Cloud Virtual Machine

Product Documentation

Contents

Cloud Virtual Machine 7
- Product Introduction 7
  - CVM Overview 7
  - Regions and AZs 10
  - Features and Advantages 15
  - Use Cases 18
  - Instance 20
    - Instance Overview 20
    - Specification 22
    - Lifecycle 26
  - Storage 30
    - Storage Overview 30
    - Cloud Block Storage 33
    - Local Disk 34
    - Cloud Object Storage 36
  - Image 37
    - Image Overview 37
    - Type 40
  - Snapshot 42
  - Network and Security 45
    - Network and Security Overview 45
    - Placement Group 47
    - Network Environment 49
    - Private Network Service 51
    - Public Network Service 53
    - Elastic Public IP 55
    - Elastic Network Interface 56
    - SSH Key 58
  - Ops and Monitoring 60
    - Instance Self Check 60
    - Monitoring and Alarms 64
  - Access Control 67
    - Access Control Overview 67
    - Authorized Resource Types 68
    - Authorization Policy Syntax 71
  - CVM Dedicated Host 75
    - CDH Overview 75
    - Strengths 77
    - Use Cases 79
    - Model Overview 81
    - Lifecycle 85
- Quick Start 86
  - How to Get Started with CVM 86
  - Custom Configuration 87
    - Selecting Cloud Disks 87
    - Planning the Network 89
    - Configure Security Group 91
    - Customizing Linux CVM Configuration 94
    - Customizing Windows CVM Configuration 97
  - CVM Dedicated Host 100
    - Assigning a Dedicated Instance on CDH 100
- Operation Guide 102
  - Overview 102
  - Use Limits 104
  - Instance 107
    - Creating an Instance 107
    - Logging In to Instance 112
      - Logging In to Linux Instances 112
      - Logging In to Windows Instances 114
    - Adjusting Configuration 116
      - Adjusting Instance Configuration 116
      - Adjusting Network Configuration 118
      - Adjusting Disk Configuration 119
      - Switching Virtual Private Clouds 120
      - Configuring the Network after Using the Imported Windows Image to Create an Instance 121
    - Viewing Information 122
      - View Instance Information 122
      - Viewing Instance Monitoring Information 124
      - Querying Instance Metadatas 125
    - Renaming Instance 133
    - Resetting Instance Password 134
    - Managing Instance IP Address 135
      - Getting the Private IP Address and Setting DNS 135
      - Modifying Private IP Addresses 137
      - Changing Public IP Addresses 139
    - Change Instance Subnet 141
    - Changing the Security Group 143
    - Searching for Instance 145
    - Exporting Instance 146
    - Restarting Instances 147
    - Shutting Down Instance 148
    - Terminating Instances 150
    - Reinstalling System 152
    - Cloning an Instance 155
    - Manage Instance Launch Templates 156
    - Rescue Mode 158
    - Billing Suspension Upon Shutdown 160
    - GPU Instance 162
      - Creating and Configuring GPU Instance 162

- Logging In to the GPU Instances ... 163
- Restarting Instances ... 164
- GPU Instance Type ... 165
- CVM Dedicated Host ... 166
- Viewing CDH Instance Information ... 166
- Searching for CDH Instances ... 167
- Modifying CDH Instance Name ... 168
- Assigning CVM Instances ... 169
- Logging in to Sub-Machine ... 172
- Image ... 173
- Creating Custom Image ... 173
- Copying an Image ... 175
- Sharing Custom Images ... 176
- Unsharing Custom Image ... 178
- Deleting Custom Image ... 179
- Importing Image ... 180
- Overview ... 180
- Forced Import Image ... 185
- Checking Virtio Driver in Linux System ... 190
- Installing Cloudbase-Init on Windows System ... 198
- Installing cloud-init on Linux System ... 203
- Export Image ... 205
- Create Linux Image ... 206
- Creating Windows Image ... 212
- Service Migration ... 216
- Offline Migration ... 216
- Online Migration ... 219
- Online Migration Overview ... 219
- Migration Operation Guide ... 221
- Online Migration: Importing a Migration Source Through the Clien ... 221
- Migration Tool Description ... 230
- Compatibility and Tool Configuration Instructions ... 230
- Migration Time Estimation Tutorial ... 240
- Network ... 243
- Elastic Public IP ... 243
- Elastic Network Interface ... 245
- EIP Direct Access ... 246
- Configuring IPv6 address ... 248
- Security ... 250
- Security Group ... 250
- Overview ... 250
- Creating Security Group ... 253
- Adding Security Group Rule ... 256
- Associating Instance with Security Group ... 259
- Managing Security Group ... 261
- Viewing Security Group ... 261
- Removing from Security Group ... 262
- Clone Security Group ... 263
- Deleting Security Group ... 264
- Adjust the Priority of Security Groups ... 265
- Managing Security Group Rule ... 267
- Viewing Security Group Rules ... 267
- Modifying Security Group Rule ... 268
- Deleting Security Group Rule ... 269
- Importing Security Group Rule ... 270
- Exporting Security Group Rule ... 271
- Adjusting the Priority of Security Groups Rules ... 272
- Security Group Use Cases ... 274
- Common Server Ports ... 279
- Sensitive Operation Protection ... 281
- Login Password ... 282
- SSH Key ... 284
- Placement Group ... 286
- Managing the Instance Placement Groups ... 288
- Tag ... 290
- Editing Tags ... 290
- Managing Instances Using Tags ... 292
- Monitoring and Alarms ... 295
- Getting Instance Monitoring Data ... 295
- Creating an Alarm ... 297
- Using Self-Service Instance Test ... 299
- Example of Cloud Access Management ... 300
- Install NVIDIA Tesla Driver ... 307
- Best Practices ... 313
- Best Practices for CVM ... 313
- Network Performance Test ... 315
- Cloud Virtual Machine Migration ... 322
- Building FTP Service ... 324
- Building FTP Services on Linux CVMs ... 324
- Building FTP Services on Windows CVMs ... 329
- Manual Setup of WIPM Environment ... 332
- Step 1: Install IIS Service ... 332
- Step 2: Deploy PHP Environment ... 335
- Step 3: Install MySQL Database ... 347
- NTP Service ... 359
- Overview ... 359
- Set NTP Service in Linux Instance ... 360
- Set NTP Service in Windows Instance ... 365
- Best Practices for Boot Modes Legacy BIOS and UEFI ... 370
- Ops Guide ... 372
- Mount Data Disk ... 372

- Initialize Data Disk (Linux Cloud Virtual Machine) ... 372
- Initialize Data Disk (Windows Cloud Virtual Machine) ... 373
- Reading the Original EXT Data Disks after Reinstalling Linux to ... 374
- Reading and Writing the Original NTFS Data Disks after Reinstall ... 377
- Environment Configuration ... 379
- Installing ACPI Power Management ... 379
- How to effectively modify the etc/hosts configuration of Linux C ... 381
- LNMP environment configuration under openSUSE ... 384
- Uploading Files ... 390
- How to copy local files to a CVM ... 390
- Uploading Files to Windows CVM via MSTSC ... 392
- Upload Files from MacOS System to Windows CVM via MRD ... 396
- Uploading Files to a Windows Cloud Server from a Linux System vi ... 401
- Uploading Files to a Linux CVM via WinSCP on Windows ... 404
- Uploading Files to a Linux Cloud Virtual Machine via SCP ... 406
- Uploading Files to CVM via FTP on Windows Systems ... 407
- Software Installation ... 409
- Cloud Platform Software Source Accelerates Software Package Down ... 409
- Installing Software on Ubuntu via Apt-get ... 416
- Installing Software on CentOS via YUM ... 417
- Install software via zypper in OpenSUSE environment ... 420
- Custom Data ... 423
- Setting Custom Data (Linux Cloud Virtual Machine) ... 423
- Setting Custom Data (Windows Cloud Virtual Machine) ... 427
- System ... 432
- System Activation ... 432
- System Update ... 434
- Shutdown ... 436
- Configuring High-performance Power Management ... 438
- Windows Recovery Mode ... 440
- Updating Virtio Network Interface Drivers ... 444
- Modifying SID Operation Instructions ... 446
- Others ... 449
- Linux Common Operations and Commands ... 449
- Setting Linux CVM to Enter Single-user Mode ... 456
- Setting to Allow Multiple Users to Remotely Log in to Windows CVM ... 467
- Allowing CVM Without a Public Network to Access the Public Netwo ... 475
- Troubleshooting ... 479
- Instance-related Failures ... 479
- Solution to the Problem of Being Unable to Log in to the CVM ... 479
- Windows Instance-related ... 483
- Unable to Log in to a Windows Instance ... 483
- Windows Instances: An Authentication Error Occurred ... 487
- Windows Instance: No Remote Desktop Services Log-in Permission ... 490
- Windows Instance: Network Level Authentication Required ... 491
- Windows Instance: Mac Remote Log-in Exception ... 495
- Windows Instance: Remote Desktop cannot connect to the remote computer ... 497
- Windows Instance: Credentials Not Work ... 504
- Windows Instance: Failed to log in to a Windows CVM due to high ... 512
- Port Problem Cause Remote Connection Failure ... 518
- Linux Instance-related ... 519
- Unable to Log in to a Linux Instance ... 519
- Unabling to Log in to the Linux Instance Via SSH ... 522
- Unabling to Log in Due to High CPU and Memory Usage of the Linux System ... 524
- The Server Is Isolated and Cannot Be Logged In ... 529
- High Bandwidth Usage Prevents Log-in ... 530
- Failing to Shut Down or Restart CVM ... 536
- Unable to Create Network Namespace ... 539
- Kernel and IO Related Problems ... 541
- Network-related Failures ... 543
- Unabling to Access Website ... 543
- High Website Latency ... 547
- CVM Network Delay and Packet Loss ... 549
- CVM Network Access Packet Loss ... 553
- Unable to ping the instance IP address ... 557
- Domain Name Cannot Be Resolved (CentOS 6.x system) ... 559
- FAQs ... 561
- General
- Storage ... 561
- System Disk and Data Disk ... 561
- Backup and Restoration ... 565
- Image
- CVM Dedicated Host ... 566
- Instance Related ... 566
- Network and Security ... 568
- Network ... 568
- Passwords and Keys ... 570
- IP Address ... 572
- Elastic IP ... 573
- Elastic Network Interface ... 575
- Firewall ... 577
- API Documentation ... 581
- Cloud Virtual Machine(cvm) ... 581
- version(2017-03-12) ... 581
- API overview ... 581
- CallingMethod ... 586
- signaturev1 ... 586
- signaturev3 ... 594
- request ... 603
- result ... 604
- PublicParameter ... 607

- CDH APIs ... 609
  - DescribeZoneHostConfigInfos ... 609
  - InquiryPriceAllocateHosts ... 611
  - TerminateHosts ... 612
- Image APIs ... 614
  - CreateImage ... 614
  - DeleteImages ... 616
  - DescribeImageQuota ... 618
  - DescribeImageSharePermission ... 620
  - DescribeImageSnapshotStatus ... 622
  - DescribeImages ... 624
  - DescribeImportImageOs ... 625
  - ImportImage ... 626
  - ModifyImageAttribute ... 628
  - ModifyImageSharePermission ... 630
  - SyncImages ... 631
- Instance APIs ... 633
  - CloneInstance ... 633
  - CreateDiagnosticReports ... 634
  - CreateDisasterRecoverGroup ... 636
  - DeleteDisasterRecoverGroup ... 638
  - DeleteDisasterRecoverGroups ... 639
  - DescribeDiagnosticReports ... 640
  - DescribeDisasterRecoverGroupQuota ... 642
  - DescribeDisasterRecoverGroups ... 644
  - DescribeInstanceConfigInfos ... 645
  - DescribeInstanceFamilyConfigs ... 646
  - DescribeInstanceInternetBandwidthConfigs ... 648
  - DescribeInstanceTypeConfigs ... 649
  - DescribeInstanceTypeDisasterGroupBlackList ... 650
  - DescribeInstanceUsbInfo ... 651
  - DescribeInstanceVncUrl ... 653
  - DescribeInstances ... 655
  - DescribeInstancesDeniedActions ... 656
  - DescribeInstancesModification ... 657
  - DescribeInstancesStatus ... 658
  - DescribeZoneInstanceConfigInfos ... 659
  - GetRecycleInfo ... 660
  - ImportSnapshot ... 662
  - InquiryPriceRenewInstances ... 664
  - InquiryPriceResetInstance ... 665
  - InquiryPriceResetInstancesInternetMaxBandwidth ... 666
  - InquiryPriceResetInstancesType ... 667
  - InquiryPriceResizeInstanceDisks ... 668
  - InquiryPriceRunInstances ... 669
  - InquiryResourceResetInstancesType ... 670
  - InstanceAttachISO ... 671
  - InstanceDetachISO ... 673
  - ModifyDisasterRecoverGroup ... 675
  - ModifyInstancesAttribute ... 676
  - ModifyInstancesDisasterRecoverGroup ... 677
  - ModifyInstancesRenewFlag ... 678
  - ModifyInstancesVpcAttribute ... 679
  - RebootInstances ... 680
  - RemoveInstancesDisasterRecoverGroup ... 681
  - RenewInstances ... 683
  - ResetInstance ... 684
  - ResetInstancesInternetMaxBandwidth ... 685
  - ResetInstancesPassword ... 686
  - ResetInstancesType ... 687
  - ResizeInstanceDisks ... 688
  - RunInstances ... 689
  - StartInstances ... 690
  - StopInstances ... 691
  - SwitchParameterRunInstances ... 692
  - TerminateInstances ... 696
  - ViewModifyInstancesAttribute ... 697
- Instance Launch Template APIs ... 698
  - CreateLaunchTemplate ... 698
  - DeleteLaunchTemplate ... 699
  - DeleteLaunchTemplates ... 701
  - DescribeLaunchTemplatesInfo ... 703
  - ModifyLaunchTemplate ... 704
  - ModifyLaunchTemplateName ... 705
- Key APIs ... 707
  - AssociateInstancesKeyPairs ... 707
  - CreateKeyPair ... 708
  - DeleteKeyPairs ... 709
  - DescribeKeyPairs ... 711
  - DisassociateInstancesKeyPairs ... 712
  - ImportKeyPair ... 713
  - ModifyKeyPairAttribute ... 714
- Other APIs ... 716
  - CreateHpcCluster ... 716
  - DeleteHpcClusters ... 718
  - DescribeHpcClusters ... 720
  - ModifyHpcClusterAttribute ... 722
- Region APIs ... 724
  - DescribeRegions ... 724
  - DescribeZones ... 726
- Data structure ... 728

- ErrorCode ... 743
- Service Migration(csm) ... 752
  - version(2021-09-15) ... 752
    - API overview ... 752
    - CallingMethod ... 754
      - signaturev1 ... 754
      - signaturev3 ... 762
      - request ... 771
      - result ... 772
      - PublicParameter ... 775
    - Instance APIs ... 777
      - CreateImageForTransitInstance ... 777
      - CreateTransitInstance ... 779
      - DescribeTransitInstance ... 781
      - ExitLiveMigrateLhInstance ... 783
      - LiveMigrateLhInstance ... 785
      - TerminateTransitInstance ... 787
    - Migration Source APIs ... 789
      - CreateSourceServer ... 789
      - DeleteSourceServer ... 790
      - DescribeSourceServerDeniedActions ... 792
      - DescribeSourceServers ... 794
      - ModifySourceServer ... 796
    - Task APIs ... 797
      - CreateMigrationJob ... 797
      - DeleteMigrationJob ... 798
      - DescribeMigrationJobDeniedActions ... 800
      - DescribeMigrationJobs ... 802
      - ModifyMigrationJob ... 804
      - StartMigrationJob ... 805
      - StopMigrationJob ... 807
    - Data structure ... 809
    - ErrorCode ... 813

Product Introduction
CVM Overview

CVM is a flexible and scalable cloud computing service that eliminates the need for upfront investment and resource usage estimation. With CVM, you can quickly launch virtual machines and deploy applications on demand.

Each CVM instance offers full customization — including CPU, memory, storage, network settings, and security configurations — allowing you to tailor resources to your specific needs. You can also scale resources effortlessly to adapt to changing workloads or business requirements.

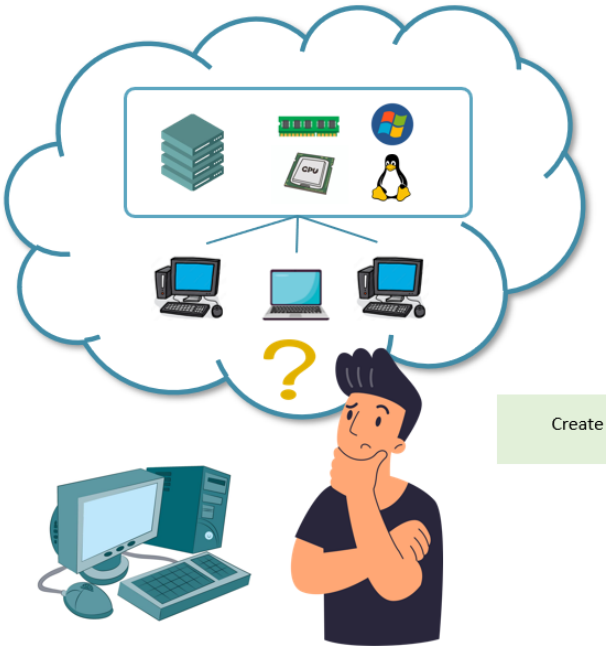
Using CVM Instances

You can configure and manage CVM instances in the following ways:

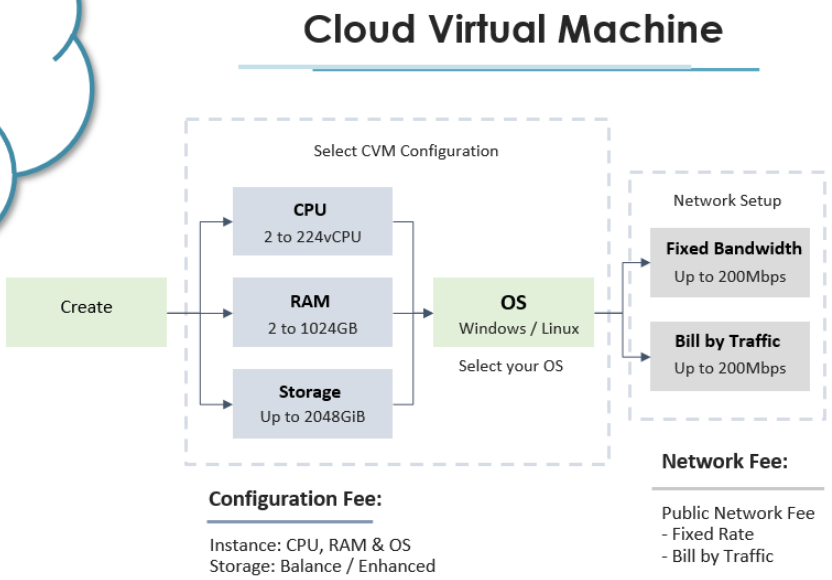
- Console: A web-based UI for configuring and managing CVM instances.
- API: Converge Cloud also provides APIs for configuring and managing CVM instances. For more information, see API Category.
- SDK: You can use SDK or Converge Cloud CLI to call CVM APIs.

CVM Use Cases

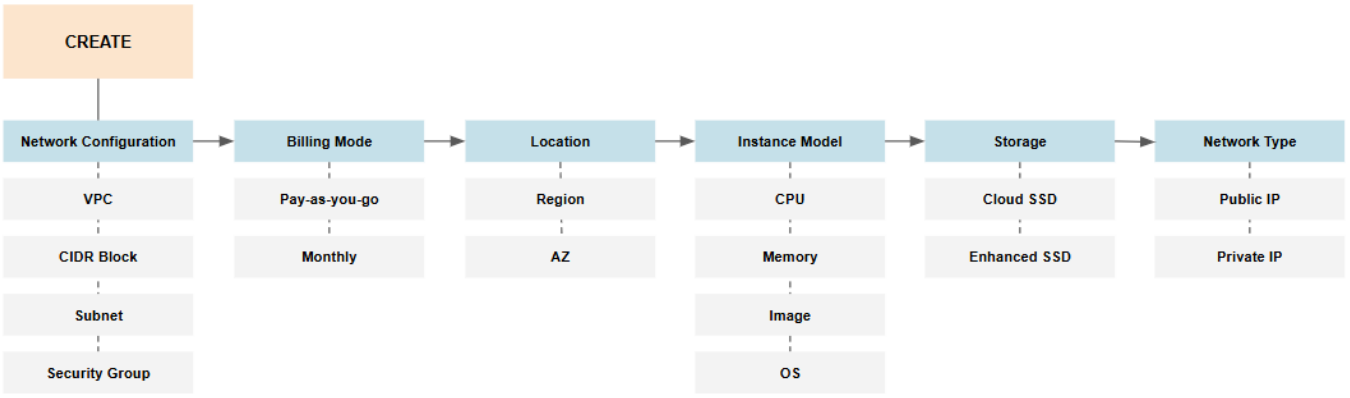
- Streaming media applications for images and videos: CVMs allow you to deploy streaming applications with custom configurations and scale them based on traffic demand, ensuring a seamless viewing experience.
- Development & Testing Environments: Quickly spin up isolated environments for development and testing purposes.
- Small-scale web/app applications and internal corporate websites: Host lightweight applications and internal portals with ease.



Allows users to instantly provision and scale computing resources as needed



CVM Instance Configuration



Key Concepts

1. Instance

A virtual computing resource containing basic computing components such as CPU, memory, OS, network, and disks. Converge Cloud provides various configurations of CPU, memory, storage, and networking capacity for CVM instances. For more information, please see Instance Types.

2. Image

A pre-configured template containing an operating system and applications that CVM instances run on. Converge Cloud CVM provides pre-configured images for Windows, Linux, and other operating systems.

3. Cloud Block Storage

A distributed and persistent block storage device provided by Converge Cloud that can serve as the system disk or an expandable data disk of an instance.

4. Virtual Private Cloud

A logically isolated virtual network space in Converge Cloud.

5. IP Address

Converge Cloud provides Private IP and Public IP addresses. Private IP addresses are for the interconnection of CVM instances within the same LAN, while public IP addresses are for public-facing services.

6. Elastic IP

Static public network IP addresses designed especially for dynamic networks to meet the demands for fast troubleshooting.

7. Security Group

A virtual firewall that features stateful data packet filtering. It is used to configure the network access control of CVMs. Security groups are an important measure for network security and isolation.

Regions and AZs

Regions

Introduction

Region refers to the geographical area of a physical data center. For Converge Cloud, different regions are completely isolated from each other to ensure maximum stability and fault tolerance between regions. To reduce access latency and improve download speed, it is recommended to choose the region closest to your customers.
You can query the list of regions through the API to see the complete list of regions.

Related Characteristics

- Networks in different regions are completely isolated, and cloud services in different regions cannot communicate through the private network by default.
- Cloud services in different regions can access the Internet through public network IP address. Cloud services in Virtual Private Cloud (VPC) can also communicate via Peering Connection provided by Converge Cloud over the Converge Cloud NSFCNET for a more stable and faster interconnection than Internet access.
- Cloud Load Balancer (CLB) currently defaults to supporting intra-region traffic forwarding and binding with CVMs within the same local region. If the cross-region binding feature is enabled, it enables CLB to bind CVMs across regions.

> Note:
> Regions that comply with the regulatory requirements of the financial industry have strengths of high security and strong isolation. Currently, services such as CVM, financial database, redis for storage, and face recognition are provided for such regions. Certified financial customers who need to use such regions can submit a ticket.

AZs

Introduction

Availability Zone (AZ) refers to the Converge Cloud physical data centers within the same region but with independent power supply and network. The goal is to ensure that failures within the availability zones are isolated from each other (except for major disasters or power failures) preventing fault propagation and ensuring that users' businesses continue to provide online services. By launching instances in independent

availability zones, users can protect applications from the impact of single-location failures.
You can query the list of availability zones.

Related Characteristics

Cloud services in different availability zones within the same region, but in the same VPC, can interconnect through the private network and can be accessed directly using private network IP addresses.

> Note:
> Intranet interconnection refers to the interconnection of resources under the same account, and the resources of different accounts are completely isolated from each other on the intranet.

How to Choose Regions and AZs?

When choosing regions and availability zones, you need to consider the following factors:

- The region where your CVM is located, and the geographical location of you and your target users. It is recommended that you choose the region closest to your customers when purchasing CVMs, to reduce access latency and improve access speed.
- Relationship between CVMs and other cloud services.
  It is recommended that you choose other cloud services with the same availability zone in the same region. Then the cloud products can communicate through the private network to reduce access latency and improve access speed.
- Considerations on business high availability and disaster recovery.
  Even if there is only one VPC, it is recommended that you deploy services at least in different availability zones to ensure fault isolation between availability zones and enable cross-availability zone disaster recovery.
- Communications between different availability zones may have network communication delays. This needs to be evaluated in combination with the actual needs of services to find the best balance between high availability and low latency.
- If you need to access hosts in other countries and districts, it is recommended that you select CVMs in other countries and districts. If you create a CVM in Converge Cloud's available regions, accessing hosts in other countries and districts will have high access latency. It is not recommended for such usage.

Resource Position Description

This document explains which Converge Cloud resources are global, which are region-specific but not

distinguished by availability zones, and which are based on availability zones.

Resources	Resource ID Format : 8-digit numbers and characters.	Type	Note
User account	Unlimited.	Unique globally.	Users can use the same account to access Converge Cloud resources around the world.
SSH Key	skey-xxxxxxxx	Available for all regions.	Users can use the SSH key to bind CVMs in any region under their account.
CVM Instance	ins-xxxxxxxx	Used only in a single availability zone of a single region.	Users can only create CVM instances in availability zones.
Custom Image	img-xxxxxxxx	Available for multiple availability zones in a single region.	Users can create custom images of instances and use them under different availability zones in the same region. If you need to use it in other regions, replicate the custom image to another region by using the image replication feature.
Elastic IP	eip-xxxxxxxx	Available for multiple availability zones in a single region.	EIP addresses are created in a certain region, and can only be associated with instances from the same region.
Security Group	sg-xxxxxxxx	Available for multiple availability zones in a single region.	Security groups are created in a certain region, and can only be associated with instances from the same region. Converge Cloud automatically creates three default security groups for the user.
CBS	disk-xxxxxxxx	Used only in a single availability zone of a single region.	Users can only create CBS under a specific availability zone and mount them on instances of the same availability zone.
Snapshot	snap-xxxxxxxx	Available for multiple availability zones in a single region.	After a snapshot is created for a certain CBS, users can use the snapshot to perform other operations (such as creating CBS) in this region.

Resources	Resource ID Format : 8-digit numbers and characters.	Type	Note
CLB	clb-xxxxxxxx	Available for multiple availability zones in a single region.	CLB can bind CVMs in different availability zones of a single region for traffic forwarding.
VPC	vpc-xxxxxxxx	Available for multiple availability zones in a single region.	A VPC is created in a certain region, and resources belonging to the same VPC can be created in different availability zones.
Subnet	subnet-xxxxxxxx	Used only in a single availability zone of a single region.	Users cannot create subnets across availability zones.
Route Table	rtb-xxxxxxxx	Available for multiple availability zones in a single region.	The user needs to specify a specific VPC when creating a routing table. Thus it adheres to the position attributes of the specified VPC.

Related Operations

Migrating Instances to Other Availability Zones

An instance that has been started cannot change its availability zone, but users can migrate the instance to another availability zone in other ways. The migration process includes creating a custom image from the original instance, starting the instance in the new availability zone using the custom image, and updating the configuration of the new instance.

1. Create a custom image of the current instance.
2. If the network environment of the current instance is a VPC and the current private IP address needs to be retained after migration, users can first delete the subnet in the current availability zone and then create a subnet in the new availability zone with the same IP address range as the original subnet. Only subnets that do not contain available instances can be deleted. Therefore, all instances in the current subnet should be moved to the new subnet.
3. Create an instance in the new availability zone using the custom image you just created. You can

select the same instance type and configuration as the original instance or select a new instance type and configuration.

4. If the original instance has been associated with an EIP address, it is disassociated from the old instance and associated with the new instance.
5. (Optional) If the original instance is of pay-as-you-go billing mode, you may choose to terminate it.

Replicating an Image to Other Regions

The actions, such as starting and viewing instances, are distinguished by region attribute. If the image of the instance to be started does not exist in the local region, you need to replicate the image to the local region.

Features and Advantages

Comprehensiveness

Cloud Virtual Machine (CVM) offers you a comprehensive range of services.

- Multi-region and Multi-availability Zones: Deploy applications in a region close to your users to achieve a lower delay.
- Multiple Machine Models:
  - Standard Type (Suitable for small and medium-sized Web applications and small and medium-sized databases).
  - MEM-Optimized Type (Suitable for applications that require a lot of memory operations, searches, and calculations).
  - High IO Type (Suitable for low-delay, I/O-intensive applications).
  - Computing (Suitable for large game servers and advertising service engines, high-performance computing, and other compute-intensive applications).
  - Big Data Type (Suitable for throughput-intensive applications such as Hadoop distributed computing, massive log processing, distributed file systems, and large data warehouses).
  - Heterogeneous Type (suitable for high-performance applications such as deep learning, scientific computing, video codec, graphics workstations, etc.).
  - Cloud Bare Metal (CBM) offers enhanced computing power with no performance overhead and provides physical server–level security isolation, fully meeting enterprise demands for data security, regulatory compliance, and service reliability.

Elastic

We are committed to building the most flexible CVM management platform in the industry, providing the following capabilities:

- Hardware Configuration: CVMs based on CBS allow instant upgrading/downgrading of hardware configurations.
- Disk Change: CVMs based on CBS allow instant scale-out of disks.
- Network Bandwidth: CVM allows instant upgrading/downgrading bandwidth.
- Operating System: The CVMs can switch between Windows and Linux systems at any time.
- Elastic IP: Supports binding hosts in various network environments.
- Image Type: Public images (various Linux and Windows operating system types), custom images (images created by users through the image creation feature), and support for cross-regional adjustment and image replication.

- Customizable Network Architecture: VPC offers users independent network environments, tailored IP ranges and addresses, as well as personalized routing policies.
  Provides port-level access control to achieve comprehensive network logical isolation.

Reliable

Committed to building the most reliable CVM in the industry.

- CVM Reliability: Host service availability is 99.95%, data reliability is 99.9999999%. Supporting seamless failover migration, data snapshots, automatic alarms, and other features to safeguard your servers.
- CBS Policy: Provides a three-replica professional storage policy to eliminate single points of fault and ensure data reliability, allowing you to safely store your data in the cloud without worrying about data loss.
- Stable Network Architecture: Mature network virtualization technology and network interface binding technology ensure high network availability. Running in T3+ and above data centers ensures the reliability of the operating environment, freeing you from worries about network availability.

Fast

Whether in terms of user operation or CVM performance, we are committed to providing fast and convenient services.

- Easy and Fast Operation: You can easily obtain one, hundreds, or even thousands of server instances in just a few minutes. You can purchase, configure, scale, and manage your services with one click.
- Fast Public Network: More than 20 BGP public networks, covering almost all network operators. No matter which ISP your customers use, they can enjoy the same extremely fast bandwidth experience. Optional public network bandwidth up to 200 Mbps, with failover within seconds.
- Excellent Private Network: Featuring seamless interconnectivity among IDCs within the same region, with an underlying network capable of reaching speeds up to 10 Gbps or 1 Gbps, we guarantee the quality of private network communication.

Secure

The cloud platform offers multiple schemes to ensure the security of CVMs, along with backup and rollback mechanisms to safeguard data security.

- Multiple ways to remotely log in to the CVM: Provides multiple log-in methods, including key log-

in, password log-in, VNC log-in, etc.
- Cloud Monitor: Supports various types of real-time alarms.
- Recycle bin protection mechanism: Allows CVMs to enter the recycle bin for a period of time before being released, helping prevent major issues such as data loss caused by immediate termination.
- Customized Access Control: Customizes host and network access policies through security groups and network ACLs and flexibly sets different firewalls for different instances.
  The security service has the following characteristics:
- Comprehensive Security Guard
  Provides integrated security services for CVMs, including health checks (such as vulnerability scanning, WebShell detection, web backdoor detection, and port security inspection) and security protection (such as intrusion detection and access control) to ensure data security and user privacy.
- Real-time Alarm and Regular Analysis
  24/7 security service, discover vulnerabilities as soon as possible and notify you in real time.
- Convenient and Secure
  No need to purchase expensive security equipment for your cloud service, you can enjoy Cloud Security service for free when you create cloud service. One-click activation, zero deployment, convenient and simple.
- Professional Team, Reliable Guarantee
  Cloud Security is created by a security team with many years of security experience and training. It provides professional security services to cloud service users and is worthy of your trust.

Easy to Use

Officially certified application software and Ops tools help you to operate and maintain conveniently, so you no longer have to worry about management tools.

- CVM provides a web-based user interface, the console, which can be used to start, adjust configurations, and reinstall the system on CVM instances just like physical machines. If you have registered a Converge Cloud account, you can log in to the CVM console directly to operate your CVM.

Cost-effective

The cloud platform lets you save on IT investment, simplify O&M operations.

- You only pay for what you need. No up-front investment, no infrastructure, no preparation, helping you effectively reduce your infrastructure construction investment.

Use Cases

Cloud Virtual Machine (CVM) provides stable, secure, flexible, and high-performance cloud computing services with a broad range of use cases. It can be used as a standalone Web server, or integrated with other Converge Cloud services to provide comprehensive solutions for users' various businesses. For example, Cloud Object Storage (COS), Virtual Private Cloud (VPC), Cloud Load Balancer (CLB), and etc.

Enterprise websites, small websites/mobile applications, or databases

For corporate websites, small Webs, Apps, or databases that have no special requirements for CPU, memory, bandwidth, and etc., and low traffic in the initial stage, you only need to purchase a low-configuration CVM to run your static web pages, applications, databases, and etc. As the subsequent business grows, you can expand the configuration of the CVM without having to worry about insufficient resources due to a sudden increase in business.

Websites and applications with many images and videos

For use cases (websites and applications) with a large number of images/videos on the pages, you can use Converge Cloud CVM to host websites and applications with a large number of images and videos, integrate with COS, CLB and CDN to achieve low-cost storage of large-capacity data and improve availability, and reduce latency and bandwidth costs.

High IO Applications

For use cases with high demands for disk read/write and latency, such as NoSQL database/memory database/data warehouse/Elasticsearch/data processing application/distributed computing, and etc., you can use a CVM with high random IOPS and high throughput to host your high I/O applications.

