodes can be used to cover Western US</td>
</tr>
<tr>
<td>na-siliconvalley-1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Silicon Valley Zone 2 (Silicon Valley nodes can be used to cover Western US)</td>
</tr>
<tr>
<td>na-siliconvalley-2</td>
<td></td>
</tr>
<tr>
<td>Eastern US (Virginia)</td>
<td>Virginia Zone 1 (Virginia nodes can be used to cover Eastern US)</td>
</tr>
<tr>
<td>na-ashburn</td>
<td>na-ashburn-1</td>
</tr>
<tr>
<td></td>
<td>Virginia Zone 1 (Virginia nodes can be used to cover Eastern US)</td>
</tr>
<tr>
<td></td>
<td>na-ashburn-1</td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td>Frankfurt Zone 1 (Frankfurt nodes can be used to cover Europe)</td>
</tr>
<tr>
<td>eu-frankfurt</td>
<td>eu-frankfurt-1</td>
</tr>
<tr>
<td></td>
<td>Frankfurt Zone 1 (Frankfurt nodes can be used to cover Europe)</td>
</tr>
<tr>
<td></td>
<td>eu-frankfurt-1</td>
</tr>
<tr>
<td>Europe (Moscow)</td>
<td>Moscow Zone 1 (Moscow nodes can be used to cover Europe)</td>
</tr>
<tr>
<td>eu-moscow</td>
<td>eu-moscow-1</td>
</tr>
<tr>
<td></td>
<td>Moscow Zone 1 (Moscow nodes can be used to cover Europe)</td>
</tr>
<tr>
<td></td>
<td>eu-moscow-1</td>
</tr>
</tbody>
</table>
A security group is a virtual firewall that features stateful data packet filtering. It is used to configure network access control for instances such as CVMs, CLBs, and TencentDB, in order to control inbound and outbound traffic at the instance level. Therefore, it is an important isolation method for network security.

You can configure security group rules to allow or deny inbound and outbound traffic of instances within the security group.

**Characteristics**

- A security group is a logical group. You can add instances (such as CVMs, ENIs, and TencentDB) with the same network security isolation requirements in the same region to the same security group.
- By default, instances associated with the same security group do not interconnect with each other. Instead, you need to add relevant rules to allow interconnection.
- Security groups are stateful. Allowed inbound traffic is automatically permitted to flow outward and vice versa.
- You can modify security group rules at any time, and the updated rules take effect immediately.

**Security Group Rules**

**Components**

A security group rule consists of the following components:

- Source: indicates the IP address of the source data (inbound) or target data (outbound).
- Protocol type and protocol port: the protocol type can be TCP, UDP, or HTTP.
- Policy: allow or deny the traffic.

**Priorities of rules**

- Security group rules have priorities. The priorities of rules are indicated by their positions in the list. The rule at the top of the list has the highest priority and is the first to be applied. The rule at the bottom has the lowest priority.
In case of rule conflict, the rule that ranks higher in the list prevails by default. When traffic goes in and out, security group rules are one by one from the top to the bottom of the list. If a certain rule is hit, the traffic is permitted, and the system no longer matches it with subsequent rules.

**Multiple security groups**

An instance can be bound with one or more security groups. When the instance is bound with multiple security groups, the system performs rule matching on the groups one by one, from the top down. You can adjust the priorities of security groups at any time.

**Security Group Templates**

When creating a security group, you can use the two security group templates provided by Tencent Cloud.

- Template that opens all ports: all inbound and outbound traffic will be permitted.
- Template that opens major ports: TCP port 22 (for Linux SSH login), ports 80 and 443 (for web services), port 3389 (for Windows remote login), ICMP protocol (for ping commands), and private network ports will be open to traffic.

If the provided security group templates cannot meet your actual needs, you can create custom security groups. For details, see [Creating a Security Group](#) and [Security Group Use Cases](#).
Access Management

Cloud Access Management Overview

If you are using multiple Tencent Cloud services such as VPC, CVM, and TencentDB that are managed by different users sharing your Tencent Cloud account key, you may encounter the following problems:

- Your key is shared by multiple users, which poses a high risk of leakage.
- You cannot limit the access permissions of other users, which poses a security risk due to potential misoperation.

To prevent these problems, you can use sub-accounts to allow different users to manage different services. By default, a sub-account has no permission to use a CVM or CVM-related resources. Therefore, you need to create a policy to grant the required resources or permissions to sub-accounts.

Overview

Cloud Access Management (CAM) is a web service provided by Tencent Cloud to help customers manage the permissions to access resources under their Tencent Cloud accounts in a secure way. You can use CAM to create, manage, and terminate users (or user groups), and use identity management and policy management to control Tencent Cloud resources that can be used by each user.

