Cloud Virtual Machine
Operation Guide

Service Notice

This document provides an overview of the as-is details of Tencent Cloud's products and services in their entirety or part. The descriptions of certain products and services may be subject to adjustments from time to time.

The commercial contract concluded by you and Tencent Cloud will provide the specific types of Tencent Cloud products and services you purchase and the service standards. Unless otherwise agreed upon by both parties, Tencent Cloud does not make any explicit or implied commitments or warranties regarding the content of this document.

Contact Us

We are committed to providing personalized pre-sales consultation and technical after-sale support. Don't hesitate to contact us at 4009100100 or 95716 for any inquiries or concerns.

Contents

Operation Guide
Operation Guide Overview

Last updated: 2024-09-24 16:05:32

This document provides an overview of CVM instances and their use cases. It also describes how to operate CVM instances.

Purchasing and Using a CVM

If this is the first time you are purchasing and using a CVM instance, we recommend following the instructions below to get started.

1. To learn about CVM instances, see CVM Overview.
2. For CVM selection and purchase, if you are an individual user and using it for the first time, we recommend using the quick configuration method: Configuring Windows Instances or Configuring Linux Instances.
3. After completing the purchase, log in to your CVM instance: Depending on the type of CVM you purchased, choose either Logging into Windows Instances or Logging into Linux Instances.
4. (Optional) You can use the purchased CVM instance to build a personal website, forum, or store files.
   - Setting Up a WordPress Personal Website Using an Image
   - Setting Up a Discuz! Forum Using an Image

Adjusting CVM Configurations

You may need to adjust the disk type, network or other configurations of the CVM instance due to changing demands. See the following documents to make corresponding changes.

- Changing Instance Configuration
- Adjusting Network Configuration
- Adjust Project Configuration
- Reinstalling System

Resetting Password and Key

If you forgot your password or lost your key, refer to the following documents to reset the password or key:

- Reset Password
- Create an SSH Key

Renewing Instances and the Billing

- Renew Instance
- Switching from Pay-as-you-go to Monthly Subscription

Creating, Importing or Deleting a Custom Image

Images provide all the information needed to launch a CVM instance. In simple terms, an image is the "installation disk" of a CVM. Tencent Cloud currently offers four types of images: Public Images, Service Marketplace Images, Custom Images, and Shared Images. The following are common operations supported by images.

- Create Custom Images
- Deleting Custom Images
- Importing Images
- Copy Image

Troubleshooting

When you are unable to log in to the CVM instance, or if you are experiencing slow response or other issues, refer to the following for troubleshooting:

- Troubleshooting CVM Login Failures
- Network Latency and Packet Loss in CVM Instances

Use Limits

Last updated: 2024-09-24 09:58:01

Account prerequisites for purchasing CVM instances

- Users need to sign up for a Tencent Cloud account. For registration guidance, please refer to Sign Up for Tencent Cloud.
- Users must complete identity verification. For qualification verification guidance, please refer to Identity Verification Guide.
- If you create a pay-as-you-go CVM, the system will freeze the cost of one-hour CVM usage. Make sure that your account has sufficient balance for the order.

Use limits for CVM instances

- Virtualized software cannot be installed or re-virtualized (such as installing VMware or Hyper-V).
- You cannot use sound cards or mount external hardware devices (such as USB flash drives, external disks, and U-keys).
- The public gateway is available only in Linux operating system.

Purchase limits for CVM instances

- Each user has a quota limit for purchasing monthly-subscribed CVM instances (non-net increase) in each availability zone. You can view the specific quota on the CVM Console Overview page.
- Each user can purchase a varying **total number** of pay-as-you-go CVM instances in each availability zone, ranging from 30 to 60 instances, depending on the actual situation on the CVM purchase page.
- For more information, please refer to CVM Instance Purchase Limits.

Image Limits

- There are no usage restrictions for public images and service marketplace images.
- Custom images: each region supports a maximum of 50 custom images.
- Shared images: each custom image can be shared with a maximum of 50 Tencent Cloud users, and only be shared with accounts in the same region as the source account.
- For more information, please refer to Image Type Restrictions.

Elastic public IP limits

Item	Description
Elastic IP quota restrictions	For more information, please refer to EIP Quota Limits.
Limits on public IPs bound to CVM	For more information, please refer to Binding CVM Limits.

ENI Limits

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

> **Note**
> The number of IPs that can be bound to a single ENI only represents the upper limit, and it does not guarantee the provision of EIP quota up to that limit. The EIP quota for an account is provided according to the EIP Usage Limits.

ENI quota for binding to CVM instances

Model	Instance Type	Number of ENIs									
		CPU: 1 core	CPU: 2 cores	CPU: 4 core	CPU: 6 core	CPU: 8 core	CPU: 10 core	CPU: 12 core	CPU: 14 core	CPU: 16 core	CPU: >16 cores
Standard	Standard S5	2	4	4	–	6	–	–	–	8	8
	Standard Storage Optimized S5se	–	–	4	–	6	–	–	–	8	8
	Instance Types	2	4	4	–	6	–	–	–	8	8
	Standard S4	2	4	4	–	6	–	–	–	8	8
	Standard Network-optimized SN3ne	2	4	4	–	6	–	8	–	8	8
	Standard S3	2	4	4	–	6	–	8	–	8	8
	Standard SA1	2	2	4	–	6	–	–	–	8	8
	Standard S2	2	4	4	–	6	–	8	–	8	8
	Standard S1	2	4	4	–	6	–	8	–	8	8
High IO	High IO IT5	–	–	–	–	–	–	–	–	8	8
	High IO IT3	–	–	–	–	–	–	–	–	8	8
Memory optimized	Memory Optimized M5	2	4	4	–	6	–	8	–	8	8
	MEM optimized M4	2	4	4	–	6	–	8	–	8	8
	MEM optimized M3	2	4	4	–	6	–	8	–	8	8
	MEM optimized	2	4	4	–	6	–	8	–	8	8

	M2										
	MEM optimized M1	2	4	4	–	6	–	8	–	8	8
Compute	Compute Optimized C4	–	–	4	–	6	–	–	–	8	8
	Compute Network-optimized CN3	–	–	4	–	6	–	–	–	8	8
	C3 for computing tasks	–	–	4	–	6	–	–	–	8	8
	C2 for computing tasks	–	–	4	–	6	–	–	–	8	8
GPU	GPU Compute GN6	–	–	–	–	–	–	–	–	–	8
	GPU Compute GN6S	–	–	4	–	6	–	–	–	–	–
	GPU Compute GN7	–	–	4	–	6	–	–	–	–	8
	GPU Compute GN8	–	–	–	4	–	–	–	8	–	8
	GPU Compute GN10X	–	–	–	–	6	–	–	–	–	8
	GPU Compute GN10Xp	–	–	–	–	–	6	–	–	–	8
FPGA-based	FPGA Accelerated FX4	–	–	–	–	–	6	–	–	–	8
Big Data	D3	–	–	–	–	6	–	–	–	8	8
	Big Data D2	–	–	–	–	6	–	–	–	8	8
	D1	–	–	–	–	6	–	–	–	–	8
Cloud Bare Metal		Not supported									

Private IP quota for a single ENI on a CVM instance

Model	Instance Type	Private IPs bound to a single ENI									
		CPU: 1 core	CPU: 2 cores	CPU: 4 core	CPU: 6 core	CPU: 8 core	CPU: 10 core	CPU: 12 core	CPU: 14 core	CPU: 16 core	CPU: >16 cores
Standard	Standard S5	6	10	10	–	20	–	–	–	30	30
	Standard Storage Optimized S5se	–	–	20	–	20	–	–	–	30	30
	Instance Types	6	10	10	–	20	–	–	–	30	30
	Standard S4	6	10	10	–	20	–	–	–	30	30
	Standard Network – optimized SN3ne	6	10	10	–	20	–	30	–	30	30
	Standard S3	6	10	10	–	20	–	30	–	30	30
	Standard SA1	Memory = 1GB: 2; Memory > 1GB: 6	10	8 GB memory: 1016 GB memory: 20	–	20	–	–	–	30	30
	Standard S2	6	10	10	–	20	–	30	–	30	30
	Standard S1	6	10	10	–	20	–	30	–	30	30
High IO	High IO IT5	–	–	–	–	–	–	–	–	30	30
	High IO	–	–	–	–	–	–	–	–	30	30

	IT3										
Memory optimized	Memory Optimized M5	6	10	10	–	20	–	30	–	30	30
	MEM optimized M4	6	10	10	–	20	–	30	–	30	30
	MEM optimized M3	6	10	10	–	20	–	30	–	30	30
	MEM optimized M2	6	10	10	–	20	–	30	–	30	30
	MEM optimized M1	6	10	10	–	20	–	30	–	30	30
Compute	Compute Optimized C4	–	–	10	–	20	–	–	–	30	30
	Compute Network – optimized CN3	–	–	10	–	20	–	–	–	30	30
	C3 for computing tasks	–	–	10	–	20	–	–	–	30	30
	C2 for computing tasks	–	–	10	–	20	–	–	–	30	30
GPU	GPU Compute GN2	–	–	–	–	–	–	–	–	–	30
	GPU Compute GN6	–	–	–	–	–	–	–	–	–	30
	GPU Compute GN6S	–	–	10	–	20	–	–	–	–	–
	GPU Compute GN7	–	–	10	–	20	–	–	–	–	30
	GPU Comput	–	–	–	10	–	–	–	30	–	30

	e GN8										
	GPU Compute GN10X	–	–	–	–	20	–	–	–	–	30
	GPU Compute GN10Xp	–	–	–	–	–	20	–	–	–	30
FPGA – based	FPGA Accelerated FX4	–	–	–	–	–	20	–	–	–	30
Big Data	D3	–	–	–	–	20	–	–	–	30	30
	Big Data D2	–	–	–	–	20	–	–	–	30	30
	D1	–	–	–	–	20	–	–	–	–	30
Cloud Bare Metal	Not supported										

Bandwidth Limits

Outbound Bandwidth Cap (Downstream Bandwidth)

- The following rules apply to instances created after 00:00, February 24, 2020 (UTC +8):

Network Billing Mode	Instance		Maximum Bandwidth(Mbps)
	Instance Billing Method	Instance Configuration	
Bill-by-traffic	Pay-as-you-go Instance	ALL	0 – 100
	Monthly Subscribed Instances	ALL	0 – 200
Bill-by-bandwidth	Pay-as-you-go Instance	ALL	0 – 100
	Monthly Subscribed Instances	ALL	0 – 200 or 0 – 1000, depending on the specific console settings.
Shared Bandwidth	ALL		0 – 2000

- The following rules apply to instances created before 00:00, February 24, 2020 (UTC +8):

Network Billing Mode	Instance		Maximum Bandwidth(Mbps)
	Instance Billing Method	Instance Configuration	

Bill-by-traffic	Pay-as-you-go Instance	ALL	0 – 100
	Monthly Subscribed Instances	Cores ⩽ 8 cores	0 – 200
		8 cores < Number of cores < 24 cores	0 – 400
		Cores ⩾ 24-core	0 – 400 or no speed limit
Bill-by-bandwidth	Pay-as-you-go Instance	ALL	0 – 100
	Monthly Subscribed Instances	Guangzhou Zone 1 Guangzhou Zone 3 Shanghai Zone 1 Hong Kong Zone 1 Toronto Zone 1	0 – 200
		Other Availability Zones	0 – 1000
Shared Bandwidth	ALL		0 – 2000

Inbound Bandwidth Cap (Upstream Bandwidth)

- If the fixed bandwidth purchased by users is greater than 10 Mbps, Tencent Cloud assigns a public network inbound bandwidth that is equal to the purchased bandwidth.
- If the fixed bandwidth purchased by users is less than 10 Mbps, Tencent Cloud assigns 10 Mbps public network inbound bandwidth.

Disk Limits

Item	Description
Elastic cloud disk capability	Since May 2018, data disks purchased with CVM instances are elastic cloud disks, which can be detached from and reattached to CVM instances. This feature is supported in all availability zones.
Cloud disk performances	I/O performance limits apply concurrently. For example, a 1TB SSD cloud disk can achieve a maximum random IOPS of 26,000, which means both read and write IOPS can reach this value. However, due to multiple performance constraints, in this case, using a block size of 4KB/8KB can achieve the maximum IOPS, while using a block size of 16KB cannot reach the maximum IOPS (as the throughput has already reached the 260 MB/s limit).
Max attachable elastic cloud disks per CVM	Up to 20.
Snapshot quota in one region	64 + the number of cloud disks in the region * 64.
Attaching	A cloud disk can only be attached to a CVM in the same availability zone.
Snapshot rollback	Snapshot data can only be rolled back to the source cloud disk where the snapshot was created.

Supported disk type	Only data disk snapshots can be used to create new elastic cloud disks.
Capacity of cloud disk created using a snapshot	The capacity of the cloud disk created using a snapshot should be greater than or equal to that of the snapshot.
Releasing overdue cloud disks	If a monthly subscription elastic cloud disk is not renewed within 7 days after its expiry, it will be moved to the recycle bin. The mounting relationship between the cloud disk and the cloud server will not be actively removed. For specific recycling mechanisms, please refer to Overdue Payment Description. Currently, when a monthly subscription elastic cloud disk is mounted to a monthly subscription cloud server, you can choose from the following renewal methods based on your actual needs: • Unified expiry time with the CVM • Enable monthly auto-renewal of the cloud disks • Attach directly without enabling auto-renewal

Security Group Limits

- Security groups are divided by region. The CVM can only be bound to security groups in the same region.
- Security groups are applicable to any CVM instances located in a network environment.
- Each user can configure a maximum of 50 security groups for each project in a region.
- A maximum of 100 inbound or outbound rules can be set for a security group.
- One CVM can have multiple security groups, and one security group can be associated with multiple CVMs.
- In the **basic network**, security groups bound to CVM instances **cannot filter** data packets from (or to) relational databases (MySQL, MariaDB, SQL Server, PostgreSQL) or NoSQL databases (Redis, Memcached) on Tencent Cloud. To filter traffic for these instances, you can use iptables or purchase a cloud firewall product.
- The quotas are as shown below:

Feature Overview	Restrictions
Number of security groups that can be created per project	50 per region
Number of security group rules	100 entries per inbound direction, 100 entries per outbound direction
Number of Cloud Virtual Machine instances associated with a single security group	2000
Number of security groups that can be associated with each CVM instance	5
Maximum number of security group IDs that can be referenced by a security group	10

VPC Limits

Resources	Limit
Number of VPCs per account per region	20
Number of subnets per VPC	100
Number of classic network CVMs can be associated with each VPC instance	100

Number of route tables per VPC	10
Number of route tables associated with each subnet	1
Number of routing policies per route table	50
Number of default HAVIPs per VPC	10

Convenience Features
Switching Instance Page View in Console

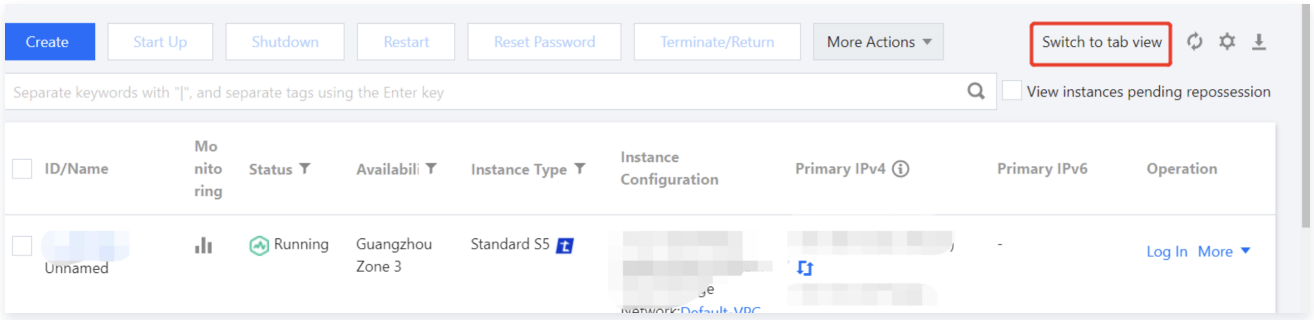
Last updated: 2024-09-24 14:30:23

Scenario

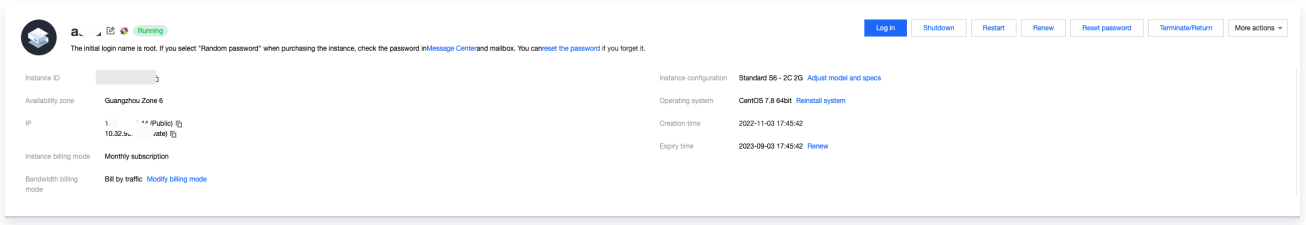
The CVM console instance list page supports both tab and list views. You can refer to this article to switch between page views. The tab view offers advantages such as automatic initiation of self-detection tools, quick access to instance information, and high-frequency operation entry points. It is recommended to use the tab view when you have ⩽ 5 CVM instances.

Instructions

1. Log in to the CVM console and select Instance on the left sidebar.
2. On the **Instance** page, you can select **Switch to tab view** on the right side of the page to switch views, as shown in the image below:



3. After the tab view is switched to successfully, the UI is as follows:
In the tab view, you can quickly get instance health status information and instance details, and work with instances.



> **Note**
> When you have multiple CVM instances, you can select **Switch to list view** on the right side of the page to switch to the list view.

Instance
Create an Instance
Guidelines for Creating Instances

Last updated: 2024-09-24 10:59:11

This document introduces several methods of creating CVM instances, from basic operations to advanced custom features.

- Creating CVM instances via the CVM purchase page is the most commonly used method. It allows you to flexibly select the configurations that meet your business requirements. For more information, see Creating Instances via CVM Purchase Page.
- If you have preferred configurations, such as operating systems and applications, you can create a custom image first and then select it during the instance creation process to improve efficiency. For more information, see Creating Instances via Custom Images.
- If you want to purchase an instance with the same configurations as those of the current instance, you can directly create an instance with the same configurations. For more information, see Purchasing with Same Configurations.

Creating Instances via CVM Purchase Page

Last updated: 2024-06-02 14:38:11

Scenario

This document guides you through how to create a Tencent Cloud Virtual Machine (CVM) instance with custom configurations.

Preparations

Before creating a CVM instance, complete the following steps:

- Sign up for a Tencent Cloud account and complete identity verification.
- To create a CVM instance with a virtual private cloud (VPC) network type, you need to create a VPC in the target region and create a subnet in the target availability zone under the VPC.
- If not using the default project created by the system, you need to create a new project.
- If you do not use the default security group, you need to create a security group in the target region and add a security group rule that meets your business requirements.
- To bind an SSH key pair when creating a Linux instance, you need to create an SSH key for the target project.
- If you need to create a CVM instance with a custom image, you must create a custom image or import an image.

Instructions

1. Log in to the Tencent Cloud official website, select **Products** > **Basic** > **Compute** > Cloud Virtual Machine, **and clickBuy Now** to access the CVM purchase page.
   - Quick Configuration: Suitable for general scenarios, allowing users to quickly select and purchase CVM instances that meet their regular requirements.
   - Custom Configuration: Suitable for specific scenarios, allowing users to select CVM instances tailored to their specific needs.
2. Configure the following information as prompted by the page:

Category	Required/Optional	Configuration Notes
Billing	Required	Select one as needed: • Monthly subscription: A prepaid billing mode for cloud servers, suitable for scenarios where resource demands can be estimated in advance, offering lower prices compared to pay-as-you-go billing. • Pay-as-you-go: A flexible billing mode for cloud servers, suitable for scenarios with sudden and significant fluctuations in demand, such as flash sales. The unit price is higher than that of the monthly/yearly subscription billing mode. • Spot Instance: A new instance operation mode suitable for big data computing, load-balanced online services, and website services, with prices generally ranging from 10% to 20% of the pay-as-you-go rate. For more information about billing modes, see Billing Mode Overview.
Region/Availability Zone	Required	• Region: We recommend you select the region closest to your end users to minimize the access latency and improve the access speed. • Availability zone: Select one as needed. If you want to purchase multiple CVM instances, we recommend you select different AZs to implement disaster recovery.

		For more information about available regions and availability zones, refer to Regions and Availability Zones.
Instance	Required	Tencent Cloud offers various instance types based on different underlying hardware. For more information on instance specifications, see Instance Types.
Video flipping	Required	Tencent Cloud offers public images, custom images, shared images, and image marketplace. You can refer to Image Types for selection.
System disk	Required	The default capacity for installing the operating system is 50 GB. The available cloud disk types may vary depending on the region. Please make your selection based on the actual page prompts. For more information about cloud disks, see Cloud Disk Types.
Data disk	Optional	Cloud disks are used to expand the storage capacity of cloud servers, providing efficient and reliable storage devices. By default, no cloud disk data disk is added. For more information about cloud disks, see Cloud Disk Types.
Period	Required	Applicable only to monthly/yearly subscribed cloud servers. Indicates the duration of cloud server usage.
Amount	Required	It indicates the quantity of CVM instances to be purchased.

3. Click **Next: Configure Network and Host** to enter the host configuration page.
4. Configure the following information as prompted by the page:

Category	Required/Optional	Configuration Notes
Networking	Required	A logically isolated network space built on Tencent Cloud, a VPC consists of at least one subnet. The system provides a default VPC and subnet for you in each region. If the existing VPC or subnet does not meet your requirements, you can create a VPC or subnet in the VPC console. Note • By default, resources in the same VPC are interconnected over the private network. • When purchasing a CVM instance, make sure that the CVM instance and its subnet are in the same AZ.
Public IP	Optional	If your CVM requires public network access, you need to assign a public IP address. You can choose to assign a public IP address when creating the CVM, or configure an Elastic Public IP for it after creation. Note: • The free independent public IP address cannot be unbound from the instance. To unbind the IP address, convert the public IP to an Elastic IP (EIP) and then unbind it. For more information about EIPs, please refer to Elastic Public IPs. • No dedicated public IP can be assigned in the following two cases, subject to the information on the purchase page: ○ The IP resources have been sold out. ○ Resources are only available in certain regions.
Bill-by-bandwidth mode	Required	Tencent Cloud provides two network billing modes. Configure a value greater than 0 Mbps as needed.

		• Bandwidth billing: Choose fixed bandwidth, and packets will be dropped when exceeding this bandwidth. Suitable for scenarios with minimal network fluctuations. • Billing by traffic usage: Charges are based on actual traffic usage. You can limit peak bandwidth to avoid unexpected costs due to traffic spikes. Packet loss will occur when instantaneous bandwidth exceeds this value. Suitable for scenarios with significant network fluctuations. • Bill by Bandwidth Package: When public network traffic peaks are distributed across different time periods, aggregated bandwidth billing can be achieved through shared bandwidth packages. This is suitable for large-scale businesses with staggered traffic between different public network instances. Currently, the bandwidth package billing mode is in beta. To use it, please apply for the beta. For more information, see Public Network Billing.
Bandwidth value	Optional	You can set the public network bandwidth cap for your cloud server as needed. For more information, see Public Network Bandwidth Cap.
IPv6 address	Optional	Enable IPv6 addresses for your CVM instance. For more information, please see Elastic Public IPv6.
Security Group	Required	If you do not have an available security group, you can choose to **Create a New Security Group**. If you have available security groups, you can select **Existing Security Groups**. For more information about security groups, see Security Group.
Tag	Optional	Optionally, add tags to the instance for categorizing, searching, and aggregating cloud resources. For more information, see Tags.
Instance Name	Optional	You can customize the name of the CVM instance to be created. • If no instance name is specified, **Unnamed** will be used by default.An instance name can contain up to 128 characters. Batch sequential naming or pattern string-based naming is also supported. • If an instance name is defined, it must be within 128 characters, and you can also use naming with consecutive numeric suffixes or designated pattern string. Note: This name is displayed only in the console. It is not the hostname of the CVM instance.
Login Options	Required	Configure the method to log in to the CVM as needed. • Set Password: Customize the password for logging in to the instance. • Associate SSH Key (Linux instances only): Link an SSH key for a more secure login to your cloud server. If you don't have a key or the existing key is not suitable, click **Create Now** to create one. For more information on SSH keys, see SSH Keys. • Random Password: An automatically generated password will be sent via the Message Center.
Instance Termination Protection	Optional	By default, this feature is disabled. You can enable instance termination protection based on your needs, which prevents the instance from being terminated through the console or API. For more information about instance termination protection, please refer to Enable Instance Termination Protection.
Security Enhancement	Optional	DDoS protection and Cloud Workload Protection (CWP) are activated by default, helping users build a secure server protection system to prevent data breaches.

Tencent Cloud Observability Platform (TCOP)	Optional	By default, cloud product monitoring is activated for free, and components are installed to obtain server monitoring metrics, which are displayed as monitoring icons. Custom alarm thresholds can also be set. Additionally, it offers comprehensive cloud server data monitoring, intelligent data analysis, real-time fault alarms, and personalized data report configurations, enabling users to accurately control the health of their business and cloud servers.
Automation Assistant	Optional	By default, it is available for free as a native CVM operations and deployment tool. Without the need for remote instance connections, it can automatically execute Shell commands in batches, completing tasks such as running automated operations scripts, polling processes, installing/uninstalling software, updating applications, and installing patches.
Advanced settings	Optional	Configure additional settings for the instance as needed. • Hostname: You can customize the name of the computer in the CVM operating system. After a CVM instance is created, you can log in to it to view the hostname. • Project: The default project is selected. You can select an existing project as needed to manage different CVM instances. • CAM Role: By setting a role, you can grant access permissions to Tencent Cloud services, operations, and resources for the cloud server. For more information, refer to Managing Instance Roles. • Placement Group: If needed, you can add instances to a placement group to improve the availability of your business. For more information, refer to Placement Group for configuration. • Custom Data: Specify custom data to configure the instance, which runs the configured script when the instance starts. If multiple CVMs are purchased at once, the custom data will run on all of them. Linux OS supports Shell format, while Windows OS supports PowerShell format, with a maximum of 16KB of raw data. For more information, refer to Custom Data. Note: Custom data configuration is only supported for some public images with Cloudinit service. For more information, see Cloud-Init.

5. Click **Next: Confirm Configuration Info** to proceed to the confirmation page.
6. Validate the information of the CVM to be purchased and the cost details of each configuration item.
7. If you have purchased a monthly or yearly subscription CVM, you can configure the following settings:

Option	Note
Unify Expiry Date	Unified expiry date allows users to synchronize the expiration time of prepaid devices to the same date each month, making it convenient for users to manage and renew their cloud servers uniformly. • If you have never used the Unified Expiration Date feature, the option will not be displayed on the purchase page. To set it up, please refer to the Unified Expiration Date operation guide. • If you have used the Unified Expiry Date feature before, the purchase page will display a checkbox for it. When purchasing a CVM with this option selected, the duration must be longer than one month. For any partial month, the system will charge you based on the monthly price converted to daily rates. For example, if you purchase a CVM on November 12th with a monthly price of 60CNY/month and a Unified Expiry Date of the 20th of each month, the CVM will expire on December 20th, and you will need to pay 76CNY (60 + 60 ÷ 30 × 8).

Auto-Renewal	Applicable only to monthly-subscribed cloud servers. Select "Auto-renew the device monthly upon expiration if your account has sufficient balance" to avoid manual renewal when the device expires.

8. Read and select "I agree to the Tencent Cloud Terms of Service, Refund Policy, and Tencent Cloud Prohibition of Virtual Currency-related Activities Statement" or "I agree to the Tencent Cloud Terms of Service and Tencent Cloud Prohibition of Virtual Currency-related Activities Statement."
9. You can perform the following operations as needed:
   - Choose **Save as Launch Template**: Save the instance configuration as a launch template, which can be used to quickly create instances. For more information, refer to Managing Instance Launch Templates.
   - Select **Generate API Explorer Best Practice Script**: Generate the OpenAPI best practice script code for the selected configuration, which you can save for purchasing cloud servers with the same configuration. For more information, see Generating Instance Creation API Explorer Best Practice Script.
10. Click **Buy Now** or **Activate** and complete the payment. After the payment is completed, you can access the CVM console to view your CVM instance.
    The instance name, public IP address, private IP address, username, initial login password, and other information will be sent to your account via in-app messages. Use this information to log in and manage your instance, and change your CVM login password as soon as possible to ensure the security of your server.

Creating Instances via Images

Last updated: 2024-09-24 15:06:11

Scenario

You can conveniently create CVM instances with the same operating system, applications, and data using custom images, thereby improving work efficiency or delivery. This guide will walk you through the process of creating instances using custom images.

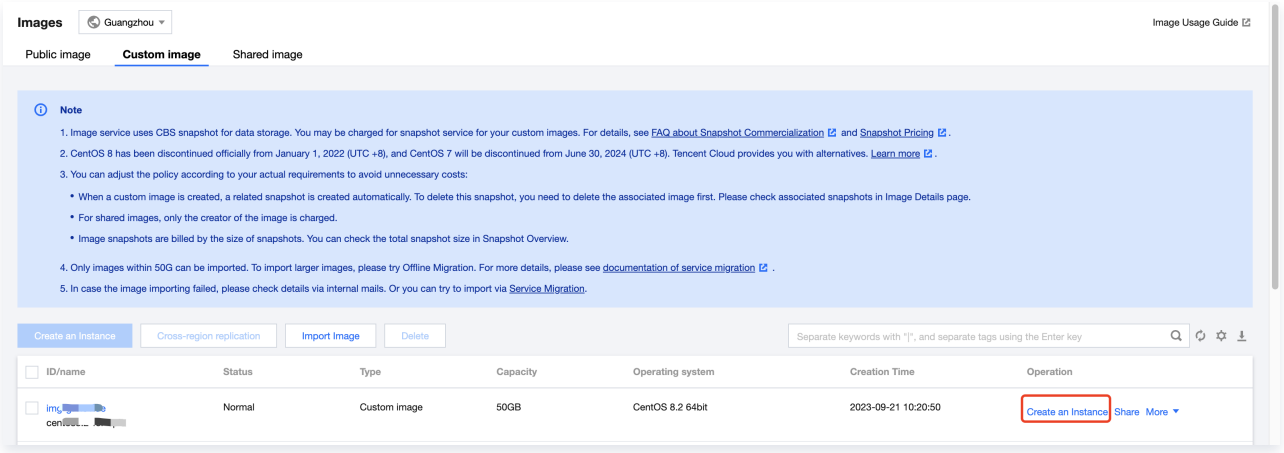
Preparations

You must have a custom image under your account and in the region where you want to create an instance.
If there is no custom image, see the following solutions:

Image Ownership	How to Use
Holding images locally or on other platforms	Import the server system disk image file from a local or another platform into the CVM custom image. For more information, see Importing Image Overview.
No custom image, but an instance is available as a template.	For more information, see Create Custom Images.
Custom images in other regions	Copy the custom image to the target region where you want to create an instance. For more information, see Copying Images.
Custom images under another account	Share the custom image with the account that needs to create an instance. For more information, see Sharing Custom Images.

Instructions

1. Log in to the CVM console.
2. Click **Image** on the left sidebar to enter the image management page.
3. Select a region at the top of the **Image** page.
4. Select a tab based on the image source to view its image list.
   - **Public Image** tab: Navigate to the Public Image interface.
   - **Custom Image** tab: Navigate to the custom image interface.
   - **Shared Images** tab: Navigate to the Shared Images interface.
5. Locate the image you wish to use, and in the operation column, click on **Create an Instance**.



6. In the pop-up prompt, click **Confirm**.

7. Follow the on-screen instructions to configure the instance information and complete the instance creation. The region and image information are automatically filled in. Configure other instance information as needed. For more details, see Creating Instances via CVM Purchase Page.

> **Note**
> If the custom image you choose contains one or more data disk snapshots, the system will automatically create an equal number of cloud disks as data disks based on these snapshots, with each cloud disk having the same capacity as its corresponding snapshot. You can increase the cloud disk capacity, but you cannot decrease it.

Documentation

You can also call the RunInstances API to create an instance by using a custom image.

> **Note**
> If you create an instance using a full-image, first call the DescribeImages API to obtain the snapshot ID associated with the image. Then, pass the snapshot ID parameter when calling the RunInstances API. Otherwise, the created cloud disk and the corresponding snapshot ID will not match, the snapshot data cannot be rolled back, and the data disk will have no data and cannot be mounted properly.

Purchasing Similar Instances

Last updated: 2024-06-02 16:05:32

Scenario

You can use the **Purchase similar** option or an instance launch template in the CVM console to create a CVM instance quickly, so as to save your time and improve the horizontal scaling efficiency.

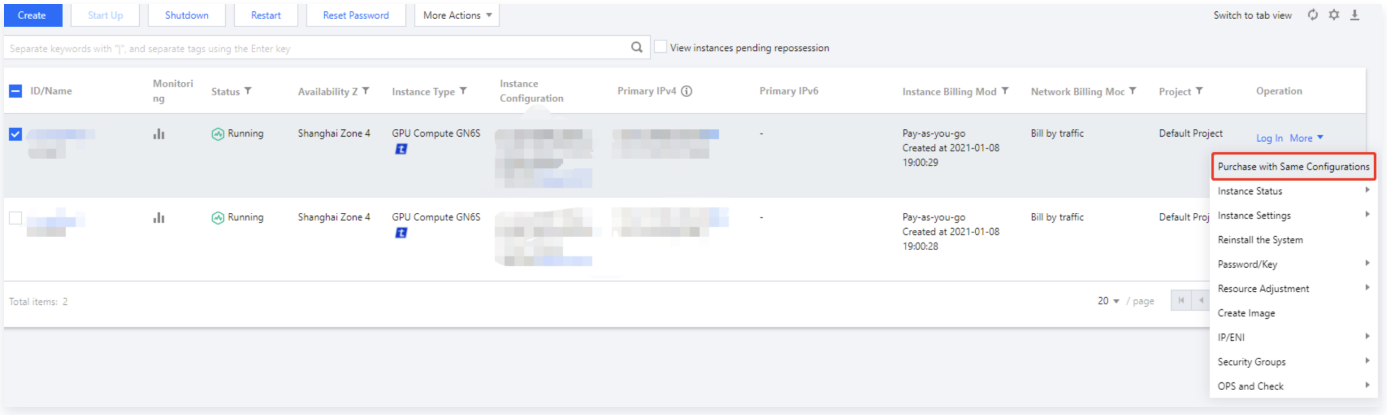
Instructions

Creating instances with the same configuration

1. Log in to the CVM console.
2. Select a region at the top of the **Instances** page.
3. On the instance management page, proceed according to the actually used view mode:

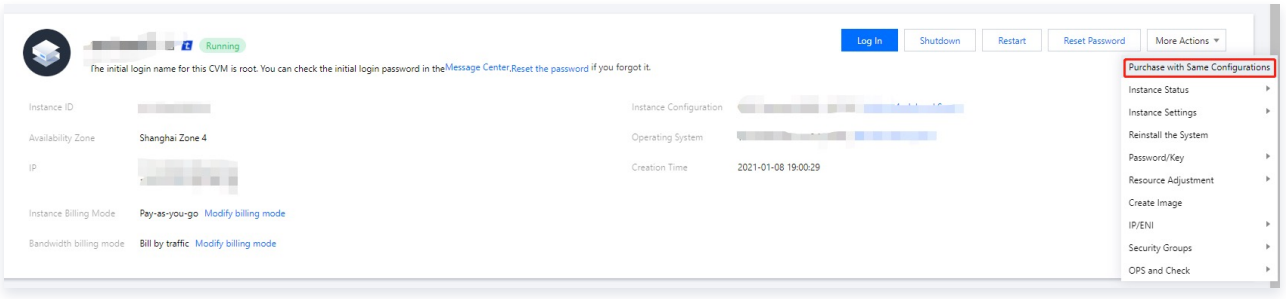
List view

Locate the instance you want to operate on, and click **More** > **Purchase with same Configurations** in the Operation column, as shown below:



Tab view

On the desired instance page, click **More** > **Purchase with same Configurations** in the upper right corner, as shown below:



4. Enter the quantity of CVMs you want to purchase and check the other automatically selected configurations. You can adjust the parameter configurations based on your actual needs.

5. Read and select "I agree to the Tencent Cloud Terms of Service, Refund Policy, and Tencent Cloud Prohibition of Virtual Currency-related Activities Statement" or "I agree to the Tencent Cloud Terms of Service and Tencent Cloud Prohibition of Virtual Currency-related Activities Statement."
6. Click **Buy Now** or **Activate** to complete the payment.

Using a launch template to create instances

To create instances quickly using an existing instance launch template, refer to Using Instance Launch Template to Create Instances.

Generating API Explorer Reusable Scripts to Create Instances

Last updated: 2024-05-15 10:25:41

Scenario

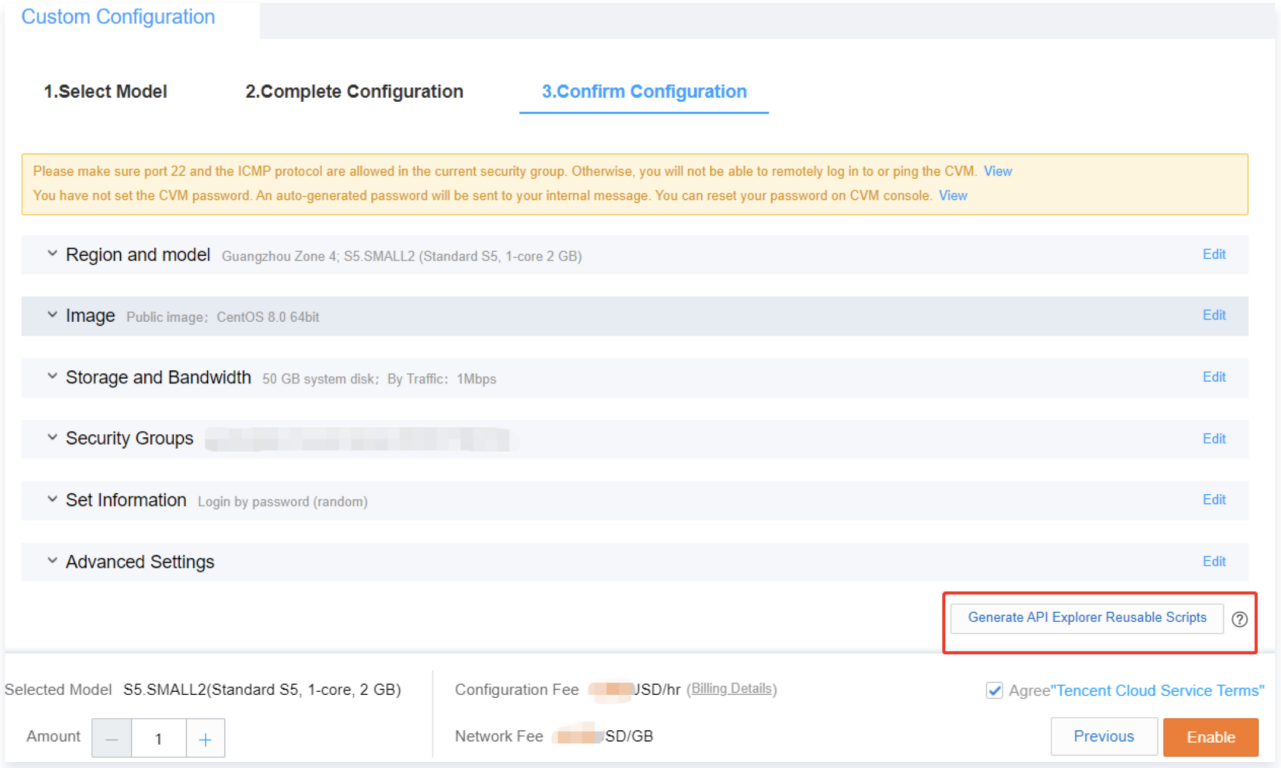
Tencent Cloud supports generating OpenAPI best practices to create instances with the selected configurations on the CVM purchase page. This feature helps you purchase CVM instances that contain the same configurations.

Preparations

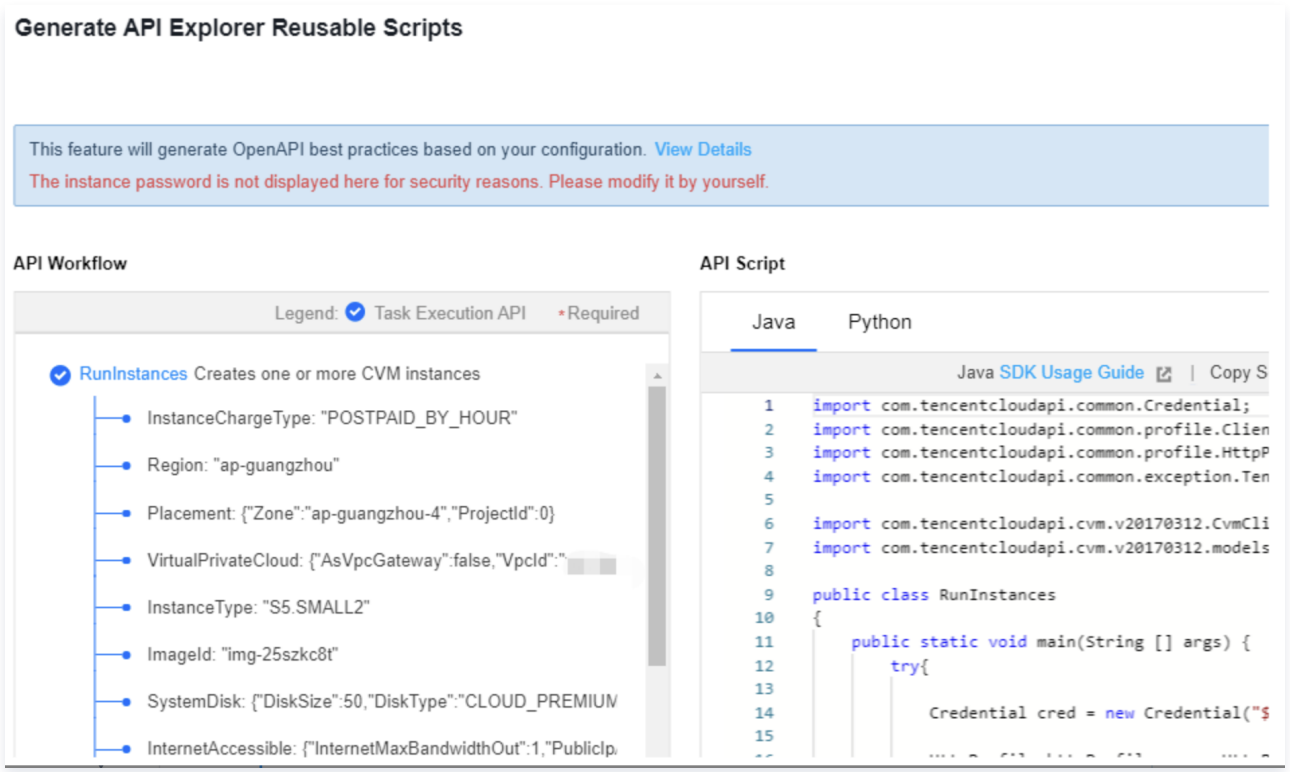
- Log in to the Tencent Cloud console and navigate to the CVM Custom Configuration Purchase page.
- You have selected the desired CVM configurations and proceeded to the configuration confirmation page. To learn more about the configuration options when purchasing a CVM, please refer to Creating Instances via CVM Purchase Page.

Instructions

1. On the configuration confirmation page, click **Generate API Explorer Reusable Scripts**. As shown below:



2. In the **Generate API Explorer Reusable Scripts** pop-up window, you can view the following information, as shown in the figure below:



- **API Workflow**: You can view the RunInstances API and the actual parameters corresponding to the selected configurations. Parameters marked with `*` are required for this API. For data that is not fully displayed in the window, you can hover your mouse over the data to view the corresponding content.
- **API Script**: You can choose either Java or Python as the scripting language for generating the code. Click **Copy Script** in the upper right corner to obtain the script code, which can be saved and used for purchasing CVM instances with the same configurations.

Note

- The instance password will not be displayed on the page or script codes for security reasons. Please modify it by yourself.
- The collective expiry date cannot be set in the API Explorer reusable script. You need to set it after creating the CVM.

Batch Sequential Naming or Pattern String-Based Naming

Last updated: 2023-10-08 15:42:31

Scenario

To allow you to name batch created instances/hosts according to a rule during creation, the features of automatically incrementing suffixed numbers and specifying pattern strings are provided.

- When you need to purchase n instances and want to generate instance/host names similar to "CVM+Sequence number" (i.e., instance/host names like CVM1, CVM2, CVM3, etc.), you can achieve this by using the automatically incrementing suffixed numbers feature.
- When you need to create n instances and specify their names/hosts with incrementing serial numbers starting from x, you can achieve this by using the specifying one pattern string feature.
- When you need to create n instances/hosts with multiple prefixes in their names, each of which contains a specified serial number, you can use the feature of Specifying Multiple Pattern Strings.

Application Scope

This document is applicable to both **Setting Instance Names** and **Setting Host Names**.

Instructions

> **Note**
> This document uses setting instance name as an example. The procedure may vary slightly according to the name type.

Automatically incrementing suffixed numbers

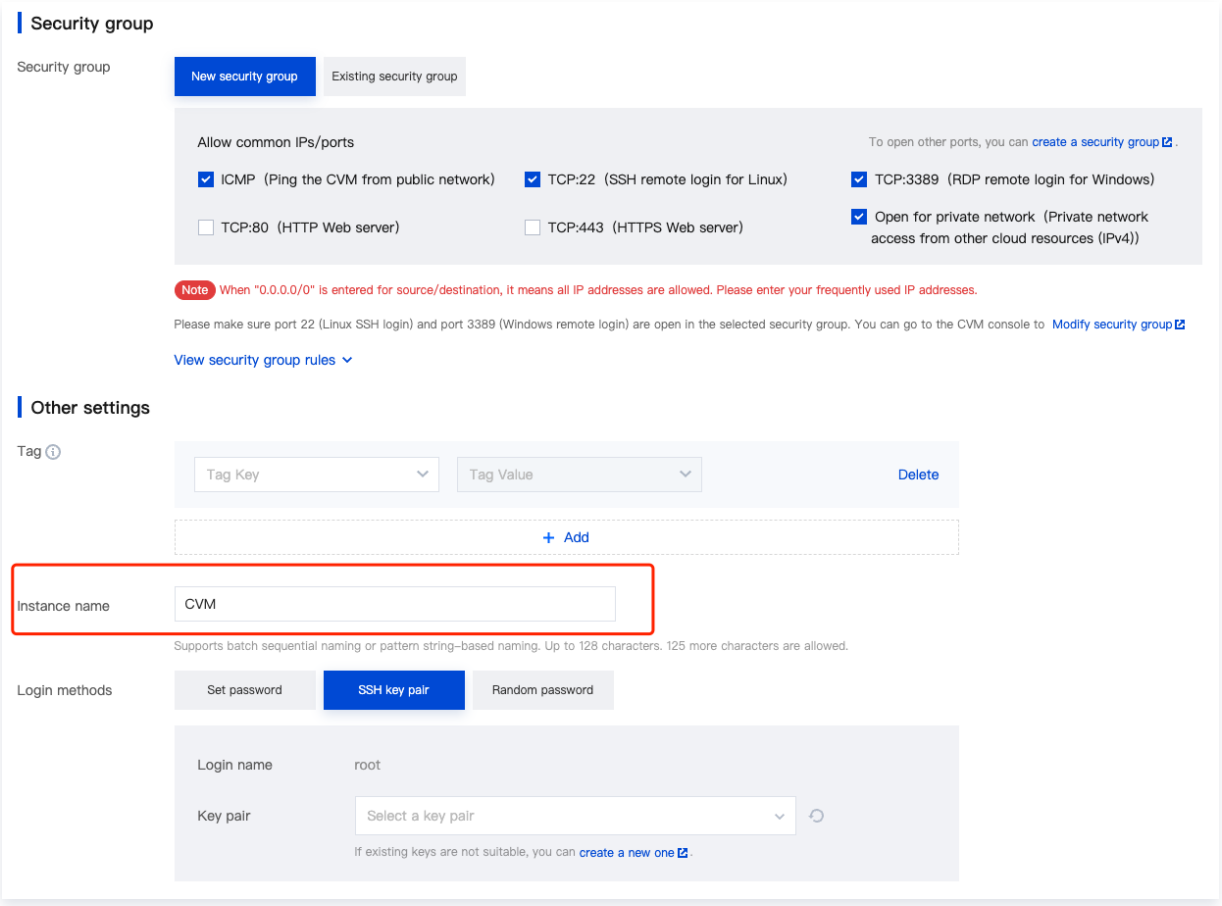
This feature allows you to name batch purchased instances with the same prefix and automatically incrementing suffixed numbers.

> **Note**
> The created instances are suffixed with numbers starting from 1 by default. You cannot specify the starting number.

The following example assumes that you have purchased three instances and want to name these instances in the form of "CVM+Sequence number" (for example, CVM 1, CVM 2, and CVM 3).

Purchase Page Operations

1. Refer to Creating Instances to purchase three instances. In **Setting Network and Host**, enter the instance name using the **prefix+serial number** naming rule, i.e., set the instance name as CVM. As shown in the following image:



2. Follow the prompts on the page and complete payment.

Configuring using API

In the RunInstances API, set the relevant fields:

- Instance Name: Set the InstanceName field to `CVM`.
- Host Name: Set the HostName field to `CVM`.

Specifying the pattern string

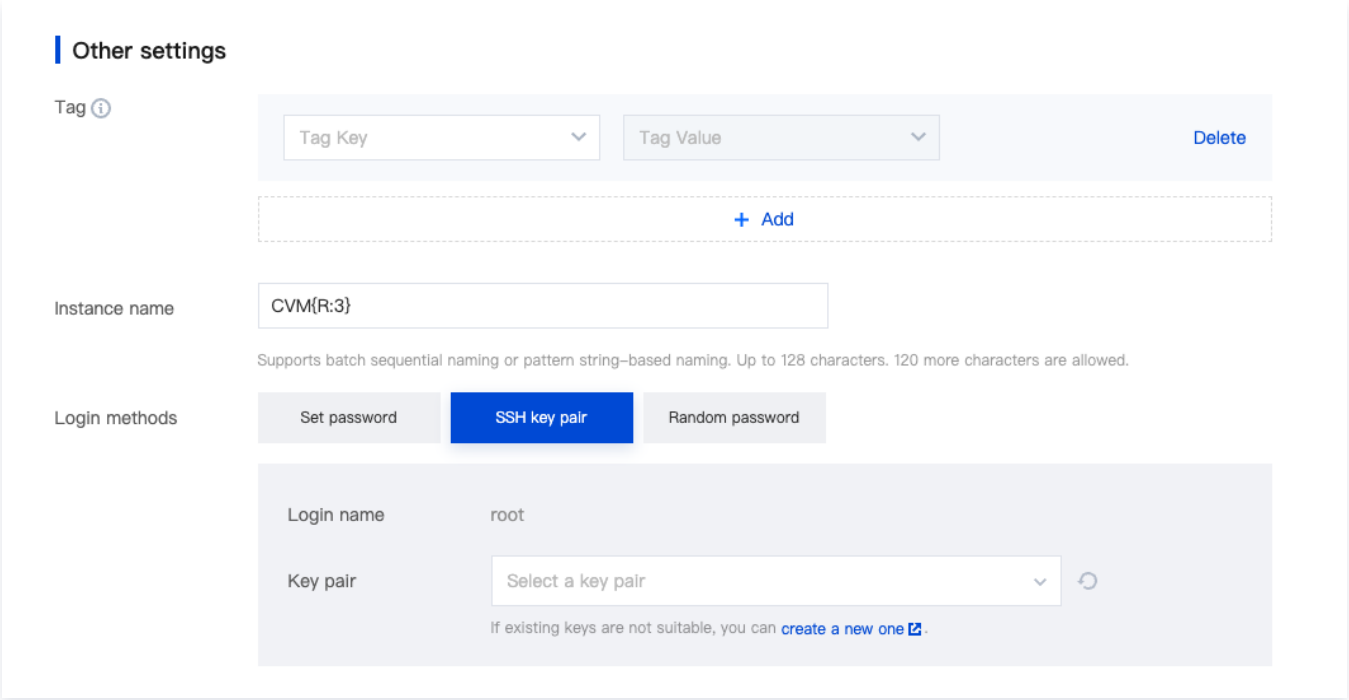
This feature allows you to name batch purchased instances in a complex format with specified serial numbers. You can use one or more pattern strings in instance names as needed.
The naming format for specifying a pattern string is **{R:x}**, where x represents the initial serial number for generating instance names.

Specifying one pattern string

The following example assumes that you want to create three instances and name them with ascending numbers starting from 3.

Purchase Page Operations

1. Refer to Creating Instance to purchase instances. In the "Configure Network and Host" section, enter the instance name using the naming rule **"prefix+specified pattern string {R:x}"**. In this case, enter `CVM{R:3}` as the instance name, as shown in the image below:



2. Follow the prompts on the page and complete payment.

Configuring using API

In the RunInstances API, set the relevant fields:

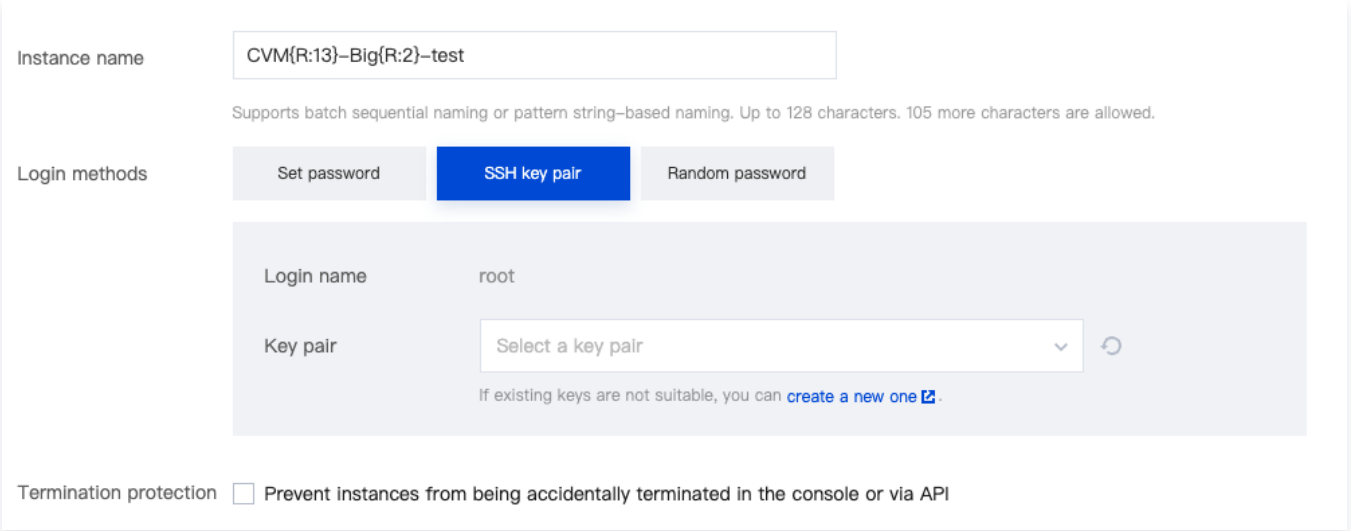
- Instance Name: Set the InstanceName field to `CVM{R:3}`.
- Host Name: Set the HostName field to `CVM{R:3}`.

Specifying multiple pattern strings

The following example assumes that you want to create three instances and name them with the **cvm**, **Big**, and **test** prefixes, where **cvm** and **Big** are followed by ascending numbers starting from 13 and 2, respectively. For example, their names are cvm13-Big2-test, cvm14-Big3-test, and cvm15-Big4-test, respectively.

Purchase Page Operations

1. Refer to Creating Instance to purchase 3 instances. In the "Configure Network and Host" section, enter the instance name in the format of **"prefix+specified pattern string {R:x}-prefix+specified pattern string {R:x}-prefix"**. In this case, enter `cvm{R:13}-Big{R:2}-test` as the instance name. See the image below:



2. Follow the prompts on the page and complete payment.

Configuring using API

In the RunInstances API, set the relevant fields:

- Instance Name: Set the InstanceName field to `cvm{R:13}-Big{R:2}-test`.
- Host Name: Set the HostName field to `cvm{R:13}-Big{R:2}-test`.

Feature Verification

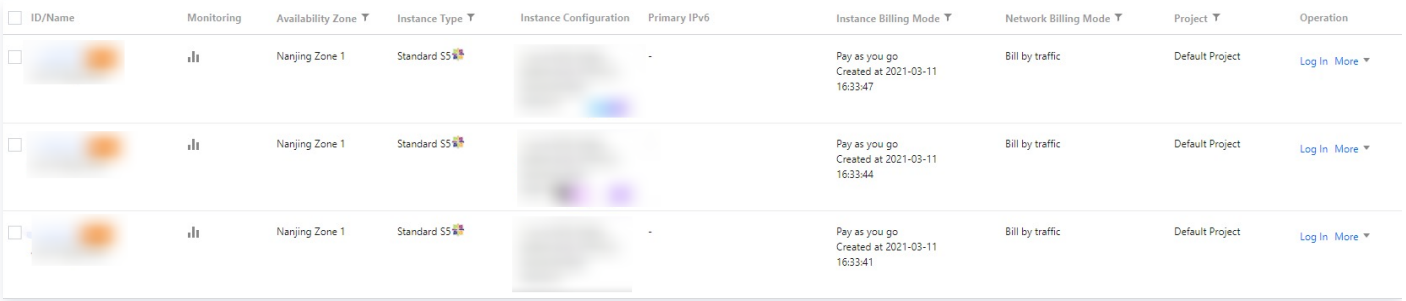
After you batch create instances through automatically incrementing suffixed numbers or specifying pattern string, you can verify the feature as follows:

Verifying instance name

Log in to the CVM console and view the newly created instances. You can see that the batch purchased instances are named according to the rule.

Verifying host name

1. Restart and log in to the CVM instance.



2. Select different steps according to the instance's operating system:

Linux Instances

On the operating system UI, run the following commands:

```
hostname
```

Windows Instances

Open the command line tool and run the following command:

```
hostname
```

3. View the returned result of the `hostname` command.
   If the returned result is similar to the following, the setting is successful.

```
cvm13-Big2-test
```

4. Repeat Step 1 – Step 3 to sequentially verify other instances purchased in batches.

Logging in To a Linux Instance
Logging in To Linux Instance (Web Shell)

Last updated: 2024-09-24 10:24:31

This article explains how to log in to a Linux instance using the standard login method (OrcaTerm).

Scenario

OrcaTerm is the recommended login method by Tencent Cloud. Regardless of whether your local system is Windows, Linux, or MacOS, as long as the instance has a public IP, you can log in via OrcaTerm. The advantages of OrcaTerm are as follows:

- Supports copy and paste operations with shortcut keys.
- Supports scrolling with mouse wheel.
- Supports Chinese input.
- Features a high security (password or key is required for each login).

Authentication Method

Password or **Key**

Preparations

- You have already obtained the administrator account and password (or key) for logging in to the Linux instance.
  - If you chose to have the system generate a random password when creating the instance, please go to Message Center (marked with: Cloud Server Creation Successful) to obtain it.
  - If you have set a login password, please use it to log in. If you have forgotten the password, you can reset the instance password.
  - If a key has already been bound to the instance, you can log in using the key. For more information about keys, please refer to SSH Key.
- Your cloud server instance has a public IP, and the remote login port (default is 22) for the OrcaTerm proxy IP has been allowed in the security group associated with the instance.
  - If you purchase a CVM instance through quick configuration, the port is opened by default.
  - If you purchase a CVM instance through custom configuration, you can manually open the port as instructed in Allowing SSH Remote Connection to Linux CVM.

Instructions

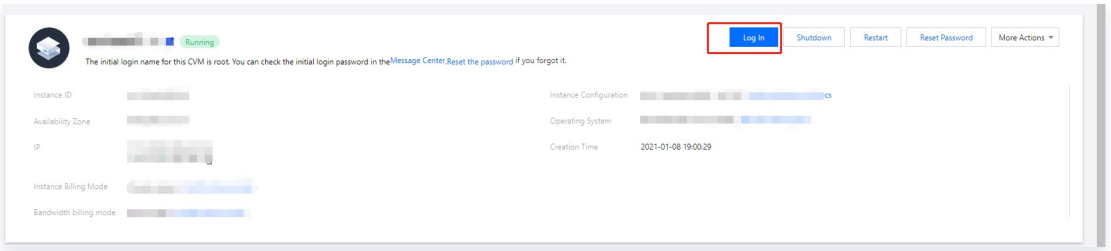
1. Log in to the CVM console.
2. On the instance management page, proceed according to the actually used view mode:

List view

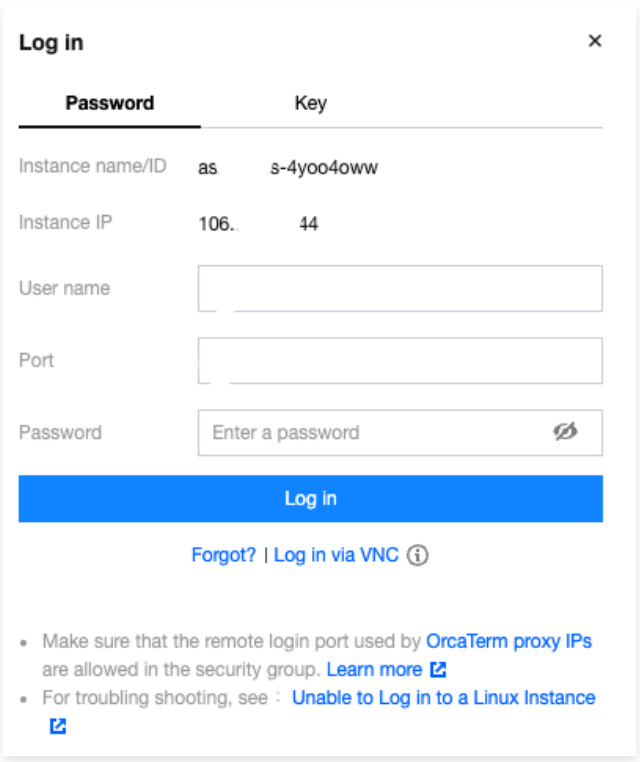
Locate the Linux CVM you want to log in to and click **Log in** on the right side, as shown in the image below:

Tab view

Select the Linux CVM tab you want to log in to and click **Log in**. As shown in the figure below:



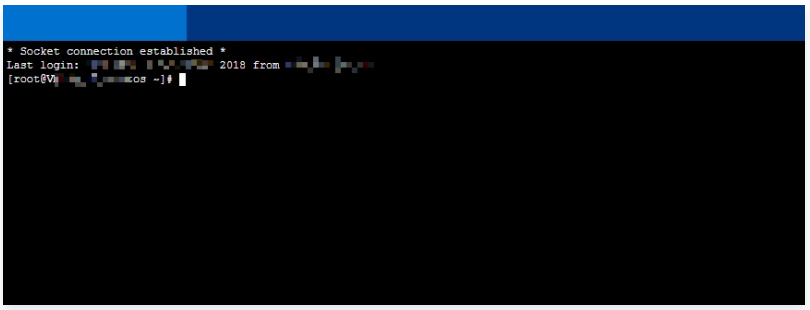
3. In the opened **Log in** window, choose either **Password Login** or **Key Login** based on your actual needs. As shown in the following figure:



4. Please refer to the following instructions to fill in the required login information:
   - **User name**: The default username for Linux instances is `root` (for Ubuntu systems, the default username is `ubuntu`). Please fill in as required.
   - **Port**: The default is 22; please fill in as needed.

     > **Note:**
     > In case the IP is blocked, please change the IP description.

   - **Password**: Enter the login password obtained from the Preparations step.
   - **Key**: Select the key bound to the instance.
5. Click **Login** to access the Linux instance.
   If the login is successful, the OrcaTerm interface will display the following prompt, as shown in the image below:



See Also

Once you have successfully logged in to the cloud server, you can set up a personal website, forum, or perform other operations on the Tencent Cloud server. For related operations, please refer to:

- Manually Building a WordPress Website
- Manually Building Discuz! Forum

Documentation

- Reset Instance Password
- Managing SSH Keys
- Status check

Logging in To Linux Instance via Remote Login Software

Last updated: 2023-10-12 14:23:16

Scenario

This document takes PuTTY as an example to describe how to log in to a Linux instance from Windows by using remote login software.