Large PC games, high-performance engineering science applications, and video encoding/decoding

Converge Cloud provides high-performance processors and cost-effective CVM, which is suitable for use cases that require high computing resource consumption, such as large-scale PC games/high-performance

engineering science applications/video encoding and decoding and other high-performance parallel computing platforms. Converge Cloud also provides exclusive physical servers, resource isolation, and custom Cloud Virtual Machine for you.

Scenarios requiring high-performance rendering and high graphics processing

Converge Cloud provides CVM with powerful graphics processing capabilities, suitable for scenes with high-performance rendering and high graphics processing requirements.

Deployment of Cloud-native (bare metal) Container

The elastic business loads of the Internet are gradually developing towards cloud-native containerization. The new generation of Cloud Bare Metal instances can meet users' performance requirements for physical machines and the native network and storage capabilities of the cloud platform through Elastic Network Interface ENI and Cloud Block Storage CBS, in combination with the VPC-CNI mode of the Kubernetes Engine and public Cloud Load Balancer, and reduce the performance loss caused by the KubeProxy component in forwarding. A single machine can support more than 400 Elastic Network Interfaces and cloud disk mounting, and can support high-density container management. Compared with virtual machines, bare metal containers provide higher deployment density, lower resource overhead, and more agile deployment efficiency. Based on the cloud-native technology, we help customers achieve the goal of reducing cloud costs.

Instance
Instance Overview

Introduction to the Instance

Instance, which can be regarded as Cloud Virtual Machine (CVM), contains the most fundamental computing components such as CPU, memory, operating system, network, and disk.
CVM instances can offer secure and elastic computing services in the cloud to fulfill computing requirements. The instances can expand or contract computing resources in real time as the business needs change. They can significantly reduce the company's software and hardware procurement costs and simplify IT operation and maintenance work.
Different instance types offer different computing and storage capabilities and are applicable to different use cases. Users can select the computing capability, storage and network access mode of the instance according to the scale of the services they need to offer. After the instance is started, the user can use it like a traditional computer, and the user has full control over the instance.

Image of Instance

Image It is a template for configuring the Cloud Virtual Machine software (operating system, pre-installed programs, and etc.). An image provides all the information required to start a Cloud Virtual Machine instance. Requires users to start instances through images. The image can start multiple instances for users to use repeatedly. In layman's terms, an image is the installation disk of Cloud Virtual Machine.
The images include the following types.

- Public images: Available to all users, and applicable to most mainstream operating systems.
- Custom images: Only available to the creator and users that share the images, and the images are created by existing running instances or imported from external sources.
- Shared images: Images offered by other users, which can only be used to create instances.

Storage of Instance

The storage of the instance is similar to that of an ordinary Cloud Virtual Machine, and it includes a system disk and a data disk.

- System disk: Similar to the C Drive in the Windows system. The system disk contains a complete copy of the image used for starting the instance, as well as the instance operating environment. Before

starting up, you must select a system disk size that is larger than that of the used image.
- Data disk: Similar to the D Drive and E Drive under the Windows system. The data disk stores the user data and supports free expansion, mounting and unmounting.
  Both system disks and data disks can use different storage types provided by the cloud platform.

Instance Security

The instance security protection means provided by Converge Cloud are as follows.

- Policy control: When the same set of cloud resources needs to be controlled by multiple different accounts, users can use policy control to manage access permissions to cloud resources.
- Security group: Control access by using security groups to allow trusted addresses to access instances.
- Log In control: Use SSH keys whenever possible to log in to the user's Linux instance, and use password to log in to the instance that needs to change the password from time to time.

Specification

When creating a Cloud Virtual Machine on the cloud platform, the instance type specified by the user determines the host hardware configuration of the instance. Each instance type provides different computing, memory and storage functions. Users can select an appropriate instance type based on the scale of applications they need to deploy. These instance families consist of different combinations of CPU, memory, storage, heterogeneous hardware, and network bandwidth, giving you the flexibility to choose the appropriate resources for your application.

Instance Type

There are multiple types of cloud platform instance families, and the specific specifications are subject to actual sales. This document takes the standard S2 and the Cloud Bare Metal BMS5 as examples.

Instance Limits

- There is a limit to the total number of instances that can be launched in a region.
- There is a limit to the total number of system disks and data disks mounted to an instance. To ensure the IO performance of disks, the cloud platform has some restrictions on the size, quantity, and type of data disks purchased with the instance. Please refer to the disk matching module of the corresponding instance family. If necessary, you can purchase an independent Cloud Block Storage to circumvent the disk restrictions of instances.
- Please pay attention to the private network bandwidth capability corresponding to the instance specification, i.e., the upper limit of the maximum private network bandwidth of the instance specification. When the traffic of the private network exceeds the limit, random packet loss may occur in the the private network of the instance.

Standard instance family

Standard instances have a balance of computing, memory and network resources, and can meet the application resource requirements in most scenes.

Standard S2

Standard S2 instances are a newer generation of standard instances. Standard S2 instances offer balanced

computing, memory and network resources, and they are a good choice for many applications.
Standard S2 instances adopt Intel® Xeon® Broadwell processors, which improve integer and floating-point computing performance by 40%; with DDR4 memory, the performance is improved by 30%; and the network sending and receiving capacity can reach up to 400,000 pps.

Specification	vCPU	Memory (GB)	Private Network Bandwidth Capacity (Gbps)
S2.SMALL1	1	1	1.5
S2.SMALL2	1	2	1.5
S2.SMALL4	1	4	1.5
S2.MEDIUM4	2	4	1.5
S2.MEDIUM8	2	8	1.5
S2.MEDIUM2	2	2	1.5
S2.LARGE8	4	8	1.5
S2.LARGE16	4	16	1.5
S2.2XLARGE16	8	16	1.5
S2.2XLARGE32	8	32	1.5
S2.2XLARGE8	8	8	1.5
S2.2XLARGE64	8	64	1.5
S2.3XLARGE24	12	24	2.5
S2.3XLARGE48	12	48	2.5
S2.4XLARGE32	16	32	3.0
S2.4XLARGE48	16	48	3.0
S2.4XLARGE64	16	64	3.0
S2.6XLARGE48	24	48	4.5
S2.6XLARGE96	24	96	4.5
S2.8XLARGE64	32	64	6.0
S2.8XLARGE128	32	128	6.0

Characteristics of Instance

- 2.4 GHz Intel Xeon E5-2680 Broadwell (v4) processor, DDR4 memory.
- The CPU performance is improved by 20% compared with the Series 1 Standard S1.
- The network's sending and receiving capacity can reach up to 400,000 pps.
- The storage can be local disks, common cloud disks, and SSD cloud disks.
- Balance of computing, memory, and network resources.

Application Scenario

It is used for small and medium-sized databases and data processing tasks that require additional memory, as well as cache clusters. It is also used for back-end servers running SAP, Microsoft SharePoint, cluster computing, and other enterprise applications.

Instance Requirements

- Supports launching S2 instances in the Virtual Private Cloud.
- S2 instances support purchasing configurations. Please refer to the instance specifications above.
- Make sure that the size of the S2 instance you choose meets the minimum CPU memory requirements of your operating system and applications. In many use cases, a larger instance size may be required for operating systems with graphical user interfaces that consume large amounts of memory and CPU resources (for example, Windows). As your workload has growing requirements for memory and CPU over time, you can scale up to a higher configuration or choose new instance types.

Standard BMS5

The standard BMS5 instance is the latest generation of Intel standard instance. It is based on the brand new generation of Cloud Bare Metal architecture and provides extreme computing, network, and storage performance through chip fast-path acceleration. There is no virtualization loss in computing performance, and nested virtualization is supported.

Specification	vCPU	Memory (GB)	Private Network Bandwidth Capacity (Gbps)
BMS5	208	768	40

Application Scenario

Standard BMS5 instances can be applied to enterprise-level applications of various types and sizes; medium and large database systems, caches, and search clusters; scenes with high network packet transmission and reception, such as video barrage, live broadcasts, and games; and applications that are sensitive to single-core performance, such as video encoding and decoding and video rendering.

Hardware specifications

Based on Star Lake servers, it provides reliable, secure and stable high-performance computing services.
CPU: 2.6GHz Intel® Xeon® Cooper Lake processor, turbo frequency 3.2GHz.
Memory: Equipped with six-channel DDR4 memory.
Storage: Cloud Block Storage can be used as system disks and data disks, and can be scaled up as needed.
Network: Supports 40Gbps private network bandwidth and has ultra-high network packet sending and receiving capabilities. Supports elastic network interface mounting.

Lifecycle

The lifecycle of a Cloud Virtual Machine instance refers to all states from the start of the instance to its release. By managing instances properly from enabling to disabling instances, applications running on instances can provide services efficiently and economically.

Instance State

- The states of an instance are as follows.

Status Name	Status Attributes	Status Description
Creating	Intermediate State	After the instance is created, it enters the status before it is running.
Running	Steady State	The iThe lifecycle of a Cloud Virtual Machine instance refers to all states from the start of the instance to its release. By managing instances properly from enabling to disabling instances, applications running on instances can provide services efficiently and economically.

Instance State

- The states of an instance are as follows.

Status Name	Status Attributes	Status Description
Creating	Intermediate State	After the instance is created, it enters the status before it is running.
Running	Steady State	The instance is running properly. Your business can be run on this instance.
Restarting	Intermediate State	The instance enters the state before it is running after being restarted by the console or through the API. If this state is maintained for a long time, exceptions may occur.
Resetting	Intermediate State	The instance enters the state before it is running after the reinstall operation or the reset disk operation is performed in the console or through the API.

Status Name	Status Attributes	Status Description
Shutting down	Intermediate State	The instance enters the state before it is shut down after being shut down by the console or through the API. If this state is maintained for a long time, it indicates an exception. Forced shutdown is not recommended.
Shut Down	Steady State	The instance is stopped normally. An instance in a shutdown state cannot provide services. Some attributes of the instance can only be modified when the system is shut down.
Terminating	Intermediate State	The instance has not been terminated 7 days after its expiration or after the user actively performs the termination.
Released	Steady State	The release operation is completed. The instance does not exist, and services are unavailable, and the data is completely cleared.

Launch an Instance

- The instance enters the creating state after the it is started. The hardware for the instance being created is configured according to the specified instance specifications), and the system starts the instance by using the image specified at the startup.
- The instance enters the running state after it is created. Instances in the running state enable normal connections and access services.

Restart an Instance

It is recommended to choose to restart an instance by using the Converge Cloud console or Converge Cloud API instead of running the restart command of the operating system in the instance.

- The instance enters the restarting state after the restart an instance operation is performed.
- Restarting an instance is equivalent to restarting a computer. After the instance is restarted, it still retains its public IP address, private IP address, and all data on its hard disk.
- Restarting an instance usually takes from tens of seconds to several minutes, depending on the instance configuration.

Shutdown an Instance

Users can use the console or API to shut an instance down.

- Shutting down an instance is equivalent to turning off your computer.
- After the instance is shut down, it will no longer provide services, but the billing will not stop.
- An instance being shut down is still displayed in the console.
- Shutting down an instance is a prerequisite for some configuration operations, such as adjusting hardware configuration and resetting passwords.
- The shutdown operation itself does not change the public network IP address, private IP address of the Cloud Virtual Machine and all the data on its hard disk.

Terminate or Release an Instance

When users no longer needs a Cloud Virtual Machine instance, they can terminate and release the instance. The termination and release can be achieved by using the Converge Cloud console or Converge Cloud API.

- Manual termination: For an instance with no outstanding payments, you can choose to manually terminate it.
- When an instance is terminated, the instance's system disk and the data disk specified at the time of purchase is released, but the elastic cloud disk mounted on it is not affected.

Restarting	Intermediate State	The instance enters the state before it is running after being restarted by the console or through the API. If this state is maintained for a long time, exceptions may occur.
Resetting	Intermediate State	The instance enters the state before it is running after the reinstall operation or the reset disk operation is performed in the console or through the API.
Shutting down	Intermediate State	The instance enters the state before it is shut down after being shut down by the console or through the API. If this state is maintained for a long time, it indicates an exception. Forced shutdown is not recommended.
Shut Down	Steady State	The instance is stopped normally. An instance in a shutdown state cannot provide services. Some attributes of the instance can only be modified when the system is shut down.
Terminating	Intermediate State	The instance has not been terminated 7 days after its expiration or after the user actively performs the termination.
Released	Steady State	The release operation is completed. The instance does not exist, and services are unavailable, and the data is completely cleared.

Launch an Instance

- The instance enters the creating state after the it is started. The hardware for the instance being created is configured according to the specified instance specifications, and the system starts the instance by using the image specified at the startup.
- The instance enters the running state after it is created. Instances in the running state enable normal

connections and access services.

Restart an Instance

It is recommended to choose to restart an instance by using the Converge Cloud console or Converge Cloud API instead of running the restart command of the operating system in the instance.

- The instance enters the restarting state after the restart an instance operation is performed.
- Restarting an instance is equivalent to restarting a computer. After the instance is restarted, it still retains its public IP address, private IP address, and all data on its hard disk.
- Restarting an instance usually takes from tens of seconds to several minutes, depending on the instance configuration.

Shutdown an Instance

Users can use the console or API to shut an instance down.

- Shutting down an instance is equivalent to turning off your computer.
- After the instance is shut down, it will no longer provide services, but the billing will not stop.
- An instance being shut down is still displayed in the console.
- Shutting down an instance is a prerequisite for some configuration operations, such as adjusting hardware configuration and resetting passwords.
- The shutdown operation itself does not change the public network IP address, private IP address of the Cloud Virtual Machine and all the data on its hard disk.

Terminate or Release an Instance

When users no longer needs a Cloud Virtual Machine instance, they can terminate and release the instance. The termination and release can be achieved by using the Converge Cloud console or Converge Cloud API.

- Manual termination: For a Pay-As-You-Go instance with no outstanding payments, you can choose to manually terminate it.
- When an instance is terminated, the instance's system disk and the data disk specified at the time of purchase is released, but the elastic cloud disk mounted on it is not affected.

Storage
Storage Overview

We provide various types of data storage devices that are flexible, economical, and easy to use for Cloud Virtual Machine instances. Different storage devices have different performance and prices and are suitable for different use cases.

Storage device classification

Storage devices can be divided into the following categories according to different classification dimensions.

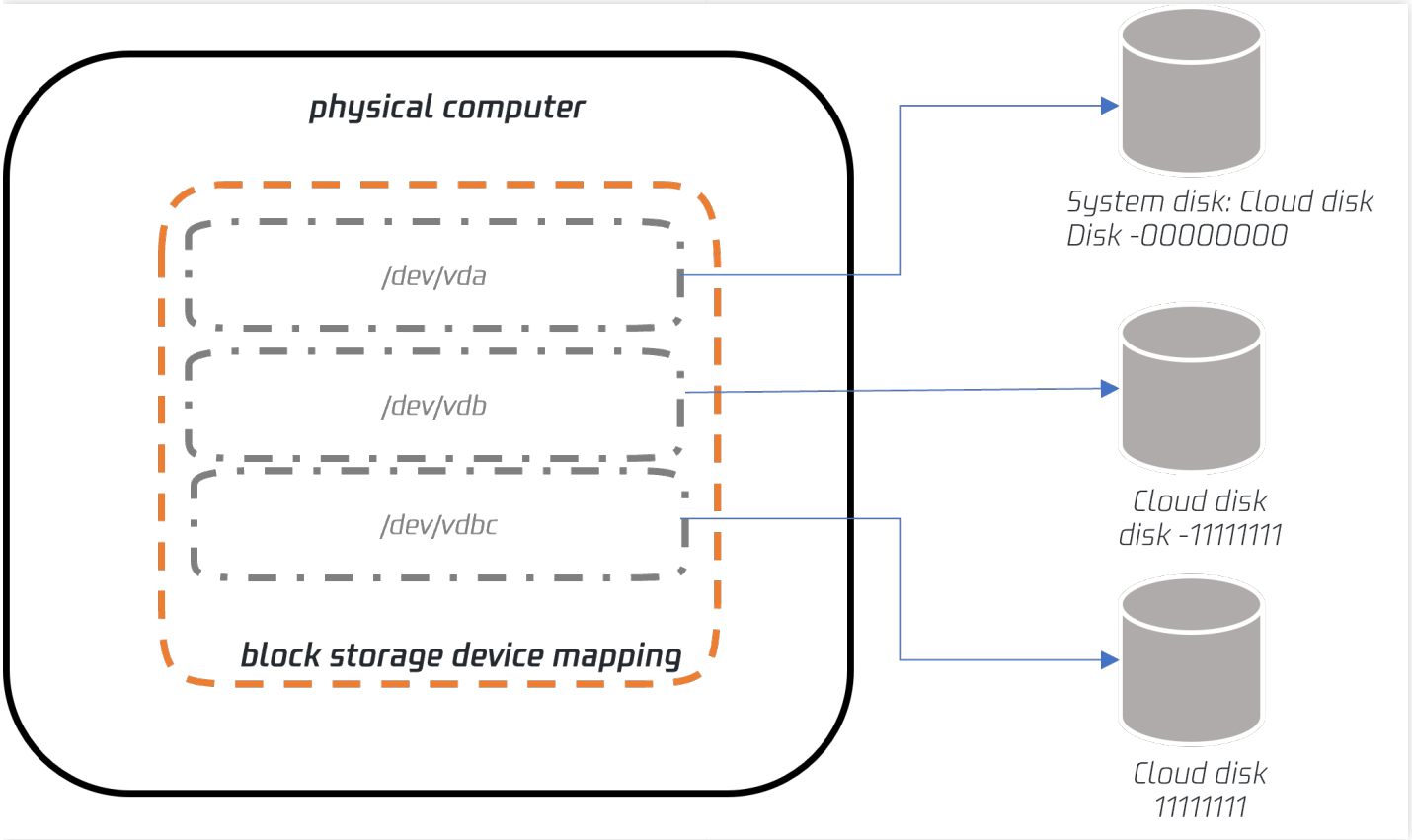
Division dimensions	Classification	Note
Storage Media	General Hard Disks	The storage medium is a mechanical hard disk. Its characteristics are low price and better reading and writing speed.
Storage Media	SSD Hard Disks	The storage medium is a solid state drive (SSD). It is characterized by excellent performance in IOPS and reading and writing speed, and can achieve up to 20 times the IOPS and 16 times the throughput of ordinary hard disks. The price is higher than ordinary hard disks.
Storage Media	Efficient cloud disk	Mixed storage types. It is suitable for small and medium-sized use cases such as Web/App servers, business logic processing, and small and medium-sized website construction with high data reliability requirements and ordinary moderate performance requirements.
Application Scenario	System Disk	A collection of systems used to store, control, and schedule Cloud Virtual Machine operations by using images.
Application Scenario	Data Disk	Used to store all user data.
Architecture Patterns	Cloud Block Storage	Cloud Block Storage is a flexible, highly available, highly reliable, low-cost, customizable network block device that can be used as an independent, scalable hard disk for the Cloud Virtual Machine. It provides data block-level data storage and adopts a three-copy distributed mechanism to ensure data reliability for CVM. If the CVM has a Cloud Block Storage, the hardware, disk, and

Division dimensions	Classification	Note
		network can be adjusted.
Architecture Patterns	Local Disk	The local disk is a part of the local storage of the physical machine where the CVM instance is located. It is a storage area of the local storage of the physical machine where the CVM instance is located. Data access can achieve lower latency, but there is a risk of single point failure of data. The hardware (CPU, memory, and disks) upgrade is not available for the CVM that uses local disks, but the bandwidth upgrade is supported.
Architecture Patterns	Cloud Object Storage	Cloud Object Storage is a data storage device located on the Internet that supports retrieval of data from a Cloud Virtual Machine instance or anywhere on the Internet, thereby reducing storage costs. Not suitable as a storage medium for low-latency, high-IO scenes.

Block storage device mapping

Each instance has a system disk to ensure basic operating data, and more data disks can be mounted to the instance. Instances use block storage device mapping to map these storage devices to locations that they can recognize.

Block storage is a storage device that is divided into blocks of bytes and supports random access. The cloud platform supports two types of block storage devices, that is, local disks and Cloud Block Storage.



This figure shows how CBS maps block storage devices to the Cloud Virtual Machine: Map /dev/vda to the system disk, and map the two data disks to /dev/vdb and /dev/vdc .

The Cloud Virtual Machine instance automatically creates block storage device mappings for local disks and Cloud Block Storage mounted to the instance.

Cloud Block Storage

Cloud Block Storage (CBS) provides you with persistent data block-level storage services for Cloud Virtual Machines.

- The data in the Cloud Block Storage is automatically stored in multiple copies within the availability zone, avoiding the risk of single point failure of data and providing up to 99.9999999% data reliability.
- Cloud Block Storage provides disk instances of various types and specifications to meet the requirements of stable and low-latency storage performance.
- Cloud Block Storage can be mounted/unmounted on instances in the same availability zone, and storage capacity can be adjusted within minutes to meet flexible data needs. You only need to pay a fair price for the configured resources to enjoy the above features.

Typical use cases

- If the Cloud Virtual Machine is found to have insufficient hard disk storage capacity during use, you can purchase one or more Cloud Block Storages and mount them to the Cloud Virtual Machine to meet the storage capacity requirements.
- No additional storage space is required when purchasing a Cloud Virtual Machine. When storage needs arise, the storage capacity of the Cloud Virtual Machine can be scaled up by purchasing a Cloud Block Storage.
- When there is a demand for data exchange among multiple Cloud Virtual Machines, the demand can be fulfilled by unmounting the Cloud Block Storage (data disk) and remounting it to other Cloud Virtual Machines.
- You can purchase multiple Cloud Block Storages and configure LVM (Logical Volume Manager) logical volumes to break the storage capacity upper-limit of a single Cloud Block Storage.
- You can purchase multiple Cloud Block Storages and configure RAID (Redundant Array of Independent Disks) policies to break the I/O capacity upper-limit of a single Cloud Block Storage.

Lifecycle

The lifecycle of elastic Cloud Block Storage is independent of the Cloud Virtual Machine instance and is not affected by the instance operation. You can attach multiple Cloud Block Storages to a single instance, or detach a Cloud Block Storage from an instance and attach it to another instance.

Local Disk

Local Disk Overview

A local disk is a storage device that is located on the same physical server as a Cloud Virtual Machine (CVM) instance and has the characteristics of high reading and writing speed IO and low latency.
The local disk is a part of the local storage of the physical machine where the CVM instance is located. It is a storage area of the local storage of the physical machine where the CVM instance is located. The local disk is a part of a single physical machine. The data reliability depends on the reliability of the physical machine, and there is a risk of single point failure.

> Note:
> - When a hardware failure occurs on the physical machine where the instance is located, there is a risk of data loss on the local disk. We recommend that you perform data redundancy at the application layer to ensure data availability. If your application lacks a data reliability architecture design, we recommend using Cloud Block Storage (CBS) in your instances concurrently to improve data reliability.
> - For Cloud Virtual Machines (CVMs) that only purchase local disks, hardware (CPU, memory, hard disk) upgrades are not supported, only bandwidth upgrades are supported.
> - Currently, local disks can only be used as data disks for CVMs, such as high IO instances.

Applicable Scenario

- Distributed Applications: I/O intensive applications such as NoSQL, MPP data warehouse, and distributed file systems. These applications inherently have distributed data redundancy capabilities.
- Large Online Application Logs: Large online applications generate a significant amount of log data, requiring high-performance storage, while the reliability requirements for storing these logs are not as stringent.

Lifecycle

The lifecycle of a local disk is the same as the CVM instance to which it is mounted. In simple terms, the local disk starts and ends along with the startup and shutdown of the CVM it is mounted to.

Note

Note:
The local disk is the local storage from the physical machine where the mounted CVM instance is located. Currently, it can only be used as a data disk of the CVM. Some types of CVMs, such as high IO instances, need to be equipped with local SSD hard disks to obtain higher I/O read and write performance of the data disk.

Please note that local storage is not suitable for scenarios where there is no data redundancy architecture at the application layer and there is a risk of data loss (for example, when the host machine crashes). We strongly recommend that you use an instance that allows you to select a CBS as a data disk.

Cloud Object Storage

Cloud Object Storage (COS) is a distributed storage service provided by cloud platforms to store massive amounts of files, enabling users to store and access data anytime over the network.
CVM users can store and retrieve data via the instance or anywhere on the Internet. COS redundantly stores user data across multiple regions and allows multiple different clients or application threads to read or write this data simultaneously. COS provides CVM users with a highly scalable, low-cost, reliable, and secure data storage solution.

Image
Image Overview

What Is Image?

Image is a template for CVM software configuration (operating system, pre-installed programs, etc.), which provides all the information required to start a CVM instance. An image provides all the information required to start a Cloud Virtual Machine instance. Requires users to start instances through images. The image can start multiple instances for users to use repeatedly. In layman's terms, an image is the installation disk of Cloud Virtual Machine.

Image Type

The images include the following types.

- Public Image: Available to all users, covering most mainstream operating systems.
- Custom Image: Only available to creators and shared objects, created from an existing running instance or imported from outside.
- Shared Image: Images shared by other users can only be used to create instances.

Image Deployment vs Manual Deployment

	Image Deployment	Manual Deployment
Deployment Time	3 to 5 minutes	1 day - 2 days
Deployment Process	Quickly create a suitable CVM based on the used solutions.	Select the appropriate operating system, database, application software, plugins, etc., and install and debug them.
Security	Except for shared images, which require users to identify their sources, other public images and custom images have been tested and reviewed.	Depends on the level of development and deployment personnel.
Usage	Public Image: genuine operating system, including the initialization components	Completely self-configured, with no basic settings required.

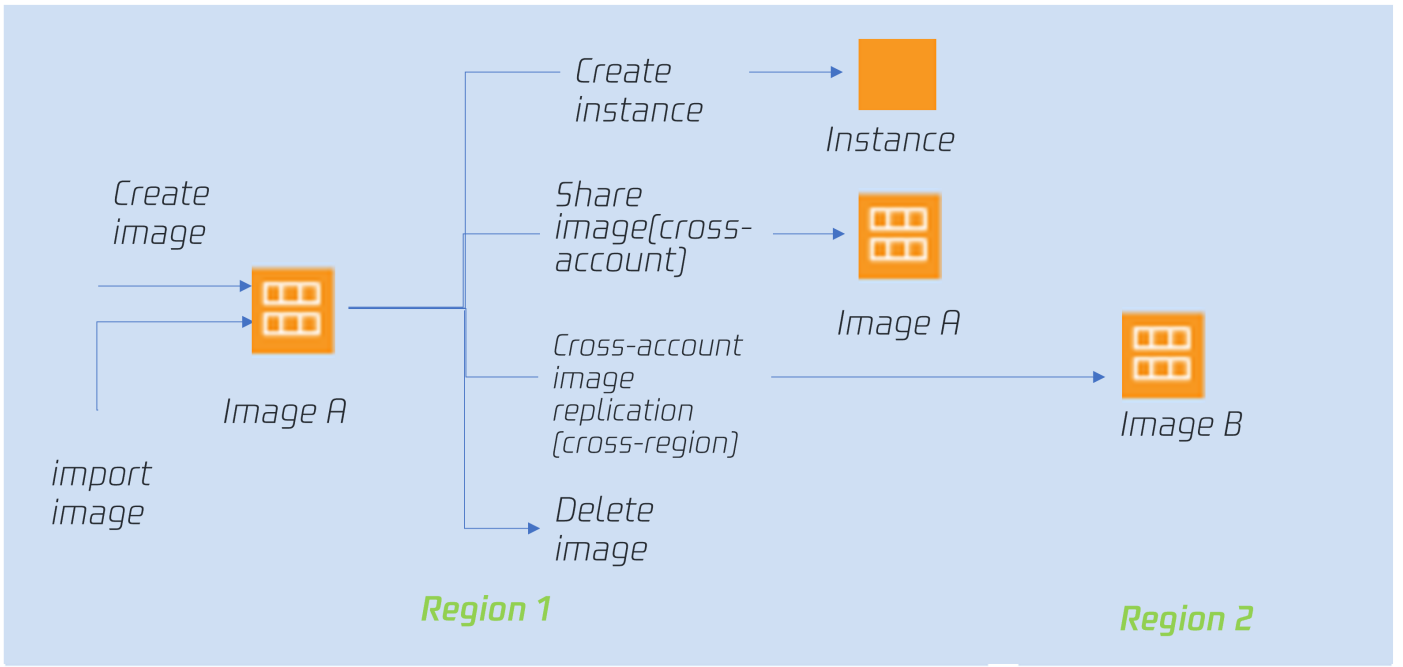
	Image Deployment	Manual Deployment
	provided by Converge Cloud. Custom Image: Quickly create the same software environment as an existing CVM or back up the environment. Shared Images: Quickly create the same software environment as other users' existing CVMs.	

Image Application

- Deployment of Specific Software Environment
  Using shared images or custom images can help quickly set up specific software environments, eliminating the tedious and time-consuming tasks of self-configuring environments and installing software. They can also meet various personalized needs such as website building, application development, and visualization management, making CVMs "ready to use" immediately, saving time, and providing convenience.
- Batch Deployment of Software Environment
  By creating an image for a CVM instance with a deployed environment, and then using the image as the operating system when creating CVM instances in batches, the CVM instance will have the same software environment as the previous CVM instances after it is successfully created, thereby achieving the purpose of batch deployment of software environments.
- Server Operating Environment Backup
  Create an image backup of the operating environment for a CVM instance.
  If the CVM instance cannot run normally due to software environment damage during use, you can use image recovery.

Image Lifecycle

The following diagram summarizes the lifecycle of a custom image. After creating or importing a new custom image, users can use it to launch new instances (users can also launch instances from existing public images). Custom images can be copied to other regions of the same account and become independent images in that region. Users can also share custom images with other users.


Create instance
Instance
Create image
Share image(cross-account)
Image A
Image A
Cross-account image replication (cross-region)
Image B
import image
Delete image
Region 1
Region 2

Type

Users can select images based on the earlier characteristics:

- Location
- Operating System Types
- Architecture (X86 or ARM; 32-bit or 64-bit)
  Depending on the source, the image types include: public image, custom image, and shared image.

Public Image

Public Image is an image officially provided, supported, and maintained by Converge Cloud, including the basic operating system and initialization components provided by Converge Cloud, and can be used by all users.
Public Image Features:

- Operating System Types: free choice (eg: based on Linux type system or Windows type system), and regularly updated.
- Software Support: Integrate the software packages provided by Converge Cloud (such as API, etc.), and support multiple versions of common software such as Java, MySQL, SQL Server, Python, Ruby, and Tomcat, and their full permissions.
- Security: The operating systems provided are completely legal and compliant, and all use official genuine operating systems. Produced by the professional security Ops team within Converge Cloud, it has undergone rigorous testing and offers optional built-in security components.
- Restrictions: no use limits.
- Fees: Except for some images (such as Windows types in overseas regions) that require a certain license fee, the rest are all free.

Custom image

Custom Image It is an image created by the user through the image creation feature or imported through the image import function. Only the creator and the sharer can use it.
Custom Image Features:

- Use Cases: Create an image for a CVM instance that has an application deployed, so that you can quickly create more instances with the same configuration.
- Feature Support: Supports users to create, copy, share, and terminate.
- Restrictions: Each region supports up to 50 custom images.

- Fees: Creation may involve fees. The specific price is based on the price displayed when the instance is created. Cross-region replication of custom images is currently free of charge.

Shared Image

Shared Image refers to a custom image that is shared by another user to the current user through the image-sharing feature.
The shared image will be displayed in the same region as the original image of the shared user.
Shared Image Features:

- Use Cases: Help other users quickly create CVMs.
- Feature Support: Shared images can only be used to create CVMs. Other operations such as modifying the name, copying, and sharing are not allowed.
- Security: Shared images are not reviewed by Converge Cloud and may pose security risks. Therefore, it is strongly recommended not to accept images from unknown sources.
- Restrictions: Each custom image can be shared with up to 50 users. Image sharing only supports sharing to accounts in the same region.

Snapshot

Description

- Real-Time Replica of Online Data
  A snapshot is a fully usable copy of a CBS. When a problem occurs in a CBS for which a snapshot has been created, the snapshot can be used to quickly restore it to its original status. It is recommended that you create a snapshot of the relevant CBS before making major business changes so that data can be quickly restored if the business change fails.

- Persistent Backup of Key Milestones
  Snapshots can serve as persistent backups of business data, preserving milestone status of business data.

- Rapid Business Deployment
  You can use business snapshot files to quickly clone multiple CBSs to quickly deploy servers.

Use Cases

Snapshot is a convenient and efficient data protection service and is recommended for the earlier business scenarios:

- Daily Data Backup
  You can use snapshots to regularly back up important business data to mitigate the risk of data loss caused by misoperation, attacks, or viruses.

- Quick Data Recovery
  You can create one or more snapshots before performing major operations such as changing the operating system, upgrading application software, or migrating business data. If any problems occur during the change operation, the business data can be restored in time through the created snapshot.

- Multi-replica Application of Production Data
  You can create production data snapshots to provide near-real-time production data for applications such as data mining, report query, development and testing.

- Rapid Deployment Environment

You can create a snapshot of a CVM and use the snapshot to create a custom image. You can create one or more instances from the created image to quickly deploy CVMs in the same environment in batches, saving time on repeated configuration.

Snapshot Type

- Manual Snapshot
  Manually create a snapshot of the CBS data at a certain point in time. This snapshot can be used to quickly create more CBSs with the same data, or to restore the CBS to the status at that point in the future.

- Periodic Snapshot
  As your business continues to evolve, periodic snapshots can be used to provide continuous backup capabilities. You only need to formulate a backup policy and associate it with the CBS to achieve continuous backup of the CBS data within a certain period, greatly improving data security.

> Note:
> During the snapshot creation process, some application data may be saved in memory but not persisted. This phenomenon may cause the snapshot to fail to capture the latest and most complete CBS data.

Case Review

Case 1: Data loss due to failure to take a manual snapshot before performing high-risk operations

For example, customer A has never created a snapshot of the CBS. On a certain day in May 2019, due to the operator's fio test on the CBS, the file system was damaged and the data could not be recovered.
Analysis: If customer A takes a snapshot of the CBS before testing, then after data corruption, snapshot rollback can be quickly enabled to restore business on time.

Case 2: Data loss due to failure to take regular snapshots of important data disks

For example, customer B had created snapshots for multiple CBSs, but after January 2019, he did not create snapshots for the newly purchased CBSs due to cost considerations. On a certain day in June 2019, a CBS that was not protected by snapshots had its data accidentally deleted at the file system layer, and the data was lost and could not be recovered.
Analysis: If customer B has performed regular snapshot protection on the CBS, then if the data is

accidentally deleted, it can be restored to the data status at the last snapshot time point to reduce losses. After the incident, customer B took the initiative to create a snapshot for the CBS, which fully enhanced data protection.

