Cloud Virtual Machine

Security and Compliance

Product Documentation

Contents

Security and Compliance
CAM
CAM Overview

Last updated：2024-01-08 09:12:28

If you use multiple Tencent Cloud services such as Cloud Virtual Machine (CVM), VPC, and TencentDB, it is likely they are managed by different users who all your account key. This presents the following challenges:

- Your key is shared by multiple users, leading to high risk of compromise.
- You cannot restrict user access to different resources, which poses a security risk due to potential misoperations.

You can use sub-accounts to solve these issues. Sub-accounts allow you to assign each user a different account so they can perform their duties without the risk of interfering with others. However, sub-accounts by default do not have the permission to access CVM instances and related resources. You need to create appropriate policies for each sub-account to grant them access.
Tencent Cloud provides a web service called Cloud Access Management (CAM) to help customers securely manage access to their resources under their Tencent Cloud accounts. CAM allows you to create, manage, or terminate users and user groups, and provides identity management and policy management to control who is allowed to access and use your Tencent Cloud resources.
You can associate CAM policies with a user or a user group to grant or deny them permissions to use specific resources to perform specific tasks. For more information on CAM policy, see Policy Syntax. For more information on how to use CAM policies, see Policies.
If you do not need to manage multi-user resource access, you can skip this section. Doing so does not affect your understanding of the rest of the article.

Getting started

A CAM policy must allow or deny one or more CVM operations, as well as the resources these actions target. A policy can also include the conditions governing the use of resources.
Some of the CVM APIs do not support resource-level permissions, which means that you must specify all resources, rather than specific resources, when performing such API operations.

Task	Link
Learn more about the basic policy structure	Policy Syntax
Define operations in the policy	CVM Operations
Define resources in the policy	CVM Resource Path

Limit the policy with conditions	CVM Condition Keys
Resource-level permissions supported by CVM	Resource-level Permissions Supported by CVM
Console samples	Console Samples

Authorizable Resource Types

Last updated: 2024-01-08 09:12:28

Resource-level permission refers to the ability to specify which resources users are allowed to operate on. Cloud Virtual Machine(CVM) has partial support for resource-level permission. This means that for certain CVMs, you can control when users are allowed to operate on them, and what specific resources users are allowed to use. For example, you authorize users to perform operations on specific CVMs in Guangzhou.
The types of resources can be authorized in Cloud Access Management (CAM) are as follows:

Resource Type	Resource Description Method in Authorization Policy
CVM Instance	`qcs::cvm:$region::instance/*`
CVM Key	`qcs::cvm:$region::keypair/*`
CVM Image	`qcs::cvm:$region:$account:image/*`

CVM Instance, CVM Key and CVM Image introduce CVM API operations that currently support resource-level permission, as well as resources and condition keys supported by these CVM API operations. When configuring the resource path, you need to change variable parameters such as `$region`, `$account` into your actual parameter information. You can also use wildcard * in the path. For more information, see Operation Examples.

> Note:
> CVM API operations not listed in the table do not support resource-level permission. You can still authorize a user to perform these operations, but you must specify * as the resource element in the policy statement.

CVM Instance

API Operation	Resource Path	Condition Key
DescribeInstanceInternetBandwidthConfigs	`qcs::cvm:$region:$account:instance/*` `qcs::cvm:$region:$account:instance/$instanceId`	cvm:region cvm:zone cvm:instance_type
ModifyInstanceInternetChargeType	`qcs::cvm:$region:$account:instance/*`	cvm:region cvm:zone cvm:instance_type

	qcs::cvm:$region:$account:instance/$instanceId	
ModifyInstancesAttribute	qcs::cvm:$region:$account:instance/* qcs::cvm:$region:$account:instance/$instanceId	cvm:region cvm:zone cvm:instance_type
ModifyInstancesProject	qcs::cvm:$region:$account:instance/* qcs::cvm:$region:$account:instance/$instanceId	cvm:region cvm:zone cvm:instance_type
ModifyInstancesRenewFlag	qcs::cvm:$region:$account:instance/* qcs::cvm:$region:$account:instance/$instanceId	cvm:region cvm:zone cvm:instance_type
RebootInstances	qcs::cvm:$region:$account:instance/* qcs::cvm:$region:$account:instance/$instanceId	cvm:region cvm:zone cvm:instance_type
RenewInstances	qcs::cvm:$region:$account:instance/* qcs::cvm:$region:$account:instance/$instanceId	cvm:region cvm:zone cvm:instance_type
ResetInstance	qcs::cvm:$region:$account:instance/* qcs::cvm:$region:$account:instance/$instanceId qcs::cvm:$region:$account:image/* qcs::cvm:$region:$account:image/$imageId qcs::cvm:$region:$account:keypair/* qcs::cvm:$region:$account:keypair/$keyId qcs::cvm:$region:$account:systemdisk/*	cvm:region cvm:zone cvm:instance_type
ResetInstancesInternetMaxBandwidth	qcs::cvm:$region:$account:instance/*	cvm:region cvm:zone

	qcs::cvm:$region:$account:instance/$instanceId	cvm:instance_type
ResetInstancesPassword	qcs::cvm:$region:$account:instance/* qcs::cvm:$region:$account:instance/$instanceId	cvm:region cvm:zone cvm:instance_type
ResetInstancesType	qcs::cvm:$region:$account:instance/* qcs::cvm:$region:$account:instance/$instanceId	cvm:region cvm:zone cvm:instance_type
ResizeInstanceDisks	qcs::cvm:$region:$account:instance/* qcs::cvm:$region:$account:instance/$instanceId	cvm:region cvm:zone cvm:instance_type
RunInstances	qcs::cvm:$region:$account:instance/* qcs::cvm:$region:$account:image/* qcs::cvm:$region:$account:image/$imageId qcs::cvm:$region:$account:keypair/* qcs::cvm:$region:$account:keypair/$keyId qcs::cvm:$region:$account:sg/* qcs::cvm:$region:$account:sg/$sgId qcs::vpc:$region:$account:subnet/* qcs::vpc:$region:$account:subnet/$subnetId qcs::cvm:$region:$account:systemdisk/* qcs::cvm:$region:$account:datadisk/* qcs::vpc:$region:$account:vpc/* qcs::vpc:$region:$account:vpc/$vpcId	cvm:region cvm:zone cvm:instance_type

StartInstances	qcs::cvm:$region:$account:instance/* qcs::cvm:$region:$account:instance/$instanceId	cvm:region cvm:zone cvm:instance_type
StopInstances	qcs::cvm:$region:$account:instance/* qcs::cvm:$region:$account:instance/$instanceId	cvm:region cvm:zone cvm:instance_type
TerminateInstances	qcs::cvm:$region:$account:instance/* qcs::cvm:$region:$account:instance/$instanceId	cvm:region cvm:zone cvm:instance_type

CVM Key

API Operation	Resource Path	Condition Key
AssociateInstancesKeyPairs	qcs::cvm:$region:$account:instance/* qcs::cvm:$region:$account:instance/$instanceId qcs::cvm:$region:$account:keypair/* qcs::cvm:$region:$account:keypair/$keyId	-
CreateKeyPair	qcs::cvm:$region:$account:keypair/*	-
DeleteKeyPairs	qcs::cvm:$region:$account:keypair/* qcs::cvm:$region:$account:keypair/$keyId	-
DescribeKeyPairs	qcs::cvm:$region:$account:keypair/*	-
DescribeKeyPairsAttribute	qcs::cvm:$region:$account:keypair/* qcs::cvm:$region:$account:keypair/$keyId	-