Applicable OS

Windows

Authentication Method

Password or **Key**

Preparations

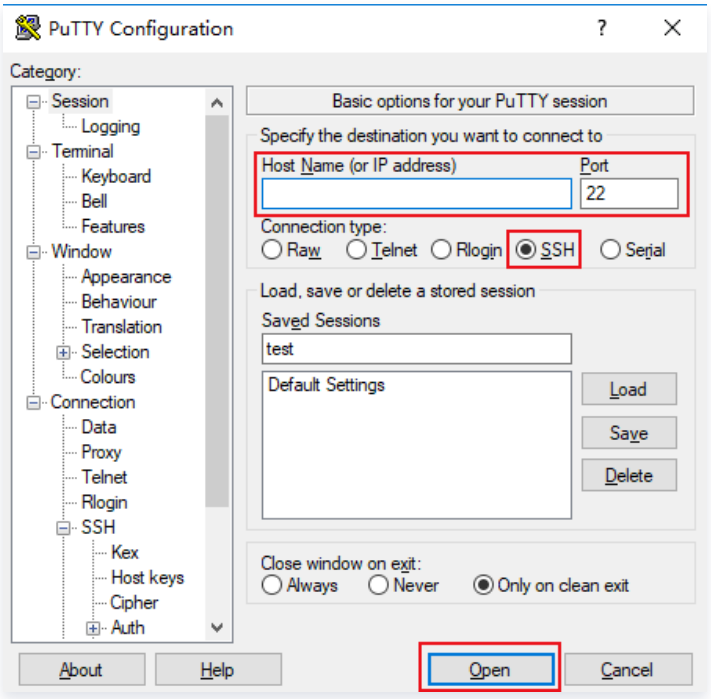
- You have obtained the administrator account and password (or key) for logging in to the instance.
  - If you use a system default password to log in to the instance, go to Message Center (marked with "CVM creation successful") to obtain the password first.
  - If you've forgotten your password, please reset the instance password.
- A public IP has been purchased and obtained for your CVM instance, and port 22 is open (this is open by default for CVM purchased with quick configuration).

Instructions

Log in using a password

1. Download the Windows remote login software, PuTTY.
2. Double-click **putty.exe** to launch the PuTTY client.

3. In the PuTTY Configuration window, enter the following information as shown below:



The parameters are explained as follows:

- **Host Name (or IP address)**: The public IP address of the CVM (Log in to the CVM console to obtain the public IP address from the list and details pages).
- **Port**: The port number of the cloud server must be set to 22.
- **Connection type**: Select **SSH**.
- **Saved Sessions**: Enter a session name, such as test.
  After configuring the **Host Name**, configure **Saved Sessions** and save it. In subsequent use, you can directly double-click the saved session name under **Saved Sessions** to log in to the server.

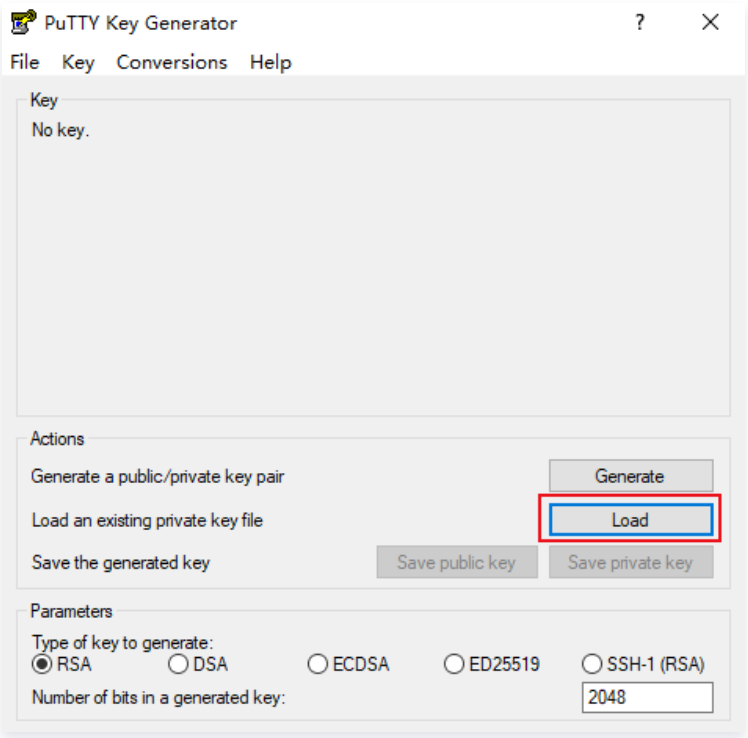
4. Click **Open** to enter the **PuTTY** interface, which prompts **login as:**.
5. Enter the username after **login as** and press **Enter**.
6. Enter the password after **Password** and press **Enter**.
   The entered password is not displayed by default, as shown below:

After logging in, the command prompt will display the information of the currently logged-in cloud server on the left side.

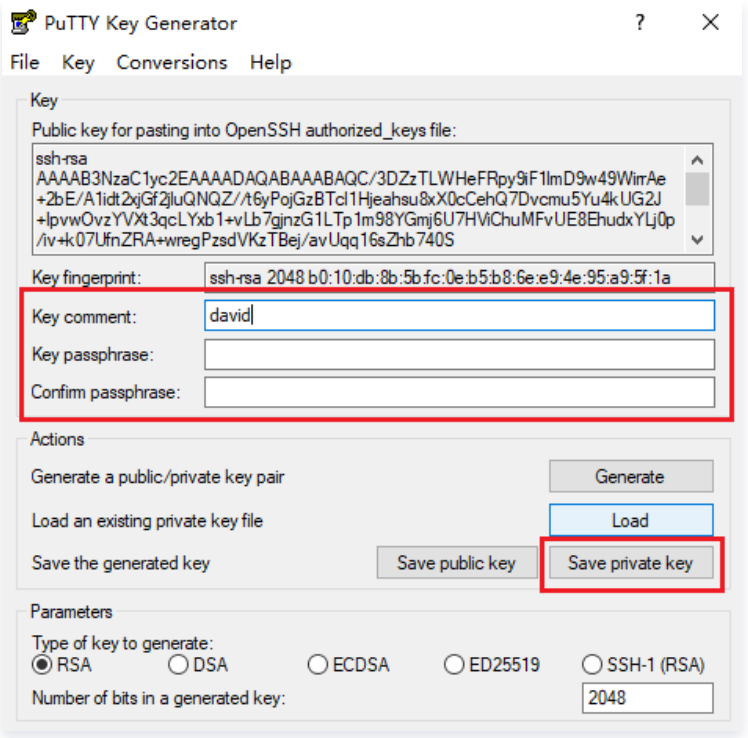
Log in using a key

1. Download the Windows remote login software, PuTTY. Please download both putty.exe and puttygen.exe software.
2. Double-click **puttygen.exe** to open the PuTTY Key client.

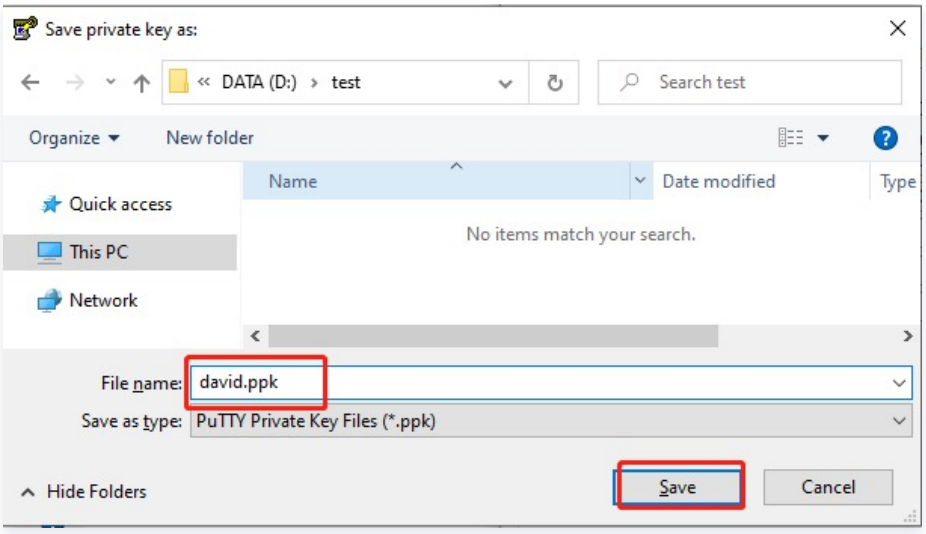
3. Click **Load**, select and open the downloaded private key storage path. The private key has been downloaded and kept by you during creation. For more information, see Manage SSH Keys.
For example, select and open the private key file named david. As shown in the image below:



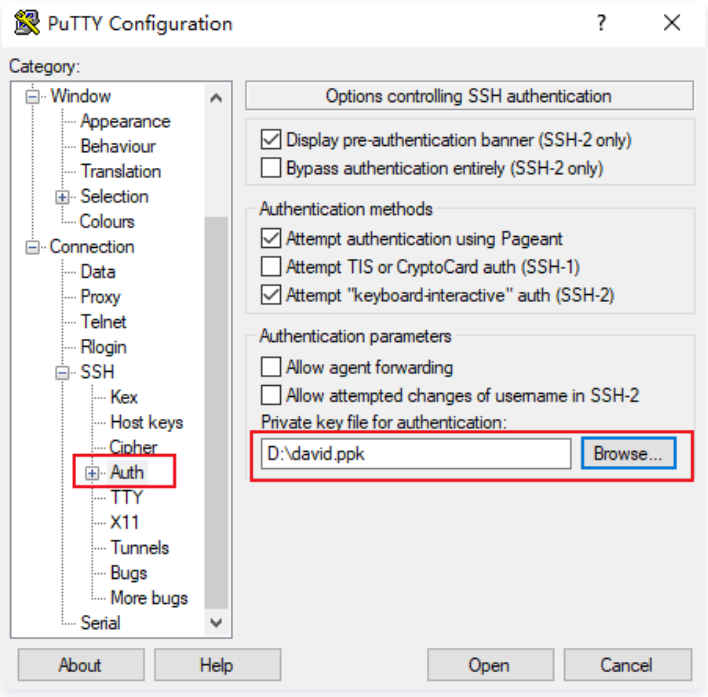
4. In the PuTTY Key Generator window, enter the key name and set the password for PuTTY to encrypt the private key (optional). After setting, click **Save private key**. As shown below:



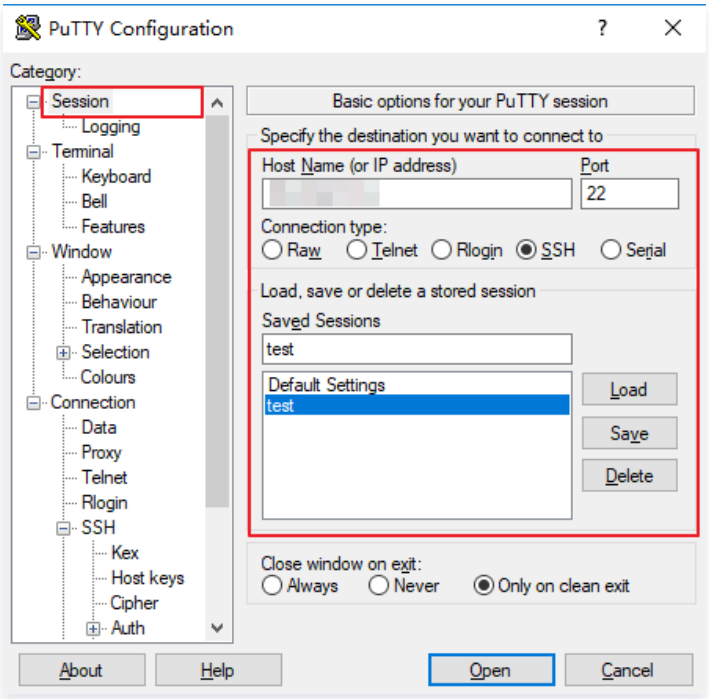
5. In the pop-up window, select the path where you store the key, enter **key_name.ppk** in the file name field, and click **Save**. For example, save the private key file "david" as the key file "david.ppk". As shown in the following figure:



6. Double-click **putty.exe** to launch the PuTTY client.
7. In the left sidebar, select **Connection** > **SSH** > **Auth** to enter the Auth configuration interface.
8. Click **Browse**, select and open the key storage path, as shown below:

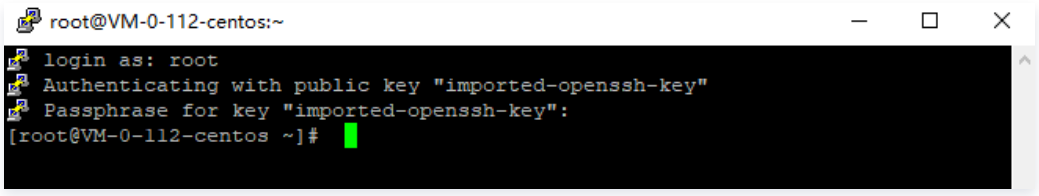


9. Switch to the Session configuration interface, configure the server's IP, port, and connection type, as shown below:



- **Host Name (IP address)**: The public IP of the CVM. Log in to the CVM console to obtain the public IP from the list page and details page.
- **Port**: The port number of the CVM instance, which has to be 22.
- **Connection type**: Select **SSH**.
- **Saved Sessions**: Enter a session name, such as test.
  After configuring the **Host Name**, configure **Saved Sessions** and save it. In subsequent use, you can directly double-click the saved session name under **Saved Sessions** to log in to the server.

10. Click **Open** to enter the **PuTTY** interface, which prompts **login as:**.
11. Enter the username after **login as** and press **Enter**.
12. If you have set a password for the encrypted private key in Step 4, please enter the password at **Passphrase for key "imported-openssh-key":** and press **Enter**.
    The entered password is not displayed by default, as shown in the image below:



After logging in, the command prompt will display the information of the currently logged-in cloud server on the left side.

See Also

Once you have successfully logged in to the cloud server, you can set up a personal website, forum, or perform other operations on the Tencent Cloud server. For related operations, please refer to:

- Manually Building a WordPress Website
- Manually Building Discuz! Forum

Logging in To Linux Instance via SSH Key

Last updated: 2023-09-07 16:55:01

Scenario

This article explains how to log in to a Linux instance using SSH from a local computer running Linux, macOS, or Windows.

Applicable OS

Linux, macOS, or Windows (Windows 10 and Windows Server 2019 versions)

Authentication Method

Password or **Key**

Preparations

- You have obtained the administrator account and password (or key) for logging in to the instance.
  - The default admin account for Linux instances is usually `root`, and for Ubuntu systems, it is `ubuntu`. You need to modify it according to your specific situation.
  - If you use a system default password to log in to the instance, go to Message Center (marked with "CVM creation successful") to obtain the password first.
  - If you log in using a key pair, you need to complete the creation of the key pair and bind it to the cloud server. For specific operations, please refer to SSH Keys.
  - If you've forgotten your password, please reset the instance password.
- A public IP has been purchased for your CVM instance, and the port 22 is open. It is open by default for a CVM instance purchased with quick configuration.

Instructions

Log in using a password

1. Execute the following command to connect to the Linux CVM.

   Note
   - If your local computer uses Mac OS, you need to open the terminal that comes with the system before executing the following command.
   - If your local computer uses Linux, you can directly execute the following command.
   - Windows 10 or Windows Server 2019: Open the command prompt (CMD) before running the following command

   ```
   ssh <username>@<hostname or IP address>
   ```

   - `Username` refers to the default account obtained in the prerequisite section.
   - `hostname or IP address` refers to the public IP address or custom domain name of your Linux instance.
2. Enter the obtained password and press **Enter** to log in.

Log in using a key

1. Execute the following command to set the private key file readable only to you.
   - If your local computer uses Mac OS, you need to open the terminal that comes with the system before executing the following command.
   - If your local computer uses Linux, you can directly execute the following command.

     ```
     chmod 400 <The absolute path of the private key downloaded to be associated with the CVM>
     ```

   - If your local computer uses Windows 10, you must first open the command prompt CMD and then execute the following commands.

     ```
     icacls <The absolute path of the private key downloaded to be associated with the CVM> /grant <Windows user account>:F
     ```

     ```
     icacls <The absolute path of the private key downloaded to be associated with the CVM> /inheritancelevel:r
     ```

2. Execute the following command for remote login.

   ```
   ssh -i <absolute path of the downloaded private key associated with the CVM> <username>@<hostname or IP address>
   ```

   - `Username` refers to the default account obtained in the prerequisite section.
   - `hostname or IP address` refers to the public IP address or custom domain name of your Linux instance.

   For example, run the command `ssh -i "Mac/Downloads/shawn_qcloud_stable.pem" ubuntu@192.168.11.123` to remotely log in to the Linux CVM.

See Also

Once you have successfully logged in to the cloud server, you can set up personal websites, forums, or perform other operations on Tencent Cloud servers. For related operations, please refer to:

- Manually Building a WordPress Website
- Manually Building Discuz! Forum

Logging in To Linux Instances (VNC)

Last updated: 2024-06-26 14:40:41

Scenario

VNC login is a method provided by Tencent Cloud for users to remotely connect to cloud servers through a web browser. In cases where remote login clients are not installed or cannot be used, and other login methods are unavailable, users can connect to the cloud server via VNC login to observe the server's status and perform basic server management operations using the cloud server account.

Usage Limits

- VNC login currently does not support copy and paste, Chinese input method, and file upload or download.
- When you use VNC to log in to CVM, mainstream browsers must be used, such as Chrome, Firefox, IE 10 and above.
- VNC login is a dedicated terminal, meaning only one user can use VNC login at a time.

Preparations

You have obtained the administrator account and password for logging in to the instance.

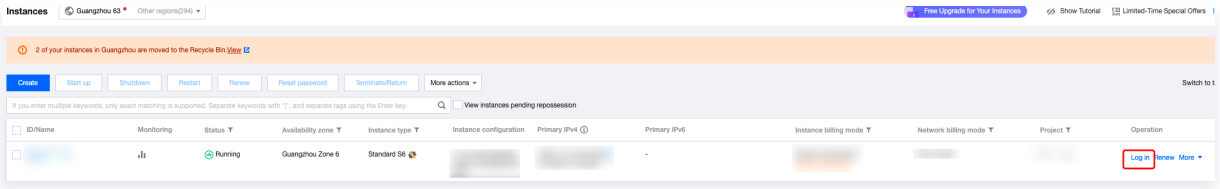
- If you choose to have the system generate a random password when creating an instance, please go to Message Center (marked with "CVM instance created successfully") to obtain it.
- If you have set a login password, please use it to log in. If you have forgotten the password, you can reset the instance password.

Instructions

1. Log in to the CVM console.
2. On the instance management page, proceed according to the actually used view mode:

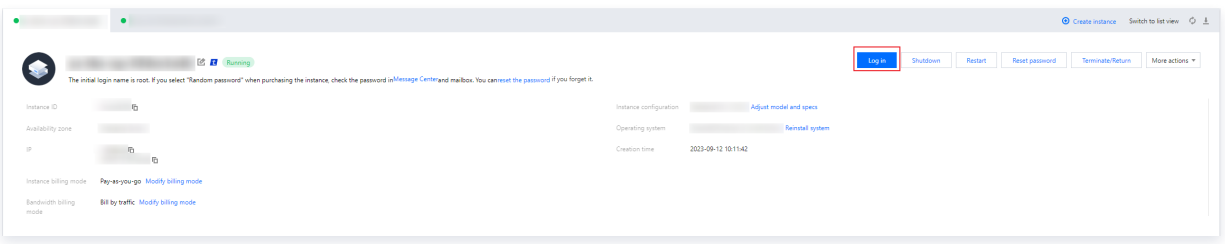
List view

Locate the Linux CVM you want to log in to and click **Log in** on the right side, as shown in the image below:

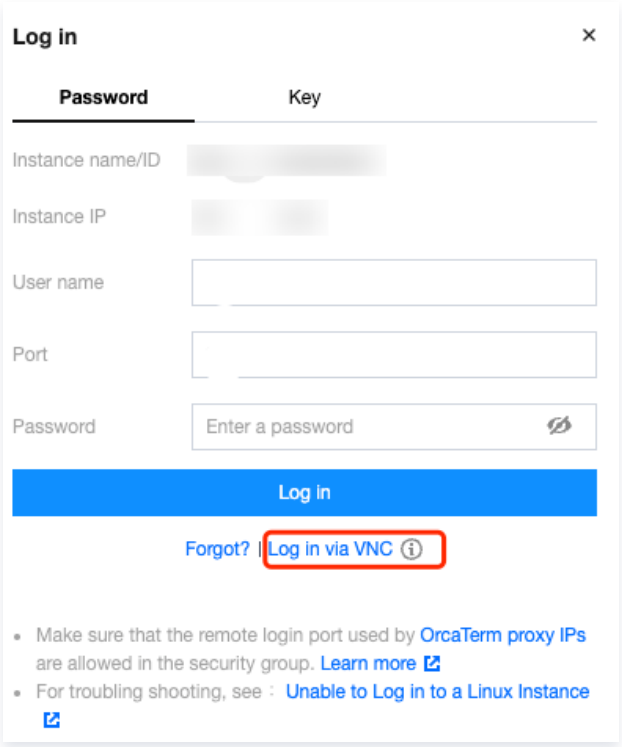


Tab view

Select the Linux CVM tab you want to log in to and click **Log in**. As shown in the figure below:



3. In the opened "Log in" window, click **Log in via VNC**, as shown in the following figure:



4. In the opened window, enter the username after "login" and press **Enter**. The default username for Linux instances is `root`, and for Ubuntu system instances, it is `ubuntu`. Please fill in as needed.
5. Enter the password after "Password" and press **Enter**.
   The entered password is not displayed by default. After logging in, the command prompt will display the current cloud server information on the left side, as shown below:

See Also

Once you have successfully logged in to the cloud server, you can set up personal websites, forums, or perform other operations on Tencent Cloud servers. For related operations, please refer to:

- Common Linux Operations and Commands
- Manually Building a WordPress Website
- Manually Building Discuz! Forum

Logging in To Linux Instances (Mobile Devices)

Last updated: 2024-06-02 14:21:11

Scenario

This document explains how to log in to a Linux instance on mobile devices with different operating systems. The connection tools used in this document are as follows:

- iOS device: Termius-SSH client
- Android device: JuiceSSH

Applicable Mobile Devices

iOS and Android devices

Preparations

- The CVM instance is in **Running** status.
- You have obtained the administrator account and password (or key) for logging in to the instance.
  - If you use a system default password to log in to the instance, go to Message Center (marked with "CVM creation successful") to obtain the password first.
  - If you've forgotten your password, please reset the instance password.
- A public IP has been purchased for your CVM instance, and the port 22 is open. It is open by default for a CVM instance purchased with quick configuration.

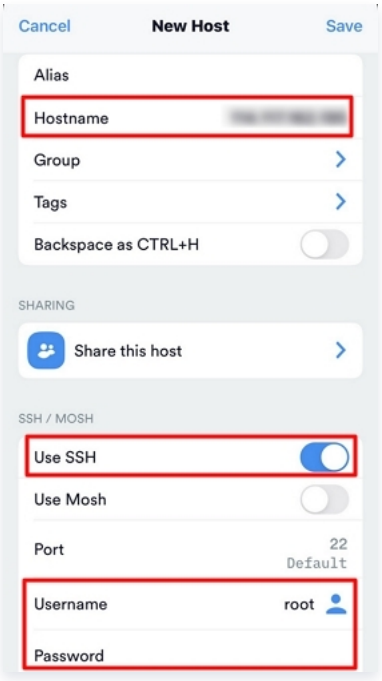
Instructions

Log in to the instance from the mobile device you are using:

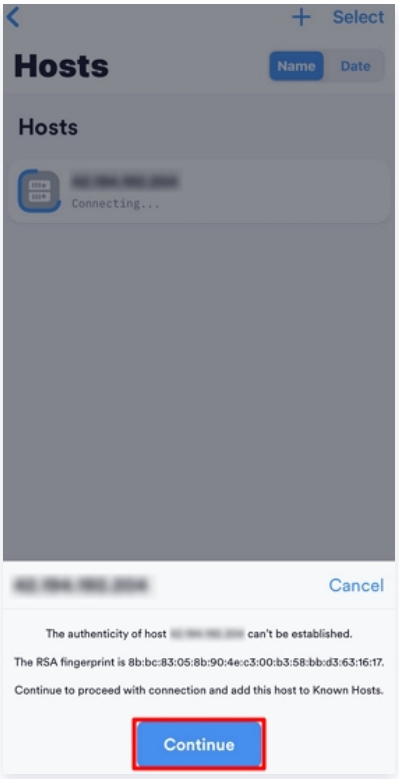
iOS Devices

1. Download the Termius-SSH client from the App Store, and register an account as instructed.
2. On the main page, click **New Host**.

3. Navigate to the **New Host** page and configure the following login information, as shown below:



   - **Hostname**: The public IP address of the cloud server. For more information on how to obtain it, see Getting Public IP Addresses.
   - **Use SSH**: Enabled by default, initiating SSH login configuration.
   - **Username**: Enter the admin account ID `root`. If you are using Ubuntu, the admin account is `ubuntu`.
   - **Password**: Enter the instance login password.
4. Click the top-right corner **Save** to save the login configuration.
5. On the **Hosts** page, select the item and click **Continue** at the bottom of the pop-up window to confirm the login, as shown in the following figure:



6. Log in to the Linux instance successfully as shown in the following figure.

Android Devices

Create Authentication Information

1. Download and install JuiceSSH.
2. On the main page, select **Connect** and click the "Authentication" tab.
3. In the **Authentication** tab, click the **+** in the bottom right corner.
4. On the **New Authentication** page, configure the login account and password.
   - **Nickname**: Customize the authentication name (optional).
   - **User Name**: Enter the administrator account `root`. For Ubuntu operating systems, the administrator account is `ubuntu`.
   - **Password**: Select **Password** and then **Settings (optional)**, and enter the instance login password in the pop-up window.
5. Click the ✔ icon in the upper right corner to create a new authentication.

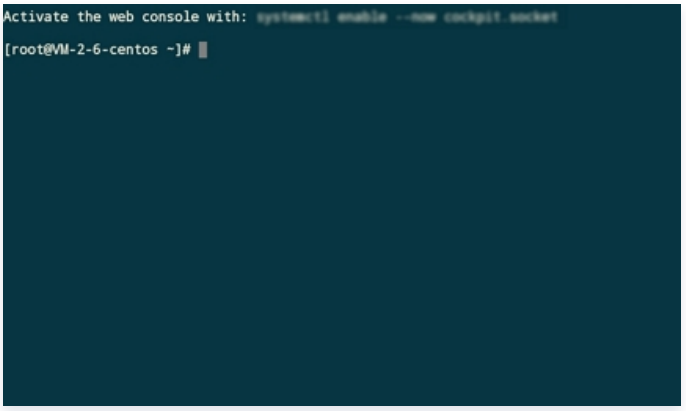
Creating a connection

1. On the main page, select **Connections** and click the **+** button in the bottom right corner of the **Connections** page.
2. On the **New Connection** page, configure the following login information.
   - **Nickname**: Customize the connection name (optional).
   - **Type**: Select **SSH**.
   - **Address**: CVM public IP. For more information about how to obtain the public IP, see Getting Public IP Addresses.
   - **Authentication**: Select the authentication information added in the Create Authentication Information step.
   - **Port**: Enter port 22.
     Keep the other parameters at their default settings.
3. Click **Add to Group** at the bottom of the page to save the login configuration.

Logging in to the instance

1. On the **Connections** page, select the instance you want to log in to and click **Accept** in the pop-up window.

2. Log in to the Linux instance successfully as shown in the following figure.



Logging in To Windows Instance
Logging in To Windows Instance via Remote Desktop Connection

Last updated: 2023-09-07 16:57:44

Scenario

This document describes how to log in to a Windows instance through remote desktop on a local computer.

Applicable OS

Windows

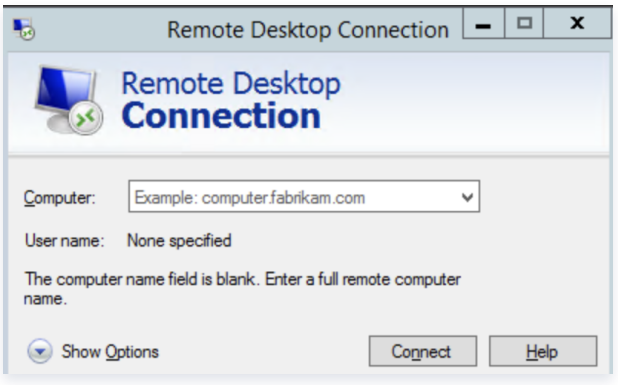
Preparations

- You have already obtained the administrator account and corresponding password required for remote login to the Windows instance.
- If you use a system default password to log in to the instance, go to Message Center (marked with "CVM creation successful") to obtain the password first.
- If you've forgotten your password, please reset the instance password.
- A public IP has been purchased for your CVM instance, and port 3389 is open (if the CVM is purchased with “Quick Configuration”, this port is open by default.)

Instructions

> **Note**
> The following takes Windows 7 as an example.

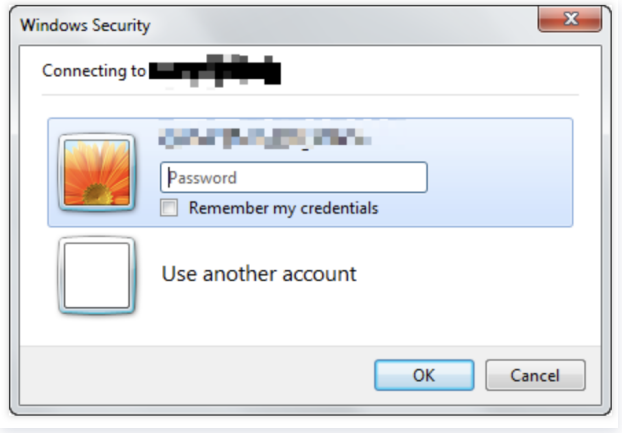
1. On your local Windows computer, click  , and in **Search programs and files**, enter **mstsc** and press **Enter** to open the Remote Desktop Connection dialog box, as shown in the following figure:



2. Enter the public IP of the Windows server after **Computer** and click **Connect**. You can get the server public IP as instructed in Getting Public IP Address.
3. Enter the instance's admin account and password in the **Windows Security** pop-up window as shown below:

> **Note**
> - If the **Do you trust this remote connection?** dialog box appears, you can select **Don't ask me again for connections to this computer** and click **Connect**.

- The default administrator account for Windows CVM instances is `Administrator`. The password can be obtained as described in Preparations.



4. Click **OK** to log in to the Windows instance.

Logging in To Windows Instance via VNC

Last updated: 2023-09-26 15:26:21

Scenario

VNC login is a method provided by Tencent Cloud for users to remotely connect to cloud servers through a web browser. In cases where remote login clients are not installed or cannot be used, and other login methods are unavailable, users can connect to the cloud server via VNC login to observe the server's status and perform basic server management operations using the cloud server account.

Usage Limits

- VNC login for cloud servers temporarily does not support file copy and paste, Chinese input method, and file upload or download.
- When logging in to a cloud server via VNC, use mainstream browsers such as Chrome, Firefox, or Microsoft Edge.
- VNC login is a dedicated terminal, meaning only one user can use VNC login at a time.

Preparations

You have already obtained the administrator account and corresponding password required for remote login to the Windows instance.

- If you have chosen a system-generated random password when creating an instance, please go to Message Center to obtain it.
- If you have set a login password, please use it to log in. If you have forgotten the password, you can reset the instance password.

Instructions

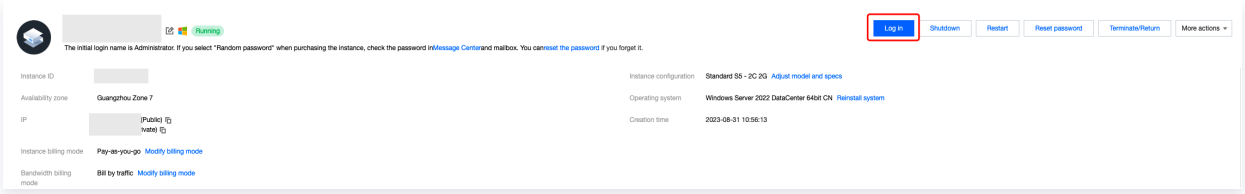
1. Log in to the CVM console.
2. On the instance management page, proceed according to the actually used view mode:

List view

Locate the Windows CVM you want to log in to and click **Log in** on the right side, as shown below:

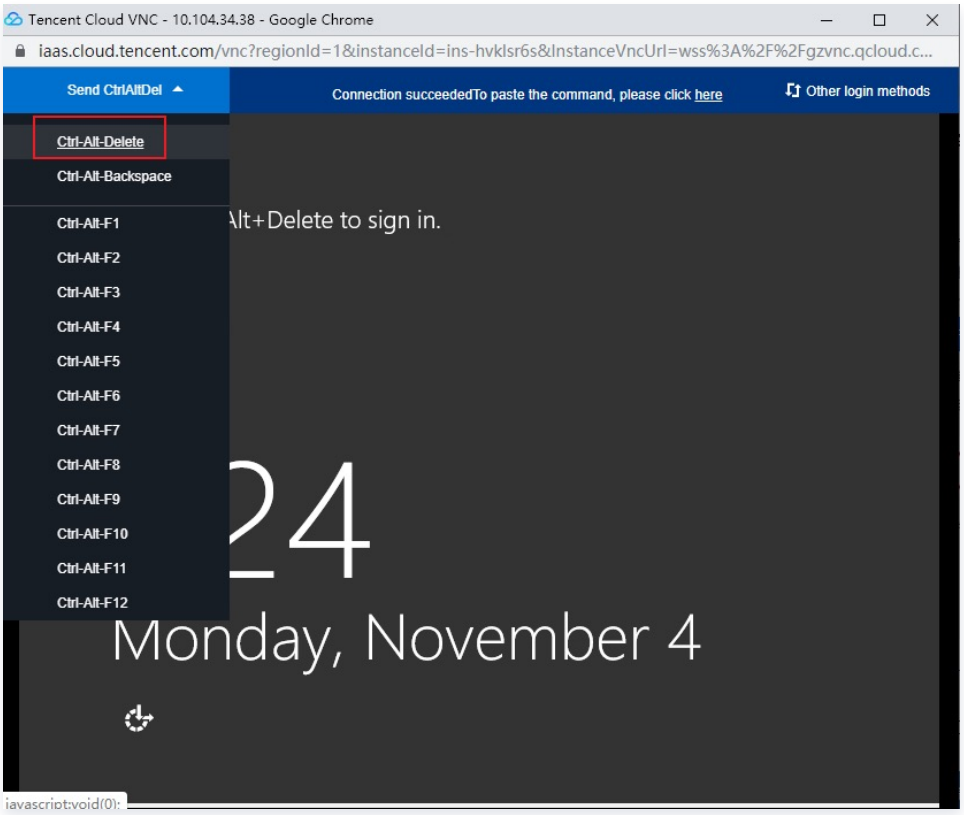
Tab view

Select the Windows CVM tab you want to log in to and click **Log in**. As shown in the following image:



3. In the opened "Log in" window, select **Log in via VNC**.

4. In the login window that appears, select **Send Remote Command** in the top left corner, and click **Ctrl-Alt-Delete** to access the system login screen, as shown below:



> **Note**
> If there is no response when sending Ctrl-Alt-Delete in VNC, it is recommended to restart the instance to recover.

5. Enter the login password and press **Enter** to log in to the Windows CVM.

Logging in To Windows Instance from Mobile Devices

Last updated: 2023-09-26 15:29:01

Scenario

This document uses Microsoft Remote Desktop client as an example to demonstrate how to log in to a Windows instance on mobile devices with different operating systems. You can also use third-party remote desktop client software, such as Parallels (for reference only).

Applicable Mobile Devices

iOS and Android devices

Preparations

- The CVM instance is in the **Running** status.
- You have obtained the administrator account and password for logging in to the instance.
  - If you use a system default password to log in to the instance, go to Message Center (marked with "CVM creation successful") to obtain the password first.
  - If you've forgotten your password, please reset the instance password.
- A public IP has been purchased for your CVM instance, and the port 3389 is open. It is open by default for a CVM instance purchased with quick configuration.

Instructions

> **Note**
> This document uses the iOS device as an example. You can also refer to it for the Android device.

1. Download Microsoft Remote Desktop and start it.
2. On the **PC** page, select the **+ in the upper right corner and click Add PC** from the dropdown menu.
3. On the **Add PC** page, configure the following login information:
   - **Computer Name**: The public IP of the cloud server. For instructions on how to obtain it, see Getting Public IP Addresses.
   - **User Account**: Select "Ask when required" by default.
4. After filling in the information, click **Save** in the upper right corner of the page.
5. On the "Computer" page, select the instance you want to log in to, and enter the admin account and password for the instance in the pop-up window:
   - **User Name**: The administrator account for Windows instances is `Administrator`.
   - **Password**: Enter the instance login password.
6. Click **Continue**. If the interface shown in the following image appears, it indicates a successful login to the Windows instance.

Adjust configuration
Modifying Instance Configuration

Last updated: 2023-10-07 16:06:01

Scenario

Tencent Cloud instances offer rapid and convenient hardware adjustments, which is a significant aspect of CVM flexibility. This document describes the methods and considerations for upgrading, downgrading, and adjusting configurations across different instance types.

Preparations

You can adjust the configuration of an instance when it is in shutdown or running status. If the instance is running, the adjustment takes effect after it is forcibly shut down and restarted.

> **Note**
> - When the target instance is in the **Shutdown** status, you can directly perform the configuration change via the console.
> - When the target instance is in the **running** state, you can adjust its configuration online. After completing the operation, you need to confirm the forced shutdown, and the configuration adjustment will take effect after the restart.
> - When performing **batch operations** for adjustments, you can do so online. If any instances in the batch are in **running** status, you must confirm to forcibly shut them down, and the changes will take effect after the restart.

Limits and Impacts

Configuration adjustment limits

Only instances with both **system disk and data disk as cloud disks** support configuration adjustments.

- Configuration Upgrade
  The number of configuration upgrades is unlimited and the upgrade takes effect immediately.
- Configuration downgrade:
  - Monthly subscribed instances can be downgraded at any time (except for expired instances), with a cumulative limit of **5** downgrade operations per instance.
  - Pay-as-you-go instances can be downgraded any number of times at any time.
- Adjustment across instance families: configurations can be adjusted between instance families without the need for data migration.
  During configuration adjustment, instance specifications that can be adjusted are related to the target specifications available in the current AZ. Pay attention to the following restrictions:
  - **Spot instances** do not support adjusting configurations across different instance types.
  - **Exclusive instances** do not support cross-model configuration adjustments. The scope of adjustments is limited by the remaining resources of the dedicated host where the instance is located.
  - **GPU, FPGA, and other heterogeneous instance types** are not supported as source or target instance specifications for cross-instance family configuration adjustments.
  - **Instances with classic network configurations** cannot be adjusted to instances that only support VPC.
  - If the target instance type does not support the CBS disk type configured for the current instance type, the configuration cannot be adjusted.

- If the target instance type does not support the image type configured for the current instance type, the configuration cannot be adjusted.
- If the target instance type does not support the current configuration's ENI or the number of ENIs, the adjustment is not allowed. For more information, refer to ENI Usage Restrictions.
- If the target instance type does not support the current public network bandwidth cap, the adjustment cannot be made. For more information, refer to Public Network Bandwidth Cap.

Related Impacts

For some instances using the classic network, the private IP address may change after adjustment. If the private IP address changes, we will display a notice on the adjustment page. If there is no such notice, the private IP address will remain unchanged.

Instructions

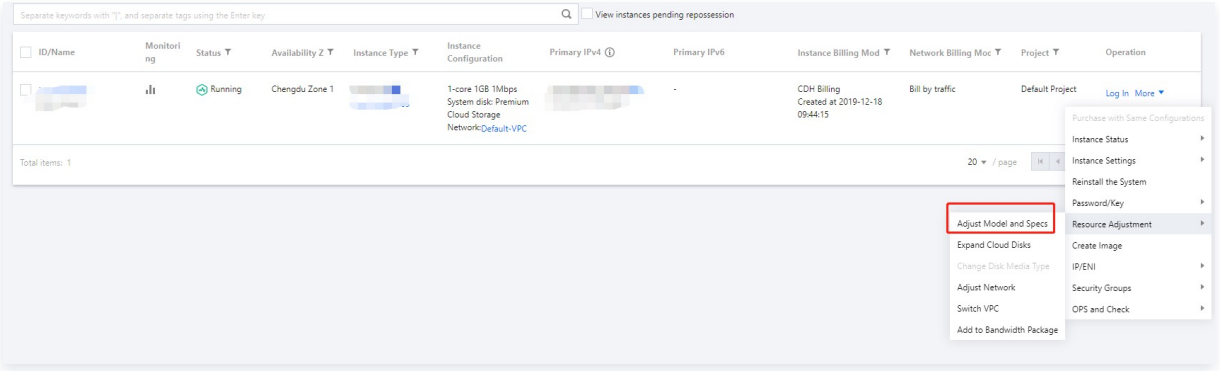
Note

- If your business changes, you can adjust the instance configuration.
- During configuration upgrade, upgrade your CVM instance accordingly and pay for fees that may be incurred.
- During configuration downgrade, confirm the refund detail and forcibly shut down and restart your CVM instance for the new configuration to take effect immediately.
- For fees related to configuration adjustments, refer to Fees of Instance Configuration Adjustment.

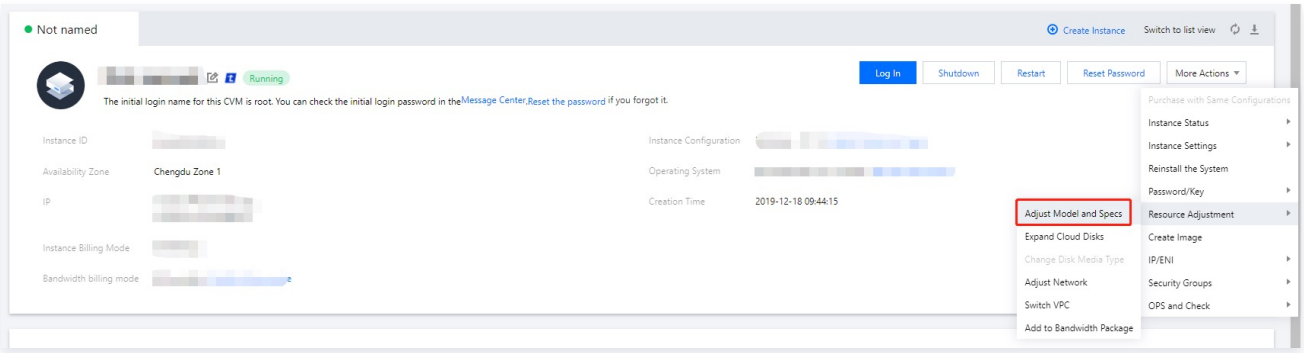
Via the console

Adjusting the configuration of a single instance

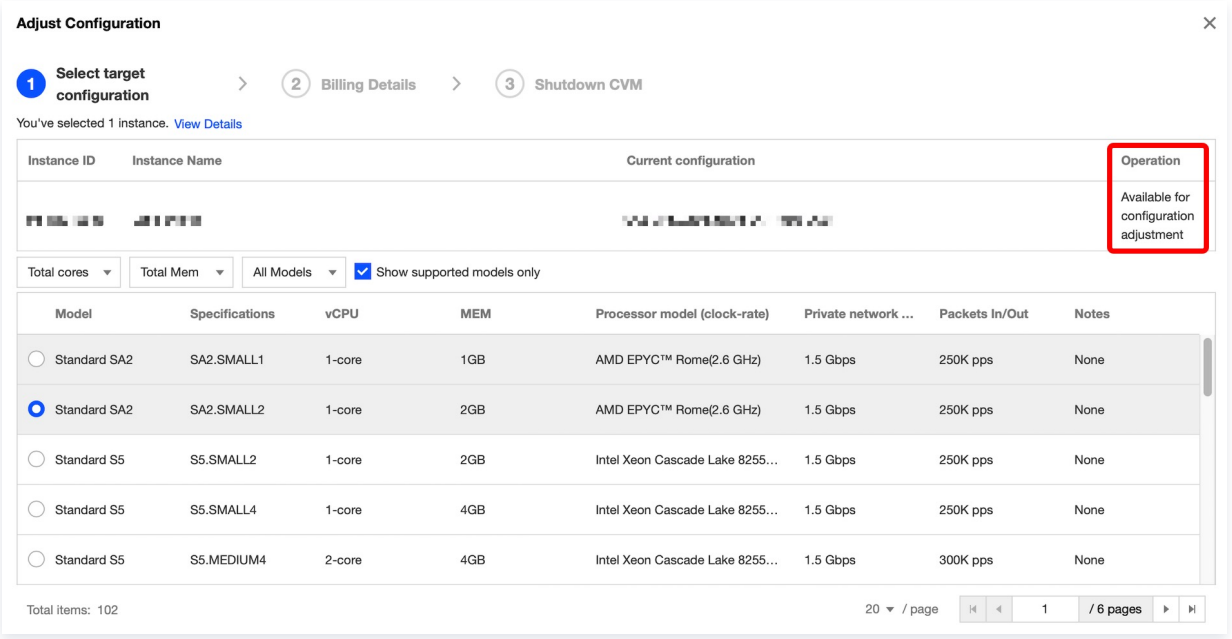
1. Log in to the Cloud Virtual Machine Console and enter the Cloud Server page.
2. Proceed according to the actually used view mode:
   - **List view**: In the operation column on the right side of the instance you want to adjust, select **More** > **Resource Adjustment** > **Adjust Model and Specs**. As shown below:



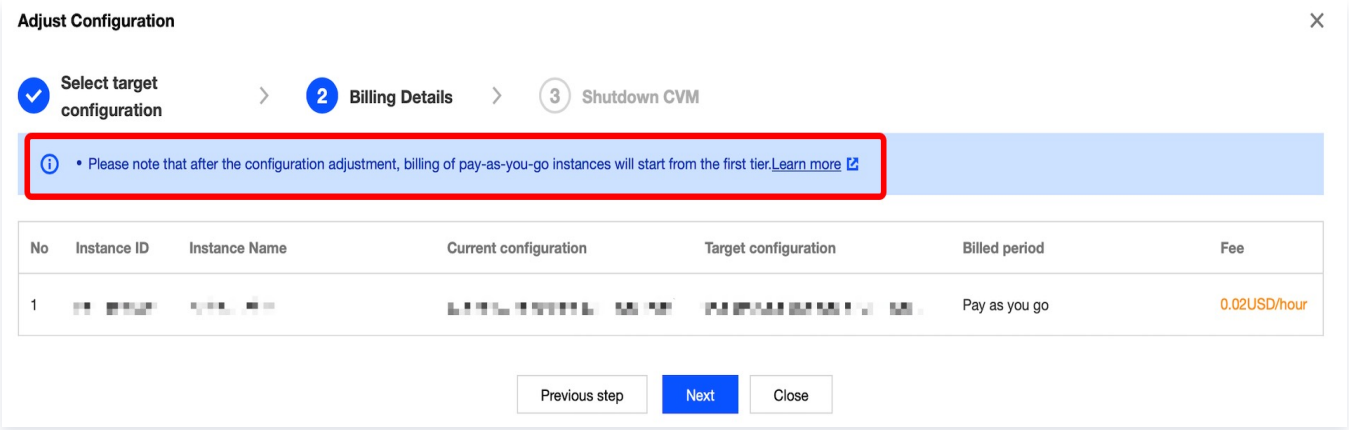
   - **Tab Mode**: On the page of the instance you want to adjust, select **More Actions** > **Resource Adjustment** > **Adjust Model and Specs** in the upper right corner, as shown below:



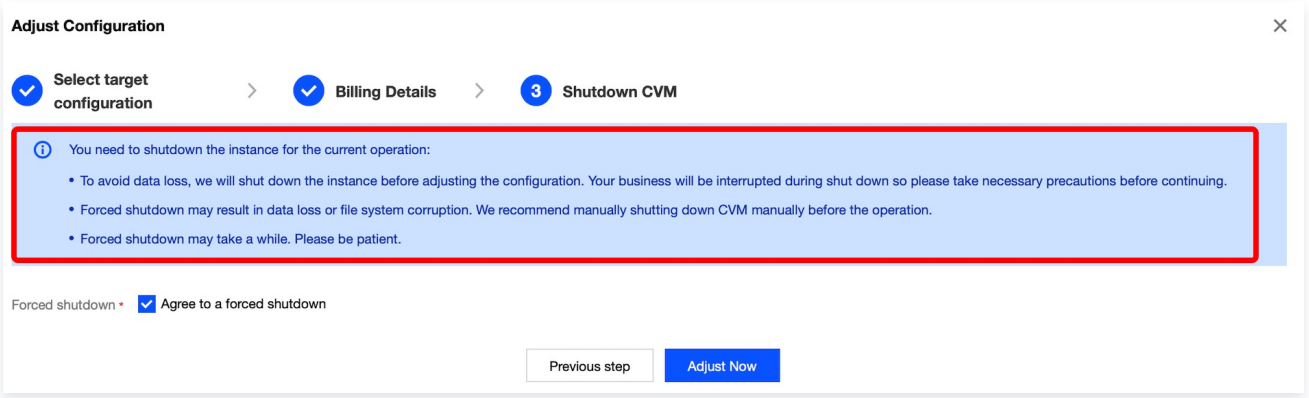
3. In the **Select target configuration** section, confirm the instance status and operation, select the required model and instance specifications, and carefully confirm the specifications and performance parameters. Click **Next** as shown in the figure below:



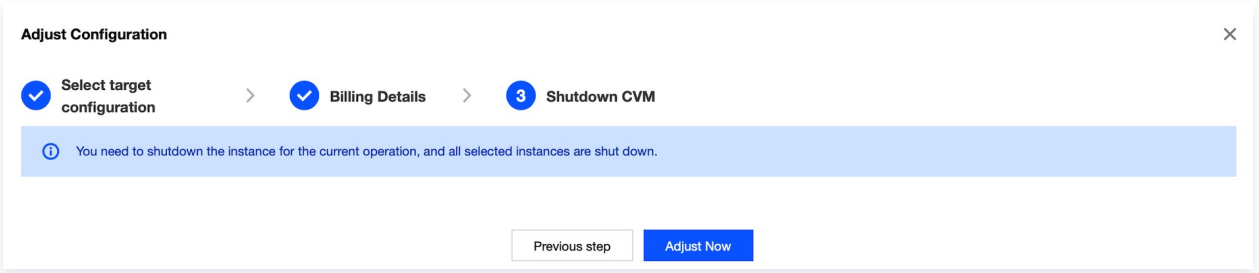
4. Based on the instance's billing mode, confirm the fees and click **Next**.



5. In the "Shutdown CVM" step, read the prompt carefully based on the instance running status.
   - If the current instance is running, read the prompt carefully and select "Agree to a forced shutdown", as shown in the following figure:



- If the current instance is shut down, the following prompt will appear:



6. Click **Adjust Now** to proceed to the order page and complete the payment.

TencentCloud APIs

You can adjust the instance configuration using the ResetInstancesType interface. For more details, refer to the Adjust Instance Configuration API documentation.

Adjusting Network Configuration

Last updated: 2023-09-07 16:59:59

Scenario

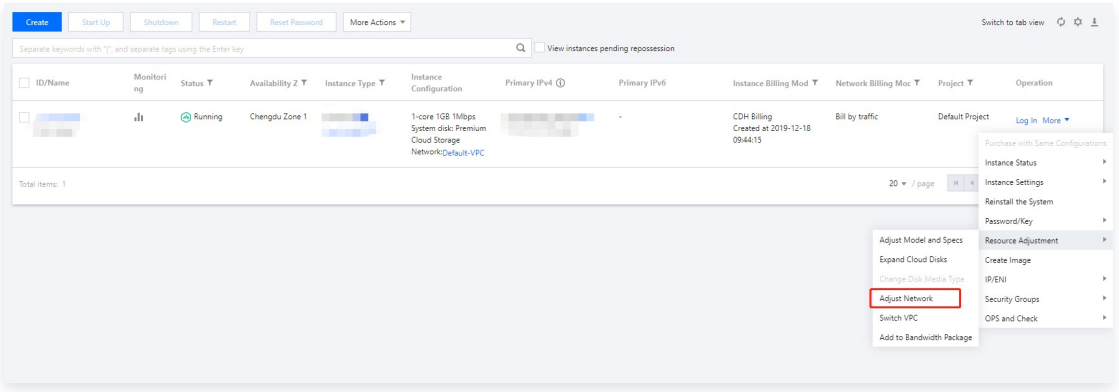
Tencent Cloud supports adjusting the public network billing mode or public network bandwidth on demand, with immediate effect. For limitations on adjusting bandwidth and billing modes, as well as the fee description after adjustment, please refer to Adjusting Public Network Billing.

Instructions

1. Log in to the CVM console. At the top of the **Instances** page, select the region where the target CVM instance resides.
2. On the instance management page, proceed according to the actually used view mode:

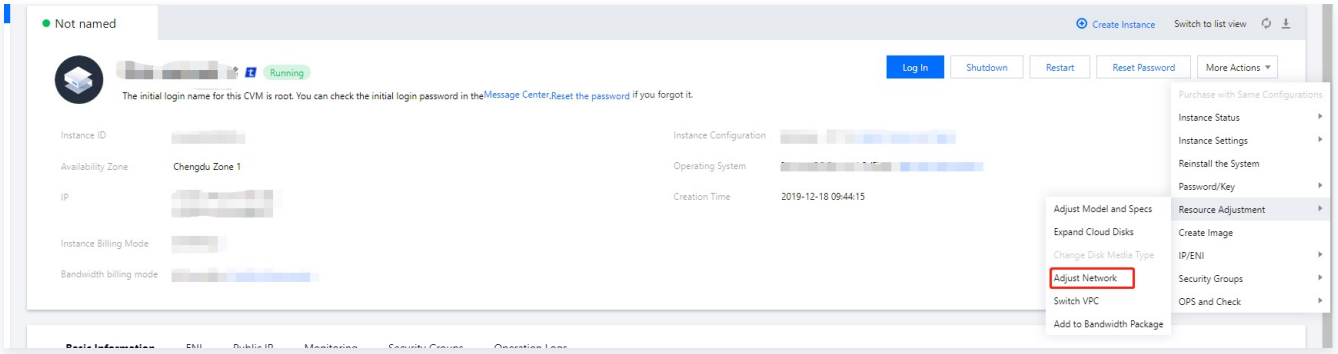
List view

Select **More** > **Resource Adjustment** > **Adjust Network** on the right side of the row where the target CVM instance is located, as shown below:



Tab view

Select **More Actions** > **Resource Adjustment** > **Adjust Network** in the upper right corner of the target CVM instance page, as shown below:



3. In the **Adjust Network** pop-up window, adjust the public network billing mode or public network bandwidth as needed:
   - Network billing mode: Tencent Cloud offers two convertible types of network billing modes: **bill-by-traffic** and **bill-by-bandwidth**. The **bill-by-bandwidth** mode includes hourly postpaid bandwidth and annual/monthly package

bandwidth billing modes. You can choose according to your needs. For detailed conversion instructions, please refer to Adjusting Configuration Fee Description.

- Target bandwidth cap: Tencent Cloud provides two network configurations: **dedicated public network** and **shared public network**. The shared public network service is billed by bandwidth package and is currently in beta testing. To use it, please submit a beta test application. This document takes adjusting the configuration of the dedicated public network as an example, i.e., adjusting the bandwidth cap of a single CVM instance.

> **Note**
> For bandwidth cap, please refer to Public Network Bandwidth Cap.

4. Select the desired target billing mode or configure the target bandwidth value, and click **Confirm**.

Documentation

- Adjust Public Network Billing
- Public Network Billing Mode
- Shared Bandwidth Package Billing Mode
- Public Network Bandwidth Cap

Adjusting Project Configuration

Last updated: 2024-09-24 15:06:11

Scenario

The project feature is used for managing cloud resources by project, allowing for subproject management of resources. When creating a cloud server instance, it must be assigned to a project. Tencent Cloud supports reassigning instances to new projects after they have been created.

> **Note**
> To assign an instance to a new project, please create a new project first. For detailed instructions, refer to Create a New Project.

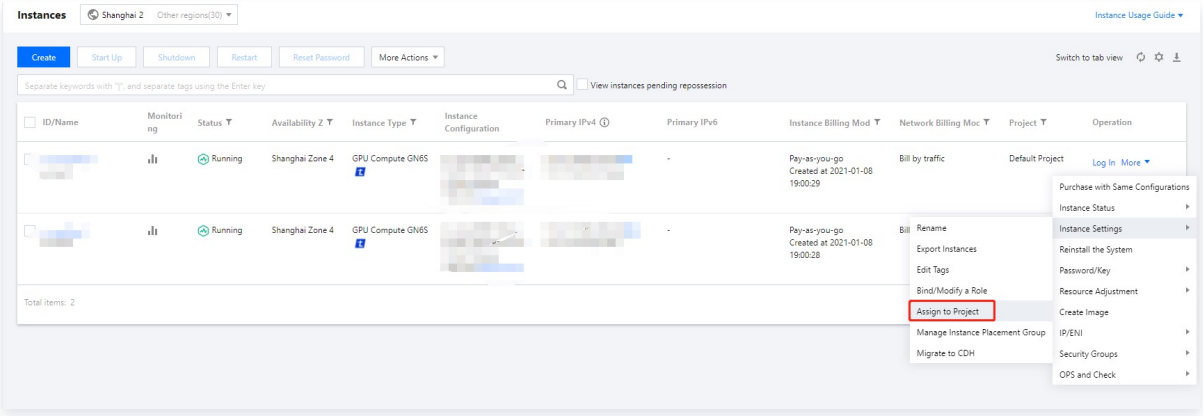
Instructions

1. Log in to the CVM console.
2. On the instance management page, proceed according to the actually used view mode:

List view

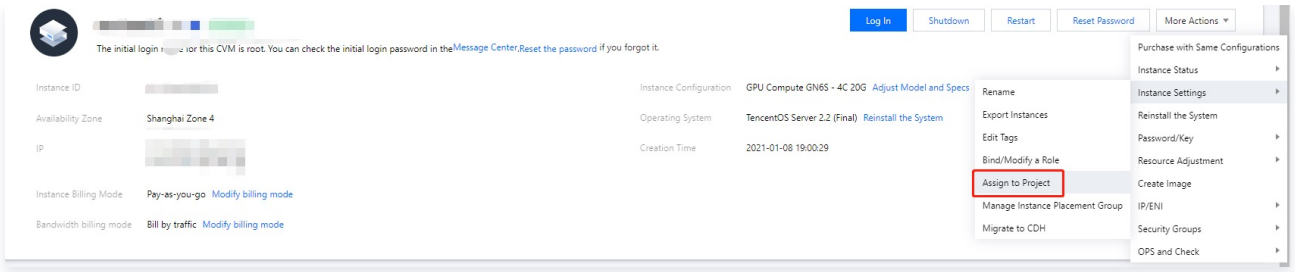
In the instance list, select the cloud server that needs to be reassigned to a new project, and choose **More** > **Instance Settings** > **Assign to Project** on the right, as shown below:

> **Note**
> If there are multiple cloud servers that need to be reassigned to a new project, select the cloud servers, and choose **More** > **Instance Settings** > **Assign to Project** at the top.

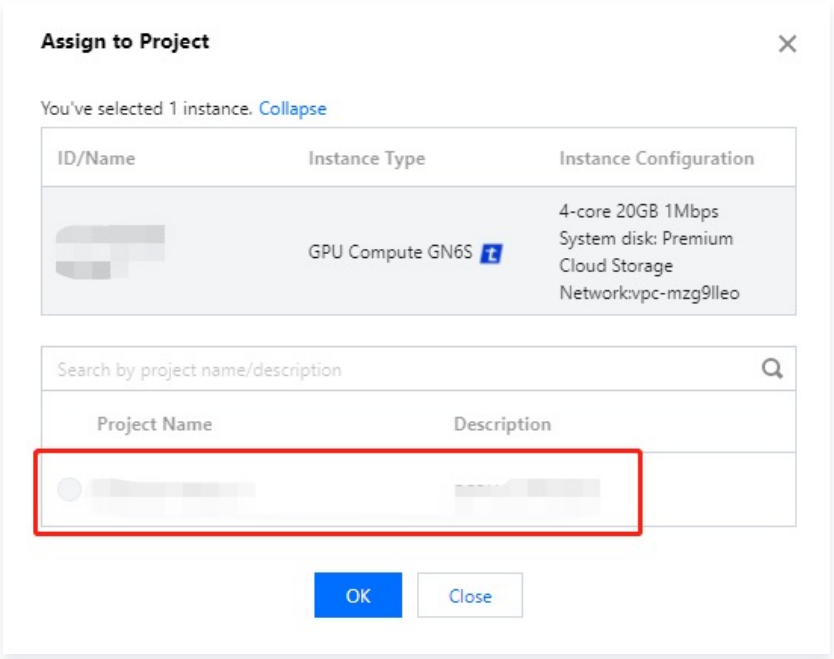


Tab view

In the cloud server page of the instance to be reassigned to a new project, select **More Actions** > **Instance Settings** > **Assign to Project** in the top-right corner, as shown below:



3. In the pop-up "Assign to Project" window, select the new project name and click **OK** to complete the assignment to the project.



Viewing Instance Details
Viewing Instance Information

Last updated: 2023-10-08 17:10:40

Scenario

Tencent Cloud provides the following three options for you to view the information of a CVM instance:

- On the Overview page of the console, you can view the total number of CVM instances under your account, their operational status, and information on resource quantities and quotas in each region.
- View the information of all CVM instances in a specific region on the Instances page of the console.
- View the details of a CVM instance on the instance details page.

Preparations

You have logged in to the CVM console.

Directions

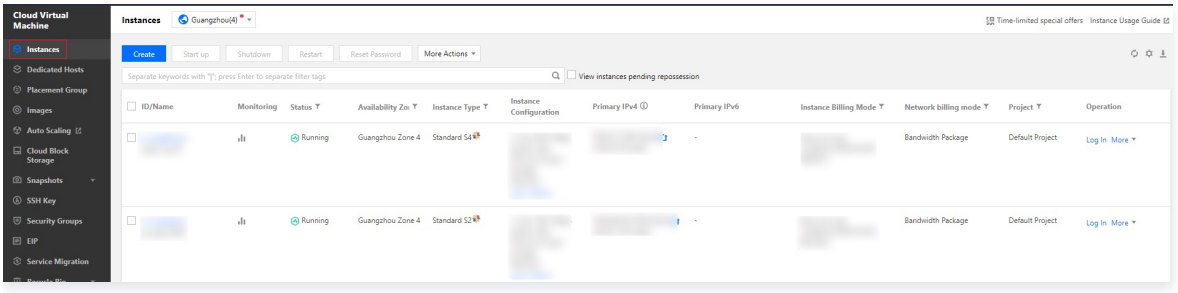
Viewing the CVM instance overview

Select Overview on the left sidebar to enter the CVM overview page.In this page, you can view the following information and perform the following operations:

- CVM status: the total number of CVMs, the number of instances that expire within the next 7 days, the number of instances in Recycle Bin, and the number of normal CVMs.
- List of CVMs to be renewed (you can renew them on this page).
- Resource quantity and quota: you can view the quotas of pay-as-you-go CVMs, custom images and snapshots. You can also apply for quotas on this page.
- Perform cross-region search for cloud resources.

Viewing the CVM instance list

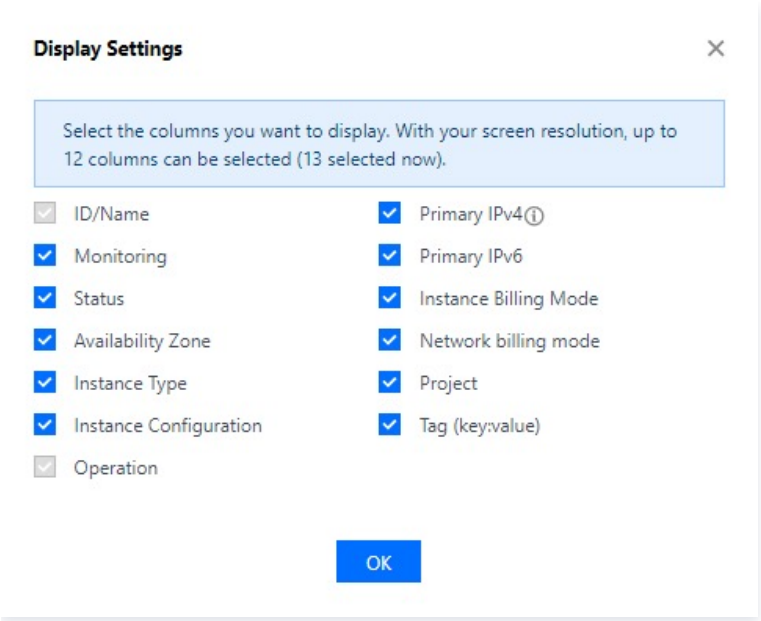
Select Instances on the left sidebar to enter the instance list page, as shown below:



The information available on this page includes CVM ID and name, monitoring information, status, availability zone, instance type, instance configuration, primary IPv4, primary IPv6, instance billing, network billing, and the project to which the CVM belongs.