Case 3: Business restore by regular snapshot rollback after an operation error

For example, customer C has snapshot protection for all CBSs. On a certain day in May 2019, the machine started abnormally due to improper operation.
Analysis: Customer C promptly restored the data using the regular snapshot from 2 days ago, and the business was not affected.

The later cases are all data loss caused by operational errors. By comparison, we can find that:

- In the case where a snapshot is not created, it becomes extremely difficult to recover data when issues arise with the server or CBS, potentially leading to significant losses.
- In the case where a snapshot has been created, data can be largely recovered in the event of issues with the server or CBS, resulting in minimal losses.

It is recommended that you create snapshots regularly for different types of businesses to improve data security and achieve low-cost and high disaster recovery for the business.

Network and Security
Network and Security Overview

The cloud platform provides network and security features to ensure that your instances can provide services internally and externally safely, efficiently, and freely.

Encrypted Login Method

Provides two encrypted login methods: password login and SSH key pair login. Users can freely choose between two methods for safely connecting to CVMs.
Instances with Windows system do not support SSH key login.

Network Access

Cloud services on the same cloud platform can be accessed via the Internet or the private network.

- Internet Access: Internet access is a service provided by Converge Cloud to instances for public data transmission. Instances are assigned public IP addresses to enable communication with other computers on the network.
- Internal Network Access: Internal network access refers to local area network (LAN) service, which is a service provided by Converge Cloud to instances through private IP addresses, enabling completely free private network communication within the same region.

Network Environment

Converge Cloud's network environment can be divided into: basic network and Virtual Private Cloud (VPC).

- Basic Network: The basic network is a public network resource pool for all users on Converge Cloud. Suitable for users who are just beginning to understand and use Converge Cloud.
- VPC: A VPC is a logically isolated network space that you customize on Converge Cloud. Instances in a VPC can be launched in a preset, custom IP range and isolated from other users. Suitable for users who are familiar with network management system.

Security Group

A security group is a stateful virtual firewall with a packet filtering function. It is used to set network access

control for one or more CVMs and is an important network security isolation method provided by Converge Cloud.
You can control access permission to your instances using the earlier methods:

- Create multiple security groups and assign different rules to each security group.
- Each instance is assigned one or more security groups. Converge Cloud will use these rules to determine which traffic can access the instance and which resources the instance can access.
- Configure the security group so that only specific IP addresses or specific security groups can access the instance.

Elastic IP

Elastic IP (EIP), also known as elastic IP address. It is a static IP address designed for dynamic cloud computing.
In the earlier scenarios, it is recommended to use EIP:

- The instance may go down due to uncontrollable reasons, and an alternative instance with the same IP address is required to ensure access.
- The instance does not have a public IP address and requires a static IP address.

Elastic Network Interface

Elastic Network Interface (ENI) is an elastic network interface bound to CVMs in a VPC, which can be freely migrated among multiple CVMs. ENI is very helpful in configuring and managing networks and building highly reliable network solutions.

Placement Group

Placement group is a policy that determines how instances are distributed and placed on the underlying hardware. Instances that you create in a placement group are launched with disaster recovery and high availability.
The CVM provides an instance placement policy, which can forcibly break up instances according to a certain policy when they are created, so as to reduce the impact of underlying hardware/software failures on the business on the CVM. You can use placement groups to deploy CVM instances involved in your business on different physical servers to ensure high availability and underlying disaster recovery capabilities of your business.
When creating instances within a placement group, we will spin up the instances in a dispersed manner within the specified region, based on the deployment policy you have previously set.
If you do not set a placement group for your instance, we will try to launch the instance on different physical machines to ensure service availability.

Distributed Placement Groups

Currently, placement groups support distributed groups. A distributed placement group is a group of instances placed on different underlying hardware to provide high availability. It is recommended that applications that require separate placement of important instances use distributed placement groups, such as primary-secondary databases, high-availability clusters, and other applications. By launching instances in distributed placement groups, you reduce the risk of instances with the same underlying hardware failing at the same time.
Distributed placement groups have regional attributes and can span multiple availability zones. There is a limit on the number of instances per group. For more information, see the console page.

> Note:
> If there is insufficient hardware to fulfill the request, the request will fail when launching instances in a distributed placement group. Generally, you can wait for a while and try your operation again.

Rules and Limitations of Distributed Placement Groups

Before using distributed placement groups, you should be aware of the following rules:

- Placement groups cannot be merged.
- Instances cannot span multiple placement groups.
- You can choose to distribute the content at three levels: physical machine, switch, and rack.

For example, if you select the physical machine level, the instances of the distributed group will not be placed on the same physical machine to ensure the high availability of the business.

- The maximum number of instances supported by groups at different placement levels is different. The specific value is subject to the console page.
- After using the disaster recovery group policy, the policy you specify will be strictly followed. It is important to note that if the underlying hardware is not sufficient to distribute the instances, some instances will fail to be created.
- Instances on CDHs do not support distributed placement groups.

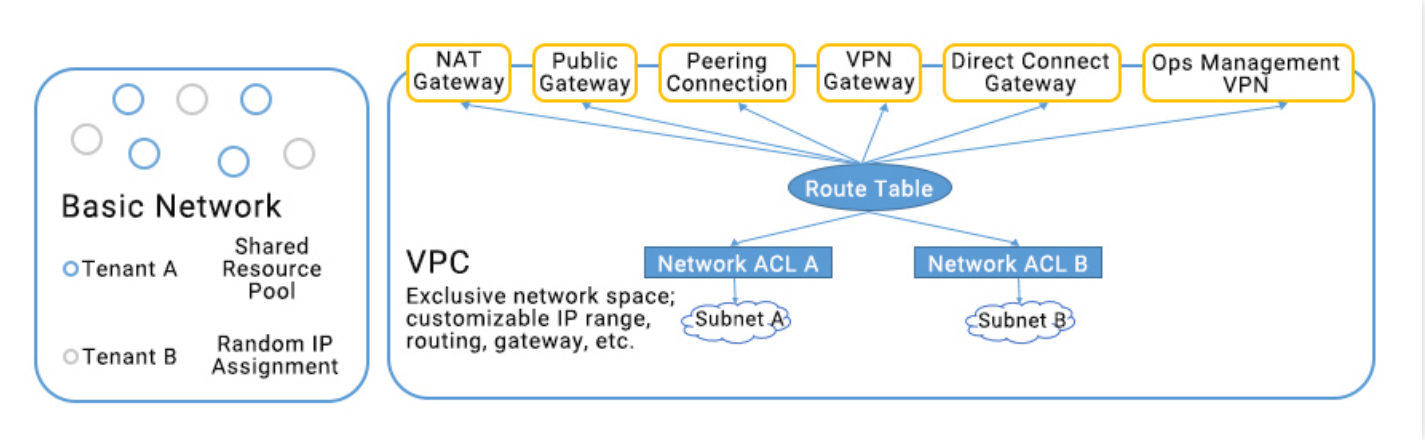
Network Environment

The network environment of the cloud platform can be divided into two types: Virtual Private Cloud (VPC) and basic network.

VPC and Basic Network

VPC

VPC is a logically isolated network space you customize. Even in the same region, different VPCs cannot communicate with each other by default. Similar to the traditional networks you operate in your data center, the cloud platform's VPC hosts your service resources on the cloud platform, including CVM, Cloud Load Balancer, and other cloud service resources. Users can fully control the VPC environment. For more detailed configuration and use cases, please refer to VPC Overview. VPCs can build more complex network architectures and are a suitable choice for users who are familiar with network management system.



Basic Network

The basic network is a public network resource pool for all users on the cloud platform. All cloud resources of users are uniformly managed by the cloud platform, ensuring simplicity and efficiency in management.

Feature Difference

Feature	Basic Network	Virtual Private Cloud (VPC)
Tenant Association	Tenant Association	Logically isolated network based on GRE encapsulation
Network Customization	Not supported.	Supported

Feature	Basic Network	Virtual Private Cloud (VPC)
Routing Customization	Not supported.	Supported
Custom IP	Not supported.	Supported
Interoperability Rules	Intercommunication between tenants in the same region	Cross-region and cross-account communication

Private Network Service

Private network services are local area network (LAN) services, and cloud services access each other via internal links. Cloud services can be accessed via the Internet, and can also access each other through the private network on a cloud platform. The Converge Cloud IDCs are interconnected with underlying 10Gbps/1Gbps networks, providing high-bandwidth and low-delay private network communication services. Additionally, private network communication within the same region is completely free, enabling you to flexibly build your network architecture.

Private IP Address

Overview

The private IP address is an IP address that cannot be accessed through the Internet and is the implementation form of Converge Cloud private network service. Each instance has a default network interface (i.e., eth0) with a private IP address that can be automatically allocated by Converge Cloud or defined by the user (only in a VPC environment).

> Note:
> Changing the private IP address by yourself within the operating system will cause the private network communication to be interrupted.

Attributes

- The private network service has user attributes, and different users are isolated from each other, which means that by default, one user cannot access another user's cloud services via the private network.
- The private network service has regional attributes, and different regions are isolated from each other, which means that by default, one cannot access cloud services in different regions under the same account via the private network.

Application Scenarios

The private IP address can be used for Cloud Load Balancer, private network access between CVM instances, and private network access between CVM instances and other cloud services.

Address Allocation

Each CVM instance is assigned a default private IP address when it is started. For different network environments, the private IP address is also different:

- Basic network: The private IP address is automatically assigned by Converge Cloud and cannot be changed.
- VPC: Currently, Converge Cloud VPC CIDR supports the use of any of the three major private IP ranges. The IP address range is as follows, and the mask range must be between 16 to 28:
    - 10.0.0.0 - 10.255.255.255
    - 172.16.0.0 - 172.31.255.255
    - 192.168.0.0 - 192.168.255.255

Private Network DNS

DNS Server Address

The private network DNS service is responsible for domain resolution. If the DNS configuration is incorrect, the domain will be inaccessible. The cloud platform provides reliable private network DNS servers in different regions.

Public Network Service

When the application deployed by the user on the CVM instance needs to provide public services, the data must be transmitted through the Internet and must have an IP address on the Internet (also called a public IP address). The Internet access provided by the cloud platform is all through the high-speed Internet in the cloud platform data center. Our domestic multi-line BGP network covers over twenty network operators, achieving second-level cross-domain switching for BGP public network exits, ensuring that your users can enjoy high-speed and secure network quality regardless of the network they use.

Public IP Address

- Overview: A public IP address is a non-reserved address on the Internet, and CVMs with public IP addresses can mutually access other computers on the Internet.
- Getting Public IP Address: When creating a CVM, set the bandwidth in the network to be greater than 0 Mbps. After completion, the Converge Cloud system will automatically assign a public IP address to the instance from the public IP address pool. This address can be changed.
- Configuration: You can log in to a CVM instance with a public IP address on the Internet and configure it accordingly.
- Conversion: The public IP address is mapped to the instance's private IP address through Network Address Translation (NAT).
- Maintenance: All public network interfaces of the cloud platform are uniformly handled by TGW. The public network interface card (NIC) of the Converge Cloud CVM instance is configured on the unified interface layer TGW, with no perception required from the CVM.
  Therefore, when users check the network API information in the CVM using the ifconfig (Linux) or ipconfig (Windows) command, they can only see the information of the private network.
  To view the public network information, users need to log in to the CVM console and navigate to the CVM list/details page.

Releasing a Public IP Address

Users cannot actively associate or release a public IP address associated with an instance.
The public IP address will be released or reallocated in the following situations:

- When terminating an instance. When a user actively terminates a pay-as-you-go instance or a monthly subscription instance expires and is terminated, Converge Cloud will release its public IP address.
- When an EIP is associated with or disassociated from the instance. When an instance is associated

with an EIP, Converge Cloud will release the original public IP address of the instance. When you disassociate an instance from an EIP, a new public IP address will be automatically assigned to the instance. The original released public IP address will be returned to the public IP address pool and you will not be able to reuse it.

If you need a fixed, permanent public IP address, you can use an EIP.

Elastic Public IP

Introduction

An EIP is a static IP address associated with an account. You can keep an EIP in your account until you release it. Unlike common public IPs, which are tied to cloud servers and follow their lifecycle, elastic public IPs can be decoupled from cloud servers and operated on as standalone cloud resources.
For example, if you need to retain a public IP address that is strongly related to your business, convert it to an EIP and keep it in your account.

Elastic Network Interface

Elastic Network Interface (ENI) is an elastic network interface bound to CVMs in a VPC, which can be freely migrated among multiple CVMs. ENI is very helpful in configuring and managing networks and building highly reliable network solutions.
An ENI combines VPC, availability zone, and subnet attributes and can only be bound to CVMs in the same availability zone. A CVM can bind multiple ENIs, and the specific number of bindings will depend on the host specifications.

Relevant Concepts

- Primary NIC and Secondary NIC: The NIC that is created simultaneously with the creation of a CVN in a VPC is the primary NIC, while those NICs created by users are considered secondary NICs. The primary NIC does not support binding or unbinding, while the secondary NICs do support binding and unbinding.
- Primary Private IP Address: The primary private IP address of the ENI is randomly assigned by the system or set by the user when the ENI is created. The primary private IP address of the primary NIC can be modified, but the primary private IP address of the secondary NIC cannot be modified.
- Secondary Private IP Address: The secondary private IP addresses bound to an ENI except the primary IP can be configured by users when creating or editing an ENI, and support binding and unbinding.
- EIP: Bind one by one with the private IP address on the ENI.
- Security Group: An ENI can be bound with one or multiple security groups.
- MAC Address: The ENI has a globally unique MAC address.

Use Cases

- Isolation of Private Network, Public Network, and Management Network:
  The network deployment of important businesses generally requires the isolation of the private network, public network, and management network for data transmission, and ensures data security and network isolation between networks through different routing policies and security group policies. Just like a physical server, you can bind three ENIs in different subnets to the CVM to achieve triple network isolation.
- High-Reliability Application Deployment:
  The key components in the system architecture need to be deployed in a multi-machine hot standby mode to ensure the high availability of the system. Converge Cloud provides ENIs and private IP addresses that can be flexibly bound and unbound. You can configure the disaster recovery settings

of Keepalived to achieve high-availability deployment of key components.

API Overview

The following table shows the APIs related to ENI and CVM.

API Feature	Action ID	Feature Description
Create an ENI	CreateNetworkInterface	Create an ENI
Apply for a private IP address using an ENI	AssignPrivateIpAddresses	Apply for a private IP address using an ENI
Bind an ENI to a CVM	AttachNetworkInterface	Bind an ENI to a CVM

SSH Key

To ensure the security of the instance, two encrypted login methods are provided: password login and SSH key pair login. This document describes the configuration of SSH key pair login.
When custom-configuring a Linux CVM, you can select the SSH key as the CVM encrypted login method.

SSH Keys Overview

An SSH key pair is a pair of keys generated by an encryption algorithm, namely a public key and a private key.
Public Key: After the SSH key pair is successfully generated, the cloud platform only stores the public key information.
Private Key: You need to download and keep the private key properly. The private key can only be downloaded once, and the cloud platform will not save your private key. Anyone with your private key can gain access to your login information, so you need to keep your private key in a safe place.
You can use a key pair to securely connect to the CVM. Using a key pair to log in to the CVM is more secure than using a regular password. You only need to specify a key pair when creating an instance, or bind a key pair after the instance is created, and then you can use the private key to log in to the Linux instance without entering a password.

Features and Advantages

Compared with the traditional username and password authentication method, using SSH keys has the following advantages:

- SSH key login authentication is more secure and reliable, and can eliminate the threat of brute force cracking.
- The SSH key login method is simpler. You only need to make simple configurations in the console and local client to remotely log in to the instance. You do not need to enter a password when you log in again.

Use Limits

- Only Linux instances are supported.
- The cloud platform will not keep your private key information. Users need to click Download to obtain the private key within 10 minutes after creating the SSH key, and keep it properly.
- For data security considerations, loading the key needs to be done while the system is powered off.

Ops and Monitoring
Instance Self Check

Overview

The self-service instance detection can detect the performance, cost, network, disk, and other statuses of CVM instances, and help you understand the running status of the instances.
This feature allows you to promptly discover and resolve instance-related issues.

Application Scenario

The earlier two scenarios recommend using self-service instance detection:

- Troubleshooting: If you encounter a fault or problem during instance operation, you can use self-service instance detection to troubleshoot and locate the problem, and handle the exceptions according to the corresponding suggestions.
- Comprehensive instance detection: During daily Ops, you can use self-service instance detection to understand the overall operation status of the instance, discover and solve problems on time, and ensure the normal operation of the business.

Detection Item Description

Account Fee Detection

Detection Items	Detection Description	Solution
Whether the CBS has expired and whether the expiration time of the instance and the CBS is consistent	Whether the CBS associated with the instance has expired or cannot be read or written to	The CBS of this instance has expired. Proceed to the CBS console to renew your subscription as soon as possible.
Whether the CBS has expired and whether the expiration time of the instance and the CBS is consistent	Whether the instance becomes unusable due to the expiration of the CBS	The CBS of this instance is not set to automatically renew. The cloud disk may expire and become unavailable. It is recommended to proceed to the CBS console to set up CBS renewal.

Instance Storage Detection

Detection Items	Detection Description	Solution
Has there been an IO HANG issue with the CBS	Has there been an IO HANG issue with the CBS	The CBS of this instance has an IO HANG issue. It is recommended that you pay attention to the usage of the CBS.
CBS Space Usage Detection	Has the disk usage of the CBS reached 100%?	It is recommended that you pay attention to the usage of the CBS
CBS io_util Detection	Has the io_util of the CBS reached 100%?	It is recommended that you pay attention to the usage of the CBS
Is the CBS in read-only mode	Is the CBS currently in read-only status	It is recommended that you pay attention to the usage of the CBS
Detection of CBS iNode Usage	Has the iNode usage of the CBS reached 100%?	It is recommended that you pay attention to the usage of the CBS
Is the CBS experiencing a high delay	Is the IO performance svctm metric abnormal	The CBS of this instance has a high delay problem. It is recommended that you pay attention to the usage of the CBS.

Instance Performance Detection

Detection Items	Detection Description	Solution
Memory Usage	Has the instance experienced excessive memory load within the last 12 hours	To avoid becoming a service bottleneck, we recommend that you check CPU usage and adjust the configuration on time.
Basic CPU Usage	Has the instance experienced a high CPU load in the last 12 hours?	Same as above
CPU Usage	Has the instance experienced a high CPU load in the last 12 hours?	Same as above

Instance Status Detection

Detection Items	Detection Description	Solution

Detection Items	Detection Description	Solution
Has the instance experienced a kernel fault?	- Has the instance experienced a hungtask in the last 12 hours? - Has the instance experienced a panic in the last 12 hours? - Has the instance experienced a soft deadlock in the last 12 hours?	The instance has experienced hungtask/panic/ soft deadlock in the last 12 hours. Please pay attention to the instance running status.
Whether the instance was restarted?	Whether the instance was restarted in the last 12 hours?	The instance has been restarted in the last 12 hours. Pay attention to the instance status.
Instance Shutdown Status Detection	Is the instance currently shut down?	The instance is shut down. You can go to the CVM console to start it up.

Instance Network Monitoring

Detection Items	Detection Description	Solution
Is the instance's public IP blocked by DDOS?	Is the public IP blocked by DDOS?	The public IP address of this instance was blocked due to DDOS attack.
Does it have a public IP?	Does the instance have a public IP?	This instance does not have a public IP. If you need a public network IP for external access, you can go to the Elastic IP console to bind an EIP.
Is the public IP disconnected due to overdue payment?	Is the public IP isolated due to overdue payment?	The public IP may be unable to communicate with the external network due to overdue payment. We recommend you to recharge your account as soon as possible.
Detection of Public Network Bandwidth Utilization	- Whether the instance has experienced excessively high public network inbound bandwidth in the last 12 hours? - Whether the instance has experienced excessively high public network outbound bandwidth in the last 12	To avoid becoming a business bottleneck, we recommend that you check the network usage.

Detection Items	Detection Description	Solution
	hours?	
Kernel Network Detection	- Whether the instance has experienced a UDP send buffer full within the last 12 hours? - Whether the instance has experienced a UDP receive buffer full within the last 12 hours? - Whether the instance has experienced a full TCP accept queue within the last 12 hours? - Whether the instance has experienced TCP request overflow within the last 12 hours?	To avoid becoming a business bottleneck, we recommend that you check the health of your business.
Whether the number of connections has reached the upper limit?	Whether the instance has reached the upper limit of the number of connections within the last 12 hours?	To avoid becoming a business bottleneck, we recommend that you check the health of your business.

Monitoring and Alarms

Monitoring and alarm is an important part to ensure high reliability, high availability and high performance of CVM. This document provides an overview of the monitoring and alarm features provided for the CVM.

Overview

CVM monitoring and alarm is a management tool for real-time monitoring of CVMs. The monitoring and alarm feature can display the most comprehensive and detailed monitoring data, extracting key indicators from the CVM in real-time and presenting them in the form of monitoring charts.
To provide you with a comprehensive understanding of your CVM's resource usage, performance, and health status.
It also supports setting custom alarm thresholds and sending notifications based on your custom rules.

Basic Features

The console provides access to the following functionalities for CVM monitoring and alarm:

Module	Capability	Main Feature
Monitoring Overview	View the overall monitoring status of cloud services.	Provide an overview of the overall situation, alarm situation, and overall monitoring information.
Alarm Management	Support for user custom alarm thresholds	Currently supports CVM alarm settings
Cloud Services Monitoring	View detailed monitoring status of cloud services.	Current CVM monitoring view
Custom Monitoring	View user-defined monitoring metric data.	Provide custom metric reporting and monitoring alarm services.
Traffic Monitoring	Monitor traffic usage.	View overall user bandwidth information.

For more information, please see the Basic features of cloud monitoring.

Application Scenario

- Daily management scene: Log in to the cloud monitoring console to view the running status of each cloud monitoring.
- Timely handling of exception scene: When the monitoring data reaches the alarm threshold, an alarm message will be sent to notify you promptly, allowing you to acquire exception notification and check the cause of the exception.
- Timely scale-out scene: After the alarm rules for monitoring items such as bandwidth, connection counts, disk usage, etc. are set, you can conveniently understand the current status of your cloud service and receive timely alarm notifications to scale out your service capacity as the business volume increases.

Monitoring Content

To monitor instance performance benchmarks, you should monitor at least the following monitoring items:

Monitoring Items	Monitoring Metrics
CPU Utilization	cpu_usage
Memory Utilization	mem_usage
Private Network Outbound Bandwidth	lan_outtraffic
Private Network Inbound Bandwidth	lan_intraffic
Outbound Bandwidth of Public Network	wan_outtraffic
Public Network Inbound Bandwidth	wan_intraffic
Disk Usage Rate	disk_usage
Disk I/O Waiting Time	disk_io_await

Monitoring Data

- Monitoring interval: Currently, cloud monitoring provides multiple monitoring data statistical granularities of 1 minute, 5 minutes, 1 hour, and 1 day. The CVM can support 1 minute monitoring granularity, that is, data is counted every 1 minute, and the default interval is 5 minutes.
- Data storage: Monitoring data with 1 minute, 5 minutes and 1 hour granularity is stored for 31 days, and monitoring data with 1 day granularity is stored for half a year.
- Alarm display: The data is displayed in easy-to-read charts. The console integrates the monitoring data of all products, which is more conducive to users to obtain a holistic operation overview.

- Alarm settings: You can set threshold values for monitoring metrics, and when the conditions are met, alarm messages will be sent promptly to the concerned group.

Access Control
Access Control Overview

If you use CVM, VPC, databases and other services in the cloud platform, and these services are managed by different people but share your cloud account key, the following problems will occur:

- The risk of your key being compromised is high since multiple users are sharing it.
- The access permission of other users is not under control. They can introduce security risks caused by misoperations.
  In this case, you can use sub-accounts to allow different users to manage different services to prevent the problems above. By default, a sub-account has no permission to use CVM or CVM-related resources. Therefore, we need to create policies to allow sub-accounts to use the resources or permissions they need.
  Cloud access management (CAM) is a set of web services provided by Converge Cloud. It primarily helps customers securely manage access permissions to resources under the cloud platform account. With CAM, you can create, manage, and terminate users (groups), and control who can use which resources through identity and policy management.
  You can use CAM to bind a user or user group to a policy that allows or denies them access to specified resources to complete specified tasks. For more basic information about CAM policies, please see Policy Syntax.
  If you do not need to manage the cloud access to CVM-related resources for your sub-account, you can skip this section. Skipping these sections does not affect your understanding and use of the rest of the documentation.

Getting Started

A CAM policy must authorize the use of one or more CVM operations, or it must deny the use of one or more CVM operations.
You must also specify the resources that can be used for the operation (it can be all resources, or some operations can be partial resources). The policy can also contain the conditions set by the operation resources.
Some API operations of CVM support resource-level permissions. That is, you cannot specify a specific resource for these API operations. Instead, you must specify all the resources for the operations.

Authorized Resource Types

Resource-level permissions refer to the ability to allow which resources a user is allowed to perform operations on. Some Cloud Virtual Machines (CVMs) support resource-level permissions, which means that for CVM operations that support resource-level permissions, they control when users can perform operations or which specific resources they are allowed to use.

The types of resources that can be authorized in Cloud Access Management (CAM) are as follows:

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

The CVM instance-related, CVM token-related, and CVM image-related sections respectively introduce the CVM API operations that currently support resource-level permissions, as well as the resources and conditional keys supported by each operation. When setting up the resource path, you need to modify the variable parameters such as $region , $account to your actual parameter information. Additionally, you can also use the wildcard character * in the path.

> Note:
> If the API operations of CVM are not listed in the table, it indicates that the API operation of CVM does not support resource-level permissions. For CVM API operations that do not support resource-level permissions, you can still grant users permission to use the operation, but the resource element of the policy statement must be specified as `*`.

CVM Instance Related

API Operations	Resource Path	Condition Key
DescribeInstanceInternetBandwidthConfigs	qcs::cvm:$region:$account:instance/* qcs::cvm:$region:$account:instance/$instanceId	cvm:region cvm:zone cvm:instance_type
ModifyInstancesAttribute	qcs::cvm:$region:$account:instance/* qcs::cvm:$region:$account:instance/$instanceId	cvm:region cvm:zone cvm:instance_type

API Operations	Resource Path	Condition Key
ModifyInstancesProject	qcs::cvm:$region:$account:instance/* qcs::cvm:$region:$account:instance/$instanceId	cvm:region cvm:zone cvm:instance_type
ModifyInstancesRenewFlag	qcs::cvm:$region:$account:instance/* qcs::cvm:$region:$account:instance/$instanceId	cvm:region cvm:zone cvm:instance_type
RebootInstances	qcs::cvm:$region:$account:instance/* qcs::cvm:$region:$account:instance/$instanceId	cvm:region cvm:zone cvm:instance_type
RenewInstances	qcs::cvm:$region:$account:instance/* qcs::cvm:$region:$account:instance/$instanceId	cvm:region cvm:zone cvm:instance_type
ResetInstance	qcs::cvm:$region:$account:instance/* qcs::cvm:$region:$account:instance/$instanceId qcs::cvm:$region:$account:image/* qcs::cvm:$region:$account:image/$imageId qcs::cvm:$region:$account:keypair/* qcs::cvm:$region:$account:keypair/$keyId qcs:::cvm:$region:$account:systemdisk/*	cvm:region cvm:zone cvm:instance_type
ResetInstancesInternetMaxBandwidth	qcs::cvm:$region:$account:instance/* qcs::cvm:$region:$account:instance/$instanceId	cvm:region cvm:zone cvm:instance_type
ResetInstancesPassword	qcs::cvm:$region:$account:instance/* qcs::cvm:$region:$account:instance/$instanceId	cvm:region cvm:zone cvm:instance_type

API Operations	Resource Path	Condition Key
ResetInstancesType	qcs::cvm:$region:$account:instance/* qcs::cvm:$region:$account:instance/$instanceId	cvm:region cvm:zone cvm:instance_type
ResizeInstanceDisks	qcs::cvm:$region:$account:instance/* qcs::cvm:$region:$account:instance/$instanceId	cvm:region cvm:zone cvm:instance_type

Authorization Policy Syntax

Policy Syntax

CAM policy:

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

- The version is required, currently only allowing a value of "2.0".
- statement is used to describe the detailed information of one or more permissions. This element includes the permissions or permission sets of multiple other elements such as effect, action, resource, and condition. A policy has one and only one statement element.
- action used to describe the operations that are allowed or denied. Operations can be APIs (described with a name prefix) or feature sets (a specific set of APIs described with a permid prefix). This element is required.
- resource describes the detailed data authorized. Resources are described using six paragraphs. The resource definition details will vary for each product. For information on how to specify resources, please refer to the product documentation corresponding to the resource declaration you have written. This element is required.
- conditions describes the constraints under which the policy takes effect. Conditions consist of operators, operation keys, and operation values. Condition values can include information such as time and IP address. Some services allow you to specify additional values in the condition. This element is optional.
- effect describes whether the statement produces an allow or explicit deny result. It includes allow and deny. This element is required.

CVM Operations

In the CAM policy statement, you can specify any API operation from any service that supports CAM. For CVM, please use name/cvm: as the prefix of APIs. For example: name/cvm:RunInstances or name/cvm:ResetInstancesPassword.

If you want to specify multiple actions in a single statement, separate them with commas as follows:

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

You can also use wildcard characters to specify multiple actions. For example, you can specify all actions whose names begin with the word " Describe " as follows:

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

To specify all operations in a CVM, please use a wildcard * as follows:

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

CVM Resource Paths

Each CAM policy statement has its own resources that apply to it.
The general format of resource paths is as follows:

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

project_id: describes the project information. It is only for compatibility with early CAM logic and does not need to be filled in.
service_type: the product abbreviation, such as VPC
region: regional information, such as bj
account: the root account information of the resource owner, such as uin/164256472
resource: specific resource details of each product, such as instance/instance_id1 or instance/*
For example, you can specify an instance (i-15931881scv4) in the statement, as shown below:

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

You can also use the * wildcard character to specify all instances belonging to a specific account, as follows:

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

If you want to specify all resources, or if a specific API operation does not support resource-level permissions, use the * wildcard in the Resource element as shown:

```
"resource": "*"
```

To specify multiple resources in one instruction, please separate them with a comma. The following is an example of specifying two resources:

resource:["resource1","resource2"]

The following table describes the resources that can be used by CVM and the corresponding methods of describing these resources. In the following table, words prefixed with $ are aliases.

- Among them, project refers to the project ID.
- Region refers to the region.
- Account refers to the account ID.

Resources	Resource Description Method in Authorization Policies
Instance	qcs::cvm:$region:$account:instance/$instanceId
Key	qcs::cvm:$region:$account:keypair/$keyId
VPC	qcs::vpc:$region:$account:vpc/$vpcId
Subnet	qcs::vpc:$region:$account:vpc/$vpcId
System Disk	qcs::cvm:$region:$account:systemdisk/*
Image	qcs::cvm:$region:$account:image/*
Subnet	qcs::vpc:$region:$account:subnet/$subnetId
Data Disk	qcs::cvm:$region:$account:datadisk/*
Security Group	qcs::cvm:$region:$account:sg/$sgId
EIP	qcs::cvm:$region:$account:eip/*

Conditional Key for CVM

In a policy statement, you can optionally specify conditions that control when a policy takes effect. Each condition consists of one or more key-value pairs. Condition keys are not case sensitive.

- If you specify multiple conditions or multiple keys in a single condition, we evaluate them using a logical AND operation.
- If you specify a key with multiple values in a single condition, we evaluate them using a logical OR operation. All conditions must be matched for permission to be granted.
  The following table describes the service-specific condition keys that CVM uses.

Condition Key	Reference Type	Key-value Pair

Condition Key	Reference Type	Key-value Pair
cvm:instance_type	String	cvm:instance_type=instance_type - Among them, instance_type refers to the instance type (for example, S1.SMALL1).
cvm:image_type	String	cvm:image_type=image_type - Image_type refers to the image type (for example, IMAGE_PUBLIC).
vpc:region	String	vpc:region=region - The region refers to the region (for example, ap-cityA).
cvm:disk_size	Integer	cvm:disk_size=disk_size - Disk_size refers to the disk size (e.g. 500).
cvm:disk_type	String	cvm_disk_type=disk_type - Disk_type refers to the disk type (e.g. CLOUD_BASIC).
cvm:region	String	cvm:region=region - The region refers to the region (for example, ap-cityA).

CVM Dedicated Host
CDH Overview

CVM Dedicated Host (CDH) provides users with exclusive physical server resources to meet users' needs for exclusive resources, the physical isolation of resources, security, and compliance, and is a supplement to CVM products. CDH is equipped with the Converge Cloud virtualization system, on which you can flexibly create and manage multiple CVM instances of custom specifications and independently plan the use of physical resources.

Relevant Concepts

When you learn about CDH, the following concepts are usually involved:

- Host type: the type of hosts. Different types of hosts have different hardware configurations.
- Local hard disk type: the disk type on the host. Different types of hosts carry different types of disks, including local hard disks and local SSD hard disks.
- CVM instance: a CVM instance allocated on a host, also referred to as instance in some documents.
- CBS: The distributed persistent block storage device provided by Converge Cloud can be used as the system disk or expandable data disk of the instance.
- Image: an instance provisioning template that contains a preconfigured server environment (operating system and other installed software).
- VPC: a customized virtual network space that is logically isolated from other resources.
- IP address: the internal and external service addresses of the CVM instance, that is, the private network IP addres and public network IP address
- SSH key: a more secure way to log in to your Linux CVM than regular passwords.
- Security group: Perform secure access control on the instance and specify the IP, protocol, and port rules for entering and exiting the instance.
- Regions and availability zones: the starting position of the resource.

Related Services

- CDHs are used by allocating CVM instances on them.
- You can use Cloud Load Balancer (CLB) to automatically distribute request traffic from clients across multiple CVM instances.

Using CDH

CDH provides a Web-based user interface. You can log in to the CDH console to operate your CVM.

Strengths

A CDH is a dedicated physical server equipped with a virtualized environment, which has the following advantages:

Exclusive Resources

By purchasing a CDH, you can enjoy exclusive host resources and physically isolate them from other user resources. The resources in the host are available for you to plan independently to avoid resource competition from other tenants.

Flexible Creation

Users can create CVM instances of customized specifications on CDHs and independently plan the use of host resources. Instance specifications support customization and flexible configuration, breaking the limitations of instance specifications, and ensuring business performance while making full use of physical server resources. It supports configuration adjustment of dedicated instances, providing the ability to adjust the network at any time without shutting down the instance and to adjust the instance configuration in the shutdown status.