DisassociateInstancesKeyPairs	qcs::cvm:$region:$account:instance/* qcs::cvm:$region:$account:instance/$instanceId qcs::cvm:$region:$account:keypair/* qcs::cvm:$region:$account:keypair/$keyId	-
ImportKeyPair	qcs::cvm:$region:$account:keypair/*	-
ModifyKeyPairAttribute	qcs::cvm:$region:$account:keypair/* qcs::cvm:$region:$account:keypair/$keyId	-

CVM Image

API Operation	Resource Path	Condition Key
CreateImage	qcs::cvm:$region:$account:instance/* qcs::cvm:$region:$account:instance/$instanceId qcs::cvm:$region:$account:image/*	cvm:region
DeleteImages	qcs::cvm:$region:$account:image/* qcs::cvm:$region:$account:image/$imageId	cvm:region
DescribeImages	qcs::cvm:$region:$account:image/*	cvm:region
DescribeImagesAttribute	qcs::cvm:$region:$account:image/* qcs::cvm:$region:$account:image/$imageId	cvm:region
DescribeImageSharePermission	qcs::cvm:$region:$account:image/*	cvm:region
ModifyImageAttribute	qcs::cvm:$region:$account:image/* qcs::cvm:$region:$account:image/$imageId	cvm:region
ModifyImageSharePermission	qcs::cvm:$region:$account:image/*	cvm:region

	`qcs::cvm:$region:$account:image/$imageId`	
SyncImages	`qcs::cvm:$region:$account:image/*` `qcs::cvm:$region:$account:image/$imageId`	cvm:region

Authorization Policy Syntax

Last updated：2024-01-08 09:12:28

Policy Syntax

CAM policy:

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

- version is required. Currently, only "2.0" is supported.
- statement describes the details of one or more permissions. This element contains a permission or permission set consisting of other elements such as effect, action, resource, and condition. One policy has only one statement.
  1.1 effect describes whether the result produced by the statement is "allowed" (allow) or "denied" (deny). This element is required.
  1.2 Action describes the allowed or denied actions. An action can be an API (described using the prefix "name") or a feature set (a set of specific APIs, described using the prefix "permit"). This element is required.
  1.3 resource describes the authorization details. 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 relevant product. This element is required.
  1.4 condition 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. This element is optional.

CVM Operations

A CAM policy allows you to perform API operations in any Tencent Cloud service that supports CAM. For CVM, use the prefix `name/cvm:` with any API, such as `name/cvm:RunInstances` or `name/cvm:ResetInstancesPassword`.
To specify multiple actions in a single statement, separate them with commas, as shown below:

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

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

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

To specify all CVM operations, use the wildcard "*" as follows:

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

CVM Resource Path

Each CAM policy defines its own resources.
The general format of resource paths is as follows:

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

project_id: project information, which is only used for compatibility purposes and can be left blank.
service_type: abbreviation of a product, such as CVM.
region: region of the resource, such as bj.
account: the root account of the resource owner, such as uin/164256472.
resource: detailed resource information of each product, such as instance/instance_id1 or instance/*.
For example, you can specify a specific instance (i-15931881scv4) in the statement as follows:

```
"resource":[ "qcs::cvm:bj:uin/164256472:instance/i-15931881scv4"]
```

You can also use the wildcard "*" to specify all instances that belong to a specific account as shown below:

```
"resource":[ "qcs::redis:bj:uin/164256472:instance/*"]
```

If you want to specify all resources or if any API operation does not support resource-level permissions, you can use wildcard "*" in `resource` 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 CVM resources and the corresponding resource description methods.
In the following table, names with the prefix $ are placeholders.

- $project is the ID of the project.
- $region is the region of the resource.
- $account is the ID of the account.

Resource	Syntax
Instance	qcs::cvm:$region:$account:instance/$instanceId
Key	qcs::cvm:$region:$account:keypair/$keyId
VPC	qcs::vpc:$region:$account:vpc/$vpcId
Subnet	qcs::vpc:$region:$account:subnet/$subnetId
Image	qcs::cvm:$region:$account:image/*
CBS	qcs::cvm:$region:$account:volume/$diskid
Security group	qcs::cvm:$region:$account:sg/$sgId
EIP	qcs::cvm:$region:$account:eip/*

CVM Condition Keys

You can use conditions to specify the conditions under which policies take effect. Each condition consists of one or more key pairs. These are not case-sensitive.

- If you specify multiple conditions or multiple keys in one condition, they are connected with the logical operator "AND".
- If you specify a key with multiple values in one condition, they are connected with the logical operator "OR".
  The following table describes CVM condition keys for specific services.

Condition key	Reference type	Key pair
cvm:instance_type	String	cvm:instance_type= `instance_type` • `instance_type` is the model of the CVM instance, such as S1.SMALL1.
cvm:image_type	String	cvm:image_type= `image_type` • `image_type` is the type of the image, such as IMAGE_PUBLIC.
vpc:region	String	vpc:region= `region` • `region` is the region of the CVM instance, such as ap-guangzhou.
cvm:disk_size	Integer	cvm:disk_size= `disk_size` • `disk_size` is the size of the disk, such as 500.
cvm:disk_type	String	cvm_disk_type= `disk_type` • `disk_type` is the type of the disk, such as CLOUD_BASIC.
cvm:region	String	cvm:region= `region` `region` is the region of the CVM instance, such as ap-guangzhou.

CVM APIs Supporting CAM

Last updated：2024-01-08 09:12:28

Basic information

Product Name	Abbreviation	Authorization Granularity
Cloud Virtual Machine	CVM	Resource-level

Note:
Three authorization granularity levels are supported by the Tencent Cloud product: 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. The Tencent Cloud product at the service level doesn't support authorization of specific APIs.
- 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. The Tencent Cloud product that supports resource-level API authorization supports resource-level authorization.

API authorization granularity

- Resource-level API: It supports the authorization of a specific resource.
- Operation-level API: It doesn't support the authorization of a specific resource.

For authentication through a resource-level API, the Tencent Cloud product will deliver the six-segment format of the specific resource to CAM for authentication, thereby supporting authorization and authentication of the specific resource.
For authentication through an operation-level API, the Tencent Cloud product will not deliver the six-segment format of the specific resource to CAM for authentication. Instead, it will deliver the `*` of any resource. To be more specific, if a resource is specified in the policy syntax during authorization but not delivered through the API for authentication, CAM will identify the API as out of the authorization scope, that is, having no permission.

CAM Policy Examples

Last updated：2024-01-06 18:00:25

Introduction

You can use Cloud Access Management (CAM) policies to manage user access to resources using the Cloud Virtual Machine (CVM) console. This document provides examples to help you understand how to use the pre-defined CAM policies using the CVM console.

Examples

Read and write (CVM)

If you want to allow a user to create and manage CVM instances, associate the user with the policy named QcloudCVMFullAccess. This policy is designed to grant users the permissions to access all the resources in CVM, Virtual Private Cloud (VPC), Cloud Load Balancer (CLB), and Cloud Monitor.
The detailed steps are as follows:
Refer to Authorization Management for instructions on how to grant the preset policy QcloudCVMFullAccess to a user.