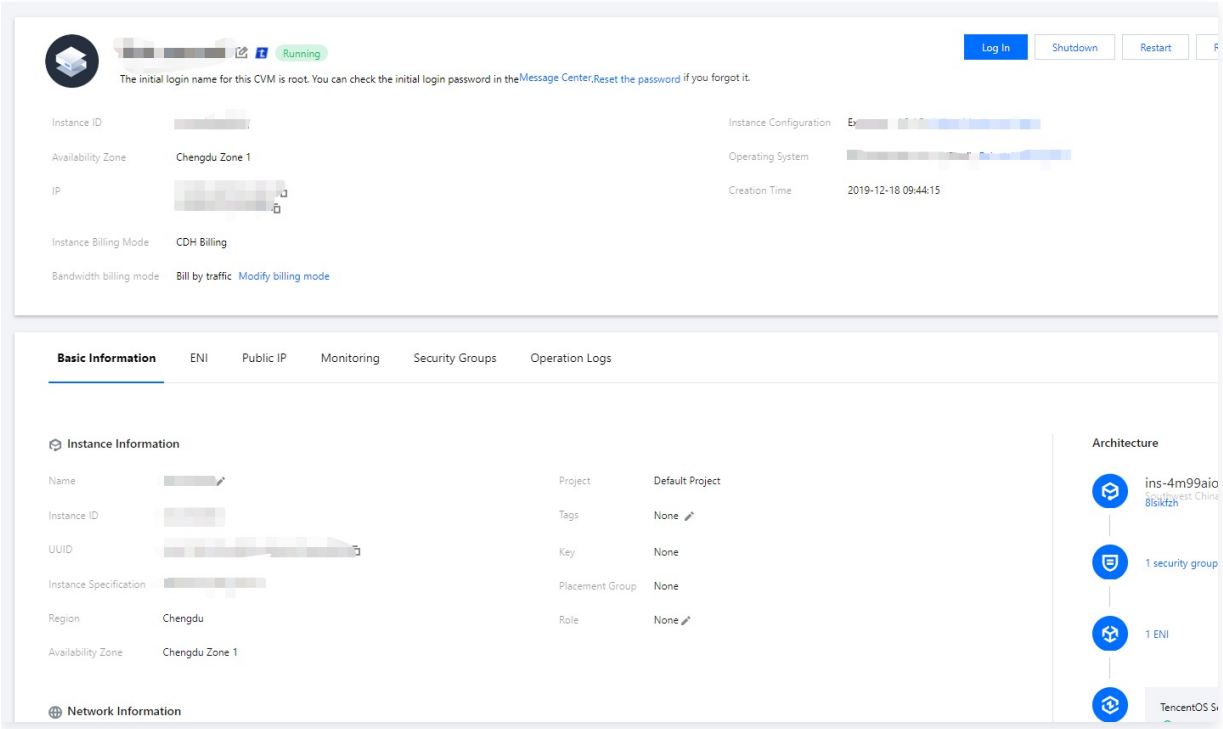
> **Note**
> You can switch the console instance page view according to your actual needs.

You can click ⚙ in the top-right corner, and in the pop-up "Display Settings" window, select the list details you want to display. As shown below:



Viewing instance details

1. Select a region at the top of the Instances management page.
2. Locate the instance you want to view the details of, and click on the ID/Instance Name to enter the instance details page, as shown below:
   On the instance details page, you can view information including instance details, architecture diagram, network information, configuration information, image information, billing information, elastic network interface, monitoring, security groups, and operation logs.



Querying Instance Metadata

Last updated: 2023-09-07 17:01:44

Instance metadata refers to data relevant to an instance. It can be used for configuring or managing a running instance.

> **Note**
> Although instance metadata can only be accessed from within the instance itself, the data is not encrypted. Anyone with access to the instance can view its metadata. Therefore, you should take appropriate precautions to protect sensitive data.

Overview

Tencent Cloud provides the following metadata:

Name	Description	Version
instance-id	Unique instance ID	1.0
instance-name	Instance Name	1.0
uuid	Unique instance ID	1.0
local-ipv4	Instance private IP address	1.0
public-ipv4	Instance public IP address	1.0
mac	MAC address of the instance's eth0 device	1.0
placement/region	Instance region	Updated on September 19, 2017
placement/zone	Instance availability zone	Updated on September 19, 2017
network/interfaces/macs/${mac}/mac	MAC address of the instance’s network interface	1.0
network/interfaces/macs/${mac}/primary-local-ipv4	Primary private IP of the instance’s network interface	1.0
network/interfaces/macs/${mac}/public-ipv4s	Public IP address of the instance’s network interface	1.0
network/interfaces/macs/${mac}/vpc-id	VPC ID of the instance’s network interface	Updated on September 19, 2017
network/interfaces/macs/${mac}/subnet-id	Subnet ID of the instance’s network interface	Updated on September 19, 2017
network/interfaces/macs/${mac}/local-ipv4s/${local-ipv4}/gateway	Gateway address of the instance’s network interface	1.0
network/interfaces/macs/${mac}/local-ipv4s/${local-ipv4}/local-ipv4	Private IP address of the instance’s network interface	1.0

network/interfaces/macs/${mac}/local-ipv4s/${local-ipv4}/public-ipv4	Public IP address of the instance's network interface	1.0
network/interfaces/macs/${mac}/local-ipv4s/${local-ipv4}/public-ipv4-mode	Public network mode of the instance's network interface	1.0
network/interfaces/macs/${mac}/local-ipv4s/${local-ipv4}/subnet-mask	Subnet mask of the instance's network interface	1.0
payment/charge-type	Instance billing plan	Updated on September 19, 2017
payment/create-time	Instance creation time	Updated on September 19, 2017
payment/termination-time	Instance termination time	Updated on September 19, 2017
app-id	AppID of the user to which the instance belongs	Updated on September 19, 2017
as-group-id	Auto scaling group ID of the instance	Updated on September 19, 2017
spot/termination-time	Spot instance termination time	Updated on September 19, 2017
instance/instance-type	Instance Specification	Updated on September 19, 2017
instance/image-id	Instance image ID	Updated on September 19, 2017
instance/security-group	Information of the security group bound to the instance	Updated on September 19, 2017
instance/bandwidth-limit-egress	Instance private network outbound bandwidth limit, in Kbit/s	Updated on September 29, 2019
instance/bandwidth-limit-ingress	Instance private network inbound bandwidth limit, in Kbit/s	Updated on September 29, 2019
cam/security-credentials/${role-name}	Temporary credentials generated by the instance CAM role policy. You can only obtain temporary credentials if the instance is bound to a CAM role. Replace the ${role-name} parameter with the name of the instance CAM role. If not specified, a 404 error will be returned.	Updated on December 11, 2019
volumes	Instance storage	1.0

Note

- In the table above, the `${mac}` and `${local-ipv4}` fields represent the device address and private IP address of the specified network interface for the instance, respectively.

- The destination URL address of the request is case-sensitive. Please strictly construct the destination URL address of a new request based on the returned result of the request.
- The current version has made changes to the placement return data. If you need to use data from a previous version, you can specify the previous version path or not specify a version path to access data from version 1.0. For placement return data, please refer to Region and Availability Zone.

Querying Instance Metadata

After logging in to an instance, you can access the metadata such as its local IP address and public IP address to manage connections with external applications.
To view all the instance metadata within a running instance, use the following URI:

```
http://metadata.tencentyun.com/latest/meta-data/
```

You can access the metadata by using cURL or an HTTP GET request, for example:

```
curl http://metadata.tencentyun.com/latest/meta-data/
```

- For non-existent resources, an HTTP error code 404 – Not Found will be returned.
- Operations on instance metadata can only be performed from **within the instance**. Please log in to the instance first. For more information on logging in to instances, refer to Logging In to a Windows Instance and Logging In to a Linux Instance.

Sample metadata query

The following example shows how to obtain the metadata version.

Note
When Tencent Cloud modifies the metadata access path or returned data, a new metadata version is released. If your application or script relies on the structure or returned data of a previous version, you can access the metadata using a specified earlier version. If no version is specified, version 1.0 will be accessed by default.

```
[qcloud-user]# curl http://metadata.tencentyun.com/
1.0
2017-09-19
latest
meta-data
```

The following example demonstrates how to view the metadata root directory. Words ending with `/` represent directories, while those not ending with `/` represent data access. For the specific meanings of data access, please refer to the previous section on **Instance Metadata Categories**.

```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/
instance-id
instance-name
local-ipv4
mac
network/
placement/
public-ipv4
```

```
uuid
```

The following example demonstrates how to obtain the physical location information of an instance. For the relationship between the returned data and the physical location, please refer to the Regions and Availability Zones document.

```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/placement/region
ap-guangzhou

[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/placement/zone
ap-guangzhou-3
```

The following example demonstrates how to obtain the private IP address of an instance. When multiple network cards are present, the network address of the eth0 device is returned.

```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/local-ipv4
10.104.13.59
```

The following shows how to obtain the public IP address of an instance.

```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/public-ipv4
139.199.11.29
```

The following example demonstrates how to obtain the Instance ID. The Instance ID is the unique identifier of the instance.

```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/instance-id
ins-3g445roi
```

The following example demonstrates how to obtain the instance UUID. The instance UUID can serve as a unique identifier for the instance, but it is recommended to use the instance ID for distinguishing instances.

```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/uuid
cfac763a-7094-446b-a8a9-b995e638471a
```

The following example shows how to obtain the MAC address of an instance's eth0 device.

```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/mac
52:54:00:BF:B3:51
```

The following example demonstrates how to obtain instance network interface information. Multiple network interfaces will return multiple lines of data, with each line representing the data directory of a network interface.

```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/network/interfaces/macs/
52:54:00:BF:B3:51/
```

The following shows how to obtain the information of a specified ENI.

```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-
data/network/interfaces/macs/52:54:00:BF:B3:51/
local-ipv4s/
```

```
mac
vpc-id
subnet-id
owner-id
primary-local-ipv4
public-ipv4s
local-ipv4s/
```

The following shows how to obtain the VPC information of a specified ENI.

```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-
data/network/interfaces/macs/52:54:00:BF:B3:51/vpc-id
vpc-ja82n9op

[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-
data/network/interfaces/macs/52:54:00:BF:B3:51/subnet-id
subnet-ja82n9op
```

The following example demonstrates how to obtain a list of private IP addresses bound to a specified network interface. If the network interface is bound to multiple private IPs, multiple lines of data will be returned.

```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-
data/network/interfaces/macs/52:54:00:BF:B3:51/local-ipv4s/
10.104.13.59/
```

The following shows how to obtain the information of a private IP address.

```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-
data/network/interfaces/macs/52:54:00:BF:B3:51/local-ipv4s/10.104.13.59
gateway
local-ipv4
public-ipv4
public-ipv4-mode
subnet-mask
```

The following example demonstrates how to obtain the private IP gateway. This information is only available for instances in VPCs. For more information on VPC instances, see Private Network.

```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-
data/network/interfaces/macs/52:54:00:BF:B3:51/local-ipv4s/10.104.13.59/gateway
10.15.1.1
```

The following example demonstrates how to obtain the private IP access mode for public networks. Only VPC instances can query this data. Instances in the basic network access the public network through a public gateway.

```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-
data/network/interfaces/macs/52:54:00:BF:B3:51/local-ipv4s/10.104.13.59/public-ipv4-mode
NAT
```

The following shows how to obtain the public IP address bound to a private IP address.

```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-
data/network/interfaces/macs/52:54:00:BF:B3:51/local-ipv4s/10.104.13.59/public-ipv4
139.199.11.29
```

The following shows how to obtain the subnet mask of a private IP address.

```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-
data/network/interfaces/macs/52:54:00:BF:B3:51/local-ipv4s/10.104.13.59/subnet-mask
255.255.192.0
```

The following shows how to obtain the billing plan of an instance.

```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/payment/charge-type
POSTPAID_BY_HOUR
```

The following shows how to obtain the creation time of an instance.

```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/payment/create-time
2018-09-18 11:27:33
```

The following example demonstrates how to obtain the instance termination time (for prepaid mode only).

```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/payment/termination-time
2018-10-18 11:27:33
```

The following example shows how to obtain the termination time for spot instances.

```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/spot/termination-time
2018-08-18 12:05:33
```

The following example shows how to obtain the account AppId to which the CVM belongs.

```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/app-id
123456789
```

The following example demonstrates how to obtain temporary credentials generated by the CAM role of an instance. CVMas is the role name used in the example.

```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/cam/security-
credentials/CVMas
{
  "TmpSecretId": "AKIDoQMxA6cW447p225cIt9NW8dhA1dwl5UvxxxxxxxxxUqRlEb5_",
  "TmpSecretKey": "Q9z24VucjF4xQQN1PEsH3exxxxxxxxxgA=",
  "ExpiredTime": 1615590047,
  "Expiration": "2021-03-12T23:00:47Z",
  "Token": "xxxxxxxxxxx",
  "Code": "Success"
}
```

The following example demonstrates how to obtain instance storage.

```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/volumes
disk-xxxxxxxx/
```

Querying Instance User Data

You can specify instance user data when creating an instance. CVM instances having cloud-init configured can access the data.

Retrieving User Data

After login, you can access user data by using the following method.

```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/user-data
179, client, shanghai
```

Renaming instance

Last updated: 2024-05-15 17:15:01

Scenario

To help users manage CVM instances on the console and locate CVMs quickly by name, Tencent Cloud allows users to rename an instance at any time and the new name takes effect instantly.

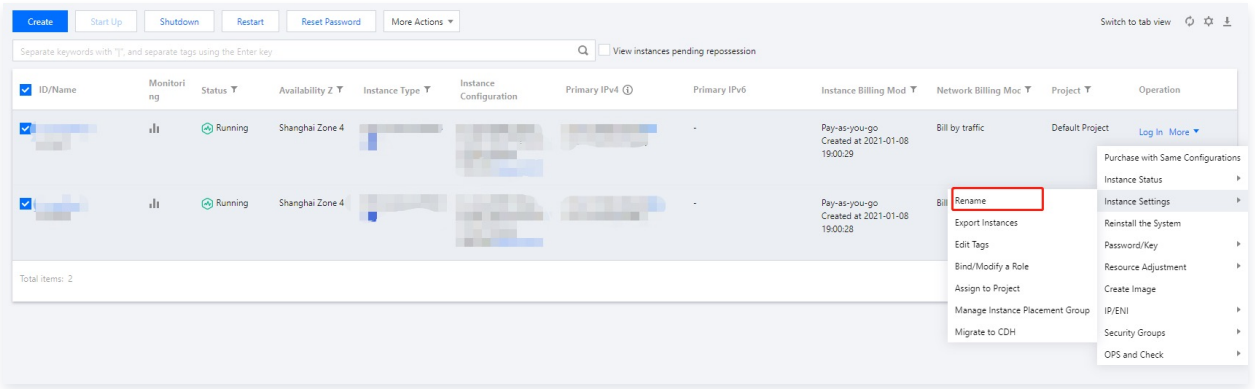
Instructions

On the instance management page, proceed according to the actually used view mode:

List view

Modifying the name of an instance

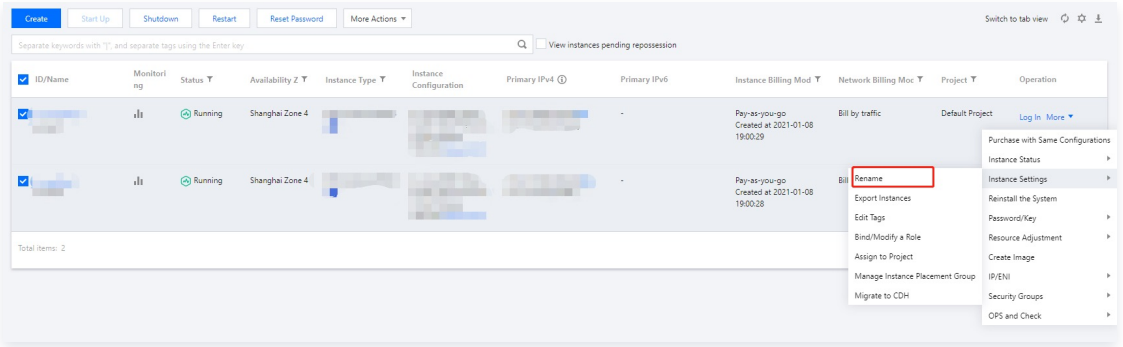
1. Log in to the CVM console.
2. In the row of the target instance in the instance list, select **More** > **Instance Settings** > **Rename** on the right as shown below:



3. In the "Rename" pop-up window, enter the new instance name and click "Confirm".

Modifying the names of multiple instances

1. Log in to the CVM console.
2. In the instance list, select multiple CVMs whose names need to be changed, and choose **More** > **Instance Settings** > **Rename** at the top. As shown below:



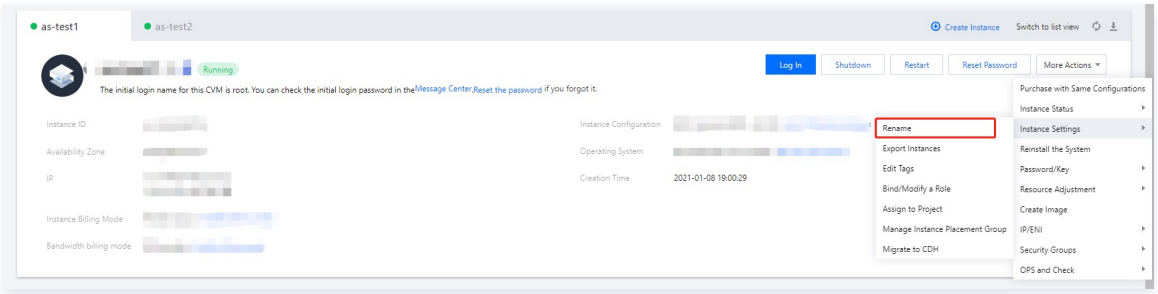
3. In the "Rename" pop-up window, enter the new instance name and click "Confirm".

Note

> CVMs modified using this method will have the same instance name.

Tab view

1. Log in to the CVM console.
2. Select the tab of the target CVM instance, and click **More Actions** > **Instance Settings** > **Rename** in the top-right corner of the page, as shown below:



3. In the "Rename" pop-up window, enter the new instance name and click "Confirm".

Resetting Instance Password

Last updated: 2023-09-26 16:21:07

Scenario

CVMs offer the functionality to reset instance login passwords. This is mainly applicable in the following scenarios:

- Log in to an instance remotely on a local computer for the first time.
- Reset the user (root) password before the first remote login or SSH key login of a Linux instance.
- Before the first login to a Windows or Linux instance, if you selected **Auto-generate Password** as the **Login Method** during instance creation, it is recommended to reset the administrator account (e.g., Administrator) password through this operation and replace it with a custom login password.
- Reset the password if you have forgotten your instance login password.

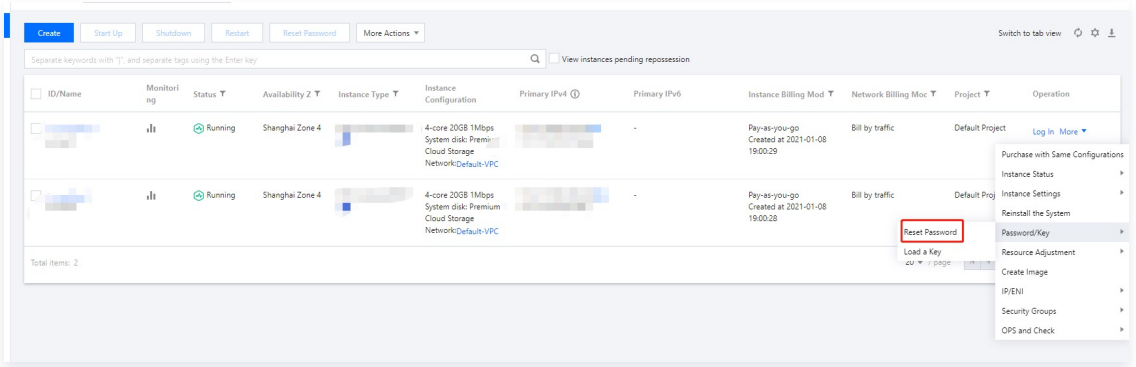
Supports and Limits

- The CVM console supports two methods for resetting passwords: **Online Reset** and **Offline Reset**.
- If you choose to reset the password offline, the server will be shut down during the process for instances that are currently running. To avoid data loss, please plan the operation ahead of time and perform it during off-peak business hours to minimize the impact.
- If you choose to reset the password online, ensure that both the Instance Status and TAT Agent Status of the selected instance are Running.

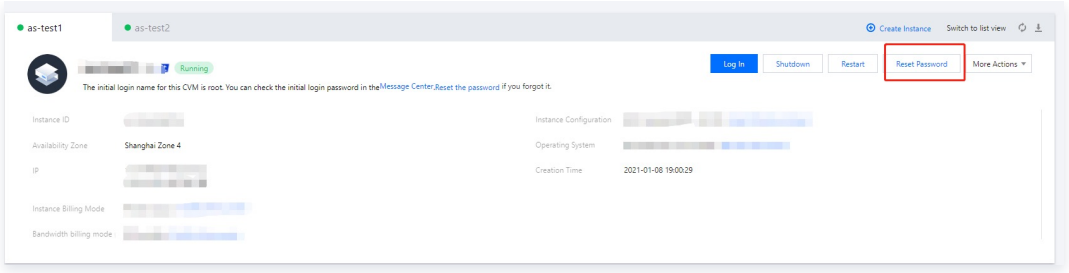
Instructions

Resetting the password for a single instance

1. Log in to the CVM console.
2. On the instance management page, proceed according to the actually used view mode:
   - **List View**: On the right side of the row where the CVM instance requiring a password reset is located, click **More** > **Password/Key** > **Reset Password**, as shown in the following figure:

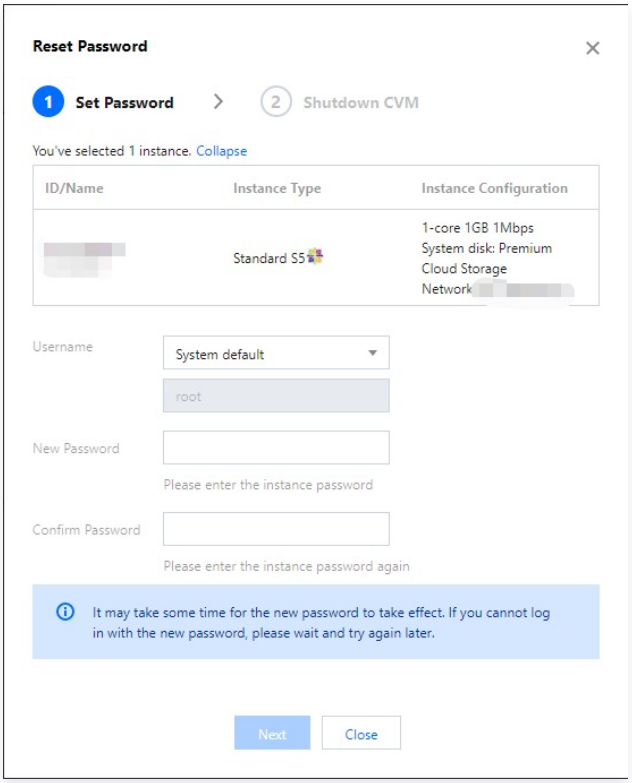


   - **Tab View**: On the page of the CVM instance that requires a password reset, click **Reset Password**. As shown in the following figure:

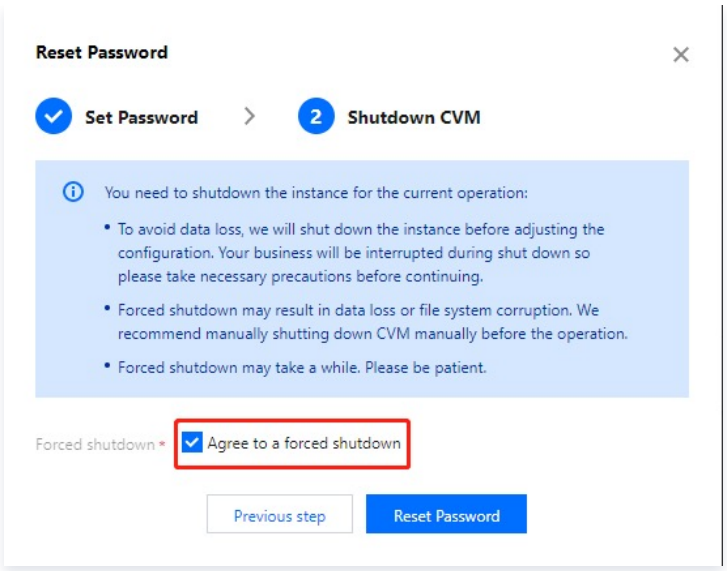


3. In the **Reset Password** step, select the **Username** type, enter the username for which the password needs to be reset, as well as the corresponding **New Password** and **Confirm Password**, then click **Next**. As shown in the image below:

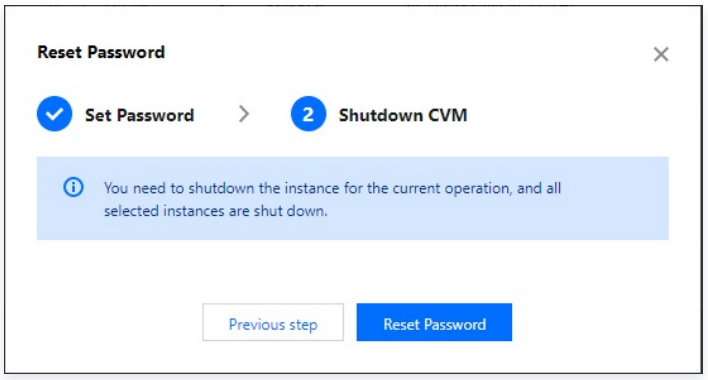
> **Note**
> By default, the **User Name** type is set to **System Default**, using the default user name for the corresponding operating system (Windows: `Administrator`, Ubuntu: `ubuntu`, other Linux versions: `root`). If you need to specify a different user name, select **Specify User Name** and enter the corresponding user name.



4. During the shutdown prompt step, the password reset operation may vary depending on the instance status, as detailed below:
   - If the instance requiring a password reset is in the **Running** state, select **Agree to a Forced Shutdown** and click **Reset Password** to complete the reset, as shown in the following figure:

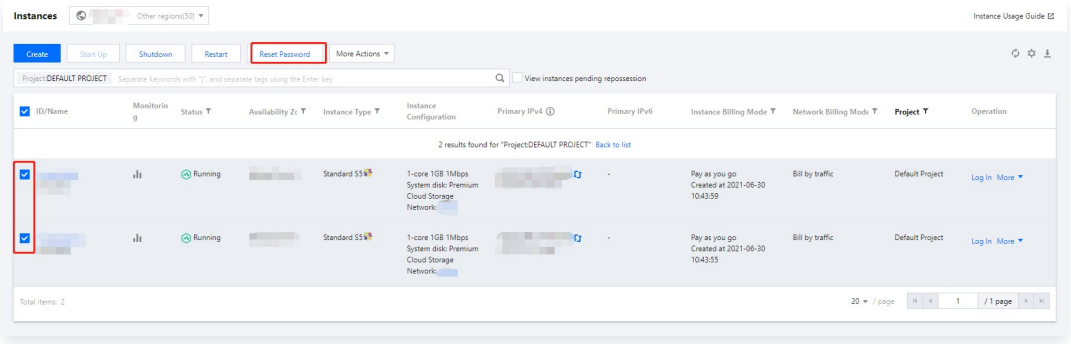


- If the instance requiring a password reset is in the "**Shutdown CVM**" state, click **Reset Password** to complete the reset, as shown in the following figure:



Reset passwords for multiple instances.

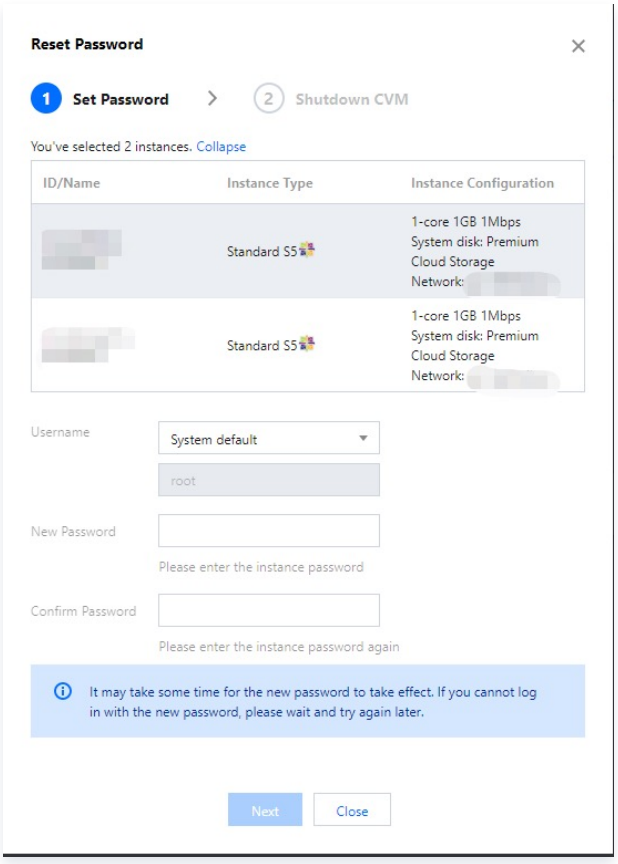
1. Log in to the CVM console.
2. On the instance management page, select the CVMs for which you need to reset the password, and click **Reset Password** at the top, as shown in the figure below:



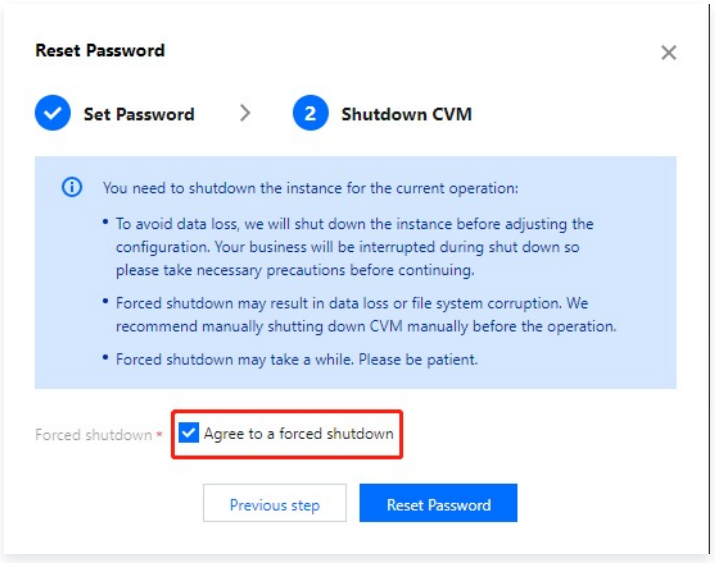
3. In the **Reset Password** step, select the **Username** type, enter the username for which the password needs to be reset, as well as the corresponding **New Password** and **Confirm Password**, then click **Next**. As shown in the image below:

> ⚠ Note

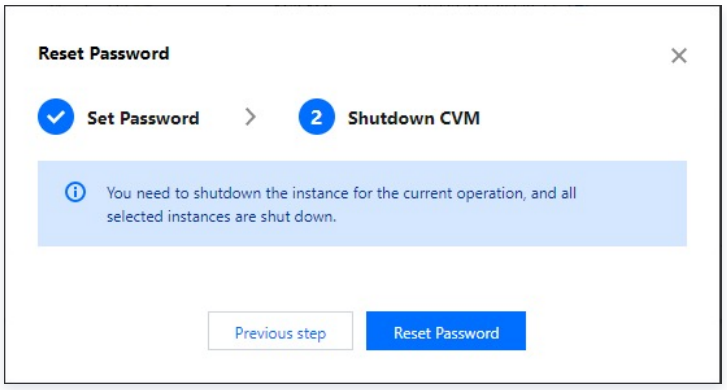
> By default, the **User Name** type is set to "System Default" and uses the default user name for the corresponding operating system (Windows: `Administrator`, Ubuntu: `ubuntu`, other Linux versions: `root`). If you need to specify a different user name, select **Specify User Name** and enter the corresponding user name.



4. In the **Shutdown Prompt** step, the password reset operation varies depending on the instance status, as detailed below:
   - If the instance requiring a password reset is in the **Running** state, select **Agree to a Force Shutdown** and click **Reset Password** to complete the reset, as shown in the following figure:



   - If the instance requiring a password reset is in the **Shutdown CVM** state, click **Reset Password** to complete the reset, as shown in the following figure:



Online Password Reset

Note:
Prerequisites: Ensure that both the **Instance Status** and **TAT Agent Status** of the selected instance are **Running**, otherwise, you will not be able to reset the password online.

1. Confirm the **username** for which the password needs to be reset.

   Note:
   The default username for Ubuntu systems is `ubuntu`.

2. Enter a **New Password** and **Confirm Password** that meet the complexity requirements.

   Note:
   When selecting both Linux and Windows instances simultaneously, the password complexity requirements must follow the Windows system requirements.

3. Click **OK** to complete the reset.
4. After resetting the password, you can go to the target instance's details page to view the reset password result. Select **Execute Command** and click on the "View Execution Details" on the right side of the command row.

Note:
- For Linux instances, if the PasswordAuthentication parameter in the sshd_config configuration file is set to "No", the parameter value will be changed to "Yes" during an online password reset. Additionally, the sshd process within the instance will be restarted, which may cause interruptions to connected SSH sessions.
- For Windows instances, if the user you choose to reset the password for is locked or disabled, the user will be automatically enabled during the online password reset process.
- If you encounter failures or invalid results while resetting the password online, please refer to Windows Instance: Troubleshooting Failed or Invalid Password Resets to identify the cause.

Offline Password Reset

Note:
If you choose to reset the password offline, the server will be shut down during the process for instances that are currently running. It is recommended to perform this operation during off-peak hours to minimize the impact of shutting down the server.

1. Confirm the **username** for which the password needs to be reset.

   Note:
   The default username for Ubuntu systems is `ubuntu`.

2. Enter a **New Password** and **Confirm Password** that meet the complexity requirements.

   Note:
   When selecting both Linux and Windows instances simultaneously, the password complexity requirements must follow the Windows system requirements.

3. Read and check the **Offline Reset Notice**, then click **OK** to complete the reset.

Note:
If you encounter a failed or invalid password reset for a Windows instance while using the offline reset method, please refer to Troubleshooting Failed or Invalid Online Password Resets.

Managing Instance IP Addresses
Getting Private IP Addresses and Setting DNS

Last updated: 2024-06-26 11:56:31

Scenario

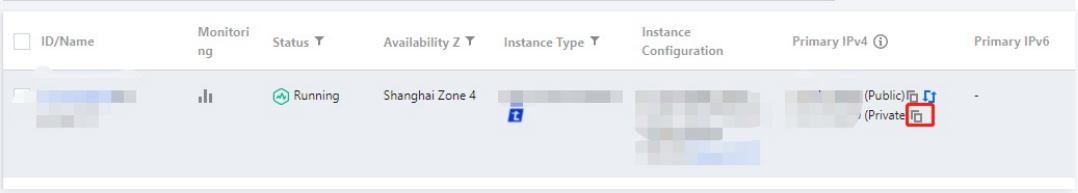
This document describes how to obtain the private IP address of a CVM instance and configure the private DNS.

Instructions

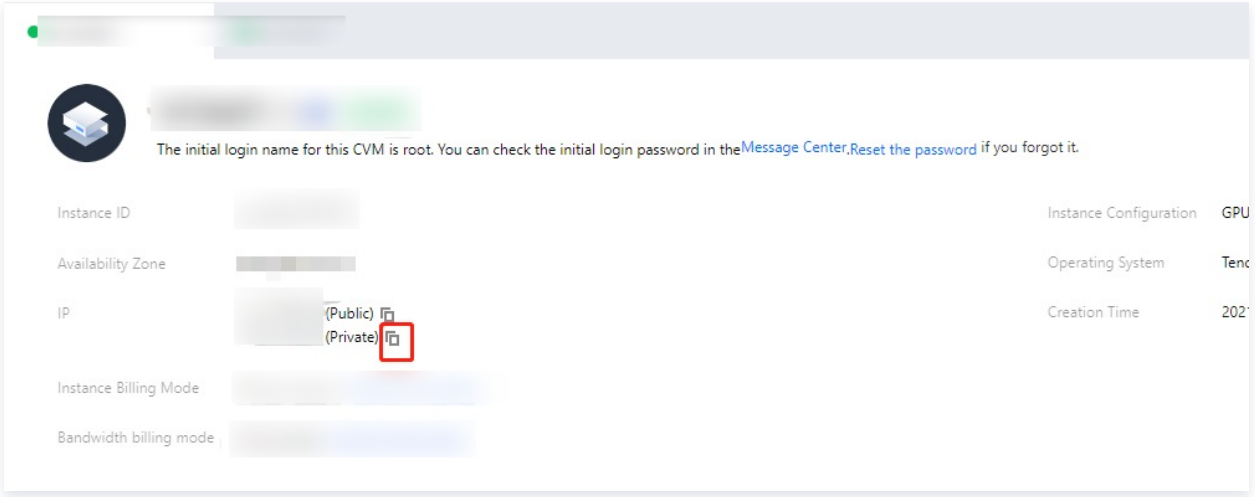
Obtaining the private IP address of an instance

Acquiring via the console

1. Log in to the CVM console.
2. On the instance management page, proceed according to the actually used view mode:
   - **List View:** Select the instance for which you want to view the private IP, move the cursor to the **Main IP Address** column, and click to copy the private IP. As shown in the image below:



   - **Tab View:** On the instance page, click the icon next to the private IP address in the **IP Address** section to copy the private IP. As shown below:



Acquiring through APIs

For more information, see the DescribeInstances API.

Obtaining through instance metadata

1. Log in to the CVM.
2. Access the instance metadata by using the cURL tool or an HTTP GET request.

> **Note**
> The following operations use the cURL tool as an example.

Execute the following command to obtain the private IP.

```
curl http://metadata.tencentyun.com/meta-data/local-ipv4
```

The returned information is the private IP address, as shown below:

```
[root@VM_58_27_centos ~]# curl http://metadata.tencentyun.com/meta-data/local-ipv4
10.XXX.XX.27
```

For more information on instance metadata, see Viewing Instance Metadata.

Configuring private network DNS

When a network resolution error occurs, you can manually configure the private network DNS based on your CVM operating system.

Linux system

1. Log into the Linux CVM.
2. Run the following command to open the `/etc/resolv.conf` file.

```
vi /etc/resolv.conf
```

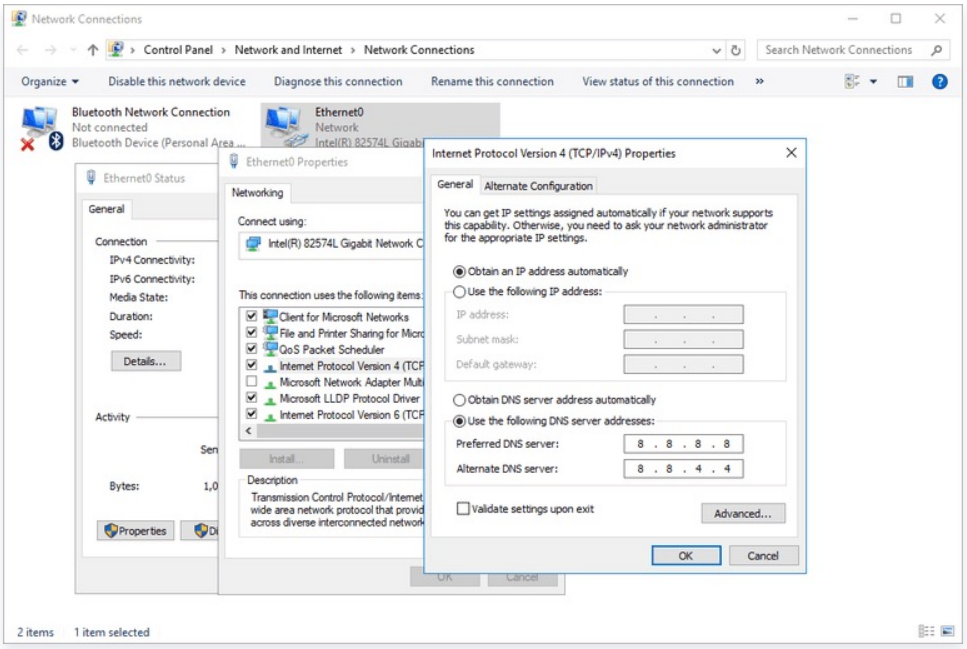
3. Press **i** to switch to edit mode, and modify the DNS IP according to the network type (basic network/private network) and region in the Private Network DNS list. If it is a private network, all regions share the same DNS IP without distinguishing regions.
For example, change the private DNS IP of the basic network in the Beijing region to the private DNS server of the basic network in the Beijing region.

```
nameserver 10.53.216.182
nameserver 10.53.216.198
options timeout:1 rotate
```

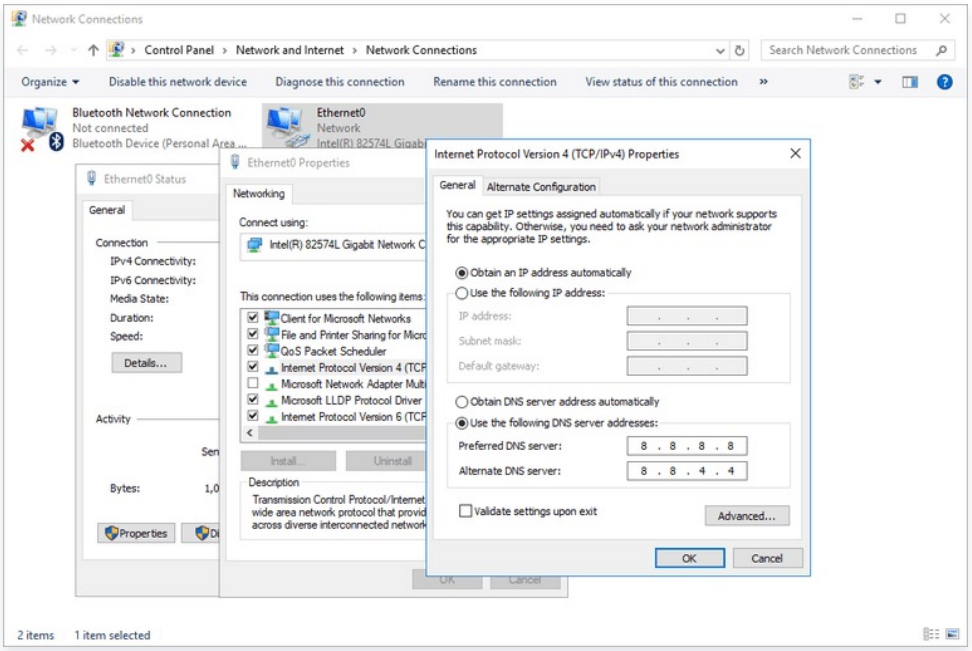
4. Press **Esc**, enter **:wq**, and save and close the file.

For Windows systems

1. Log in to the Windows CVM.
2. On the operating system interface, open **Control Panel** > **Network and Sharing Center** > **Change Adapter Settings**.
3. Right-click the **Ethernet** icon and select **Properties** to open the **Ethernet Properties** window.
4. In the **Ethernet Properties** window, double-click to open Internet Protocol Version 4 (TCP/IPv4), as shown in the figure below:



5. Select **Use the following DNS server addresses** and modify the DNS IP according to the corresponding region in the Private Network DNS list.



6. Click **OK**.

Modifying Private IP Addresses

Last updated: 2024-06-02 10:51:51

Scenario

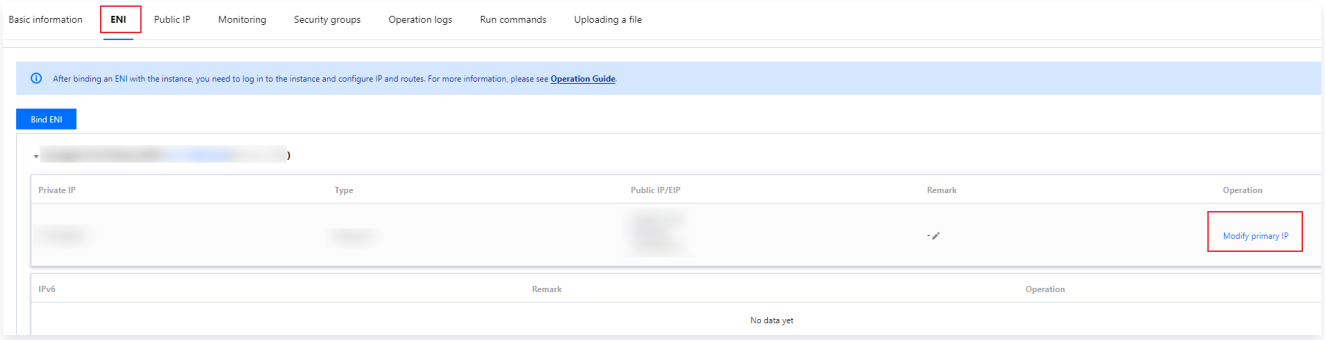
You can directly modify the private IP of a Cloud Virtual Machine (CVM) instance in the Virtual Private Cloud (VPC) through the console, or change the instance's private IP by changing the subnet to which the CVM instance belongs. This document guides you on how to modify the private IP of a CVM instance in a VPC through the Tencent Cloud CVM console.
For information on changing subnets, please refer to Changing Instance Subnet.

Limits

- Modifying the primary IP of a primary ENI may cause the CVM to restart.
- The primary IP of a secondary ENI cannot be modified.

Instructions

1. Log in to the CVM console.
2. Select the region of the instance whose private IP you want to modify, and click the instance ID/name to enter its details page.
3. In the Instance Details page, select the **ENI** tab and click ▸ to expand the primary ENI.
4. In the primary ENI's operation column, click **Modify Primary IP**.



5. In the "Modify Primary IP" window that pops up, enter the new IP and click **OK**. The changes will take effect after the instance has finished restarting.

> **Note**
> You can only enter a private IP that belongs to the current subnet CIDR.

Getting Public IP Addresses

Last updated: 2023-09-07 17:04:22

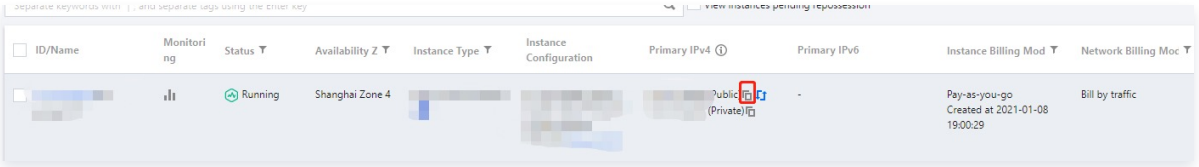
Scenario

This document describes how to obtain the public IP address through console, API, or Instance metadata.

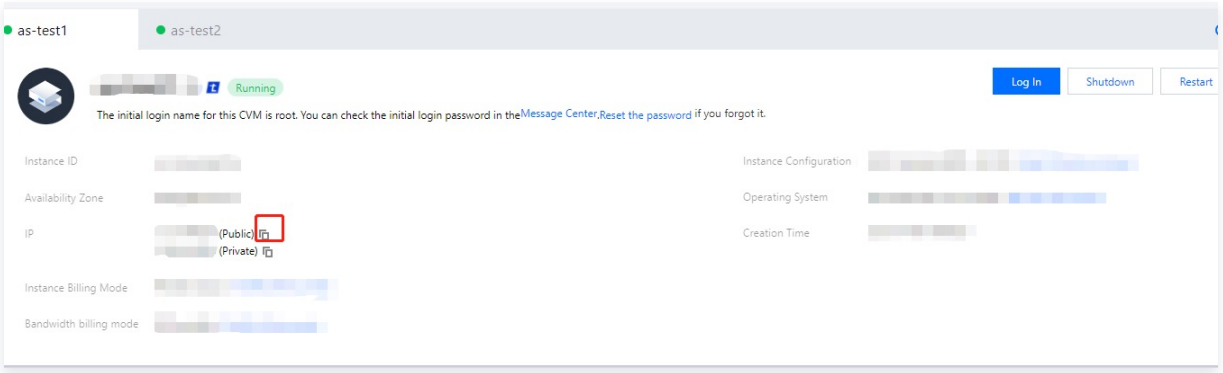
Instructions

Acquiring via the console

1. Log in to the CVM console.
2. On the Instance console management page, proceed according to the used view mode:
   - **List View**: Hover over the Primary IPv4 Address column and click to copy the IP address, as shown below:



   - **Tab View**: On the instance page, click after the public address in **IP Address** to copy the public IP. As shown in the figure:



> **Note**
> Since the public IP address is mapped to the private IP address through NAT, you will not see the public IP address when viewing the network interface properties within the instance (e.g., using `ifconfig (Linux)` or `ipconfig (Windows)` commands). To determine the public IP address of the instance from within the instance, refer to Obtaining via Instance Metadata.

Acquiring through APIs

Please refer to the DescribeDBLogFiles related interface.

Obtaining through instance metadata

1. Log in to the CVM instance.
   For specific login methods, refer to Logging in to Linux Instance and Logging in to Windows Instance.
2. To obtain the public IP address, you can access the metadata by using the cURL tool or an HTTP GET request.

```
curl http://metadata.tencentyun.com/meta-data/public-ipv4
```

If the returned value is in the following structure, you can view the public IP address:

For more information, see Querying Instance Metadata.

Changing Public IP Addresses

Last updated: 2023-09-26 17:27:21

This article outlines two methods for changing the public IP address.

- Directly change the public IP: Applicable to scenarios where the CVM already has a standard public IP.
- Switch to an EIP first, then unbind the EIP: Applicable to scenarios where traditional account type users need to change their public IP address.

Supports and Limits

If you choose **Directly change the public IP**, please note the following considerations:

- Each account can change the public IP address up to three times per day in each region.
- Each instance **can only change its public IP once**.
- **The original public IP will be released after the change.**

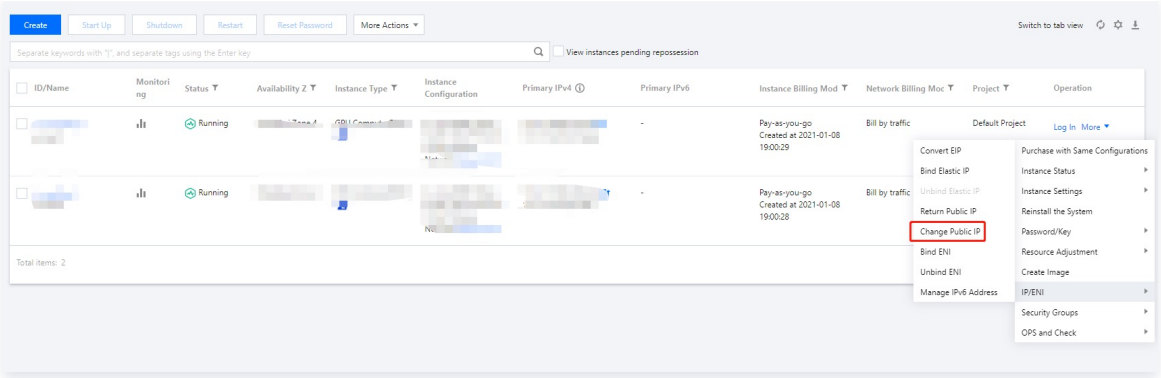
If you choose **Switch to an EIP first, then unbind the EIP**, please note the following considerations:

- When an EIP is bound to a cloud server instance, the current public IP address of the instance will be released.
- Each account has a quota of 20 Elastic Public IPs per region.
- To ensure the effective utilization of IP resources, EIPs not bound to instances will be charged an IP Resource Fee on an hourly basis.

Instructions

Method 1: Replace public IP directly

1. Log in to the CVM console.
2. On the instance management page, select the region of the CVM with the IP to be converted, and in the corresponding CVM row, click **More** > **IP/ENI** > **Change Public IP**, as shown in the following figure:



3. In the pop-up "Replace IP" window, click **Confirm** to complete the change.

Method 2: First convert to Elastic Public IP, and then unbind Elastic Public IP

> **Note**
> This method is only applicable to bill-by-CVM account types.

Step 1: Change the Elastic IP

1. Log in to the CVM console.
2. On the instance management page, select the region of the CVM with the IP to be converted, and click in the corresponding row of the CVM.

3. In the pop-up "Convert to Elastic Public IP" window, click **OK**.

Step 2: Unbind the EIP

1. After the conversion is complete, find the target CVM, click **More** > **IP/Network Card** > **Unbind EIP**.
2. In the "Unbind EIP" pop-up window, check the box **Reassign a standard public IP after unbinding**, and click **OK**.
3. In the pop-up prompt, click **OK** to complete the change.

Step 3: Release the EIP (optional)

> **Note**
> Since the unbound EIP still remains under the account when unbinding an EIP, it is recommended to perform the following operation to release the EIPs not bound to instances, in order to avoid incurring charges for idle and unused IPs.

1. Log in to the Public IP console.
2. At the top of the Public IP page, select the recently unbound EIP, then click **More** > **Release**.
3. In the pop-up "Confirm to release the selected EIP?" window, check **Confirm to release the above IP** and click **Release**.

Changing Security Group

Last updated: 2024-05-15 17:46:12

Scenario

A security group is a stateful packet filtering virtual firewall used to configure network access control for single or multiple CVM instances. It is an essential network security isolation measure provided by Tencent Cloud. When creating a CVM instance, it is necessary to configure a security group for the instance. Tencent Cloud allows users to change the security group associated with a CVM instance after its creation.

> **Note**
> If you want to configure a new security group for the instance, please create a new security group first. For detailed instructions, see Create a Security Group.

Preparations

You have logged in to the CVM console.

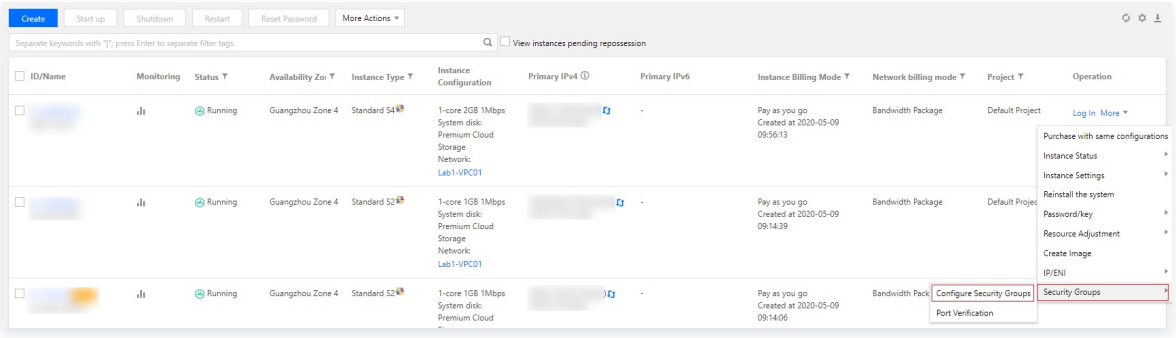
Instructions

Change the configured security group

On the instance management page, proceed according to the actually used view mode:

List View

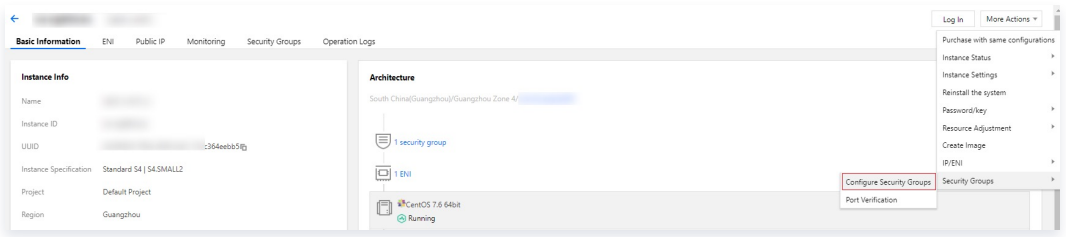
1. On the instance management page, select a CVM instance that needs to be reassigned to a new security group, and click **More** > **Security Groups** > **Configure Security Groups**. As shown in the image below:



2. In the "Configure Security Groups" window that appears, select the new security group name(s) and click **OK** to complete the security group change.

Tab Mode

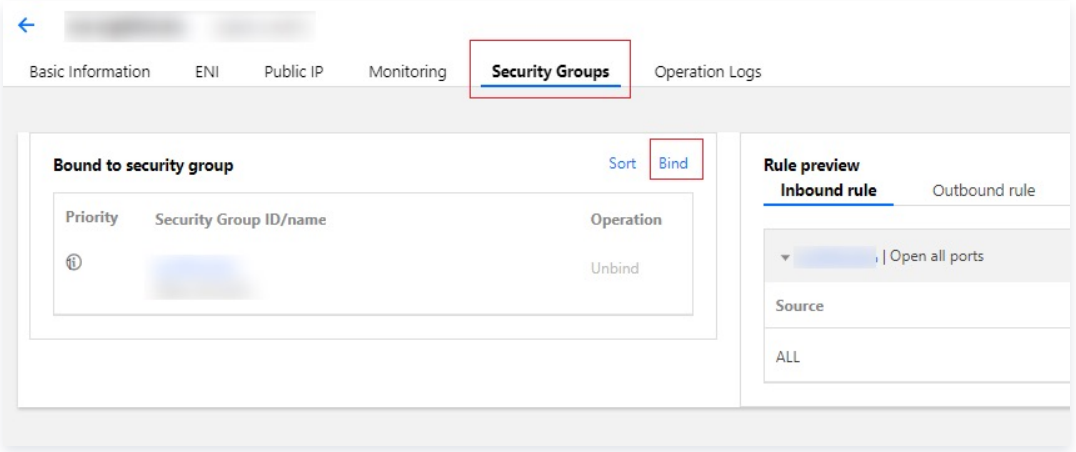
1. On the instance management page, select a tab of the CVM instance for which a new security group needs to be configured.
2. On the instance details page, select the top-right **More Actions** > **Security Groups** > **Configure Security Groups**, as shown below:



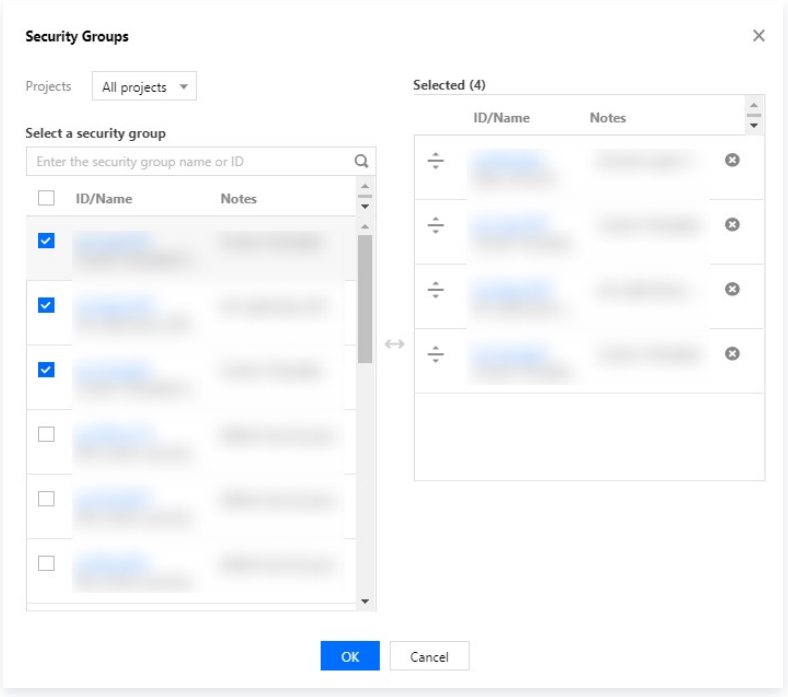
3. In the "Configure Security Groups" pop-up window, select the new security group name(s) (multiple selections allowed), and click **OK**.

Change the bound security group

1. On the instance management page, click the CVM instance ID/name for which you want to bind the security group and enter the instance details page.
2. On the Instance Details page, select the **Security Groups** tab, and in the "Bound to security group" section, click **Bind**. As shown in the image below:



3. In the "Security Groups" pop-up window, select the security groups you need to bind according to your requirements, and click **OK** to complete the binding. As shown in the following figure:



Changing the Billing Mode from Pay-As-You-Go to monthly Subscription

Last updated: 2024-06-02 09:50:32

Scenario

Tencent Cloud CVM allows you to change the instance billing mode from pay-as-you-go to monthly subscription for long-term and stable use. You can change the billing mode in the CVM console or by using Cloud API. This document describes how to change the billing mode of a CVM instance from pay-as-you-go to monthly subscription in the CVM console.

Switching rules

The CVM console allows you to switch the billing mode based on the following rules:

- You can change the billing mode of one or multiple CVM instances at a time.
- A renewal order is generated for the change of billing mode. The change takes effect only after you pay for the renewal order.
  If the payment is suspended or failed, you can view the order and make the payment on the Order Center page.
- The five-day free return policy does not apply to CVM instances whose billing mode is changed from pay-as-you-go to monthly subscription.
- The new billing period of a changed CVM instance starts the moment when the billing mode is changed.
- Before you make the payment of the renewal order, you cannot change the billing mode of a CVM instance again.
- Before you make the payment of the order, if the configuration information of the instance mismatches the order amount due to changes such as the adjustment of instance specifications, bandwidth, or disks, or system reinstallation, the payment is prohibited. In this case, you must cancel the unpaid order in the Order Center and start a new change process.
- The pay-as-you-go to monthly subscription feature supports synchronous conversion of instance and disk billing modes. After the instance billing mode is changed, the network bandwidth billing mode remains unchanged, except for standard account types with ordinary public IPs billed by hourly bandwidth and traditional account types with hourly bandwidth, which can be changed to bandwidth package monthly subscription billing.

Usage Limits

- If the remaining monthly subscription quota in the availability zone is less than the number of instances to be converted, the conversion is not supported. To proceed, please increase the instance purchase quota and try again.
- Non-pay-as-you-go instances cannot be switched.
- Spot instances cannot be converted.
- Instances with network billing mode set to bill-by-usage period of bandwidth are not supported for conversion.
- Instances using images from the Cloud Marketplace are not eligible for conversion.
- Batch instances BC1 and BS1 do not support conversion.
- Instances with pending conversion orders cannot be switched.
- Instances with scheduled termination cannot be switched. To switch, please cancel the scheduled termination first and then proceed with the conversion.

Instructions

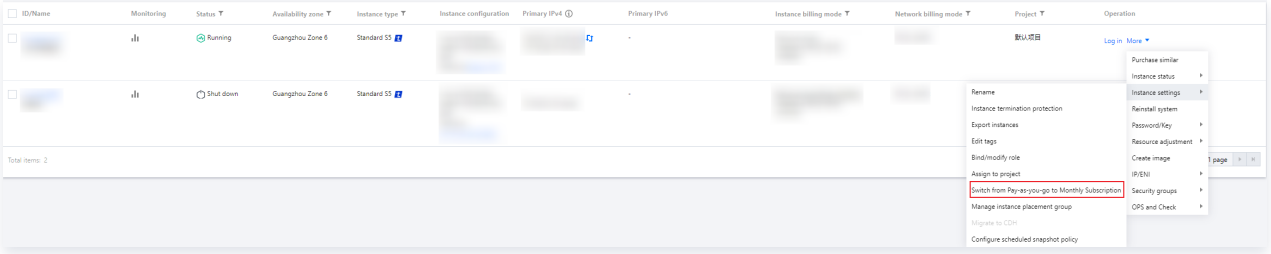
1. Log in to the CVM console.
2. On the instance management page, select one or more instances as needed.