Security and Compliance

It provides physical isolation of host-level resources, with CPU, memory, disk, and network resources dedicated to a single tenant. Physical machine-level resource isolation provides sensitive business data protection and disk degaussing capabilities, meeting the stringent regulatory requirements of the financial industry.

Monitoring Management

It provides multi-dimensional management and monitoring functions for hosts and dedicated instances, offers cloud monitoring services for free, and supports multiple real-time alarm notifications.

Light Asset

Purchase on demand, with minute-level delivery. Converge Cloud provides standardized Ops management

services to ensure the stable operation of your resources. Customers do not need to worry about underlying maintenance, thus saving manpower and operational costs, and allowing them to focus on their core business.

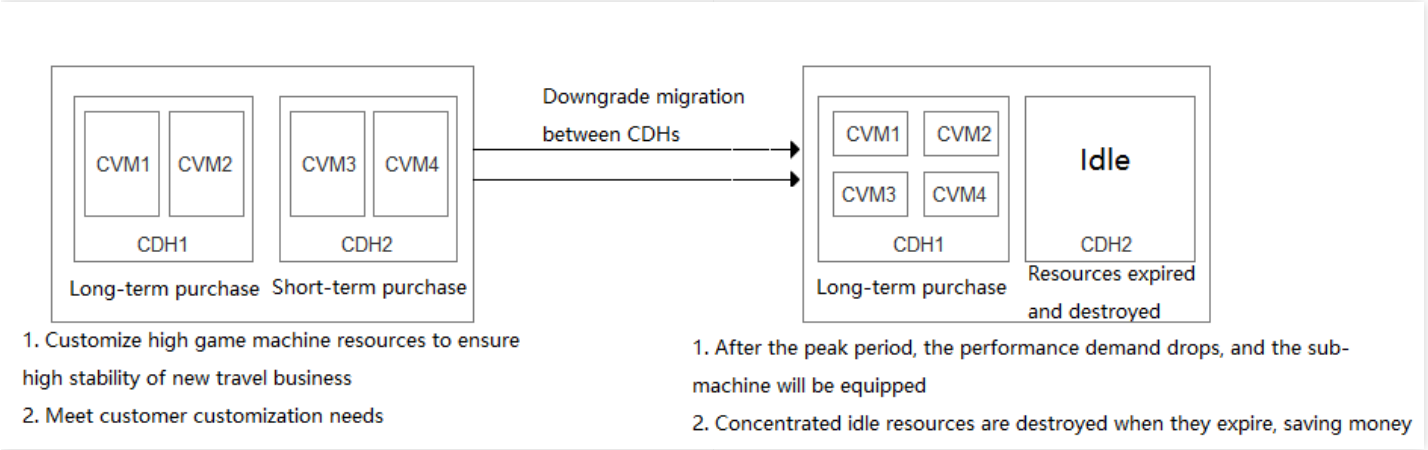
CVM-featured

A dedicated instance is the instance of CVM Dedicated Host created on a CDH, providing support for images, security groups, configuration adjustments, SSH keys, etc. The usage of each function and feature remains the same as that of an ordinary CVM.

Use Cases

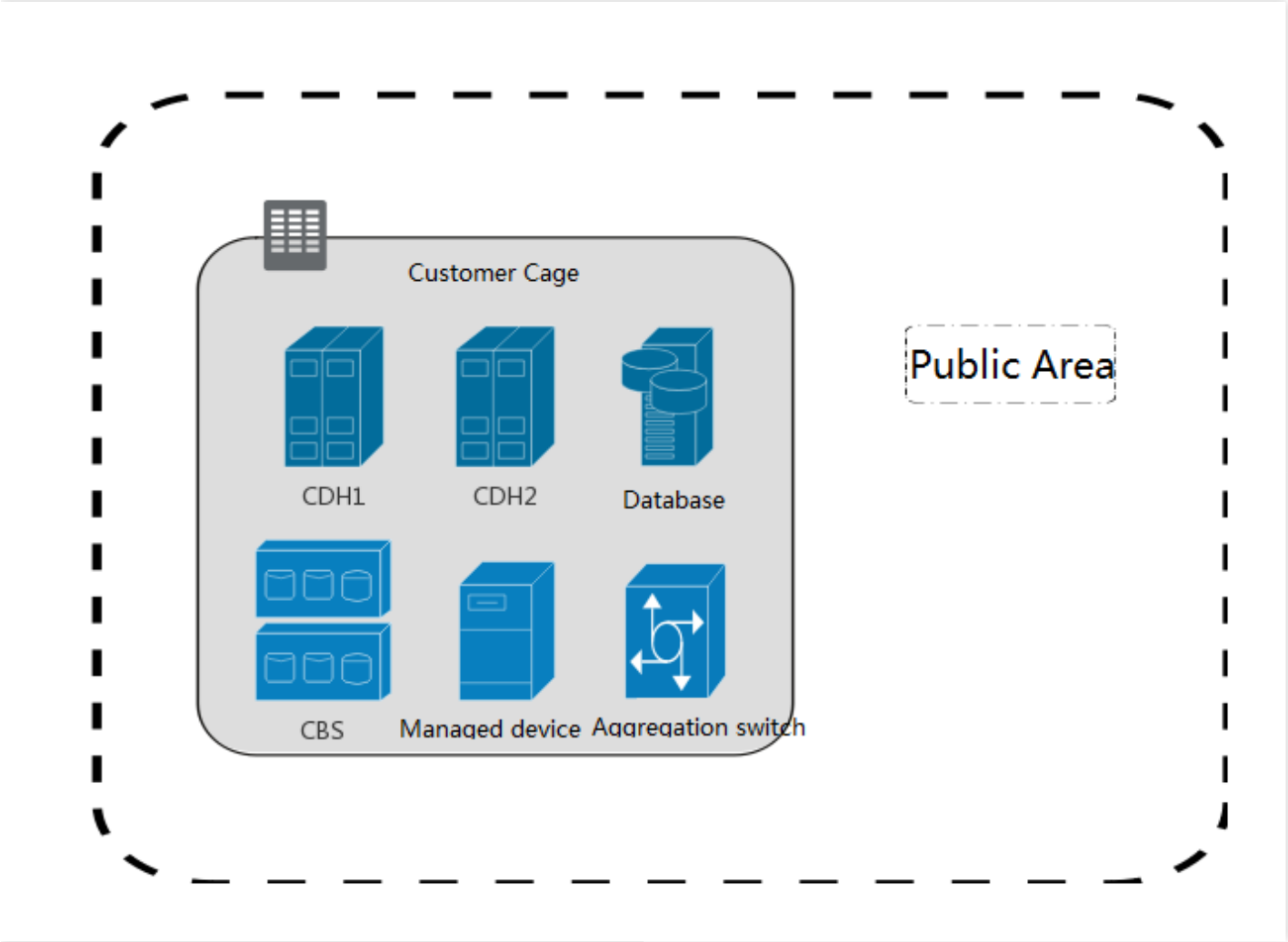
Game Application Scenarios

Game customers can purchase multiple host servers and estimate the duration of CDH usage during peak business hours before creating instance.
Some machines can be deployed specifically for the launch of new games based on business needs. After the peak business period, the business can be downgraded and migrated from the original machines to other host servers.
You can also perform operations such as merging servers. Centralize stable business on the same independent host server and concentrate idle resources on another one.
Idle host servers can be terminated upon expiration or continue to serve new games.
Game customers can also customize their host servers by using exclusive host servers. Please contact the Major Customer Manager or submit a ticket to apply.



Finance-Specific Use Cases

The financial industry has strict data security supervision, and independent host servers can meet the security and compliance needs of major financial customers. Resources are physically isolated to meet the needs of sensitive business data protection and disk degaussing.
It supports purchasing and creating CVMs by specifying a single host server or multiple ones, with no restrictions on specifications and supporting customization based on host server resources.
It supports specifying products for cage purchase, which can be combined with other offerings to establish an exclusive single-tenant environment, ensuring dedicated host servers, networks, memory, and disks for each tenant.


Customer Cage
CDH1
CDH2
Database
CBS
Managed device
Aggregation switch
Public Area

Model Overview

A CDH is a physical server equipped with a virtualized environment. Each model corresponds to different physical server configurations, including the physical CPU model, number of CPU cores, memory size, local disk type, disk size, and other hardware resource configuration information. You can choose the appropriate CDH model that suits your business characteristics and scale.
At present, CDH models include:

CDH Type	Standard HS20	Standard HS10	High IO HI20	High IO HI10	Memory-Optimized HM20	Compute HC20
Physical CPU Model	Intel Xeon E5-2680 Broadwell(v4)	Intel Xeon CPU	Intel Xeon E5-2680 Broadwell(v4)	Intel Xeon CPU	Intel Xeon E5-2680 Broadwell(v4)	Intel Xeon® E5-2667v4
Number of CPU Logical Cores	56	48	56	48	56	32
Memory Size (GB)	224	96	224	220	480	96
Local Disk Type	Local disk	Local disk	Local SSD	Local SSD	Local disk	Local SSD
Local Disk Size (GB)	2452	2452	7052	7104	2452	1000

Standard Family

The standard type is a balance of computing, memory, and network resources, which can meet the application resource requirements in most scenarios.

Standard HS20

The Standard HS20 is the latest generation of standard CDH instances, utilizing the Intel® Xeon® Broadwell processor. It offers a 40% improvement in integer and floating-point operation performance compared to previous generations. Paired with DDR4 memory, it achieves a 30% performance increase. This CDH type

provides balanced computing, memory, and network resources, making it an excellent choice for many applications.

Model Characteristics

- Intel Xeon E5-2680 Broadwell (v4) processor with a base clock rate of 2.4 GHz, DDR4 memory;
- CPU performance is 20% higher than Series 1 Standard HS10;
- Balance of computing, memory, and network resources.

Standard HS10

The Standard HS10 meets users' needs for flexible configuration options, featuring moderate pricing and configurable flexibility.

Model Characteristics

- Covering low-core to high-core, users can flexibly choose configurations.
- Intel Xeon CPU, with DDR3 memory.
- Balance of computing, memory, and network resources.

High IO Family

The High IO I2 instances are optimized to provide applications with tens of thousands of low-delay random I/O operations per second (IOPS), making them the best choice for high IOPS use cases.

High IO HI20

The High IO HI20 instance is optimized to provide applications with tens of thousands of low-delay random I/O operations (OLTP) per second, making it the best choice for high-IOPS application scenarios. The High IO HI20 instance uses an Intel Broadwell processor and is equipped with DDR4 memory.

Model Characteristics

- 2.4 GHz Intel Xeon E5-2680 Broadwell (v4) processor, DDR4 memory.
- Using SSD instance storage, system disks are all local SSD disks, providing high IOPS and high throughput performance to meet the needs of users with high disk read and write requirements.
- Low delay: In typical scenarios, it provides sub-millisecond access delay (blocksize = 4 k, iodepth = 1).

Applicable Scenario

- High-performance databases, NoSQL databases (such as MongoDB), and clustered databases.
- I/O-intensive applications that require low delay, such as online transaction processing (OLTP) systems and Elastic Search.

High IO HI10

The High IO HI10 is equipped with high-performance local SSD, which can meet the needs of users with high requirements for disk reading, writing and latency.

Model Characteristics

- Intel Xeon CPU, covering low-core to high-core, users can flexibly choose the configurations.
- Equipped with high-performance local SSD, it can meet the needs of users with high requirements for disk reading, writing and latency.
- Low delay, providing sub-millisecond access delay.

Applicable Scenario

- High-performance databases, NoSQL databases (such as MongoDB), and clustered databases.
- I/O-intensive applications that require low latency, such as online transaction processing (OLTP) systems and Elastic Search.

Memory-Optimized Family

The Memory-Optimized family, characterized by its large memory capacity, is suitable for high-performance databases and distributed memory caching, and other applications that require extensive memory operations, lookups, and calculations.

Memory-Optimized HM20

The Memory-Optimized HM20 is designed to deliver fast performance for workloads that process large data sets in memory. Its characteristic is large memory, which makes it the best choice for high-memory computing applications.

Model Characteristics

- 2.4 GHz Intel Xeon® E5-2680v4 processor, DDR4 memory.
- The processor to memory ratio is 1:8.

Applicable Scenario

- High-performance databases, distributed memory caching, and other applications that require extensive memory operations, lookups, and calculations.
- Gene computation and other scenarios with self-built Hadoop clusters.

Compute Family

The Compute family is equipped with a base frequency of 3.2 GHz and has the highest single-core computing performance. Suitable for computationally intensive applications such as batch processing, high-

performance computing, and large-scale game servers.

Compute HC20

The Compute HC20, with its high-performance processor and excellent cost-performance ratio, is an ideal choice for applications that require high computational performance and high concurrent read/write capabilities, among other computationally intensive applications.

Model Characteristics

3.2GHz Intel Xeon® E5-2667v4 processor, turbo frequency up to 3.6 GHz, DDR4 memory.

Applicable Scenario

The Compute C2 type is highly suitable for the following scenarios:

- Processing workloads in batch.
- High-traffic web servers, massively multiplayer online (MMO) game servers.
- High Performance Computing (HPC) and other compute-intensive applications.
  For best performance, we recommend that you use current generation instance types when you create new instances.

Lifecycle

The lifecycle of a CVM dedicated host (CDH) refers to the statuses it goes through from startup to termination. Proper management of CDH instances from startup to termination ensures that applications running on the instances can provide services efficiently and economically.

Statuses of CDH Instance

Status Name	Status Attribute	Status Description
Creating	Intermediate status	Status after a CDH instance is created and before it enters the running status.
Running	Stable status	Normal running status, in which CVM instances can be created on a CDH instance.
Recycled	Stable status	Status in which a CDH enters the recycle bin.
Terminated	Stable status	Once the termination operation is completed, the original CDH will no longer exist and be unable to provide services, and the data will be completely cleared.

CDH Instance Recycling Mechanism

- After a CDH instance enters the recycle bin, you can still restore it. If restoration is completed during the recycle bin period, the CVM instances and their associated networks and CBS on the CDH will become available again.
- If your CDH resources are not restored after being kept in the recycle bin for a few days, the system will release the resources. All CVM instances on the CDH will be terminated, and the data on local disks and CBS associated with the CVM instances will be cleared and cannot be restored.

Quick Start
How to Get Started with CVM

To help you use Cloud Virtual Machine (CVM) effectively, this document provides a guide to getting started with CVM.

Getting Started with CVM

The Getting Started section helps you understand the basic concepts of CVM. It is suitable for users who have no basic knowledge or are new to Converge Cloud services. <!--You can learn the following points:

- What is CVM?
- The Features and Strength of CVM -->

Learn About CVM

Before purchasing and using a CVM, we will help you make a better choice that suits your needs:

- When you are faced with a variety of models and do not know how to choose, CVM Model Selectionhelps you understand the applicable scenarios and performance of different models, and helps you choose the model that suits your business scenario.
- If you are not sure where to configure, Region and Availability Zone helps you understand the best options for regions and availability zones.

Others

- Adjust instance configuration: If you choose a lower hardware configuration when your application is in its early stages and the number of requests is small, and as your application grows rapidly and the number of service requests increases dramatically, you can adjust the instance configuration by quickly upgrading the hardware to improve service processing speed and better meet your changing needs.

Custom Configuration Selecting Cloud Disks

When configuring an instance, you can select a local disk or Cloud Block Storage (CBS) as your system disk or data disk. Before selecting a storage medium, please understand the characteristics and differences in applicable scenarios between local disks and CBS.

> Note:
> - The types of system disks and data disks that can be purchased on the purchase page vary by the instance specifications you have selected. For example, only users who choose a high IO instance type can choose a local SSD.
> - CVMs that use local disks (including system disks and data disks) do not support configuration upgrades (CPU, memory, and hard disk), but only bandwidth upgrades.
> - After successful purchase, the system disk does not support storage media replacement.

The differences and applicable scenarios of storage media (local SSD, Basic Cloud Disk, Premium Disk and Cloud SSD) are shown in the following table:

Storage Media	Strengths	Applicable Scenario
Local SSD	Low delay: Provides microsecond-level access delay.	Used as temporary read cache: Local SSD has excellent random read performance (4 KB/8 KB/16 KB random read), and is suitable as a read-only slave database for relational databases such as MySQL and Oracle. The memory cost is still higher than that of SSD. Therefore, Local SSD can also serve as the secondary cache for cache-based services such as redis and Memcached. Note: Local disks have the risk of single point failure. It is recommended to perform data redundancy at the application layer to ensure data availability. It is recommended to use Cloud SSD for core businesses.
Basic Cloud Disk	Low-cost storage with the same data persistence as Cloud SSD. It can be used for cold data backup and archiving of important business. The single disk	Suitable for sequential reading and writing of large files, such as log flow, streaming media services, data warehousing, etc., to meet the needs of

Storage Media	Strengths	Applicable Scenario
	capacity is up to 16 TB.	offline analysis of TB-level and massive data under the Hadoop framework.
Premium Disk	Suitable for 90% of I/O scenarios, providing the best choice with high quality and low costs.	Suitable for scenarios such as small and medium-sized databases, web servers, providing long-term stable I/O performance output. Meeting the I/O requirements of core business testing and development and debugging environments.
Cloud SSD	High performance and high data reliability: Use the industry's best NVMe solid-state storage as the disk media. It is suitable for I/O-intensive businesses and provides long-term stable and ultra-high single-disk performance.	Applicable to the following scenarios: - Medium and large databases: It can support medium and large-sized relational database applications such as MySQL, Oracle, SQL Server, MongoDB, etc. with millions of rows in tables. - Core business system : Core business systems such as I/O intensive systems that have high requirements for data reliability. - Big data analysis: Provides distributed processing capabilities for TB and PB-level data, suitable for data analysis, mining, business intelligence and other fields.

Planning the Network

A Virtual Private Cloud (VPC) is a logically isolated network space customized by users on a cloud platform. Within a VPC, you can freely define IP range, IP addresses, and routing policies. Therefore, Converge Cloud recommends that you choose a VPC.
To help you better use VPC, the following network planning suggestions are provided:

Determining the number of VPCs

Known features:

- VPC has regional attributes. By default, the private networks of cloud services in different regions are not interconnected. When cross-region communication is required, you can establish a peering connection to satisfy.
- By default, different VPC private networks in the same region cannot communicate with each other. When cross-VPC communication is required, you can establish a peering connection to satisfy.
- By default, different availability zones in the same VPC can communicate with each other through private networks.
  Related Suggestions:
- If your business requires the deployment of systems in multiple regions, you will inevitably need to use multiple VPCs. You can choose to establish a VPC in a region close to your customers to reduce access delay and increase access speed.
- If you have multiple business deployments in the current region and want to isolate the networks between different businesses, you can create a corresponding VPC for each business in the current region.
- If you do not need to deploy in multiple regions and do not need network isolation between businesses, you can use only one VPC.

Defining Subnet Division

Known Features:

- A subnet is a block of IP addresses within a VPC. All cloud resources in a VPC must be deployed in a subnet.
- In the same VPC, subnet IP range cannot be repeated.
- The initial private IP address is automatically allocated by Converge Cloud in the VPC IP range. Converge Cloud VPC CIDR supports the use of any of the three major private IP ranges. The IP address range is as follows. The mask range must be between 16 and -28. The specific value is determined by the VPC where the instance is located.
  - 10.0.0.0-10.255.255.255
  - 172.16.0.0-172.31.255.255

    - 192.168.0.0-192.168.255.255
- After the VPC is created successfully, you can not modify the IP range.
  Related Suggestions:
- If it is just VPC subnet planning and does not involve network communication with the basic network or IDC, you can choose any of the above IP ranges to create a new subnet.
- If you need to communicate with the infrastructure network, please establish the network of 10.[0~47].0.0/16 and its subsets as required.
- If you need to establish a VPN, the VPC IP range and the peer IP range (your IDC IP range) cannot overlap, so be sure to avoid the peer IP range when creating a new subnet.
- When dividing the IP range, the IP capacity of the range should also be considered, that is, the number of available IP addresses.
- Finally, it is recommended that the services under the same VPC be divided into subnets according to business modules. For example, subnet A is used for the web layer, subnet B is used for the logic layer, and subnet C is used for the DB layer. This is conducive to combining network ACL for access control and filtering.

Defining Routing Policy

Known Features:

- A route table consists of multiple routing policies that control the outbound traffic direction of subnets in the VPC.
- Each subnet must be associated with one and only one route table.
- Each route table can be associated with multiple subnets.
- When a user creates a VPC, the system automatically generates a default route table for it. The default routing table means that the VPC and the private network can communicate with each other.
  Related Suggestions:
- If there is no need to perform special control on the traffic flow of the subnet, and the VPC private network is interconnected by default, the default routing table can be used without configuring a custom routing policy.

Configure Security Group

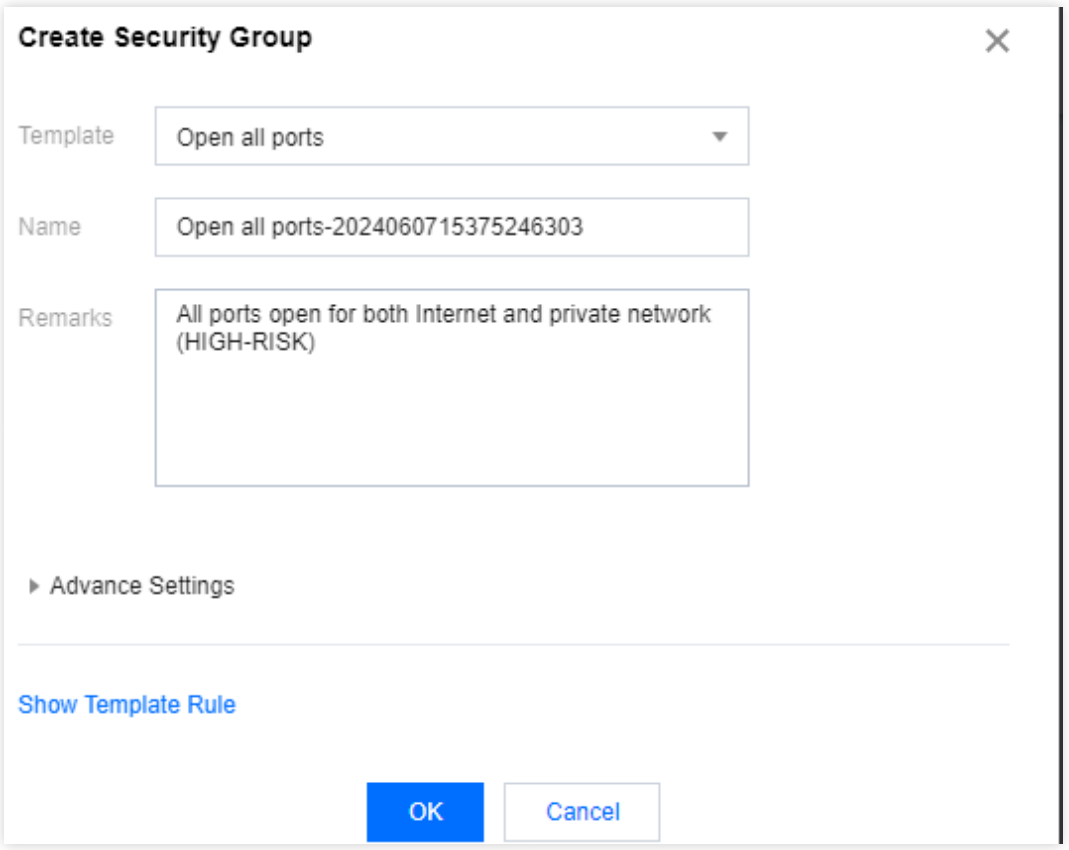
This document takes creating a security group as an example to introduce how to use the security group rules provided by Converge Cloud to configure a security group for the first time when you customize the configuration instance. For more information about security groups, you can go to the Security Group page in the Cloud Virtual Machine console.

Set Security Group

1. When setting security group, select Create Security Group based on actual needs.
   When creating a new security group, use the following two rules:
   - TCP Ports 22, 80, 443, 3389 and ICMP Open: Allow access to SSH port 22, RDP port 3389, HTTP port 80 and HTTPS port 443 and ICMP protocol. The private network is fully opened, while all other ports are denied external access.
   - Open All Ports: Open all ports. It can be accessed from both private network and public network.

     > Note:
     > Opening all ports has a high security risk, please choose carefully.

2. Select the security group rules provided by Converge Cloud based on actual needs.
   For example, if you select TCP Ports 22, 80, 443, 3389 and ICMP Open, the detailed security group inbound/outbound rules will be displayed in Security Group Rules. As shown below:



3. When the configured security group inbound/outbound rules meet your requirements, configure additional information according to the page prompts and click Next: Confirm Configuration Information.

> Note:
> If the two security group setting rules provided by Converge Cloud do not meet your needs, you can also refer to Security Group Application Case to Create Security Group. For security reasons, it is recommended that you open only the ports required for business purposes to avoid unnecessary security risks.

Security group rules

Inbound rule: Indicates that inbound traffic is allowed to the Cloud Virtual Machine associated with the security group.
Outbound rule: Indicates outbound traffic leaving the Cloud Virtual Machine.

- Priority of the security group rules: The higher the position, the higher the priority.
- When Cloud Virtual Machine is bound to a security group without rules, all inbound and outbound traffic is denied by default. (If there are rules, they take precedence).
- When Cloud Virtual Machine is bound to multiple security groups, the priority of the security group:

the smaller the number, the higher the priority.

- When Cloud Virtual Machine is bound to multiple security groups, the default deny rule of the security group with the lowest priority takes effect.

Security Group Limits

For more information, please see Security Group Limits.

Customizing Linux CVM Configuration

This document describes how to customize the configuration of a Linux CVM.
Different from the quick configuration, the custom configuration has complete options, and you can choose the appropriate configuration according to your needs.

Prerequisites

1. Log in to the cloud platform's official website and select Cloud Products > Cloud Computing & Networking > Cloud Virtual Machine.
2. Click Create to enter the Custom Configuration page of CVM.

Selecting Region and Model

1. Choose regions and availability zones. When you need multiple CVMs, you can choose different availability zones to achieve disaster recovery.
2. Select the model and configuration.
   The cloud platform currently provides multiple series based on the underlying hardware. The higher the instance family version, the higher the next generation (hereinafter referred to as old next-generation instance) and new generation instances).
   For best performance, we recommend that you use a new generation instance type when you create instances. For a detailed description of instance types, see Instance Type Overview.

3. Click Next: Select Image to enter the Select Image page.

Selecting Image

1. Select an image provider.
   The cloud platform provides public images, custom images, and shared images. For users who are just starting to use the cloud platform, it is recommended to choose a public image.
2. Select your operating system.
   The cloud platform provides CentOS, Windows Server, Debian, and Ubuntu. You are requested to build the subsequent operating environment by yourself.
3. Select the system version.
4. Click Next: Select Storage and Bandwidth to go to the Select Storage and Bandwidth page.

Selecting Storage and Bandwidth

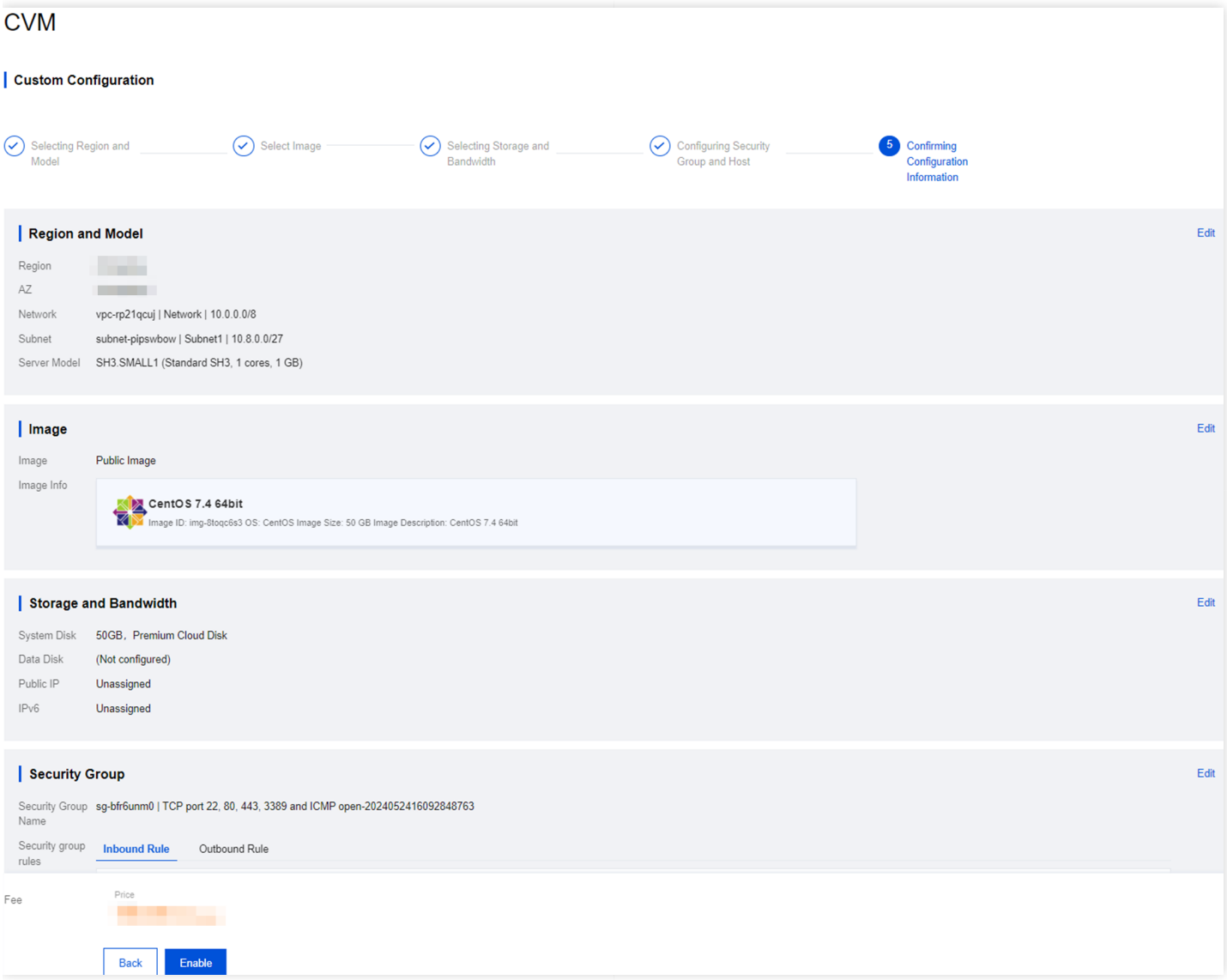
1. Select the system disk size and data disk size.
   The cloud platform provides the following types. (The default system disk is 50 GB, and the system disk size can be selected)
   - Premium Cloud Disk
   - HDD Cloud Disk
   - SSD
2. Select a data disk.
3. Select whether you need a public IP and bandwidth.
4. Click Next: Set Security Groups and Hosts.

Setting up Security Groups and Hosts

1. Security Group: You can choose to create a new security group or use an existing security group.
2. Project: The project can help you solve the complexity of resource grouping and authorization management within a single cloud account.
3. Instance Name: You can choose to name it after creation or name it immediately.
4. Login Method:
   - Custom Password: Enter the host password settings.
   - Random Password: The automatically generated password will be sent through the message center.
5. Set whether to enable security reinforcement, cloud monitoring, and Automation Tools.
6. Advanced Settings (Optional):
   - The computer name of the operating system content.
   - Placement Group: Select as required.
     Note: If the instance type of the sub-machine you created is set by the administrator to not support placement groups, this feature is not available. If modification is needed, please contact the administrator.
   - Label: Select as needed.
   - Custom Data: Used to start the instance configuration, supports Shell format, and the original data cannot exceed 16 KB.

Confirming Configuration Information

After you confirm that the selected region, model, image, storage and bandwidth, and security group information are correct, you can activate it.


CVM
Custom Configuration
Selecting Region and Model
Select Image
Selecting Storage and Bandwidth
Configuring Security Group and Host
5
Confirming Configuration Information
Region and Model
Edit
Region
AZ
Network
vpc-rp21qcuj | Network | 10.0.0.0/8
Subnet
subnet-pipswbow | Subnet1 | 10.8.0.0/27
Server Model
SH3.SMALL1 (Standard SH3, 1 cores, 1 GB)
Image
Edit
Image
Public Image
Image Info
CentOS 7.4 64bit
Image ID: img-8toqc6s3 OS: CentOS Image Size: 50 GB Image Description: CentOS 7.4 64bit
Storage and Bandwidth
Edit
System Disk
50GB，Premium Cloud Disk
Data Disk
(Not configured)
Public IP
Unassigned
IPv6
Unassigned
Security Group
Edit
Security Group Name
sg-bfr6unm0 | TCP port 22, 80, 443, 3389 and ICMP open-202405241609284876 3
Security group rules
Inbound Rule
Outbound Rule
Fee
Price
Back
Enable

Customizing Windows CVM Configuration

This document introduces the custom configuration method for Windows CVM.
Unlike Quick Configuration, Custom Configuration offers comprehensive options, allowing you to select the appropriate configuration based on your requirements.

Prerequisites

1. Log in to the cloud platform's official website and select Cloud Products > Cloud Computing & Networking > Cloud Virtual Machine.
2. Click Create to navigate to the CVM's Custom Configuration page.

Selecting Region and Model

1. Choose regions and availability zones. When you need multiple CVMs, you can choose different availability zones to achieve disaster recovery.

2. Select the model and configuration.
   The cloud platform currently provides multiple series based on the underlying hardware. The higher the instance family version, the higher the next generation (hereinafter referred to as old next-generation instance and new generation instances).
   For optimal performance, we recommend that you use a new generation instance type when you create instances. For a detailed description of instance types, see Instance Type Overview.

   > Note:
   > The series and instance types may vary under different Regions and Availability Zones.

3. Click Next: Select Image to enter the Select Image page.

Selecting Image

1. Select an image provider.
   The cloud platform provides public images, custom images, and shared images.
2. Select operating system: Select Windows.
3. Select the system version.
   - Suitable for running programs developed under Windows, such as .NET.
   - Supports SQL Server and other databases (need to be installed by yourself).