Read-only (CVM)

If you want to allow a user to only query, but not create, delete or start/shutdown CVM instances, associate the user with the policy named QcloudCVMInnerReadOnlyAccess. This policy is designed to grant users the permissions to perform all operations starting with "Describe" and "Inquiry" in CVM. The detailed steps are as follows:
Refer to Authorization Management for instructions on how to grant the preset policy QcloudCVMInnerReadOnlyAccess to a user.

Read-only (CVM and associated resources)

If you want to to allow a user to only query, but not create, delete or start/shut down CVM instances and associated resources (VPC and CLB), associate the user with the policy named QcloudCVMReadOnlyAccess. This policy is designed to grant users the permissions to perform the following operations:

- All operations starting with "Describe" and "Inquiry" in CVM.
- All operations starting with "Describe", "Inquiry", and "Get" in VPC.
- All operations starting with "Describe" in CLB.
- All operations in the Monitor.

The detailed steps are as follows:
Refer to Authorization Management for instructions on how to grant the preset policy

QcloudCVMReadOnlyAccess to a user.

CBS policies

If you want to allow a user to view, create, and use cloud disks on the CVM console, add the following operations to your policy and associate the policy with the user.

- CreateCbsStorages: create a cloud disk.
- AttachCbsStorages: mount the specified cloud disk to the specified CVM.
- DetachCbsStorages: unmount the specified cloud disk.
- ModifyCbsStorageAttributes: modify the name or the project ID of the specified cloud disk.
- DescribeCbsStorages: query the details of a cloud disk.
- DescribeInstancesCbsNum: query the number of mounted cloud disks of a CVM and the maximum number of cloud disks that are allowed to be mounted to the CVM.
- RenewCbsStorage: renew the specified cloud disk.
- ResizeCbsStorage: resize the specified cloud disk.

The detailed steps are as follows:

1. Refer to Policies for information and create a custom policy that grants the permissions to view cloud disk information on the CVM console and to create and use cloud disks.
   Use the following as a syntax reference:

```
{
 "version": "2.0",
 "statement": [
     {
         "effect": "allow",
         "action": [
             "name/cvm:CreateCbsStorages",
             "name/cvm:AttachCbsStorages",
             "name/cvm:DetachCbsStorages",
             "name/cvm:ModifyCbsStorageAttributes",
             "name/cvm:DescribeCbsStorages"
         ],
         "resource": [
             "qcs::cvm::uin/1410643447:*"
         ]
     }
 ]
}
```

2. Find the created policy, and in the “Action” column of the row, click Associate User/Group.
3. In the “Associate User/Group” window, select the user/group you want to associate, and click OK.

Security group policies

To allow a user to view and use security groups on the CVM console, add the following operations to your policy, and associate the policy with the user.

- DeleteSecurityGroup: delete a security group.
- ModifySecurityGroupPolicys: replace all the policies of a security group.
- ModifySingleSecurityGroupPolicy: modify a single policy of a security group.
- CreateSecurityGroupPolicy: create a security group policy.
- DeleteSecurityGroupPolicy: delete a security group policy.
- ModifySecurityGroupAttributes: modify the attributes of a security group.

The detailed steps are as follows:

1. Refer to Policies for information and create a custom policy that grants the permissions to create, delete, and modify security groups on the CVM console.
   Use the following as a syntax reference:

```
{
 "version": "2.0",
 "statement": [
     {
         "action": [
             "name/cvm:ModifySecurityGroupPolicys",
             "name/cvm:ModifySingleSecurityGroupPolicy",
             "name/cvm:CreateSecurityGroupPolicy",
             "name/cvm:DeleteSecurityGroupPolicy"
         ],
         "resource": "*",
         “effect": "allow"
     }
 ]
}
```

2. Find the created policy, and in the “Action” column of the row, click Associate User/Group.
3. In the “Associate User/Group” window, select the user/group you want to authorize, and click OK.

Policy for EIPs

If you want to allow a user to view and use EIPs on the CVM console, add the following operations to your policy, and associate the policy with the user.

- AllocateAddresses: assign an EIP to a VPC or CVM instance.
- AssociateAddress: associate an EIP with an instance or a network interface.
- DescribeAddresses: view EIPs on the CVM console.
- DisassociateAddress: disassociate an EIP from an instance or a network interface.
- ModifyAddressAttribute: modify the attributes of an EIP.
- ReleaseAddresses: release an EIP.

The detailed steps are as follows:

1. Refer to Policies for information and create a custom policy.
   This policy allows users to view an EIP and assign it to and associate it with an instance on the CVM console. Users cannot modify the attributes of the EIP, disassociate it from an instance, or release the EIP. Use the following as a syntax reference:

```
{
 "version": "2.0",
 "statement": [
     {
         "action": [
             "name/cvm:DescribeAddresses",
             "name/cvm:AllocateAddresses",
             "name/cvm:AssociateAddress"
         ],
         "resource": "*",
         “effect": "allow"
     }
 ]
}
```

2. Find the created policy, and in the “Action” column of the row, click Associate User/Group.
3. In the “Associate User/Group” window, select the user/group you want to authorize, and click OK.

Policy for authorizing users to perform operations on specific CVMs

If you want to authorize a user to perform operations on a specific CVM, associate the following policy with the user. The detailed steps are as follows:

1. Refer to Policies for information and create a custom policy.
   This policy authorizes the user to operate a CVM instance with the ID of ins-1 in the Guangzhou region. Use the following as a syntax reference:

```
{
 "version": "2.0",
 "statement": [
     {
         "action": "cvm:*",
         "resource": "qcs::cvm:ap-guangzhou::instance/ins-1",
         “effect": "allow"
     }
 ]
}
```

2. Find the created policy, and in the “Action” column of the row, click Associate User/Group.
3. In the “Associate User/Group” window, select the user/group you want to authorize, and click OK.

Policy for authorizing users to perform operations on the CVMs in a specific region

If you want to authorize a user to perform operations on the CVMs in a specific region, associate the following policy with the user. The detailed steps are as follows:

1. Refer to on Policies for information and create a custom policy.
   This policy authorizes the user to operate CVM instances in the Guangzhou region. Use the following as a syntax reference:

```
{
 "version": "2.0",
 "statement": [
     {
         "action": "cvm:*",
         "resource": "qcs::cvm:ap-guangzhou::*",
         “effect": "allow"
     }
 ]
}
```

2. Find the created policy, and in the “Action” column of the row, click Associate User/Group.
3. In the “Associate User/Group” window, select the user/group you want to authorize, and click OK.

Granting a sub-account all permissions to CVM instances except payment

Assume that the account CompanyExample, whose ownerUin is 12345678, has a sub-account called Developer. Developer requires full management permissions (including all operations such as creation and management) for the CVM instance, except payment, which means Developer can make orders but cannot pay for them.
You can do this by using one of the following two solutions:

- Solution A
  The account owner of CompanyExample associate the preset policy QcloudCVMFullAccess with Developer. For more information, refer to Authorization Management.
- Solution B

1. Use the following as a syntax reference and create a custom policy.

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

2. Associate the policy to the sub-account. For more information, see Authorization Management.

Granting a sub-account the permission to manage projects

Assume that the enterprise account, CompanyExample, with ownerUin of 12345678, has a sub-account called Developer. The owner of CompanyExample wants to allow Developer to manage projects, including assigning and removing resources, on the console.
The detailed steps are as follows:

1. Create a custom policy for project management.
   For more information, refer to Policies.
2. Refer to Authorization Management for information on how to associate the custom policy with the sub-account.
   If you run into permission issues when attempting to view snapshots, images and EIPs, associate preset policies QcloudCVMAccessForNullProject, QcloudCVMOrderAccess, and QcloudCVMLaunchToVPC with the sub-account. For more information on authorization, refer to Authorization Management.