Converting a single instance

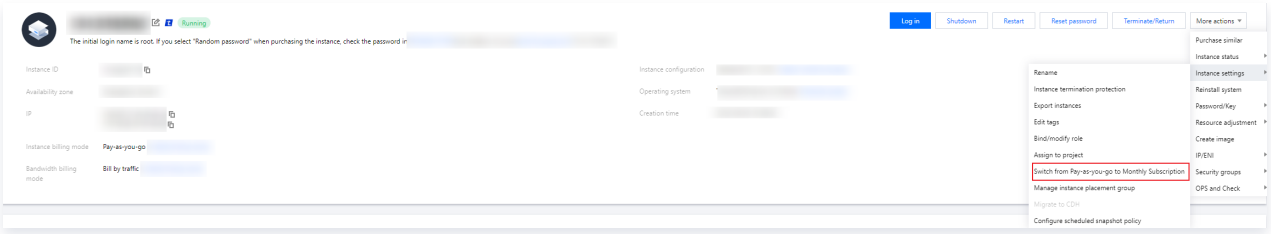
On the instance management page, proceed according to the actually used view mode:

- **List view**: In the Actions column of the target instance, choose **More** > **Instance settings** > **Switch from pay-as-you-go to monthly subscription**,

> **Note**
> You can also select the instances you want to change, and click **More Actions** > **Switch to Monthly Subscription** at the top.



- **Tab View**: In the instance page, select **More Actions** > **Instance Settings** > **Switch from Pay-as-you-go to Monthly Subscription** in the upper right corner.



Switching multiple instances

Select all instances you want to switch, and click **More Actions** > **Switch to Monthly Subscription** at the top to change the billing mode of multiple instances,
Instances that cannot be switched will display the reason.

3. In the "Pay-as-you-go to Monthly Subscription" pop-up window, set the renewal duration and whether to enable auto-renewal according to your needs:
   - Renewal period: Select the validity period after converting to a monthly subscription. If you are converting multiple instances at once, you must set the same validity period for all instances.
   - Auto-Renewal: Choose auto-renewal based on your requirements.
4. Check the box "**I have read and agreed to the Rules on Switching from Pay-as-you-go to Monthly Subscription**", and click **Switch Now**. If there are no pending orders for the instance, you will be redirected to the payment page.
5. Follow the prompts on the page and complete the payment to finish the conversion process.

FAQs Overview

For any questions about the change, see FAQs about Billing.

Swhitching the billing mode from monthly subscription to pay-as-you-go

Last updated: 2023-09-26 17:45:17

Scenario

Tencent Cloud CVM allows you to switch the instance billing mode from monthly subscription to pay-as-you-go. This document describes how to do it in the CVM console.

> **Note**
> - The monthly subscribed instances in shutdown status will be retained after they are switched to pay-as-you-go instances, and they will continue to incur fees. You can enable the "No Charge when Shut Down" feature for the instances to save costs. For more information, see Enabling No Charge when Shut Down for a pay-as-you-go instance.
> - For monthly subscribed instances purchased at a special offer price, if you switch them to pay-as-you-go and then back to monthly subscription, the special offer will not be available.

Switching rules

The CVM console allows you to switch the billing mode based on the following rules:

- You can switch the billing mode of one or multiple CVM instances at a time.
- Monthly bandwidth can be switched to traffic-based billing. However, bandwidth packages and EIPs of Standard Account Type cannot be switched.
- The billing mode of the elastic cloud disks and mounted local disks is changed to pay-as-you-go along with the monthly subscribed instance.
- Expired cloud disks cannot be switched; you need to renew or detach them first. Instances with non-elastic data cloud disks cannot be switched from monthly subscription to pay-as-you-go.
- The new billing period of a changed CVM instance starts the moment when the billing mode is changed.

Usage Limits

- If the remaining quota of pay-as-you-go instances for the zone is less than the number of monthly-subscribed instances to be changed, the billing mode cannot be changed. In this case, you must increase instance purchase quota before changing the billing mode.
- You can change only monthly-subscribed instances.
- A monthly-subscribed instance with an unpaid renewal order cannot be changed.

Instructions

1. Log in to the CVM console.
2. On the instance management page, select one or more instances as needed.

Converting a single instance

On the instance management page, proceed according to the actually used view mode:

- **List view**: In the Actions column of the target instance, choose **More** > **Instance settings** > **Changing from monthly subscription to pay-as-you-go**,

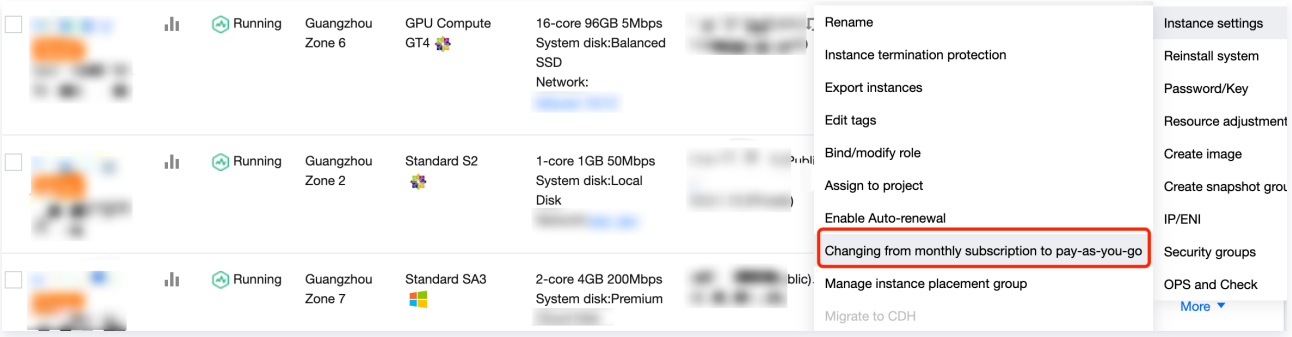
> **Note**

> You can also select the instances, click **More actions** at the top and select **Changing from monthly subscription to pay-as-you-go**.

- **Tab view**: On the details page of the instance, click **More actions** and choose **Instance settings** > **Changing from monthly subscription to pay-as-you-go.**

Switching multiple instances

Select the instances you want to switch, and click **More Actions** > **Switch to Pay-as-you-go** at the top to change the billing mode for multiple instances, as shown below:
Reasons will be displayed for instances that cannot be switched.



3. In the 'Changing from monthly subscription to pay-as-you-go' pop-up window, confirm the refund amount and freezing amount.
4. Check the box "**I have read and agree to the rules for switching from monthly subscription to pay-as-you-go**", and click **Confirm**. In the "Switch from Monthly Subscription to Pay-as-you-go" window, you can see that the instance has been successfully switched.

FAQs Overview

For any questions about the change, see FAQs about Billing.

Searching for Instance

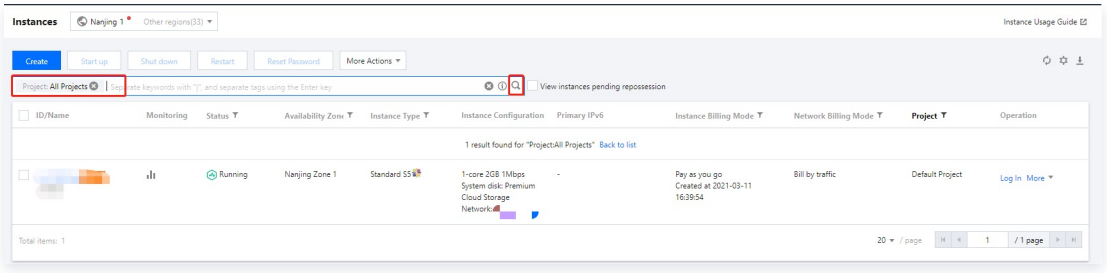
Last updated: 2024-05-15 09:53:23

Scenario

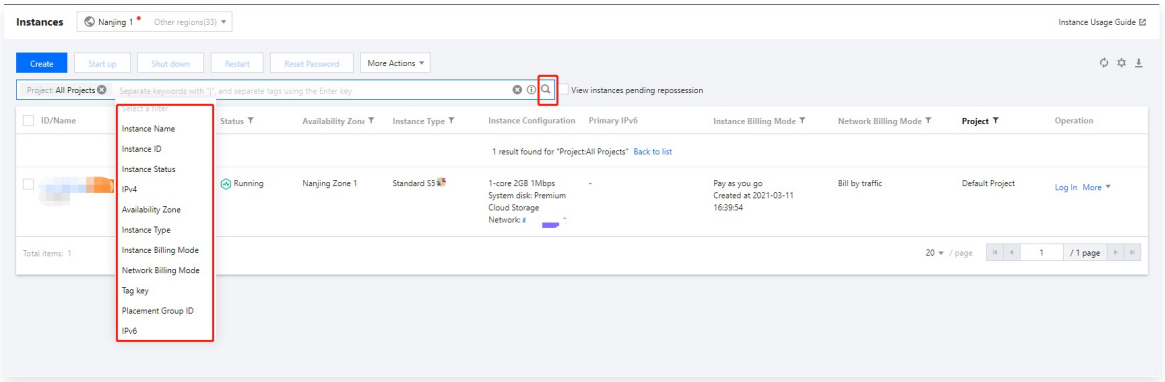
By default, the CVM console displays all CVM instances in the current region and across all projects. To help users quickly search for CVM instances in the current region, Tencent Cloud provides a search feature that allows filtering by attributes such as project, billing mode, instance type, availability zone, IP, instance ID, and instance name.

Instructions

1. Log in to the CVM console.
2. In the search box, enter the content you want to search based on your requirements, and click to perform the search.
   - Enter the keyword in the search text box, and click , as shown below:

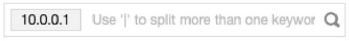
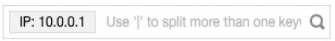
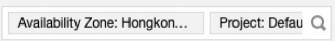
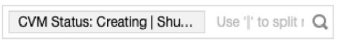
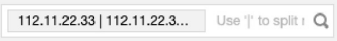


   - Select the resource dimensions you want to search (e.g., project, billing mode, instance type, etc.), and click . As shown in the image below:



3. To learn more about search syntax, click to view the syntax for related search examples.

   More search example syntax is shown in the image below:

	Enter Format	Example	Display in Search Box	Description
Single keyword	[Keyword]	10.0.0.1		List all instances including the keyword “10.0.0.1”
Multiple keywords	[Keyword] [Enter key ↵] [Keyword]	10.0.0.1 www.123.com 192.169.23.54		List all instances that include all the three keywords“10.0.0.1”,“www.123.com”and“192.169.23.54”
Single resource type	[Resource type]: [Keyword]	IP: 10.0.0.1		List all instances whose IP is “10.0.0.1”
Multiple resource types	[Resource type]: [Keyword][Enter key ↵][Resource type]: [Keyword]	Availability Zone: Hong Kong Zone 2 Project: Default		List all instances whose“Availability Zone”is“Hong Kong Zone 2” and “Project “ is “Default”
Single resource type and multiple keywords	[Resource type]: [Keyword] | [Keyword]	CVM Status: Creating | Shutdown		List all instances whose “CVM Status “ is “Creating” or “Shutdown”
Pasted contents	{pasted contents}	112.11.22.33 112.11.22.34 112.11.22.53		List all instances include the keywords “112.11.22.33”, “112.11.22.34” or “112.11.22.53”

Exporting Instance List

Last updated: 2024-09-24 16:42:36

Scenario

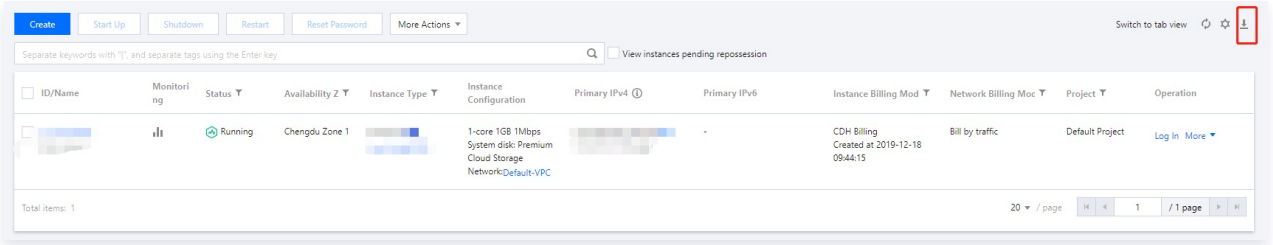
You can export a list of CVM instances for a specific region in the console and customize the fields in the exported list. You can select up to 27 fields for customization, including: ID, instance name, status, region, availability zone, instance type, operating system, image ID, CPU, memory, bandwidth, public IP, private IP, system disk type, system disk size, data disk type, data disk size, associated network, subnet, related VPC, creation time, expiration time, instance billing mode, network billing mode, project, dedicated host ID, and tags.

Instructions

1. Log in to the CVM console.
2. On the instance management page, select a region and proceed according to the actually used view mode:

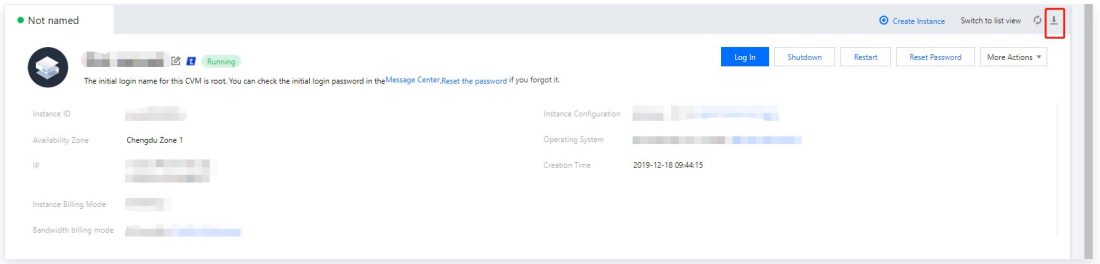
List view

Click ⬇ in the upper right corner of the instance list, as shown below:

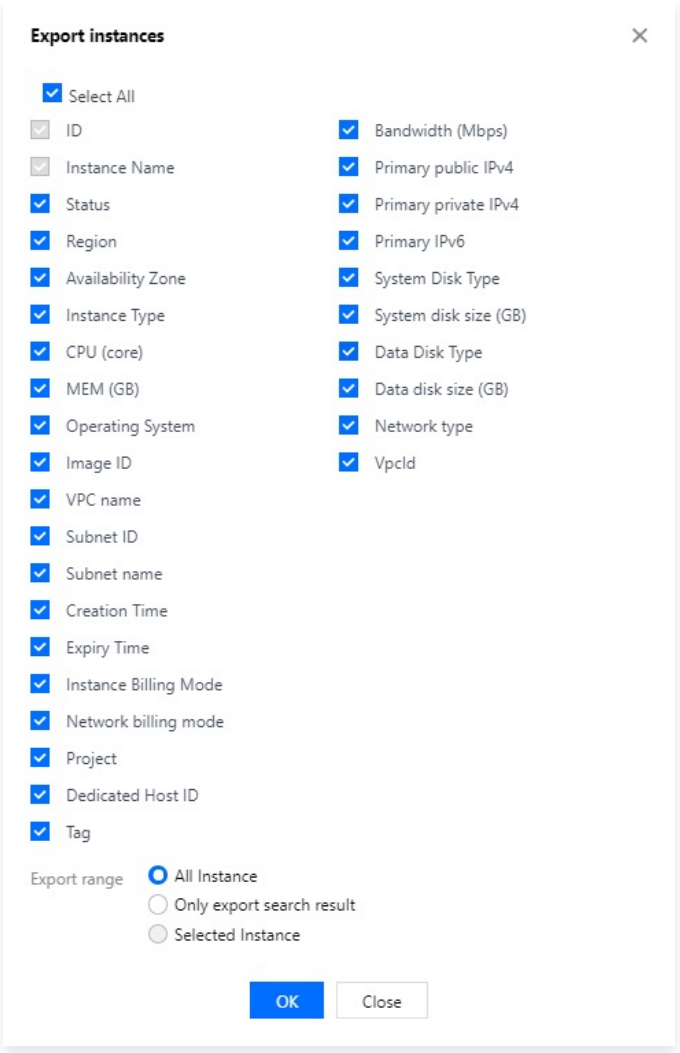


Tab view

Click ⬇ in the upper right corner of the instance page, as shown below:



3. In the **Export instances** pop-up window, select the fields you want to export and click **OK** to proceed. As shown in the image below:



Renewing Instance

Last updated: 2023-09-26 17:51:25

Scenario

The billing modes for cloud servers can be divided into two types: **monthly subscription** and **pay-as-you-go**. **Bidding instances** are also a type of pay-as-you-go billing. For more information, see Billing Modes.

- If you need to renew a **monthly subscription instance**, you can perform **manual renewal** or set up **auto-renewal** directly in the **Cloud Server >** Instances or **Billing Center >** Renewal Management console. You can also set a **unified expiration time**, **modify the auto-renewal cycle**, and **batch renewal** in the **Billing Center >** Renewal Management console. For more information, see Renewal Management.
- If you need to renew a **pay-as-you-go instance**, simply maintain a sufficient account balance for automatic renewal (fees will be deducted directly from the account balance). Please refer to Online Recharge and Bank Transfer. Additionally, you can also refer to Balance Alerts to set up warnings to prevent instances from being terminated.

This document will introduce how to perform manual renewal and set up auto-renewal for **monthly subscription instances**.

Manual Renewal Steps

> **Note**
> The following steps demonstrate how to renew a monthly subscription instance using the Cloud Server console as an example.

Renewing through the console

Renewing a repossessed instance

1. Log in to the Cloud Server console and select **Recycle Bin** > Instance Recycle Bin on the left sidebar.
2. On the Cloud Server Recycle Bin management page, choose different operation steps according to your actual needs.
   - **Renewing a Single Instance:**
     2.1.1 Select the instance row that needs to be renewed, and click **Recover** in that instance row.
     2.1.2 In the "Restore Instance" pop-up window, select the renewal period, click **OK**, and complete the renewal payment.
   - **Batch Renewal of Instances:**
     2.1.1 Select all instances that need to be renewed and click **Batch Renewal** at the top.
     2.1.2 In the "Restore Instance" pop-up window, select the renewal period, click **OK**, and complete the renewal payment.

Renewing Running Instances

Renewing one instance

1. Log in to the CVM console.
2. On the instance management page, proceed according to the actually used view mode:
   - **List View:** Select the instance row you want to renew and click **Renew** within that row.

- **Tab View**: In the instance page that needs renewal, select **Renew** in the top right corner, as shown in the image below:

3. In the "Instance Renewal" pop-up window, select the renewal period, click **OK**, and complete the renewal payment.

Batch renewing instances

1. Select all instances that need renewal and click **Renew** at the top.
2. In the "Instance Renewal" pop-up window, select the renewal period, click **OK**, and complete the renewal payment.

Renewal via API

You can use the RenewInstances API to renew instances. For more information, please refer to Renew Instances.

Steps to set up auto-renewal

Note

- The following steps demonstrate how to set up auto-renewal for monthly subscription instances in the Renewal Management page of the console, avoiding the need to manually renew each time the instance is about to expire.
- If your account balance is sufficient and you have enabled auto-renewal, the instance will automatically deduct the fees for the next billing cycle on the expiration date and automatically enter the next cycle.

Setting via the console

Setting through the Cloud Server Console

1. Log in to the CVM console.
2. On the instance management page, choose different operation steps according to your actual needs.
   - **Set auto-renewal for a single instance:**
     2.1.1 Select the monthly subscription instance row for which you want to set up auto-renewal, and click **More** > **Instance Settings** > **Set Auto-Renewal** in that instance row.
     2.1.2 In the "Set Auto-renewal" pop-up prompt, click **OK**.
   - **Set auto-renewal for multiple instances:**
     2.1.1 Select all monthly subscription instances for which you want to set up auto-renewal, and click **More Actions** > **Instance Settings** > **Set Auto-Renewal** at the top of the page.
     2.1.2 In the "Set Auto-renewal" pop-up prompt, click **OK**.

Setting through the Billing Center Console

1. Log in to the Tencent Cloud console.
2. Move the cursor to the top-right corner and hover over **Expense**, then click Renew in the drop-down menu.
3. On the Renewal Management page, choose different operation steps according to your actual needs.
   - **Set auto-renewal for a single instance:**
     3.1.1 Select the monthly subscription instance row for which you want to set up auto-renewal, and click **Set to Auto-Renewal** in that instance row.
     3.1.2 In the "Set as Auto-renewal Item" pop-up prompt, click **Confirm**.

- **Setting auto-renewal for multiple instances:**
  3.1.1 Select all monthly subscription instances that require auto-renewal, and click **Set to Auto-Renewal** at the top
  3.1.2 In the "Set as Auto-renewal Item" pop-up prompt, click **Confirm**.

Set up via API

Users can use the ModifyInstancesRenewFlag API to set up auto-renewal for instances. For more information, please refer to Modify Instance Renewal Flag.

Starting Up Instances

Last updated: 2024-05-15 10:25:42

Scenario

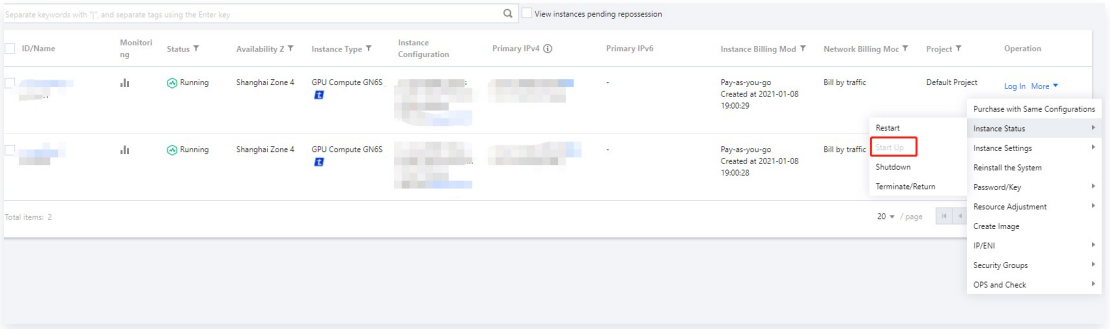
This document describes how to start up an instance via the console or an API.

Instructions

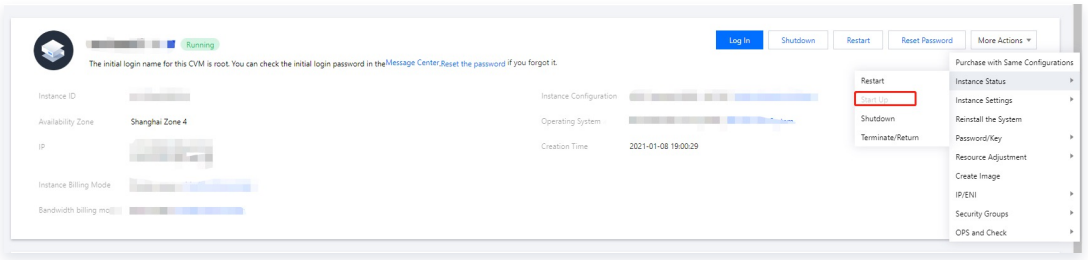
Power on Instance via Console

Starting up one instance

1. Log in to the CVM console.
2. On the instance management page, proceed according to the actually used view mode:
   - **List View**: Select the instance you want to start, and choose **More** > **Instance Status** > **Start up**, as shown below:

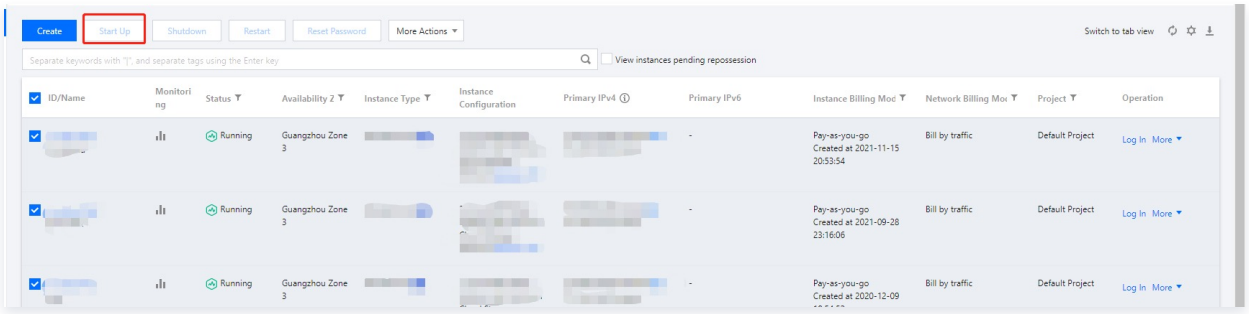


   - **Tab View**: On the desired instance page, click **Start up** in the upper right corner, as shown below:



Starting up multiple instances

Select the instances you want to start up, and click **Start up** at the top of the list to start the selected instances, as shown below:



Power on Instance via API
Please refer to the StartInstances API.

See Also

Once the instance starts up, you can perform the following operations:

- **Log in to the instance**: Depending on the instance's operating system, Log in to a Linux instance or Log in to a Windows instance.
- Initializing cloud disks: Perform initialization operations on the mounted cloud disks, such as formatting, partitioning, and creating a file system.

Shutting Down Instances

Last updated: 2024-03-26 14:33:01

Scenario

Users may need to shut down an instance to stop its services or to modify configurations that can only be changed when the instance is powered off. Shutting down an instance is similar to shutting down a local computer.

Supports and Limits

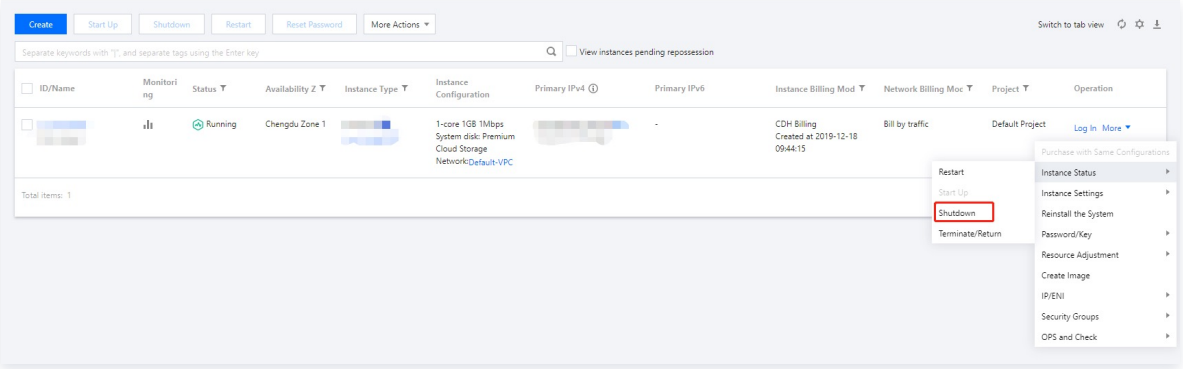
- You can use system commands to shut down the instance (such as the "shutdown" command in Windows and Linux systems) or use the Tencent Cloud console to do so. It is recommended to monitor the shutdown process through the console to identify any potential issues.
- Once the instance is shut down, it will no longer provide services. Therefore, before shutting down, please ensure that the CVM has suspended all business requests.
- When an instance is shut down normally, its status changes to "Shutting Down" first, and then to "Shut Down" upon completion. If the shutdown process takes too long, there might be issues. For more information, see Shutdown-related. Avoid forcing a shutdown.
- After the instance is shut down, all storage remains connected to the instance, and all disk data is preserved. However, data in memory will be lost.
- Shutting down an instance does not change its physical properties. The public and private IPs of the instance remain unchanged; Elastic Public IPs maintain their binding relationships, but due to service interruption, accessing these IPs will result in error responses; Basic Network Intercommunication relationships remain unchanged.
- If the shut down instance belongs to a backend server cluster of a CLB instance, it will not be able to provide services after shutting down. If a health check policy is configured, the shut down instance will be automatically blocked and no longer receive forwarded requests. If no health check policy is configured, clients may receive a 502 error response. For more information, please refer to Health Check.
- If the shut down instance is part of an Elastic Scaling Group, the Auto Scaling service may mark the instance as unhealthy, potentially removing it from the group and launching a replacement instance. For more information, please refer to Elastic Scaling.

Instructions

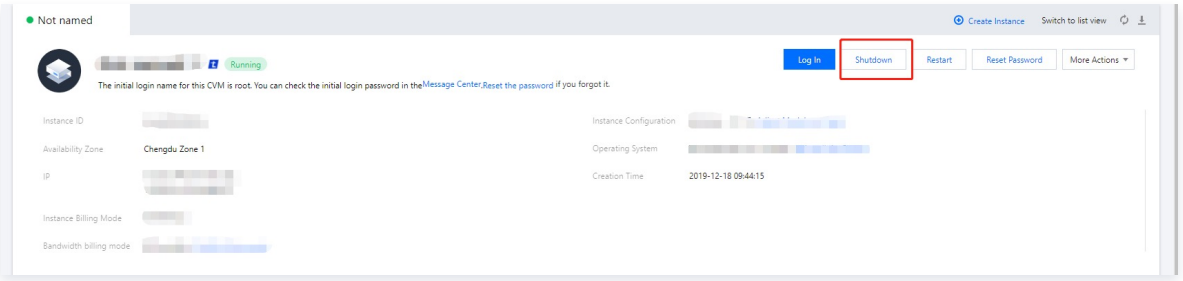
Shutting Down Instances in the Console

Shutting down a single instance

1. Log in to the CVM console.
2. On the instance management page, proceed according to the actually used view mode:
   - **List View**: Select the instance you want to shut down, and in the operation column on the right, choose **More** > **Instance Status** > **Shutdown**. As shown below:

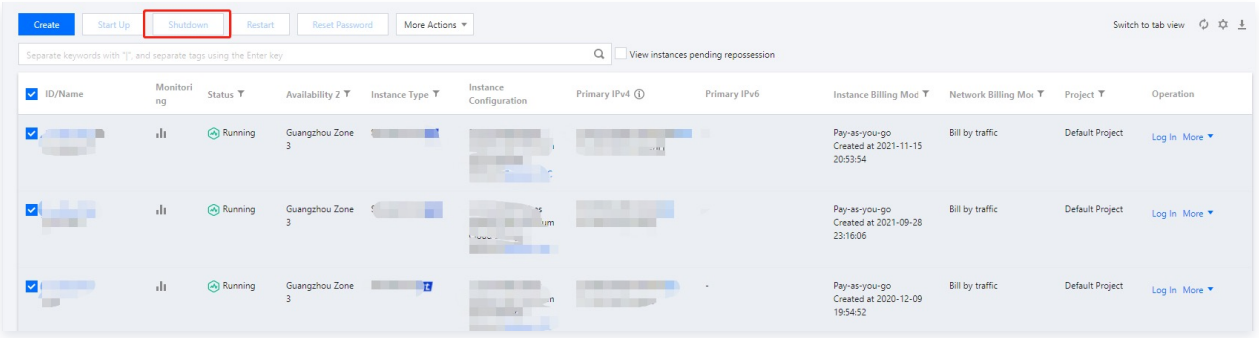


- **Tab View:** On the instance page that needs to be shut down, select **More Actions** > **Instance Status** > **Shutdown** in the top-right corner, as shown below:



Shutting down multiple instances

1. Log in to the CVM console.
2. Select all the instances you want to shut down and click **Shutdown** at the top of the list to shut down instances in batches as shown below:



> **Note**
> Reasons are given for instances that cannot be shut down.

Shutting Down Instances via API

Please refer to the StopInstances API.

See Also

You can modify the following attributes only if the instance has been shut down.

- **Instance Configuration (CPU, Memory):** To change the instance type, please refer to Adjusting Instance Configuration.
- **Change Password:** Please refer to Login Password.
- **Load SSH Key:** Please refer to SSH Key.

Restarting Instance

Last updated: 2024-05-15 10:15:21

Scenario

Restarting is a common method for maintaining cloud servers, and restarting an instance is equivalent to rebooting the operating system on a local computer. This document guides you on how to restart an instance.

Supports and Limits

- **Restart Preparation:** During the restart, the instance will not be able to provide services normally. Therefore, before restarting, ensure that the CVM has suspended business requests.
- **Restart Method:** We recommend using the restart operation provided by Tencent Cloud to restart the instance, rather than running restart commands within the instance (such as the Restart command in Windows and the Reboot command in Linux).
- **Restart Duration:** Generally, it only takes a few minutes to complete the restart operation.
- **Instance Physical Features:** Restarting an instance does not change its physical characteristics. The public IP, private IP, and any stored data of the instance will remain unchanged.
- **Billing:** Restarting an instance will not start a new instance billing period.

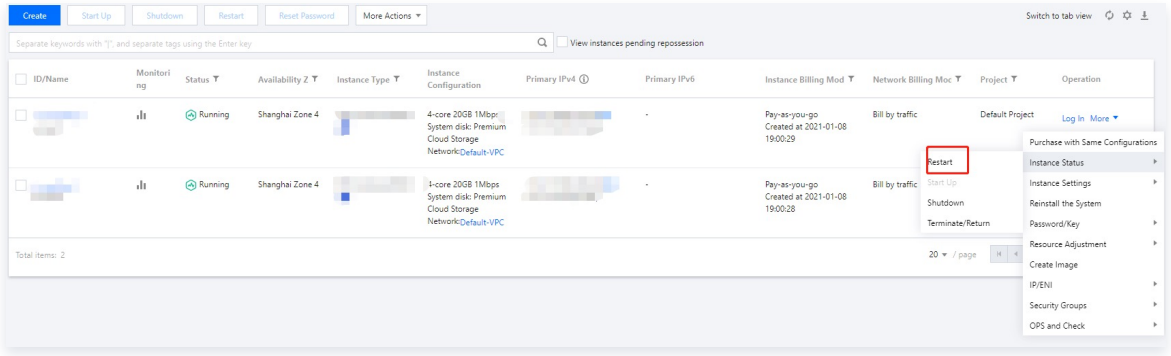
Instructions

You can restart instances via the following methods:

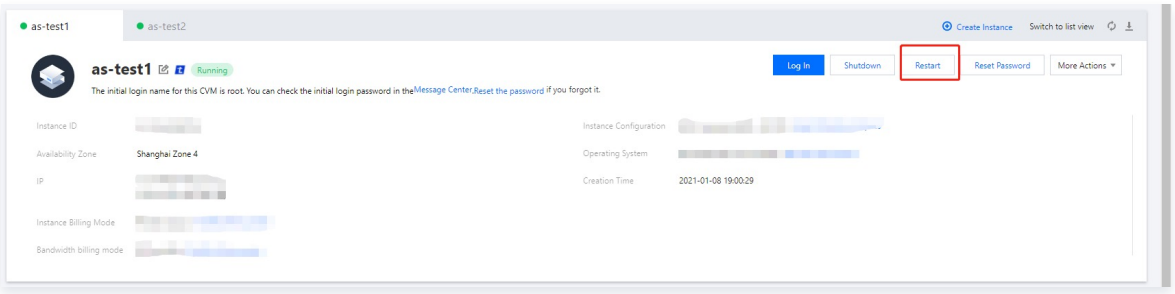
Restarting an Instance Using the Console

Restarting a single instance

1. Log in to the CVM console.
2. On the instance management page, proceed according to the actually used view mode:
   - **List View:** In the row of the instance that needs to be restarted, select **More** > **Instance Status** > **Restart**. As shown in the image below:

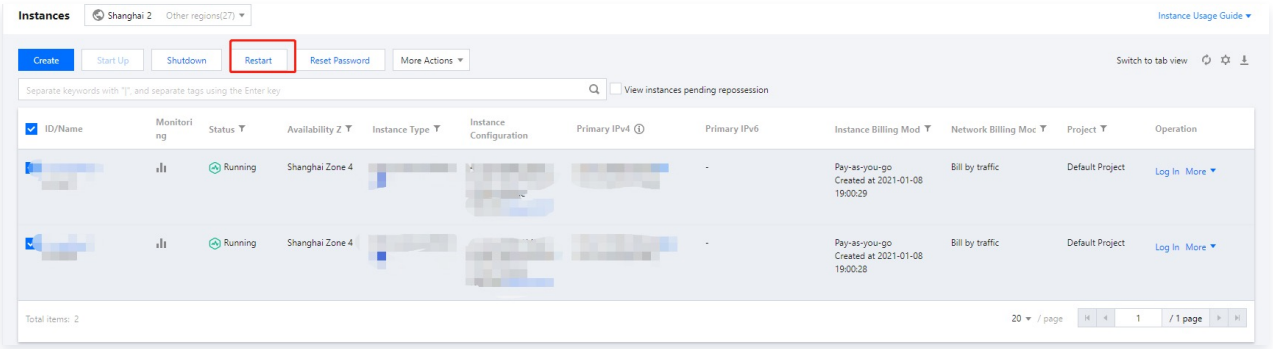


   - **Tab View:** In the instance page that needs to be restarted, select **Restart** in the upper right corner, as shown in the image below:



Restarting multiple instances

1. Log in to the CVM console.
2. Select the instances you want to restart, and click **Restart** at the top of the list to restart instances in batches. If an instance cannot be restarted, the reason will be displayed, as shown below:



> **Note**
> A single instance can also be restarted in this method.

Restarting an Instance Using API

Please refer to the RebootInstances API.

Reinstalling System

Last updated: 2024-06-02 10:48:01

Scenario

Reinstalling the system enables the instance to return to its initial state upon launch, serving as a crucial recovery measure in the event of a system failure. The following video and document provide guidance on how to reinstall the operating system.

Watch video

CVM supports the following two reinstallation types:

- **Reinstall on the same platform**: CVMs in all regions can be reinstalled to the OS of the same platform.
  For example, you can always reinstall a Linux instance on a Linux OS, and Windows instance on a Windows OS.
- **Reinstall on a different platform**: Only supported in Mainland China regions (excluding Hong Kong, China).
  For example, you can reinstall a Linux instance on a Windows OS, and a Windows instance on a Linux OS.

> **Note**
> - Currently, all newly added cloud disk instances and local disk instances support cross-platform reinstallation. However, some existing 20GB local disk instances temporarily do not support cross-platform reinstallation via the console. Users with these local disk instances need to apply through online support.
> - Spot instances do not support system reinstallation.

Supports and Limits

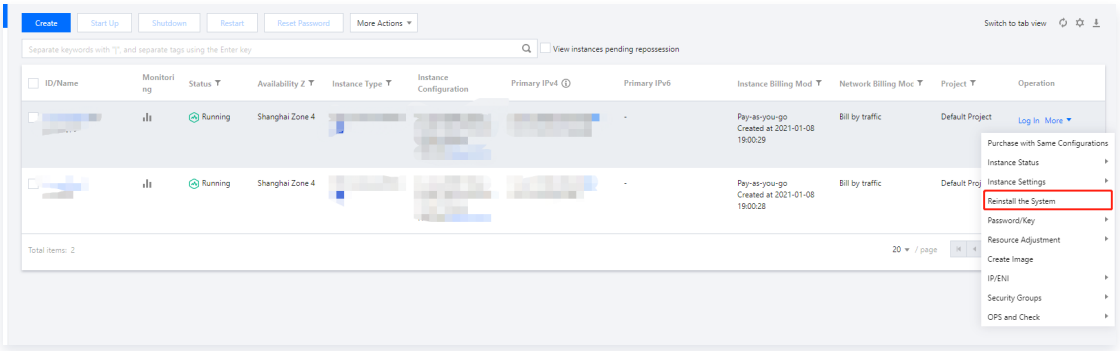
- **Preparation for reinstallation:** Reinstalling the system will directly erase the data in the system disk. You need to back up important data in the system disk before reinstalling. If you need to retain system operation data, it is recommended to create a custom image before reinstalling the system and choose that image for reinstallation.
- **Image selection:** We recommend using the images provided by Tencent Cloud or custom images for reinstallation, rather than those from unknown or other sources. Please refrain from performing other operations while the system disk is being reinstalled.
- **Instance physical features:** The public IP of the instance will not change.
- **Instance Specification Limitations**: If you need to reinstall your instance with a Windows 2016 or 2019 image, the instance memory must be greater than 2 GB.
- **Billing-related:** When adjusting the system disk size (only supported for cloud disks), charges will be applied according to the cloud disk pricing standards. For more details, please refer to Disk Pricing.
- **Follow-up actions:** After reinstalling the system disk, the data in the data disks remains unaffected but needs to be remounted before it can be used.

Instructions

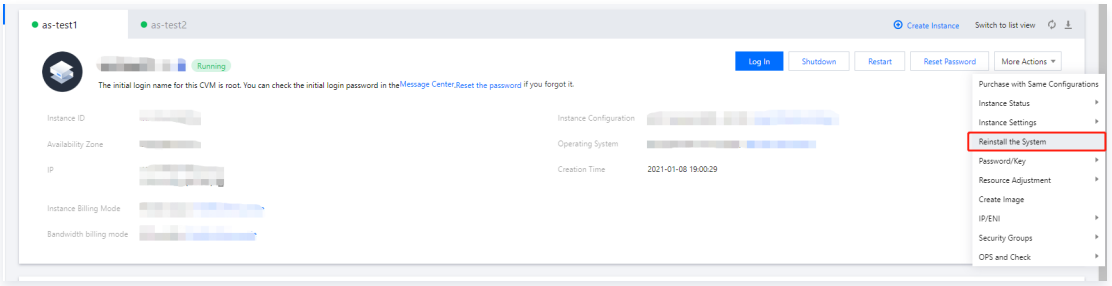
You can reinstall the operating system in two ways:

Reinstalling the system using the console

1. Log in to the CVM console.
2. On the instance management page, proceed according to the actually used view mode:
   - **List view**: In the row of the instance requiring system reinstallation, select **More** > **Reinstall the System**. As shown in the image below:

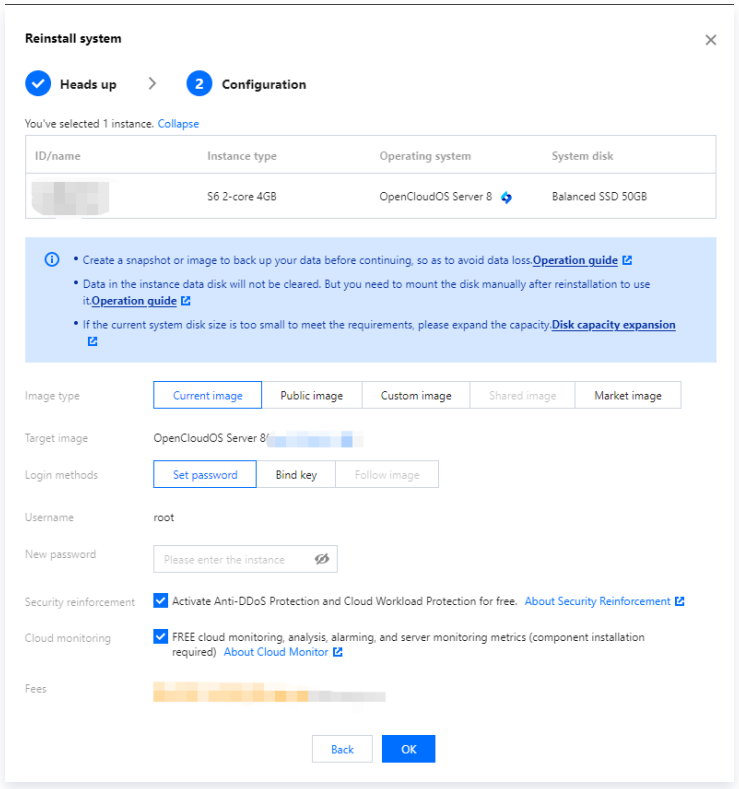


- **Tab view:** On the instance page where the system needs to be reinstalled, select **More actions** > **Reinstall the system** in the upper right corner. As shown in the image below:



3. In the "Reinstall System" pop-up window, read the "Reminders" and click **Next** after understanding the instructions.
4. Choose to use the current instance image or another image, set the instance's login method, and click **OK**, as shown in the figure below:

> **Note**
> Only when the image type is **custom image** or **shared image** can you select **Follow image** as the login method.



Reinstalling the system using APIs

For more information, see the ResetInstance API.

See Also

If the CVM has attached a data disk and you need to reinstall it on a different platform, please see the following documents about how to read data from the data disks of the original operating system:

- Read/Write EXT Data Disks after Reinstalling a Linux CVM to Windows CVM
- Read/Write NTFS Data Disks after Reinstalling a Windows CVM to Linux CVM

Using Tencent Cloud Automation Tools to execute commands

Last updated: 2023-09-07 17:10:26

Scenario

Tencent Cloud Automation Tools (TAT) is a native operation and deployment tool for Cloud Virtual Machines and Light Application Servers. Without remotely connecting to instances, TAT can automatically execute Shell commands in batches to complete tasks such as running automated operation and maintenance scripts, polling processes, installing/uninstalling software, updating applications, and installing patches. For more information about Tencent Cloud Automation Tools, please refer to Tencent Cloud Automation Tools.
This document describes how to use TAT to execute commands for instance management.

Preparations

The CVM instance must have the TAT agent installed. For more information, see Installing TAT Agent.

> **Note**
> Some existing CVM instances may not support TAT temporarily. Full support for all instances is expected in the future. Please follow the New Feature Release Notes for the latest updates.

Instructions

Refer to the following documents to create, execute, and view command execution status:

- Create Command
- Execute Command or Execute Command without Login
- View Command Execution Status

Terminating/Returning Instances Overview

Last updated: 2025-08-05 19:16:00

This document provides an overview and instructions on terminating and releasing instances. For more information on expiration, please refer to Expiration Reminder.

Overview

When you no longer need an instance, you can terminate it, and the terminated instance will be placed in the recycle bin. For instances in the recycle bin, you can renew, restore, or release them based on different scenarios and requirements.

> **Note**
> If your account is overdue, you need to make up the overdue payment to resume the PAYG instances.

Methods for Termination/Release

For both monthly subscription and pay-as-you-go instance types, the methods for instance termination and release are as follows:

- **Manual termination method:** For unexpired monthly subscribed instances or pay-as-you-go instances without overdue payments, you can choose to manually terminate them. Monthly subscribed instances will be completely released after being kept in the recycle bin for up to 15 days. Pay-as-you-go instances will be completely released after being kept in the recycle bin for up to 2 hours.
- **Scheduled Termination:** Set a scheduled termination for pay-as-you-go instances. You can choose a future time to terminate the resources, with the termination time accurate to the second. Instances set for scheduled termination will be released immediately without entering the recycle bin. You can cancel the scheduled termination at any time before it occurs.
- **Automatic termination for expired/overdue instances:** For subscription instances, they will be retained in the recycle bin for up to 15 natural days after expiration and will be automatically released if not restored. Pay-as-you-go instances will be automatically released after 2 hours of negative balance + 15 days (fees will continue to be deducted for the first 2 hours, and the instance will be shut down and stop charging for the next 15 days. Overdue pay-as-you-go instances do not enter the recycle bin, and you can view them in the instance list). You can continue using the instances by completing the renewal within the specified time.

Instance Type	Manually terminate (not overdue)	Scheduled Termination (No Overdue Payment)	Auto-termination upon expiration/overdue payment
Monthly Subscription Instance Type	After termination, instances will be retained in the recycle bin for up to 15 days. If not restored within this period, the instance will be released.	-	Instances terminated after expiration will be placed in the recycle bin and retained for up to 15 days. If not restored within this period, the instance will be released.
Pay-as-you-go Instances	After termination, the instance will be retained in the recycle bin for up to	Instances for which timed termination is set will be	After an instance becomes overdue, it will continue to be billed and function normally for the first 2 hours. For the following 15 days, the instance will be shut down and billing will stop.

	two hours. If not restored within this period, the instance will be released.	released immediately as scheduled, instead of going into the recycle bin.	Overdue pay-as-you-go instances will not be placed in the recycle bin. If the payment is not made during this period, the instance will be released.

Related Impacts

When an instance is terminated, the relevant impact on instance data, EIPs, and billing is as follows:

- **Billing:** Once the instance status changes to "Terminating" or "Released," it will no longer incur fees associated with that instance.
- **Instance Data:** Mounted local disks and non-elastic cloud disks will be released together, and the data cannot be retrieved. Please back up in advance. Elastic cloud disks will follow their own lifecycle.
- **Elastic IP:** The Elastic IP (including the IP on the secondary network interface) of the terminated instance will be retained, and idle IPs will incur fees. If you don't need to keep them, please release them promptly.

Instructions

You can manually terminate/release instances through the following ways:

- To terminate or return an instance using the console, please refer to Terminating or Returning an Instance in the Console.
- To terminate or return an instance using an API, please refer to the TerminateInstances API.

Terminating/Returning Instance in Console

Last updated: 2025-08-05 19:16:33

Scenario

This document describes how to terminate or return instances with monthly/yearly subscription or pay-as-you-go billing modes through the console.

> **Note**
> Please refer to Related Impacts for the consequences of terminating or returning cloud server instances.

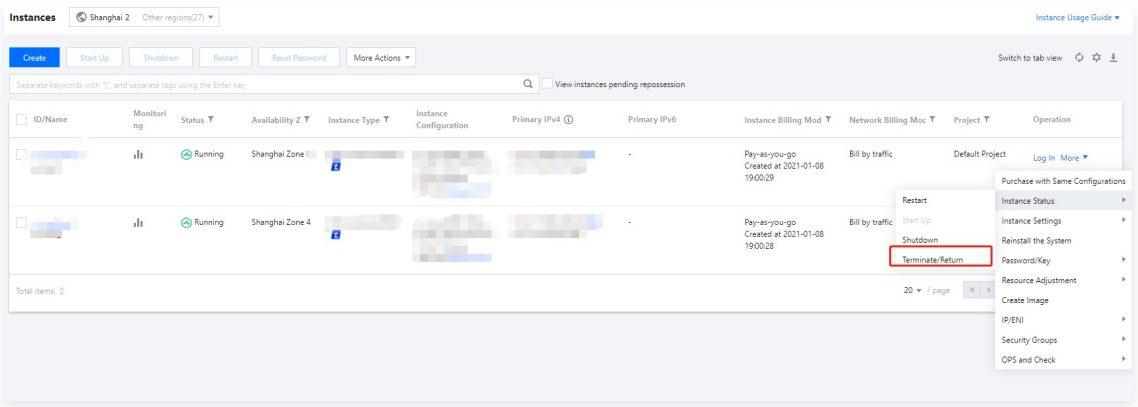
Instructions

Terminate and release monthly subscribed instances

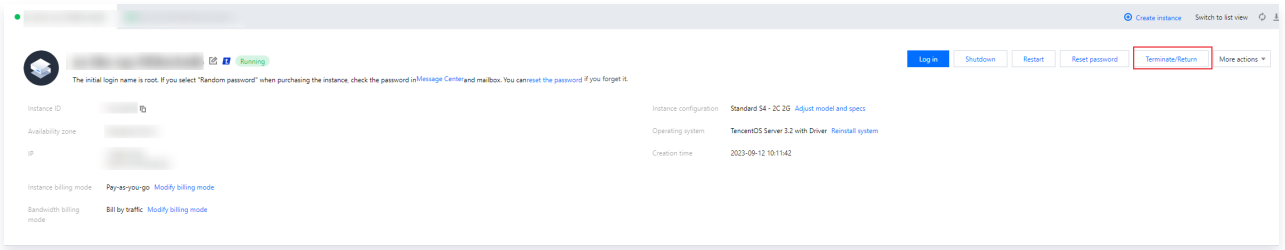
Terminating unexpired instances using the console

When you no longer need a monthly/yearly subscription instance, you can terminate it. Once the instance's status changes to "Terminating" or "Terminated," it will no longer incur fees related to that instance. The instance will be moved to the cloud server recycle bin and retained for 15 days, during which the services running on the instance will be completely interrupted.

1. Log in to the CVM console.
2. On the instance management page, proceed according to the actually used view mode:
   - **List View**: Select **More** > **Instance Status** > **Terminate/Return** on the right side of the row where the instance to be terminated is located, as shown in the image below:



   If you need to terminate multiple instances simultaneously, select the instances and choose **More Actions** > **Terminate/Return** at the top of the list.
   - **Tab View**: On the page of the instance you want to terminate, click **Terminate/Return** in the top-right corner, as shown below:



3. In the pop-up window, confirm the instructions for terminating the cloud server, select "I have read and agreed to Refund Rules," and click **Next**.

> ⚠ **Note**
> Upon returning a monthly subscribed instance, the local disks and non-elastic cloud disks attached to the instance will also be returned, and the data stored on these disks will be lost. For elastic cloud disks mounted on the instance:
> - For monthly subscription cloud disks, whether they are released during termination depends on whether you choose to destroy them along with the instance.
> - For pay-as-you-go cloud disks, whether to release them depends on the cloud disk attribute. You can modify the attribute in the Cloud Disk Console on the right side under **More**.

4. Review the resources to be terminated and retained, then select **Next** and click **Confirm**.
5. On the "Review Refund Information" page, carefully review the refund information for the relevant instances, and click **Confirm Refund** to initiate the refund and terminate the instance. After termination, the resources and data of the cloud server will be retained in the recycle bin for 7 days.
   For specific rules on actively returning monthly/yearly subscription instances, refer to Refund Rules for Returning Monthly/Yearly Subscription Instances.

Releasing a monthly subscribed instance from the recycle bin

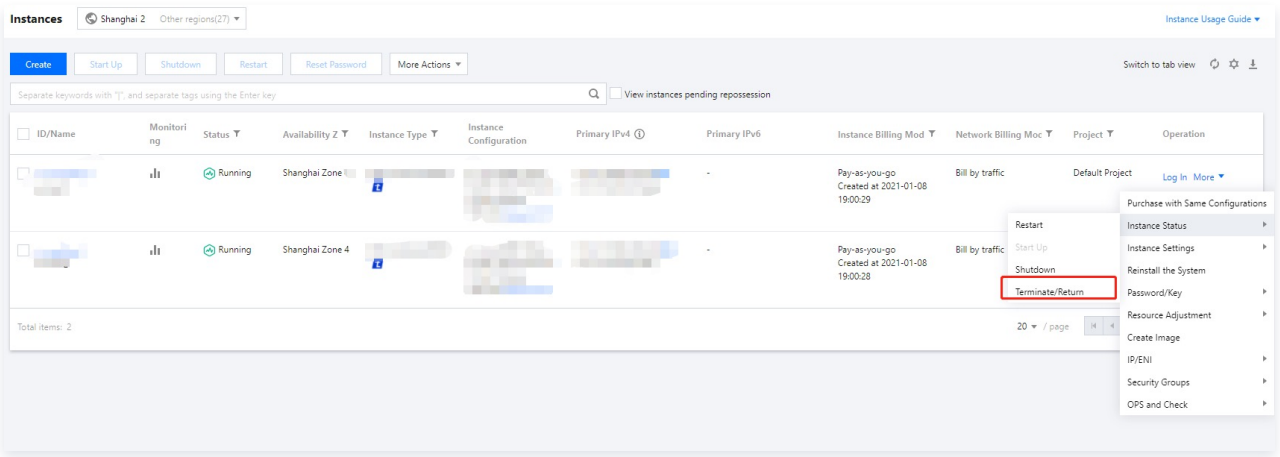
You can release monthly/yearly subscription instances located in the Recycle Bin through the console.

1. Log in to the CVM console, click on the left sidebar **Recycle Bin** > **Instance Recycle Bin** to access the cloud server recycle list.
2. Select **Release** on the right side of the row where the instance to be terminated is located.
   If you need to terminate multiple instances simultaneously, select the instances and choose **Batch Release** at the top of the list.
3. In the pop-up window, confirm the instructions related to releasing the cloud server, check the box for "I have read and agree to the refund rules", and click on **Next**.
4. Review the resources to be terminated and retained, then click **OK** to complete the release.

Terminating and releasing pay-as-you-go instances

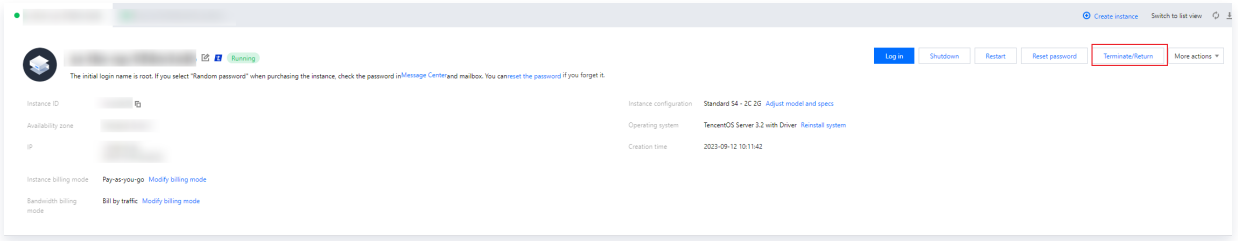
For pay-as-you-go instances, you can choose immediate termination or timed termination.

1. Log in to the CVM console.
2. On the instance management page, proceed according to the actually used view mode:
   - **List View**: Select **More** > **Instance Status** > **Terminate/Return** on the right side of the row where the instance to be terminated is located, as shown in the image below:



If you need to terminate multiple instances simultaneously, select the instances and choose **More Actions** > **Terminate/Return** at the top of the list.

- **Tab View**: On the page of the instance you want to terminate, click **Terminate/Return** in the top-right corner, as shown below:

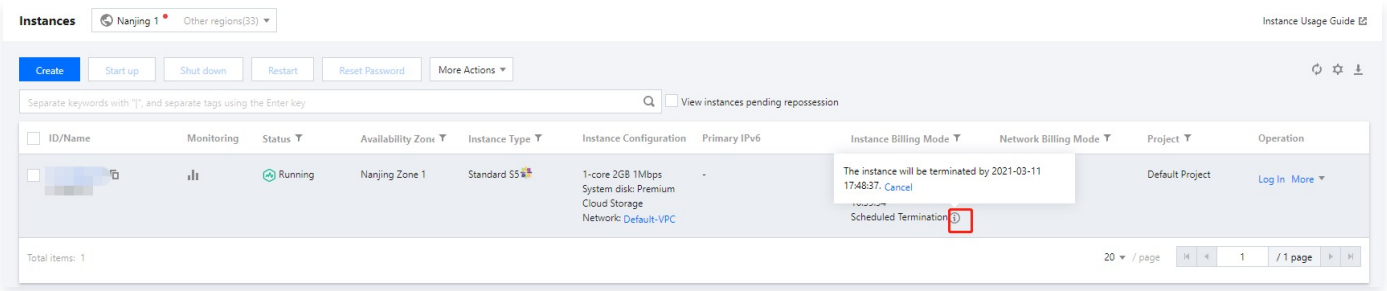


3. In the pop-up "Terminate/Return" window, you can choose between **Immediate Termination** or **Scheduled Termination** for the instance.
   - **Immediate Termination**: If you choose to terminate immediately, you can decide whether to release resources right away or after 2 hours. If you opt for immediate release, the associated data of the instance will be erased and cannot be recovered.
   - **Scheduled Termination**: If you choose scheduled termination, you need to set a specific time for the instance to be terminated. Upon reaching the scheduled time, the instance will be terminated and released, and the data cannot be recovered.
4. After selecting the termination method, click **Next** to confirm the actual instances and related resources to be terminated and retained.
5. After confirming the resources to be terminated, click **Start Termination**.

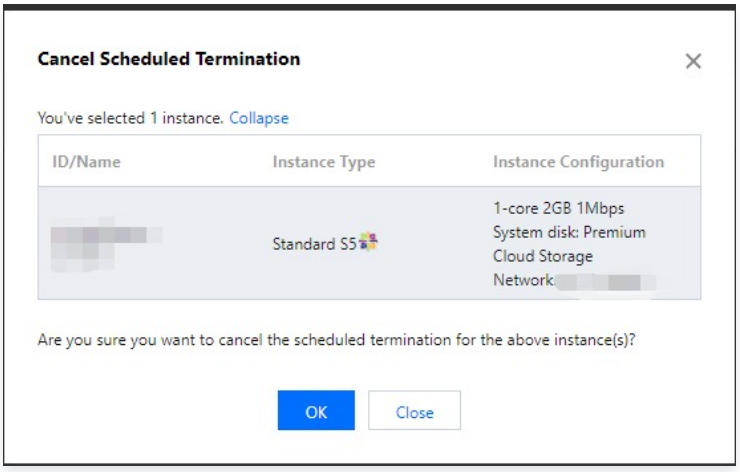
Related Actions

Canceling timed termination

1. Log in to the CVM console.
2. In the instance list, locate the instance for which you want to cancel the scheduled termination. Find "**Scheduled Termination**" in the "**Instance Billing Mode**" column, and hover over ⓘ to display the scheduled termination tooltip, as shown below:



3. Click **Cancel** to display the confirmation dialog box for canceling the scheduled termination.
4. In the pop-up prompt, confirm the instance information for canceling the scheduled termination, and click **OK**. The cancellation takes effect immediately, as shown in the following image:



Using APIs to terminate/return prepaid instances and mounted cloud disks

Last updated: 2024-05-15 10:25:42

Scenario

This document describes how to terminate a prepaid CVM instance and the prepaid cloud disks mounted to it by using the Tencent Cloud Developer Kit (SDK) 3.0 and cloud APIs. This document also provides sample code in Python for your reference.

> **Note**
> For more information about the impact of terminating/returning a CVM instance, see Impacts.

Preparations

- You have purchased a prepaid CVM instance and mounted a cloud disk to the instance.
- You have obtained the SecretId and SecretKey on the Manage API Key page.

Instructions

Install the dependencies and SDK

Perform the following steps to install the dependencies and SDK based on your actual development language:

Python

1. Install Python of a version from 3.6 to 3.9. For more information, see the official website of Python.
2. Run the following command to install Python SDK: For more information, see Tencent Cloud SDK 3.0 for Python.

```
pip install --upgrade tencentcloud-sdk-python
```

Run the sample code

The following sample code is provided for your reference.

Python

The sample code of the main program:

```
-- coding: utf-8 --
import sys
from tencentcloud.common.exception.tencent_cloud_sdk_exception import
TencentCloudSDKException
from TerminateTotalInstance import TerminateTotalInstance

if __name__ == '__main__':
    try:
        region = "ap-beijing"
        ins = "ins-irmer451"
```

```
        TerminateTotalInstance(region=region).process(instance_id=instance_id)
        print("done!")
    except TencentCloudSDKException as e:
        print(e)
    except Exception as e:
        print("failed")
```

The sample code for terminating CVM instances and cloud disks

```
# -*- coding: utf-8 -*-
import logging
import time

from tencentcloud.common import credential
from tencentcloud.common.exception.tencent_cloud_sdk_exception import
TencentCloudSDKException
from tencentcloud.common.profile.client_profile import ClientProfile
from tencentcloud.common.profile.http_profile import HttpProfile
from tencentcloud.cvm.v20170312 import cvm_client, models as cvm_models
from tencentcloud.cbs.v20170312 import cbs_client, models as cbs_models


class TerminateTotalInstance(object):
    def __init__(self, region):
     Retrieve secretId and secretKey from environment variables TENCENTCLOUD_SECRET_ID and
TENCENTCLOUD_SECRET_KEY by default
  For more credential management methods, please refer to:
https://github.com/TencentCloud/tencentcloud-sdk-python#credential-management
        self.cred = credential.EnvironmentVariableCredential().get_credential()
        self.cbs_client = self.__create_cbs_client(region)
        self.cvm_client = self.__create_cvm_client(region)

    def get_cred(self):
        # If the identity is obtained based on the token, you need to check if the token is
valid here.
        # If invalid, reacquire the credential
        if not self.cred:
            self.cred = credential.EnvironmentVariableCredential().get_credential()
        return self.cred
    def process(self, instance_id):
        # Retrieve cloud disk
        cbs_ids = self.describe_disks_for_instance(instance_id)

        # Return instance
        cvm_resp, cvm_api_errors = self.terminate_instance(instance_id)
        if cvm_api_errors:
            raise Exception(cvm_api_errors)

        # Confirm the successful return of the instance
        is_succ, cvm_api_errors = self.check_terminate_instance_success(instance_id)
        if not is_succ:
            raise Exception(cvm_api_errors)

        # Unmount and batch return cloud disks
```

```
        if not cbs_ids:
            return
        cbs_resp, cbs_api_errors = self.detach_disks(cbs_ids)
        if cbs_api_errors:
            raise Exception(cbs_api_errors)

        cbs_resp, cbs_api_errors = self.terminate_disks_for_instance(cbs_ids)
        if cbs_api_errors:
            raise Exception(cbs_api_errors)

    def terminate_instance(self, instance_id):
        # Call failure history
        cvm_api_errors = []

        for i in range(0, 5):
            try:
                req = cvm_models.TerminateInstancesRequest()
                params = '{"InstanceIds":["%s"]}' % instance_id
                req.from_json_string(params)
                resp = self.cvm_client.TerminateInstances(req)
                cvm_api_errors.clear()
                return resp, cvm_api_errors

            except TencentCloudSDKException as e:
                # Retry on failure and log errors
                cvm_api_errors.append(e)
                logging.error(e)
            time.sleep(3)

        return None, cvm_api_errors

    def check_terminate_instance_success(self, instance_id):
        # Call failure history
        cvm_api_errors = []

        for _ in range(0, 30):
            try:
                req = cvm_models.DescribeInstancesStatusRequest()
                params = '{"InstanceIds":["%s"]}' % instance_id
                req.from_json_string(params)
                resp = self.cvm_client.DescribeInstancesStatus(req)
                cvm_api_errors.clear()
                if resp.TotalCount > 0:
                    if resp.InstanceStatusSet[0].InstanceState == "SHUTDOWN":
                        return True, cvm_api_errors
                    else:
                        logging.error(resp)

            except TencentCloudSDKException as e:
                # Retry on failure and log errors
                cvm_api_errors.append(e)
                logging.error(e)
            time.sleep(6)

        return False, cvm_api_errors
```

```
    def describe_disks_for_instance(self, instance_id):
        # Retrieve the data disks attached to the instance
        req = cbs_models.DescribeDisksRequest()
        params = '{"Filters": [ { "Name": "instance-id", "Values": [ "%s" ]}]}' %
instance_id
        req.from_json_string(params)
        disks = self.cbs_client.DescribeDisks(req)
        if hasattr(disks, "DiskSet"):
            cbs_ids = [disk.DiskId for disk in disks.DiskSet if disk.DiskUsage ==
"DATA_DISK"]
        else:
            cbs_ids = list()
        return cbs_ids

    def detach_disks(self, cbs_ids):
        # Unmount data disk
        cbs_api_errors = []
        for _ in range(0, 5):
            try:
                req = cbs_models.DetachDisksRequest()
                req.DiskIds = cbs_ids
                resp = self.cbs_client.DetachDisks(req)
                cbs_api_errors.clear()
                return resp, cbs_api_errors

            except TencentCloudSDKException as e:
                # Retry on failure and log errors
                cbs_api_errors.append(e)
                logging.error(e)
            time.sleep(3)

        return None, cbs_api_errors

    def terminate_disks_for_instance(self, cbs_ids):
        # Return data disk
        cbs_api_errors = []
        for _ in range(0, 10):
            try:
                req = cbs_models.TerminateDisksRequest()
                req.DiskIds = cbs_ids
                resp = self.cbs_client.TerminateDisks(req)
                cbs_api_errors.clear()
                return resp, cbs_api_errors

            except TencentCloudSDKException as e:
                # Retry on failure and log errors
                cbs_api_errors.append(e)
                logging.error(e)
            time.sleep(6)
        return None, cbs_api_errors

    def __create_cbs_client(self, region):
        http_profile = HttpProfile()
        http_profile.endpoint = "cbs.tencentcloudapi.com"
```

```
        client_profile = ClientProfile()
        client_profile.httpProfile = http_profile
        return cbs_client.CbsClient(self.get_cred(), region, client_profile)

    def __create_cvm_client(self, region):
        http_profile = HttpProfile()
        http_profile.endpoint = "cvm.tencentcloudapi.com"

        client_profile = ClientProfile()
        client_profile.httpProfile = http_profile
        return cvm_client.CvmClient(self.get_cred(), region, client_profile)
```

Enabling instance termination protection

Last updated: 2023-09-27 11:20:00

Scenario

Under normal circumstances, when you no longer need an instance, you can destroy it through the console or API. To prevent accidental destruction of the instance, you can enable instance termination protection. Once enabled, you will not be able to destroy the instance via the console or API. If you have confirmed that the instance needs to be destroyed, you can disable instance termination protection and then proceed with the destruction operation.
You can enable instance termination protection to safeguard instances containing your business data from accidental destruction. This article explains how to enable and disable instance termination protection through the console.