4. Click Next: Select Storage and Bandwidth to go to the Select Storage and Bandwidth page.

Selecting Storage and Bandwidth

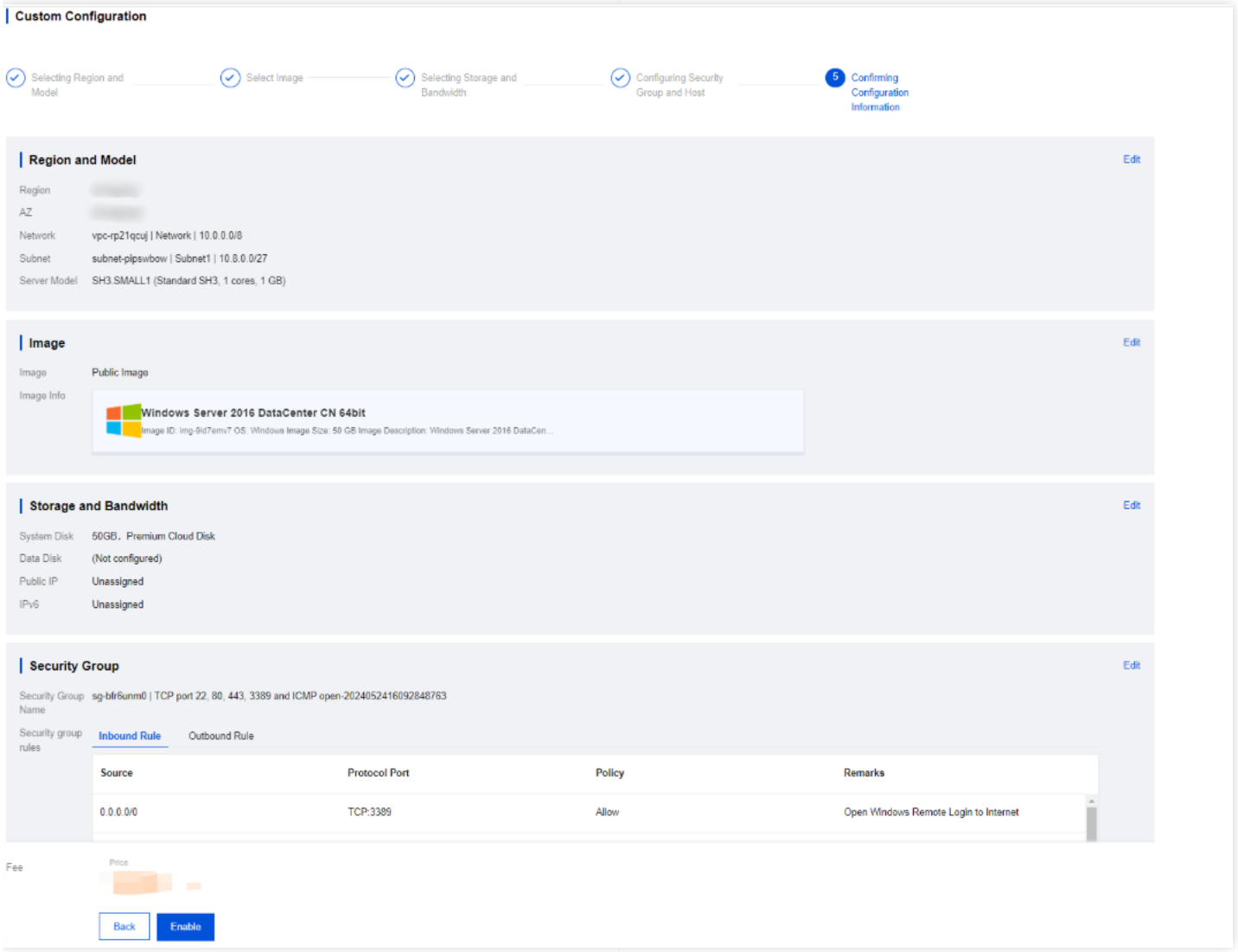
1. Select the system disk size and data disk size.
   The cloud platform provides the following types. (The default system disk is 50 GB, and the system disk size can be selected)
   - Premium Cloud Disk
   - HDD Cloud Disk
   - Cloud SSD
2. Select a data disk.
3. Select whether you need a public IP and bandwidth.
4. Click Next: Set Security Groups and Hosts.

Configuring Security Group and Host

1. Security Group: You can choose to create a new security group or use an existing security group.
2. Project: The project can help you solve the complexity of resource grouping and authorization management within a single cloud account.
3. Instance Name: You can name it immediately or after creation.
4. Login Method:
   - Custom Password: Enter the host password settings.
   - Random Password: The automatically generated password will be sent through the message center.
5. Set whether to enable security reinforcement, cloud monitoring, and Automation Tools.
6. Advanced Settings (Optional):
   - The computer name of the operating system content.
   - Placement Group: Select as required.
     Note: If the instance type of the sub-machine you created is set by the administrator to not support placement groups, this feature is not available. If modification is needed, please contact the administrator.
   - Label: Select as needed.
   - Custom Data: Used to start the instance configuration, supports Shell format, and the original data cannot exceed 16 KB.

Confirming Configuration Information

After you confirm that the selected region, model, image, storage and bandwidth, and security group information are correct, you can activate it.



CVM Dedicated Host
Assigning a Dedicated Instance on CDH

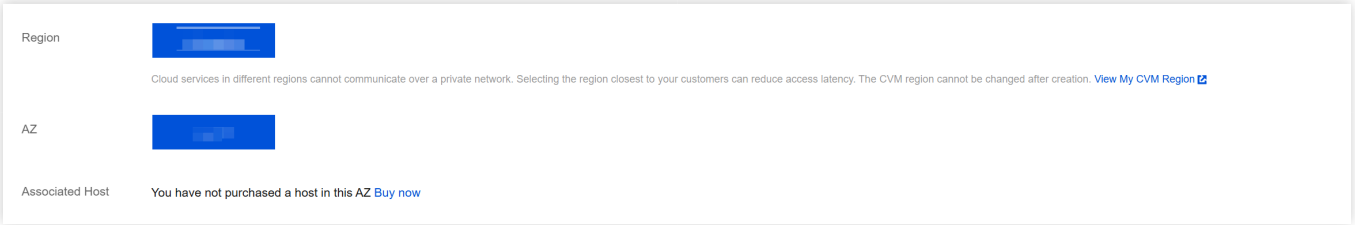
Assigning CVM

1. Go to the instance assignment page.
2. Open the CDH console.
3. Check the host in the list and click Assign CVM above.

Selecting a Host

Select the region and availability zone where the host resources you purchased are located, and select a dedicated host in that availability zone.

- If you select a host, your dedicated instance will be assigned to this specified host.
- If you select multiple hosts of the same type, the hosts you select will serve as the resource pool for assigning dedicated instances.



Select the CPU and Memory Configuration for the Instance

You can customize the CPU and memory configuration of the instance based on the remaining resources of the selected host/host resource pool. The instance resource configuration you specify will affect the number of instances created.

Select Other Configurations of the Instance and Start the Instance

The selection of the dedicated instance image, hard disk, network, and other configurations, as well as the startup of the instance, are the same as for an ordinary CVM instance.

- The instance network defaults to a monthly billing model: When you select the instance's network

configuration, you only need to select the upper bandwidth limit of the instance network.

Operation Guide Overview

This document introduces common scenarios and related operations when using Cloud Virtual Machine instances and Cloud Virtual Machine related products for your reference.

Purchase and Use Cloud Virtual Machine for the First Time

If you purchase and use Cloud Virtual Machine for the first time, it is recommend that you learn about, purchase, and use it in the following order.

1. To understand the concept of Cloud Virtual Machine, see Cloud Virtual Machine Overview.
2. Cloud Virtual Machine selection and purchase. If you are an individual user and use it for the first time, it is recommended that you use the quick configuration method to Configure Windows instance or Configure Linux instance.
3. After the purchase is completed, log in to the Cloud Virtual Machine: Depending on the type of Cloud Virtual Machine you purchased, you can choose Log in to the Windows Instance or Log in to the Linux Instance.
4. (Optional) You can use the purchased Cloud Virtual Machine to build a personal website, forum, or storage files.

Adjust Cloud Virtual Machine Configuration

After you purchase a Cloud Virtual Machine, you may need to adjust the hard disk, network, and other configurations of the Cloud Virtual Machine due to changes in requirements. You can see the following documents to complete the operation.

- Adjust instance configuration.
- Adjust network configuration.
- Reinstall the system.

Reset Password and Key

If you forget your Cloud Virtual Machine password or lose your key, you can see the following document to reset your password or key.

- Reset password
- Create SSH keys

Create, Import, or Delete Custom Image

Image provides all the information required to launch a Cloud Virtual Machine instance. Generally speaking, the image is the installation disk of the Cloud Virtual Machine. Currently, Converge Cloud provides three types of images: public images, custom images, and shared images. The following describes the common operations supported by the image.

- Create custom image
- Delete custom image
- Import image
- Copy image

Troubleshooting for Cloud Virtual Machine

If you are unable to log in to a Cloud Virtual Machine or the Cloud Virtual Machine is operating slowly, you can see the following documents for troubleshooting.

- Solution to the problem of being unable to log in to the Cloud Virtual Machine
- Cloud Virtual Machine network delay and packet loss

Use Limits

Account Limits for Purchasing CVM Instances

- You need to sign up for a cloud platform account.
- Users are required to perform identity verification.

Limits on Image

- Public images: No use limits.
- Custom images: Each region supports up to 50 custom images.
- Shared images: Each custom image can be shared with up to 500 Converge Cloud users, and the accounts of these users should be in the same region.
- For more details, see Image Type Limits.

Limits on Elastic IP

For details, please see Use Limits of EIP.

Limits on Network Interface

For details, see Use Limits of ENIs.

Limits on Bandwidth

- Inbound bandwidth limit (upstream bandwidth):
  - When the fixed bandwidth purchased by the user is greater than 10 Mbps, Converge Cloud will allocate a public network inbound bandwidth equal to the purchased bandwidth.
  - When the fixed bandwidth purchased by the user is less than 10 Mbps, Converge Cloud will allocate 10 Mbps public network inbound bandwidth.

Limits on Disk

For details, see Cloud Block Storage Use Limits.

Limits on Security Group

- Security groups are divided by region. A Cloud Virtual Machine (CVM) can be bind only to security groups in the same region.
- The security group are applicable to any Cloud Virtual Machine instance in the network environment.
- Each user can set up to 50 security groups under each project in each region.
- A maximum of 100 inbound or outbound access policies can be set for each security group.
- One Cloud Virtual Machine can join multiple security groups, and one security group can be associated with multiple Cloud Virtual Machines at the same time.
- Security groups bound to CVM instances on a basic network cannot filter data packets from (or to) relational databases (MySQL and MariaDB) and elastic cache (redis and Memcached) on Converge Cloud. If you need to filter traffic on such instances, you can use iptables.
- Related quota limits are as follows:

Feature Description	Quantities
Security Group	50/region
Access Policy	100/inbound, 100/outbound

Cloud GPU Service

Note: As a special instance of CVM, the purchase, operation and maintenance methods of Cloud GPU Service are the same as those of CVM.

1. Data backup
   Cloud GPU Service provides powerful computing capabilities. To avoid data loss in extreme situations, be sure to back up your data regularly to ensure data security. To ensure data security and reliability, you can also purchase and mount an elastic cloud storage separately.
2. External devices
   Cloud GPU Service does not support direct loading of external hardware devices yet, such as hardware dongles, USB flash drives, external hard drives, bank U keys.
3. Configuration upgrade
   Cloud GPU Service does not support configuration upgrades or degrades yet.
4. Not support hot migration or configuration changes

Limits on VPC

For details, see Virtual Private Cloud Quota Limits.

Limits on Dedicated Lines

For details, see Direct Connect Use Limits.

Instance
Creating an Instance

Scenarios

This document uses the custom configuration method as an example to guide you on how to create a CVM instance.

Prerequisites

Before creating a CVM instance, you need to complete the following tasks:

- Create a cloud platform account.
- To create a CVM instance with a network type of VPC, you need to create a VPC in the target region and a subnet in the target AZ within the VPC.
- If you do not want to use the system's automatically created default security group, you need to create a security group in the target region and add security group rules that meet your business needs.
- If you need to bind an SSH key pair when creating a Linux instance, you need to create an SSH key in the target project.
- If you need to create a CVM instance with a custom image, you need to create a custom image or import an image.

Operation Steps

1. Log in to the cloud platform, select Cloud Virtual Machine > CVM List, and click New to enter the Cloud Virtual Machine purchase page.
    - Custom configuration: suitable for use in specific scenarios, making it convenient for users to purchase CVM instances that meet their specific needs.
2. Follow the on-page prompts to configure the following information:

Category	Required/ Optional	Configuration Instructions
Region/AZ	Required	- Region: It is recommended to choose the region closest to your customers to reduce latency and improve access speed. - AZ: Select according to your actual needs. If you need to purchase multiple CVM instances, it is recommended that you choose different AZs to achieve disaster recovery. For more information about selectable regions and AZs, see Regions and AZs.
Network	Required	It represents a logically isolated network space built on the cloud platform. A VPC consists of at least one subnet. The system will provide a default VPC and subnet for each region. If the existing VPC/subnet does not meet your requirements, you can create one in the VPC console. Note: - Resources within the same VPC communicate with each other by default. - A CVM instance must be created within a subnet that has the same AZ attribute as the CVM. - When you manually allocate private IP addresses, the number of editable IP addresses in the IP address input box is related to the quantities of CIDR in the subnet.
Instance	Required	Based on different underlying hardware, the cloud platform currently offers various instance types. For optimal performance, it is recommended to use the latest generation of instance types. For more details on instances, see Instance Specification.
Image	Required	The cloud platform provides public images, custom images, and shared images. You can choose based on Image Types.
System disk	Required	Used to install the operating system. The default size is 50 GB. Different regions will affect the available types of cloud disks. Please select based on the actual prompts on the page. For more information about cloud disks, please see Cloud Disk Types.
Data disk	Optional	Used to expand the storage capacity of CVM instances and provide efficient and reliable storage devices. By default, no cloud data disk is added. For more information about cloud disks, please see Cloud Disk Types.
Scheduled snapshot	Optional	The snapshot service provides regular backup of cloud disk data to deal with risks such as virus infection and accidental data deletion.
Public IP address	Required	If you need to assign a public network IP address to an instance, select Allocate Now. The IP address allocated in this way cannot be unbound

Category	Required/ Optional	Configuration Instructions
		from the instance, but the public IP address can be converted into an elastic public IP address and then unbound. For more information about elastic IP addresses, see Elastic Public IP.

3. Click Next: Set Security Group and Host to proceed to the configuration page.
4. Follow the on-page prompts to configure the following information:

Category	Required/ Optional	Configuration Instructions
Security group	Required	- If you do not have an available security group, you can select Create Security Group. - If you have an available security group, you can select Existing Security Group. For more information about security groups, please see Security Group.
Instance name	Optional	User-customized, indicating the name of the CVM instance to be created. - If you do not define an instance name, the instance name after creation will be "Unnamed". - If an instance name is defined, it must be within 60 characters. Note: This name is only displayed in the console and is not the hostname of the CVM instance.
Login method	Required	Set the method for users to log in to the CVM instance according to actual needs. - Set password: Customize the password for logging in to an instance. - Associate Key Immediately (Linux Instances Only): Associate an SSH key for a more secure login to the CVM instance. If you do not have a key or the existing key is not suitable, you can click Create Now to create one. For more information on SSH keys, see SSH Key. - Automatically generate password: The automatically generated password will be sent through the message center.
Security reinforcement	Optional	If this option is selected, the HSS security product will be installed to help users build a server security protection system and prevent data leakage.
Cloud Monitor	Optional	Cloud service monitoring is enabled free of charge by default. Install components to obtain host monitoring metrics and display them in the form of monitoring icons. It also supports customizing alarm

Category	Required/ Optional	Configuration Instructions
		thresholds. It also provides three-dimensional CVM instance data monitoring, intelligent data analysis, real-time fault alarms, and personalized data report configuration, allowing users to accurately control the health of their business and CVM instances.
Automation Tools (TAT)	Optional	After purchasing TAP-related features, you can use the capabilities of the Cloud Platform Automation Tool. This is a native Ops deployment tool for CVM, which allows for automated batch execution of Shell commands without remote connection to instances. It can complete tasks such as running automation Ops scripts, installing/uninstalling software, updating applications, and installing patches.
Advanced settings	Optional	Instances can be further configured according to actual needs. - Host name: Users can customize the computer name inside the CVM operating system. After the CVM instance is successfully put into operation, you can check it by logging in to it. - Placement group: Instances can be added to a placement group as needed to improve business availability. For detailed setup, see Placement Groups. Note: If the type of the instance you created is set by the administrator as not supporting placement groups, this feature will be unavailable. If modification is needed, please contact the administrator. - Custom data: Specify custom data to configure an instance, that is, run the configured script when the instance starts. If more than one CVM instance is purchased at a time, custom data runs on all of them. The Linux operating system supports the Shell format, and the Windows operating system supports the PowerShell format, up to 16 KB of raw data. For more details, see Setting Custom Data (Linux Cloud Virtual Machine). Note: Custom data configuration is only supported by certain public images with cloud-init services. For details, see Cloud-Init and Cloudbase-Init.

5. Click Next: Confirm Configuration to proceed to the Confirm Configuration page.
6. Review the information about the CVM you are purchasing and understand the cost details of each configuration.
7. Click Open to complete the creation. After the creation is completed, you can go to the CVM console to check your CVM instance.
8. The instance name, public IP address, private IP address, login name, initial login password, and other

information of the CVM instance will be sent to your account via Message center. You can use this information to log in and manage the instance. Please change your CVM login password as soon as possible to ensure host security.

Logging In to Instance
Logging In to Linux Instances

Overview

After you create a Linux instance, you can choose different log-in methods to connect and log in to the CVM instance based on the local operating system and whether there is a public IP.

Prerequisites

- You have obtained the administrator account and password (or key) for logging in to the instance.
- Administrator Account: The administrator account is different for different types of Linux instances.
  - SUSE/CentOS/Debian: root
  - ubuntu: ubuntu
- Password log-in.
  - If you set an automatic password when purchasing an instance, you can log in to the Converge Cloud console and click the message icon in the upper right corner to enter the site message page, which will contain the CVM log-in administrator account and initial password.
  - If you selected a custom password, the password is the password you specified when you purchased the CVM instance.
- Key log-in.
  - If you choose key log-in when purchasing an instance, please remember the absolute path where the key is stored locally.
  - If you forget the password or key for logging into the CVM, see Reseting the Instance Password or Creating SSH Keys to perform a reset.

The CVM port 22 has been opened: You can check the network connectivity through to check whether port 22 is open. If the port is not open, you can set inbound/outbound rules for the port when configuring security groups.

Remote Log-in to Instances Using VNC

VNC log-in is a way we provide for users to remotely connect to the CVM through a web browser. Users can log in to the CVM via VNC, track the status of the CVM. And through the CVM account, basic management operations on the CVM can be performed.

Applicable Local Operating System

Windows, Linux and Mac OS

Use Limits

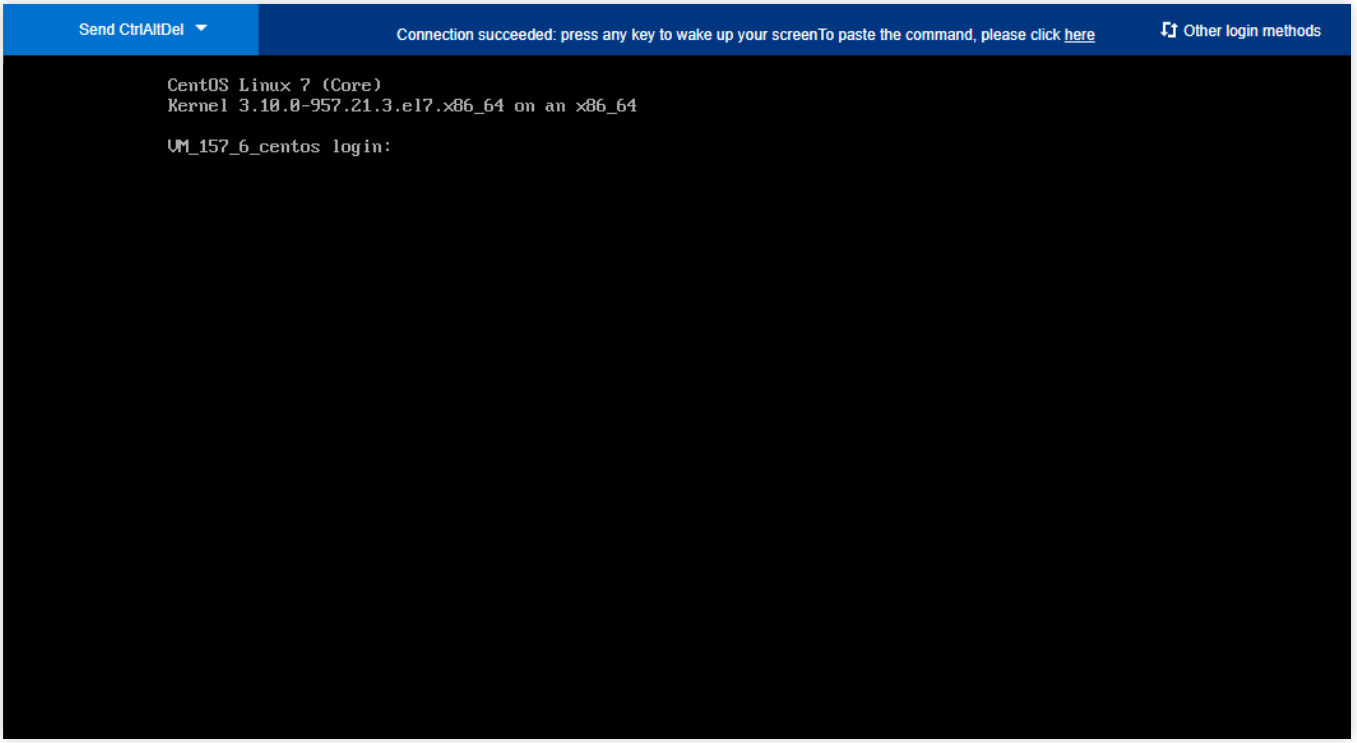
- If you log in the Cloud Virtual Machine via VNC, the CVM currently does not support copy and paste, as well as file upload and file download.
- When you log into the CVM via VNC, you need to use a major browser, such as Chrome, Firefox, IE 10 and above.
- VNC log-in is a dedicated remote terminal, meaning that only one user can log in to the current CVM via VNC at any given time.

Prerequisites

You have obtained the administrator account and password (or key) for logging in to the instance.

Directions

1. Log in to the CVM Console.
2. In the instance list, select the Linux CVM you want to log in to and click Log In.
3. In the pop-up dialog box, enter your user name and password to complete the log-in. As shown below:



Logging In to Windows Instances

Overview

After you create a Windows instance, you can connect to and log in to the CVM instance based on your local operating system.

Prerequisites

- You have obtained the administrator account and password required to remotely log in to the Windows instance.
    - The administrator account for Windows instances is unified as Administrator.
- If you use the system default password to log in to the instance, please go to the Message Center to obtain it.
- The CVM port 3,389 has been opened. You can check if port 3,389 is open by checking network connectivity. If the port is not open, you can set inbound/outbound rules for the port when configuring security groups.

Remote Log-in to Instances Using VNC

VNC log-in is a way provided by Converge Cloud for users to remotely connect to the CVM through a web browser. If the remote log-in client is not installed or the client remote log-in is unavailable, users can log in to the CVM via VNC log-in, observe the CVM status, and perform basic CVM management operations through the CVM account.

Use Limits

- Logging in via VNC does not currently support copy and paste, as well as file upload and download.
- When you log into the CVM via VNC, you need to use a major browser, such as Chrome, Firefox, IE 10 and above.
- VNC log-in provides an exclusive terminal session, meaning that only one user can log in via VNC at any given time.

Applicable Local Operating System

Windows, Linux and Mac OS

Directions

1. Log in to the CVM Console.
2. In the instance list, select the Windows CVM you want to log in to and click Log In.
3. In the log-in window that pops up, select Send Remote Command at the upper left corner and click Ctrl-Alt-Delete to enter the system log-in interface.

Adjusting Configuration
Adjusting Instance Configuration

Scenarios

The hardware equipment of the instance can be adjusted quickly and easily, which is an important manifestation of the flexibility of CVM.
This document describes how to upgrade and downgrade configurations and related precautions.

Limitations and Impacts

Adjusting Configuration Limits

Only instance whose system and data disks are both CBS cloud disks supports configuration adjustment.

- Configuration upgrade
  No limit on the number of configuration upgrades. All changes take effect immediately.
- Configuration downgrade

When you configure an adjustment, the instance specifications that can be changed depend on whether the current availability zone provides the target specifications. Please pay attention to the following restrictions:

- FPGA, and Cloud Bare Metal physical server instances do not support becoming the source or target instance specifications for cross-instance family configuration adjustments.
- Instances configured with a basic network do not support being adjusted to instances that only support VPCs.
- If the target instance specification does not support the CBS type of the current specification configuration, then the adjustment is not supported.
- If the target instance specification does not support the image type configured for the current specification, then the adjustment is not supported.
- If the target instance specification does not support the Elastic Network Interface (ENI) or the quantity configured for the current specification, then the adjustment is not supported.
  For details, see Use Limits of Elastic Networks.
- If the target instance specification does not support the maximum limit of public network bandwidth configured for the current specification, then the adjustment is not supported.

Impact

In very rare cases, the private IP address may change after adjustment. If there is a change in the private IP, we will display it in text on the adjustment page. If there is no relevant display, the private IP will not change.

Operation Steps

> Note
>
> - When your business changes, you can adjust the configuration to meet your needs.
> - When you downgrade the configuration, please confirm the refund details and the new configuration takes effect immediately after forced shutdown and restart, and the CVM will immediately run according to the new configuration.

Adjusting Configuration Via the Console

Single Unit Adjustment

1. log in to CVM Console, and enter the CVM List.
2. In the operation bar on the right side of the instance that needs to be adjusted, choose More > CVM Configuration > Adjust configuration.
3. In Adjust configuration, select Adjustment with CVM shutdown or Adjustment with CVM running, and click Next.
4. In the Select Target Model step that pops up, select the target model and click Next.
   Note: You can filter the specifications that need to be adjusted by selecting the target number of CPU cores or memory capacity and model.
5. After carefully reading the relevant prompts and verifying the information on the prompt page, click Start Adjusting to initiate the configuration change.
   Note: If you select Shutdown Adjustment, then in the Prompt step, you need to check Agree to force shutdown.
6. After you start the adjustment, the adjustment progress bar will be displayed to facilitate your understanding of the adjustment progress. After completion, click Close.

Adjusting Network Configuration

Operation Steps

1. Log in to the Cloud Virtual Machine console.
2. In the In, select the instance that needs a Network Configuration change, click More > CVM Configuration > Adjust Bandwidth.
3. In the pop-up Adjust Bandwidth window, adjust the target bandwidth upper limit, and click Confirm.

Adjusting Disk Configuration

Scenarios

This document describes the operation methods and related precautions of the system disk scale-out.

Limitation Factor

1. The disk configuration can be adjusted only when the system disk is cloud storage.
2. To prevent data loss, the system disk only supports scale-out but not support scale-in.

Operation Steps

1. Log in to the CVM Console.
2. In the cloud host list, select the instance for which you want to adjust the system disk and click More > CVM Configuration > Adjust Disk.
3. In the pop-up Adjust Disk window, select a disk and click Next.
4. Scale out according to actual needs and click Next.
5. Read the page prompts carefully, then click Start adjusting.
6. On the CVM list page, the status column will display Expansion Instance Disk. When this field disappears, the disk adjustment is complete.

Switching Virtual Private Clouds

Prerequisites

1. You can shut down first, and switch to Virtual Private Cloud to operate.
2. Before migration, unbind the private/public network LB and Elastic Network Interface by yourself, release the secondary IP of the primary network interface, and then bind them after migration.
3. During the migration process, the instance needs to be restarted. Do not perform other operations.
4. After migration, check the instance running status, private network access, and remote log-in to see if they are normal.
5. Switching from a basic network to a VPC is irreversible. After a CVM is switched to a VPC, CVM cannot communicate with cloud services on other basic networks.

Operation Steps

1. Log in to the CVM Console.
2. In the instances list, select the instance for which you want to switch the VPC and click More > CVM Configuration > Switching Private Network.
3. On the page that pops up, read the precautions carefully and click Next.
4. Select the target network and subnet, then click Next.
5. Set the pre-allocated IP address and HostName options, and click Next.
   Note: If the pre-allocated IP address is empty, the system will automatically allocate one.
6. Read the precautions carefully, determine whether forced shutdown is required and click OK.
7. On the Instances page, the status column will display Modify instance vpc attributes. After the modification is successful, the corresponding configuration will be updated to the latest network information.

Configuring the Network after Using the Imported Windows Image to Create an Instance

After importing the Windows image and creating a cloud server, log in to the newly created Cloud Virtual Machine via Log-in next to the Cloud Virtual Machine list in the console and configure the network.

The network configuration information of Windows machines is saved in the file C:\qcloud-network-config.ini , open the configuration file, the structure is as follows:

```
[ip]
ip= x.x.x.x
mask = x.x.x.x
gateway = x.x.x.x

[dns]
dns = x.x.x.x
```

Modify the network according to this configuration file information.

Viewing Information
View Instance Information

Overview

To facilitate users to view Cloud Virtual Machine instance information, the paths are as follows:

- View information about all Cloud Virtual Machine instances in a region on the CVM List page in the console.
- View detailed information about the Cloud Virtual Machine instance on the Instance Details page.

Prerequisites

You have logged in to the Cloud Virtual Machine console.

Directions

Viewing Cloud Virtual Machine List Information

1. Select CVM List in the left sidebar to enter the CVM List page.
2. On this page, you can view the following information: ID/host name, monitoring, status, AZ, architecture, host type, configuration, primary IPv4 address, billing mode, placement group, creation time, Action, etc.

   You can click in the upper right corner, and select the list details that you want to display in the pop-up Custom List Fields window.

Viewing Instance Details Information

1. On the CVM List management page, select Region.
2. Find the instance whose details you want to view, click ID/Host Name to enter the CVM Details page. On the CVM Details page, you can view instance information, including instance information, configuration information, image information, SSH keys, Elastic Network Interface, public network IP, monitoring, security group, operation log.

Viewing Instance Monitoring Information

Overview

To facilitate users to view Cloud Virtual Machine instance monitoring information, the cloud platform provides the following two paths to view:

- View the monitoring information of a Cloud Virtual Machine instance in the Cloud Monitor console.
- View the monitoring information of a Cloud Virtual Machine instance on the Instance Details page in the CVM console.
  For public network traffic monitoring information, go to the Cloud Monitor > Traffic Monitor page to view it.

Directions

View instance monitoring information in the Cloud Monitor console

1. Log in to the Cloud Monitor Console.
2. Select Cloud Product Monitoring > CVM to enter the CVM Basic Monitoring Page.
3. Select the region where the instance whose monitoring information you want to view belongs.
4. Click Instance ID to enter the instance monitoring information page, where you can view the monitoring information of the CVM instance, including CPU, memory, private network bandwidth, public network bandwidth, and disk usage.

View instance monitoring information in the Cloud Virtual Machine console

1. Log in to the CVM Console.
2. Select the region where the instance whose monitoring information you want to view belongs.
3. Click Instance ID to enter the Instance Details page.
4. Select the Monitor tab to enter the monitoring information page and view the monitoring information of the Cloud Virtual Machine instance, including CPU, memory, private network bandwidth, public network bandwidth, and disk usage.

Querying Instance Metadatas

Instance metadata refers to data related to an instance and can be used to configure or manage the running instance.

> Note:
> Although instance metadata can only be accessed from within the instance itself, the data is not encrypted. Anyone who can access an instance can view its metadata. Therefore, it is recommended that you take appropriate precautions to protect sensitive data (such as using persistent encryption keys).

Instance Metadata Classification

Provide the following metadata information:

Data	Description	Introducing Version
instance-id	Instance ID	1.0
instance-name	Instance Name	1.0
uuid	Instance ID	1.0
local-ipv4	The private IP address of the instance	1.0
public-ipv4	The public IP address of the instance	1.0
mac	The mac address of the instance eth0 device	1.0
placement/region	Information about the region where the instance is located	Updated on 2017-09-19
placement/zone	Information about the availability zone where the instance is located	Updated on 2017-09-19
network/interfaces/macs/${mac}/mac	Device address of the instance network API	1.0
network/interfaces/macs/${mac}/primary-local-ipv4	Primary private IP address of the instance network API	1.0

Data	Description	Introducing Version
network/interfaces/macs/${mac}/public-ipv4s	Public IP address of the instance network API	1.0
network/interfaces/macs/${mac}/vpc-id	VPC network ID of the instance network API	Updated on 2017-09-19
network/interfaces/macs/${mac}/subnet-id	Subnet ID of the instance network API	Updated on 2017-09-19
network/interfaces/macs/${mac}/local-ipv4s/${local-ipv4}/gateway	Gateway address of the instance network API	1.0
network/interfaces/macs/${mac}/local-ipv4s/${local-ipv4}/local-ipv4	Private IP address of the instance network API	1.0
network/interfaces/macs/${mac}/local-ipv4s/${local-ipv4}/public-ipv4	Public IP address of the instance network API	1.0
network/interfaces/macs/${mac}/local-ipv4s/${local-ipv4}/public-ipv4-mode	Public network mode of the instance network API	1.0
network/interfaces/macs/${mac}/local-ipv4s/${local-ipv4}/subnet-mask	Subnet mask of the instance network API	1.0
payment/charge-type	Instance billing type	Updated on 2017-09-19
payment/create-time	Instance Creation Time	Updated on 2017-09-19
payment/termination-time	Instance destruction time	Updated on 2017-09-19
app-id	AppId of the user to whom the instance belongs	Updated on 2017-09-19
as-group-id	ID of the auto scaling group where the instance is located	Updated on 2017-09-19
spot/termination-time	Spot instance destruction time	Updated on 2017-09-19
/instance/bandwidth-limit-egress	The outbound bandwidth limit of the instance private network, in Kbit/s	Updated on 2017-09-19

Data	Description	Introducing Version
/instance/bandwidth-limit-ingress	The inbound bandwidth limit of the instance private network, in Kbit/s	Updated on 2017-09-19
/meta-data/instance/instance-type	Instance Specifications	Updated on 2017-09-19
/instance/image-id	Instance image ID	Updated on 2017-09-19
/instance/security-group	Instance bound to security group information	Updated on 2017-09-19
/volumes	get disk id	2025-06-06 update
/volumes/${disk_id}/disk-type	Get the disk type	2025-06-06 update
/ntp/servers	Get the ntp server address	2025-06-06 update

Note:
The fields ${mac} and ${local-ipv4} in the above table represent the device address and private IP address of the specified network interface of the instance, respectively.