Custom policy

If preset policies cannot meet your requirements, you can create custom policies.
For detailed instructions, refer to Policies.
For more information on CVM policy syntax, refer to Authorization Policy Syntax.

Network Overview

Last updated：2024-01-08 09:12:28

Tencent Cloud offers network infrastructure and security services to ensure your business stays secure, efficient, and flexible.

Encrypted Login

Tencent Cloud provides two encrypted login methods using Login Password and SSH Key. You can use either one of these to connect to your CVM instance. Windows CVM does not support login using SSH keys.

Network access

Tencent Cloud products can communicate with one another using Internet Access or Private Network Access.

- Internet Access: CMV instances and other Tencent Cloud products use Internet access to provide public-facing services. They are assigned public IP addresses to communicate with other computers on the Internet.
- Private Network Access: Tencent Cloud assigns private IP addresses to resources in the same region so they can communicate with one another on the same LAN for free.

Network Environment

Tencent Cloud provides two types of Network Environments: basic network and private networks (VPC).

- Basic network is a shared networking resource pool for all users. We recommend basic network for beginners.
- VPCs are custom network spaces that are logically isolated. You can launch CVM instances on a predefined and customized IP range to isolate your resources from those of other users. We recommend VPCs for users who are comfortable with network administration.

Security Groups

A security group is a stateful virtual firewall capable of filtering. As an important means of network security isolation provided by Tencent Cloud, it can be used to set network access controls for one or more TencentDB instances.
The following is a list of typical security group use cases:

- Create multiple security groups and populate them with different rules.

- Associate one or more security groups with each of your CVM instances. The system uses these security groups to control traffic to your instances and the resources your instances can access.
- Configure your security groups so that only specific IP addresses or security groups can access your instances.

Elastic Public IPs

Elastic Public IPs, or EIPs, are static IP addresses specially designed for cloud computing.
We recommend using EIPs in the following cases:

- An instance can go down for unforeseeable reasons, and the failover instance needs to use the same IP address to provide uninterrupted service.
- An instance does not have a public IP address but still needs a static IP address.

ENIs

An Elastic Network Interface (ENI) is an elastic network interface that can be bound to a CVM instance on a VPC to provide network connection. ENIs can be freely migrated among instances. This is essential when configuring and managing networks and implementing high availability deployments.

Network Environment

Last updated：2024-01-08 09:12:28

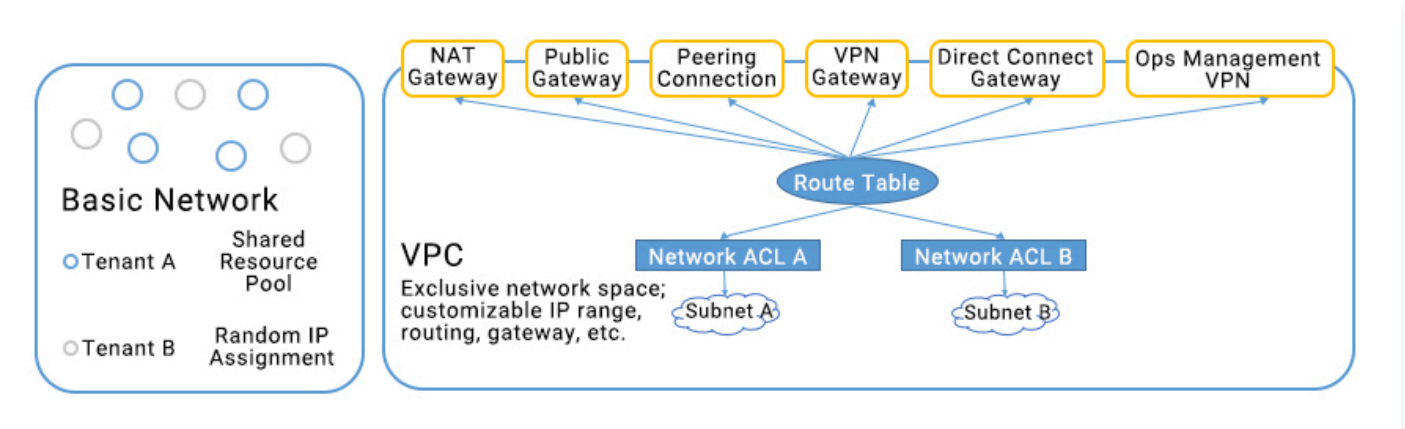
Tencent Cloud provides two network environments, Virtual Private Cloud (VPC) and classic network. For Tencent Cloud accounts created after June 13, 2017, only VPC is available. We recommend you use a VPC for the following reasons:

- Complete features: VPC covers all classic network features, while providing more flexible network services such as custom IP range, routing, Direct Connect, VPN, NAT, etc.
- Smooth migration: There is no completely smooth migration solution in the industry (the need to shut down, change private IP, etc). If you need to use a VPC for business development later, the migration process may affect your business.

VPC and Classic Network

VPC

With Tencent Cloud's Virtual Private Cloud (VPC), you can customize a logical isolated virtual network on the cloud. Even in the same region, different VPCs cannot communicate with each other by default. Similar to the traditional network that you run in your data center, your Tencent Cloud resources, including CVM, Cloud Load Balancer, and TencentDB for MySQL, are hosted on Tencent Cloud's VPC to give you full control over the environment. For more information on configuration and application scenarios, see VPC. The VPC helps you build more complex network architecture and is suitable for those who are familiar with network management.



Classic network

Classic network is the public network resource pool for all Tencent Cloud users. All your Tencent Cloud resources will be centrally managed by Tencent Cloud.

Feature differences

Feature	Classic Network	VPC
Tenant association	Tenant association	Logical isolated network based on GRE encapsulation
Network customization	Not Supported	Supported
Routing customization	Not Supported	Supported
Custom IP	Not Supported	Supported
Interconnection rules	Interconnection is allowed for the same tenant in the same region	Cross-region and cross-account interconnection are supported
Security control	Security groups	Security groups and Network ACL

Sharing Between Classic Network and VPC

Some Tencent Cloud resources and features support both the classic network and VPC, and can be shared or accessed via the two different networks.

Resource	Description
Image	An image can be used to launch a CVM instance in any network environment
Elastic Public IP	Elastic Public IPs can bind to a CVM instance under any network environment
Instances	Instances in the classic network and VPC can communicate with each other through the Public IP or Classiclink
SSH Key	SSH key supports loading a CVM instance under any network environment
Security Groups	Security groups support binding CVM instances under any network environment

Note:
A Cloud Load Balancer can not work on both the classic network and VPC, even if the VPC and the classic network are interconnected.

Migrating from Classic Network to VPC

Please see Switch to VPC to migrate instances in the classic network to VPC.

Private Network Services

Last updated：2025-10-31 17:35:18

Private network services are LAN services, where cloud services can access each other through internal linkages. Tencent Cloud services can access each other through internet access or the private network of Tencent Cloud. Tencent Cloud data centers are interconnected with underlying networks of megabytes/gigabytes. They enable communications via private networks with large bandwidth and low latency, which are free of charge if in the same region to help you build a network architecture flexibly.

Private IP Address

Overview

Private IPs are addresses that cannot be accessed through the Internet. Each instance has a default network interface (i.e., eth0) for assigning private IPs. Private IPs can be automatically assigned by Tencent Cloud, or you can specify on your own (only for VPC environment).