Notes

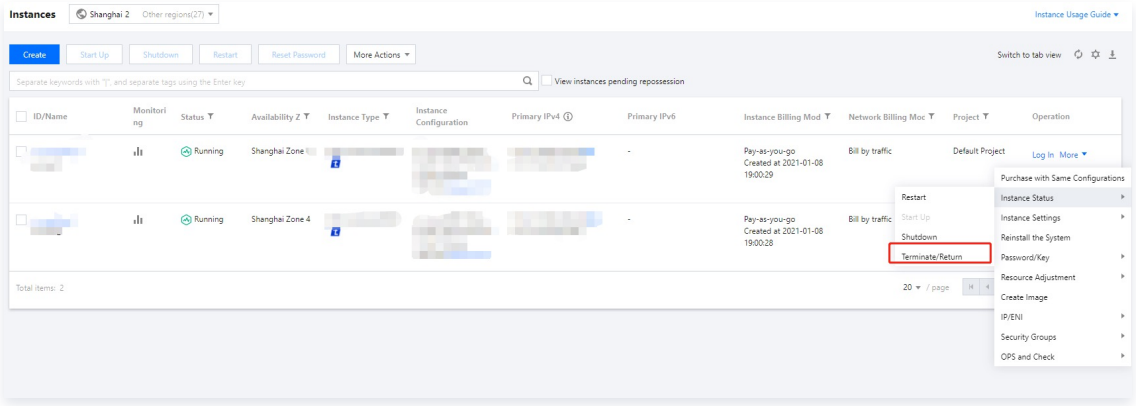
- Instance termination protection is disabled by default for newly purchased and existing instances. You can enable it as needed.
- Instance termination protection does not apply to system-level destruction. For example, pay-as-you-go instances destroyed due to overdue payments and shutdowns, or instances on a yearly or monthly plan that have expired and been in the recycle bin for more than 7 days.
- Spot instances do not support termination protection. This is because spot instances use market-based pricing and may be automatically repossessed by the system due to reduced resource inventory or competition from other users' bids.

Instructions

Enabling instance termination protection

Enabling termination protection for existing instances

1. Log in to the CVM console.
2. You can enable instance termination protection for one or multiple instances as needed:
   - **Enable termination protection for a single instance:**
     On the "Instances" page, find the instance for which you want to enable termination protection, and select **More** > **Instance Status** > **Terminate / Return** on the right side of its row, as shown in the following image:



   - **Enable instance termination protection in bulk:**
     On the "Instances" page, select the instances for which you want to enable termination protection, and choose **More** > **Instance Settings** > **Set Instance Termination Protection** at the top of the list.

3. In the "Set Instance Termination Protection" pop-up window, select "Enable" and click **OK** to enable instance termination protection.

Enable Termination Protection for Newly Purchased Instances

When purchasing a new instance, select "Custom Configuration" and check "Instance Termination Protection" under "Other Settings".

> **Note**
> For other parameter settings, please refer to Creating Instances via CVM Purchase Page.

Disabling instance termination protection

If you are sure that an instance can be terminated, follow the steps below to disable instance termination protection first before terminating it.

1. Log in to the CVM console.
2. You can disable instance termination protection for one or multiple instances as needed:
   - **Disable termination protection for a single instance:**
     On the "Instances" page, find the instance for which you want to disable termination protection, and select **More** > **Instance Settings** > **Set Instance Termination Protection** on the right side of the corresponding row.
   - **Batch disable instance termination protection:**
     On the "Instances" page, select the instances for which you want to disable termination protection, and choose **More** > **Instance Settings** > **Set Instance Termination Protection** at the top of the list.
3. In the "Set Instance Termination Protection" pop-up window, select "Disable" and click **OK** to disable instance termination protection.

Documentation

- Creating Instances via CVM Purchase Page
- Terminate/Return Instances

Instance Repossession or Recovering

Last updated: 2025-08-06 12:07:40

This document outlines the instance repossession mechanism and the process for restoring instances. For additional information, please refer to Arrears Guidance.

Instance Isolation Policies

Tencent Cloud Recycle Bin is a cloud service recovery mechanism. The instance isolation policies for different billing modes are as follows:

- **Monthly Subscribed Instances**: If the instance is terminated on the expiration date or before, it will be shut down and automatically moved to the recycle bin on the same day. If the account has sufficient balance and auto-renewal is enabled, the instance will be automatically renewed upon expiration and continue to operate normally.
- **Pay-as-you-go Instances**: Instances will be moved to the recycle bin after being manually terminated or scheduled for termination. In case of overdue payments, pay-as-you-go instances do not have a repossession mechanism, and the instance resources will be directly released after 2 hours of overdue payment + 15 days.

Instance status in the recycle bin are as follows:

Monthly Subscribed Instance Entering the Recycle Bin

- **Retention Period:** Instances in the recycle bin are retained for 15 natural days.
- **Expiration Handling:** If the instance is not renewed within 15 natural days, the system will release the resources, and they cannot be restored. The associated Elastic Public IP will be retained. If you no longer need this Elastic Public IP, please release it promptly.
- **Association:** After an instance enters the recycle bin, it **does not actively disassociate** from the load balancer, elastic cloud disk, or basic network intercommunication.
- **Operational Restrictions**: For instances within the recycle bin, only Renewal and Restoration, Termination/Return of Instance, and **Image Creation** operations can be performed (excluding special instance types).

Pay-as-you-go Instance Enters Recycle Bin

- **Retention Duration:** Instances that are voluntarily terminated by the user without overdue payments will be retained in the recycle bin for 2 hours.
- **Expiration Handling**: For instances that have not been renewed on time, the system will release the instance resources and automatically terminate/return the instance after the retention period has passed, making it non-recoverable. The associated Elastic Public IP will be retained. If you no longer need this Elastic Public IP, please release it promptly.
- **Association**: After an instance enters the recycle bin, the **associations** with load balancing, elastic cloud disks, and basic network interconnection are not actively removed.
- **Operational Restrictions**: For instances within the recycle bin, only Renewal and Restoration, Termination/Return of Instance, and **Image Creation** operations can be performed (excluding special instance types).

> **Note**
> - For pay-as-you-go instances in the recycle bin, you can not recover them when your account is overdue. Please make up the payment first.

- Pay-as-you-go instances are stored in the recycle bin for a maximum of 2 hours. Please note the release time and renew the payment in time to repossess the instances.
- In case of overdue payments, pay-as-you-go instances do not enter the recycle bin, and you need to check them on the Cloud Server Instance List page. If no payment is made after 2 hours of overdue payment + 15 days, the instance will be released.

Repossessing Instances

1. Log in to the CVM console and select **Recycle Bin** > **Instance Recycle Bin** on the left sidebar.
2. On the **Instance Recycle Bin** page, perform different operations as needed.

Restoring a Single Instance

Locate the instance you wish to restore in the list, click **Restore** under the operation column, and complete the renewal payment.

Batch Restore Instances

Select all the instances you want to restore from the list, and click **Batch Restore** at the top.

Spot Instances

Last updated: 2024-05-15 15:25:32

Scenario

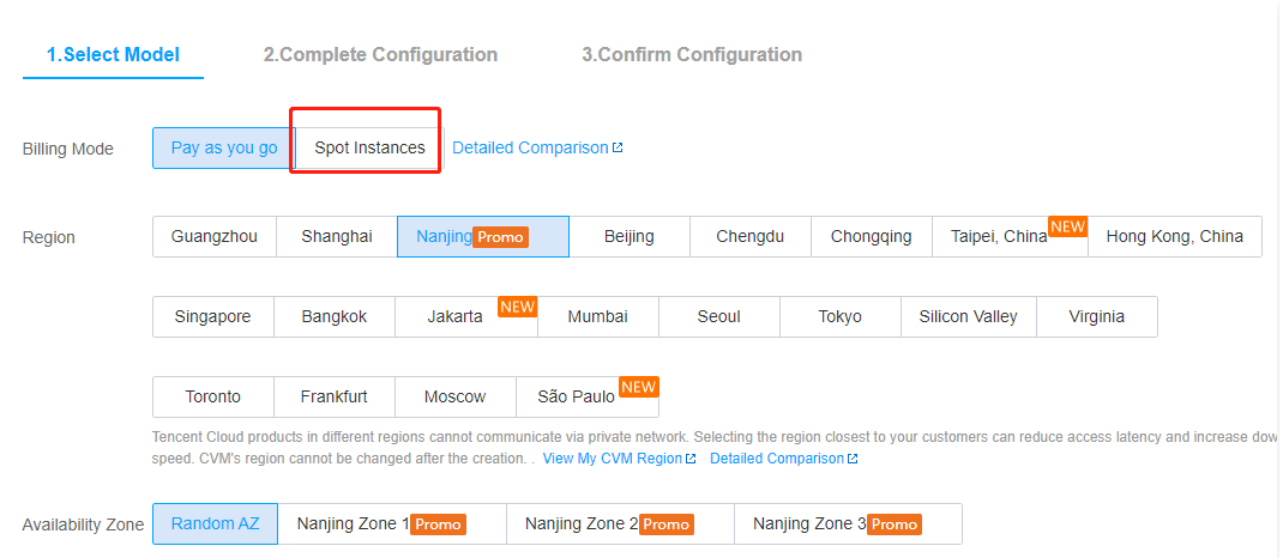
This document provides guidance on managing and purchasing spot instances. Spot instances are available through the following channels:

- **Cloud Virtual Machine Console**: The CVM purchase page supports spot instance mode.
- **Batch Compute Console**: Batch Compute supports selecting spot instances when submitting jobs and creating compute environments.
- **Cloud API**: The RunInstance interface has added parameters related to spot instances.

Instructions

Cloud Virtual Machine Console

1. Log in to the Cloud Virtual Machine Purchase Page.
2. When selecting an instance type, choose **Spot Instance** as the billing mode.



3. Select region, availability zone, network type, instance and other configuration information as needed and prompted by the page.
4. Check the information of the spot instance to be purchased and the cost details of each configuration item.
5. Click **Activate** to complete the payment.
   After the payment is completed, you can access your spot instances in the Cloud Virtual Machine Console.

Batch Compute Console

BatchCompute feature description

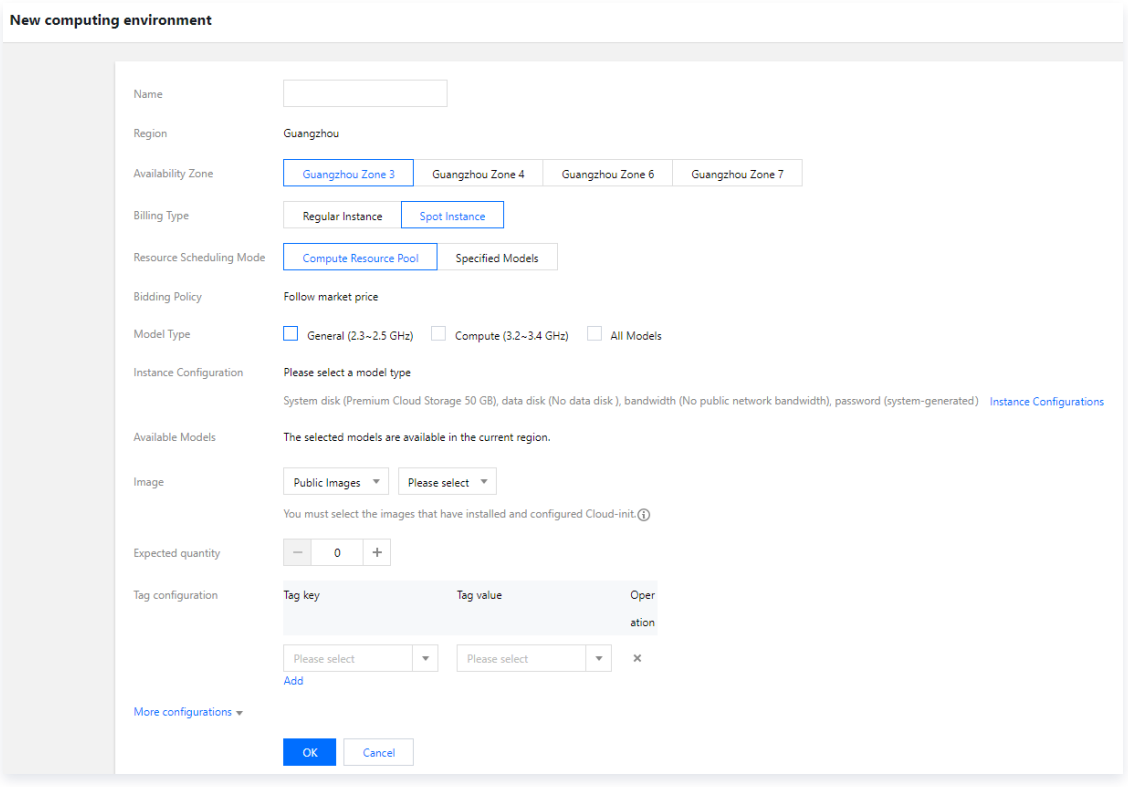
- **Asynchronous Interface**
  When submitting jobs, creating compute environments, or modifying the desired number of instances in a compute environment, Batch Compute processes your requests asynchronously. This means that if your current request cannot be fulfilled due to inventory or pricing constraints, Batch Compute will continue to request spot

instance resources until the desired number is met.
To release instances, you need to adjust the number of instances in the compute environment through the Batch Compute Console. If you release instances from the Cloud Virtual Machine Console, Batch Compute will automatically create new instances for you until the desired number is reached.

- **Cluster Mode**
  Batch Compute's compute environment supports maintaining a group of spot instances in a cluster mode. You only need to submit the required quantity, configuration, and maximum bid. The compute environment will automatically initiate requests until the desired quantity is met, and will automatically re-initiate requests to replenish the quantity in case of interruptions.
- **Fixed Price**
  At this stage, a fixed discount model is used. You must set the parameter to be greater than or equal to the current market price. For detailed market prices, please refer to Supported Regions, Instance Types, and Specifications for Spot Instances.

Directions

1. Log in to the Batch Compute console.
2. On the Compute Environment Management page, select any region (e.g., Guangzhou), and click **Create**.
   You will be directed to the New Compute Environment page.
3. On the Create Compute Environment page, set the "Billing Type" to **Spot Instance** and select the desired model, image, name, expected quantity, and other information based on your requirements.



4. Click **Confirm** to complete the creation.
   After the creation is complete, you can view the newly created compute environment in the Batch Compute Console. Meanwhile, the CVMs within the compute environment are being created synchronously. You can check the creation status through the **Activity Log** and **Instance List** of the compute environment.

TencentCloud API

In the RunInstance interface, the InstanceMarketOptionsRequest parameter can be used to specify the spot instance mode and configure related information.

- **Synchronous Interface**: Currently, RunInstance provides a one-time synchronous request interface. If the application fails (due to insufficient inventory or a request price lower than the market price), it will immediately return a failure and will not continue to apply.
- **Fixed Price**: At this stage, a fixed discount mode is used. You must set the parameter to be greater than or equal to the current market price. For detailed market prices, please refer to Supported Regions, Instance Types, and Specifications for Spot Instances.

Example

You have an instance located in Guangzhou Zone 3 with an hourly postpaid spot pricing mode. The specific spot pricing configuration details are as follows:

- MaxPrice: 0.6 CNY/hour
- SpotInstanceType: one-time
- ImageId: img-pmqg1cw7
- InstanceType: S2.MEDIUM4 (Standard 2, 2-core, 4GB)
- InstanceCount: 1

Request Parameters

```
https://cvm.tencentcloudapi.com/?Action=RunInstances
&Placement.Zone=ap-guangzhou-3
&InstanceChargeType=SPOTPAID
&InstanceMarketOptions.MarketType=spot
&InstanceMarketOptions.SpotOptions.MaxPrice=0.60
&InstanceMarketOptions.SpotOptions.SpotInstanceType=one-time
&ImageId=img-pmqg1cw7
&InstanceType=S2.MEDIUM4
&InstanceCount=1
&<Common request parameter>
```

Response parameters

```
{
  "Response": {
    "InstanceIdSet": [
      "ins-1vogaxgk"
    ],
    "RequestId": "3c140219-cfe9-470e-b241-907877d6fb03"
  }
}
```

Querying the Repossession Status of a Spot Instance

Last updated: 2024-05-15 15:25:33

Cloud Server Spot Instance mode may result in instances being automatically reclaimed by the system due to pricing or inventory reasons. To facilitate users in performing custom operations before instance reclamation, an interface is provided to obtain the reclamation status from within the instance using the Metadata mechanism. The specific usage is as follows:

Metadata

Instance metadata refers to the data related to an instance, which can be used to configure or manage running instances. You can access and obtain instance metadata from within the instance. For more information, see Viewing Instance Metadata.

Using metadata to obtain information about repossession status of a spot instance

Run the following command using the cURL tool. You can also send an HTTP GET request.

```
curl metadata.tencentyun.com/latest/meta-data/spot/termination-time
```

- If the instance has been terminated, the termination time of the spot instance is returned, as shown below.

> **Note**
> The termination time refers to the OS time of the spot instance when it's terminated (in UTC+8).

```
2018-08-18 12:05:33
```

- If the error code 404 is returned, the instance is not a spot instance or repossession has not been triggered.

For more information, see Querying Instance Metadata.

No Charges When Shut Down for Pay-as-You-Go Instances

Last updated: 2024-05-15 15:25:33

Scenario

"No Charges When Shut Down" refers to the cessation of instance (CPU, memory) fees for pay-as-you-go instances after they enter the **Shut Down** state through the shutdown operation. Components such as cloud disks (system disk and data disk), public network bandwidth, and images will continue to be billed.

> **Note**
> After enabling the "No Charges When Shut Down" feature, the instance's CPU and memory will **no longer be reserved**, and the public IP address will be **automatically released**. For more information on feature descriptions, usage restrictions, and impacts, please refer to Pay-as-you-go Instances: No Charges When Shut Down.

Instructions

Via the Console

1. Log in to the CVM console.
2. On the instance management page, you can shut down a single instance or multiple instances as needed:
   - **Shutting down a single instance**: Perform the operation according to the actual view mode used.
     - **List View**: Select the instance you wish to shut down, and in the operation column on the right, choose **More** > **Instance Status** > **Shut Down**.
     - **Tab View**: On the page of the instance you want to shut down, select **Shut Down** in the top-right corner.
   - **Shut Down Multiple Instances**: Select all the instances you want to shut down, and click **Shutdown** at the top of the list.
3. In the "Shutdown" window that appears, you can choose the "Shutdown Mode".
4. Select "**No Charges When Shut Down**" and click **OK.**

TencentCloud API Operation

You can use the StopInstances API to shut down instances. Refer to the Shutting Down Instances documentation. Add the following parameters:

Parameter name	Required	Local Disk Types	Description
StoppedMode	Not required	String	"No Charges When Shut Down" is only applicable to pay-as-you-go cloud disk instances. **Value Range:** KEEP_CHARGING: Continue charging after shutdown; STOP_CHARGING: No charges when shut down. **Default Value:** KEEP_CHARGING

Managing Roles

Last updated: 2023-09-27 11:31:50

Scenario

Cloud Access Management (CAM) roles are virtual identities with a set of permissions, used to grant access to services, operations, and resources within Tencent Cloud. You can associate CAM roles with Cloud Virtual Machine (CVM) instances, and access other cloud product APIs within the instance using Tencent Cloud's Security Token Service (STS) temporary keys (which are periodically updated). This method provides enhanced security for your account's SecretKey and allows for more granular control and permission management through CAM capabilities, compared to using SecretKey directly for access control.
This document describes how to bind, modify, and delete a role.

Strengths

Binding a CAM role to instances comes with the following features and advantages.

- You can access other Tencent Cloud services using STS temporary keys. For more information, see STS APIs.
- Grant roles with different permissions to different instances for a refined permission control.
- You don't need to save SecretKey in an instance. Instead, you can easily control the access permissions of the instance by changing the role authorization.

Notes

- Instances only support binding roles with the role entity containing `cvm.qcloud.com`. For more information, see Role Basics.
- The CVM instance must reside in a VPC.
- You can grant only one role to a CVM instance at a time.
- Binding, modifying and deleting roles are free of charge.

Instructions

Binding/modifying roles

Binding/modifying the role of one CVM

1. Log in to the Cloud Virtual Machine console and select **Instance** on the left sidebar.
2. On the instance management page, proceed according to the actually used view mode:
   - **List View**: In the row of the target instance, select **More** > **Instance Settings** > **Bind/Modify Role.**
   - **Tab view**: In the CVM page, select **More** > **Instance Settings** > **Bind/Modify Role** in the upper right corner.
3. In the "Bind/Modify Role" pop-up window, select the role to bind and click **OK.**

Batch binding/modifying roles

1. In the "Instances" list page, select the CVMs that need to be bound or have their roles modified, and click **More Actions** > **Instance Settings** > **Bind/Modify Role.**
2. In the "Bind/Modify Role" pop-up window, select the role to bind and click **OK.**

> **Note**
> CVMs modified using this method will have the same role name.

Deleting roles

Deleting the role of one CVM

1. Log in to the Cloud Virtual Machine console and select **Instance** on the left sidebar.
2. On the instance management page, proceed according to the actually used view mode:
   - **List View**: In the row of the target instance, select **More** > **Instance Settings** > **Remove Role.**
   - **Tab View**: In the Cloud Virtual Machine page, select **More Actions** > **Instance Settings** > **Delete Role** in the top-right corner.
3. In the "Delete Role" pop-up window, click **Confirm** to proceed.

Batch deletion of instance roles

1. In the "Instances" list page, select the cloud server for which you want to delete the role, and click **More Actions** > **Instance Settings** > **Delete Role** at the top.
2. In the "Delete Role" pop-up window, click **Confirm** to proceed.

Images
Creating a Custom Image

Last updated: 2023-09-07 17:20:47

Scenario

In addition to using public images and service marketplace images provided by Tencent Cloud, you can also create custom images. After creating a custom image, you can quickly create Tencent Cloud CVM instances with the same configuration as the image through the Tencent Cloud console.

Note

Notes on snapshot usage

- A free tier of 80GB is available in each region in the Chinese mainland. For more information, see Free Tier.
- When creating a custom image, a snapshot associated with the image will be created by default, and retaining the custom image will incur certain snapshot fees. For more information, see Snapshot Billing Overview.
- If your Tencent Cloud account becomes overdue, to prevent data loss, we will retain your custom images and associated snapshots without incurring any additional charges.

Supports and Limits

- Each region supports a maximum of 50 custom images.
- If your Linux instance has a data disk, but you only create a custom image of the system disk, please ensure that `/etc/fstab` does not contain data disk configurations. Otherwise, instances created using this image may not start up normally.
- The creation process takes ten minutes or more, which depends on the data size of the instance. Please prepare in advance to avoid business impacts.
- If your Windows instance needs to join a domain and use a domain account, please execute the Sysprep operation before creating a custom image to ensure the SID remains unique after the instance joins the domain. For more information, see Ensure Unique SID for CVM Instances Joined to a Domain Using Sysprep.
- If you are using a bare metal server with a 25Gbps network card (i.e., the instance's internal bandwidth value is 25Gbps), creating custom images through the console and API is currently not supported.

Instructions

Creating from an Instance via the Console

Shutting down the instance (optional)

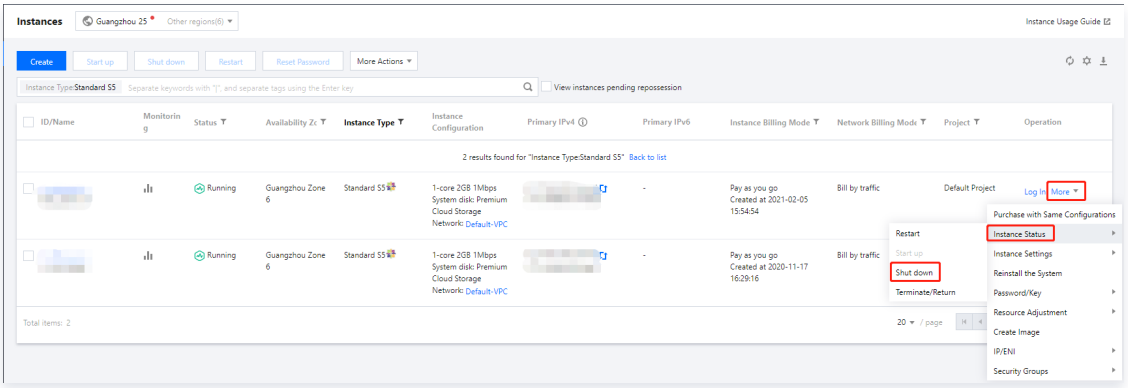
1. Log in to the CVM console and check whether the corresponding instance needs to be shut down.

   Note

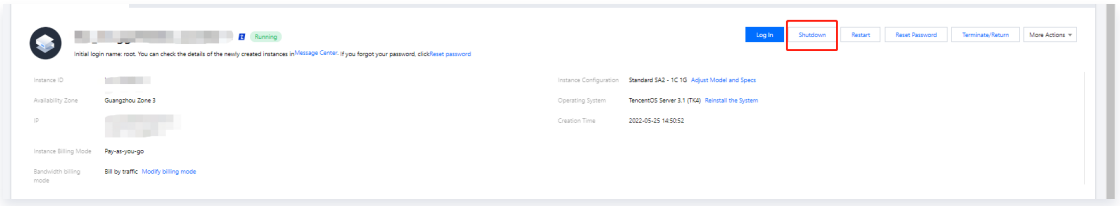
   For CVMs created based on public images after July 2018, you can create images without shutting down the instance. For other CVMs, shut down the instance before creating a custom image to ensure that the image has the same environment deployment as the current instance.

   - If the instance needs to be shut down, proceed to the next step.
   - If the instance doesn't need to be shut down, please proceed to Create a custom image.
2. On the instance management page, proceed according to the actually used view mode:

- **List View:** In the row where the instance is located, click **More** > **Instance Status** > **Shut down** on the right, as shown below:

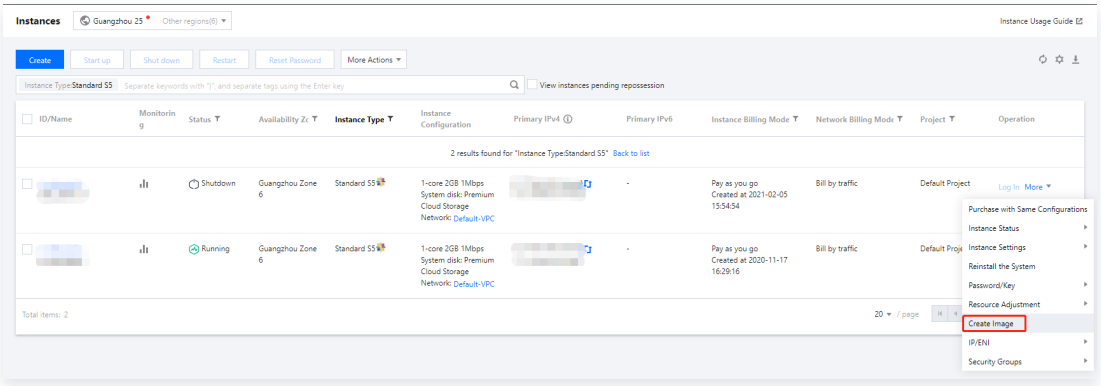


- **Tab View:** Select **Shutdown** in the instance details page, as shown below:

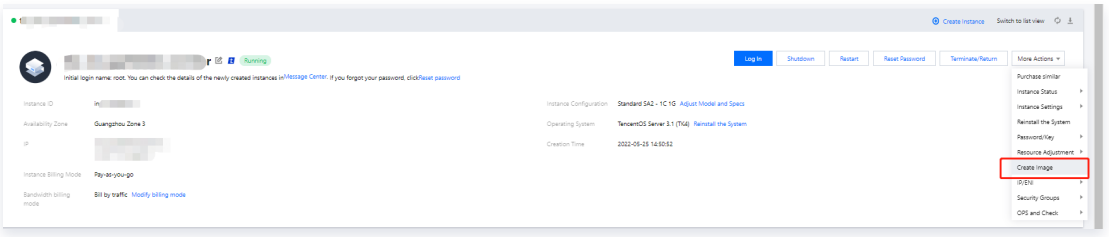


Creating a custom image

1. On the instance management page, proceed according to the actually used view mode:
   - **List view:** Select **More** > **Create image**.



   - **Tab view:** Select **More actions** in the top-right corner > **Create image**. As shown in the figure below:



2. In the **Create Custom Image** pop-up window, refer to the following information for configuration:
   - **Image Name** and **Image Description**: Customize the name and description.
   - **Tags**: You can add tags as needed for resource categorization, search, and aggregation. For more information, see Tags.

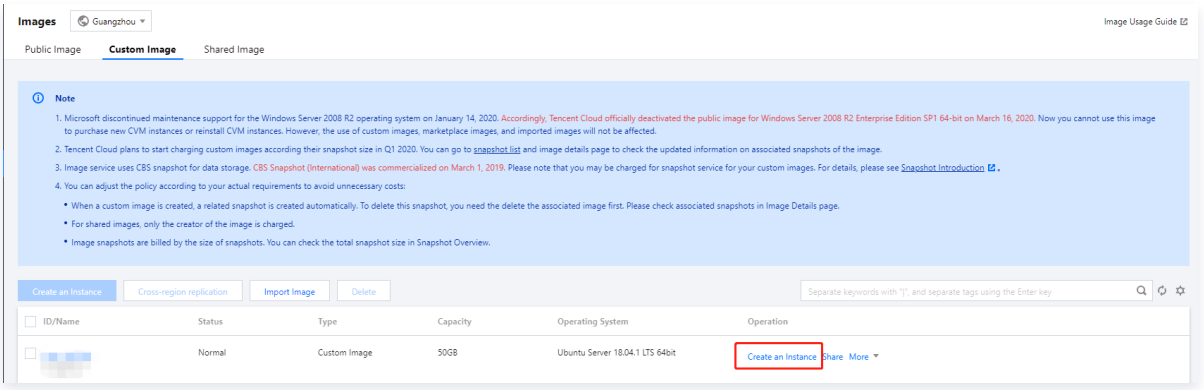
> **Note**

> If you need to create a custom image that includes both system and data disks, please contact Online Customer Service to request access to this feature.

3. Click **Create Image** to proceed.
   You can view the image creation progress in the **Images** page by clicking Image in the left sidebar.

Using custom image to create instance (optional)

Select the image you created in the image list, and click **Create an instance** on the right side to purchase a server with the same configuration as the image, as shown in the following figure:



Creating via API

You can create a custom image using the CreateImage API. For more information, see Create Image API.

Best practices

Migrate data on a data disk

If you need to retain the data on the original instance's data disk when launching a new instance, you can first create a snapshot of the data disk and use that snapshot to create a new cloud disk data disk when launching the new instance. For more information, please refer to Create Cloud Disk with Snapshot.

Sharing Custom Images

Last updated: 2023-09-07 17:21:19

Scenario

Shared Images allow you to share your **Custom Images** with **other Tencent Cloud accounts**. You can easily obtain shared images from other Tencent Cloud accounts and acquire the necessary components and add custom content.

> **Note**
> Tencent Cloud does not guarantee the integrity or security of shared images. Please only use shared images from reliable sources.

Supports and Limits

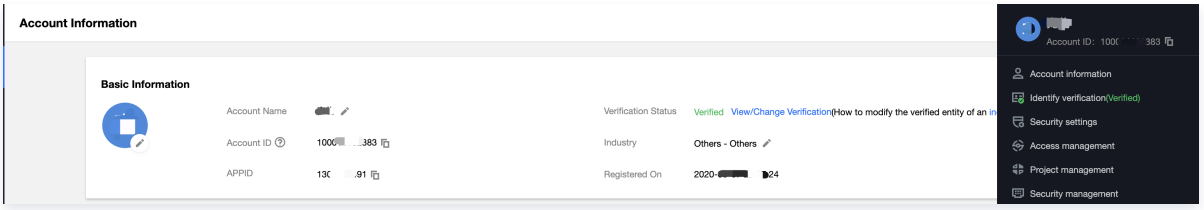
- Each image can be shared with a maximum of 50 Tencent Cloud accounts. An image can be shared with up to 50 Tencent Cloud accounts at a time.
- You can not change the name and description of the images shared from others. They can only be used to create or reinstall CVM instances.
- When you share an image to others, the shared replicas do not count against your image quota.
- You can delete an image shared with other Tencent Cloud accounts, but you must first cancel all shares of that image. For details on how to unshare an image, see Unsharing Custom Images. Shared images obtained cannot be deleted.
- Custom images can only be shared with accounts in the same region as the source account. To share an image with users in another region, you need to copy it to the target region before sharing.
- The shared images that you obtain from others cannot be re-shared.

Instructions

Obtaining the ID of the root account to which you want to share the image

The image sharing requires the unique ID of the root account to whom an image will be shared. Request the other user to record the account ID as instructed below:

1. Log in to the CVM console.
2. Click the account name in the upper right corner and select **Account Information**.
3. On the **Account Information** management page, view and note down the main account ID, as shown below:



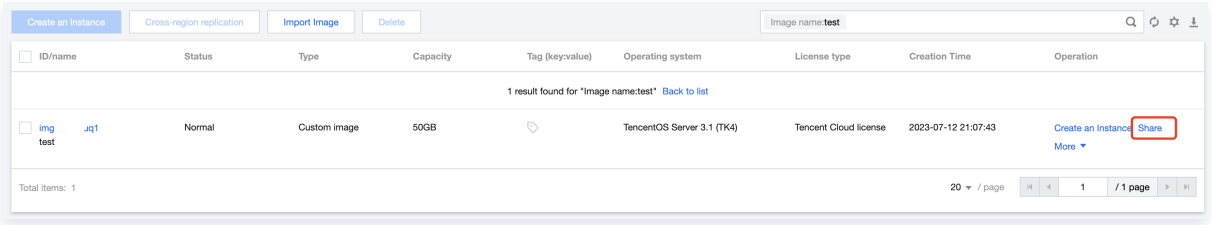
4. Send his/her account ID to you.

Shared Image

Sharing via Console

1. Log in to the CVM console and select **Image** on the left sidebar.
2. Select the **Custom Images** tab to enter the custom image management page.

3. In the custom image list, select the custom image you want to share and click **Share** on the right.



4. In the **Share Image** window that appears, enter the account ID of the other party's primary account and click **Share**.
5. Inform the recipient to log in to the Cloud Server Console and select **Images** > **Shared Images** to view the shared image. If you need to share with multiple Tencent Cloud accounts, please repeat the above steps.

Sharing via API

You can use the ModifyImageSharePermission API to share images. For more information, refer to Modify Image Share Permission.

Related Actions

Sharing image with Lighthouse

You can share custom images between Lighthouse and CVM, enabling rapid offline migration of services. You can also quickly create instances using shared images to obtain required components or add custom content. For more information, please refer to Managing Shared Images.

Cancelling Image Sharing

Last updated: 2024-05-15 15:25:33

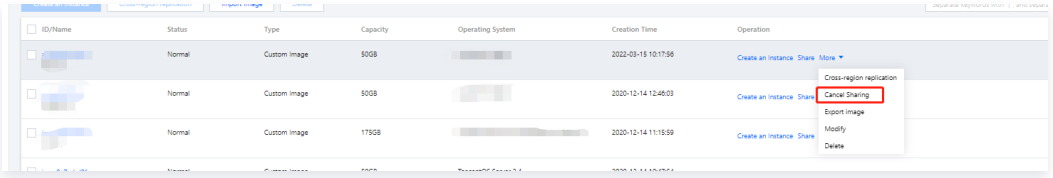
Scenario

This document guides users on how to unshare custom images. Users can terminate the sharing status of an image with others at any time, deciding not to share it with a specific user anymore. This operation will not affect instances created by other users using the shared image, but they will no longer be able to view or use the image to create more instances.

Instructions

Cancel Sharing via Console

1. Log in to the CVM console and select **Image** on the left sidebar.
2. Select the **Custom Images** tab to enter the custom image management page.
3. In the custom image list, select the custom image you want to unshare, and click **More** > **Cancel Sharing**, as shown in the figure below:



4. On the new page, select the unique ID of the target account you want to unshare with, and click **Cancel Sharing**.
5. In the pop-up prompt, click **Confirm** to complete the unsharing of the image.

Cancel Sharing via API

Users can unshare images using the ModifyImageSharePermission API. For more information, refer to Modify Image Share Permission.

Deleting Custom Images

Last updated: 2024-05-15 17:15:02

Scenario

This document describes how to delete custom images.

Supports and Limits

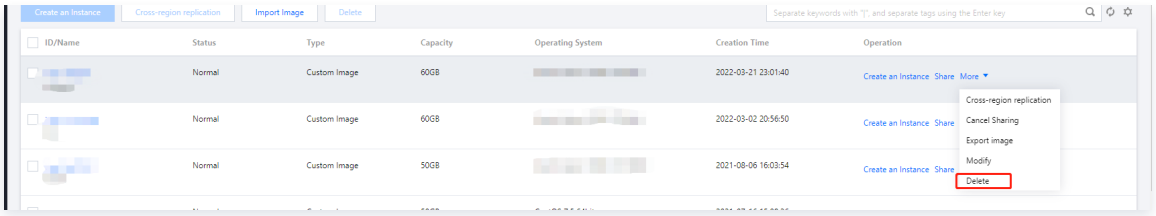
Before deleting custom images, please note the following items:

- After deleting a custom image, you will no longer be able to create instances from it, but it will not affect instances that have already been launched. If you need to delete all instances launched from this image, refer to Reclaim Instances or Terminate/Return Instances.
- Shared images cannot be deleted. You must first cancel all shares before deleting them. To unshare an image, refer to Unshare Custom Images.
- Only custom images can be deleted; public images and shared images cannot be actively removed.

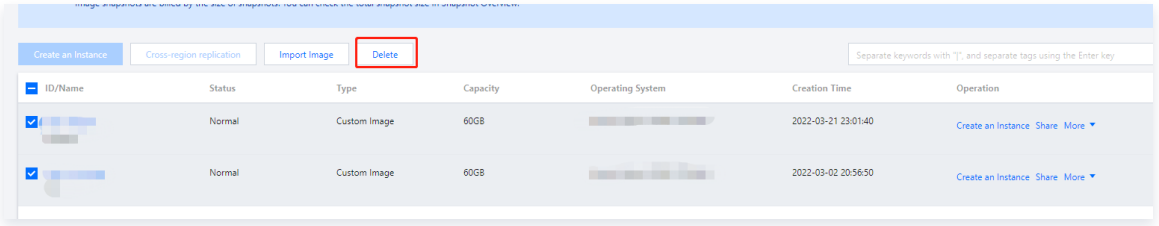
Instructions

Deleting via the Console

1. Log in to the CVM console and select **Image** on the left sidebar.
2. Select the **Custom Images** tab to access the custom image management page.
3. Select the method to delete custom images based on actual needs.
   - **Delete a single image**: In the list, locate the custom image you want to delete, and select **More** > **Delete**. As shown below:



   - **Delete multiple images**: Select all custom images you want to delete from the list and click **Delete** at the top. As shown in the image below:



4. In the pop-up prompt, click **Confirm**.
   If the image cannot be deleted, the reason will be displayed.

Deleting via API

Users can use the DeleteImages API to share images. For more information, see Delete Images.

Image Replication

Last updated: 2023-09-07 17:22:26

Overview

Common Steps

Copying Images includes two features: **Custom Image – Cross-region Replication** and **Shared Image – Intra-region Replication**.

Image Copying Function	Advantages	Note
Custom Image – Cross-region Replication	Helps users quickly deploy identical CVM instances **across regions**.	You can replicate custom images across regions, and then create cloud servers using the copied images in the new region.
Shared Image – Intra-region Replication	Assists users in copying shared images to custom images for more flexible usage.	The replicated custom image has no special restrictions and possesses the same features as other custom images.

Notes

- Custom images can be replicated across regions, and shared images support intra-region replication.
- **Region Restrictions**:
  - Currently, image replication supports copying from domestic regions to domestic regions, and from overseas regions to overseas regions. If you need to copy an image from a domestic region to an overseas region, or from an overseas region to a domestic region, please apply through Online Support.
  - Due to data security restrictions in Finance Zones, image copying is supported within Finance Zones but not between Finance Zones and non-Finance Zones.
- Image replication is free of charge. But you need to pay for snapshot service for store the copied custom images.
- Cross-region replication takes 10 to 30 minutes.
- Cross-region replication is not available for full images.

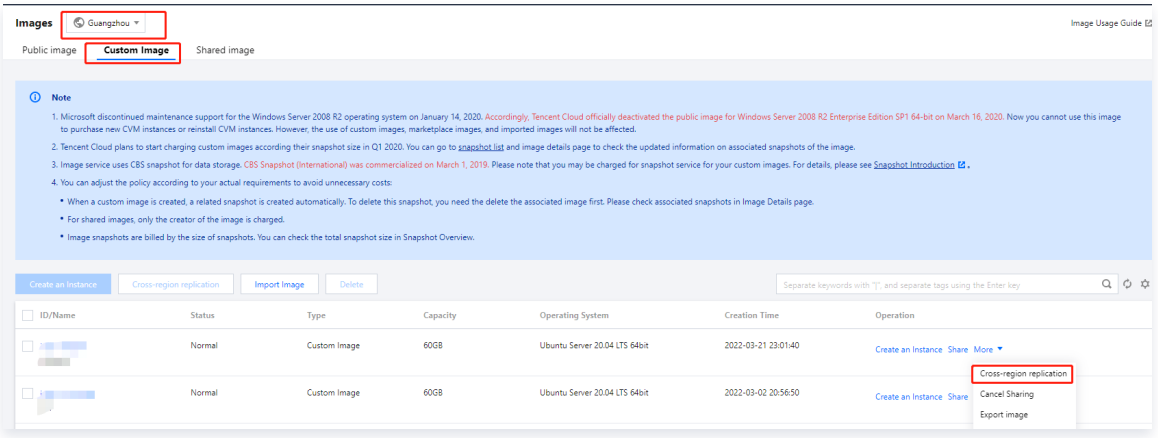
Methods

Cross-region Replication of Custom Images

Copying via the Console

1. Log in to the CVM console.
2. Click **Image** in the left sidebar to enter the Image Management page.
3. Select the region of the original image to be copied, and click the **Custom Image** tab. As shown in the figure below:

For example, select the Guangzhou region.



4. In the row of the instance with the image to be copied, select **More** > **Cross-region Replication**.
5. In the **Cross-region Image Copy** pop-up window, select the destination region to copy the image to, and click **Confirm**.
   After the copy is successful, the image list in the destination region will display images with the same name but different IDs.
6. Switch to the destination region, and in the image list for that region, select the successfully copied image. Click **Create Instance** to create an identical cloud server instance.

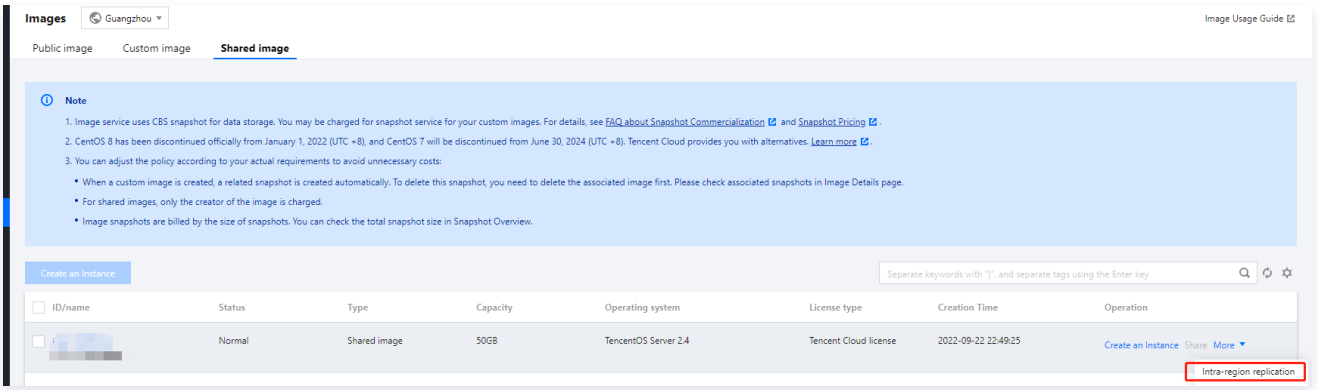
Copying Using APIs

You can use the SyncImages API to copy images. For more information, see Image Synchronization API.

Intra-region Replication of Shared Images

Copying via the Console

1. Log in to the CVM console.
2. Click **Image** in the left sidebar to enter the Image Management page.
3. Select the region of the original image to be copied, and click the **Shared Image** tab. As shown in the image below:
   For example, choose the Guangzhou region.



4. In the row of the instance with the image to be copied, select **More** > **Intra-region Replication**.
5. In the **Cross-region Image Copy** pop-up window, select the destination region to copy the image to, and click **Confirm**.

After the copy is successful, the image list in the destination region will display images with the same name but different IDs.

6. Switch to the Custom Images tab, select the successfully copied image, and click **Create Instance** to create an identical cloud server instance. The copied custom image has no special restrictions and possesses the same features as other custom images.

Copying Using APIs

You can use the SyncImages API to copy images. For more information, see Image Synchronization API.

Importing Images Overview

Last updated: 2023-09-27 14:12:00

In addition to using the Create Custom Image feature, Tencent Cloud also supports importing images. You can import local or other platform server system disk image files into CVM custom images. After importing, you can use the imported image to create a new CVM or reinstall the system on an existing CVM.

Note

Notes on snapshot usage

- An 80 GB free tier is provided in domestic regions. For more information, see Free Quota.
- When creating a custom image, a snapshot associated with the image will be created by default, and retaining the custom image will incur certain snapshot fees. For more information, see Snapshot Billing Overview.
- If your Tencent Cloud account becomes overdue, to prevent data loss, we will retain your custom images and associated snapshots without incurring any additional charges.

Preparations

Prepare an image file that meets the import requirements.

Linux system image limitations

Image Attributes	Conditions
Operating System	• Images based on CentOS, CentOS Stream, Ubuntu, Debian, OpenSUSE, CoreOS, FreeBSD, Kylin, UnionTech, TencentOS, Fedora, AlmaLinux, Rocky Linux, OpenCloudOS, and other Linux distributions. • Supports 32-bit, 64-bit, and arm_64-bit architectures.
Image format	• Supported image formats include RAW, VHD, QCOW2, and VMDK. • Run qemu-img info imageName | grep 'file format' to check the image format. For other image file formats, you can refer to Converting Image Format for conversion before importing.
File System Type	GPT partition is not supported.
Image size	• The actual image size cannot exceed 50 GB. Run qemu-img info imageName | grep 'disk size' to check the image size. • The image's virtual size (vsize) must not exceed 500 GB. Use the command qemu-img info imageName | grep 'virtual size' to check the image's vsize. **Attention**: When importing an image, the review size is based on the image information after converting to the QCOW2 format.
Networking	• Tencent Cloud provides the eth0 network interface by default for instances. • Users can query the network configuration of an instance through the metadata service within the instance. For more information, see Instance Metadata.
Driver	• The image must have the Virtio driver installed for the KVM virtualization platform. For more information, see Checking Virtio Drivers in Linux Imported Images.

	• Install cloud-init in the image. For more information, see Installing Cloud-Init in Linux Imported Images. • If the image cannot install cloud-init due to other reasons, please configure the instance according to Force Import Image.
Kernel Limitations	Native kernel is preferred for an image. Any modifications on the kernel may cause the import to fail.
Available Regions	Importing images from COS in another region is unavailable for the Shanghai Finance and Shenzhen Finance.

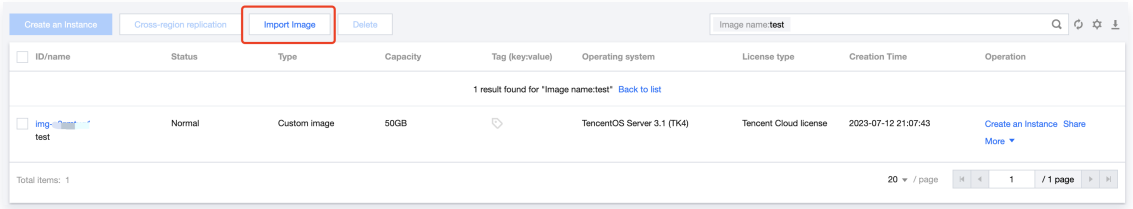
Windows System Image Limitations

Image Attributes	Conditions
Operating System	• Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012, Windows Server 2008, and other related Windows versions. • Supports 32-bit, 64-bit, and arm_64-bit architectures.
Image format	• Supported image formats include RAW, VHD, QCOW2, and VMDK. • Use `qemu-img info imageName | grep 'file format'` to check the image format. For other image file formats, you can refer to Converting Image Format for conversion before importing.
File System Type	• Only NTFS file systems using MBR partitioning are supported. • GPT partition is not supported. • Logical Volume Management (LVM) is not supported.
Image size	• The actual image size cannot exceed 50 GB. Use `qemu-img info imageName | grep 'disk size'` to check the image size. • The image's virtual size (vsize) must not exceed 500 GB. Use `qemu-img info imageName | grep 'virtual size'` to check the image's vsize. **Attention**: When importing an image, the review size is based on the image information after converting to the QCOW2 format.
Networking	• Tencent Cloud provides a local connection network interface for instances by default. • Users can query the network configuration of an instance through the metadata service within the instance. For more information, see Instance Metadata.
Driver	The image must have the Virtio driver for the KVM virtualization platform installed. Windows systems do not have the Virtio driver installed by default. Users can install the Windows Virtio driver and then export the local image. The download links for the Windows Virtio driver are as follows, please choose the appropriate link based on your actual network environment: • Public network download address: http://mirrors.tencent.com/install/windows/virtio_64_1.0.9.exe • Private network download address: http://mirrors.tencentyun.com/install/windows/virtio_64_1.0.9.exe

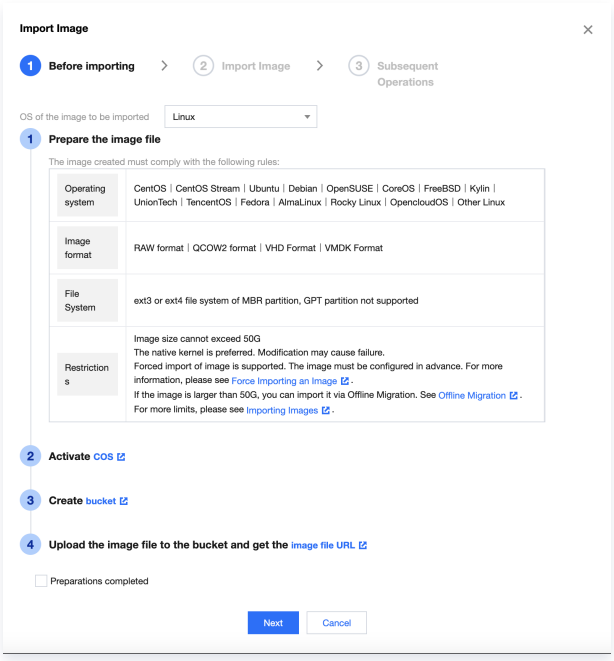
Available Regions	Importing images from COS in another region is unavailable for the Shanghai Finance and Shenzhen Finance.
Others	The imported Windows system image does not provide Windows Activation service.

Directions

1. Log in to the CVM console and click **Images** in the left sidebar.
2. Select **Custom Image** and click **Import Image**.



3. As per the operational interface requirements, first activate COS, then create a bucket, upload the object image file to the bucket and obtain the image file URL.



4. Click **Next**.
5. Complete the configurations and click **Import**.

> **Note**
> Ensure the entered COS file URL is correct.

You will be notified about the result of import via Message Center.

Failed Imports

After initiating the image import operation in the console, the task may fail due to various reasons. In case of failure, you can troubleshoot the issue based on the following information.

Supports and Limits

Before troubleshooting the failure reasons mentioned in this article, please ensure that you have subscribed to product service notifications in the Message Center Management Page to receive in-app messages, SMS, and emails containing the failure reasons.

> **Note**
> If you do not subscribe to product service notifications, you will not receive the notification from Message Center about whether an import is successful.

Troubleshooting the causes of failure

You can refer to the following information for troubleshooting on errors. See Error Codes for detailed error prompts and error descriptions.

InvalidUrl: Invalid COS link

The InvalidUrl error indicates that an incorrect COS URL has been entered. The possible causes are:

- An image link not from Tencent Cloud Object Storage was entered.
- The permission of the COS URL is not public read and private write.
- The COS file has private read access, but the signature has expired.

> **Note:**
> Signed COS URLs can only be accessed once.

- When importing an image outside the Chinese mainland, a COS link in a different region is used.

> **Note:**
> The image import service outside the Chinese mainland only supports COS instances in the same region; that is, a COS link in the same region needs to be used for import.

- The user's image file has been deleted.

Upon receiving an "Invalid COS link" error, you can troubleshoot the issue based on the aforementioned reasons.

InvalidFormatSize: Format or size does not meet requirements

The InvalidFormatSize error indicates that the format or size of an image to be imported does not meet the following requirements of Tencent Cloud:

- Supported image file formats are `qcow2`, `vhd`, `vmdk`, and raw.
- The actual file size of the imported image must not exceed 50 GB (based on the qcow2 format image file).
- The system disk size of the imported image must not exceed 500 GB.

If you receive an error message that the image format or size is invalid:

- You can follow the image format conversion steps in Linux Image Creation to convert the image file into a suitable format and streamline the image content to meet size limitations before re-importing the image.
- You can also use the Offline Instance Migration feature to migrate instances, which supports a maximum image file size of 500 GB for migration.

VirtioNotInstall: Virtio driver not installed

An error message VirtioNotInstall indicates that the pre-imported image does not have the Virtio driver installed. Tencent Cloud uses KVM virtualization technology, which requires the user-imported image to have the Virtio

driver installed. Most Linux operating systems already have the Virtio driver installed, except for a few custom Linux systems. For Windows operating systems, users need to manually install the Virtio driver:
- For Linux image import, see Checking Virtio Drivers in Linux.
- For Windows image import, see Creating Windows Images for installing Virtio drivers.

CloudInitNotInstalled: cloud-init not installed

The CloudInitNotInstalled error indicates that the pre-imported image does not have the cloud-init program installed. Tencent Cloud uses the open-source program cloud-init to initialize instances; therefore, the absence of the cloud-init program may result in instance initialization failure.
- For Linux image import, see Installing Cloud-Init on Linux.
- For Windows image import, see Installing Cloudbase-Init on Windows.
- After installing cloud-init or cloudbase-init, please replace the configuration file according to the documentation to ensure that the instance pulls data from the correct data source upon startup.

PartitionNotPresent: Partition information not found

The PartitionNotPresent error indicates that the imported image is incomplete. Check whether the boot partition was included when the image was created.

RootPartitionNotFound: Root partition not detected

The RootPartitionNotFound error indicates that the imported image does not contain a root partition. Please check the image file. Some previously encountered reasons are provided for reference:
- The installation package was uploaded.
- The data disk image was uploaded.
- The boot partition image was uploaded.
- An incorrect file was uploaded.

InternalError: Other errors

The InternalError error indicates that the cause of error has not yet been recorded. Contact the customer service and our technical personnel will help you resolve the issue.

Error Code

Error Code	Cause	Suggested Solution
InvalidUrl	Invalid COS link.	Verify if the COS link and the import image link are the same.
InvalidFormatSize	Invalid format or size	Images must meet the image format and `image size` requirements in `Preparations`.
VirtioNotInstall	Virtio driver not installed	Install the Virtio driver in the image by referring to the Driver section in `Preparations`.
CloudInitNotInstalled	cloud-init not installed	Install cloud-init in the Linux image by referring to the Driver section in `Preparations`.
PartitionNotPresent	Partition information not found.	Image corruption may be caused by an incorrect image creation method.
RootPartitionNotFound	Root partition not found.	Image corruption may be caused by an incorrect image creation method.
InternalError	Other errors.	Please contact customer service to address the issue.

Forcibly Importing Image

Last updated: 2024-06-02 10:12:31

Scenario

When a user's Linux image cannot install cloud-init for some reason, the **forced image import** feature can be used to complete the image import. Since the forcibly imported image does not have cloud-init installed, Tencent Cloud cannot initialize the configuration for the user's CVM. Therefore, when using a forcibly imported image, users need to set up scripts according to the configuration files provided by Tencent Cloud to configure the CVM. This document guides users on how to configure a CVM under the premise of forcibly importing an image.
Tencent Cloud provides a CD-ROM device containing configuration information for users to configure themselves. Users need to mount the CD-ROM and read the information in `mount_point/qcloud_action/os.conf` for configuration. If users need to use other configuration data or UserData, they can directly read the files under `mount_point/`.

os.conf Configuration File

The content of os.conf is as follows.

```
hostname=VM_10_20_xxxx
password=GRSgae1fw9frsG.rfrF
eth0_ip_addr=10.104.62.201
eth0_mac_addr=52:54:00:E1:96:EB
eth0_netmask=255.255.192.0
eth0_gateway=10.104.0.1
dns_nameserver="10.138.224.65 10.182.20.26 10.182.24.12"
```

> **Note**
> The parameter names above are for reference only, and the parameter values are for illustration purposes.

The description of each parameter in the os.conf configuration file is as follows:

Parameter name	Description
hostname	Host name
password	Encrypted password
eth0_ip_addr	Local area network IP of eth0 network interface
eth0_mac_addr	MAC address of the eth0 network interface
eth0_netmask	Subnet mask of eth0 network interface
eth0_gateway	Gateway for eth0 network interface
dns_nameserver	DNS Resolution Server

Limits

- The image still needs to meet the requirements for Linux image import in Importing Images (excluding cloud-init).
- The system partition for importing the image is not full.
- The imported image contains no vulnerability that can be exploited remotely.

- We recommend you change the password immediately after the instance is created successfully with the forcibly imported image.

Supports and Limits

Note the following when configuring script parsing:

- The script is executed automatically at startup. Please implement this requirement based on your operating system.
- The script must mount `/dev/cdrom` and read the `qcloud_action/os.conf` file under the mount point to obtain configuration information.
- The password placed in the CD-ROM by Tencent Cloud is encrypted. Users can set it using `chpasswd -e`. **Since the encrypted password may contain special characters, it is recommended to place it in a file first and then set it using `chpasswd -e < passwd_file`.**
- When creating an image from an instance made using a forcibly imported image, ensure that the script is still executed to guarantee the correct configuration of the instance. Alternatively, you can install cloud-init within the instance.

Instructions

> **Note**
> Tencent Cloud provides a sample script based on CentOS. Users can create a configuration script for their own image according to the sample script. During the creation process, please pay attention to the following points:
> - **Place the script correctly in the system before importing the image.**
> - This script may not be suitable for all operating systems. Users need to make appropriate modifications according to their own operating system to meet the requirements.

1. Create the `os_config` script based on the following example.
   Users can modify the `os_config` script according to their actual situation.

```
#!/bin/bash
### BEGIN INIT INFO
# Provides:          os-config
# Required-Start:    $local_fs $network $named $remote_fs
# Required-Stop:
# Should-Stop:
# Default-Start:     2 3 4 5
# Default-Stop:      0 1 6
# Short-Description: config of os-init job
# Description: run the config phase without cloud-init
### END INIT INFO
####################user settings####################
cdrom_path=blkid  -L config-2
load_os_config() {
 mount_path=$(mktemp -d /mnt/tmp.XXXX)
 mount /dev/cdrom $mount_path
 if [[ -f $mount_path/qcloud_action/os.conf ]]; then
     . $mount_path/qcloud_action/os.conf
     if [[ -n $password ]]; then
         passwd_file=$(mktemp /mnt/pass.XXXX)
         passwd_line=$(grep password $mount_path/qcloud_action/os.conf)
         echo root:${passwd_line#*=} > $passwd_file
     fi
     return 0
 else
```

```
        return 1
    fi
}
cleanup() {
    umount /dev/cdrom
    if [[ -f $passwd_file ]]; then
        echo $passwd_file
        rm -f $passwd_file
    fi
    if [[ -d $mount_path ]]; then
        echo $mount_path
        rm -rf $mount_path
    fi
}
config_password() {
    if [[ -f $passwd_file ]]; then
        chpasswd -e < $passwd_file
    fi
}
config_hostname(){
    if [[ -n $hostname ]]; then
        sed -i "/^HOSTNAME=.*/d" /etc/sysconfig/network
        echo "HOSTNAME=$hostname" >> /etc/sysconfig/network
    fi
}
config_dns() {
    if [[ -n $dns_nameserver ]]; then
        dns_conf=/etc/resolv.conf
        sed -i '/^nameserver.*/d' $dns_conf
        for i in $dns_nameserver; do
            echo "nameserver $i" >> $dns_conf
        done
    fi
}
config_network() {
    /etc/init.d/network stop
    cat << EOF > /etc/sysconfig/network-scripts/ifcfg-eth0
DEVICE=eth0
IPADDR=$eth0_ip_addr
NETMASK=$eth0_netmask
HWADDR=$eth0_mac_addr
ONBOOT=yes
GATEWAY=$eth0_gateway
BOOTPROTO=static
EOF
    if [[ -n $hostname ]]; then
        sed -i "/^${eth0_ip_addr}.*/d" /etc/hosts
        echo "${eth0_ip_addr} $hostname" >> /etc/hosts
    fi
    /etc/init.d/network start
}
config_gateway() {
    sed -i "s/^GATEWAY=.*/GATEWAY=$eth0_gateway" /etc/sysconfig/network
}
####################init#######################
```

```
start() {
 if load_os_config ; then
     config_password
     config_hostname
     config_dns
     config_network
     cleanup
     exit 0
 else
     echo "mount ${cdrom_path} failed"
     exit 1
 fi
}
RETVAL=0
case "$1" in
 start)
     start
     RETVAL=$?
 ;;
 *)
     echo "Usage: $0 {start}"
     RETVAL=3
 ;;
esac
exit $RETVAL
```

2. Place the `os_config` script in the `/etc/init.d/` directory and run the following command.

```
chmod +x /etc/init.d/os_config
chkconfig --add os_config
```

3. Run the following command to check whether `os_config` has been added to the startup services.

```
chkconfig --list
```

> **Note**
> Users need to ensure the correct execution of the script. If issues such as inability to connect to the instance via SSH or lack of network connection are encountered after importing the image, try connecting to the instance through the console and re-executing the script to troubleshoot the problem. If the issue persists, please contact customer support.