The target URL of the request is case sensitive. Construct the target URL address of the new request strictly according to the return result of the request.

The current version has changed the placement returned data. If you need to use the data of the previous version, you can specify the previous version path or not specify the version path to access the data of version 1.0. For the placement return data, see Region and Availability Zone.

Query Instance Metadata

Within the instance, you can access the instance's local IP, public network IP, and other data through instance metadata to manage connections with external applications.
To verify the display of instance metadata for all categories from within a running instance, use the

following URI:

```
http://product-cvm-metadata.${region_name}.${domain_name}/latest/meta-data/
```

You can access metadata using the cURL tool or GET request of HTTP, for example:

```
curl http://product-cvm-metadata.${region_name}.${domain_name}/latest/meta-data/
```

- For non-existent resources, the HTTP error code 404 - Not Found is returned.
- Operations on instance metadata can only be performed from within the instance. Complete the instance log-in operation first. For more information about logging in to the instance, see Logging in to the Windows Instance and Logging in to the Linux Instance.

Query Metadata Example

The following example shows how to obtain metadata version information.

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

```
[qcloud-user]# curl http://product-cvm-metadata.${region_name}.${domain_name}/
1.0
2017-09-19
latest
meta-data
```

The following example shows how to view the metadata root directory. Among them, words ending with / indicate the directory, and words not ending with / indicate access to data. For the specific meaning of access data, see the previous Instance Metadata Classification.

```
[qcloud-user]# curl http://product-cvm-metadata.${region_name}.${domain_name}/latest/meta-data/
instance-id
instance-name
local-ipv4
mac
network/
placement/
public-ipv4
```

uuid

The following example shows how to obtain the physical location information of the instance. For the relationship between the returned data and physical location, see Region and Availability Zone.

```
[qcloud-user]# curl http://product-cvm-metadata.${region_name}.${domain_name}/latest/meta-data/placement/region
ap-cityA

[qcloud-user]# curl http://product-cvm-metadata.${region_name}.${domain_name}/latest/meta-data/placement/zone
ap-cityA-3
```

The following example shows how to obtain the private IP address of the instance. If the instance has multiple network interface, the network address of the eth0 device is returned.

```
[qcloud-user]# curl http://product-cvm-metadata.${region_name}.${domain_name}/latest/meta-data/local-ipv4
10.104.13.59
```

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

```
[qcloud-user]# curl http://product-cvm-metadata.${region_name}.${domain_name}/latest/meta-data/public-ipv4
139.199.11.29
```

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

```
[qcloud-user]# curl http://product-cvm-metadata.${region_name}.${domain_name}/latest/meta-data/instance-id
ins-3g445roi
```

The following example shows how to obtain the instance uuid. The instance uuid can be used as the unique identifier of the instance. It is recommended to use the instance ID to distinguish instances.

```
[qcloud-user]# curl http://product-cvm-metadata.${region_name}.${domain_name}/latest/meta-data/uuid
cfac763a-7094-446b-a8a9-b995e638471a
```

The following example shows how to obtain the mac address of the instance eth0 device.

```
[qcloud-user]# curl http://product-cvm-metadata.${region_name}.${domain_name}/latest/meta-data/
mac
52:54:00:BF:B3:51
```

The following example shows how to obtain instance network interface information. Multiple network interfaces will return multiple lines of data, each line of data is the data directory of one network interface.

```
[qcloud-user]# curl http://product-cvm-metadata.${region_name}.${domain_name}/latest/meta-data/network/interfaces/macs/
52:54:00:BF:B3:51/
```

The following example shows how to obtain information about a specified network interface.

```
[qcloud-user]# curl http://product-cvm-metadata.${region_name}.${domain_name}/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 example shows how to obtain information about the Virtual Private Cloud to which a specified network interface belongs.

```
[qcloud-user]# curl http://product-cvm-metadata.${region_name}.${domain_name}/latest/meta-data/network/interfaces/macs/52:54:00:BF:B3:51/vpc-id
vpc-ja82n9op
```

```
[qcloud-user]# curl http://product-cvm-metadata.${region_name}.${domain_name}/latest/meta-data/network/interfaces/macs/52:54:00:BF:B3:51/subnet-id
subnet-ja82n9op
```

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

```
[qcloud-user]# curl http://product-cvm-metadata.${region_name}.${domain_name}/latest/meta-data/network/interfaces/macs/52:54:00:BF:B3:51/local-ipv4s/
10.104.13.59/
```

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

```
[qcloud-user]# curl http://product-cvm-metadata.${region_name}.${domain_name}/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 shows how to obtain the private IP address gateway. This data can only be queried for VPC models. For VPC models, see Virtual Private Cloud.

```
[qcloud-user]# curl http://product-cvm-metadata.${region_name}.${domain_name}/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 shows how to obtain a private IP address to access the public network. This data can only be queried for VPC models. Basic network models access the public network through a public network gateway.

```
[qcloud-user]# curl http://product-cvm-metadata.${region_name}.${domain_name}/latest/meta-data/network/interfaces/macs/52:54:00:BF:B3:51/local-ipv4s/10.104.13.59/public-ipv4-mode
NAT
```

The following example shows how to obtain a private IP address to bind to the public network IP.

```
[qcloud-user]# curl http://product-cvm-metadata.${region_name}.${domain_name}/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 example shows how to obtain the subnet mask of the private IP address.

```
[qcloud-user]# curl http://product-cvm-metadata.${region_name}.${domain_name}/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 example shows how to obtain the instance billing type.

```
[qcloud-user]# curl product-cvm-metadata.${region_name}.${domain_name}/latest/meta-data/payment/charge-type
POSTPAID_BY_HOUR
```

The following example shows how to obtain the instance creation time.

```
[qcloud-user]# curl product-cvm-metadata.${region_name}.${domain_name}/latest/meta-data/paymen
```

```
t/create-time
2018-09-18 11:27:33
```

The following example shows how to obtain the instance destruction time. (Prepaid mode only)

```
[qcloud-user]# curl product-cvm-metadata.${region_name}.${domain_name}/latest/meta-data/paymen
t/termination-time
2018-10-18 11:27:33
```

The following example shows how to obtain the instance destruction time for a spot instance.

```
[qcloud-user]# curl product-cvm-metadata.${region_name}.${domain_name}/latest/meta-data/spot/ter
mination-time
2018-08-18 12:05:33
```

The following example shows how to obtain the AppId of the account to which the sub-machine belongs.

```
[qcloud-user]# curl product-cvm-metadata.${region_name}.${domain_name}/latest/meta-data/app-id
123456789
```

Query Instance User Data

You can specify instance user data when creating an instance, which can be accessed by the child machine after setting cloud-init.

Retrieve User Data

Users can access user data in the following ways within the child machine.