> Note:
> If you change the private IP within the operating system, the private network may be interrupted.

Attributes

- User-level isolation: The private networks of different users are isolated from each other. By default, cloud services of different accounts can not communicate over the private network.
- Regional isolation: The private networks in different regions are isolated from each other. By default, cloud services under the same account in different regions can not communicate over the private network.

Application Scenarios

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).

IP Allocation

Each CVM instance is assigned a default private IP address upon the launch. The private IP varies by the network environment:

- Classic network: private IP address is automatically assigned by Tencent Cloud and cannot be changed.
- VPC: Tencent Cloud VPC CIDR currently allows you to use one of the following IP ranges, and the maximum:

- 10.0.0.0 – 10.255.255.255 (minimum masks are /12 and /28)
- 172.16.0.0 – 172.31.255.255 (minimum masks are /12 and /28)
- 192.168.0.0 – 192.168.255.255 (minimum masks are /16 and /28)

Private Network DNS

DNS Server Address

Private network DNS service is used for domain name resolution. If DNS is configured incorrectly, domain name cannot be accessed.
Tencent Cloud provides reliable private network DNS servers in different regions. Specific configurations are shown below:

Network Environment	Region	Private Network DNS Server
Classic Network	Guangzhou	Guangzhou Zone 1: 10.112.65.31 10.112.65.32
		Guangzhou Zone 3: 10.59.218.193 10.59.218.194
		Guangzhou Zone 4: 100.121.190.140 100.121.190.141
	Shanghai	9.193.104.247 11.122.34.35
	Beijing	10.53.216.182 10.53.216.198
	North America	10.116.19.188 10.116.19.185
	Hong Kong, China	10.243.28.52 10.164.55.3
	Singapore	100.78.90.19 100.78.90.8
	Guangzhou Open Zone	10.59.218.18 10.112.65.51

	Chengdu	100.88.222.14 100.88.222.16
	Silicon Valley	100.102.22.21 100.102.22.30
	Frankfurt	100.120.52.60 100.120.52.61
	Seoul	10.165.180.53 10.165.180.62
VPC	All Regions	183.60.83.19 183.60.82.98

Operation Guide

You can view or modify the private IP address of the instance. For detailed instructions, see:

- Getting Private IP Addresses and Setting DNS
- Modifying Private IP Addresses

Public Network Services

Last updated: 2024-01-08 09:12:28

In order to host public-facing services on your CVM instance, which involves transmitting data over the Internet, you need a public IP address. Tencent Cloud provides Internet access via high-speed connected networks of Tencent Cloud IDC. The domestic multi-line BGP network covers more than 20 network operators and the public network egress can implement cross-region switchover in a matter of seconds. This ensures that your users can enjoy a high-speed and secure network no matter which networks they use.

Public IP address

- Overview: public IP addresses are non-reserved addresses on the Internet. A CVM with a public IP address can access other computers on the Internet and be accessed by other computers.
- Obtaining a public IP address: set your bandwidth to more than 0 Mbps when creating your CVM instance. The system automatically picks a public IP address from the public IP address pool and assigns it to your instance. This address can be changed later. For details, refer to Change Instance Public IP.
- Configuring your CVM instance: you can log in to your CVM instance from a public network to configure it. For more information, refer to Log in to Linux Instances and Log in to Windows Instances.
- Translating your public IP address: you can map your public IP address to the private IP address of your CVM instance using Network Address Translation (NAT).
- Retrieving public IP address information: all Tencent Cloud public network interfaces are managed by Tencent Gateway (TGW), which means all public network interfaces of all CVM instances are maintained by TGW. This process is imperceptible to CVM instances. Therefore, when you run the command `ifconfig` on your Linux CVM instance or `ipconfig` on your Windows CVM instance, you get private IP address information. For information regarding your public IP addresses, log in to your CVM console and check instance detail pages.
- Billing: using public IP addresses to offer services may incur fees. For details, refer to Public Network Billing Methods.

Public IP Address Release

You cannot actively associate or release a public IP address that is already associated with an instance. In the following cases, a public IP address associated with an instance is released or reassigned:

- When you terminate an instance. Tencent Cloud releases a public IP address when you terminate an on-demand CVM instance.

- When you associate or disassociate an Elastic Public IP with an instance. When you associate an EIP with your instance, the existing public IP address is released back into the public IP pool. When you disassociate an EIP from your instance, Tencent Cloud assigns a new public IP address to your instance. You will not be able to use your old public IP address.

If you need a static public IP address, use an Elastic Public IP (EIP).

Operation Guide

For detailed instructions on how to obtain and change your public IP address, refer to:

- Obtaining a Public IP Address of the Instance
- Changing Your Public IP Address

Elastic IP Address

Last updated：2025-08-26 17:25:23

Overview

Elastic IP (EIP) is a regional static IP designed for dynamic cloud computing. With EIP, you can quickly map an address to another instance (or NAT gateway instance) in your account for failure isolation. The lifecycle of a public IP is bound with a CVM, which means that the public IP is released when the associated CVM is terminated. However, the lifecycle of an EIP is independent of the CVM. An EIP is always available under your account unless you release it. If you want to retain a public IP after the termination of the associated CVM, convert it to an EIP.

IP Address Type

Tencent Cloud supports various types of EIPs, such as general BGP IP, premium BGP IP, accelerated IP, and static single-line IP.

- General BGP IP: The domestic multi-line BGP network covers more than twenty ISPs (including the three major ISPs, CERNET, and China Broadnet). The BGP public network outbound supports switchover across regions within seconds, providing your users with high-speed and secure networks.
- Premium BGP IP: The dedicated line that avoids detours through common ISP networks. The latency is lower, It has lower latency, which effectively improves the coverage quality of overseas businesses for users in the Chinese mainland.
- Accelerated IP: Anycast is used for acceleration to ensure more stable and reliable public network access with a low latency.
- Static single-line IP: Users can access the public network using services of a single ISP, featuring low cost and convenient scheduling.
- Anti-DDoS EIP: This type of GBP IP provides Tbps-level cloud-native DDoS protection capability and should be used together with Anti-DDoS Pro for Enterprise. After the IP address is bound to business resources and Anti-DDoS Pro resources, users can enjoy the anti-DDoS capability.

IP Resource Pool

- If certain adjacent IP addresses need to be reserved for your services or IP addresses in a specific network segment should be allocated, you can submit a ticket for consultation. A dedicated IP resource pool will be assigned for you.
- Dedicated resource pools are supported for general and premium BGP IPs and static single-line IPs currently.
- For the fees, please consult your business manager.

Public IP vs EIP

Both public IPs and EIPs are used of internet access.

- Public IP: It is assigned automatically upon the creation of CVM and cannot be unbound from the CVM.
- EIP: It's purchased independently. It can be bound with/unbound from cloud resources (CVM, NAT gateway, ENI, and HAVIP) at any time.

> Note:
> Only general BGP IP lines are applicable for the current common public IP addresses.

For more details about EIPs, see IP Addresses.

Item	Public IP	EIP
Public network access	✓	✓
Independent lifecycle	×	✓
Bind/unbind anytime	×	✓
Adjust bandwidth1	✓	✓
Idle fee	×	✓

> Note:
> In the Public IP console, you can only adjust the bandwidth of EIPs. To adjust the bandwidth of public IPs, see Adjusting Network Configuration.