Exporting an image

Last updated: 2024-09-24 11:34:41

Scenario

Tencent Cloud supports exporting custom images to Object Storage COS buckets, allowing you to export the required images.

Preparations

- You have already activated the Object Storage service in the COS console.
- A bucket has been created in the region where the custom image is located. For more information, see Creating a Bucket.

Supports and Limits

- Images with licensing restrictions cannot be exported, including Windows Server images, Tencent Cloud-authorized Red Hat Enterprise Linux images (those with built-in licenses can be exported), and custom images created from cloud marketplace images.
- For a custom image, the capacity of a system disk or data disk cannot be greater than 500 GB.
- When the image of an entire CVM instance is exported, the CVM instance cannot contain more than 5 data disks.

Billing Description

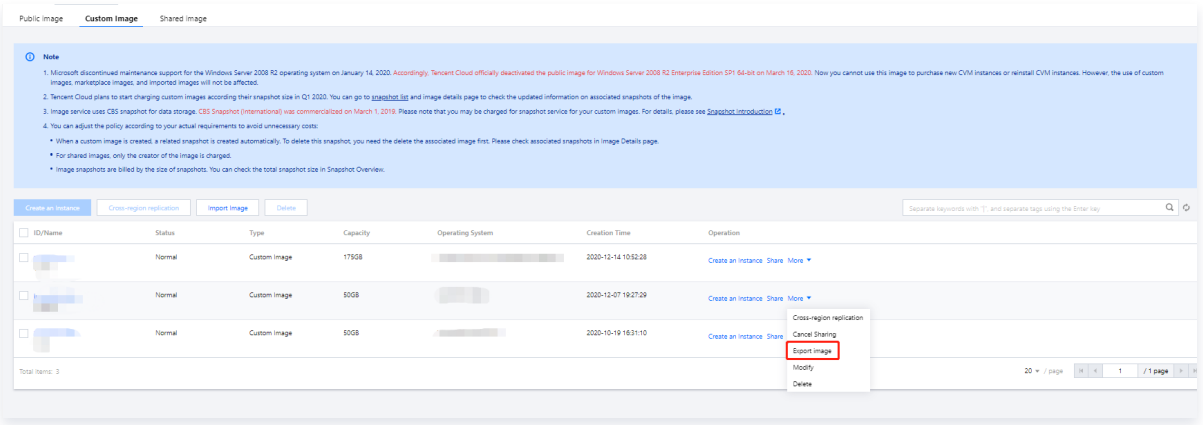
- If you use other services such as COS when using CVM, fees will be calculated according to the billing rules of the actually used services.
- The fees are as described below:

Scenes	Billing	Document
Exporting an image to a COS bucket	Storage usage fees. Storing an image in a COS bucket will incur storage usage fees. COS will calculate the object size and charge fees based on the storage type and region of the target object.	Storage Capacity Fees
	Request fees. Exporting an image to a COS bucket will incur write request fees. COS will calculate the number of write requests and charge fees accordingly.	Request Fees
	Traffic fees. Exporting an image to a COS bucket will generate outbound traffic. COS will calculate the traffic size, and both internal and external outbound traffic are free of charge.	Traffic Fees
Downloading an image from a COS bucket	Request fees. Downloading an image from a COS bucket will incur write request fees. COS will calculate the number of write requests and charge fees accordingly.	Request Fees
	Traffic fees. Downloading an image from a COS bucket will generate outbound traffic. COS will calculate the traffic size, with private network outbound traffic being free and public network outbound traffic being charged.	Traffic Fees

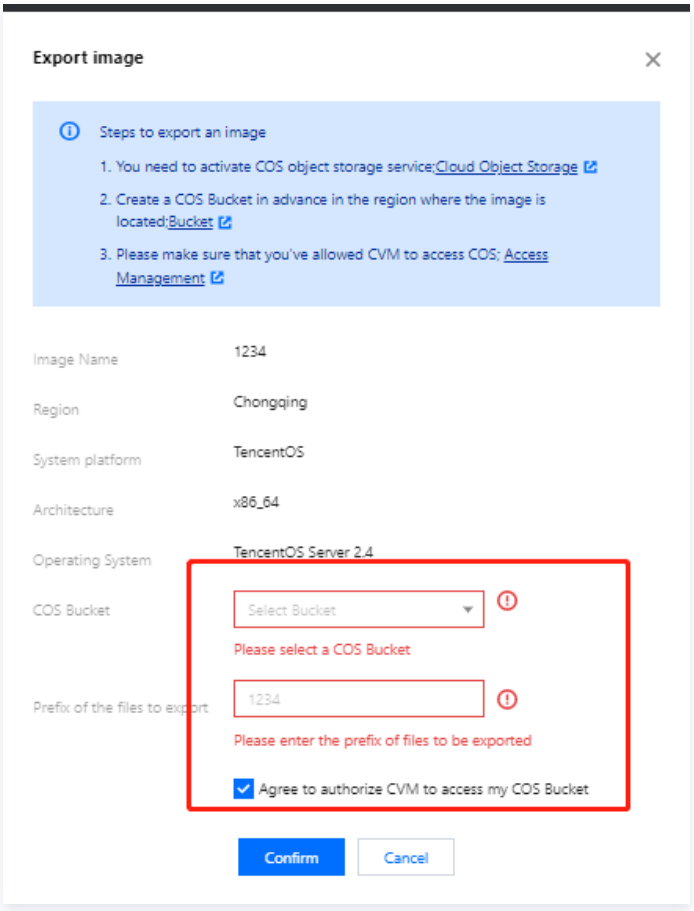
Instructions

1. Log in to the CVM console and select Image on the left sidebar.
2. At the top of the **Image** page, select the region where the custom image to be exported is located, and click the **Custom Image** tab.

3. Select **More** > **Export Image** on the right side of the image row, as shown in the figure below:



4. In the **Export Image** pop-up window, make the following settings, as shown in the figure below:



   - **COS Bucket**: Select the bucket where the image to be exported is located, which must be in the same region as the image.
   - **Export File Prefix**: Customize the export file prefix.
     Select "Agree to authorize CVM to access my COS Bucket".
5. Click **OK** to start the image export task.
6. Click **OK** in the confirmation pop-up window.
   The export time depends on the size of the image and the workload of the task queue. Please be patient. Once the export task is completed, the image file will be stored in the target bucket. You can go to the Bucket List page, click on the bucket ID to enter the details page, and the file named `custom_prefix_name_xvda.raw` is the exported image file.

FAQs

1. How is the public network downstream traffic generated in COS? How is it billed?

Public network downstream traffic refers to the data transmitted from COS to the client through the internet. Traffic generated by users directly downloading objects via **object links** or browsing objects through **static website origin** is considered public network downstream traffic, with corresponding fees as public network downstream traffic charges. For detailed information on public network downstream traffic billing, please refer to Billing Items and Product Pricing.

2. Will downloading files through the COS console, tools, API, or SDK incur public network downstream traffic fees?

The traffic generated by accessing COS (private network traffic or public network traffic) is not related to your usage method. Only when cloud products in the same region access COS, the private network is used by default and no public network outbound traffic fees are charged. To determine if you are accessing via a private network, please refer to the Private Network Access documentation.

3. How does COS differentiate public network traffic?

Public network downstream traffic refers to the data transferred from COS to the client over the internet. Examples include downloading files stored in COS through the COS console, accessing or downloading objects using tools, previewing objects in a browser, or accessing and downloading objects using object URLs or custom domain names. For more information, see the Determining Private Network Access document.

4. Will using private network access for Object Storage incur any fees?

When accessing Object Storage via the private network, **traffic fees are waived**, but **storage capacity** and **request count** will still incur related costs. For more information, see Billing Items.

CentOS Linux EOL Guidance
CentOS outage instructions and recommended solutions

Last updated: 2024-06-26 18:34:23

Background of CentOS End of Maintenance

CentOS plans to officially discontinue support for CentOS Linux, with details shown in the table below. For more information, see CentOS's official announcement.

OS Version	EOL	Impact
CentOS 8	January 1, 2022	After end of maintenance, any software maintenance and support including bug fixes and feature updates are unavailable.
CentOS 7	June 30, 2024	

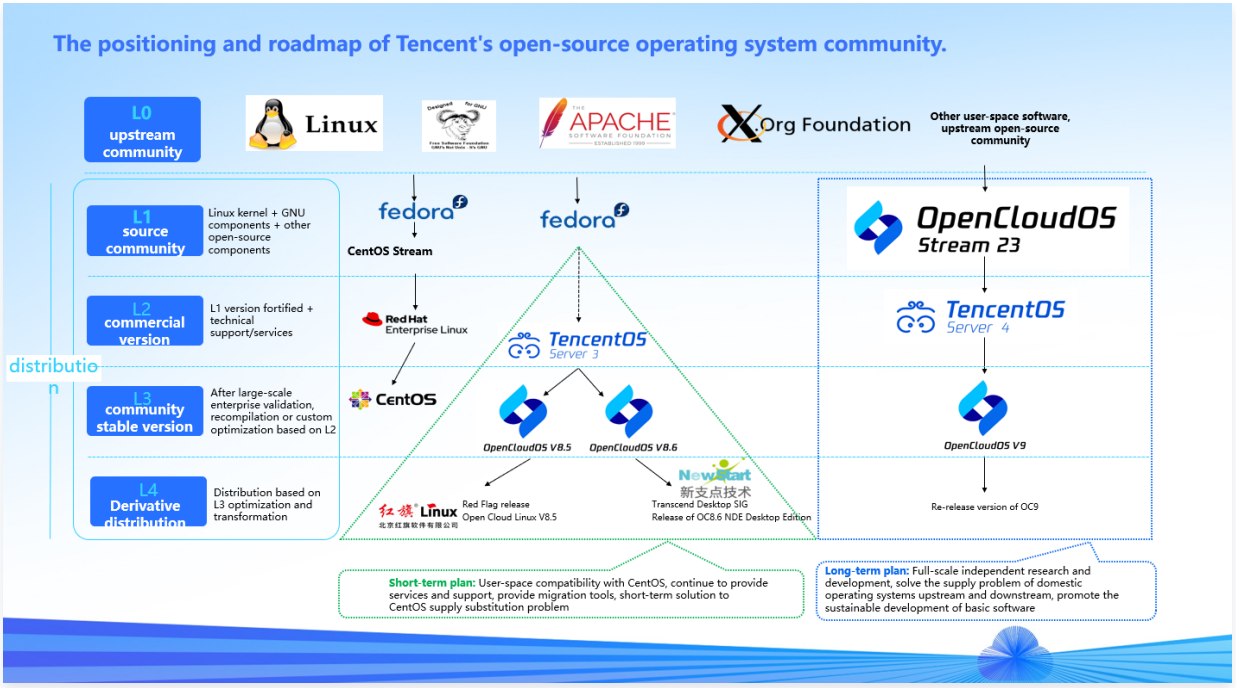
Choose the OpenCloudOS Community Stable Edition (free of charge) or TencentOS Server images for newly purchased CVMs

Introduction to OpenCloudOS and TencentOS Server

- Initiated by Tencent and its partners, **OpenCloudOS** is a standalone, fully open OS and ecosystem with security, stability, and high performance.
  - For more information about OpenCloudOS, see: OpenCloudOS Introduction.
- TencentOS Server is Tencent's Linux OS designed for cloud scenarios. With specific features and optimized performance, TencentOS Server provides a high-performance, secure, and reliable operating environment for applications in CVM instances.
  - For more information about TencentOS Server, see TencentOS Server Introduction.

Linux editions issued in the ecosystem supply chain are classified into four categories here:

- L1 Stream Edition, such as OpenCloudOS Stream and the well-known Fedora and Debian.
- L2 Commercial Edition, the majority of which are issued by commercial companies, such as TencentOS Server by Tencent, RHEL by Redhat, and Ubuntu by Canonical.
- L3 Community Stable Edition, usually a free reissue of a commercial system such as OpenCloudOS and the original CentOS. This edition has few differences from the L2 Commercial Edition.
- L4 Community Derived Edition, an optimized and customized edition based on L3.



OpenCloudOS falls under the L3 Community Stable Edition category and TencentOS Server the L2 Commercial Edition category. OpenCloudOS to TencentOS Server is what CentOS to RHEL.
OpenCloudOS is derived from the commercial stable edition of TencentOS Server and has basically the same source code. The main difference is that the commercial edition provides SLA guaranteed technical support.

	OpenCloudOS	TencentOS Server
Kernel version	Tencent Linux 5.4 kernel	Tencent Linux 5.4 kernel
User mode	Compatible with CentOS 8 (OpenCloudOS 8.X)	Compatible with CentOS 7 (TencentOS Server 2.4) and CentOS 8 (TencentOS Server 3.1)
Technical support	From the OpenCloudOS community	From TencentOS Server technical support
Flaw/vulnerability publish	In the community	By TencentOS Server technical support

OpenCloudOS is a community-based OS, available to you for free and maintained by developers in the community. If you need service and maintenance from a professional OS team, you can purchase the TencentOS Server subscription service.

Directions for CentOS migration

- For more information about migrating CentOS 8 instances to OpenCloudOS, see Migrating CentOS to OpenCloudOS.
- For more information about migrating CentOS 8 instances to TencentOS Server, see Migrating CentOS to TencentOS Server.

Migrating CentOS to TencentOS Server

Last updated: 2023-11-29 19:31:05

Scenario

CentOS plans to officially discontinue support for CentOS Linux, with details shown in the table below. For more information, see CentOS's official announcement.

OS Version	EOL	Impact
CentOS 8	January 1, 2022	After end of maintenance, any software maintenance and support including bug fixes and feature updates are unavailable.
CentOS 7	June 30, 2024	

If you need to purchase a new CVM instance, you are advised to use a TencentOS Server image. If you are using a CentOS instance, replace it with TencentOS Server by referring to the directions provided in this document.

Release notes

Supported OS versions for source servers:

- CentOS 7 series:
  - CentOS_7.2_64-bit, CentOS_7.3_64-bit, CentOS_7.4_64-bit, CentOS_7.5_64-bit, CentOS_7.6_64-bit, CentOS_7.7_64-bit, CentOS_7.8_64-bit, and CentOS_7.9_64-bit
- CentOS 8 series:
  - CentOS_8.0_64-bit, CentOS_8.2_64-bit, and CentOS_8.4_64-bit

Recommended OS Version for Target Host:

- If you are using CentOS 7 series, migrate it to TencentOS Server 2.4 (TK4).
- If you are using CentOS 8 series, migrate it to TencentOS Server 3.1 (TK4).

> **Note**
> CentOS 7.2 and CentOS 7.3 public images may contain packages for 32-bit systems by default. Delete these packages before update.

Supports and Limits

- OS migration is not supported in the following cases:
  - A GUI is installed.
  - An i686 RPM package is stalled.
- Business may fail to run properly after migration under the following conditions:
  - The business program is installed with and relies on a third-party RPM package.
  - Business applications depend on a specific kernel version or have custom-compiled kernel modules. The target version after migration is tkernel4, based on the 5.4 kernel. This version is newer than the kernels of CentOS 7 and CentOS 8, and some older features may change in the new version. It is recommended that users with strong kernel dependencies understand the features they rely on or consult Tencent Cloud Assistant for advice.
  - The business program relies on a fixed GCC version.
    Currently, TencentOS 2.4 is installed with GCC v4.8.5 by default, and TencentOS 3.1 is installed with GCC v8.5 by default.
- After migration, you need to restart the instance to enter the TencentOS kernel.
- Migration does not affect data disks. Upgrade only in the OS layer does not involve any operation on data disks.

Resource Requirements

- The memory has a free space of over 500 MB.
- The system disk has a free space of over 10 GB.

Instructions

Preparing for the migration

1. Migration is irreversible. To ensure business data security, you are advised to create a snapshot to back up system disk data.
2. Check whether an i686 RPM package is installed and, if so, uninstall the package.

Migration execution

Migrate CentOS 7 series to TencentOS Server 2.4 (TK4)

1. Log in to the target CVM instance. For operation details, see Logging in to Linux Instance Using Standard Login Method.
2. Run the following command to install Python 3:

```
yum install -y python3
```

3. Run the following command to obtain the migration tool:

```
wget
https://mirrors.cloud.tencent.com/tencentos/2.4/tlinux/x86_64/RPMS/migrate2tencentos-1.0-
4.tl2.noarch.rpm
```

4. Execute the following command to install the migration tool, which will create migrate2tencentos.py in the /usr/sbin directory.

```
rpm -ivh migrate2tencentos-1.0-4.tl2.noarch.rpm
```

5. Run the following command to start migration:

```
python3 /usr/sbin/migrate2tencentos.py -v 2.4
```

The migration takes some time. When the script execution is completed, the following information is displayed:

```
Metadata Cache Created
Switch complete. TencentOS recommends rebooting this system.
[root@VM-2-43-centos ~]#
```

6. Restart the instance, for more information, see Restart Instance.
7. Check the migration result.

7.1 Run the following command to check the OS release information:

```
cat /etc/os-release
```

The information shown in the figure below is displayed:

```
[root@VM-2-43-centos ~]# cat /etc/os-release
NAME="TencentOS Server"
VERSION="2.4"
ID="tencentos"
ID_LIKE="rhel fedora centos tlinux"
VERSION_ID="2.4"
PRETTY_NAME="TencentOS Server 2.4"
ANSI_COLOR="0;31"
CPE_NAME="cpe:/o:tencentos:tencentos:2"
HOME_URL="https://cloud.tencent.com/product/ts"
```

7.2 Run the following command to check the kernel:

```
uname -r
```

The information shown in the figure below is displayed:

```
[root@VM-2-43-centos ~]# uname -r
5.4.119-19-0009.1
[root@VM-2-43-centos ~]#
```

Note
By default, the kernel is the latest version of YUM.

7.3 Run the following command to check YUM:

```
yum makecache
```

The information shown in the figure below is displayed:

```
[root@VM-2-43-centos ~]# yum makecache
Loaded plugins: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
 * epel: mirrors.tencentyun.com
 * tlinux: mirrors.tencentyun.com
 * tlinux-extras: mirrors.tencentyun.com
 * tlinux-os: mirrors.tencentyun.com
 * tlinux-updates: mirrors.tencentyun.com
epel
tlinux
tlinux-extras
tlinux-os
tlinux-tkernel4
tlinux-updates
Metadata Cache Created
[root@VM-2-43-centos ~]#
```

Migrate CentOS 8 series to TencentOS 3.1 (TK4)

1. Log in to the target CVM instance. For operation details, see Logging in to Linux Instance Using Standard Login Method.
2. Run the following command to install Python 3:

```
yum install -y python3
```

3. Run the following command to obtain the migration tool:

```
wget https://mirrors.cloud.tencent.com/tlinux/3.1/Updates/x86_64/RPMS/migrate2tencentos-1.0-4.tl3.noarch.rpm
```

4. Execute the following command to install the migration tool, which will create migrate2tencentos.py in the /usr/sbin directory.

```
rpm -ivh migrate2tencentos-1.0-4.tl3.noarch.rpm
```

5. Run the following command to start migration:

```
python3 /usr/sbin/migrate2tencentos.py -v 3.1
```

The migration takes some time. When the script execution is completed, the following information is displayed:

```
Metadata cache created.
Switch complete. TencentOS recommends rebooting this system.
[root@VM-2-2-centos ~]#
```

6. Restart the instance, for more information, see Restart Instance.
7. Check the migration result.

7.1 Run the following command to check the OS release information:

```
cat /etc/os-release
```

The information shown in the figure below is displayed:

```
[root@VM-2-2-centos ~]# cat /etc/os-release
NAME="TencentOS Server"
VERSION="3.1 (Final)"
ID="tencentos"
ID_LIKE="rhel fedora centos"
VERSION_ID="3.1"
PLATFORM_ID="platform:el8"
PRETTY_NAME="TencentOS Server 3.1 (Final)"
ANSI_COLOR="0;31"
CPE_NAME="cpe:/o:tencentos:tencentos:3"
HOME_URL="https://cloud.tencent.com/product/ts"
```

7.2 Run the following command to check the kernel:

```
uname -r
```

The information shown in the figure below is displayed:

```
[root@VM-2-2-centos ~]# uname -r
5.4.119-19-0009.1
[root@VM-2-2-centos ~]#
```

> **Note**
> By default, the kernel is the latest version of YUM.

7.3 Run the following command to check YUM:

```
yum makecache
```

The information shown in the figure below is displayed:

```
[root@VM-2-2-centos ~]# yum makecache
TencentOS Server 3.1 - TencentOS
TencentOS Server 3.1 - Updates
TencentOS Server 3.1 - TencentOS-AppStream
TencentOS Server 3.1 - Base
TencentOS Server 3.1 - AppStream
TencentOS Server 3.1 - Extras
TencentOS Server 3.1 - PowerTools
Extra Packages for TencentOS Server 3.1 - x86_64
Extra Packages for TencentOS Server 3.1 Modular - x86_64
Metadata cache created.
[root@VM-2-2-centos ~]#
```

If you encounter any issues during the migration process, please contact Tencent Cloud Assistant.

Migrating to OpenCloudOS

Last updated: 2023-09-07 17:33:31

Scenario

CentOS has officially discontinued support for CentOS 8. For more information, see CentOS's official announcement.

OS Version	EOL	Impact
CentOS 8	January 1, 2022	After end of maintenance, any software maintenance and support including bug fixes and feature updates are unavailable.

If you are using a CentOS 8 instance, migrate CentOS 8 to OpenCloudOS 8 by referring to the directions provided in this document.

Release notes

OS versions supported for source servers

Name	Version
CentOS 8 series	CentOS_8.0_64-bit, CentOS_8.2_64-bit, CentOS_8.3_64-bit, CentOS_8.4_64-bit, and CentOS_8.2_ARM_64-bit

OS versions recommended for target servers

- If you are using CentOS 8 series, migrate it to OpenCloudOS 8.
- OS migration is not supported for CentOS Stream 8 public images.

Supports and Limits

- OS migration is not supported in the following cases:
  - A GUI is installed.
  - An i686 RPM package is stalled.
- Business may fail to run properly after migration under the following conditions:
  - The business program is installed with and relies on a third-party RPM package.
  - The business program relies on a fixed kernel version or has its own kernel module compiled. The target version after migration is tkernel4 (TK4) based on the v5.4 kernel. This version is later than the kernel versions of CentOS 8 and may have changes in some old features. If your business program relies heavily on the kernel, we recommend that you know which features your business program actually relies on. You can also visit the OpenCloudOS community Bugtracker.
  - The business program relies on a fixed GCC version. Currently, OpenCloudOS 8 is installed with GCC v8.5 by default.
- After migration, you need to restart the instance to enter the OpenCloudOS kernel.
- Migration does not affect data disks. Upgrade only in the OS layer does not involve any operation on data disks.

Resource Requirements

- The memory has a free space of over 500 MB.
- The system disk has a free space of over 10 GB.

Instructions

Preparing for the migration

1. Create a snapshot to backup the system disk.
2. Check whether an i686 RPM package is installed and, if so, uninstall the package.
3. Install Python 3 in your operating environment if you have not installed it. You can install Python 3 using a CentOS Vault repository.

```
# cat <<EOF | sudo tee /tmp/centos8_vault.repo
[c8_vault_baseos]
name=c8_vault - BaseOS
baseurl=https://mirrors.cloud.tencent.com/centos-vault/8.5.2111/BaseOS/\$basearch/os/
gpgcheck=0
enabled=1
[c8_vault_appstream]
name=c8_vault - AppStream
baseurl=https://mirrors.cloud.tencent.com/centos-vault/8.5.2111/AppStream/\$basearch/os/
gpgcheck=0
enabled=1
EOF
# yum -y install python3 --disablerepo=* -c /tmp/centos8_vault.repo --enablerepo=c8_vault*
```

Migration execution

Steps to migrate from CentOS 8 to OpenCloudOS 8

1. Log in to the target host. For Tencent Cloud CVM users, please refer to Logging in to Linux Instance Using Standard Login Method.
2. Run the following command to install Python 3: If no YUM repository is available, install Python 3 using a CentOS Vault repository. For more information, see item 3 in the **Preparation** section.

```
yum install -y python3
```

3. Run one of the following commands based on your Python version to download the migration tool:

```
#x86 version
wget
https://mirrors.opencloudos.tech/opencloudos/8.6/AppStream/x86_64/os/Packages/migrate2openclo
udos-1.0-1.oc8.noarch.rpm
#ARM version
wget
https://mirrors.opencloudos.tech/opencloudos/8/AppStream/aarch64/os/Packages/migrate2openclou
dos-1.0-1.oc8.noarch.rpm
```

4. Run the following command to install the migration tool. The command will create the `migrate2opencloudos.py` file in `/usr/sbin`.

```
rpm -ivh migrate2opencloudos-1.0-1.oc8.noarch.rpm
```

5. Run the following command to start migration:

```
python3 /usr/sbin/migrate2opencloudos.py -v 8
```

The migration takes some time. When the script execution is completed, the following information is displayed:

```
Metadata cache created.
Switch complete. OpenCloudOS recommends rebooting this system.
[root@VM-64-6-centos ~]#
```

6. Restart the instance. For more information about cloud server instances, see Restarting Instances.
7. Check the migration result.
   - Run the following command to check the OS release information:

     ```
     cat /etc/os-release
     ```

     The information shown in the figure below is displayed:

     ```
     [root@VM-64-27-centos ~]# cat /etc/os-release
     NAME="OpenCloudOS"
     VERSION="8.6"
     ID="opencloudos"
     ID_LIKE="rhel fedora"
     VERSION_ID="8.6"
     PLATFORM_ID="platform:oc8"
     PRETTY_NAME="OpenCloudOS 8.6"
     ANSI_COLOR="0;31"
     CPE_NAME="cpe:/o:opencloudos:opencloudos:8"
     HOME_URL="https://www.opencloudos.org/"
     BUG_REPORT_URL="https://bugs.opencloudos.tech/"
     ```

   - Run the following command to check the kernel:

     ```
     uname -r
     ```

     The information shown in the figure below is displayed:

     ```
     [root@VM-64-27-centos ~]# uname -r
     5.4.119-19.0010.ocrelease.7
     ```

     By default, the kernel is the latest version of YUM.
   - Run the following command to check YUM:

     ```
     yum makecache
     ```

     The information shown in the figure below is displayed:

     ```
     [root@VM-64-6-centos ~]# yum makecache
     OpenCloudOS 8 - Base
     OpenCloudOS 8 - AppStream
     OpenCloudOS 8 - Extras
     OpenCloudOS 8 - HighAvailability
     OpenCloudOS 8 - PowerTools
     OpenCloudOS 8 - ResilientStorage
     Extra Packages for OpenCloudOS 8 - x86_64
     Extra Packages for OpenCloudOS 8 Modular - x86_64
     Metadata cache created.
     [root@VM-64-6-centos ~]#
     ```

Migrating CVM Instances Online Migration Overview

Last updated: 2023-09-07 17:34:34

Online migration is a method of server migration that allows you to synchronize the systems and service programs on a server or virtual machine from a self-built IDC or cloud platform to Tencent Cloud without system downtime.

Online migration utilizes Tencent Cloud's proprietary migration tool, go2tencentcloud. Once executed on the source host, the entire host can be migrated to the target cloud server on Tencent Cloud. This migration tool eliminates the need for tedious preparation tasks such as creating, uploading, and importing images, and supports direct migration from the source to the cloud, facilitating business requirements such as enterprise cloud adoption, cross-cloud platform migration, cross-account regional migration, and hybrid cloud deployment.

> **Note**
> The source servers mentioned in the document can be physical servers, virtual machines, or cloud servers from other cloud platforms. Other cloud platforms include, but are not limited to, AWS, Google Cloud Platform, VMware, Alibaba Cloud, and Huawei Cloud virtual machine platforms.

Scenarios

Online migration is applicable to the following scenarios (including but not limited to):

- Migrating self-built IDC to the cloud
- Cross-cloud vendor migration

  Supports migration of lightweight application servers to Cloud Virtual Machines (CVM)
- Local virtual machines to the cloud
- Hybrid cloud architecture deployment
- Cross-account, cross-region/availability zone migration

Differences from offline migration

Offline migration requires creating an image of the source server's system disk or data disk and then migrating the image to your specified cloud server or cloud disk. In contrast, online migration does not require creating an image; simply run the migration tool on the source server to migrate it to the specified Tencent Cloud CVM.

Starting the Migration

Online migration offers two migration methods. You can choose the appropriate migration method based on your business scenario:

Migration method	Overview	Scenarios	Advantage
Online Migration: Importing Migration Source from Client	Log in to the source instance, run the tool to register the migration source, create a migration task in the console, and complete the migration.	• Public network migration & private network migration • Cross-cloud migration: Suitable for various source environments. • IDC to Cloud Migration	High Compatibility

Online Migration: One-click Migration via Console	Verify access identity on the console to easily import the migration source and create a migration task with a single click.	• No need to log in to the source server • Migration over public network • Cross-cloud migration: Suitable for source instances on Alibaba Cloud.	One-click batch migration

FAQs Overview

For more information, please see Server Migration Details.

Operation Guide on Migration
Online Migration Directions

Last updated: 2024-09-24 10:37:14

Online migration enables you to synchronize and migrate systems and service programs on a server or virtual machine from a self-built IDC or cloud platform to Tencent Cloud without system downtime.
Online migration offers two migration methods. You can choose the appropriate method based on your business scenario and refer to the corresponding documentation for detailed operation guidance.

Migration method	Overview	Scenarios	Advantage
Online Migration: Importing Migration Source from Client	Log in to the source instance, run the tool to register the migration source, create a migration task in the console, and complete the migration.	• Public network migration & private network migration • Cross-cloud migration: Suitable for various source environments. • IDC to Cloud Migration	High Compatibility
Online Migration: One-click Migration via Console	Verify access identity on the console to easily import the migration source and create a migration task with a single click.	• Migration over public network • Cross-cloud migration: Suitable for source instances on Alibaba Cloud.	One-click batch migration console operation

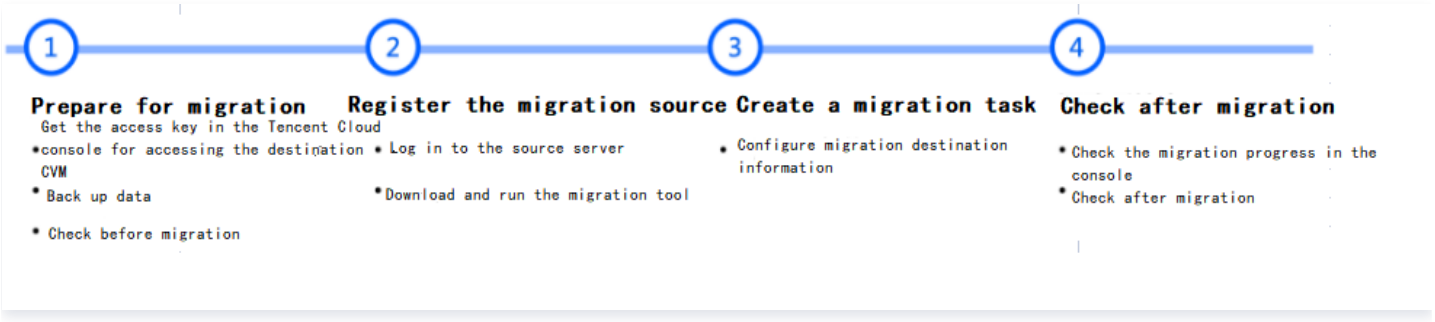
Migrating with a Migration Tool

Last updated: 2023-09-27 15:39:07

This document describes how to migrate your source server to Tencent Cloud CVM online by using the client.

Migration Workflow

The following figure shows the process of online migration by importing the migration source from the client:



Migration Directions

Step 1. Prepare for migration

- Go to Manage API Key to create a key and obtain the `SecretId` and `SecretKey`.
- We recommend that you suspend applications on the server and back up your data to resist possible impact on existing applications during the migration.
  - Source server: You can use the snapshot feature or other methods to back up data on the source server. The source server is the server to be migrated.
  - Destination CVM: Create a snapshot of the instance (See Creating Snapshots)
- If you are using a sub-account, ask the root account to assign you the `QcloudCSMFullAccess` and `QcloudCVMFullAccess` permissions in the CAM console.
- Before migration, check the following items according to your actual situation:
  - If the migration destination is a CVM instance, you need to check the source server and destination CVM.
  - If the migration destination is a CVM image, you need to check only the source server.

Linux source server	1. Check and install Virtio. For more information, see Checking Virtio Drivers on Linux. 2. Run the `which rsync` command to check whether rsync has been installed. If not, install it. For more information, see How do I install Rsync. 3. Check whether SELinux is enabled. If yes, refer to How to Disable SELinux for instructions on disabling it. 4. Ensure the current system time is correct, because the Tencent Cloud API will use the UNIX timestamp to check the generated token after receiving a migration request.
Windows source server	1. Check and install Virtio. For more information, see Checking Virtio Drivers on Windows. 2. (Optional) Check and install Cloudbase-Init. For more information, see Installing Cloudbase-Init on Windows. You can install it on the source server before the migration, or install it on the destination instance after the migration. ○ If you install it before the migration, network configuration and activation are performed automatically after the migration. ○ If you do not install it before the migration, you need to Log into Windows Instance via VNC, and manually modify the network configuration.

	3. We recommend that you pause your anti-virus program to prevent the migration tool from being mistakenly killed, which results in migration failure.
Destination CVM	1. Storage space: the cloud disks of the destination CVM (including system and data disks) should have sufficient capacity to save data migrated from the source server. 2. Security group: Port 80, port 443 and port 3389 are opened. 3. Bandwidth: Set the bandwidth cap on both the two ends to the highest possible value. During the process, the traffic consumed is approximately the amount of data migrated. Adjust the billing mode beforehand if necessary. 4. Network: If the source or destination server supports only IPv6 but not IPv4, see Parameters in the client.json file.

Note

- Check the source server by executing `sudo ./go2tencentcloud_x64 --check`.
- By default, go2tencentcloud automatically performs checks upon launch. To skip checks, open the `client.json` file, set `Client.Extra.IgnoreCheck` to `true`.

Step 2. Register the migration source

Register source server

Linux server

1. On the source server to be migrated, execute the following command to download the migration tool go2tencentcloud.zip and navigate to the corresponding directory.

```
wget https://go2tencentcloud-1251783334.cos.ap-guangzhou.myqcloud.com/latest/go2tencentcloud.zip
```

```
unzip go2tencentcloud.zip
```

```
cd go2tencentcloud/go2tencentcloud-linux
```

Note
The files in the `go2tencentcloud` directory will not be migrated. Do not place the files to be migrated in this directory.

2. (Optional) Exclude files or directories that do not need to be migrated on the source server.
Add files and directories that don't need to be migrate to the rsync_excludes_linux.txt file.
3. Register the source

3.1 i. For example, on a 64-bit Linux source server, execute the following command in sequence as the root user to run the tool.

```
chmod +x go2tencentcloud_x64
```

```
sudo ./go2tencentcloud_x64
```

3.2 Enter the `SecretId` and `SecretKey` of the account API access key obtained in Prerequisites and press **Enter**, as shown below:

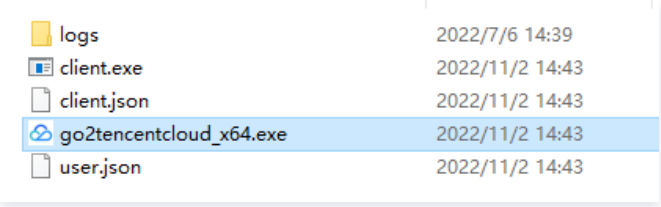
```
[root@VM-0-28-centos go2tencentcloud]# ./go2tencentcloud_x64
[2021-11-29 10:47:25] Start go2tencentcloud 2.2.3
[2021-11-29 10:47:25] Start loading data...
Please Enter SecretId:
Please Enter SecretKey: ********************************
```

If the following message appears, the source server information is registered. You can now check the source server in the CVM console.

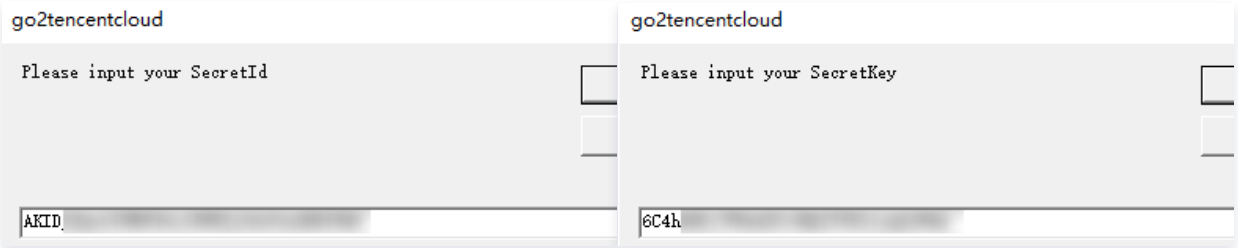
```
[2021-11-29 10:47:54] Load user.json successfully.
[2021-11-29 10:47:54] Load client.json successfully.
[2021-11-29 10:47:54] Calculating the size of file system, please wait...
[2021-11-29 10:47:55] Check environment...
[2021-11-29 10:47:59] Check environment successfully.
[2021-11-29 10:47:59] Start import source server...
[2021-11-29 10:47:59] Import source server [server-03tw3wlr] successfully.
```

Windows Server

1. Download and upload `go2tencentcloud.zip` to the source server. Decompress the file to the `go2tencentcloud` folder. Extract `go2tencentcloud-windows.zip` and decompress it.



2. Run `go2tencentcloud_x64.exe`
   - Method 1: Right-click `go2tencentcloud_x64.exe` and run it as admin. Enter `SecretId` and `SecretKey` in the pop-up window.
   - Method 2: Start cmd or PowerShell command line as admin: cd /d **absolute path of the directory of go2tencentcloud_x64.exe**, and run `go2tencentcloud_x64.exe` .
3. Enter Tencent Cloud API key (`SecretId` and `SecretKey`) in the pop-up window.



4. If the following message appears, the source server information is registered. You can now check the source server in the CVM console.

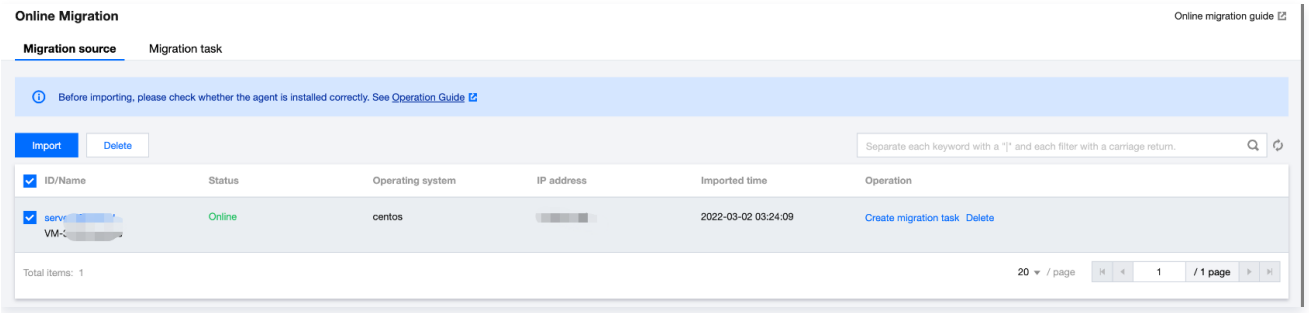
```
[2022-11-02 14:47:20] Start go2tencentcloud 2.2.3
f the input window does not pop up, there may be a problem with your operating system.
ry manually modifying the SecretId and SecretKey fields in user.json[2022-11-02 14:47:34] Load user.json successfully.
[2022-11-02 14:47:34] Load client.json successfully.
[2022-11-02 14:47:34] Calculating the size of file system, please wait...
[2022-11-02 14:47:34] Check environment successfully.
[2022-11-02 14:47:35] Start import source server...
[2022-11-02 14:47:35] Import source server [server-[redacted]] successfully.
[2022-11-02 14:47:35] Start check migrate job status...
aiting for a migrate job to be created in the console, Used: 00:00:03
```

Note

If "Import source server successfully" does not appear, check the logs in the `logs/log` file under the migration tool directory for troubleshooting.

Check the registered server in the console

Log in to the CVM console and view the imported server. Its status should be **Online**, as shown below:



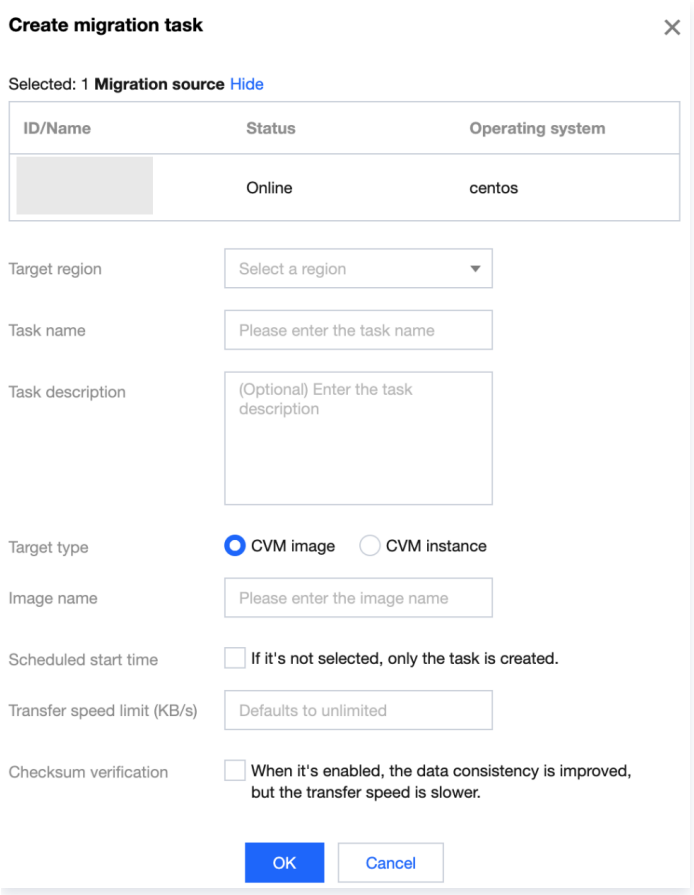
Note

Importing the source server is the first step of migration. Keep the migration tool alive till the whole migration progress ends. Otherwise, the migration task fails after the migration source becomes offline.

Step 3. Create a migration task

1. Create a migration task

Log in to the CVM console, go to the online migration page, and click **Create Migration Task** on the right of the desired migration source. In the **Create Migration Task** pop-up window, configure the task as instructed, as shown below:



Configuration description:

- Basics:

Configuration Item	Required	Note
Destination Region	Supported	Tencent Cloud region to which the source server is to be migrated. For more information about supported regions, see Regions and Availability Zones.
Task Name	Supported	Name of the migration task.
Task Description	Not required	Migration task description.
Destination Type	Supported	Set the destination type for the source server to be migrated to Tencent Cloud. • **CVM image**: A destination CVM image will be generated for the migration source after the migration task ends. Image name: Name of the destination CVM image that will be generated for the migration source. If the name already exists, the migration task ID is appended to the name. • **CVM instance**: Select a CVM instance in the destination region as the migration destination. Destination Instance: We recommend you use the same operating system for the source server and destination CVM instance. For example, to migrate a CentOS 7 source server, select a CentOS 7 CVM as the destination.
Network mode	Supported	The network used for transferring data.

		• **Public Network Transfer**: Public network transfer is used when migrating data to the destination CVM or transit instance. • **Private Network Transfer**: Use private network transfer when migrating data to the target CVM or intermediate instance. For more information, see Private Network Migration Guide. VPC: When migrating to a CVM image, the intermediate instance will be created in this VPC. Subnet: When migrating to a CVM image, the intermediate instance will be created in this subnet.
Migration method	Supported	For Linux instances: • **Linux File-level Migration**: Migration granularity at the file level, offering high compatibility and relatively lower transfer efficiency. • **Linux block-level migration**: The migration granularity is at the disk logical storage unit **block** level, offering high transfer efficiency and relatively lower compatibility.
		Windows block-level migration: The migration granularity is at the disk logical storage unit **block** level, which is the default for Windows migration, offering high compatibility and transfer efficiency.
Configure incremental sync	Not required	You can customize the incremental sync duration to continuously sync the data. • **Disabled**: The migration tool scans for and migrate the increments. Generally, it is implemented for once. • **Enabled**: You can select the incremental sync duration. The migration tool will continuously sync the data to Tencent Cloud. You can also manually stop the incremental sync in the task list.
Scheduled execution time	Not required	The time when the migration task is automatically started after creation. It can be as early as 10 minutes after the current time.

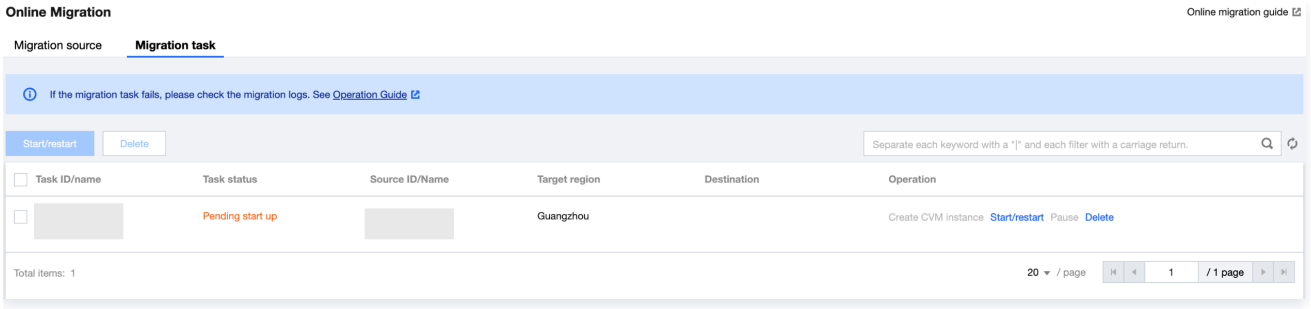
- Advanced (Optional):

Configuration Item	Required	Note
Transfer Restriction (KB/s)	Not required	The bandwidth for data transfer during the migration ranges from 0 to 25600 KB/s. The transfer rate is unlimited by default. This configuration item is not supported on Windows.
Checksum verification	Not required	After it is enabled, data consistency check will be enhanced, but the transfer speed may be reduced. This configuration item is not supported on Windows.

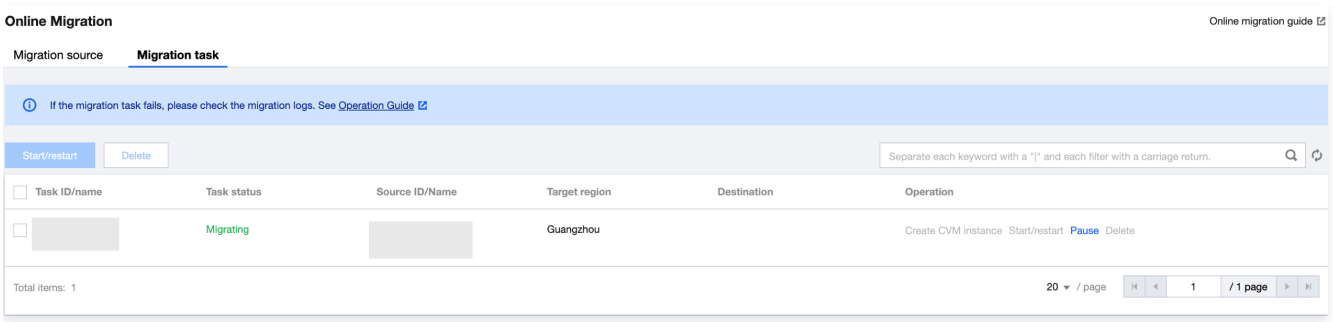
2. Start the migration task

> **Note**
> You can skip this step if your task is scheduled, which will automatically start running at the scheduled execution time.

After creating a migration task, you can click the **Migration Task** tab to view the task as shown below:



Click **Start/restart** on the right side of the task row, and click **OK** in the pop-up confirmation window to start the migration task. The task status will change to **Migrating**. As shown in the following figure:



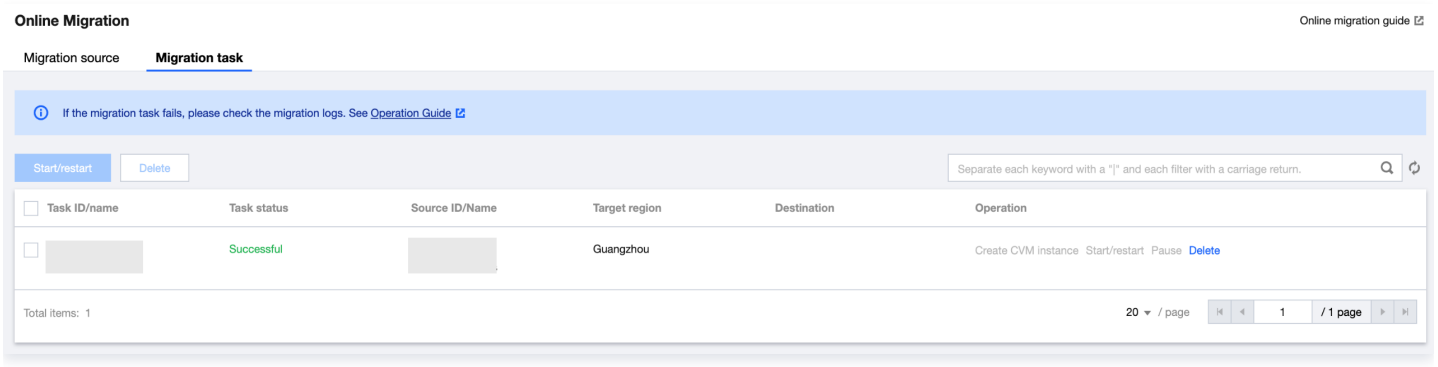
Note

- If the migration destination is a CVM, the destination CVM enters migration mode after the migration starts. Do not reinstall the system, shut down, terminate, or reset passwords of the destination CVM until the migration ends and the destination CVM exits the migration mode.
- If the migration destination is a CVM image, a relay instance named `do_not_delete_csm_instance` will be created under your account after the migration starts. Do not reinstall, shut down, or terminate the relay instance or reset its password. It will be automatically terminated by the system after the migration ends. The instance incurs instance fees and cloud disk fees. For more information about the fees, see Billing.

Step 4. Check after migration

1. View the migration progress in the console

After the migration task status becomes **Successful**, the migration is completed, as shown below:



Note

- The time required for data transfer depends on the size of the data on the source server, network bandwidth, etc. Please wait for the migration process to complete.
- After the migration task starts, you can click **Pause** on the row of the task to stop it.

- The migration tool supports checkpoint restart. After a task is paused, you can click **Start/Retry** again to resume migration from where you paused.
- A migration task can be paused during data transfer. After you click **Pause** for it in the console, the migration tool will pause the data transfer in progress.
- If the migration process is time-consuming and you need to stop it, you can pause the migration task first and click **Delete** to delete it.

2. Check after migration

- **Failed migration:**
  Check the error information in log files (under the migration tool directory by default), operation guides, or FAQs about Service Migration for troubleshooting methods. After troubleshooting, click **Start/Retry** in the Actions column to restart the migration task.
- **Successful migration:**
  Migrating to a CVM: The destination CVM starts up normally. Data on the CVM is consistent with that on the source server. The network and other system services are normal.
  Migrating to a CVM image: Click the **CVM image ID** on the row of the migration task to go to the CVM image page and view the image information. You can use this image to create CVM instances.

If you have any questions or the migration has an exception, see FAQs about Service Migration or contact us.

Migrating via the Console

Last updated: 2023-10-11 14:50:28

This document explains how to perform a one-click online migration of your source server to Tencent Cloud CVM using the console.

Scenario

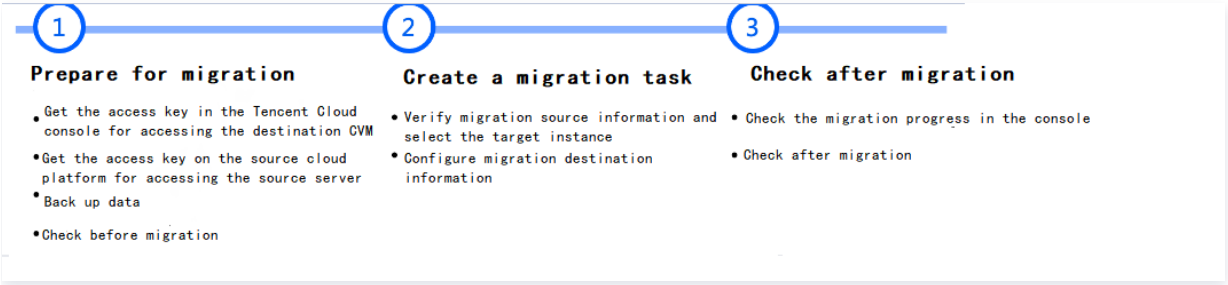
One-click migration is an agile solution under the Online Migration Overview, eliminating the need for complex operations such as logging into the source server and downloading tools. It allows for the creation of batch migration tasks with a single click, synchronizing the source operating system and service programs to Tencent Cloud. One-click migration is applicable to both Linux and Windows operating systems, and also supports querying migration progress through the Online Migration page on the Tencent Cloud server console.

Usage Limits

- The console's one-click migration has certain requirements for the source server environment. The source server needs to have the corresponding cloud assistant installed (e.g., Alibaba Cloud ECS Cloud Assistant), be configured with a public IP, and use VPC networking (classic networking is not supported).
- Currently, the console's one-click migration supports migrating Alibaba Cloud servers to Tencent Cloud, while other platforms are not yet supported.
- The console's one-click migration feature is currently being iteratively optimized and only supports a limited number of scenarios. If it does not meet your requirements, we recommend using Online Migration: Client Import Migration Source, which offers greater compatibility.

Migration Workflow

The process of performing online migration using the console's one-click migration is illustrated in the following diagram:



Migration Directions

Step 1. Prepare for migration

- **Obtain Access Keys in Tencent Cloud Console**
  Create and obtain **SecretId and SecretKey** in the API Key Management page of Tencent Cloud Access Management Console. For detailed operations, please refer to the Access Keys documentation.

> **Note**
> If you are using a sub-account for console migration, you need to log in to the Access Management Console as the root account and grant the sub-account QcloudCSMFullAccess and QcloudCVMFullAccess permissions.

- **Obtain Access Keys on the Source Cloud Platform**
  Follow these steps to obtain the Alibaba Cloud AccessKeyID and AccessKeySecret:
  1.1 Log in to the Alibaba Cloud RAM console and go to the **Identity Management** > User page.
  1.2 Click **Create User**, select **Open API Access Method (other access methods will not take effect)** for the access method, and confirm the creation. Please save the AccessKeyID and AccessKeySecret information promptly.
  1.3 In the user list, add permissions to the newly created user **Add Permissions**, granting read-only access to Elastic Compute Service (ECS) (AliyunECSReadOnlyAccess) and management of ECS Cloud Assistant service (AliyunECSAssistantFullAccess).
- **Pause applications and perform data backup (optional)**
  We recommend that you suspend applications on the server and back up your data to resist possible impact on existing applications during the migration.
  - Source server: You can use the snapshot feature or other methods to back up data on the source server. The source server is the server to be migrated.
  - Source Host: When migrating a Windows system, it is recommended to temporarily disable antivirus software to avoid mistakenly blocking the migration tool and causing migration failure.
  - Destination CVM: Create a snapshot of the instance (See Creating Snapshots)
- **Destination CVM Check**
  If the migration target is a CVM, check the destination CVM.

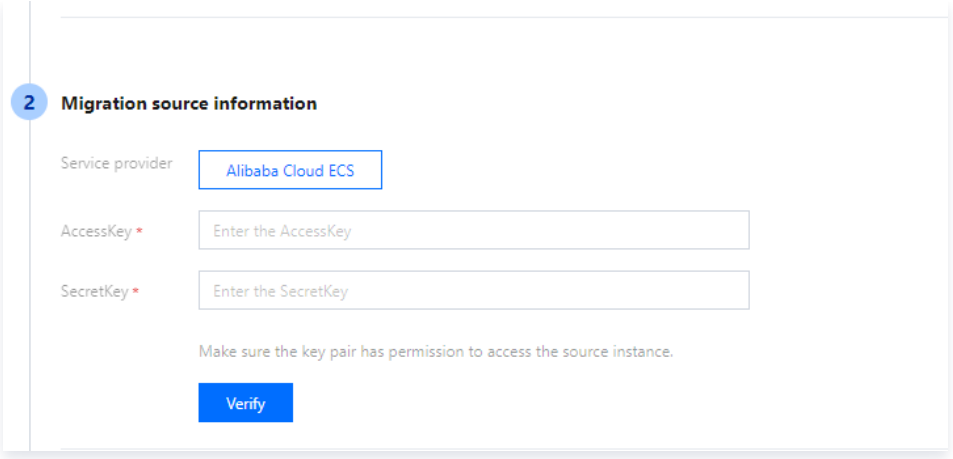
Destination CVM	1. Storage space: the cloud disks of the destination CVM (including system and data disks) should have sufficient capacity to save data migrated from the source server. 2. Security group: Port 80, port 443 and port 3389 are opened. 3. Bandwidth: Set the bandwidth cap on both the two ends to the highest possible value. During the process, the traffic consumed is approximately the amount of data migrated. Adjust the billing mode beforehand if necessary. 4. Network: If the source or destination server supports only IPv6 but not IPv4, see Parameters in the client.json file.

- **Access the One-Click Migration Page in the Console**
  1.1 Log in to the CVM console, go to **Server Migration** > Online Migration page. Click **Import Migration Source** to enter the Import Migration Source page.
  1.2 Select the **Console One-Click Migration** option to start creating migration tasks in bulk.

Step 2. Create a migration task

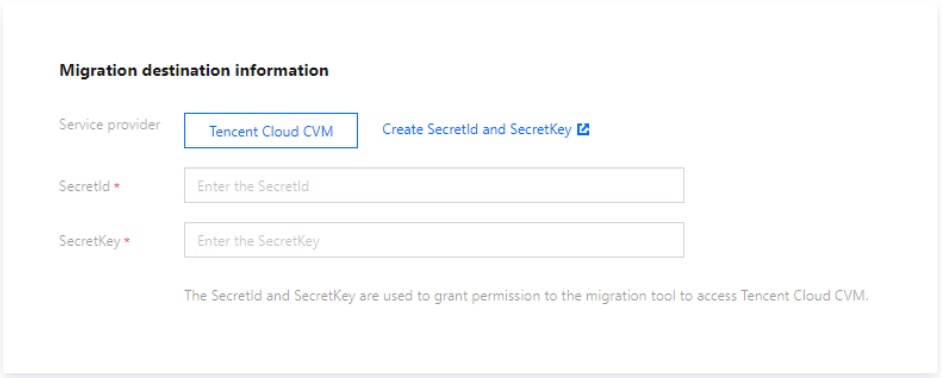
1. **Configure Task**
   Enter the task name and task description.
2. **Configure Source Migration Information**
   The current source service provider is set to Alibaba Cloud ECS by default. You need to enter the AccessKey and SecretKey of your Alibaba Cloud account (How to obtain) and verify to **ensure access to the source server information**, as shown in the figure:

> ⚠ **Note**
> Keep your access key confidential. We recommend you delete or disable the access key after the migration.



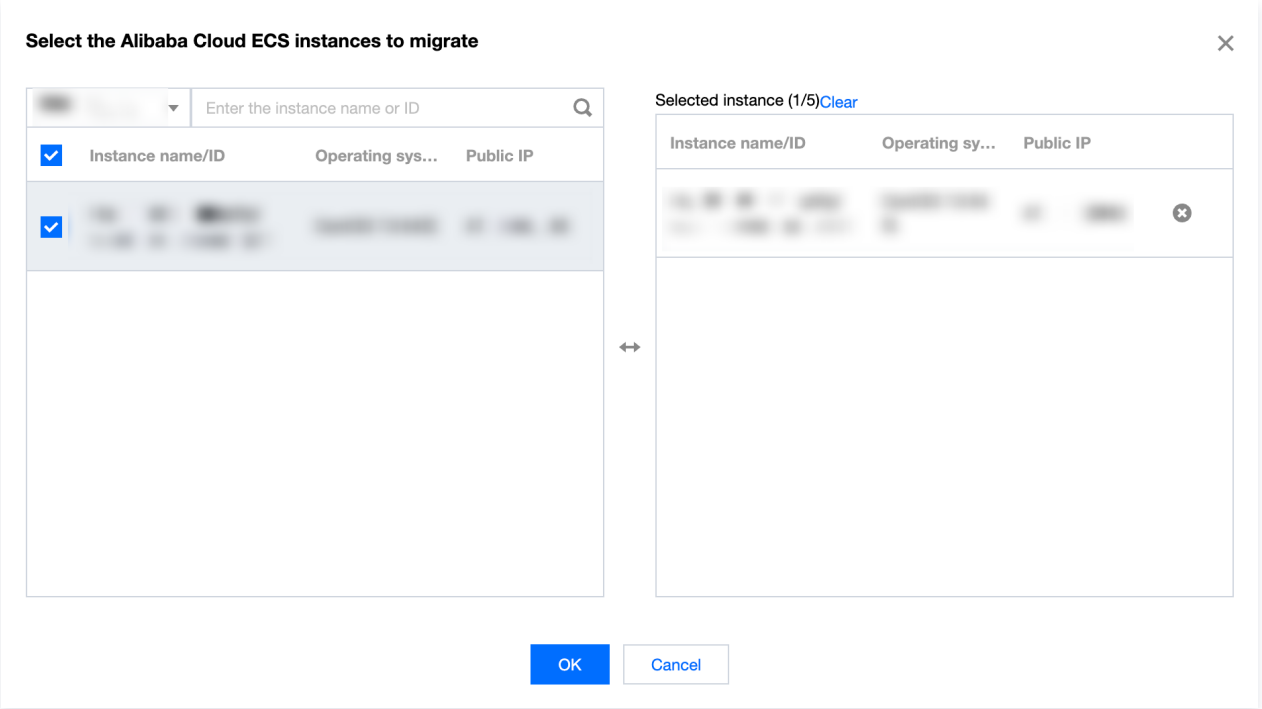
3. **Configure Migration Target**
   The current source service provider has been set to Tencent Cloud CVM by default. You need to enter the Tencent Cloud API key's SecretId and SecretKey (How to Obtain)**to obtain the necessary permissions for Tencent Cloud CVM**. You can directly copy the key information from the API Key Management page. Please verify that the API key is correct, as incorrect keys may result in migration failure.

> **Note**
> Keep your access key confidential. We recommend you delete or disable the access key after the migration.

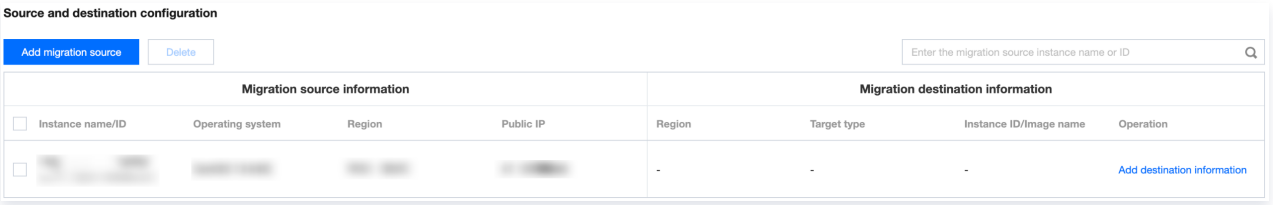


4. **Configure Migration Information**
   4.1 After the migration source information is successfully verified, you can click **Add Migration Source** to enter the pop-up window and select the instances to be migrated.
   4.2 After selecting the corresponding region in the top left corner of the pop-up window, you can obtain the **Instance List** for that **region**. The number following the region name indicates the number of instances, making it convenient to choose the appropriate region.
   4.3 Select the instances you want to migrate to add them to the **Selected instance** list on the right.