```
[qcloud-user]# curl product-cvm-metadata.${region_name}.${domain_name}/latest/user-data
179, client, cityS
```

Renaming Instance

Scenarios

To facilitate users to manage Cloud Virtual Machine instances in the Cloud Virtual Machine console and quickly identify the name of each Cloud Virtual Machine instance, Converge Cloud supports naming each instance and can be changed at any time with immediate effect.

Operation Steps

Modifying the Name of Single Instance

1. Log in to the CVM console.
2. In the instance list, select the CVM whose instance name you want to modify and click More > CVM Configuration > Rename on the right.
3. In the pop-up Rename 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 Cloud Virtual Machine whose instance names need to be modified and click Rename at the top.
3. In the pop-up Rename window, enter the new instance name and click Confirm.

> Note:
> The names of multiple instances modified in this way are the same.

Resetting Instance Password

Scenarios

If you have forgotten your password, you can reset the instance's log-in password in the console. This document only describes how to change the instance log-in password in the Cloud Virtual Machine management console.

> Note:
> - The password reset operation is allowed only for instances that are in shutdown status.
> - For a running instance, after you change the instance password in the console, the server will be shut down during the password reset process. To avoid data loss, plan the operation time in advance. It is recommended to operate during business off-peak hours to minimize the impact.

Operation Steps

Resetting Password for Single Instance

1. Log in to the CVM console.
2. On the instance management page, select the row of the Cloud Virtual Machine that needs the password reset, click More > Password/Key > Reset Password.
3. In the pop-up Reset Password window, select the type of Username, enter the user name whose password needs to be reset, select the corresponding new Password and Confirm Password, and click Confirm.

Resetting Passwords for Multiple Instances

1. Log in to the CVM console.
2. On the instance management page, select the Cloud Virtual Machine whose password needs to be reset and click Reset Password.
3. In the pop-up Reset Password window, select the type of Username, enter the user name whose password needs to be reset, select the corresponding New Password and Confirm Password, and click Confirm.

Managing Instance IP Address
Getting the Private IP Address and Setting DNS

This document describes how to obtain the private IP address of the instance and how to set private network DNS.

Obtain the Private IP Address of the Instance

Using Console to Obtain

1. Log in to the CVM console.
2. On the Instance Management page, select the instance whose private IP address you want to view, move the mouse to the Primary IPv4 Address column, and will display.
3. Click to copy the IP address.

Use Instance Metadata to Obtain

1. Log in to the CVM.
2. Use the CURL tool or GET requests of HTTP to access instance metadata.

   > Note: The following operations take the cURL tool as an example.

   Execute the following command to obtain the private IP address.

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

   The returned information is the private IP address, as shown in the following figure:

For more information about instance metadata, see View Instance Metadata.

Set Private Network DNS

When network resolution errors occur, you can manually set private network DNS based on the type of CVM operating system.

Linux

1. Log in to the Linux CVM.
2. Execute the following command to open /etc/sysctl.conf file.

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

3. Press i to switch to Edit mode, and modify DNS IP according to the corresponding region in the Private Network DNS list.
   For example, change the private DNS IP address to the private DNS server in City B region.

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

4. Press Esc, enter :wq to save the file and return.

Windows

1. Log in to the Windows CVM.
2. In the operating system interface, open Control Panel > Network and Sharing Center > Change Adapter Devices.
3. Right click Ethernet and select Attribute to open the Ethernet Attribute window.
4. In the Ethernet Attribute window, double-click Internet Protocol Version 4 (TCP/IPv4).
5. Select Use the Following DNS Server Address, and modify the DNS IP according to the different regions corresponding to the Private Network DNS list.
6. Click OK.

Modifying Private IP Addresses

Overview

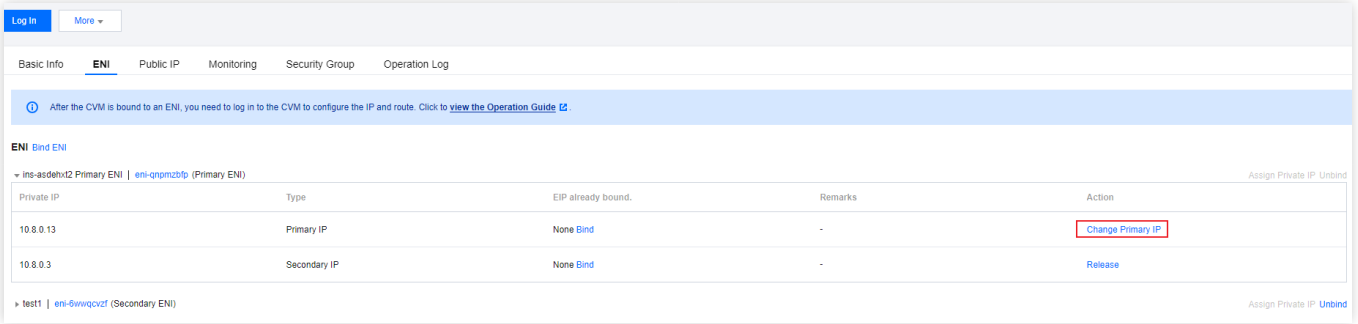
You can directly modify the private IP address of a Cloud Virtual Machine (CVM) instance in the Virtual Private Cloud in the console, or you can change the private IP address of an instance by changing the subnet to which the CVM instance belongs. This document guides you to modify the private IP address of a CVM instance in the Virtual Private Cloud in the Cloud Virtual Machine console.
For more information about how to change the subnet, see Change Instance Subnet.

Limitation Factor

- Changing the primary IP of the primary network interface will cause the associated Cloud Virtual Machine to automatically restart.
- The secondary network interface cannot modify the primary IP.

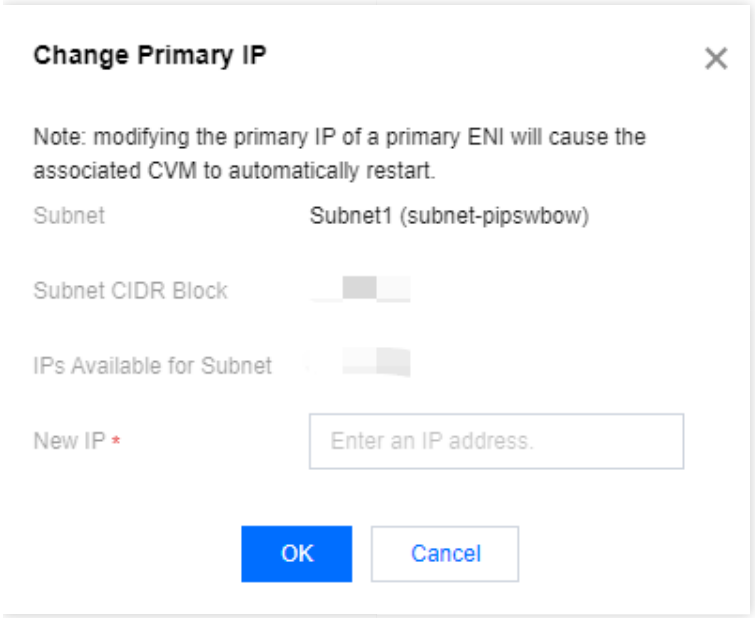
Directions

1. Log in to the CVM Console.
2. Select the region where the instance whose private IP address is to be modified belongs, and click ID/Host Name of the instance to enter the Instance Details page.
3. On the Instance Details page, select the ENI tab and click Change Primary IP.



4. In the pop-up Change Primary IP window, enter a new IP, click OK, and wait until the instance is restarted to take effect.

> Note:
> Only the private IP address that belongs to the current subnet CIDR can be filled in.



Changing Public IP Addresses

Scenarios

This document guides you on how to change your public IP address. There are two ways to change the public IP address:

- Directly change the public IP address
- First change to an Elastic IP, then unbind the Elastic IP.

Must-Knows

If you select Directly change the public IP address, you should note the following:

- Each account can change the public IPs of Cloud Virtual Machine (CVM)s in the same region a maximum of 3 times per day.
- The public IP address of a single instance can only be changed once.
- After the change, the original public IP address will be released.

If you select First change to an Elastic IP, then unbind the Elastic IP, you should note the following:

- When an elastic IP address is bound to a Cloud Virtual Machine instance, the current public IP address of the instance will be released.
- The quota for Elastic IP for a single account in a single region is 20.
- To ensure effective use of IP resources, Elastic IP addresses that are not bound to instances are charged a small fee per hour.

Prerequisites

You have logged in to the Cloud Virtual Machine console.

Operation Steps

Method 1: Directly Change the Public IP Address

1. On the Instance Management page, locate the CVM whose IP address you want to convert and click More > EIP > Bind EIP.
2. In the pop-up box, confirm the information and click Confirm to complete the replacement.

Method 2: First Change to an Elastic Public IP, Then Unbind It

Changing to Elastic IP

1. On the Instance Management page, select the row of the CVM whose IP is to be converted and click .
2. In the pop-up Convert into EIP window, click Confirm.

Unbind the Elastic IP address

1. After the conversion is complete, locate the CVM and click More > EIP > Unbind EIP.
2. In the pop-up window, select "Free allocation of public network IP after unbinding (Note: This public network IP is randomly assigned and cannot be unbound from the instance.)", and then click OK.
3. In the pop-up dialog box, click OK to complete the change.

Releasing the Elastic IP (Optional)

> Note:
> When an EIP is unbound, it remains under your account. To avoid being charged for unused idle IP addresses, it is recommended to perform the following steps to release any EIPs that are not bound to instances.

1. In the left sidebar, click Elastic IP to enter the Elastic IP management page.
2. On the Elastic IP management page, select the Elastic IP you just unbound and click Release.
3. In the pop-up Release Elastic IP window, enter the Elastic IP address to be released and click Confirm.
4. In the pop-up Prompt Box, click Confirm.

Change Instance Subnet

Overview

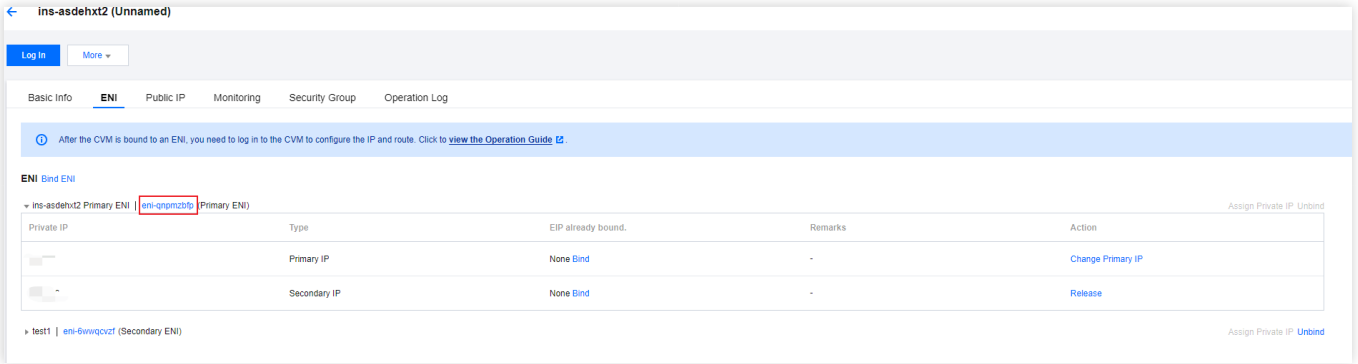
This document guides you to directly change the subnet to which a Cloud Virtual Machine instance in a Virtual Private Cloud belongs in the console.

limitation factor

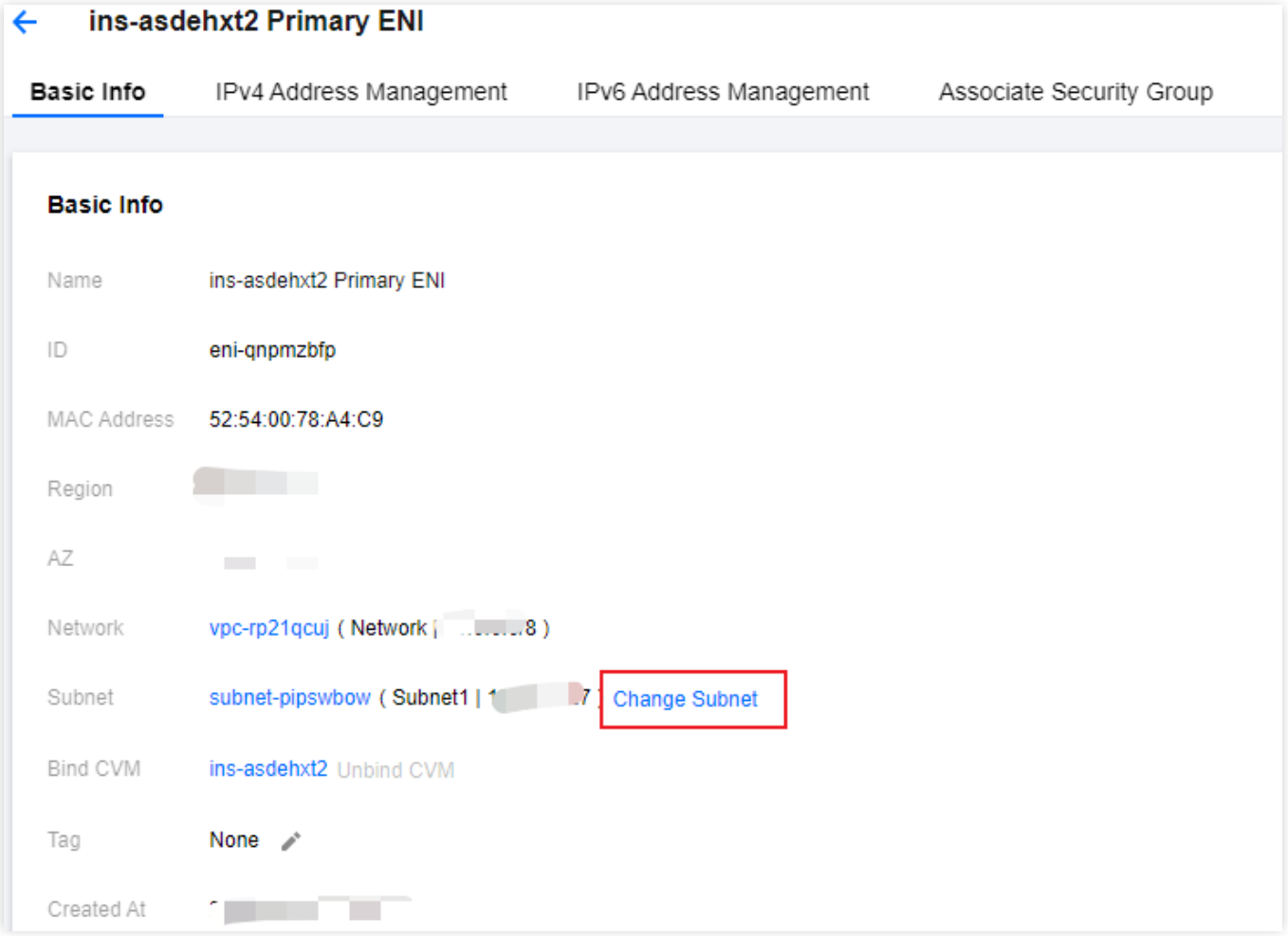
- Changing the subnet will cause the associated Cloud Virtual Machine to automatically restart.
- The secondary network interface cannot change the subnet.

Directions

1. Log in to the CVM Console.
2. On the CVM host list page, select the region where the instance whose subnet needs to be changed belongs.
3. On the CVM host list page, find the instance whose subnet needs to be changed and click ID/Host Name of the instance to enter the Instance Details page.
4. On the Instance Details page, select the ENI tab and click Primary ENI ID.
   Enter the Primary Network Interface Management page.



5. On the Primary Network Interface Management page, click Change Subnet.



6. In the pop-up Change Subnet window, select a new subnet, enter a new primary IP, and click OK.
   After the instance is restarted, it takes effect.

> Note:
> - If you have not yet created a subnet in this availability zone, please create one first.

- When entering the new primary IP, you can only enter a private IP that belongs to the current subnet CIDR.

Changing the Security Group

Scenarios

A security group is a stateful virtual firewall with packet filtering. It is used to set network access control for one or more Cloud Virtual Machine (CVM)s and is an important network security isolation method provided by Converge Cloud. Creating a CVM instance necessitates assigning a security group to the instance. Converge Cloud allows users to change the security group to which the instance belongs after creating the CVM instance.

> Note:
> If you want to configure a new security group for the instance, please create a security group first. For specific operations, see Creating Security Group.

Prerequisites

You have logged in to the Cloud Virtual Machine console.

Operation Steps

Changing a Configured Security Group

There are two configuration entries for configuring security groups: configure on the instance management page (that is, the CVM list page) or configure on the instance details page.

Configuring Security Groups on the Instance Management Page

1. On the CVM list page, select the CVM you want to reassign to a new security group and click More > Configure Security Group.
2. In the Configure Security Group window that pops up, check the new security group name (multiple selections are allowed) and click Confirm to complete the process of changing the security group.

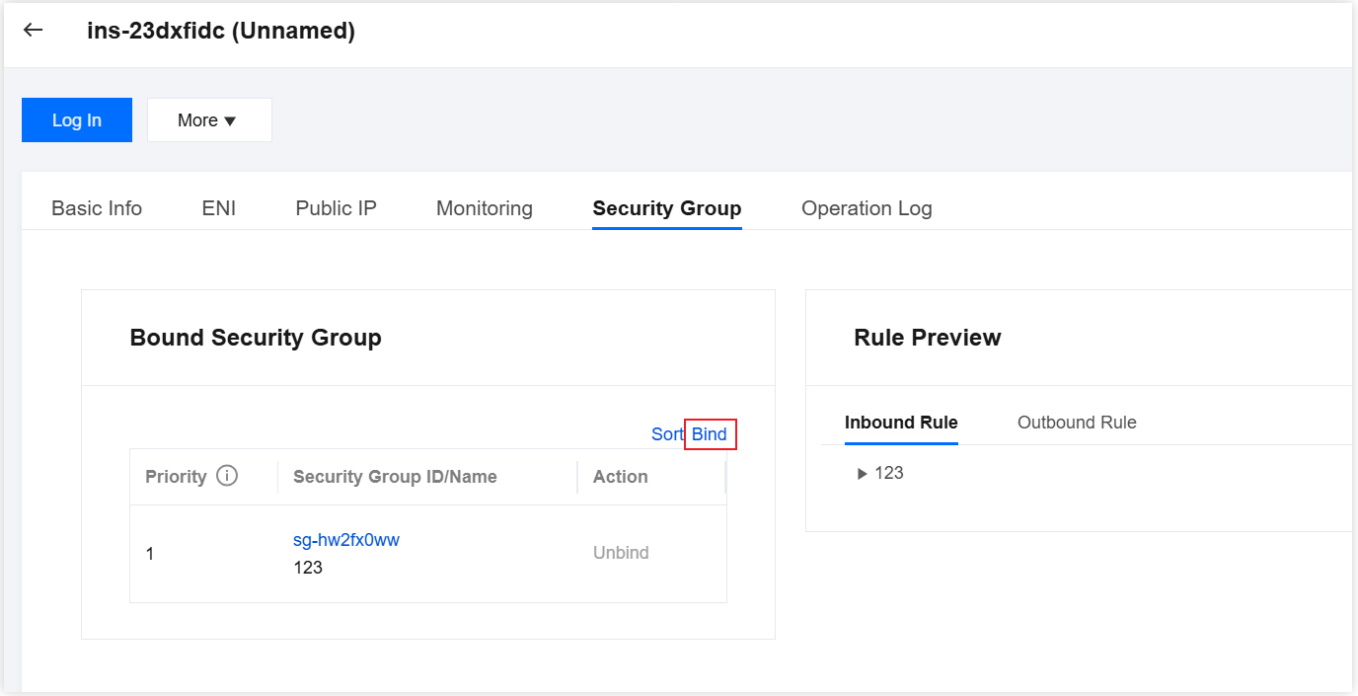
Configuring Security Groups on the Instance Details Page

1. On the CVM list page, click the ID/hostname of the CVM instance whose security group needs to be changed to enter the instance details page.
2. On the instance details page, click More Actions > Configure Security Group in the upper right corner.

3. In the Configure Security Group window that pops up, check the new security group name (multiple selections are allowed) and click Confirm.

Changing a Bound Security Group

1. On the CVM list page, click the ID/hostname of the CVM instance whose security group needs to be bound to enter the instance details page.
2. On the instance details page, select the Security Group tab and click Bind in the Bound Security Group column.



3. In the Configure Security Group window that pops up, select the security group to be bound according to actual needs and click OK to complete the binding.

Searching for Instance

Overview

By default, the Cloud Virtual Machine console displays the Cloud Virtual Machine of all projects in the current region. To help users quickly search for Cloud Virtual Machines in the current region, Converge Cloud provides a Cloud Virtual Machine search feature, which can currently be filtered by resource attribute dimensions such as project, instance type, availability zone, IP, instance ID, and instance name.

Directions

1. Log in to the CVM Console.
2. In the search box, enter the content you want to search for according to your actual needs and click to search.
   - Select a searchable resource dimension (such as host name, host ID, host type), and click .
   - Enter a keyword and click .

Exporting Instance

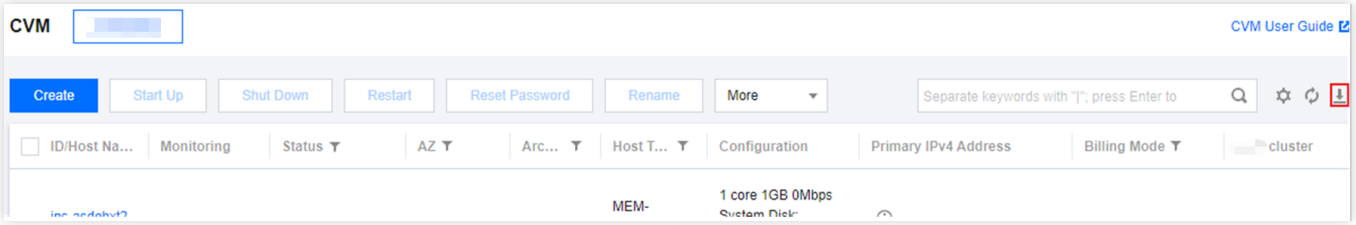
Overview

You can export a list of Cloud Virtual Machine instances in a certain region in the console and customize the fields in the exported list. You can select up to 26 fields for custom export fields. The fields currently supported for export include: ID, host name, status, region, availability zone, host type, operating system, image ID, CPU (cores), memory (G), bandwidth (Mbps), primary IPv4 public network IP, primary IPv4 private network IP, primary IPv6 address, system disk type, system disk size (GB), data disk type, data disk size, network, subnet, associated vpc, project, creation time, billing mode, tag, and placement group.

Directions

1. Log in to the CVM Console.
2. Select region.

3. Click in the upper right corner of the instance list.



4. In the pop-up Custom Export Fields window, check the fields you want to export and click OK to export.

Restarting Instances

Restarting is a common way to maintain the Cloud Virtual Machine. Restarting an instance is equivalent to restarting the operating system of a local computer.

Overview

- Restart preparation: The instance can not provide services normally during the restart, so before it is restarted, make sure that the Cloud Virtual Machine has suspended business requests.
- Restart operation mode: It is recommended to use the restart operation provided by the cloud platform to restart the instance instead of running the restart command in the instance (such as the restart command in Windows and the Reboot command in Linux).
- Restart time: Generally speaking, the restart operation only takes a few minutes.
- Instance physical characteristics: Restarting an instance does not change the instance's physical characteristics. The instance's public network IP, private network IP, and any stored data do not change.

Restarting an Instance in the Console

1. Log in to the CVM console.
2. Restart instance.
    - Restart one instance: Select the instance you want to restart and click Restart at the top of the list. Alternatively, choose More > CVM Status > Restart in the right-side action column.
    - Restart multiple instances: Select all instances that need to be restarted, and click Restart at the top of the list to restart instance in batch. Instances that cannot be restarted will display the reason.

Shutting Down Instance

Scenarios

If you need to stop the instance service or need to perform a configuration that can only be modified when the instance is shut down, you can shut down the instance. Shutting down an instance is equivalent to shutting down the local computer.

Must-Knows

- You can use system commands to shut down the instance (such as the shutdown command in Windows and the shutdown command in Linux), or you can use the Converge Cloud console to shut down the instance. It is recommended to open the console during shutdown to view the shutdown process to see if there is any problem.
- After the instance is shut down, services will not be available. Therefore, before the shutdown, ensure that the Cloud Virtual Machine has suspended business requests.
- The instance is shut down normally. The status changes to Shutting Down first, and then changes to Shutdown after the shutdown is complete. If the shutdown time is too long, problems may occur. For details, see Shutdown Related to avoid forced shutdown.
- After the instance is shut down, all storage remains connected to the instance and all disk data is preserved. Data in memory will be lost.
- Shutting down an instance does not change the physical characteristics of the instance. The public network IP and private network IP of the instance remain unchanged; Elastic IP maintains the binding relationship, but due to the service interruption, you will get an error response when accessing these IPs.
- If the shutdown instance belongs to the backend server cluster of the Cloud Load Balancer instance, after shutdown, services will not be available.
- If a health check policy is configured, the shutdown instance can be automatically masked and no requests will be forwarded to it. If no health check policy is configured, the client may receive a 502 error response. For more information, see Health Check.
- If the shutdown instance is in Auto Scaling Group, the Auto Scaling service will mark the shutdown instance as poor health, may remove it from the auto scaling group, and launch a replacement instance. For more information, see Auto Scaling.

Operation Steps

Shut down instance via console

1. Log in to the CVM console.
2. Select different operation modes according to actual needs.
    - Shut down a single instance: Select the instance that needs to be shut down, and in the action bar on the right, choose More > CVM Status > Shut Down.
    - Shut down multiple instances: Select all instances you want to shut down and click Shutdown at the top of the list to shut them down in batch.
      Instances that cannot be shut down will display the reason.

      > Note:
      > If a manual forced shutdown command is issued, the forced shutdown action will be performed first.

Shut down the Instance via API

Refer to API Documentation > StopInstances API.

Subsequent Operations

You can modify the following instance attributes only when the instance is shut down:

- Instance configuration (CPU, memory): To change the instance type, see Adjusting Instance Configuration.
- The size of the mounted Cloud Block Storage: To adjust the size of the Cloud Block Storage, see Scale-out Cloud Block Storage.
- Change password: Refer to Log-in Password.
- Load key: Refer to SSH Keys.

Terminating Instances

This document describes the overview and methods of terminating and releasing instances.

Overview

When you no longer need an instance, you can terminate it and the services running on the terminated instance will be terminated.

Related Impact

When an instance is in the terminateed status, the instance data, elastic IP, and billing are affected as follows:

- Billing related: Once the instance status changes to being terminated or released, no charges will be incurred for the instance.
- Instance data: The mounted local disk and non-elastic Cloud Block Storage will be released together, and the data cannot be recovered. Please back up in advance. The elastic Cloud Block Storage will follow its own life cycle.
- Elastic IP: The elastic IP of the terminated instance (including the IP on the secondary network interface) will continue to be retained, and idle IP will incur fees. If there is no need to keep it, release it in time.

Terminating an Instance

Using Console to Terminate an Instance

When you no longer need the instance, you can choose to terminate the instance. At the same time, the services running on the instance will be completely interrupted.

After the instance is terminated , the local disk and non-elastic Cloud Block Storage mounted on the instance will be returned, and the data stored on the storage will be lost. Whether the elastic cloud storage mounted on the instance is released when it is terminated depends on whether you choose to terminate it together with the instance.

1. Log in to the CVM Console.
2. Select different instance termination operations based on actual needs.

- Terminate one instance: In the list, find the instance you want to terminate and click More > CVM

Status > Terminate on the right.

- Terminate instances in batch: Select all instances that need to be terminated, and click More > Terminate at the top. Instances that cannot be terminated will display the reason.

3. In the pop-up window, you can select Terminate Now or Scheduled Termination of instances.
    - Terminate Now: If you select immediate termination, you can choose to release the resources immediately or after a period of time. If you choose to release immediately, the data related to the instance will be cleared and cannot be restored. If you choose to release resources after a period of time, the instance will be moved to the Recycle Bin and will not be released until the expiration date.
    - Scheduled Termination: If you select scheduled termination, you need to set a scheduled termination time. After the expiration, the instance will be scheduled to be terminated and released, and the data cannot be restored.
4. Select the termination method, then click Next Step: Confirm Termination to confirm the actual and related resources to be terminated and retained.
5. Confirm the termination of resources, then click Submit.

Reinstalling System

Scenarios

The system reinstallation operation can recover an instance to its initial status after its first launch. It serves as a key recovery method when the instance encounters system failures. This document provides guidance on how to reinstall the operating system.
CVMs support the following two types of system reinstallation, both of which are available across all regions.

- Reinstall on the same platform: For example, Linux is reinstalled as Linux, and Windows is reinstalled as Windows.
- Reinstall on different platforms: For example, Linux is reinstalled as Windows, and Windows is reinstalled as Linux.

> Note:
> Currently, all newly added Cloud Block Storage instances and local disk instances support system reinstallation on different platforms.

Must-Knows

- Reinstallation preparation: The contents of the system disk are lost after reinstallation, so you need to back up important information on the system disk before reinstallation. If you need to preserve system running data, it is recommended that you create a custom image before you reinstall the system and select the image for reinstallation.
- Image selection suggestions: It is recommended to use the image provided by Converge Cloud or a custom image for reinstallation. It is not recommended to use images from unknown sources or other sources. Do not perform other operations while reinstalling the system disk.
- Reinstall time: Generally speaking, it takes 10 minutes to 30 minutes.
- Instance physical properties: The public network IP of the instance will not be changed.
- System disk related: The system disk size can be adjusted during reinstallation, but only Cloud Block Storage is supported.
- Subsequent operations: After the system disk is reinstalled, the data on the data disk is not affected but needs to be mounted again.

Operation Steps

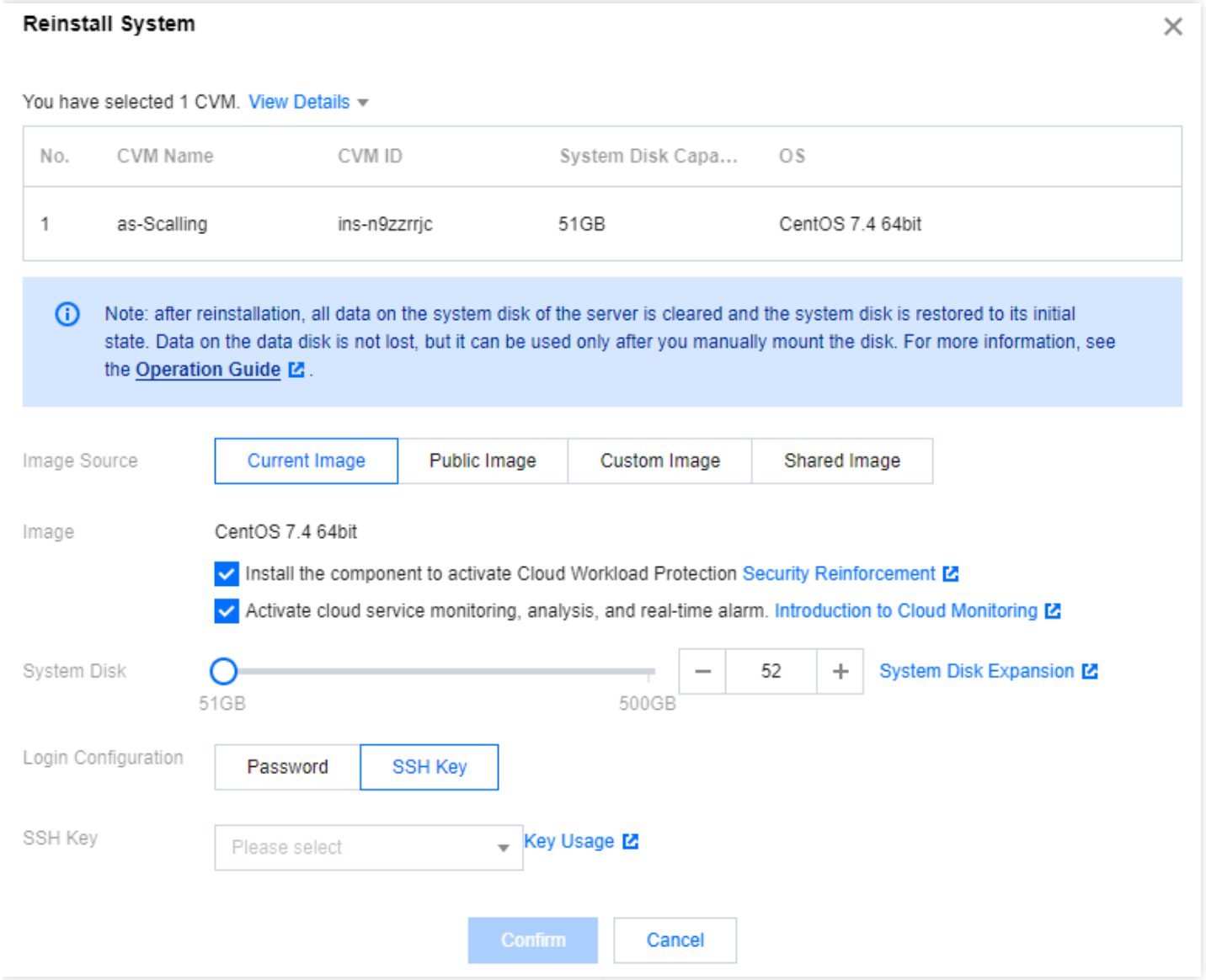
You can reinstall the operating system in the following ways:

- Using Console to Reinstall System
- Use API to Reinstall System

Using Console to Reinstall System

1. Log in to the CVM console.
2. In the row of the instance where the system needs to be reinstalled, click More > Reinstall System.
3. In the pop-up Reinstall System window, select Use the current machine image or other image, adjust the disk size, enter the password, and click Start Reinstallation.

   > Note:
   > The password is the one you configured when configuring the Cloud Virtual Machine instance or the one that is automatically generated. If you have forgotten your Cloud Virtual Machine log-in password, see Reset Instance Password to reset the password.



Using API to Reinstall System

Refer to API Documentation > ResetInstance API.

Cloning an Instance

Scenarios

The cloud host cloning feature allows you to quickly create a CVM instance by making a full machine image of the current instance.

Prerequisites

A cloud host is running in normal status without any data disks.

Operation Steps

1. Log in to the CVM console.
2. Choose Cloud Host > Cloud Host List to find the cloud host to be cloned in the list.
3. Choose More > Clone Cloud Host in the operation column to go to the page for confirming the configuration information.
4. Click Previous or Next as needed to edit the information on the page and enter the clone quantity.
5. Click Enable to complete the cloning process.

Manage Instance Launch Templates

Overview

The instance launch template stores the configuration information (except the instance password) required to create the Cloud Virtual Machine instance. You can use the specified instance launch template to quickly create an instance to improve efficiency and user experience. This document describes how to create, manage, and use instance launch templates through the Cloud Virtual Machine console to quickly create instances.

Directions

Create Template

1. Log in to the CVM Console.
2. In the left sidebar, click CVM > Cloud Host Template to enter the template list page.
3. Click Create, select configurations as needed on the Create CVM Template page, enter the template name and description in Step 5: Confirm Configuration Information, and click Activate to create the template.
4. After the template is created, you can view it on the Template List page.

Edit Template

1. On the Template List page, click More > Edit Template in the Operation column of the template you want to modify to enter the Edit CVM Template page.
2. Adjust the configuration as needed. After the adjustment is completed, click Save.
3. Return to the Template List page, the template details have been updated.

Rename Template

1. On the Template List page, click More > Rename in the Operation column of the template you want to modify to enter the Rename page.
2. Enter a new name in the new template name input box, then click OK to modify the template.

Deleting Template

1. On the Template List page, click More > Delete in the Operation column of the template you want to modify to enter the Delete page.
2. Read the relevant information about deletion carefully, then click Delete to delete the template.

Create an instance

1. On the Template List page, click Create CVM in the Operation column of the template to enter the Create CVM page.
2. Select the purchase quantity as needed, confirm that you have no objection to the cost, and click Create to create the instance.

Rescue Mode

Overview

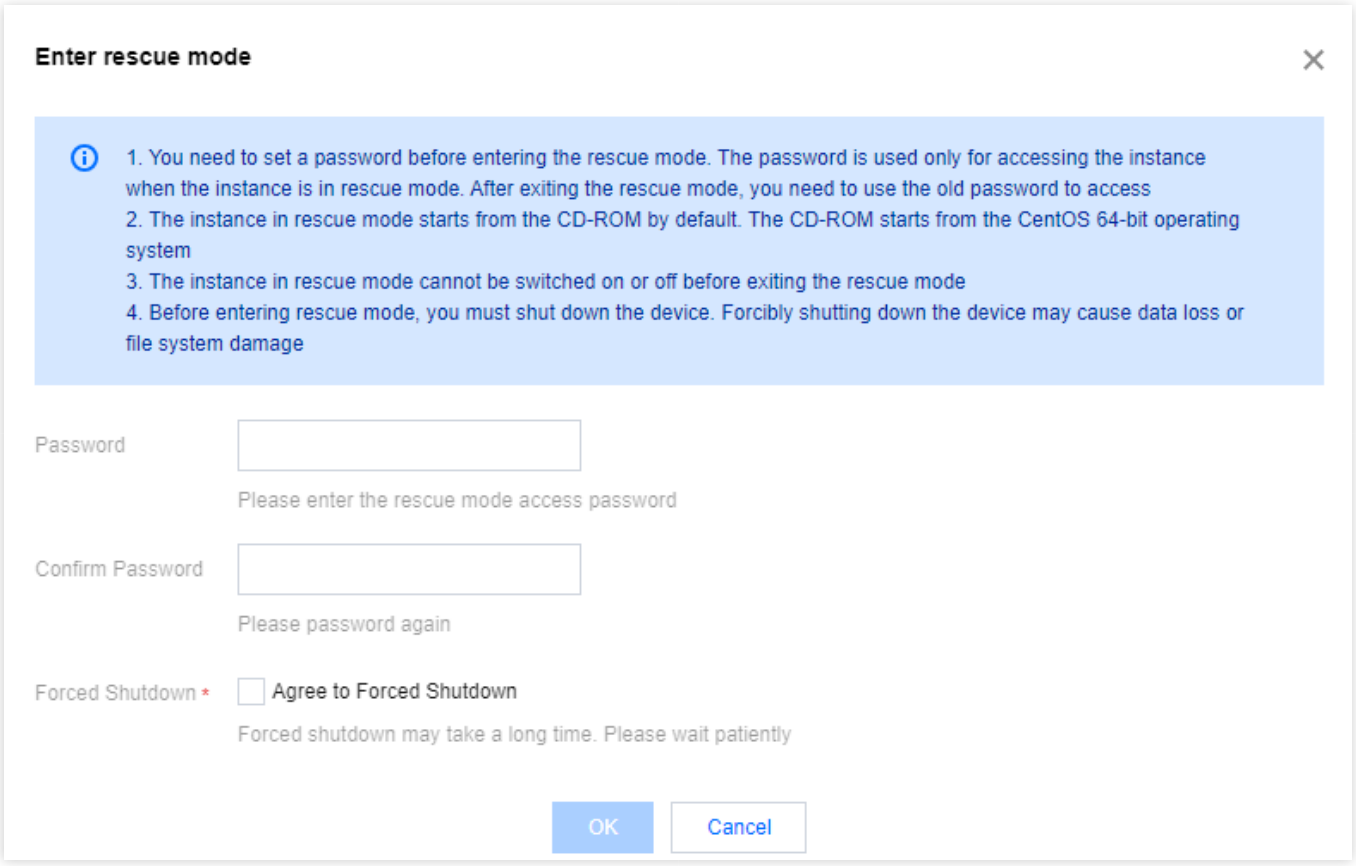
When using the CVM operating system, if the machine grub boot file is lost, key system files are missing, and lib dynamic library files are damaged or missing, the operating system may fail to enter the single-user mode and complete the repair. In this case, you need to use the CVM rescue mode to repair the system. This document describes how to use the rescue mode through the CVM console.

Directions

Enter Rescue Mode

> Note:
> Before you enter rescue mode, it is strongly recommended that you back up the instance to prevent any impact caused by misoperation. Cloud Block Storage can be backed up via Create Snapshots, and local system disks can be backed up via Create Custom Images.

1. Log in to the CVM console.
2. In the Action column of the instance for which you want to enter rescue mode, click More > Operation and Detection > Enter Rescue Mode.
3. In the Enter Rescue Mode page that pops up, enter the instance login password and confirm the password, then click OK.
   If the instance is in the running state, you need to check the Force Shutdown option before clicking OK.



4. After the rescue mode is entered, the status of the CVM list is displayed as Rescue Mode and multiple functions in the Action column are grayed out, with a prompt Instance (instance ID) that does not support rescue mode.

Exit Rescue Mode

1. After the instance is repaired, click More > Operation and Detection > Exit Rescue Mode in the Operation column.
2. Read the prompts carefully, then click OK. After the CVM list is entered, the status displays Exiting rescue mode.
3. Wait for a while and the status changes to Running, indicating that the rescue mode has been exited successfully. Other operations can be performed normally.

Billing Suspension Upon Shutdown

Scenarios

Billing suspension upon shutdown means you will not be charged for CPU and memory after pay-as-you-go instances enter shutdown status through a shutdown operation. Components such as cloud disks (system disks and data disks), public network bandwidth, and images will still be billed.

Use Limits

Billing suspension upon shutdown only applies to pay-as-you-go instances whose system disks and data disks are both cloud disks.
The feature does not apply to the following scenarios:
Instances are started up and shut down within the instances.
Instances are equipped with local disks.
Instances are shut down due to overdue payment. The billing for the instances and associated resources stops after they are shut down due to overdue payment. Computing resources and public IP addresses will be released. The billing will resume if the account balance becomes positive after a top-up.
For instance types that support pay-as-you-go three-tier pricing, the accumulation of usage time for the three-tier pricing is suspended during the billing suspension period. After the instances are restarted, the accumulation resumes from where it left off before the instances are shut down.
If a batch shutdown operation involves instances that are eligible for billing suspension upon shutdown and others that are not, then:
Instances that support billing suspension upon shutdown will not be charged for CPU and memory after shutdown.
Instances that do not support billing suspension upon shutdown will continue to be normally charged after shutdown.

Impact After Enabling the Feature

After billing suspension upon shutdown is enabled, the following effects occur when an instance is shut down:
Since the CPU and memory of the instance will be released, restarting the instance may fail due to insufficient resources. In this case, you can try restarting the instance later. If it still fails, you may attempt to adjust the instance configuration.
If the instance has been assigned a public IP address, the public IP address will be automatically released

after shutdown, which may cause the instance to fail upon restart. After a successful restart, the instance will be assigned a new public IP address, while the private IP address remains unchanged. To prevent changes to the public IP address, you can convert the public IP address to an EIP address before shutting down the instance. For an instance bound to an EIP address, the EIP address is retained after shutdown and remains upon restart. No idle fees will be charged for the EIP address during the shutdown period.
During the shutdown period, operations (such as adjusting disks, modifying network configurations, reinstalling the system, restarting instances, and resetting passwords) cannot be performed. If these operations are required, please perform them after starting the instance.
When Ops operations such as configuration adjustment, disk modification, or system reinstallation are performed, the instance must be shut down. During shutdown, the billing suspension upon shutdown policy is not applied.

Operation Steps

1. Log in to the CVM console.
2. On the instance management page, you can shut down one or multiple instances at a time as needed:
    - Shut down a single instance: Proceed according to the actually used view mode.
        - List view: Select the instances to be shut down, and then choose More > Instance Status > Shutdown in the operation column on the right side.
    - Shut down multiple instances: Select all instances to be shut down and click Shutdown at the top of the list.
3. In the pop-up Shutdown window, you can select the Shutdown Mode as needed.
   To avoid charges during shutdown, select CVM No Charge When Shutdown and click OK.

GPU Instance
Creating and Configuring GPU Instance

Creating GPU Instances

Cloud GPU Service is a special instance of CVM. Its purchase and operation methods are the same as CVM. For detailed instructions, see Creating CVM.

> Note:
>
> Cloud GPU Service can run properly only after the corresponding GPU driver is available. You can install the corresponding driver in the following ways:
>
> If you select Public Image, after the GPU instance is successfully created, you can refer to Installing the NVIDIA Tesla Driver to manually install the corresponding driver.

Windows Cloud GPU Service

The steps for creating and configuring the Windows Cloud GPU Service instance are the same as those for the Windows CVM instance. For details, see Quickly Configuring the Windows CVM.

Linux Cloud GPU Service

The steps for creating and configuring the Linux Cloud GPU Service instance are the same as those for the Linux CVM instance. For details, see Quickly Configuring the Linux CVM.

Logging In to the GPU Instances

After you purchase and launch a GPU instance, you can connect to and log in to it. The login method varies depending on your local operating system, GPU instance operating system, and whether the instance can be accessed via the Internet.

Prerequisites

To log in to a GPU instance using a password, you must have an admin account ID and password.
To log in to a GPU instance using a key, you must create and download a private key.

Log-in Guide

For Linux-based GPU instances, see Logging In to Linux Instances.
For Windows-based GPU instances, see Logging In to Windows Instances.

Restarting Instances

Restarting an instance is a common approach for troubleshooting the Cloud GPU Service. Restarting a GPU instance is equivalent to restarting the operating system of a local PC.

Overview

Restart preparation: The instance cannot provide service during restart. Make sure the Cloud GPU Service has suspended service requests before you restart it.
Restart operation mode: It is recommended to use the restart operation below to restart the instance instead of running the restart command in the instance (such as the restart command in Windows and the Reboot command in Linux).
Restart time: Generally speaking, the restart operation only takes a few minutes.
Instance physical characteristics: Restarting an instance does not change the instance's physical characteristics. The instance's public network IP, private network IP, and any stored data do not change.
Billing related: Restarting an instance does not start a new instance billing period.

Restarting an Instance via the Console

Log in to the CVM Console.

- Restart one instance: Select the instance you want to restart and click the Restart button at the top of the list. Alternatively, click More > CVM Status > Restart in the right-side action column.
- Restart multiple instances: Select all instances that need to be restarted, and click Restart button at the top of the list. to restart instance in batch. Instances that cannot be restarted will display the reason.

Restarting Instances via API

Refer to API Documentation > RebootInstances API.

GPU Instance Type

Standard GAA1

StandardGAA1 is not only suitable for GPU general computing scenarios such as deep learning, but also for graphics and image processing (3D rendering, video encoding, and decoding) scenarios.
Applicable Cases
High cost-effectiveness, suitable for the following scenarios:

- Reasoning scenarios and small-scale training scenarios for deep learning. For example:
  - AI reasoning for large-scale deployment
  - Small-scale training for deep learning
- Graphics and image processing scenario. For example:
  - Graphics and image processing
  - Video encoding and decoding
  - Graphic databases

    Hardware Specifications
- CPU: 2.45GHz AMD EPYCTM Milan processor
- GPU: NVIDIA® A10(62.5 TFLOPS single-precision floating-point calculation, 250 INT8 TOPS, 500 INT4 TOPS).
- Storage: You can select Cloud Block Storage Type. If you need to scale out, you can create a new elastic cloud storage and mount it.

  GAA1 instance provides the following configurations:

Model	GPU (NVIDIA A10)	GPU Memory (GDDR6)	vCPU	Memory Optimized (DDR4)
GAA1.8 XLARGE56	1	1 x 24 GB	32 cores	56 GB
GAA1.16 XLARGE112	2	2 x 24 GB	64 cores	112 GB
GAA1.32 XLARGE224	4	4 x 24 GB	128 cores	224 GB

CVM Dedicated Host
Viewing CDH Instance Information

Viewing CDH Instance Information via the Console

1. Log in to the CVM console.
2. In the navigation tree on the left, click CDH.
3. Select the corresponding region at the top of the CDH interface, and you can view the information of the CDH you own in the current region, including the availability zone, model, total resources, remaining available resources, and expiration date.
4. Click the ID of a CDH to open its details page, where you can view detailed information about the CDH and instances on it.

Searching for CDH Instances

Currently, the console supports searching by the ID and name of the CVM Dedicated Host.

Searching for CDH instances via the Console

1. Log in to the CVM Dedicated Host console.
2. Select the corresponding region, enter the ID or name of the host in the search box in the upper right corner, and click to search.

Modifying CDH Instance Name

Modifying CDH Instance Name via the Console

1. Log in to the CDH console.
2. Select the corresponding region, select the CVM Dedicated Host whose name you want to modify, and click More > Rename at the top of the list.
3. In the pop-up Rename window, enter the new host name and click OK.

Assigning CVM Instances

Scenarios

You can create a CVM instance on the purchased CVM Dedicated Host through the console.

Prerequisites

To assign a CVM to a CDH instance, complete the following preparations as needed:

- To create a CVM instance with a Virtual Private Cloud (VPC) as the network type, you need to create a VPC in the target region and add a subnet in the target availability zone under the VPC.
- If you do not use the default security group automatically created by the system, you need to Create Security Group in the target region, and add security group rules that meet your business needs.
- When the Linux instance is created, you need to bind an SSH key pair. You need to Create SSH Key in the target project.
- When a CVM instances with a custom image is created, you need to create custom image or import image.

Must-Knows

The number of CVM that can be created on a CVM Dedicated Host depends on the remaining available CPU, memory, local disk resource size, and CVM specifications. For example, a completely idle HS20 (56 cores, 224 GB memory) can be assigned with seven 8-core 32 GB CVMs.

Operation Steps

Going to the CVM Assignment Page

1. Log in to the CDH console.
2. On the CVM Dedicated Host management page, select the corresponding region, check the CVM Dedicated Host, and click Assign CVM.

Selecting CPU and Memory Configurations for CVMs

1. On the Select Region and Model page, select the region and model.
   The main parameters are described as follows:

- CPU: Customize the CPU of the CVM based on the remaining resources of the selected host machine/host machine resource pool.
- Memory: Customize the memory configuration of the CVM based on the remaining resources of the selected host machine/host machine resource pool.
  Note: The CVM resource configuration you specify will affect the number of CVMs created.

2. Click Next: Select Image.

Selecting Image

1. On the Select Image page, select an image.
   The main parameters are described as follows:
   - Image provider: Based on different sources, Converge Cloud provides public images, custom images, and shared images. For more information about image types, see Image Type Introduction.
   - Operating system: Select an operating system according to actual needs.
   - System version: Select a system version according to actual needs.
2. Click Next: Select Storage and Network.

Selecting Storage and Network

1. On the Select Storage and Network page, select the system disk and data disk, and set the network information.
   The main parameters are described as follows:
   - System disk: It is required. The default capacity is 50 GB, which is used to install the operating system. You can select the cloud storage type and capacity used for the system disk. Different regions will affect the types of cloud storage that can be selected.
   - Data disk: It is optional. You can choose to add a data disk after the instance is created; you can add a data disk when purchasing and select the cloud storage type and capacity of the data disk; you can also create an empty data disk or use a data disk snapshot to create a data disk. The CVM supports the following storage types: local hard disk/local SSD hard disk, Cloud Block Storage, high-efficiency Cloud Block Storage, and SSD Cloud Block Storage. For more information about Cloud Block Storage, see Cloud Block Storage Classification.
   - VPC: You should select a VPC and a subnet. If no VPC or subnet has been created in advance, you can select the default VPC and subnet.
   - Public network IP: The CVM network on the CVM Dedicated Host only supports traffic-based billing. If you need to allocate a public IP address to the CVM, select Purchase Now. The IP address allocated in this way cannot be directly unbound from the instance, but the public IP address can be converted to an Elastic IP and then unbound.
   - Public network bandwidth: Configure based on actual needs.
   - Number of servers: Configure based on actual needs.
2. Click Next: Set Information.

Setting Information

1. On the Set Information page, set the project, host name, log-in method, and security group.
   The main parameters are described as follows:
   - Host Name:
     - Select Name after Creation, and after the Cloud Virtual Machine is created, it is named Unnamed. This name is only displayed in the console and is not the hostname of the Cloud Virtual Machine.
     - Select Name Now and enter a semantic name within 60 characters.
   - Login Method:
     - If a Linux Cloud Virtual Machine is selected for the image, you can log in via Set Password, Immediately Associate Key, or Automatically Generate Password.
     - If a Windows Cloud Virtual Machine is selected for the image, you can log in via Set Password or Automatically Generate Password.
   - Security Group:
     - If you have not created a security group yourself, select Create Security Group.
     - If you already have a security group, select Existing Security Group. You can also preview the security group rules. For details about security group rules, see Security Group Overview.
   - Security Reinforcement: Anti-DDoS, WAF, and cloud mirror host protection are enabled free of charge. For more information, see Cloud Workload Protection Product Introduction.
   - Cloud Monitor: Cloud service monitoring is enabled free of charge by default. Install components to obtain host monitoring metrics and display them in the form of monitoring icons. It also supports customizing alarm thresholds. For details, see Cloud Monitor Product Overview.
2. Click Buy Now to complete the creation.

> Note:
> After the Cloud Virtual Machine is created, you will receive an intra-site message containing information such as the instance name, public IP address, private IP address, log-in name, and initial log-in password (if you choose to automatically generate a password). You can use the information to log in to and manage the instance.

Logging in to Sub-Machine

The log-in operation of the dedicated sub-machine is the same as that of a common CVM. For detailed operation guide, see the following sections.

Logging In to Windows Instances

For details, see Logging In to Windows Instances.

Logging In to Linux Instances

For details, see Logging In to Linux Instances.

Image
Creating Custom Image

Overview

When you create an image, you can choose to launch an instance based on a public image and connect the image to your instance to deploy the software environment yourself. When the instance is running normally, you can create a new custom image based on it according to your actual needs. After you create a new custom image, you can use the image to launch more new instances with the same custom items as the original instance.

> Note:
> - When you create a custom image, the system will create a related snapshot by default. Before deleting this snapshot, you need to delete the associated image first.
> - When you create custom images for other instances, shut down the instance first to ensure that the image is completely consistent with the current instance deployment environment.

Notes

- Each region currently supports 50 custom images.
- The following directories/files will be cleared:
  /var/log/
  /root/.bash_history, /home/ubuntu/.bash_history (Ubuntu system)
- When you create a custom image for a Linux instance, make sure that /etc/fstab does not contain data disk configuration. Otherwise, the instance created using the image will not be able to start normally. If the Linux instance for which you created the custom image has a data disk mounted, you need to comment or delete the configuration related to the self-configured data disk in /etc/fstab.
- The creation process will take ten minutes or longer. The specific time depends on the data size of the instance. Make relevant preparations in advance to avoid affecting your business.

Operation Steps

Creating from Instance using Console

1. Log in to the CVM console.

2. In the instance management page, select the instance for which you need to create an image, and choose More > CVM Status > Shut Down.
3. After the instance is shut down, in the row of that instance, click More > Create Image
4. In the pop-up Create Custom Image window, enter Image Name and Image Description, and click OK to create the image.
5. After the image is created, click Image in the left sidebar to enter the Image Management page.
6. In the image list, select the image you created and click Create CVM to purchase a server with the same image as before.

Copying an Image

Overview

Conventional Thinking

The image replication feature helps users deploy the same CVM instance across regions quickly. You can copy a custom image to another region, and use the created copy to create a CVM instance in the new region.

Instruction

- The copied image must be a custom image. You need to create a custom image first. For details, see Creating Custom Image.
- The waiting time for copying the image is 10 to 30 minutes.
- Cross-region replication of full-instance images is currently not supported.

Methods

By Console

1. Log in to the CVM console.
2. In the left sidebar, click Images to enter the image management page.
3. Select the region where the original image you want to copy resides, and click the Custom Image tab.
4. Find the instance whose image needs to be copied, click More > Cross-Region replication.
5. In the pop-up window, select the regions where the image will be copied to and click OK.
   After the copying is completed, the image list in the destination regions will display images with the same name and different IDs.
6. Switch to the target region for replication. In the image list under the region, select the successfully replicated image and click Create CVM to create the same CVM instance.

Sharing Custom Images

Overview

Shared image is a custom image that you have created to share with other users. Users can easily obtain shared images and get the necessary components from other users, and add their custom content.

> Note:
> The cloud platform cannot guarantee the integrity or security of images shared by other users. It is recommended that users only use shared images from reliable sources.

Notes

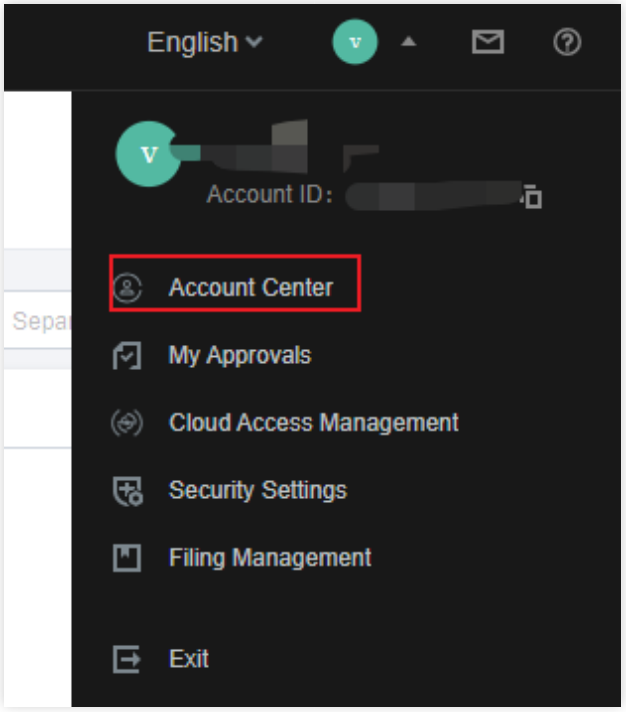
- Each image can be shared with up to 50 users.
- The name and description of a shared image cannot be changed and it can only be used to create the Cloud Virtual Machine instance.
- Images shared with other users do not occupy their own image quota.
- Images shared with other users can be deleted, but all sharing of the image must be canceled first. For details on unshare operation, see Unshare Custom Image. The obtained shared image cannot be deleted.
- Images can be shared to accounts in the same region. If you need to share to different regions, you need to copy the image to different regions before sharing.
- The obtained shared image cannot be shared with other users.

Directions

Obtain Account ID

The shared image is identified by the unique ID of the peer account. You can notify the user to obtain it in the following ways:

1. Log in to the CVM Console.
2. Click Account Name in the upper-right corner and select Account Center.
3. On the Account Information management page, check and record the account ID.



4. Inform the other party to send the obtained account ID to you.

Share via the Console

1. Log in to the CVM Console.
2. In the left sidebar, click Image.
3. Select the Custom Image tab. In the custom image list, select the custom image you want to share and click Share on the right.
4. In the pop-up Shared Image window, enter the other party's account ID and click Share.
5. Inform the other party to log in to the Cloud Virtual Machine console and select Image > Shared Image to view the shared image.
6. To share with multiple users, repeat the above steps.

Unsharing Custom Image

Overview

This document guides users to unshare custom images. Users can terminate the sharing status of the image shared with others at any time to decide not to share it with other users. This operation does not affect instances that other users have already created using this shared image, but other users will no longer be able to view this image or create more instances using this image.

Directions

Unsharing via the Console

1. Log in to the CVM Console.
2. In the left sidebar, click Image.
3. Select the Custom Image tab. In the custom image list, select the custom image you want to unshare and click More > Cancel Sharing.
4. In the new page, select the unique ID of the peer account that needs to be unshared and click Unshare.
5. In the pop-up dialog box, click Confirm to complete the image unsharing.

Unsharing via API

Users can use the ModifyImageSharePermission API to unshare an image. For details, see API Interface documentation > Modify Image Sharing Information.

Deleting Custom Image

Overview

This document guides you to delete custom images.

Notes

Before deleting, note the following:

- After you delete custom images, you cannot create instances using this image. However, this does not affect instances that have already been started.
- A shared image cannot be deleted. You must first unshare all images before deleting them. To unshare images, see Unshare Custom Image.
- Only custom images can be deleted. Public images and shared images cannot be deleted actively, and obtained images cannot be deleted either.

Directions

Delete via the Console

1. Log in to the CVM Console.
2. In the left sidebar, click Image and select the Custom Image tab to enter the custom image management page.
3. Select the operation method for deleting a custom image based on actual needs.
    - Delete a single image: Find the custom image you want to delete in the list and click More > Delete.
    - Delete multiple images: Select all custom images to be deleted in the list and click Delete at the top.
4. In the pop-up dialog Box, click OK.
   If deletion cannot be complete, the reason will be prompted.

Delete via API

Users can use the DeleteImages API to share images. For details, see API Interface Documentation > Delete Image.

Importing Image Overview

In addition to using the Create Custom Image feature, Converge Cloud also supports to import. You can import image files of local server system disk or other platform into the custom image of Cloud Virtual Machine (CVM). After you import, you can use the imported image to create the Cloud Virtual Machine or reinstall the system on an existing Cloud Virtual Machine.

Import Preparation

You need to prepare an image file that meets the import restrictions in advance.

- Image limits of Linux system type:

Image Attribute	Condition
OS	- Images based on CentOS, Ubuntu, and Debian distributions. - Supports 32-bit and 64-bit
Image Format	- Support RAW, VHD, QCOW2, VMDK image formats - Use qemu-img info imageName | grep 'file format' to view image format.
Image Size	Use qemu-img info imageName | grep 'disk size' to check the actual size of the image. Use qemu-img info imageName | grep 'virtual size' to view image vsize. Note: When importing an image, the size is based on the image information after conversion to QCOW2 format.
Network	- By default, eth0 network API is provided for the instance. - IPv6 is not supported yet. - Users can query the network configuration of an instance through the metadata service within the instance. For details, see Instance Metadata.
Drive	- The image must be installed with the Virtio driver of the virtualization platform KVM. For details, see Import Image on Linux to Check Virtio Driver. - It is recommended to install cloudinit in the image. For details, see Import Image on Linux to Install Cloudinit. - If the image cannot be installed with cloudinit due to other reasons, use Forced Import Image to self-configure instance.
Kernel Limits	The image should preferably be a native kernel. Modification may cause the Cloud Virtual Machine to fail to import.

- Image limits of Windows system type:

Image Attribute	Condition
OS	- Windows Server 2008 related versions, Windows Server 2012 related versions, and Windows Server 2016 related versions. - Supports 32-bit and 64-bit
Image Format	- Support RAW, VHD, QCOW2, VMDK image formats - Use qemu-img info imageName | grep 'file format' to view image format.
File System Type	- Only NTFS file systems that use MBR partitions are supported - GPT partitions are not supported. - Logical Volume Management (LVM) is not supported.
Image Size	Use qemu-img info imageName | grep 'disk size' to check the actual size of the image. Use qemu-img info imageName | grep 'virtual size' to view image vsize. Note: When importing an image, the size is based on the image information after conversion to qcow2 format.
Network	By default, this version provides a local connection network API for the instance. IPv6 is not supported by this version. Users can query the network configuration of an instance through the metadata service within the instance. For details, see Instance Metadata.
Drive	The image must be installed with the Virtio driver of the virtualization platform KVM. The Virtio driver is not installed by default in Windows. You can install the Windows Virtio driver and then export the local image.
Others	The imported Windows system images do not provide Windows Activation service.

Import Steps

1. Log in to the CVM Console.
2. Click Image in the left sidebar.
3. Select Custom Image and click Import Image.
4. According to the requirements of the operation interface, activate COS first, then create a bucket, upload the image file to the bucket. On the image file details page, directly click the temporary link and copy the temporary link to obtain the image file URL.
5. Check Preparations completed. Then click Next: Import Image.
6. Enter the form according to the actual situation and click Start Importing.
   Ensure that the Cloud Object Storage file URL you enter is correct. Whether the import is successful or failed, you will be notified via message center.

Import Failed

After the image import operation is performed on the console, the task may fail due to some reasons. If the task fails, you can troubleshoot based on the following information.

Notes

Before troubleshooting the cause of the failure according to this document, make sure that you have subscribed to product and service related notifications in the Message Subscription column of the Message Center Management page to ensure that you can receive message center, short message service, and emails containing the cause of the failure.

> Note:
> If you do not subscribe to product and service related information in the message center, you will not be able to receive message center notifications about the success/failure of the import.

Troubleshooting Cause of Failure

For detailed error prompts and error descriptions, see the error code.

InvalidUrl: The Cloud Object Storage Link is Invalid

The InvalidUrl error is reported, error prompts: An incorrect Cloud Object Storage link was entered on the image import page. Possible reasons are as follows:

- The image link entered is not an Cloud Object Storage service.
- The access permission to the Cloud Object Storage file is private read, but the signature has expired. > Note:
  The Cloud Object Storage file link with a signature can be accessed only once.
- A Cloud Object Storage link in another region was entered. > Note:
  Import image service accesses the Cloud Object Storage server in the local region through the private network.
- The user's image file has been deleted.
  If you receive an error reporting that the Cloud Object Storage link is invalid, you can troubleshoot the problem based on the reasons listed above.

InvalidFormatSize: The format or Size does not Meet the Requirements

The InvalidFormatSize error is reported, error prompts: The format or size of the pre-imported image does

not meet the limits of the import image feature. The limits are as follows:

- Import image supports 4 image file formats: qcow2 , vhd , vmdk , and raw .
- The size of the system disk of the import image must not exceed 500 GB.
  After an error reporting that the format or size does not meet the requirements is received:
- Based on the image format conversion content of Linux Image Creation, you can convert the image file to a suitable file format, condense the image content to meet the size limit, and then re-import the image.
- You can also use Offline Instance Migration to migrate example. This feature supports migration of image files with a maximum size of 500 GB.

VirtioNotInstall: Virtio Driver is not Installed

The VirtioNotInstall error is reported, error prompts: The Virtio driver is not installed on the pre-imported image. Converge Cloud uses KVM virtualization technology, which requires the virtio driver to be installed in the image that the user imports. The Virtio driver has been installed on most Linux operating systems except a few user-customized Linux operating systems. For Windows operating system, you need to manually install the Virtio driver:

- For Linux image import, see the document Check Virtio Driver in Linux System.
- For Windows image import, see the document Windows Image Creation to install the Virtio driver.

CloudInitNotInstalled: The Cloud-init Program is not Installed

The CloudInitNotInstalled error is reported, error prompts: The cloud-init driver is not installed on the pre-imported image. Converge Cloud uses the open source program cloud-init to initialize the sub-machine. Therefore, if the cloud-init program is not installed, the user's sub-machine initialization will fail.

- For Linux image import, see the document Install cloud-init on Linux System.
- For Windows image import, see the document Installing cloudbase-init on Windows Operating System.
- After cloud-init/cloudbase-init is installed, replace the configuration file according to the documentation so that the sub-machine can pull data from the correct data source when it starts.

PartitionNotPresent: Partition Information is Lost

The PartitionNotPresent error is reported, error prompts: The imported image is incomplete. Check whether the boot partition is included when making the image.

RootPartitionNotFound: The Root Partition is Lost

The RootPartitionNotFound error is reported, error prompts: The imported image is not detected to contain a root partition. Check the image file. The reasons that have occurred are as follows for reference:

- The installation package file is uploaded.

- The data disk image is uploaded.
- The boot partition image is uploaded.
- The wrong file is uploaded.

InternalError: Unknown Error

The InternalError error is reported, error prompts: The import image service does not include the error cause. Contact customer service to handle this problem, and the technician will solve the problem as soon as possible.

Error Code

Error Code	Error Cause	Suggested Handling Method
InvalidUrl	COS link is invalid.	Check if the COS link is the same as the import image link.
InvalidFormatSize	The format or size does not meet the requirements.	The image must meet the requirements of Image Format and Image Size in the import preparation.
VirtioNotInstall	Virtio driver is not installed.	The virtio driver needs to be installed for images. For details, see Driver section in the import preparation.
PartitionNotPresent	Partition information is not found.	The image is damaged, which may be caused by the wrong image creation method.
CloudInitNotInstalled	cloud-init is not installed.	The cloud-init needs to be installed for Linux images. For details, see Driver section in the import preparation.
RootPartitionNotFound	Root partition is not detected.	The image is damaged, which may be caused by the wrong image creation method.
InternalError	Other Errors	Contact customer service to handle the problem.

Forced Import Image

Overview

When the user's Linux image cannot install cloudinit for some reason, you can use the Forced Import Image feature to import the image. If the user uses the forced import image for import, Converge Cloud will not be able to initialize the configuration of the user's CVM. You need to set a script to configure the CVM according to the configuration file provided by Converge Cloud. This document guides users on how to configure the CVM under the premise of forced import image.

Limitation Factor

- The image still needs to meet the imported image limits in Import Image for Linux images (except cloudinit).
- The system partition where the image is imported is not full.
- The imported image must not have vulnerabilities that can be exploited remotely.
- It is recommended that users change the password immediately after the instance is created successfully by forced import image.

Directions

The forced import image does not use cloudinit and therefore cannot be automatically configured. Converge Cloud provides a cdrom device containing configuration information for users to configure themselves. Users need to mount cdrom and read mount_point/qcloud_action/os.conf information to configure. If the user needs to use other configuration data or UserData, they can directly read the files under mount_point/ .

os.conf Configuration File Content

The basic contents of os.conf are 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 in the above information are for reference only, and the parameter values are only examples.

The meaning of each parameter in os.conf is as follows:

Parameter Name	Parameter Meaning
hostname	Host name
password	Encrypted password
eth0_ip_addr	LAN IP of the eth0 network interface
eth0_mac_addr	MAC address of the eth0 network interface
eth0_netmask	Subnet mask of the eth0 network interface
eth0_gateway	Gateway of the eth0 network interface
dns_nameserver	DNS resolution server

Configure Script Resolution

Notes

- The script is automatically executed at boot. Implement this requirement according to the type of operating system.
- The script must mount `/dev/cdrom` , and read `os_action/os.conf` file under the mount point to obtain configuration information.
- The password placed in the cdrom by Converge Cloud is an encrypted password. Users can use `chpasswd -e` to set it.
  The encrypted password may contain special characters. It is recommended to put it in a file first and then use `chpasswd -e < passwd_file` to set it.
- When recreating an image using an instance created by forced import image, you need to ensure that the script is still executed to ensure that the instance is correctly configured. You can also install

cloudinit in this instance.

Example

Converge Cloud provides a sample script based on CentOS. Users can create configuration scripts for their own images based on the sample script. During the creation process, note the following points:

- This script needs to be correctly placed in the system before importing the image.
- This script is not suitable for all operating systems. Users need to modify it according to their own operating system to meet the semantics.

1. Create os_config script according to the following script example.
   Users can modify os_config script according to actual conditions.