EIPs can be decoupled from the lifecycle of the cloud resource and operate independently. For example, if you need to keep a certain public IP that is strongly associated with your business, you can change it to an EIP and keep it in your account.

Rules and Limits

Use Rules

- An EIP is applicable to instances in the basic network and VPC, and NAT gateway instances in VPC.
- When you bind an EIP with a CVM instance, the original public IP is released at the same time.
- When a CVM/NAT gateway instance is terminated, it will be disassociated from its EIP.
- For details on EIP billing rules, see Elastic IP Billing.
- For the step-by-step operations of EIPs, see Elastic IP.

Quota

Resource	Quota
EIPs/region	20
Daily purchase (times)	Regional EIP quota * 2
Public IPs assigned due to disassociation of EIPs/day	10

Note:

- By default, the EIP quota cannot be adjusted. You can free some quota by converging IPs in NAT gateway and Cloud Load Balancer.
- If you do need to adjust the quota, submit a ticket or contact your sales rep.

Limits on public IPs bound to CVM

Note:

For CVM instances purchased before 00:00, September 18, 2019, the number of public IPs can be bound to each instance is equal to the number of supported private IPs.

CPU cores	Public IPs + EIPs
1–5	2
6–11	3
12–17	4
18–23	5
24–29	6
30–35	7
36–41	8
42–47	9
⩾ 48	10

Elastic Network Interface

Last updated：2025-11-21 16:21:05

Elastic Network Interface (ENI) is an elastic network interface bound to CVMs in a VPC, which can be migrated among multiple CVMs. ENI is very useful for configuring management networks and establishing highly reliable network solutions.
ENI has VPC, availability zone and subnet attributes. You can only bind it to CVMs under the same availability zone. A CVM can be bound with multiple ENIs, and the maximum number allowed varies by CVM specifications.

Concepts

- Primary ENI and secondary ENI: The ENI created when creating the CVM in a VPC is the primary ENI, and those created by users are secondary ENIs. The primary ENI does not support binding and unbinding, but secondary ENIs do.
- Primary private IP: The primary private IP of an ENI is randomly assigned by the system or customized by users when the ENI is created. You can modify the primary private IP of the primary ENI, but not those of secondary ENIs.
- Secondary private IP: The secondary private IPs bound to the ENI, other than the primary IP, are configured by users when they create or modify the ENI. Users can also bind/unbind these IPs.
- EIP: Bound with private IPs of an ENI one by one.
- Security group: An ENI can be bound with one or more security groups.
- MAC address: An ENI has a globally unique MAC address.

Applications

- Isolation among private network, public network and management network:
  Isolation among private network, public network and management network for secure data transmission is required for the network deployment of key businesses. Different routing policies and security group policies can guarantee data security and network isolation. Like a physical server, CVM can be bound with ENIs residing in different subnets to achieve isolation among three networks.
- Highly reliable application deployment:
  The high availability of key components in the system architecture is ensured through multi-server hot backup. Tencent Cloud provides ENIs and private IPs that can be flexibly bound and unbound. You can configure Keepalived disaster recovery to achieve highly available deployment of key components.

Limits

Based on CPU and memory configurations, the number of ENIs bound to a CVM differs from the number of private IPs bound to an ENI. The quotes are as shown below:

Caution:

The number of IPs that can be bound to a single ENI indicates the upper limit of IPs bound only. The EIP use limits, rather than the upper limit, determines the actual EIP quota.

Number of ENIs bound to a CVM instance

Model	Instance Type	Number of ENIs				
		CPU: 1 core	CPU: 2 cores	CPU: 4 cores	CPU: 6 cores	CPU: 8 cores
Standard	Standard S5	2	4	4	–	6
	Standard Storage Optimized S5se	–	–	4	–	6
	Standard SA2	2	4	4	–	6
	Standard S4	2	4	4	–	6
	Standard Network-optimized SN3ne	2	4	4	–	6
	Standard S3	2	4	4	–	6
	Standard SA1	2	2	4	–	6
	Standard S2	2	4	4	–	6
	Standard S1	2	4	4	–	6
High IO	High IO IT5	–	–	–	–	–

	High IO IT3	–	–	–	–	–
MEM Optimized	Memory Optimized M5	2	4	4	–	6
	Memory Optimized M4	2	4	4	–	6
	Memory Optimized M3	2	4	4	–	6
	Memory Optimized M2	2	4	4	–	6
	Memory Optimized M1	2	4	4	–	6
Compute	Compute Optimized C4	–	–	4	–	6
	Compute Network-optimized CN3	–	–	4	–	6
	Compute C3	–	–	4	–	6
	Compute C2	–	–	4	–	6
GPU-based	GPU Compute GN2	–	–	–	–	–
	GPU Compute GN6	–	–	–	–	–

	GPU Compute GN6S	–	–	4	–	6
	GPU Compute GN7	–	–	4	–	6
	GPU Compute GN8	–	–	–	4	–
	GPU Compute GN10X	–	–	–	–	6
	GPU Compute GN10Xp	–	–	–	–	–
FPGA-based	FPGA Accelerated FX4	–	–	–	–	–
Big Data	Big Data D3	–	–	–	–	6
	Big Data D2	–	–	–	–	6
	Big Data D1	–	–	–	–	6
Cloud Physical Machine 2.0		Not supported				

Number of private IPs bound to a single ENI on CVM instances

Model	Instance Type	Number of private IPs bound to a single ENI				
		CPU: 1 core	CPU: 2 cores	CPU: 4 cores	CPU: 6 cores	CPU: 8 cores

Standard	Standard S5	6	10	10	–	20
	Standard Storage Optimized S5se	–	–	20	–	20
	Standard SA2	6	10	10	–	20
	Standard S4	6	10	10	–	20
	Standard Network–optimized SN3ne	6	10	10	–	20
	Standard S3	6	10	10	–	20
	Standard SA1	1 GB memory: 2>1 GB memory: 6	10	8 GB memory: 1016 GB memory: 20	–	20
	Standard S2	6	10	10	–	20
	Standard S1	6	10	10	–	20
High IO	High IO IT5	–	–	–	–	–
	High IO IT3	–	–	–	–	–
MEM Optimized	Memory Optimized M5	6	10	10	–	20
	Memory Optimized M4	6	10	10	–	20

	Memory Optimized M3	6	10	10	–	20
	Memory Optimized M2	6	10	10	–	20
	Memory Optimized M1	6	10	10	–	20
Compute	Compute Optimized C4	–	–	10	–	20
	Compute Network-optimized CN3	–	–	10	–	20
	Compute C3	–	–	10	–	20
	Compute C2	–	–	10	–	20
GPU-based	GPU Compute GN2	–	–	–	–	–
	GPU Compute GN6	–	–	–	–	–
	GPU Compute GN6S	–	–	10	–	20
	GPU Compute GN7	–	–	10	–	20
	GPU Compute GN8	–	–	–	10	–

	GPU Compute GN10X	–	–	–	–	20
	GPU Compute GN10Xp	–	–	–	–	–
FPGA-based	FPGA Accelerated FX4	–	–	–	–	–
Big Data	Big Data D3	–	–	–	–	20
	Big Data D2	–	–	–	–	20
	Big Data D1	–	–	–	–	20
Cloud Physical Machine 2.0		Not supported				

API Overview

The APIs related to the ENI and CVM are shown in the following table. For more information, see API Category.