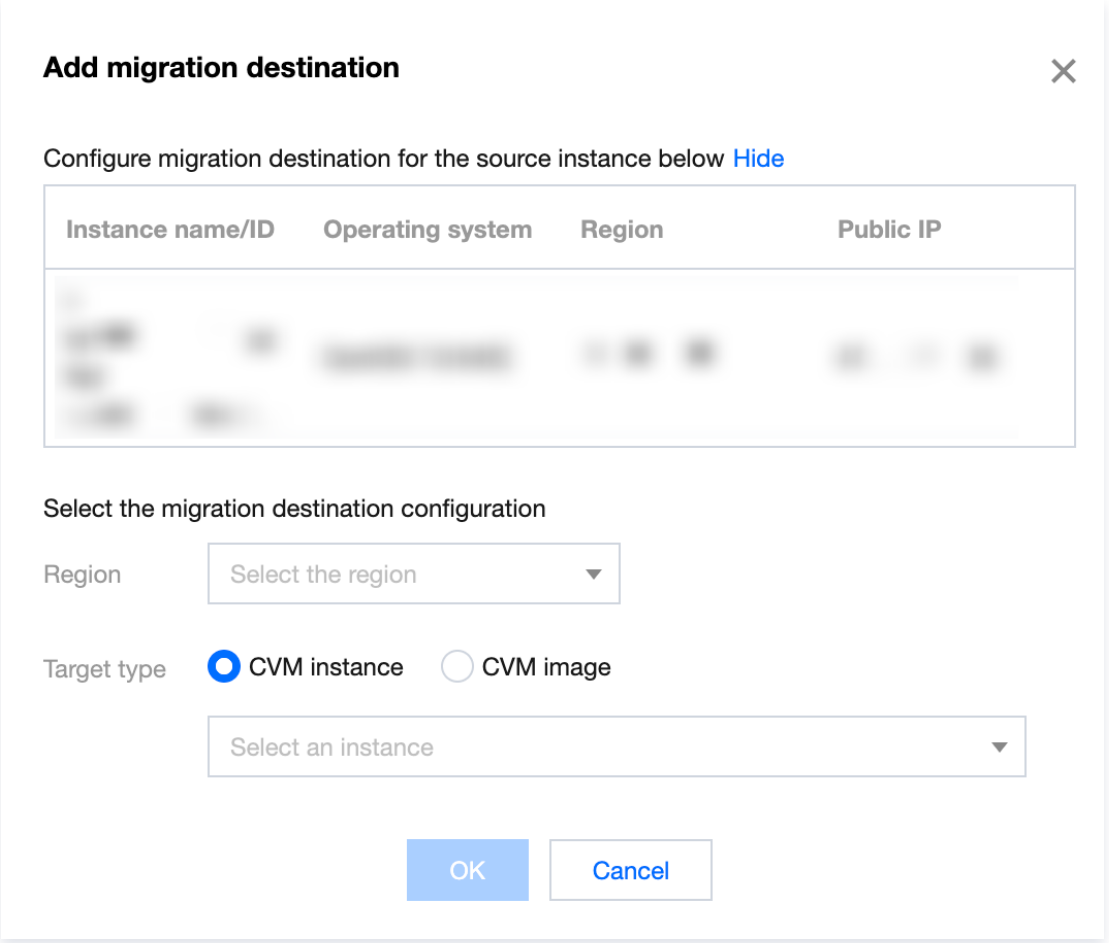
> **Note**
> - Supports **multi-instance, multi-region** batch migration, allowing you to add multiple migration sources multiple times.
> - Currently, you can batch migrate up to five instances.



4.4 After clicking **OK**, the instance information to be migrated will be displayed in the Migration Source Information list. You can click **Add deetination Information** in the operation column to configure the migration target information.



4.5 In the **Add Migration deetination** pop-up window, configure the region and migration target type:



Configuration Item	Required	Note
Destination Region	Supported	The destination Tencent Cloud region for the source server migration. For information on regions, please refer to Regions and Availability Zones.
Destination Type	Supported	Set the destination type for the source server to be migrated to Tencent Cloud. CVM image: Create a CVM image for the source server Image name: Name of the destination CVM image that will be generated for the migration source. If the name already exists, the migration task ID is appended to the name. CVM Instance: Select a CVM instance in the target region as the migration destination. Target Instance: It is recommended that the target CVM's operating system is as close as possible to the source server's operating system type. For example, when migrating a CentOS 7 system source server, choose a CentOS 7 CVM as the migration target. Additionally, the target CVM's system disk and data disk capacities should both be larger than the source server's.

5. **Click to create and start a migration task, and you will see a friendly reminder. Please pay attention:**
   - You need to wait a minute before the progress can be viewed in the console, as it takes some time to execute the task on the migration source.
   - If the source environment is abnormal or the information is incorrect, preventing the import of the migration source, the Tencent Cloud console may not display the failure reason. Please recreate the task or switch to Online Migration.

Step 3. Check after migration

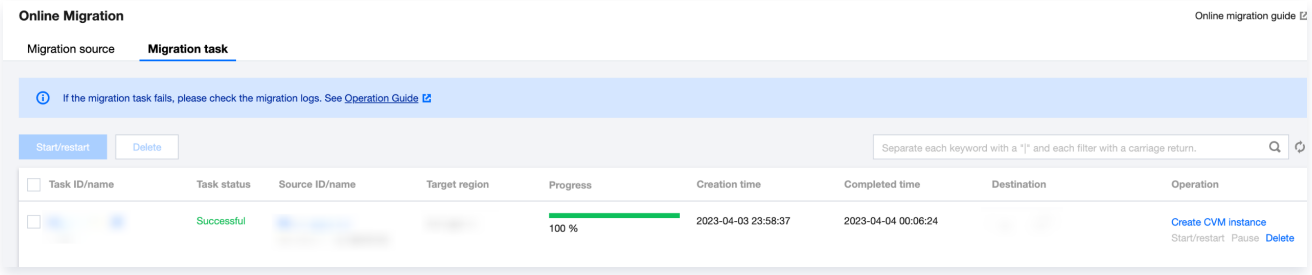
1. **View Migration Status and Progress**
   After confirming the new task, the migration task will be executed automatically. You can query the migration source

information and view the task progress on the Migration Source Page.

Note

- If the migration destination is a CVM, the destination CVM enters migration mode after the migration starts. Do not reinstall the system, shut down, terminate, or reset passwords of the destination CVM until the migration ends and the destination CVM exits the migration mode.
- When the migration target is a CVM image, a relay instance named "do_not_delete_csm_instance" will be created under your account after the migration starts. Please do not perform operations such as reinstalling the system, shutting down, destroying, or resetting the password on the relay instance until the migration is complete. The system will automatically destroy the relay instance created for this migration. The relay instance will incur certain costs, including instance fees and cloud disk fees. For detailed fee information, please refer to Billing Instructions.

2. **Wait for the migration task to complete**
   When the migration task status is **Successful**, it indicates that the migration has been successfully completed. As shown in the following figure:



Note

- The time required for data transfer depends on the size of the data on the source server, network bandwidth, etc. Please wait for the migration process to complete.
- After the migration task starts, you can click **Pause** on the row of the task to stop it.
- The migration tool supports checkpoint restart. After a task is paused, you can click **Start/Retry** again to resume migration from where you paused.
- A migration task can be paused during data transfer. After you click **Pause** for it in the console, the migration tool will pause the data transfer in progress.
- If the migration process is time-consuming and you need to stop it, you can pause the migration task first and click **Delete** to delete it.

3. **Checking After Migration**
   - **Failed migration:**
     Check the error information in log files (under the migration tool directory by default), operation guides, or FAQs about Service Migration for troubleshooting methods. After troubleshooting, click **Start/Retry** in the Actions column to restart the migration task.
   - **Successful migration:**
     - Migrating to a CVM: The destination CVM starts up normally. Data on the CVM is consistent with that on the source server. The network and other system services are normal.
     - If the migration target is a CVM image, click the "CVM Image ID" in the migration task row to access the CVM Image Page and view the image information. You can use this image to create a cloud server.

If you have any questions or encounter migration issues, please refer to Common Questions about Server Migration or contact us for assistance.

Diverse Migration Scenario Tutorials
Migrating Linux Instances Using Tools

Last updated: 2023-09-07 17:37:51

This document introduces how to use the migration tool "go2tencentcloud" to migrate the Linux-based CVM online.

Considerations

- You already have a Tencent Cloud account and a destination CVM.
- Stop applications on the source server to prevent existing applications from being affected by the migration.
- Download the migration tool compressed package.
- Create and obtain the SecretId and `SecretKey` in the `API Key Management` page.
- Verify that the source server and destination CVM meet the migration requirements. For example, the cloud disk of the destination CVM must have sufficient storage space to accommodate the data from the source server.
- Before migration, it is recommended to back up your data using the following methods:
  - Source server: you can use the source server's snapshot feature or other methods to back up data.
  - Destination CVM: Create a snapshot of the instance (See Creating Snapshots)

Migration Toolkit

Files in the Compressed Package

After extracting `go2tencentcloud.zip`, the file descriptions are as follows:

File Name	Note
go2tencentcloud-linux.zip	Linux system migration compressed package.
readme.txt	Directory Overview File.
release_notes.txt	Migration Tool Changelog

After decompressing `go2tencentcloud-linux.zip`, the file descriptions are as follows:

File Name	Note
go2tencentcloud_x64	Migration tool executable for 64-bit Linux systems.
go2tencentcloud_x32	Migration tool executable for 32-bit Linux systems.
user.json	User information during migration.
client.json	Migration tool configuration file.
rsync_excludes_linux.txt	Configure rsync to exclude unnecessary file directories in the Linux system from migration.

> **Note**
> The configuration files cannot be deleted. You must store them under the same folder as the go2tencentcloud executable program.

User.json File Parameter Description

The user.json configuration file is described as below:

Parameter name	Local Disk Types	Required	Note
SecretId	String	Supported	Account API access key SecretId, for more information, please refer to Access Key.
SecretKey	String	Supported	Account API access key SecretKey, for more information, please refer to Access Key.
Region	String	Supported	Specify the region of the destination CVM, without specifying the availability zone. Refer to the Region list for valid values.
InstanceId	String	Supported	The instance ID of the destination CVM, in the format of ins-xxxxxxxx.
DataDisks	Array	Not required	List of data disks to be migrated from the source server. Each element indicates a data disk. Up to 20 data disks are supported.
DataDisks.Index	Integer	Not required	The serial number of data disk ranges from 1 to 20. If the value is 1, it indicates that the data disk is the first one to be migrated and attached to the destination CVM; if the value is2, it indicates that the data disk is the second one to be migrated and attached to the destination CVM, and so on.
DataDisks.Size	Integer	Not required	Size of the source data disk in GB. The value range is [10,16000].
DataDisks.MountPoint	String	Not required	Source data disk mount point, such as "/mnt/disk1".

You can refer to the following examples to modify the configuration file based on the actual business scenarios.

- Example 1: Migrate a Linux source host to a CVM in the Tencent Cloud Guangzhou region, with the `user.json` file configured as follows:

```
{
 "SecretId": "your secretId",
 "SecretKey": "your secretKey",
 "Region": "ap-guangzhou",
 "InstanceId": "your instance id"
}
```

- Example 2: Migrate a Linux source host (including a data disk with a mount point of `/mnt/disk1` and a size of `10GB`) to a Tencent Cloud CVM in the Guangzhou region (with at least one data disk attached). The `user.json` file is configured as follows:

```
{
 "SecretId": "your secretId",
 "SecretKey": "your secretKey",
 "Region": "ap-guangzhou",
 "InstanceId": "your instance id",
 "DataDisks": [
     {
         "Index": 1,
         "Size": 10,
         "MountPoint": "/mnt/disk1"
     }
 ]
```

```
}
```

- Example 3: Migrate a Linux source server with two data disks (Disk 1 mounted at `/mnt/disk1`, size `10GB`, to be migrated to the first data disk of the destination CVM; Disk 2 mounted at `/mnt/disk2`, size `20GB`, to be migrated to the second data disk of the destination CVM) to a Tencent Cloud CVM in the Guangzhou region (with at least two data disks attached). The `user.json` file is configured as follows:

```
{
 "SecretId": "your secretId",
 "SecretKey": "your secretKey",
 "Region": "ap-guangzhou",
 "InstanceId": "your instance id",
 "DataDisks": [
     {
         "Index": 1,
         "Size": 10,
         "MountPoint": "/mnt/disk1"
     },
     {
         "Index": 2,
         "Size": 20,
         "MountPoint": "/mnt/disk2"
     }
 ]
}
```

Client.json File Parameter Description

The client.json configuration file is described as below:

Parameter name	Local Disk Types	Required	Note
Client.ToolMode	bool	Not required	The migration tool mode flag parameter has a default value of false. To use the tool mode for migration, change it to true or add the --no-console parameter when running the tool.
Client.Net.Mode	Integer	Supported	Migration mode parameter: By default, public network transmission is used, with a value of 0. The value range is: 0 (Public Network Migration Mode), 1 (Private Network Migration Mode: Scenario 1), 2 (Private Network Migration Mode: Scenario 2), 3 (Private Network Migration Mode: Scenario 3).
Client.Extra.IgnoreCheck	Bool	Not required	The default value is false. By default, the migration tool automatically checks the source server environment when the tool starts running. To skip the check, set this parameter to true.
Client.Rsync.BandwidthLimit	String	Not required	Bandwidth limit in KBytes/s, which is empty by default, i.e., no limit during transfer.
Client.Rsync.Checksum	Bool	Not required	Enable transfer verification by setting it to true, which enhances transfer consistency checks but increases the source host's CPU load

			and slows down the transfer speed. The default value is false, meaning no verification is performed by default.

If either the source server or the destination CVM cannot directly access the public network, you can establish a connection channel through VPC Peering, VPN Connection, Cloud Connect Network, or Dedicated Line Access before proceeding with the private network migration. Determine the appropriate migration mode based on the network environment of your source server and destination CVM.

Description of rsync_excludes_linux.txt File

Exclude files or configuration files in specified directories that do not need to be migrated from the Linux source host. The following directories and files are excluded by default, **please do not modify or delete.**

```
/dev/*
/sys/*
/proc/*
/var/cache/yum/*
/lost+found/*
/var/lib/lxcfs/*
/var/lib/docker-storage.btrfs/root/.local/share/gvfs-metadata/*
```

To exclude other directories and files, append the content at the end of the file. For example, exclude all content of the data disk mounted at `/mnt/disk1`.

```
/dev/*
/sys/*
/proc/*
/var/cache/yum/*
/lost+found/*
/var/lib/lxcfs/*
/var/lib/docker-storage.btrfs/root/.local/share/gvfs-metadata/*
/mnt/disk1/*
```

Parameters of the Migration Tool

Parameter	Note
`--help`	Prints help information.
`--no-console`	Only migrates via tool (not migration in console).
`--check`	Checks the source server
`--log-file`	Configures the log file name, which is log by default.
`--log-level`	Configures the logging level. Valid values: 1(ERROR level), 2 (INFO level) and 3(DEBUG level). Default value: 2.
`--clean`	Force the destination CVM to exit migration mode and clean up the environment. For example, if the console prompts "Please execute '--clean' option manually.", use this option to make the destination CVM exit migration mode.
`--version`	Prints the version number.

Migration Directions

Backing up Data

- Source server: you can use the source server's snapshot feature or other methods to back up data.
- Destination CVM: you can create a snapshot or use other methods to back up data.

Checking before Migrating

Before the migration, check the following items of the source server and destination CVM:

Destination CVM	1. Storage space: the cloud disks of the destination CVM (including system and data disks) should have sufficient capacity to save data migrated from the source server. 2. Security group: port 443 and port 80 cannot be restricted in the security group. 3. Bandwidth: Set the bandwidth cap on both the two ends to the highest possible value. During the process, the traffic consumed is approximately the amount of data migrated. Adjust the billing mode beforehand if necessary. 4. Ensure the OS types of the destination CVM and source server are consistent: Inconsistencies in the OS types may cause discrepancies between the image information and the actual OS. It is recommended to choose a destination CVM with the same OS type as the source server. For example, when migrating a CentOS 7 source server, select a CVM with CentOS 7 as the migration target.
Linux source server	1. Check and install Virtio. For more information, see Checking Virtio Drivers in Linux. 2. Execute the `which rsync` command to check whether rsync is installed. If not, please refer to How to Install Rsync for installation. 3. Check whether SELinux is enabled. If yes, follow the instructions in How to Disable SELinux to disable it. 4. After initiating a migration request to the Tencent Cloud API, the API will use the current UNIX time to check the generated token. Ensure that the system time is accurate.

Note

- To automatically check the source server, use the command `./go2tencentcloud_x64 --no-console --check`.
- By default, the go2tencentcloud migration tool automatically checks before running. To skip the check and force migration, set the `Client.Extra.IgnoreCheck` field in the client.json file to `true`.

Starting the Migration

If you use go2tencentcloud supporting checkpoint restart provided by Tencent Cloud for migration, the migration process includes the following three stages. You can intuitively view the migration progress when the tool is running.

- **Stage 1**: The destination CVM enters migration mode, preparing for migration.
- **Phase 2**: The destination CVM is in migration mode, transferring data.
- **Stage 3**: The destination CVM exits migration mode, and the migration is complete.

Each stage generates subtasks to perform related operations, and some time-consuming subtasks have default maximum timeout durations. As data transfer time is affected by factors such as source data size and network bandwidth, please be patient and wait for the migration process to complete.

Note

The destination CVM enters migration mode after the migration starts. Do not reinstall the system, shut down, terminate, or reset passwords of the destination CVM until the migration is completed and the destination CVM exits the migration mode.

Migration over public network

1. Download or upload `go2tencentcloud.zip` to the source server and run the following command to enter the corresponding directory.
   1.1 Run the following commands in sequence to decompress `go2tencentcloud.zip` and enter the directory.

```
unzip go2tencentcloud.zip
```

```
cd go2tencentcloud
```

   1.2 ii. Run the following commands in sequence to decompress `go2tencentcloud-linux.zip` and enter the directory.

```
unzip go2tencentcloud-linux.zip
```

```
cd go2tencentcloud-linux
```

> **Note**
> The files in the `go2tencentcloud` directory will not be migrated. Do not place the files to be migrated in this directory.

2. Configure the destination CVM in the `user.json` file.
   Please set the required and necessary values according to the user.json file parameter description.
3. Configure the migration mode and other settings in the `client.json` file.
   Set the `Client.ToolMode` value in the `client.json` file to `true`, indicating tool mode migration. Additionally, if you need to configure other settings, follow the client.json file parameter description.
4. (Optional) Exclude files or directories on the source server that do not need to be migrated.
   If there are files or directories on the Linux source server that do not need to be migrated, add them to the rsync_excludes_linux.txt file.
5. Run the tool.
   For example, on a 64-bit Linux source server, execute the following command as the root user to run the tool.

```
sudo ./go2tencentcloud_x64
```

> **Note**
> If you have not modified `Client.ToolMode` in client.json to `true`, you need to add the parameter `--no-console` when running the tool, as follows:
>
> ```
> sudo ./go2tencentcloud_x64 --no-console
> ```

After running the tool, please wait patiently for the migration process to complete. Generally, in public network migration mode, the console output for a successful migration is as shown below:

```
[root@VM_32_44_centos go2tencentcloud]# sudo ./go2tencentcloud_x64
[2019-09-23 10:49:56] Start go2tencentcloud 1.3.0
[2019-09-23 10:49:56] Load user.json successfully.
[2019-09-23 10:49:56] Load client.json successfully.
[2019-09-23 10:49:57] [1/3] Initialize instance
[2019-09-23 10:49:57] Restart remote instance...
Used: 00:01:24 | Max Timeout: 00:10:00
[2019-09-23 10:51:22] Restart remote instance successfully.
[2019-09-23 10:51:22] Start preparing remote server...
[2019-09-23 10:51:22] Prepare remote server successfully.
[2019-09-23 10:51:22] Start initializing remote server...
Used: 00:00:13 | Max Timeout: 00:03:00
[2019-09-23 10:51:36] Initialize remote server successfully.
[2019-09-23 10:51:36] [2/3] Synchronize files
[2019-09-23 10:51:36] Transmitting files...
[################################################################################] 100% | 00:03:42
[2019-09-23 10:55:18] Transmit files successfully.
[2019-09-23 10:55:18] Reconfigure remote instance...
Used: 00:00:06 | Max Timeout: 00:05:00
[2019-09-23 10:55:25] Reconfigure remote instance successfully.
[2019-09-23 10:55:25] [3/3] Release instance
[2019-09-23 10:55:25] Clean temporary data successfully.
[2019-09-23 10:55:25] Migrate successfully.
```

Private Network Migration Scenario 1

1. Establish a connection between the source server and the destination CVM.
   Create a connection channel between the source server and the destination CVM using methods such as VPC Peering Connection, VPN Connection, or Cloud Connect Network.
2. Download or upload `go2tencentcloud.zip` to the source server and run the following command to enter the corresponding directory.
   2.1 Run the following commands in sequence to decompress `go2tencentcloud.zip` and enter the directory.

   ```
   unzip go2tencentcloud.zip
   ```

   ```
   cd go2tencentcloud
   ```

   2.2 ii. Run the following commands in sequence to decompress `go2tencentcloud-linux.zip` and enter the directory.

   ```
   unzip go2tencentcloud-linux.zip
   ```

   ```
   cd go2tencentcloud-linux
   ```

   > **Note**
   > The files in the `go2tencentcloud` directory will not be migrated. Do not place the files to be migrated in this directory.

3. Configure the destination CVM in the `user.json` file.
   Please set the required and necessary values according to the user.json file parameter description.

4. Configure the migration mode and other settings in the `client.json` file.
   - Set the `Client.ToolMode` value in the `client.json` file to `true`, indicating the tool mode migration.
   - Set the `Client.Net.Mode` item in the `client.json` file to `1`, which corresponds to the private network migration mode: scenario 1. Additionally, if you need to configure other settings, follow the client.json file parameter description.
5. (Optional) Exclude files or directories on the source server that do not need to be migrated.
   If there are files or directories on the Linux source server that do not need to be migrated, add them to the rsync_excludes_linux.txt file.
6. Run the tool on a server (such as the gateway) that can access the public network.
   For example, on a server that can access the public network, execute the following command to run the tool for migration stage 1.

```
sudo ./go2tencentcloud_x64
```

> **Note**
> If you have not modified `Client.ToolMode` in client.json to `true`, you need to add the parameter `--no-console` when running the tool, as follows:
>
> ```
> sudo ./go2tencentcloud_x64 --no-console
> ```

If `Stage 1 is finished and please run next stage at source machine.` is prompted, stage 1 has been completed. As shown below:

```
[root@VM_0_12_centos go2tencentcloud]# sudo ./go2tencentcloud_x64
[2019-09-23 11:19:27] Start go2tencentcloud 1.3.0
[2019-09-23 11:19:27] Load user.json successfully.
[2019-09-23 11:19:27] Load client.json successfully.
[2019-09-23 11:19:28] [1/3] Initialize instance
[2019-09-23 11:19:29] Restart remote instance...
Used: 00:01:23 | Max Timeout: 00:10:00
[2019-09-23 11:20:53] Restart remote instance successfully.
[2019-09-23 11:20:53] Start preparing remote server...
[2019-09-23 11:20:53] Prepare remote server successfully.
[2019-09-23 11:20:53] Start initializing remote server...
Used: 00:00:11 | Max Timeout: 00:03:00
[2019-09-23 11:21:05] Initialize remote server successfully.
[2019-09-23 11:21:05] Stage 1 is finished and please run next stage at source machine.
```

7. Run the tool on the source server to be migrated.
   After completing Step 6 (i.e., Stage 1), copy the entire tool directory from Stage 1 to the source server to be migrated, and then run the tool for Stage 2 migration.
   For example, execute the following command to run the tool for Stage 2 migration.

```
sudo ./go2tencentcloud_x64
```

> **Note**
> If you have not modified `Client.ToolMode` in client.json to `true`, you need to add the parameter `--no-console` when running the tool, as follows:

```
sudo ./go2tencentcloud_x64 --no-console
```

If `Stage 2 is finished and please run next stage at gateway machine.` is prompted, stage 2 has been completed. As shown below:

```
[root@VM_0_7_centos go2tencentcloud]# sudo ./go2tencentcloud_x64
[2019-09-23 11:23:27] Start go2tencentcloud 1.3.0
[2019-09-23 11:23:27] Load user.json successfully.
[2019-09-23 11:23:27] Load client.json successfully.
[2019-09-23 11:23:28] [2/3] Synchronize files
[2019-09-23 11:23:28] Transmitting files...
[##################################################################################] 100% | 00:02:15
[2019-09-23 11:25:42] Transmit files successfully.
[2019-09-23 11:25:42] Reconfigure remote instance...
Used: 00:00:09 | Max Timeout: 00:05:00
[2019-09-23 11:25:52] Reconfigure remote instance successfully.
[2019-09-23 11:25:52] Stage 2 is finished and please run next stage at gateway machine.
```

8. Run the tool on a host (such as a gateway) that has access to the public network. After completing Step 7 (i.e., Stage 2), copy the entire tool directory from Stage 2 to the host used in Stage 1, and then run the tool for Stage 3 migration. For example, execute the following command to run the tool for Stage 3 migration.

```
sudo ./go2tencentcloud_x64
```

> **Note**
> If you have not modified `Client.ToolMode` in client.json to `true`, you need to add the parameter `--no-console` when running the tool, as follows:
>
> ```
> sudo ./go2tencentcloud_x64 --no-console
> ```

If `Migrate successfully.` is prompted, the entire migration task has been completed, as shown below:

```
[root@VM_0_12_centos go2tencentcloud]# sudo ./go2tencentcloud_x64
[2019-09-23 11:30:08] Start go2tencentcloud 1.3.0
[2019-09-23 11:30:08] Load user.json successfully.
[2019-09-23 11:30:08] Load client.json successfully.
[2019-09-23 11:30:11] [3/3] Release instance
[2019-09-23 11:30:11] Clean temporary data successfully.
[2019-09-23 11:30:11] Stage 3 is finished.
[2019-09-23 11:30:11] Migrate successfully.
```

Private Network Migration Scenario 2

1. Establish a connection between the source server and the destination CVM.
   Create a connection channel between the source server and the destination CVM using methods such as VPC Peering Connection, VPN Connection, or Cloud Connect Network.
2. Download or upload `go2tencentcloud.zip` to the source server and run the following command to enter the corresponding directory.
   2.1 Run the following commands in sequence to decompress `go2tencentcloud.zip` and enter the directory.

```
unzip go2tencentcloud.zip
```

```
cd go2tencentcloud
```

2.2 ii. Run the following commands in sequence to decompress `go2tencentcloud-linux.zip` and enter the directory.

```
unzip go2tencentcloud-linux.zip
```

```
cd go2tencentcloud-linux
```

> **Note**
> The files in the `go2tencentcloud` directory will not be migrated. Do not place the files to be migrated in this directory.

3. Configure the destination CVM in the `user.json` file.
   Please set the required and necessary values according to the user.json file parameter description.
4. Configure the migration mode and other settings in the `client.json` file.
   - Set the `Client.ToolMode` value in the `client.json` file to `true`, indicating the tool mode migration.
   - Set the `Client.Net.Mode` item in the `client.json` file to `2`, which corresponds to the private network migration mode: scenario 2. Additionally, if you need to configure other settings, follow the client.json file parameter description.
5. (Optional) Exclude files or directories on the source server that do not need to be migrated.
   If there are files or directories on the Linux source server that do not need to be migrated, add them to the rsync_excludes_linux.txt file.
6. Run the tool.
   For example, on a 64-bit Linux source server, execute the following command as the root user to run the tool.

```
sudo ./go2tencentcloud_x64
```

> **Note**
> If you have not modified `Client.ToolMode` in client.json to `true`, you need to add the parameter `--no-console` when running the tool, as follows:
>
> ```
> sudo ./go2tencentcloud_x64 --no-console
> ```

Please wait for the migration process to complete. If the following appears on the console, the migration has been completed successfully.

```
[root@VM_0_12_centos go2tencentcloud]# sudo ./go2tencentcloud_x64
[2019-09-24 20:06:08] Start go2tencentcloud 1.3.0
[2019-09-24 20:06:08] Load user.json successfully.
[2019-09-24 20:06:08] Load client.json successfully.
[2019-09-24 20:06:09] [1/3] Initialize instance
[2019-09-24 20:06:09] Restart remote instance...
Used: 00:01:30 | Max Timeout: 00:10:00
[2019-09-24 20:07:40] Restart remote instance successfully.
[2019-09-24 20:07:40] Start preparing remote server...
[2019-09-24 20:07:40] Prepare remote server successfully.
[2019-09-24 20:07:40] Start initializing remote server...
Used: 00:00:10 | Max Timeout: 00:03:00
[2019-09-24 20:07:51] Initialize remote server successfully.
[2019-09-24 20:07:51] [2/3] Synchronize files
[2019-09-24 20:07:51] Transmitting files...
[##################################################################################] 100% | 00:04:12
[2019-09-24 20:12:04] Transmit files successfully.
[2019-09-24 20:12:04] Reconfigure remote instance...
Used: 00:00:06 | Max Timeout: 00:05:00
[2019-09-24 20:12:11] Reconfigure remote instance successfully.
[2019-09-24 20:12:11] [3/3] Release instance
[2019-09-24 20:12:11] Clean temporary data successfully.
[2019-09-24 20:12:11] Migrate successfully.
```

Private Network Migration Scenario 3

1. Establish a connection between the source server and the destination CVM.
   Create a connection channel between the source server and the destination CVM using methods such as VPC Peering Connection, VPN Connection, or Cloud Connect Network.
2. Download or upload `go2tencentcloud.zip` to the source server and run the following command to enter the corresponding directory.
   2.1 Run the following commands in sequence to decompress `go2tencentcloud.zip` and enter the directory.

   ```
   unzip go2tencentcloud.zip
   ```

   ```
   cd go2tencentcloud
   ```

   2.2 ii. Run the following commands in sequence to decompress `go2tencentcloud-linux.zip` and enter the directory.

   ```
   unzip go2tencentcloud-linux.zip
   ```

   ```
   cd go2tencentcloud-linux
   ```

   > **Note**
   > The files in the `go2tencentcloud` directory will not be migrated. Do not place the files to be migrated in this directory.

3. Configure the destination CVM in the `user.json` file.
   Please set the required and necessary values according to the user.json file parameter description.

4. Configure the migration mode and other settings in the `client.json` file.
   - Set the `Client.ToolMode` value in the `client.json` file to `true`, indicating the tool mode migration.
   - Set the `Client.Net.Mode` item in the `client.json` file to `3`, which corresponds to the private network migration mode: scenario 3.
   - Set the `Client.Net.Proxy.Ip` and `Client.Net.Proxy.Port` fields in the `client.json` file to the IP address and port of your network proxy. If your network proxy requires authentication, enter the username and password in the `Client.Net.Proxy.User` and `Client.Net.Proxy.Password` fields. If authentication is not required, leave them blank.
     Additionally, if you need to configure other settings, follow the client.json file parameter description.
5. (Optional) Exclude files or directories on the source server that do not need to be migrated.
   If there are files or directories on the Linux source server that do not need to be migrated, add them to the rsync_excludes_linux.txt file.
6. Run the tool.
   For example, on a 64-bit Linux source server, execute the following command as the root user to run the tool.

```
sudo ./go2tencentcloud_x64
```

> **Note**
> If you have not modified `Client.ToolMode` in client.json to `true`, you need to add the parameter `--no-console` when running the tool, as follows:
>
> ```
> sudo ./go2tencentcloud_x64 --no-console
> ```

Please wait for the migration process to complete. If the following appears on the console, the migration has been completed successfully.

```
[root@VM_0_7_centos go2tencentcloud]# sudo ./go2tencentcloud_x64
[2019-09-25 21:06:08] Start go2tencentcloud 1.3.0
[2019-09-25 21:06:08] Load user.json successfully.
[2019-09-25 21:06:08] Load client.json successfully.
[2019-09-25 21:06:09] [1/3] Initialize instance
[2019-09-25 21:06:10] Restart remote instance...
Used: 00:01:16 | Max Timeout: 00:10:00
[2019-09-25 21:07:27] Restart remote instance successfully.
[2019-09-25 21:07:27] Start preparing remote server...
[2019-09-25 21:07:27] Prepare remote server successfully.
[2019-09-25 21:07:27] Start initializing remote server...
Used: 00:00:11 | Max Timeout: 00:03:00
[2019-09-25 21:07:39] Initialize remote server successfully.
[2019-09-25 21:07:39] [2/3] Synchronize files
[2019-09-25 21:07:39] Transmitting files...
[##################################################################################] 100% | 00:02:40
[2019-09-25 21:10:19] Transmit files successfully.
[2019-09-25 21:10:19] Reconfigure remote instance...
Used: 00:00:09 | Max Timeout: 00:05:00
[2019-09-25 21:10:29] Reconfigure remote instance successfully.
[2019-09-25 21:10:29] [3/3] Release instance
[2019-09-25 21:10:29] Clean temporary data successfully.
[2019-09-25 21:10:29] Migrate successfully.
```

Checking after the migration

- If the migration fails, please check the error messages in the log file (default is the log file in the migration tool directory), refer to the documentation, or consult the Common Issues in Server Migration to troubleshoot and resolve the issue.
- If the migration is successful, check whether the target CVM starts up normally, whether data on the target CVM is consistent with that on the source server, and whether the network and other system services are normal.

If you have any questions or encounter migration issues, please refer to Common Questions about Server Migration or contact us for assistance.

Migrating via Private Network

Last updated: 2023-09-07 18:28:02

Scenario

This article outlines the steps to migrate the system and applications from a source server in your IDC or cloud platform to Tencent Cloud CVM using the **private network migration** mode through the CVM console's online migration feature. Compared with the public network mode, migration over the private network has a higher migration transfer speed, which can significantly improve the migration efficiency. Plus, it doesn't restrict the public network access capability of the source server, making the migration configuration more flexible.

Considerations

- You have a Tencent Cloud account.
- If you are using a sub-account for console migration, log in to the Access Management Console as the root account and grant the sub-account `QcloudCSMFullAccess` permission.
- Create and obtain the SecretId and `SecretKey` in the `API Key Management` page.
- Download the migration tool compressed package.
- Stop applications on the source server to prevent existing applications from being affected by the migration.

Instructions

Backing up Data

- Source server: you can use the source server's snapshot feature or other methods to back up data.
- Destination CVM: you can create a snapshot or use other methods to back up data.

Getting migration tool

Click here to obtain the migration tool package.

Choosing a Migration Mode Based on the Network Environment

Based on the network environment of your source server and target CVM, determine the appropriate migration mode. The console's online migration currently supports public network mode and private network migration mode, with the latter further divided into three scenarios. Different migration modes/scenarios have varying network requirements for the source server and target CVM. If both the source server and target CVM can access the public network, you can directly perform the default mode migration. If either the source server or target CVM cannot directly access the public network, you can choose to establish a connection channel through VPC peering, VPN connection, Cloud Connect Network, or Dedicated Line Access before proceeding with the private network mode migration.

Checking before Migrating

Before migration, check the following items according to your actual situation:

- If the migration destination is a CVM instance, you need to check the source server and destination CVM.
- If the migration destination is a CVM image, you need to check only the source server.

Linux source server	1. Check and install Virtio. For more information, see Checking Virtio Drivers in Linux. 2. Run the `which rsync` command to check whether rsync has been installed. If not, install it. For more information, see How do I install Rsync. 3. Check whether SELinux is enabled. If yes, refer to How to Disable SELinux for instructions on disabling it.

	4. After initiating a migration request to the Tencent Cloud API, the API will use the current UNIX time to check the generated token. Ensure that the system time is accurate.
Destination CVM (optional)	1. Storage space: the cloud disks of the destination CVM (including system and data disks) should have sufficient capacity to save data migrated from the source server. 2. Security group: port 443 and port 80 cannot be restricted in the security group. 3. Bandwidth: Set the bandwidth cap on both the two ends to the highest possible value. During the process, the traffic consumed is approximately the amount of data migrated. Adjust the billing mode beforehand if necessary. 4. Ensure the OS types of the destination CVM and source server are consistent: Inconsistency in the OS types may cause discrepancies between the image information and the actual OS. It is recommended to choose a destination CVM with the same OS type as the source server. For example, when migrating a CentOS 7 source server, select a CVM with CentOS 7 as the migration target.

Note

- Check the source server by executing `sudo ./go2tencentcloud_x64 --check`.
- By default, go2tencentcloud automatically performs checks upon launch. To skip checks, open the `client.json` file, set `Client.Extra.IgnoreCheck` to `true`.
- For more information on the go2tencentcloud migration tool, see Migration Tool.

Starting the Migration

1. Establish a private network connection between the source server and Tencent Cloud.
   - If the migration target is a destination CVM: Establish a connection channel between the source server and the destination CVM using methods such as VPC Peering Connection, VPN Connection, or Cloud Connect Network.
   - If the migration target is a CVM image: Establish a connection channel between the source server and Tencent Cloud VPC using methods such as VPC peering, VPN connection, or Cloud Connect Network.
2. Download or upload `go2tencentcloud.zip` to the source server and run the following command to enter the corresponding directory.

   2.1 Run the following commands in sequence to decompress `go2tencentcloud.zip` and enter the directory.

   ```
   unzip go2tencentcloud.zip
   ```

   ```
   cd go2tencentcloud
   ```

   2.2 ii. Run the following commands in sequence to decompress `go2tencentcloud-linux.zip` and enter the directory.

   ```
   unzip go2tencentcloud-linux.zip
   ```

   ```
   cd go2tencentcloud-linux
   ```

   Note
   The files in the `go2tencentcloud` directory will not be migrated. Do not place the files to be migrated in this directory.

3. (Optional) Exclude files or directories that do not need to be migrated on the source server.
   Add files and directories that don’t need to be migrate to the rsync_excludes_linux.txt file.

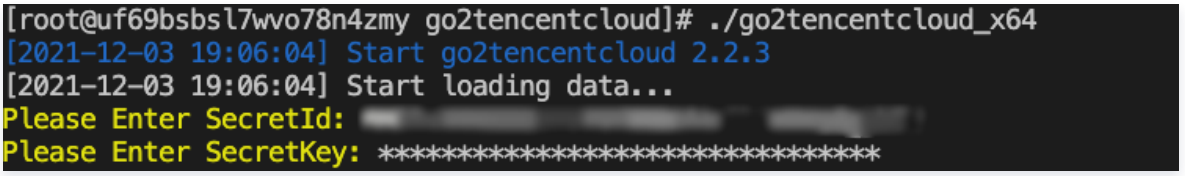
4. (Optiona) Set the network proxy.
   - If your migration scenario is private network mode: scenario 2, please skip this step.
   - If your migration scenario is private network migration mode: scenario 3, you need to configure the IP address and port of the proxy network:
     - You need to set the `client.json` file's `Client.Net.Proxy.Ip` and `Client.Net.Proxy.Port` fields to the IP address and port of the network proxy.
     - If your network proxy requires authentication, enter the username and password for the network proxy in the `Client.Net.Proxy.User` and `Client.Net.Proxy.Password` fields. If authentication is not required, leave these fields blank.
5. Register the source

   5.1 i. For example, on a 64-bit Linux source server, execute the following command in sequence as the root user to run the tool.

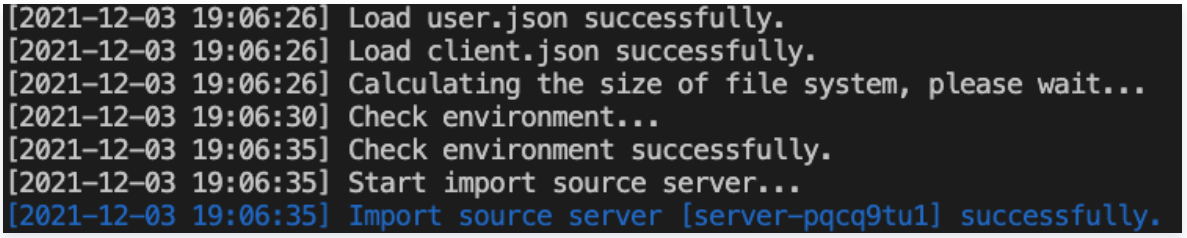
```
chmod +x go2tencentcloud_x64
```

```
sudo ./go2tencentcloud_x64
```

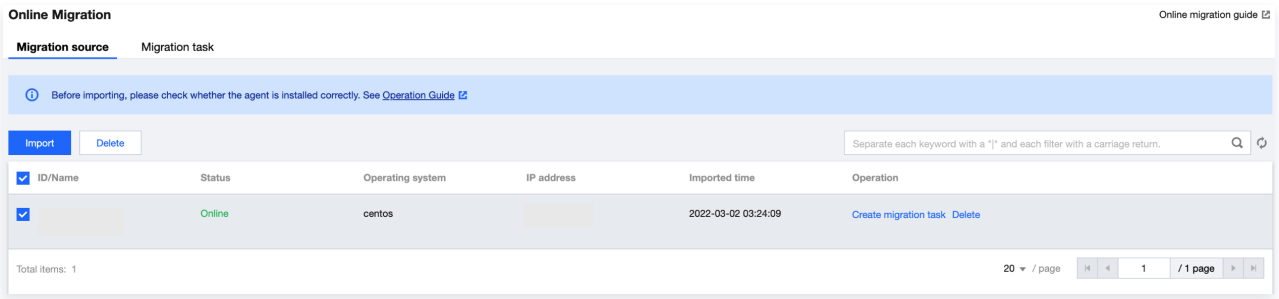
   5.2 Enter the `SecretId` and `SecretKey` of the account API access key obtained in Prerequisites and press **Enter**, as shown below:



   If the following message appears, the source server information is registered. You can now check the source server in the CVM console.



   Log in to the Online Migration Console to view the imported migration sources with the status "Online," as shown in the image below:

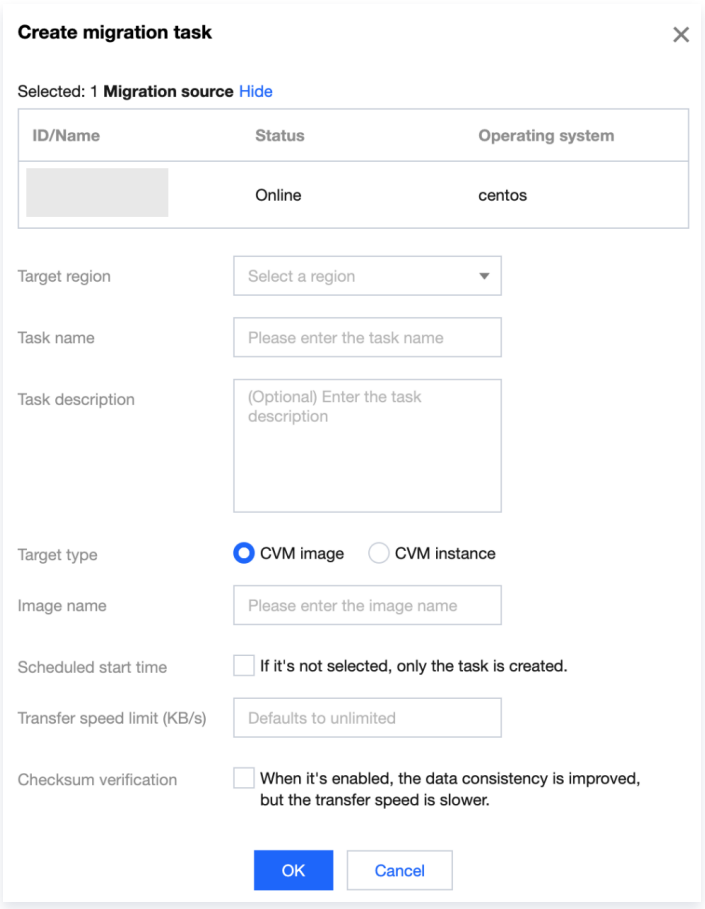


   If "Import source server successfully" does not appear, check the logs in the `logs/log` file under the migration tool directory for troubleshooting.

> **Note**

> Importing the source server is the first step of migration. Keep the migration tool alive till the whole migration progress ends. Otherwise, the migration task fails after the migration source becomes offline.

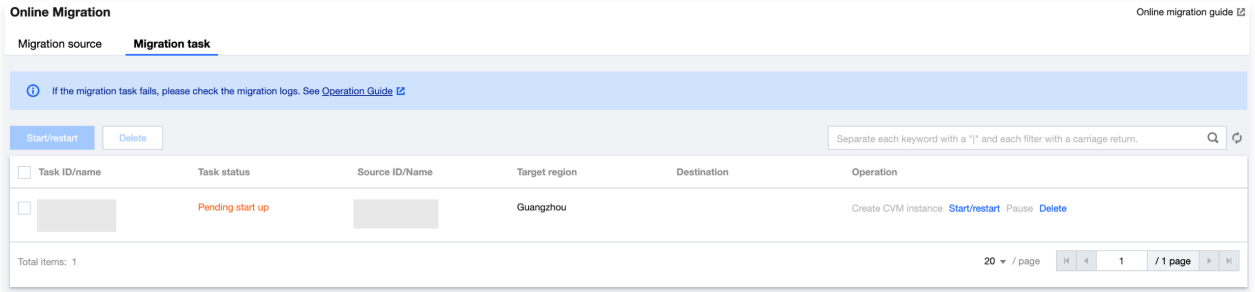
6. Go to the online migration page in the CVM console to create a migration task.
   6.1 Log in to the CVM console, go to the online migration page, and click **Create migration task** on the right of the desired migration source.
   6.2 In the pop-up **Create migration task** window, follow the Online Migration Operation Guide for configuration. For example, to migrate a Linux source host to Tencent Cloud's Shanghai region using the private network and create a destination CVM image, configure the migration task as shown in the following image:



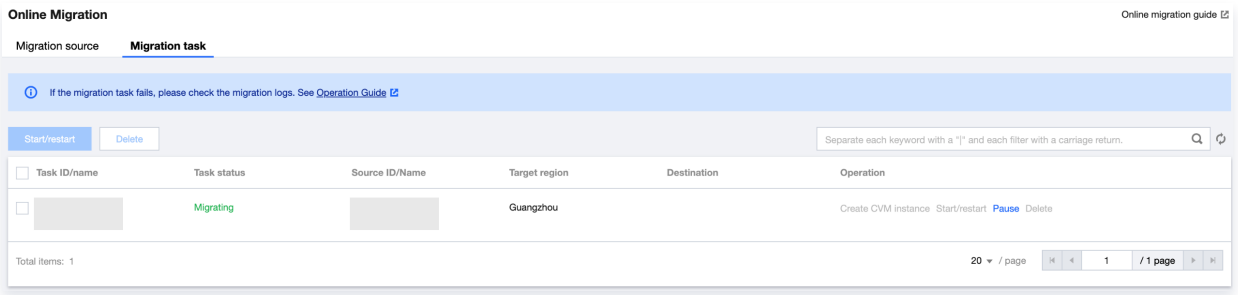
7. Start the migration task.

> **Note**
> You can skip this step if your task is scheduled, which will automatically start running at the scheduled execution time.

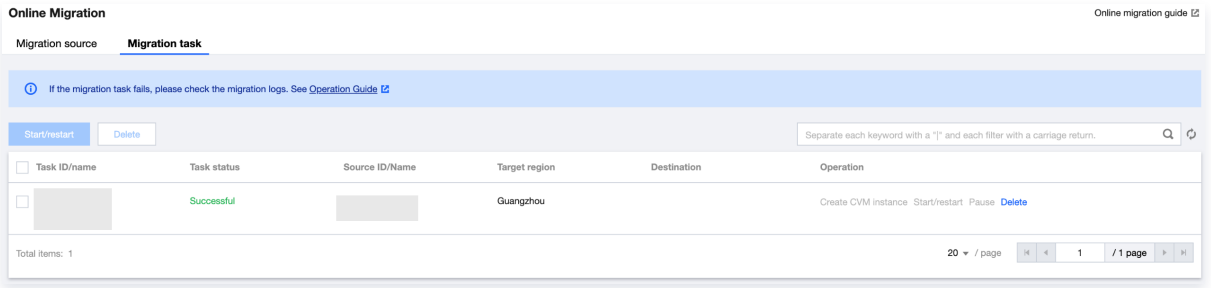
After creating a migration task, you can click the **Migration task** tab to view the task as shown below:



Click **Start/Retry** on the right side of the task row, and click **OK** in the pop-up confirmation window to start the migration task. The task status will change to "Migrating" as shown in the image below:



8. Wait for the migrate task to end.
   After the migration task status becomes **Successful**, the migration is completed, as shown below:



> **Note**
> As the data transfer duration is affected by factors such as the size of the source data and network bandwidth, please be patient and wait for the migration process to complete. The migration tool supports resuming data transfer from breakpoints.

Checking after the migration

- **Failed migration:**
  Check the error information in log files (under the migration tool directory by default), operation guides, or FAQs about Service Migration for troubleshooting methods. After troubleshooting, click **Start/Retry** in the Actions column to restart the migration task.
- **Successful migration:**
  - Migrating to a CVM: The destination CVM starts up normally. Data on the CVM is consistent with that on the source server. The network and other system services are normal.
  - Migrating to a CVM image: Click the **CVM image ID** on the row of the migration task to go to the CVM image page and view the image information. You can use this image to create CVM instances.

If you have any questions or encounter migration issues, please refer to Common Questions about Server Migration or contact us for assistance.

Migration Tool Compatibility and Tool Configuration Description

Last updated: 2023-09-07 17:39:17

Supported OS

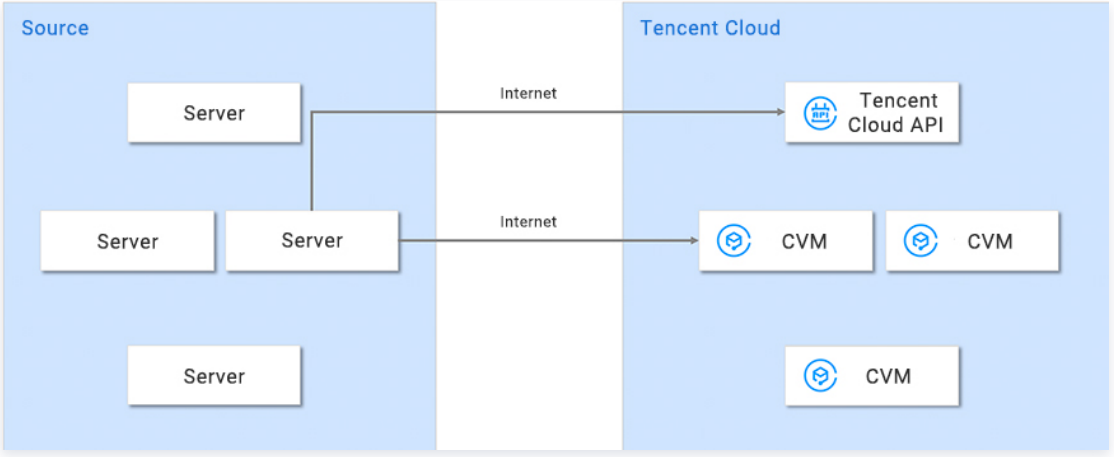
Operating systems supported by the online migration tool include but not limited to the following:

Linux OS	Windows OS
CentOS 5/6/7/8	Windows Server 2008 Windows Server 2012 Windows Server 2016 Windows Server 2019 Windows Server 2022
Ubuntu 10/12/14/16/18/20	
Debian 7/8/9/10	
SUSE 11/12/15	
openSUSE 42	
Amazon Linux AMI	
Red Hat 5/6/7/8	
Oracle Linux 5/6/7/8	

Supported Migration Modes

Public Network Migration Mode

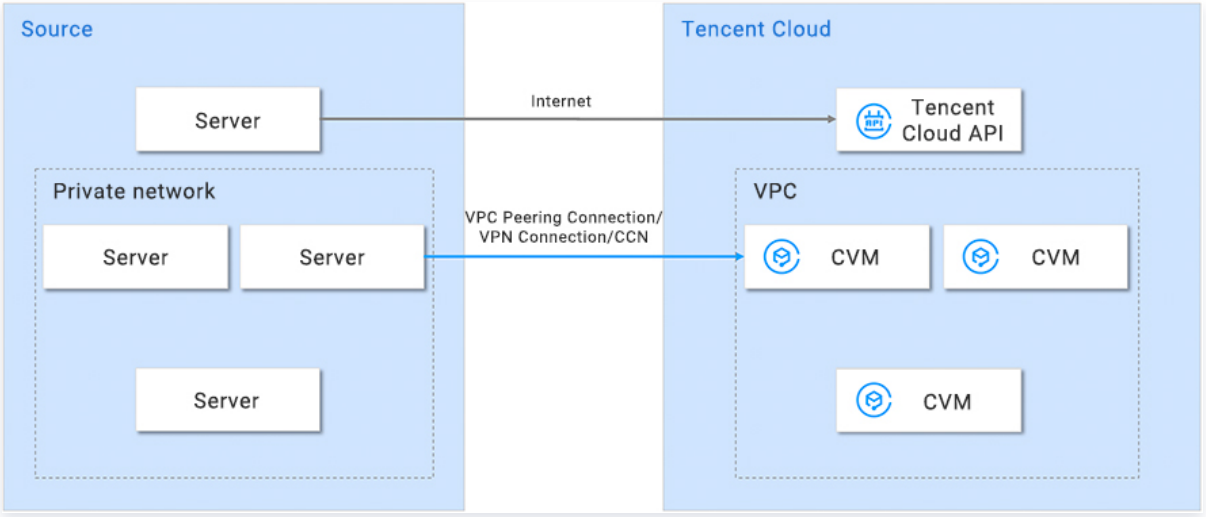
If both your source server and destination CVM have public network access capabilities, you can use the public network migration mode for migration. In the current public network migration mode, the source server accesses Tencent Cloud API via the internet to initiate migration requests and transfers data to the destination CVM, migrating the source server to the Tencent Cloud destination CVM. The public network migration scenario is shown in the following diagram:



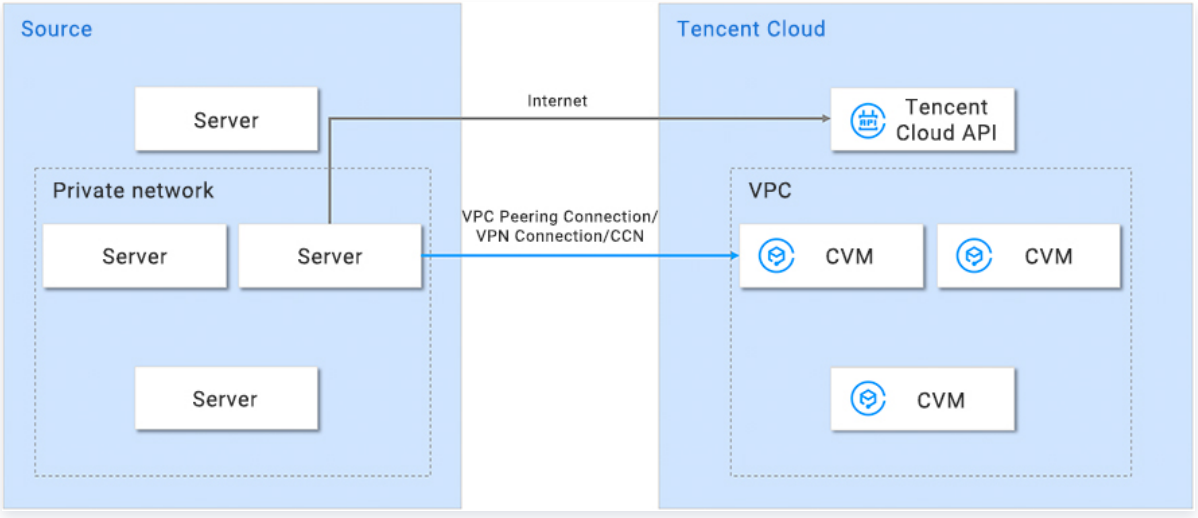
Private Network Migration Mode

If your source server or destination CVM is in a private network or VPC and cannot establish a direct connection through the internet, you can use the private network migration mode. This mode requires establishing a connection between the source server and the destination CVM using methods such as VPC Peering, VPN Connection, Cloud Connect Network, or Dedicated Line Access.

- **Scenario 1:** (This scenario only supports tool-based migration) If your source host or target CVM cannot access the public network, you can initiate a migration request by accessing Tencent Cloud API through a host with public network access (such as a gateway), and then transfer data to the target CVM via a connection channel for migration. This scenario does not require public network access for the source host and target CVM.

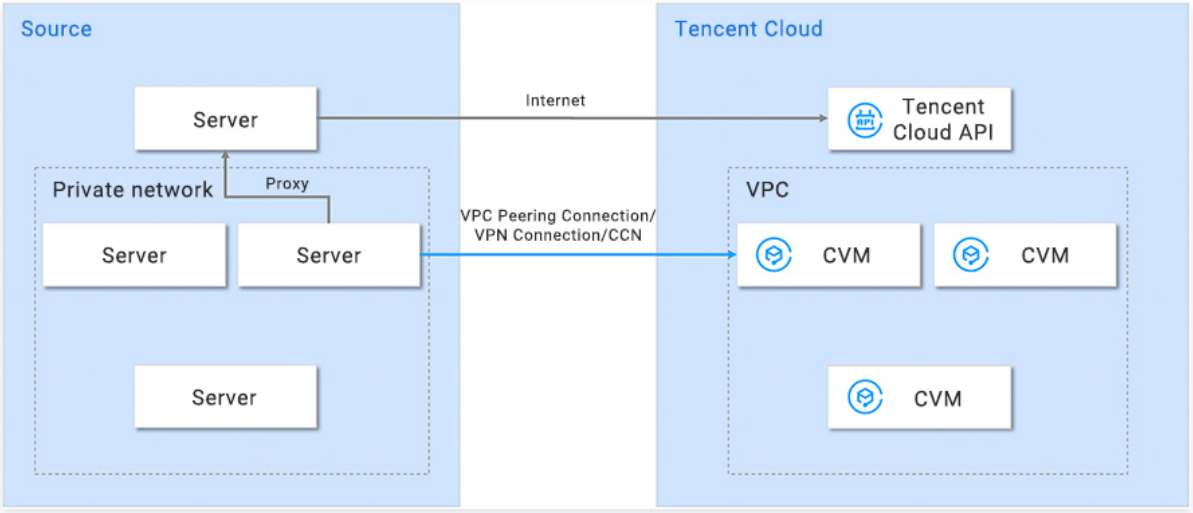


- **Scenario 2:** If your source server can access the public network, you can initiate a migration request by accessing Tencent Cloud API from the source server, and then transfer data to the destination CVM through a connection channel. This scenario requires the source server to have public network access capability, while the destination CVM does not.



- **Scenario 3:** If your source host can access the public network through a proxy, you can initiate a migration request to Tencent Cloud API via the network proxy on the source host, and then transfer data to the target cloud server through a connection channel for migration. This scenario does not require public network access

capabilities for the source host and target cloud server.



Files in the Compressed Package

After extracting `go2tencentcloud.zip`, the file descriptions are as follows:

File Name	Note
go2tencentcloud-linux.zip	Linux system migration compressed package.
go2tencentcloud-windows.zip	Windows system migration package.
readme.txt	Directory Overview File.
release_notes.txt	Migration Tool Changelog

After decompressing `go2tencentcloud-linux.zip`, the file descriptions are as follows:

File Name	Note
go2tencentcloud_x64	Migration tool executable for 64-bit Linux systems.
go2tencentcloud_x32	Migration tool executable for 32-bit Linux systems.
user.json	User information during migration.
client.json	Migration tool configuration file.
rsync_excludes_linux.txt	Configure rsync to exclude unnecessary file directories in the Linux system from migration.

After decompressing `go2tencentcloud-windows.zip`, the file descriptions are as follows:

File Name	Note
go2tencentcloud_x64.exe	Migration tool executable for 64-bit Windows systems.
user.json	User information during migration.
client.json	Migration tool configuration file.
client.exe	Executable migration program for Windows systems.

> **Note**
> The configuration files cannot be deleted. You must store them under the same folder as the go2tencentcloud executable program.

User.json File Parameter Description

The user.json configuration file is described as below:

Parameter name	Local Disk Types	Required	Note
SecretId	String	Supported	Account API access key SecretId, for more information, please refer to Access Key.
SecretKey	String	Supported	Account API access key SecretKey, for more information, please refer to Access Key.

Client.json File Parameter Description

The client.json configuration file is described as below:

Parameter name	Local Disk Types	Required	Note
Client.Extra.IgnoreCheck	Bool	Not required	The default value is false. The migration tool automatically checks the source host environment when it starts running. If you wish to bypass this check, please set it to true.
Client.Extra.Daemon	Bool	Not required	The default value is false. If you require the migration tool to run in the background, please set it to true.
Client.Net.Proxy.Ip	String	Not required	The default value is empty. If the migration scenario is private network migration: scenario 3, the IP address of the network proxy must be configured.
Client.Net.Proxy.IPv6	Bool	Not required	The default value is false. If you expect to use IPv6 for data transmission (e.g., when the source or destination has only IPv6 IPs in the migration scenario), you need to set this option to true. Otherwise, migration traffic will be transmitted via IPv4.
Client.Net.Proxy.Port	String	Not required	The default value is empty. If the migration scenario is private network migration Scenario 3, the port for the network proxy must be configured.
Client.Net.Proxy.User	String	Not required	The default value is empty. If the migration scenario is private network migration: scenario 3 and your network proxy requires authentication, you need to configure the username for the network proxy.
Client.Net.Proxy.Password	String	Not required	The default value is empty. If the migration scenario is private network migration: scenario 3 and your network proxy requires authentication, you need to configure the network proxy password.

> **Note**

> Except for the above parameters, other configuration items in the `client.json` file usually don't need to be entered.

Description of rsync_excludes_linux.txt File

Exclude files or configuration files in specified directories that do not need to be migrated from the Linux source host. The following directories and files are excluded by default, **please do not modify or delete**.

```
/dev/*
/sys/*
/proc/*
/var/cache/yum/*
/lost+found/*
/var/lib/lxcfs/*
/var/lib/docker-storage.btrfs/root/.local/share/gvfs-metadata/*
```

To exclude other directories and files, append the content at the end of the file. For example, exclude all content of the data disk mounted at `/mnt/disk1` .

```
/dev/*
/sys/*
/proc/*
/var/cache/yum/*
/lost+found/*
/var/lib/lxcfs/*
/var/lib/docker-storage.btrfs/root/.local/share/gvfs-metadata/*
/mnt/disk1/*
```

Parameters of the Migration Tool

Parameter	Note
`--help`	Prints help information.
`--check`	Checks the source server
`--log-file`	Configures the log file name, which is log by default.
`--log-level`	Configures the logging level. Valid values: 1(ERROR level), 2 (INFO level) and 3(DEBUG level). Default value: 2.
`--version`	Prints the version number.
`--clean`	Ends the migration task.

Migration Time Estimation

Last updated: 2023-09-07 17:39:42

This document describes how to estimate the time for online migrating the system and applications from a source server in your IDC or cloud platform to Tencent Cloud CVM.
The migration time is subject to the data transfer speed during migration. You can estimate it by testing the transfer speed between the source server and destination CVM.

Estimating Migration Time in Different Scenarios

Scenario 1

When the target of a Linux system migration is a CVM instance, the migration time depends on the actual time required for data transfer.
When the target of a Windows system migration is a CVM instance, the migration time depends on the time required to transfer the total disk capacity.
For instance, if the size of the data on all disks to be migrated on the Linux source server is 50 GB and the outbound bandwidth is 100 Mbps, the estimated total migration time will be 1.14 hours as calculated below:

1. Convert the unit
   - Convert the unit of the actual bandwidth to MB/s: 100 Mbps = 100 / 8 = 12.5 MB/s
   - Convert the actual disk data size to MB: 50 GB = 50 × 1,024 = 51,200 MB.
2. Estimate the actual data migration time
   51200 / 12.5 = 4096 seconds = 1.14 hours

Scenario 2

When the target of a Linux system migration is a CVM instance, the migration time depends on the actual time required for data transfer and the time to create an image.
When the target of a Windows system migration is a CVM instance, the migration time depends on the time required for transferring the total disk capacity and creating the image.
For instance, if the total disk capacity to be migrated from your Windows system source server is 50 GB and the egress bandwidth is 100 Mbps, the estimated total migration time would be 1.23 hours. The steps are as follows:

1. Convert the unit
   - Convert the unit of the actual bandwidth to MB/s: 100 Mbps = 100 / 8 = 12.5 MB/s
   - Convert the actual disk data size to MB: 50 GB = 50 × 1,024 = 51,200 MB.
2. Estimate the actual data migration time
   51200 / 12.5 = 4096 seconds = 1.14 hours
3. Calculate the image creation time at a speed of about 160 MB/s
   51200 / 160 = 320 seconds = 0.089 hour
4. Calculate the total migration time
   1.14 + 0.089 = 1.23 hours

Relevant Operations: Testing Data Transfer Speed

You can use the **iperf3** tool to test the data transfer speed, such as bandwidth and speed of data transfer from client to server.