When using CAM, you can associate a policy to a user or a group of users. The policy can authorize or deny users’ requests of using specified resources to complete specified tasks.

- For more basic information on CAM policies, see Syntax Logic.
- For more usage information on CAM policies, see Policies.

If you do not need to manage the access permissions of sub-accounts for VPC resources, you can skip this section. This will not affect your understanding and usage of other parts in the document.

Getting Started
A CAM policy must authorize or deny the use of one or more VPC operations. At the same time, it must specify the resources (which can be all resources or partial resources for certain operations) that can be used for the operations. The policy can also include the conditions set for the operation resources.

Some VPC API operations support resource-level permissions. That is, when calling these APIs, you cannot specify some resources for the operations. Instead, you must specify all resources for the operations.

<table>
<thead>
<tr>
<th>Task</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic structure of a policy</td>
<td>Policy Syntax</td>
</tr>
<tr>
<td>Define operations in the policy</td>
<td>VPC Operations</td>
</tr>
<tr>
<td>Define resources in the policy</td>
<td>VPC Resource Paths</td>
</tr>
<tr>
<td>Resource-level permissions supported by VPC</td>
<td>Resource-Level Permissions Supported by VPC</td>
</tr>
<tr>
<td>Console example</td>
<td>Console Example</td>
</tr>
</tbody>
</table>
Authorizable Resource Types

Last updated : 2020-04-02 16:08:55

Policy Syntax

CAM policy:

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

- **version** is required. Currently, only the "2.0" value is allowed.
- **statement** describes the details of one or more permissions. This element contains a permission or permission set of other elements such as effect, action, resource, and condition. Each policy has one statement element.
  - **action** describes the action to be allowed or denied. An action can be an API (described using the prefix "name") or a feature set (a set of specific APIs described with the prefix "permid"). This element is required.
  - **resource** describes the details of authorization. A resource is described in a six-piece 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. This element is required.
  - **condition** describes the condition for the policy to take effect. A condition consists of an operator, an action key, and an action value. A condition value may contain information such as the time and IP address. Some services allow you to specify additional values in a condition. This element is optional.
  - **effect** describes whether the result produced by the statement is "allow" or "deny". This element is required.
VPC Operations

In the statement of a CAM policy, you can specify any API action from any service that supports CAM. For VPC, use APIs with the prefix "name/vpc:", for example, name/vpc:Describe or name/vpc:CreateRoute.

To specify multiple actions in a single statement, separate them with commas, as shown below:

```
"action": ["name/vpc:action1","name/vpc:action2"]
```

2. You can also specify multiple actions by using a wildcard. For example, you can specify all actions whose names begin with "Describe", as shown below:

```
"action": ["name/vpc:Describe*"]
```

To specify all actions in VPC, use the wildcard "*" as follows:

```
"action": ["name/vpc:*"]
```

VPC Resource Paths

Each CAM policy statement has its own resources. The general format of a resource path is as follows:

```
qcs::project_id:service_type:region:account:resource
```

- **project_id**: project information. This element is only used to enable compatibility with legacy CAM logic and can be left empty.
- **service_type**: the product abbreviation, such as VPC.
- **region**: region information, such as bj.
- **account**: the root account of the resource owner, such as uin/164256472.
- **resource**: resource details of each product, such as vpc/vpc_id1 or vpc/*. 

For example, you can specify an instance (vpc-d08sl2zr in this case) in the statement, as shown below:

```
"resource": ["qcs::vpc:bj:uin/164256472:instance/vpc-d08sl2zr"]
```

You can also use the wildcard "*" to specify all instances under a specific account, as shown below:
"resource": ["qcs::vpc:bj:uin/164256472:instance/*"]

To specify all resources or if any API action does not support resource-level permissions, you can use the wildcard "+*" in the Resource element, as shown below:

"resource": ["*"]

To specify multiple resources in one instruction, separate them with commas. In the following example, two resources are specified:

"resource": ["resource1", "resource2"]

The following table describes the resources that can be used by VPC and the corresponding methods of describing these resources.

In the following table, the words prefixed with "$" are all alternative names.

- **project** indicates the project ID.
- **region** indicates the region.
- **account** indicates the account ID.

<table>
<thead>
<tr>
<th>Resource</th>
<th>Resource Description Method in the Authorization Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPC</td>
<td>qcs::vpc:$region:$account:vpc/$vpcId</td>
</tr>
<tr>
<td>Subnet</td>
<td>qcs::vpc:$region:$account:subnet/$subnetId</td>
</tr>
<tr>
<td>Security group</td>
<td>qcs::cvm:$region:$account:sg/$sgId</td>
</tr>
<tr>
<td>EIP</td>
<td>qcs::cvm:$region:$account:eip/*</td>
</tr>
</tbody>
</table>