Feature	Action ID	Description
Create ENI	CreateNetworkInterface	Create an ENI
Assign Private IP for ENI	AssignPrivateIpAddresses	Assign a private IP for an ENI
Bind ENI to CVM	AttachNetworkInterface	Bind an ENI to a CVM

Configuring the Jumbo Frame Capability

Last updated：2025-06-24 16:04:47

This document describes how to use the jumbo frame capability of CVM instances, including enabling the jumbo frame capability during CVM instance creation and enabling it for existing CVM instances.

Prerequisites

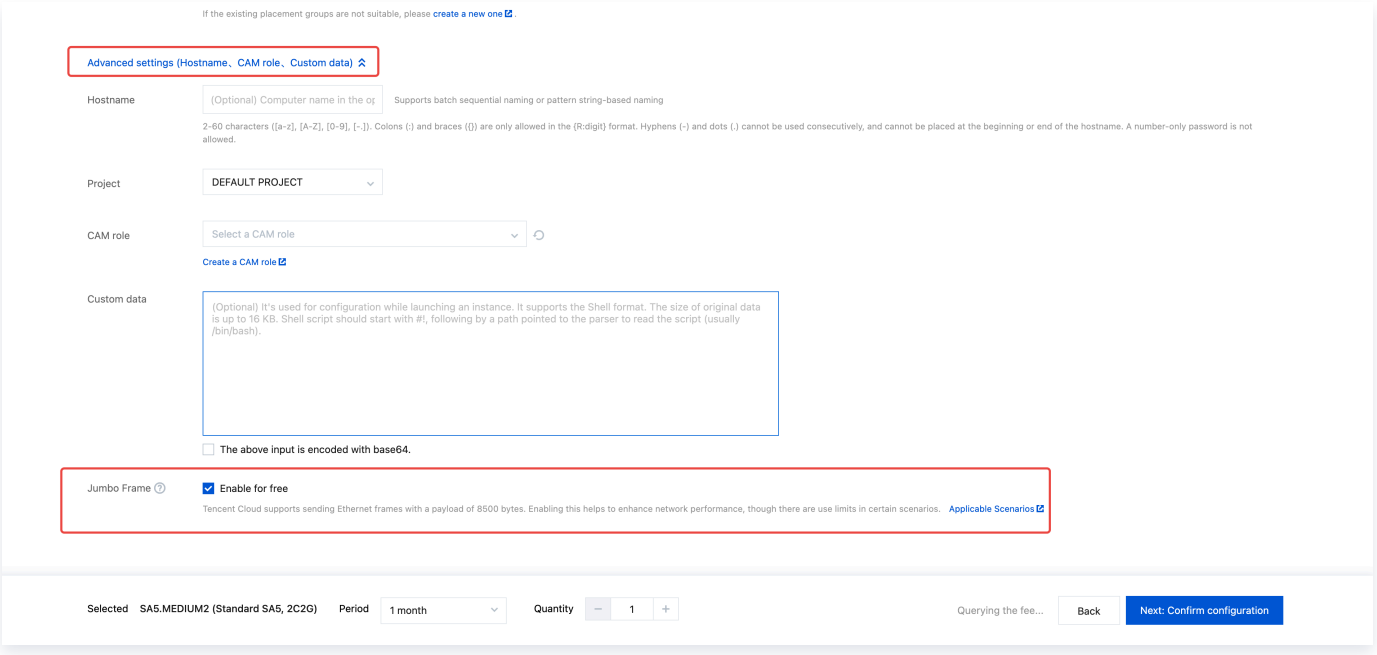
See the Families and Models to determine the CVM models that support the jumbo frame capability.

Directions

Enabling the Jumbo Frame Capability During CVM Instance Purchase

1. Log in to the Tencent Cloud official website, choose Products> Compute > Cloud Virtual Machine, and click Buy Now to enter the CVM instance purchase page.
2. Follow the wizard of Creating Instances via CVM Purchase Page, complete the basic configuration.
3. Enable the jumbo frame capability in the step of network and CVM settings.

   Find the advanced settings, select the jumbo frame enabling option, and click Next: Confirm Configuration.