Factors affecting transfer speed

- Outbound bandwidth of the source server and inbound bandwidth of the destination instance.
  For example, if the outbound bandwidth of the source server is 50 Mbps and the inbound bandwidth of the destination instance is 100 Mbps, the actual transfer speed won't exceed 50 Mbps theoretically.

- During the migration, the bandwidth isn't always fully used, and you can dynamically adjust the inbound bandwidth of the destination or relay instance.
- If the source server and destination instance are in different regions, the transfer speed will be lower than that when they are in the same region.

> **Note**
> - During an online migration via the console, if the migration target is a CVM image, a transit instance (named do_not_delete_csm_instance) will be created during migration, with a bandwidth cap of 50Mbps.
> - You can dynamically adjust the inbound bandwidth of the destination or relay instance in the console during migration to control the migration speed.

Speed test for migration to Linux CVM instance

For example, using the online migration feature in the console to migrate a server to a Tencent Cloud CentOS 7.5 instance. The steps for testing the transfer speed are as follows:

1. Create a pay-as-you-go CentOS 7.5 CVM instance in the migration destination region.

   > **Note**
   > - If the migration target is a CVM image, a CentOS 7.5 relay instance will be created during migration. To test its speed, it is recommended to choose a standard type with lower CPU and memory configurations, which is closer to the actual migration scenario.
   > - The default port of the iperf3 server is TCP 5201. You need to add it to and open it in the inbound traffic configuration in the security group of the CentOS 7.5 instance.

2. Install iperf3 on the source server and in the testing destination instance respectively.
   - Run the following command to install iperf3 in the destination CentOS 7.5 instance:

     ```
     yum -y install iperf3
     ```

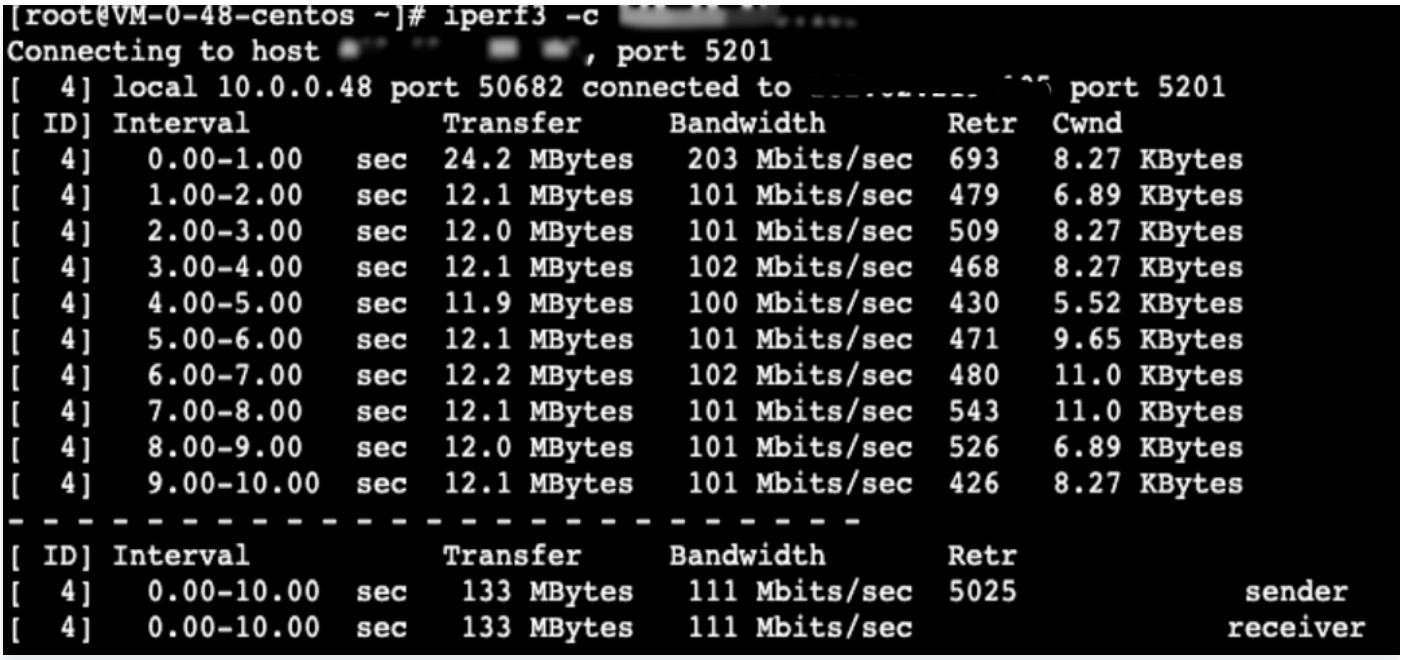
   - Install the iperf3 tool on the source server. Please use the corresponding installation command for the Linux distribution of the source server to install the iperf3 tool.
3. Run the following command to start iperf3 in the testing destination CentOS 7.5 instance as the server:

   ```
   iperf3 -s
   ```

   If "Server listening on 5201" is returned, the start succeeded.
4. Run the following command to start iperf3 on the source server as the client:

   ```
   iperf3 -c [destination instance IP]
   ```

   The returned test result is as shown below, indicating that the transfer speed between the source server and the test CentOS 7.5 instance is 111 Mbps.



```
[root@VM-0-48-centos ~]# iperf3 -c
Connecting to host , port 5201
[  4] local 10.0.0.48 port 50682 connected to  port 5201
[ ID] Interval           Transfer     Bandwidth       Retr  Cwnd
[  4]   0.00-1.00   sec  24.2 MBytes   203 Mbits/sec  693   8.27 KBytes
[  4]   1.00-2.00   sec  12.1 MBytes   101 Mbits/sec  479   6.89 KBytes
[  4]   2.00-3.00   sec  12.0 MBytes   101 Mbits/sec  509   8.27 KBytes
[  4]   3.00-4.00   sec  12.1 MBytes   102 Mbits/sec  468   8.27 KBytes
[  4]   4.00-5.00   sec  11.9 MBytes   100 Mbits/sec  430   5.52 KBytes
[  4]   5.00-6.00   sec  12.1 MBytes   101 Mbits/sec  471   9.65 KBytes
[  4]   6.00-7.00   sec  12.2 MBytes   102 Mbits/sec  480   11.0 KBytes
[  4]   7.00-8.00   sec  12.1 MBytes   101 Mbits/sec  543   11.0 KBytes
[  4]   8.00-9.00   sec  12.0 MBytes   101 Mbits/sec  526   6.89 KBytes
[  4]   9.00-10.00  sec  12.1 MBytes   101 Mbits/sec  426   8.27 KBytes
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bandwidth       Retr
[  4]   0.00-10.00  sec   133 MBytes   111 Mbits/sec  5025             sender
[  4]   0.00-10.00  sec   133 MBytes   111 Mbits/sec                  receiver
```

Billing

Last updated: 2024-06-26 10:37:02

Server migration services are provided free of charge. However, during the migration process, costs may be incurred for aspects such as **intermediate instances** and **networking**. This document explains the potential cost items and billing methods associated with server migration.

Relay Instances

- If the migration destination is a Cloud Virtual Machine (CVM) image, a relay instance named `do_not_delete_csm_instance` will be created under your account after the migration starts. The instance incurs instance fees and cloud disk fees.
- Billing mode: pay-as-you-go
- Do not reinstall, shut down, or terminate the relay instance or reset its password. It will be automatically terminated by the system after the migration ends.

Network Traffic

Network traffic is generated during online migration, which is billed as follows:

- For migration over the public network, if your source server has a bandwidth plan, no additional fees will incur on the source server. The inbound traffic on the destination CVM does not incur fees.
- For migration over the public network, if your source server is billed by traffic, traffic fees will incur on the source server. The inbound traffic on the destination CVM does not incur fees.
- Establish a connection channel through VPC peering, VPN connection, Cloud Connect Network (CCN), or Direct Connect. The costs are based on the specific network fees.

Offline Migration

Last updated: 2024-03-26 14:33:02

The following videos and documents introduce how to use offline migration:
Watch video

Scenario

Server migration is a migration platform developed by Tencent Cloud to facilitate enterprise users' transition to the cloud. This platform enables the migration of the source host's operating system, applications, and application data to Tencent Cloud's Cloud Virtual Machine (CVM) or Cloud Block Storage (CBS), fulfilling business requirements such as enterprise cloud adoption, cross-cloud platform migration, cross-account/region migration, and hybrid cloud deployment.
Server migration currently includes offline migration and online migration, with offline migration comprising the following two types:

- Offline instance migration, which involves migrating the system disk image (and data disk image, if the mounted data disk needs to be migrated as well) to the specified cloud server.
- Offline data migration, which involves migrating the data disk image to the specified cloud disk.

Preparations

Offline migration requires the support of Tencent Cloud Object Storage (COS). Please ensure that your region is within the scope of COS support. For the current list of supported regions, refer to Regions and Access Domain Names.

Considerations

> **Note**
> - Tencent Cloud's server migration currently supports image formats such as qcow2, vhd, vmdk, and raw. It is recommended to use compressed image formats to save time during transmission and migration.
> - The COS region where the image is uploaded must be the same as the region of the cloud server you are migrating to, and it must have public read access permissions.
> - If you need to import both the system disk images and data disk images, the target instances must be mounted with a corresponding amount of data disks.
> - The capacity of the target disk should be greater than (as recommended) or equal to that of the source disk.
> - Offline migration does not support the import of snapshot files (files with names like *-00000*.vmdk).

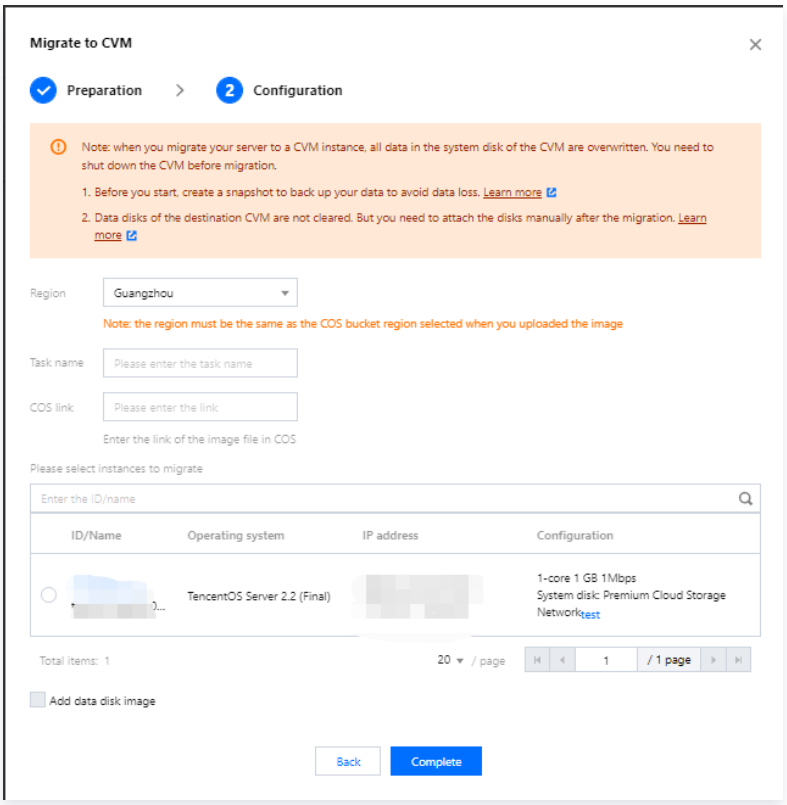
- Create an image for the server that needs to be migrated as instructed in the image creation documentation.
  - For Windows systems, please refer to Windows Image Creation Documentation.
  - For Linux systems, please refer to Linux Image Creation Documentation.
- Upload the created image file to COS.
  - Since image files are generally large and web uploads are prone to disconnections, it is recommended to use COSCMD for uploading images. For detailed operations, please refer to the COSCMD Tool Documentation.
  - If images exported from other cloud platforms are compressed packages (such as .tar.gz files), you can upload them directly to COS.
- Obtain the COS address for the image upload.
  In the Object Storage Console, locate the image file you just uploaded and copy the temporary link from the image file details page.
- Prepare the CVM or CBS to be migrated to.
  - Go to the CVM purchase page

- View Cloud Disk Purchase Guide

Instructions

Offline Instance Migration

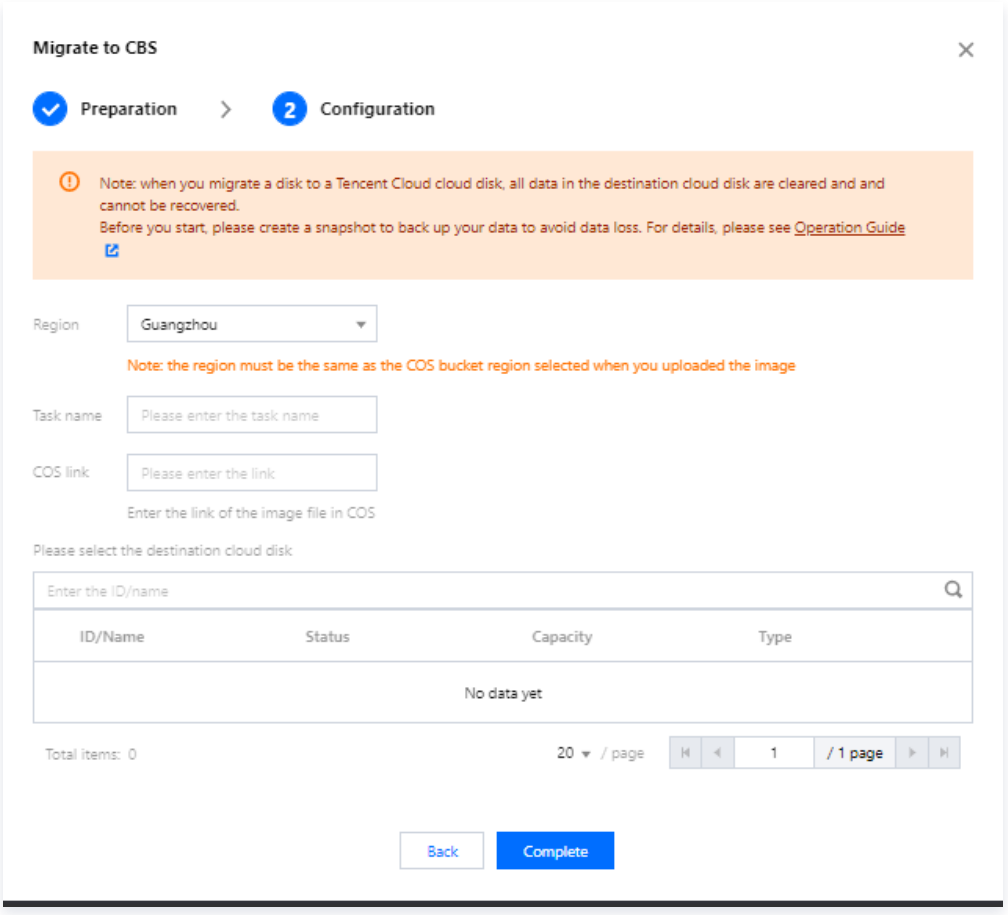
1. Log in to the CVM console and click **Server Migration** in the left navigation.
2. On the "Offline Migration" page, click **Create Instance Migration**.
3. In the **Migration to CVM** window that pops up, prepare and confirm the migration setup, then click **Next**.
4. Select the region, enter the task name, COS link, and the cloud server to be migrated, along with other migration configuration information, as shown in the image below:



5. Click **Complete** to successfully create a migration task. During the migration process, you can exit or close the Server Migration page and return to it at any time to view the progress of the migration task.

Offline Data Migration

1. Log in to the CVM console and click **Server Migration** in the left navigation.
2. On the "Offline Migration" page, click **Create Data Migration**.
3. In the **Migrate to CBS** window that appears, prepare and confirm the migration preparation, then click **Next**.
4. Select the region, enter the task name, COS link, and the cloud disk to be migrated, along with other migration configuration information, as shown in the image below:



5. Click **Complete** to successfully create the migration. During the migration process, you can exit or close the Server Migration page and return to it at any time to view the progress of the migration task.

FAQs Overview

For more information, please see About Service Migration.

Maintenance Tasks Overview

Last updated: 2024-09-24 14:07:27

Maintenance Task is designed to provide users with standardized CVM troubleshooting and authorized maintenance services.
To enhance instance performance and stability, and ensure the underlying platform's secure and efficient operation, regular online maintenance and upgrades will be performed on the host machines and platform architecture. During this process, your CVM will continue to run smoothly, and your business applications can enjoy the performance improvements brought by the platform upgrade without interruption.
Maintenance Tasks help users monitor and handle various unexpected situations in CVM instances, proactively mitigate potential downtime risks, and improve maintenance efficiency while reducing user costs. Users can back up essential data from affected instances according to their business characteristics and operational scenarios, ensuring stable business operations. Additionally, Maintenance Tasks allow users to create pre-authorized policies based on their needs or integrate with cloud APIs to build flexible and controllable automated operations for CVM failure and risk scenarios.

Strengths

Free enablement

Maintenance Task is now fully available by default, with no additional purchase required for free use. After creating and using cloud service instances, you can log in to the Maintenance Task Console to view the complete maintenance task records for all CVM instances under your account.

Full coverage of exceptions and risks

All kinds of sudden exceptions (such as sudden abnormal downtime of underlying CDH, causing the CVM to abnormally restart), running risks (predict the risks of various software and hardware failures of the underlying CDH), disk exceptions/warnings (instance disk usage exceptions/ early warnings) and scheduled maintenance and upgrade tasks are covered.

Elastic configuration

Supports setting various pre-authorized policies based on individual business scenarios and operational requirements. Each policy can be associated with different compute product instance families and supports quick binding through CVM tags.

Flexible authorization

Maintenance Tasks offer users a flexible and convenient usage experience. In addition to providing a Maintenance Task console, it also supports users in automating maintenance authorization through pre-authorized policies and cloud API integration.

Scenarios

Real-time awareness of instance exceptions and quick recovery

Users are notified with all kinds of CVM instance exceptions. Corresponding maintenance tasks are created. You can log in to the Maintenance Task console to check the recovery of the affected instances and avoid risks in time, ensuring stable business operations.

Real-time monitoring of risks on instances and avoid in advance

When the CVM instances are currently running normally, but the platform detects that there are software and hardware risks on the underlying CDH, or there are maintenance tasks planned by the platform for the CVM instances, users can receive relevant information in real time, make maintenance plans, and authorize for maintenance during low-peak business periods to avoid failures in advance and eliminate potential downtime risks.

Automatic Ops for CVM exceptions

Users can quickly integrate with pre-authorized policies and cloud APIs. When a CVM triggers new maintenance tasks and alarm events, automated operations can be utilized to achieve self-healing, improving operational efficiency.

Usage Limits

Maintenance Task is applicable to CVM, CDH and CBM instances.

Maintenance Task Type and Processing Policy

Last updated: 2023-09-07 17:41:35

Upon detecting anomalies that affect instance availability and performance (e.g., sudden host failures or proactive identification of potential hardware and software issues to mitigate downtime risks), the platform initiates a maintenance process, logs corresponding repair tasks, and notifies users of affected instances. Upon receiving such notifications, you can promptly visit the Maintenance Task Console to view the repair schedule and progress of the abnormal instances, and authorize the platform to perform maintenance to restore normal operation.
CVM instance maintenance tasks are categorized based on their triggering causes, which can be divided into several types. The specific meanings, recommended responses, and optional authorization policies for each task type are shown in the table below:

Maintenance Task Type

Viewing Task Types	Description	Suggested Solution	Available Authorization Policy
Instance running exception	Sudden software and hardware failures or system errors of the underlying CDH of the instance, which cause abnormal downtime or restart of the instance.	When a maintenance task is triggered due to an instance running abnormally, the platform immediately performs relevant maintenance operations and attempts to restart the abnormal instance to quickly restore its availability. We recommend waiting for the instance to automatically restart and monitoring the progress of the maintenance task status updates.	Choose the policy based on the current status of the maintenance task: • When the task is in the "Processing" state, the platform is urgently performing maintenance operations on the abnormal instance. Upon completion, the task status will be updated promptly, and you will be notified accordingly. • When the task is in "Ended" status, the abnormal instance has automatically restarted and restored. You can verify whether the instance and application have been restored to normal mode.
Instance running risk	The instance is currently running normally, but there are risks on software and hardware of the CDH or the underlying platform, which may cause the fluctuation of the instance performance or the abnormal downtime.	To complete the maintenance as soon as possible to avoid risks of the underlying software and hardware and potential downtime, it is recommended to back up your business data in advance and go to the Maintenance Task console to perform the following operations: 1. (Optional) Back up the instance data. 2. Authorize the platform to initiate maintenance immediately, or reserve a planned maintenance within 48 hours in advance.	According to the fixing method of the underlying risks of the instance, the following authorization methods can be selected: • Authorization for migration without CVM shutdown (the instance does not need to be shut down, and the CVM may experience short-term high load or network jitter during the migration). • Authorization for shutdown maintenance (the instance is fast restored after restart). **Note:**

		3. Wait for the system to automatically initiate maintenance at the scheduled maintenance time.	1. If the user does not authorize within 48 hours, the system will initiate maintenance at the scheduled maintenance time. 2. Local disk instances do not support quick recovery through restart and require a longer maintenance period to fix underlying hardware issues. If necessary, users can choose to redeploy the local disk instance to quickly mitigate risks (local disk data cannot be retained).
Instance disk exception	A sudden failure occurs on the local disk, which may cause reduced I/O performance of the instance or damage to the disk.	To complete the maintenance as soon as possible to restore the disk, it is recommended to back up your business data in advance and go to the Maintenance Task console to perform the following operations: 1. (Optional) Back up the instance data. 2. Authorize the platform to change the abnormal disk immediately, or reserve a planned maintenance within 48 hours in advance. 3. Wait for the platform to replace the abnormal disk, and reattach and use the replaced local disk according to the prompts in the restoration notification.	According to the fixing method of the abnormal disk, the following authorization methods can be selected: • Change disk without CVM shutdown (replace the abnormal disk without CVM shutdown. During the maintenance, the I/O of the abnormal disk is temporarily unavailable. After the maintenance is completed, you can attach and use the new disk). • Shut down to change disk (the instance needs to be shut down to replace the abnormal disk. The local disk data may be retained. A long maintenance period is required). • (Optional) Disk Abandonment Migration: Redeploy the local disk instance without retaining local disk data. Rapidly restore instance availability within minutes.
Instance disk warning	The local disk of the instance may be damaged, or its service life is about to end, which may cause instance I/O exceptions or disk offline.	To complete the maintenance as soon as possible to eliminate the potential failure risks of the local disk, it is recommended to back up your business data in advance and go to the Maintenance Task console to perform the following operations: 1. (Optional) Back up the instance data. 2. Authorize the platform to change the disk with potential	According to the fixing method of the abnormal disk, the following authorization methods can be selected: • Change disk without CVM shutdown (replace the abnormal disk without CVM shutdown. During the maintenance, the I/O of the abnormal disk is temporarily unavailable. After the maintenance is completed,

		failure risks immediately, or reserve a planned maintenance within 48 hours in advance. 3. Wait for the platform to replace the abnormal disk, and reattach and use the replaced local disk according to the prompts in the restoration notification.	you can attach and use the new disk). • Shut down to change disk (the instance needs to be shut down to replace the abnormal disk. The local disk data may be retained. A long maintenance period is required). • (Optional) Disk Abandonment Migration: Redeploy the local disk instance without retaining local disk data. Rapidly restore instance availability within minutes.
Instance network connection exception	A sudden failure occurs at the underlying network connection of the instance, which may cause network jitter or abnormal network connection.	When a maintenance task is triggered due to an instance network connection anomaly, the platform immediately performs relevant maintenance operations on the underlying network and attempts to restore the network connection availability of the abnormal instance. We recommend waiting for the automatic network connection repair to complete and monitoring the progress of the maintenance task status updates.	Choose the policy based on the current status of the maintenance task: • When the task is in the "Processing" state, the platform is urgently performing maintenance operations on the underlying network of the abnormal instance. Upon completion, the task status will be updated promptly, and you will be notified accordingly. • When the task is in "Ended" status, the network connection of the abnormal instance has been recovered. You can verify whether the instance and application have been restored to normal mode.
Instance maintenance and upgrade	Maintenance without CVM shutdown is initiated due to reasons such as underlying CDH architecture and software upgrades to improve instance performance and security.	To complete maintenance as soon as possible to improve instance performance and security, it is recommended to back up your business data in advance, and go to the Maintenance Task console to perform the following operations: 1. (Optional) Back up the instance data. 2. Authorize the platform to initiate maintenance immediately, or reserve a planned maintenance within 48 hours in advance. 3. Wait for the system to automatically initiate	You can choose from the following authorization methods: Maintenance without CVM shutdown (the instance does not need to be shut down, and the CVM may experience short-term high load or network jitter during the maintenance). **Note:** If the user does not authorize within 48 hours, the system will initiate maintenance at the scheduled maintenance time.

		maintenance at the scheduled maintenance time.	

Task Status

Task Status	Description
Pending authorization	Awaiting user authorization, users can choose the maintenance method and time. For non-disk-related tasks, if the user has not authorized within 48 hours, the system will initiate maintenance by default at the scheduled time and change the task status to "In Progress."
Scheduled	The user has granted authorization and scheduled a maintenance time. Within 48 hours of task creation, the default system maintenance time can be modified.
Handling	The maintenance task is currently in progress.
Stopped	The maintenance task has been completed.
Unnecessary	When there are ongoing maintenance tasks for an instance, user actions such as returning, terminating, or adjusting the configuration of the instance will interrupt and prevent the current maintenance task from proceeding.
Canceled	This maintenance task has been canceled by the system.

Viewing Maintenance Task

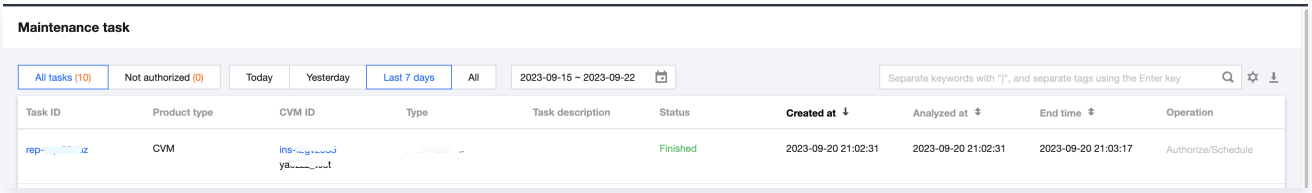
Last updated: 2024-09-24 16:59:21

Scenario

This document describes how to view the lists of pending and historical maintenance tasks and the detailed troubleshooting information in the CVM console.

Instructions

1. Log in to the CVM console and select **Maintenance Tasks** > **Task List** on the left sidebar.
2. On the **Maintenance Task** list page, select the filter conditions above the list to obtain the required maintenance task list:



3. Click the ID of a maintenance task to view more information on the task details page.

Authorizing Maintenance Policy and Scheduling Maintenance Time

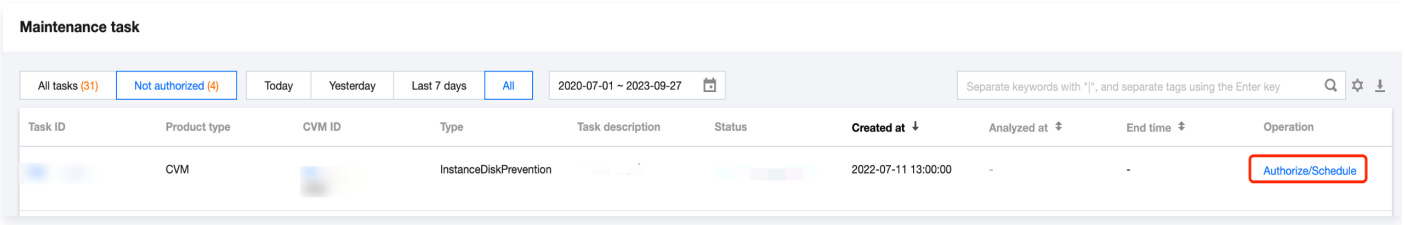
Last updated: 2023-10-08 17:21:31

Scenario

This document describes how to select a specific maintenance policy and schedule the maintenance time for a maintenance task in the CVM console.

Instructions

1. Log in to the CVM console and select **Maintenance Tasks** > **Task List** on the left sidebar.
2. Click Authorize/Schedule on the right of the row of the target Maintenance task:



3. In the pop-up window, specify the authorized maintenance method and scheduled maintenance time.

> **Note**
> - The authorization maintenance method is determined by the task type. For more information, please refer to Maintenance Task Types and Handling Policies.
> - If the **scheduled maintenance time** is not specified, maintenance will start immediately by default.

4. Click **OK** to complete the authorization of the maintenance policy.

Configuring Preset Authorization Policy

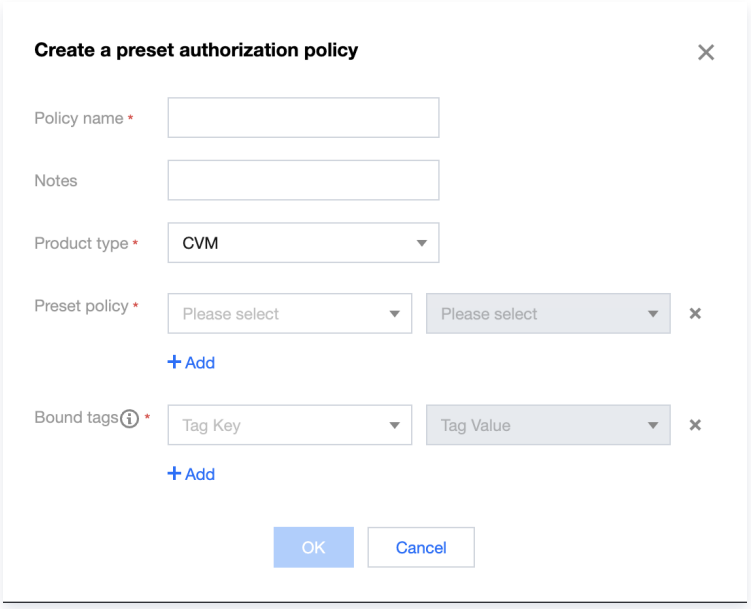
Last updated: 2024-05-15 14:46:01

Scenario

You can set a preset maintenance authorization policy for all CVM instances under a specific tag. When a maintenance task is generated, it will be processed according to the configured preset policy, eliminating the need for separate authorization operations. This article explains how to set a preset maintenance authorization policy through the CVM console.

Instructions

1. Log in to the CVM console, and select **Maintenance Tasks** > **Preset Authorization Policies** in the left navigation pane.
2. On the "Preset Authorization Policies" page, click **Create**.
3. In the **Create a Preset Authorization Policy** pop-up window, select the specific product type, metric, and policy for preset authorization and associate tags.



4. Click **OK**. After an instance associated with a set tag generates a maintenance task, the preset policy will be used by default for maintenance.

Configuring Maintenance Task Alarm Notification

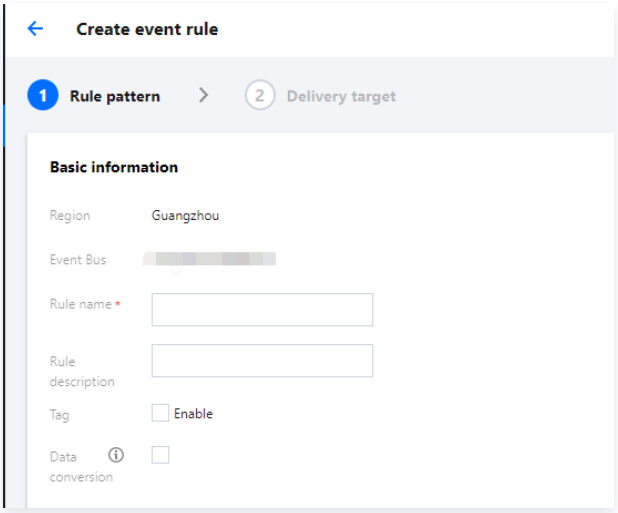
Last updated: 2023-09-07 20:53:53

Scenario

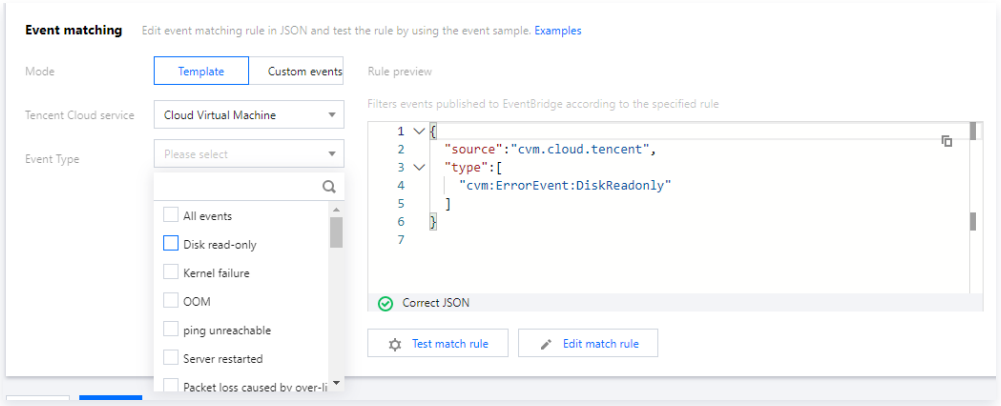
You can set up alarms for maintenance tasks related to your CVM instances, and be notified promptly via channels such as WeChat, email, SMS, and phone calls when an exception occurs. This article explains how to set up CVM instance event alarms through the EventBridge console by using the EventBridge feature.

Instructions

1. Log in to the EventBridge console and follow the Activate EventBridge guide to enable the service.
2. Select Event Rules in the left sidebar, choose the region and event set at the top of the **Event Rules** page, and click **Create event rule**.
3. Navigate to the **Create event rule** page:
   3.1 In **Basic Information**, enter the **Rule name**. As shown in the figure below:



   3.2 In the **Event matching** section, set the **Event matching** parameters according to the information below, and configure the remaining parameters as needed. See the following image:



   - **Tencent Cloud Service**: Select **Cloud Virtual Machine** from the dropdown list.
   - **Event Type**: Check the desired options in the dropdown list as needed.

   3.3 Click **Next**.
   3.4 In "Event Target," select the desired "Trigger Method" from the dropdown list and configure it according to your requirements.
   - For **Trigger Method**, select **Log Service (CLS)** and refer to CLS Target Delivery for configuration.

- For **Trigger Method**, select **Message Push** and refer to Message Push Target Delivery for configuration.

4. Click **Finish** to complete the configuration.

Network
Switching to VPC

Last updated: 2024-05-15 16:42:51

Scenario

Tencent Cloud offers both classic networks and Virtual Private Clouds (VPCs), each providing distinct high-quality services. Building upon this foundation, we deliver more flexible solutions to facilitate network management.

- Switching between networks:
  - **Classic Network to VPC**: Tencent Cloud offers services to switch from classic networks to VPCs for both individual and batch cloud servers.
  - **VPC A to VPC B**: Tencent Cloud provides services to switch from VPC A to VPC B for both individual and batch cloud servers.
- Specifying a custom IP address.
- Choosing to retain the original private IP and `HostName` of the instance.

Preparations

Before migration, unbind the CVM instance from the CLB instances and secondary ENIs in the private and public networks and release the secondary IP of the primary ENI. Rebind them after migration.

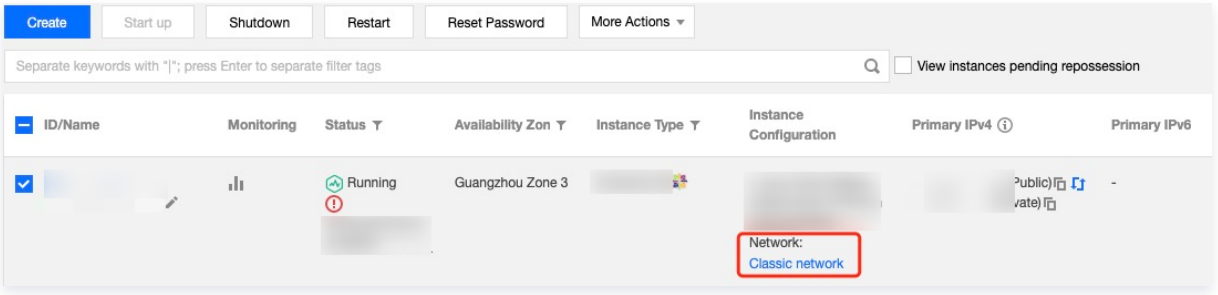
Instructions

Determining the network attribute of the CVM instance

1. Log in to the CVM console.
2. On the "instance" list page, view the target instance of which the network is pending switched based on the actually used view mode.

List view

If the **Instance Configuration** displays the network as **Classic Network**, it indicates that the instance belongs to a classic network, as shown in the following image:



Tab view

If the **Basic Information** section displays **Network Information** as **Classic Network**, it indicates that the instance belongs to a classic network.

Note

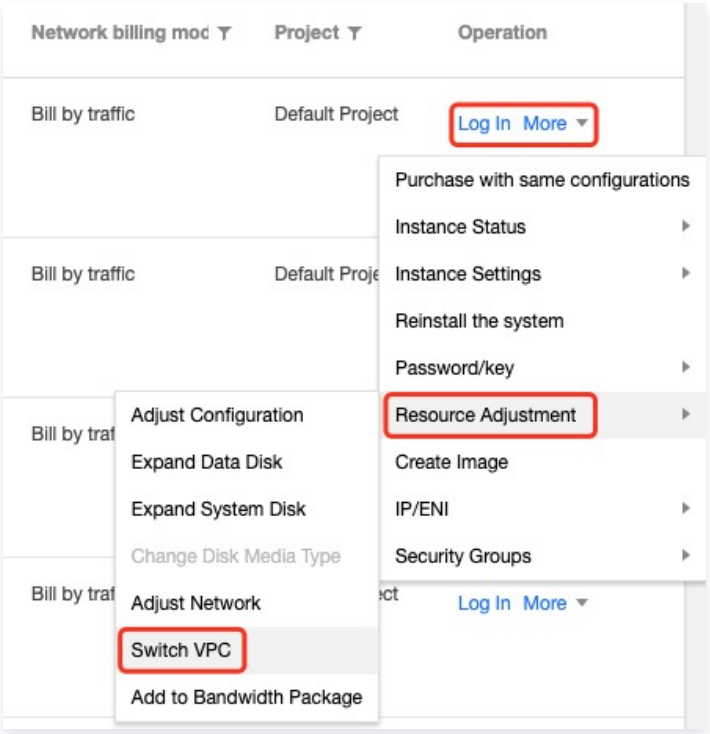
- Switching from a classic network to a VPC is irreversible. A CVM instance cannot communicate with CVM instances in classic networks after being migrated from a classic network to a VPC.
- Before switching from a classic network to a VPC, you need to create a VPC in the same region as the cloud server you want to migrate, as well as a subnet in the same availability zone. For more information, see Creating VPC.
- After understanding the network attributes of the instance, please follow the steps in Switching VPC as needed for the corresponding operation.

Migrating to VPC

1. Log in to the CVM console.
2. On the **Instances** page, migrate the target instance to VPC.

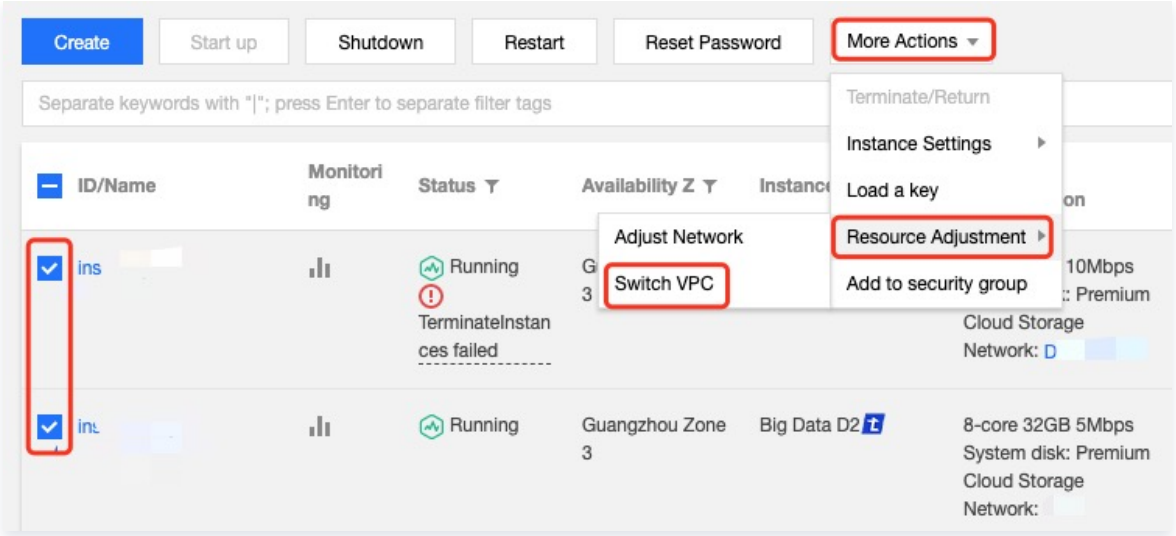
List view

- **Switching VPC for a single instance**
  Select the target instance for the network switch, and on the right-side action bar, choose **More** > **Resource Adjustment** > **Switch VPC**. As shown in the image below:



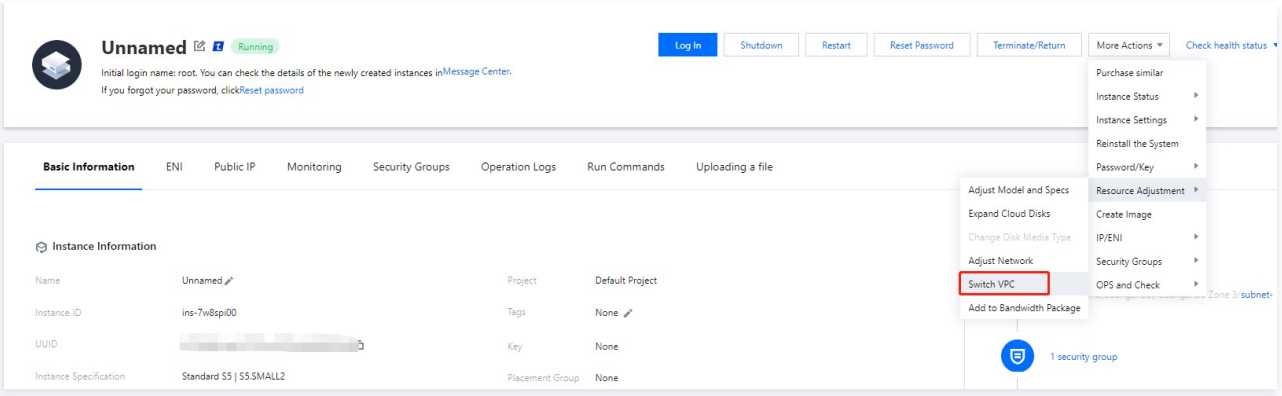
- **Batch migrating instances to the VPC**
  To switch the target instances to a VPC in bulk, select the instances to be switched, and then choose **More Actions** > **Resource Adjustment** > **Switch VPC** above the instance list, as shown in the following figure:

  Note
  When you switch the network for multiple CVMs all at once, the selected CVMs must be in the same availability zone.

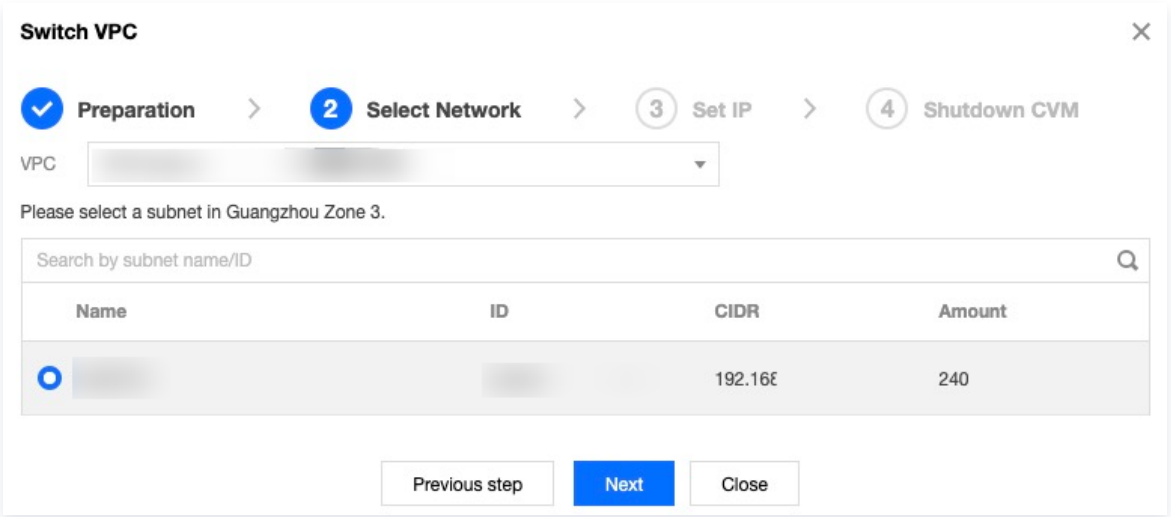


Tab view

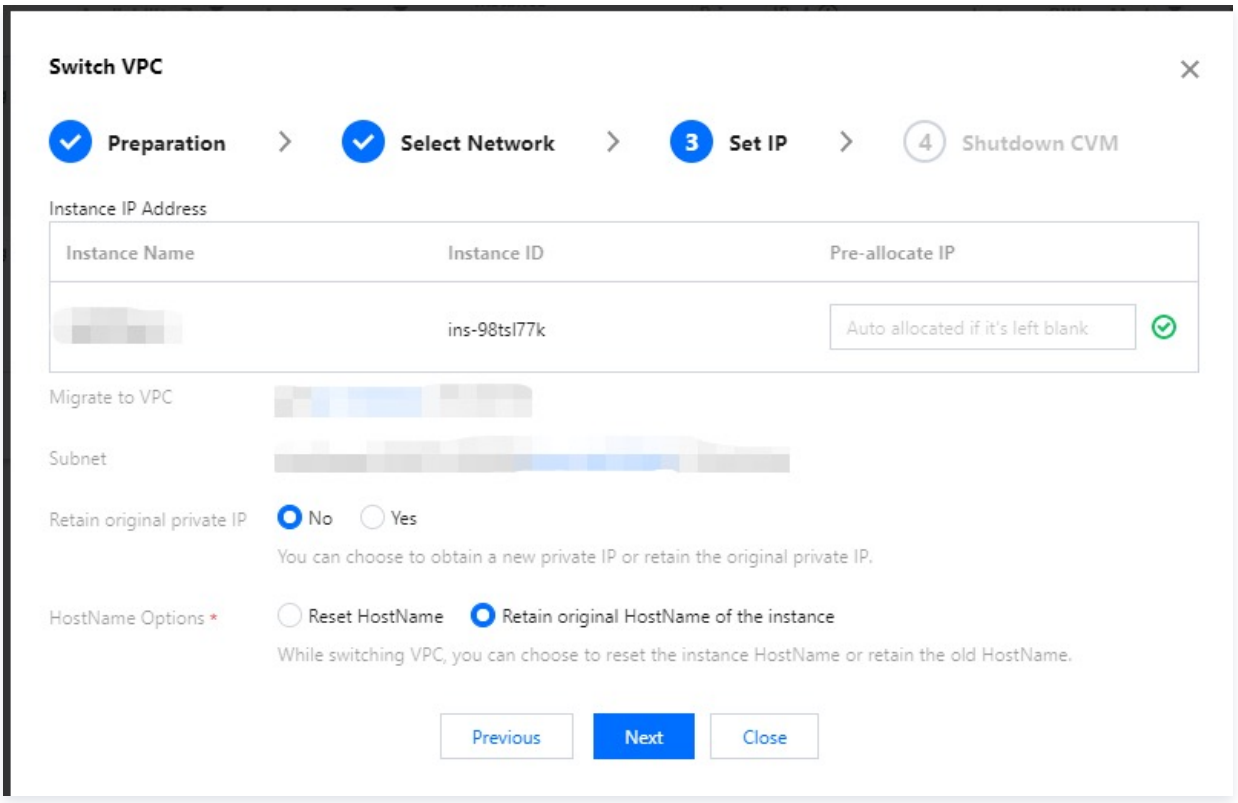
Select the target instances tab for the network switch, and click **More Actions** > **Resource Adjustment** > **Switch VPC** in the top-right corner, as shown below:



3. In the **Switch VPC** pop-up window, confirm the precautions and click **Next**.
4. Select the desired VPC and corresponding subnet, then click **Next**.



5. Configure the private IP address and HostName options under the selected subnet according to your actual requirements, as shown in the following figure:

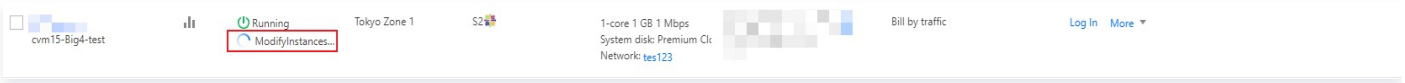


The main parameters are as follows:

- **Pre-allocated IP Address**: If you do not wish to retain the original private IP address of the instance, you can enter a **pre-allocated IP address**. If left blank, the system will automatically assign one.
- **Retain Original Private IP**: You can choose whether to retain the original private IP address of the instance as needed.
- **HostName Options**: You can choose whether to retain the original HostName of the instance as needed.

6. Click **Next**, follow the shutdown prompts, and click **Start Migration**. The instance modification status on the console page will display as **Modifying Instance VPC Attributes**, as shown below:

> **Note**
> - During the migration, the CVM instance or instances need to be restarted. Therefore, do not perform other operations.
> - After the migration, please check whether the CVM instance or instances are running normally and can be accessed via a private network and logged in to remotely.



Common Public IP

Last updated: 2024-05-15 14:46:01

Scenario

This document describes how to use a public IP address. Public IPs can only be assigned when purchasing a CVM and cannot be unbound from the CVM. If not assigned during purchase, it cannot be obtained later.

Note

- For traditional accounts, when unbinding the EIP from CVM, each account can reallocate a common public IP 10 times per day for free.
- Only BGP IPs are applicable for the current common public IP addresses.

Directions

You can use the following common public IP features:

Feature	Scenario	Documentation
Recovering public IP addresses	If you release or return a public IP (including EIP and common public IP) by mistake, you can recover it in the console, and the recovered public IP will be an EIP.	Retrieve Public IP Address
Converting common public IPs to EIPs	Converting a CVM's common public IP to an Elastic IP (EIP) allows for easy unbinding and binding with the CVM at any time, providing more flexible management of public IP addresses.	Convert a Public IP to an EIP
Changing the public IP	Change the common public IP of the CVM and release the original public IP.	• Change Public IP in the Public IP Console • Change Public IP in the CVM Console
Adjusting the network bandwidth	Adjust the bandwidth or billing mode as needed. This feature will take effect in real time.	Adjusting Network Configuration

Tag
Managing Instances via Tags

Last updated: 2024-05-15 09:43:51

Scenario

Tags are key-value pairs provided by Tencent Cloud for identifying cloud resources. Tags can help you conveniently categorize and manage cloud server resources from various perspectives, such as business, purpose, and person in charge.
Please note that Tencent Cloud does not use the tags you set; they are solely for your management of server resources.

Usage Limits

You need to pay attention to the following use limits of tags:

- Quantity: each resource can have at most 50 tags.
- Tag key limitations:
  - `qcloud`, `tencent`, and `project` prefixes are reserved for system tag keys and cannot be created.
  - Tags can only contain `numbers`, `letters`, and `+=.@-`, with a maximum length of 255 characters for the tag key.
  - Tag value limit: A tag value can contain up to 127 characters. Only `null strings or digits`, `letters`, and `+ = . @ -` symbols are supported.

Directions and Use Cases

Use case

A company has purchased six CVM instances, of which the business group, scope and owners are as follows:

Instance instance-id	Business Group	Business Scope	Owner
ins-abcdef1	E-commerce	Marketing campaigns	John Smith
ins-abcdef2	E-commerce	Marketing campaigns	Chris
ins-abcdef3	Gaming	Game A	Jane Smith
ins-abcdef4	Gaming	Game B	Chris
ins-abcdef5	Entertainment	Post-production	Chris
ins-abcdef6	Entertainment	Post-production	John Smith

Taking ins-abcdef1 as an example, we can add the following 3 sets of tags to the instance:

Tag Key	Tag Value
dept	ecommerce
business	mkt
owner	zhangsan

Similarly, you can add tag key-value pairs to other instances based on the business group, scope and owners.

Setting tags in the CVM console

Take the preceding case as an example. After designing the tag key-value pairs, you can log in to the CVM console to specify the tags.

1. Log in to the CVM console.
2. On the instance management page, proceed according to the actually used view mode:

List view
Select the instance for which you want to edit tags, then choose **More** > **Instance Settings** > **Edit Tags.**

Tab view
Select the instance(s) you want to edit tags for, then choose the top-right corner **More Actions** > **Instance Settings** > **Edit Tags**.

3. In the **Edit Tags** pop-up window, set the tags .
   For example, add three sets of tags to the instance ins-abcdef1.
4. Click **OK**, and the system will display a successful modification message.

Filtering instances by tags

To filter instances by tag, follow the steps below:

1. In the search box, select **Tag Key**.
2. Enter the tag key after **Tag Key:** and click to search.

   You can filter by multiple tag keys simultaneously. For example, entering `Tag Key: key1|key2` will filter instances with the tag keys `key1` or `key2`.

Editing Tag

Last updated: 2024-06-26 14:40:42

Scenario

This document describes how to edit resource tags.

Usage Limits

There are several limits on tags:

- Quantity: each resource can have at most 50 tags.
- Tag key limitations:
  - `qcloud`, `tencent`, and `project` prefixes are reserved for system tag keys and cannot be created.
  - Tags can only contain numbers, letters, and the characters +=.@-, with a maximum length of 255 characters.
- Tag value limit: A tag value can contain up to 127 characters. Only `null strings or digits`, `letters`, and `+ = . @ -` symbols are supported.

Preparations

You have logged in to the CVM console.

Instructions

Editing the Tag of a Single Instance

1. On the instance management page, proceed according to the actually used view mode:
   - **List View**: Select the instance for which you want to edit tags, then choose **More** > **Instance Settings** > **Edit Tag**.
   - **Tab View**: Select the instance(s) for which you want to edit tags, then click on **More Actions** > **Instance Settings** > **Edit Tag** in the top-right corner.
2. Add, modify, or delete tags in the "1 cloud resource(s) selected" pop-up window based on your needs.

Editing the Tags of Multiple Instances

> **Note**
> You can batch edit tags for up to 20 resources at a time.

1. On the instance management page, select the instances you want to edit tags for, then click **More Actions** > **Edit Tag** at the top.
2. Add, modify, and delete tags in the "n cloud resource(s) selected" pop-up window based on your needs.

Operation Examples

For information on how to use tags, see Managing Instances with Tags.

Monitoring and alarms
Getting Monitoring Statistics

Last updated: 2024-06-02 15:05:23

Scenario

Tencent Cloud inherently offers the functionality of the Tencent Cloud Observability Platform to all users, eliminating the need for manual activation. The platform commences data collection and monitoring only after a certain Tencent Cloud product has been utilized by the user. This document elucidates the process of acquiring instance monitoring data.

Instructions

Obtain via Tencent Cloud Service Console

> **Note**
> In the CVM console, there is a dedicated monitoring data retrieval page. On this page, users can view monitoring data for CPU, memory, network bandwidth, and disk usage of CVM instances, and can adjust the time period for viewing as needed.

1. Log in to the CVM console.
2. In the instance management page, click the ID of the CVM to enter its details page and view the monitoring data.
3. Click the **Monitoring** tab to obtain instance monitoring data.

Obtain via Tencent Cloud Observability Platform Console

> **Note**
> The Tencent Cloud Observability Platform Console serves as a unified entry point for monitoring data across all products. Users can view monitoring data for cloud servers, such as CPU, memory, network bandwidth, and disk usage, and freely adjust the time period for viewing.

1. Log in to the TCOP console.
2. In the left navigation pane, select **Cloud Product Monitoring** > **Cloud Server** to access the **Cloud Server – Basic Monitoring** management page.
3. Click the ID of the CVM Instance to enter its details page and view the monitoring data.

Obtain via Tencent Cloud Observability Platform Dashboard

You can create a Dashboard for cloud server metrics, and Tencent Cloud Observability Platform will automatically display the monitoring data in the form of charts on the monitoring panel. Various chart types make the monitoring data more intuitive, assisting you in analyzing metrics through trends and anomalies.

1. Log in to the Tencent Cloud Observability Platform console and select **Dashboard** > **Default Dashboard**.
2. Refer to Create Dashboard Quickly to create a dashboard and obtain monitoring data.

Retrieve via API

Users can obtain monitoring data for all products using the GetMonitorData API. For more information, please refer to Retrieve Metric Monitoring Data .

CAM Examples

Last updated: 2024-06-02 14:48:02

Scenario

You can grant a user the permission to view and use specific resources in the Cloud Virtual Machine (CVM) Console by using a Cloud Access Management (CAM) policy. This document provides examples of granting permissions to view and use specified resources, guiding users on how to apply specific policies within the console.

Sample:

Full read/write policy for CVM

If you want a user to have the permission to create and manage CVM instances, you can apply the `QcloudCVMFullAccess` policy to that user. This policy grants the user the ability to operate on all resources within CVM, VPC (Virtual Private Cloud), CLB (Cloud Load Balance), and MONITOR.

Follow these steps:
Refer to Authorization Management and grant the preset policy `QcloudCVMFullAccess` to the user.

Read-only policy for CVM

If you want a user to have the permission to query CVM instances but not create, delete, or power on/off, you can apply the `QcloudCVMInnerReadOnlyAccess` policy to that user. This policy grants the user the ability to perform all operations starting with the word **Describe** and all operations starting with the word **Inquiry** within CVM.

Follow these steps:
Refer to Authorization Management and grant the preset policy `QcloudCVMInnerReadOnlyAccess` to the user.

Read-only policy for CVM-related resources

If you want a user to have the permission to query CVM instances and related resources (VPC, CLB) but not to create, delete, or power on/off instances, you can apply the `QcloudCVMReadOnlyAccess` policy to that user. This policy grants the user the ability to perform the following operations:

- All operations in CVM that begin with the word **Describe** and all operations that begin with the word **Inquiry**.
- All operations in VPC that begin with the word **Describe**, all operations that start with the word "Inquiry", and all operations that commence with the word **Get**.
- All operations in CLB that start with the word **Describe**.
- All operations in the Cloud Monitor.

Follow these steps:
Refer to Authorization Management and grant the preset policy `QcloudCVMReadOnlyAccess` to the user.

Elastic Cloud Disk-related policies

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 cloud disks.
- **AttachCbsStorages:** Mount the specified elastic cloud disk to the designated cloud server.
- **DetachCbsStorages:** Detach the specified elastic cloud disk.
- **ModifyCbsStorageAttributes:** Modify the name or project ID of the specified cloud disk.
- **DescribeCbsStorages:** Retrieve detailed information about cloud disks.

- **DescribeInstancesCbsNum:** Query the number of elastic cloud disks mounted on the CVM and the total number of elastic cloud disks that can be mounted.
- **RenewCbsStorage:** Renew the specified elastic cloud disk.
- **ResizeCbsStorage:** Scale up the specified elastic cloud disk.

The detailed steps are as follows:

1. Based on Policy, create a custom policy that allows viewing cloud disk information in the CVM Console, as well as other permissions such as creating and using cloud disks.

   You can refer to the following policy syntax for setting the policy content:

```
{
 "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. Locate the created policy and click **Associate User/Group** in the **Operation** column.
3. In the **Associate User/User Group** window that pops up, select the user/group you want to authorize and click **Confirm**.

Security Group-related Policies

If you want a user to have the ability to view and use security groups within the CVM Console, add the following actions to your policy and then associate the policy with the user.

- **DeleteSecurityGroup:** Delete a security group.
- **ModifySecurityGroupPolicys:** Replace all security group policies.
- **ModifySingleSecurityGroupPolicy:** Modify a single security group policy.
- **CreateSecurityGroupPolicy:** Create a security group policy.
- **DeleteSecurityGroupPolicy:** Delete security group policy.
- **ModifySecurityGroupAttributes:** Modify security group attributes.

The detailed steps are as follows:

1. Create a custom policy according to Policy that allows users to have permissions such as creating, deleting, and modifying security groups in the CVM Console.
   The policy content can be set by referring to the following policy syntax:

```
{
 "version": "2.0",
 "statement":[
```

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

2. Locate the created policy and click **Associate User/Group** in the **Operation** column.
3. In the **Associate User/User Group** window that pops up, select the user/group you want to authorize and click **Confirm**.

Elastic IP address-related policies

If you want a user to have the permission to view and use Elastic IP addresses in the CVM Console, you can first add the following actions to your policy and then associate the policy with the user.

- **AllocateAddresses:** Assign addresses to VPC or CVM.
- **AssociateAddress:** Associate an elastic IP address with an instance or a network interface.
- **DescribeAddresses:** View Elastic IP addresses in the CVM Console.
- **DisassociateAddress:** Disassociate an elastic IP address from an instance or network interface.
- **ModifyAddressAttribute:** Modify the attributes of an Elastic IP address.
- **ReleaseAddresses:** Disassociate elastic IP addresses.

The detailed steps are as follows:

1. Create a custom policy as instructed in Policy.
   This policy grants the user the permission to view Elastic IP addresses in the CVM Console, assign them to instances, and associate them, but not to modify the attributes of Elastic IP addresses, disassociate them, or release them. The policy content can be set by referring to the following policy syntax:

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

2. Locate the created policy and click **Associate User/Group** in the **Operation** column.
3. In the **Associate User/User Group** window that pops up, select the user/group you want to authorize and click **Confirm**.

Policy for granting user permission to manipulate a specific CVM

To grant a user the permission to perform specific CVM operations, you can associate the following policy with the user. The steps are as follows:

1. Create a custom policy as instructed in Policy.
   This policy grants the user the permission to operate on the CVM instance with ID `ins-1` located in the Guangzhou region. The policy content can be set by referring to the following policy syntax:

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

2. Locate the created policy and click **Associate User/Group** in the **Operation** column.
3. In the **Associate User/User Group** window that pops up, select the user/group you want to authorize and click **Confirm**.

Policy for granting user permission to manipulate CVM in a specific region

To grant a user the permission to operate CVM instances in a specific region, you can associate the following policy with the user. The steps are as follows:

1. Create a custom policy as instructed in Policy.
   This policy grants the user the permission to operate on CVM instances in the Guangzhou region. The policy content can be set by referring to the following policy syntax:

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

2. Locate the created policy and click **Associate User/Group** in the **Operation** column.
3. In the **Associate User/User Group** window that pops up, select the user/group you want to authorize and click **Confirm**.

Granting a sub-account full permissions for CVMs with the exception of billing

Suppose there is a sub-account (Developer) under the enterprise account (CompanyExample, ownerUin is 12345678). This sub-account needs to have full management permissions for the enterprise account's CVM service (such as creating, managing, and all other operations), but not payment permissions (can place orders but cannot pay).

We can implement this through the following two solutions:

- **Solution A**
  The enterprise account `CompanyExample` directly grants the preset policy `QcloudCVMFullAccess` to the sub-account `Developer`. For the authorization method, please refer to Authorization Management.
- **Option B**

1. Create a Custom Policy based on the following policy syntax:

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

2. Grant this policy to the sub-account. For the authorization method, please refer to Authorization Management.

Grant sub-account the permission to manage projects

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

1. Create a custom project management policy based on business permissions.
   For more information, please refer to Policy.
2. Refer to Authorization Management and grant the custom policy you created to the sub-account.
   If the sub-account encounters permission issues while managing projects, such as viewing snapshots, images, VPC, or Elastic Public IP, you can grant the sub-account the preset policies `QcloudCVMAccessForNullProject`, `QcloudCVMOrderAccess`, and `QcloudCVMLaunchToVPC`. For granting permissions, please refer to Authorization Management.

Custom Policy

If you find that the preset policy does not meet your requirements, you can achieve your goal by creating a custom policy.
For specific steps, please refer to Policy.
For more CVM-related policy syntax, see Authorization Policy Syntax.