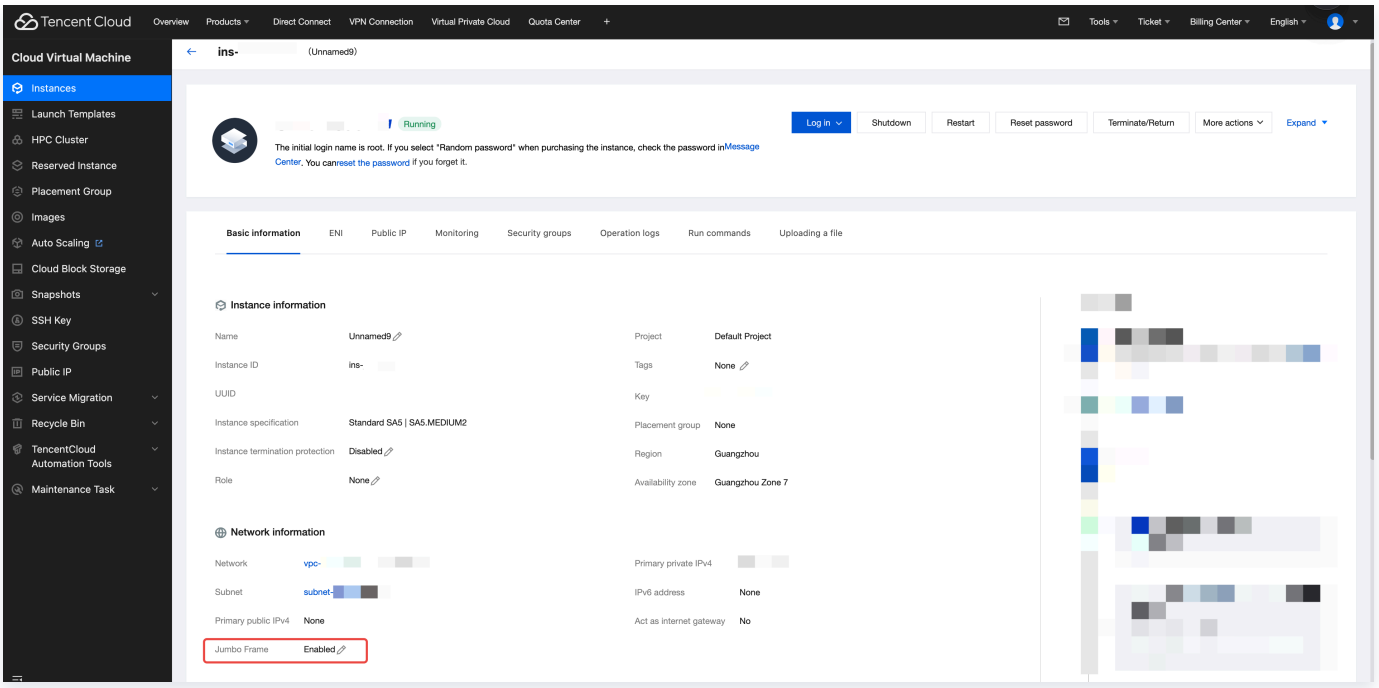


4. Follow the wizard of Creating Instances via CVM Purchase Page to complete the CVM instance purchase.

Enabling/Disabling the Jumbo Frame Capability for Purchased CVM Instances

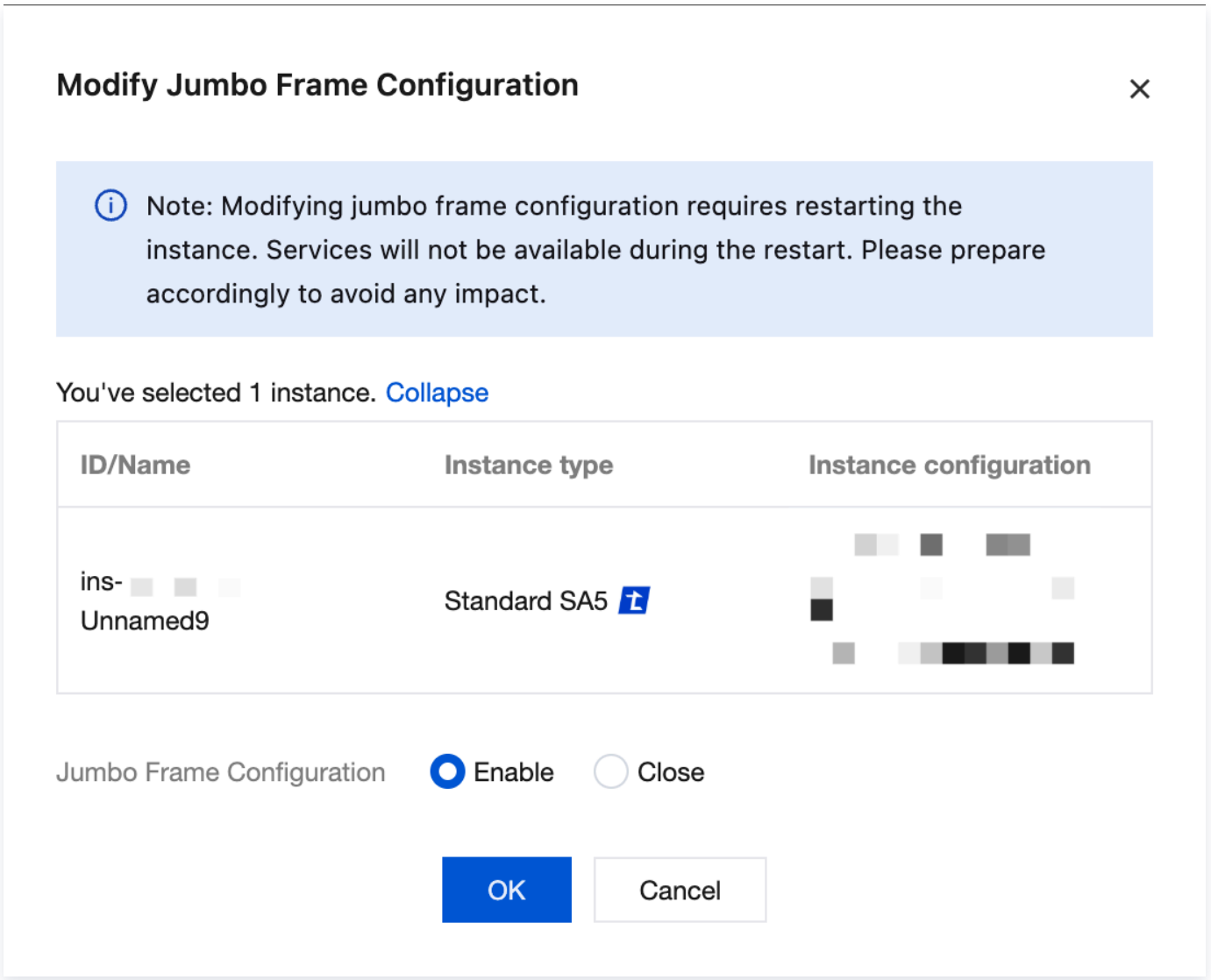
1. Log in to the CVM console and enter the CVM instance list page.

2. Click the name of the target CVM instance to enter the instance details page.
3. Find the jumbo frame field in the network information.



4. Click the editing icon to modify the jumbo frame enabling status, select Enable or Close, and click OK.

> **Note:**
> Modifying the jumbo frame configuration of a CVM instance requires an instance restart. Services are not provided during restart. Please make preparations accordingly to avoid impact.



CWPP

Last updated：2024-01-08 09:12:28

Overview

Based on Tencent Security's massive amounts of threat data, Tencent Cloud Workload Protection Platform (CWPP) leverages machine learning to provide a wide variety of security services ranging from intrusion detection to vulnerability alerting. It offers various security features such as brute force attack prevention, unusual login location reminding, trojan protection, and high-risk vulnerability detection, helping build a security protection system to cope with major network security risks faced by servers and prevent data leakage.
CWPP is available in Basic and Pro editions. When creating a CVM instance, you can choose to activate CWPP Basic by default.

> Note:
> For more information on the features of CWPP Basic and Pro editions and their differences, see Features in Different Editions.

Billing Mode

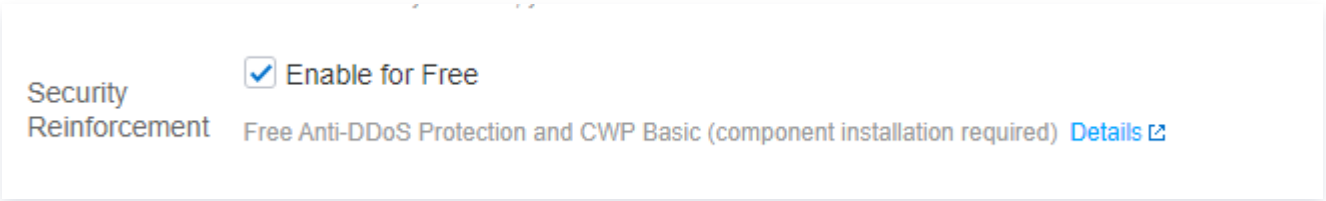
CCWPP Basic is free of charge.

Installing CWPP Basic

You can install CWPP Basic in one of the following methods based on the actual conditions:

Automatic installation during CVM instance creation

When creating a CVM instance, you can choose to activate CWPP Basic by default. On the CVM instance purchase page, select Enable for Free for Security Reinforcement to automatically install CWPP as shown below:



Manual installation for existing CVM instance

You can use one of the following methods to install CWPP for an existing instance based on its operating system:

- Windows CVM environment
- Linux CVM environment

After successful installation, you can view the security status of the CVM instance on the in the CWPP console.

See Also

- Features in Different Editions
- Security Overview

Anti-DDoS Basic

Last updated：2024-01-08 09:12:28

Overview

Anti-DDoS Basic provides CVM, CLB and other resources with free basic protection capability to meet your daily security protection needs. Tencent Cloud will dynamically adjust the blocking threshold according to your security reputation score. Anti-DDoS Basic is enabled by default to monitor network traffic in real time, cleanse attack traffic once detected, and start protection for Public IPs on Tencent Cloud within seconds.

Billing Mode

Anti-DDoS Basic service is free of charge. For details on other DDoS protection schemes, see Comparison of Anti-DDoS Protection Schemes.

Enabling Anti-DDoS Basic

Tencent Cloud CVM can enable Anti-DDoS Basic for free by default when creating an instance. You can click "Security Reinforcement" on the CVM instance purchase page and check "Free Enablement" to enable Anti-DDoS Basic.
After Anti-DDoS Basic is enabled, you can view the protection configuration of CVM on the Overview Page of CVM Console or Anti-DDoS Basic page of DDOS protection console.