```
#!/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 os_config script in /etc/init.d/ directory and execute the following command.

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

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

```
chkconfig --list
```

Note: Users need to ensure that the script is executed correctly. If the instance cannot be connected through SSH or the network connection is unavailable after the image is imported, connect to the instance through the console and run the script again to troubleshoot. If the problem still cannot be solved, contact customer service.

Checking Virtio Driver in Linux System

Scenarios

To run on the cloud platform normally, a Cloud Virtual Machine (CVM) should have a kernel supporting virtio drivers (including the block device driver virtio_blk and the NIC driver virtio_net). To prevent a created CVM instance from failing to start normally after importing a custom image, you need to check whether it is required to check and fix the support for virtio drivers in the source server before importing the image. This document uses the CentOS operating system as an example to describe how to check and fix the support for virtio drivers in an image before you import the image.

Operation Steps

Step 1: Check Whether the Kernel Supports Virtio Driver

Execute the following command to check whether the current kernel supports the Virtio driver.

```
grep -i virtio /boot/config-$(uname -r)
```

The result resembles the following is returned:

```
[root@VM_0_120_centos ~]# grep -i virtio /boot/config-$(uname -r)
CONFIG_VIRTIO_VSOCKETS=m
CONFIG_VIRTIO_VSOCKETS_COMMON=m
CONFIG_VIRTIO_BLK=m
CONFIG_SCSI_VIRTIO=m
CONFIG_VIRTIO_NET=m
CONFIG_VIRTIO_CONSOLE=m
CONFIG_HW_RANDOM_VIRTIO=m
CONFIG_DRM_VIRTIO_GPU=m
CONFIG_VIRTIO=m
# Virtio drivers
CONFIG_VIRTIO_PCI=m
CONFIG_VIRTIO_PCI_LEGACY=y
CONFIG_VIRTIO_BALLOON=m
CONFIG_VIRTIO_INPUT=m
# CONFIG_VIRTIO_MMIO is not set
```

- If the values of the CONFIG_VIRTIO_BLK parameter and the CONFIG_VIRTIO_NET parameter are m in the returned result, execute Step 2.
- If the values of the CONFIG_VIRTIO_BLK parameter and the CONFIG_VIRTIO_NET parameter are y in the returned result, it means that the operating system contains the virtio drivers. You can directly import the custom image to the cloud platform. For detailed operations, see Overview of Importing an Image.
- If there is no information about the CONFIG_VIRTIO_BLK parameter and the CONFIG_VIRTIO_NET parameter in the returned result, it means that the operating system does not support importing images to

the cloud platform. Please download and compile the kernel.

Step 2: Check Whether the Temporary File System Contains the Virtio Driver

If the value of the parameters is m in the execution result of Step 1, you need to further check and confirm whether the temporary file system initramfs or initrd contains the virtio drivers. Execute the corresponding command according to the operating system:
CentOS Stream operating system:

```
lsinitrd /boot/initramfs-$(uname -r).img | grep virtio
```

CentOS 6/CentOS 7/CentOS 8/RedHat 6/RedHat 7 operating systems:

```
lsinitrd /boot/initramfs-$(uname -r).img | grep virtio
```

RedHat 5/CentOS 5 operating systems:

```
mkdir -p /tmp/initrd && cd /tmp/initrdzcat /boot/initrd-$(uname -r).img | cpio -idmvfind . -name "virtio*"
```

Debian/Ubuntu operating systems:

```
lsinitramfs /boot/initrd.img-$(uname -r) | grep virtio
```

OpenSUSE Leap operating system:

```
lsinitrd /boot/initrd-$(uname -r) | grep virtio
```

The result resembles the following is returned:

```
[root@VM_0_120_centos ~]# lsinitrd /boot/initramfs-$(uname -r).img | grep virtio
-rw-r--r--   1 root     root         7744 Apr 21  2018 usr/lib/modules/3.10.0-862.el7.x86_64/kernel/drivers/block/virtio_blk.ko.xz
-rw-r--r--   1 root     root        12944 Apr 21  2018 usr/lib/modules/3.10.0-862.el7.x86_64/kernel/drivers/char/virtio_console.ko.xz
-rw-r--r--   1 root     root        14296 Apr 21  2018 usr/lib/modules/3.10.0-862.el7.x86_64/kernel/drivers/net/virtio_net.ko.xz
-rw-r--r--   1 root     root         8176 Apr 21  2018 usr/lib/modules/3.10.0-862.el7.x86_64/kernel/drivers/scsi/virtio_scsi.ko.xz
drwxr-xr-x   2 root     root            0 Jan 21  2019 usr/lib/modules/3.10.0-862.el7.x86_64/kernel/drivers/virtio
-rw-r--r--   1 root     root         4556 Apr 21  2018 usr/lib/modules/3.10.0-862.el7.x86_64/kernel/drivers/virtio/virtio.ko.xz
-rw-r--r--   1 root     root         9664 Apr 21  2018 usr/lib/modules/3.10.0-862.el7.x86_64/kernel/drivers/virtio/virtio_pci.ko.xz
-rw-r--r--   1 root     root         8280 Apr 21  2018 usr/lib/modules/3.10.0-862.el7.x86_64/kernel/drivers/virtio/virtio_ring.ko.xz
```

It can be seen that initramfs already contains the virtio_blk driver, as well as virtio.ko, virtio_pci.ko, and virtio_ring.ko on which the driver depends. In this case, you can directly import the custom image to the cloud platform. For detailed operations, see Overview of Importing an Image. If initramfs or initrd does not contain the virtio drivers, execute Step 3.

Step 3: Reconfigure the Temporary File System

If the execution result of Step 2 shows that the temporary file system initramfs or initrd does not contain the virtio drivers, you need to reconfigure the temporary file system initramfs or initrd to ensure that it contains the virtio drivers. Please select the corresponding operation according to the operating system:
CentOS Stream operating system:

```
mkinitrd -f --allow-missing --with=virtio_blk --preload=virtio_blk --with=virtio_net --preload=virtio_net --wi
th=virtio_console --preload=virtio_console /boot/initramfs-$(uname -r).img $(uname -r)
```

CentOS 8/RedHat 8 operating system:

```
mkinitrd -f --allow-missing --with=virtio_blk --preload=virtio_blk --with=virtio_net --preload=virtio_net --wi
th=virtio_console --preload=virtio_console /boot/initramfs-$(uname -r).img $(uname -r)
```

CentOS 6/CentOS 7/RedHat 6/RedHat 7 operating systems:

```
mkinitrd -f --allow-missing --with=xen-blkfront --preload=xen-blkfront --with=virtio_blk --preload=virtio_bl
k --with=virtio_pci --preload=virtio_pci --with=virtio_console --preload=virtio_console /boot/initramfs-$(un
ame -r).img $(uname -r)
```

RedHat 5/CentOS 5 operating systems:

```
mkinitrd -f --allow-missing --with=xen-vbd  --preload=xen-vbd --with=xen-platform-pci --preload=xen-plat
form-pci --with=virtio_blk --preload=virtio_blk --with=virtio_pci --preload=virtio_pci --with=virtio_console
--preload=virtio_console /boot/initrd-$(uname -r).img $(uname -r)
```

Debian/Ubuntu operating systems:

```
echo -e 'xen-blkfront\nvirtio_blk\nvirtio_pci\nvirtio_console' >> /etc/initramfs-tools/modulesmkinitramfs -o
/boot/initrd.img-$(uname -r)
```

OpenSUSE Leap operating system:

```
mkinitrd -m "virtio_blk virtio_net"
```

Appendix

Downloading and Compiling the Kernel

Downloading the Kernel Installation Package

1. Execute the following command to install the components necessary for kernel compilation.

```
yum install -y ncurses-devel gcc make wget
```

2. Execute the following command to query the version of the kernel currently used by the system.

```
uname -r
```

A result similar to the following will be returned. The version of the kernel used by the current system is

2.6.32-642.6.2.el6.x86_64.

```
[root@VM_0_139_centos ~]# uname -r
2.6.32-642.6.2.el6.x86_64
```

3. Go to the Linux kernel download page and download the source code of the corresponding or closest kernel version. For example, for the kernel version 2.6.32-642.6.2.el6.x86_64, download the installation package linux-2.6.32.tar.gz. Its download path is https://mirrors.edge.kernel.org/pub/linux/kernel/v2.6/linux-2.6.32.tar.gz.
4. Execute the following command to switch the directory.

```
cd /usr/src/
```

5. Execute the following command to download the installation package.

```
wget https://mirrors.edge.kernel.org/pub/linux/kernel/v2.6/linux-2.6.32.tar.gz
```

6. Execute the following command to decompress the installation package.

```
tar -xzf linux-2.6.32.tar.gz
```

7. Execute the following command to establish a connection.

```
ln -s linux-2.6.32 linux
```

8. Execute the following command to switch the directory.

```
cd /usr/src/linux
```

Compile the kernel.

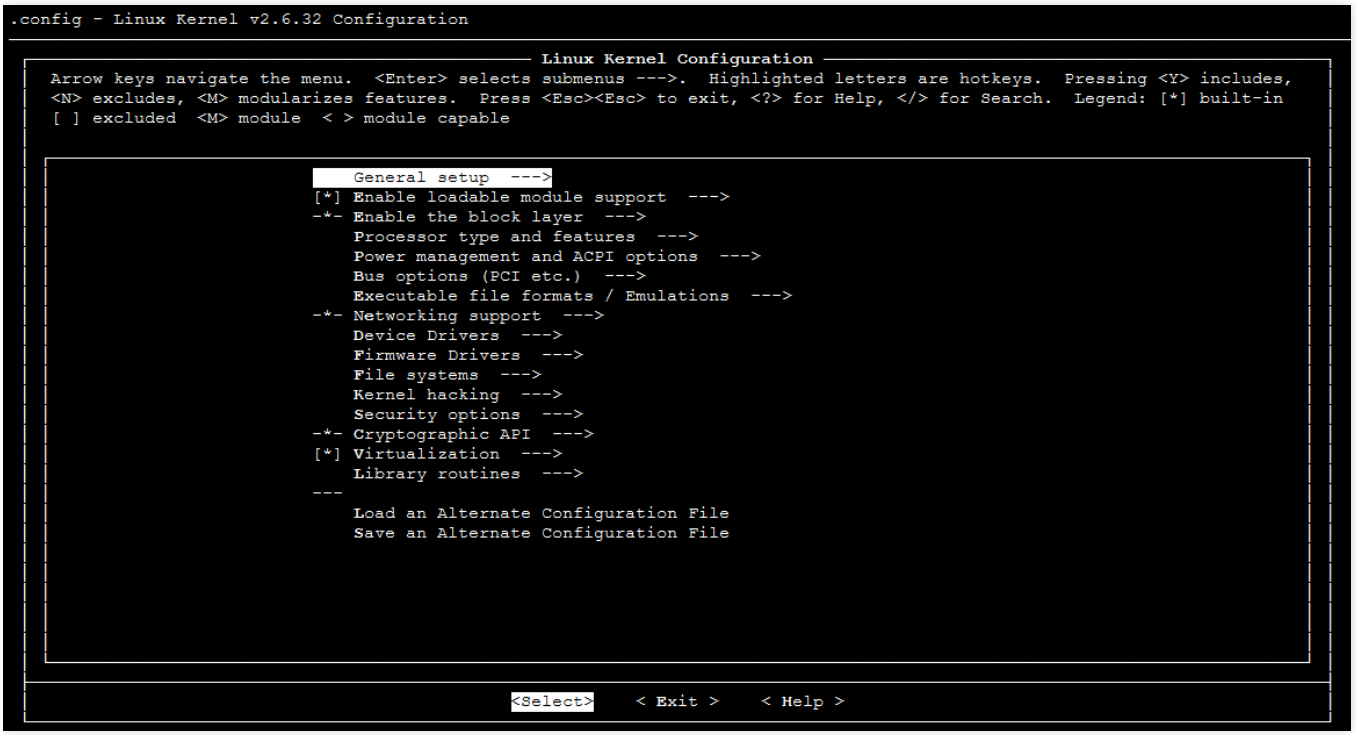
1. Execute the following commands in sequence to compile the kernel.

```
make mrproper
```

```
cp /boot/config-$(uname -r) ./.config
```

```
make menuconfig
```

Go to the Linux Kernel vX.X.XX Configuration interface.

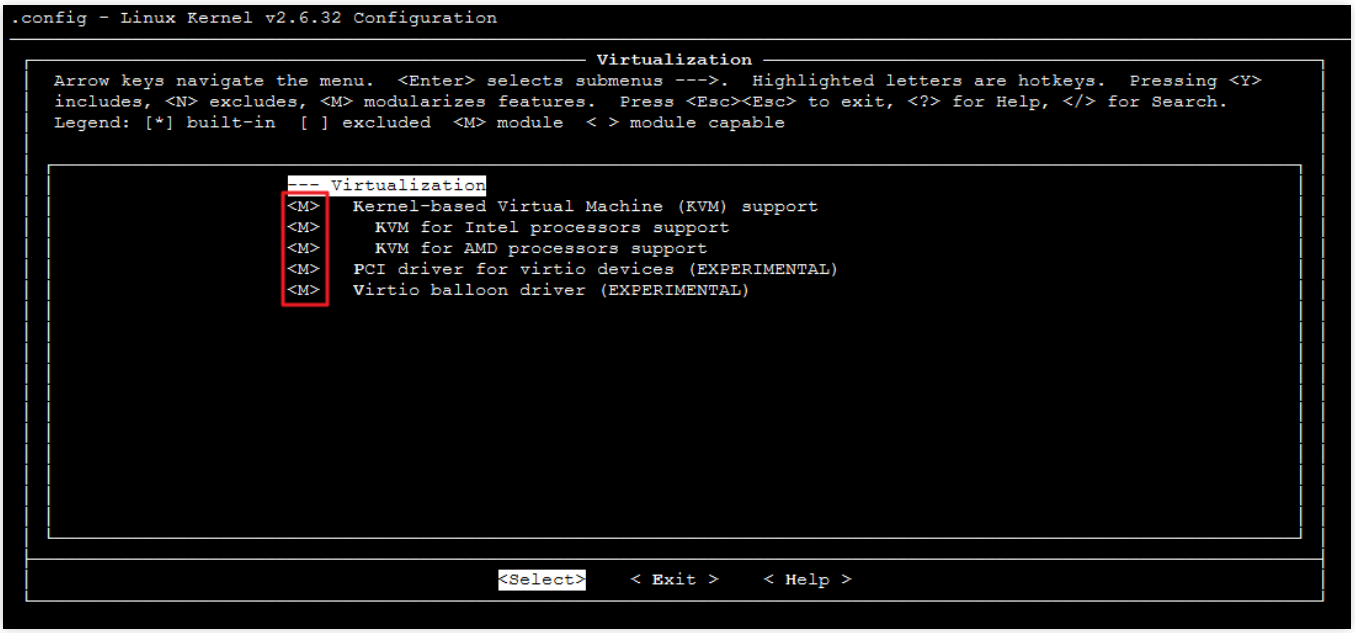


Note:

If you cannot go to the Linux Kernel vX.X.XX Configuration interface, please execute Step 18. On the Linux Kernel vX.X.XX Configuration interface:

- Press Tab or the ↑/↓ key to move the cursor.
- Press Enter to select or execute the item selected by the cursor.
- Press the space bar to select the item selected by the cursor. "*" means compiling to the kernel, and "M" means compiling to a module.

2. Press the ↓ key to move the cursor to Virtualization and press the space bar to select Virtualization.
3. Press Enter at Virtualization to go to the Virtualization details interface.
4. On the Virtualization details interface, confirm whether the Kernel-based Virtual Machine (KVM) support option is selected, as shown in the figure below:



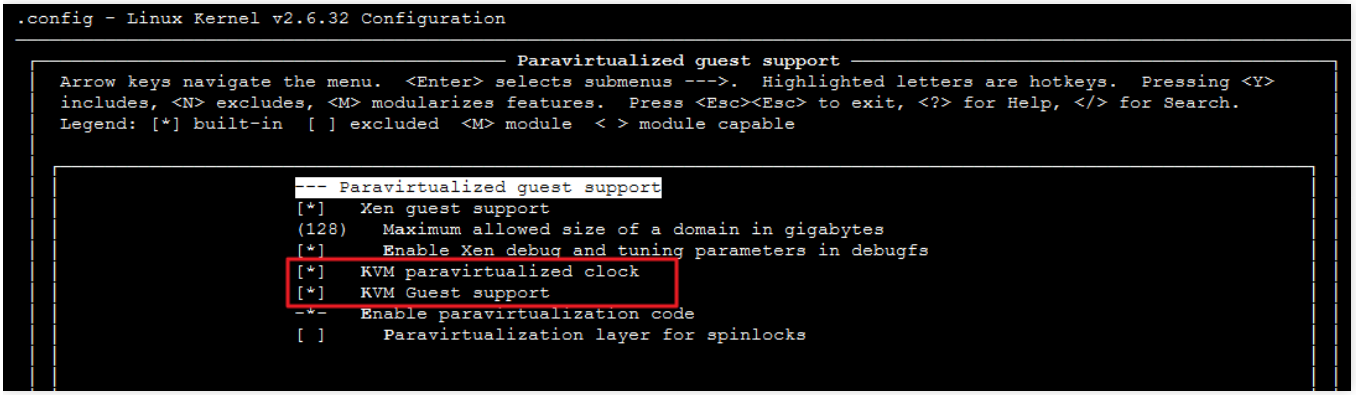
If it is not selected, press the space bar to select the Kernel-based Virtual Machine (KVM) support option.

5. Press Esc to return to the Linux Kernel vX.X.XX Configuration main interface.

6. Press the ↓ key to move the cursor to Processor type and features, and press Enter to go to the Processor type and features details interface.

7. Press the ↓ key to move the cursor to Paravirtualized guest support and press Enter to go to the Paravirtualized guest support details interface.

8. On the Paravirtualized guest support details interface, confirm whether KVM paravirtualized clock and KVM Guest support are selected.



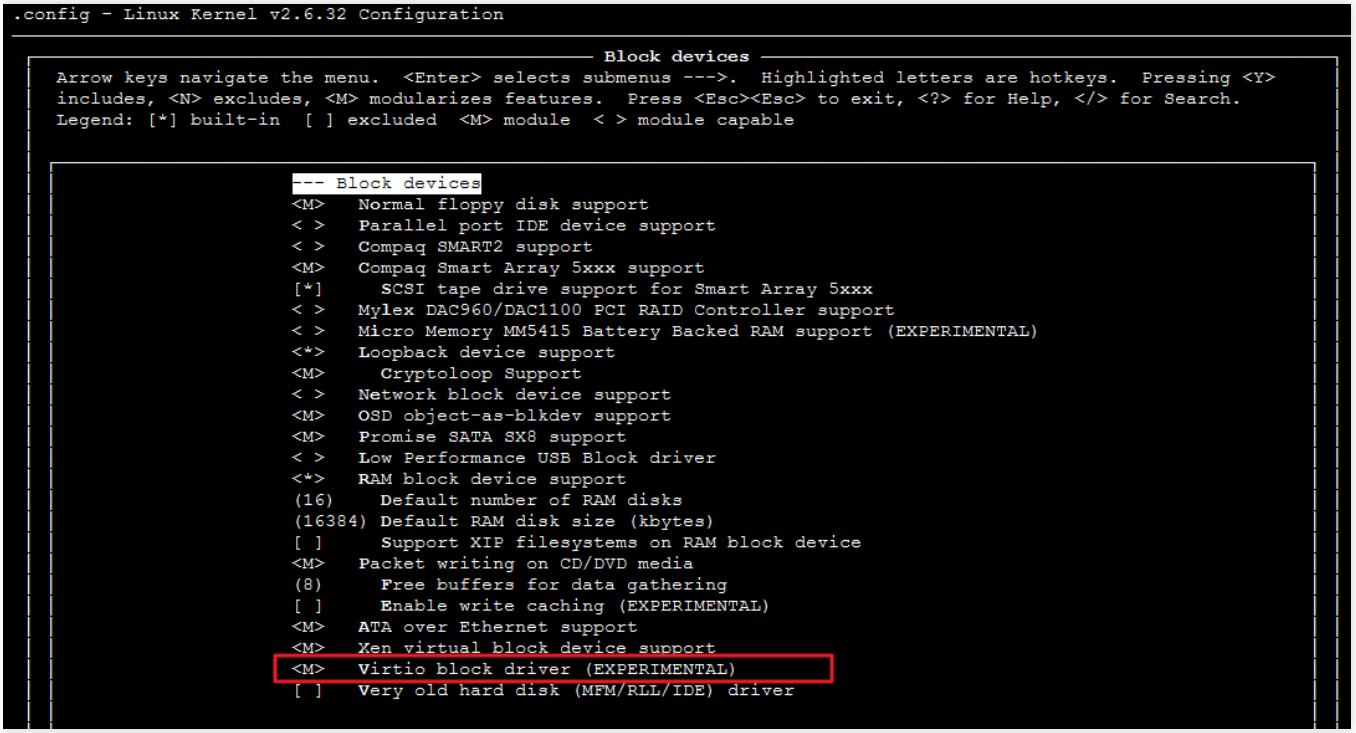
If they are not selected, press the space bar to select the KVM paravirtualized clock and KVM Guest support options.

9. Press Esc to return to the Linux Kernel vX.X.XX Configuration main interface.

10. Press the ↓ key to move the cursor to Device Drivers and press Enter to go to the Device Drivers details interface.

11. Press the ↓ key to move the cursor to Block devices and press Enter to go to the Block devices details interface.

12. On the Block devices details interface, confirm whether Virtio block driver (EXPERIMENTAL) is selected.

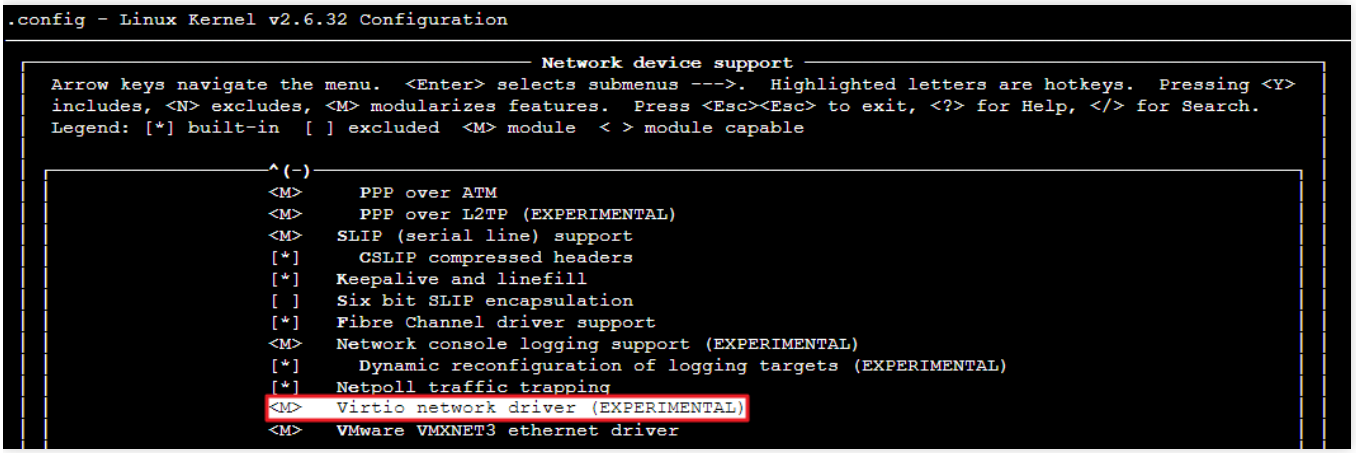


If it is not selected, press the space bar to select the Virtio block driver (EXPERIMENTAL) option.

13. Press Esc to return to the Device Drivers details interface.

14. Press the ↓ key to move the cursor to Network device support and press Enter to go to the Network device support details interface.

15. On the Network device support details interface, confirm whether Virtio network driver (EXPERIMENTAL) is selected.



If it is not selected, press the space bar to select the Virtio network driver (EXPERIMENTAL) option.

16. Press Esc to exit the kernel configuration interface, and select YES to save the .config file according to the pop-up prompt.

17. See Step 1: Check whether the kernel supports the virtio drivers, and verify whether the virtio drivers have been configured correctly.

18. (Optional) Execute the following command to manually edit the .config file.

> Note:
> It is recommended that you perform this operation if you meet either of the following conditions:
>
> - After checking, you find that there is still no related configuration information about the virtio drivers in the kernel.
> - When compiling the kernel, you cannot go to the kernel configuration interface or fail to save the .config file successfully.

```
make oldconfig

make prepare

make scripts

make

make install
```

19. Execute the following command in sequence to view the installation of the virtio drivers.

```
find /lib/modules/"$(uname -r)"/ -name "virtio.*" | grep -E "virtio.*"

grep -E "virtio.*" < /lib/modules/"$(uname -r)"/modules.builtin
```

If the returned result of any of the command outputs a list of files such as virtio_blk, virtio_pci, and virtio_console, it means that you have installed the virtio drivers correctly.

Installing Cloudbase-Init on Windows System

Scenarios

Cloudbase-Init is a tool installed on the Windows operating system that enables users to automatically configure and initialize Windows virtual machines (VMs) in the cloud environment. In the cloud environment, users need to quickly create and deploy VMs. In this case, Cloudbase-Init can help users automatically complete the initialization tasks when creating VMs, such as network configuration, software installation, and script execution. Taking the Windows Server 2022 64-bit operating system as an example, this document guides you to install Cloudbase-Init on the Windows operating system.

Preparing the Software

To install Cloudbase-Init, the following software is required:

Software	Access Path	Description
CloudbaseInitSetup_X_X_XX_xXX.msi	Download the corresponding Cloudbase-Init installation package according to the bits of the operating systems actually used: Stable version: It is recommended. Windows 64-bit operating system Windows 32-bit operating system Beta version For more details, see the official website of Cloudbase-Init.	Used to install Cloudbase-Init.
XXXCloudRun.ps1		Used to modify the Cloudbase-Init configuration file.
localscripts.py		Used to ensure that Cloudbase-Init can start normally.

Operation Steps

Prerequisites: Images must be created by administrators.
Installing Cloudbase-Init

1. Download CloudbaseInitSetup_X_X_XX_xXX.msi to your server. On the operating system interface, double-

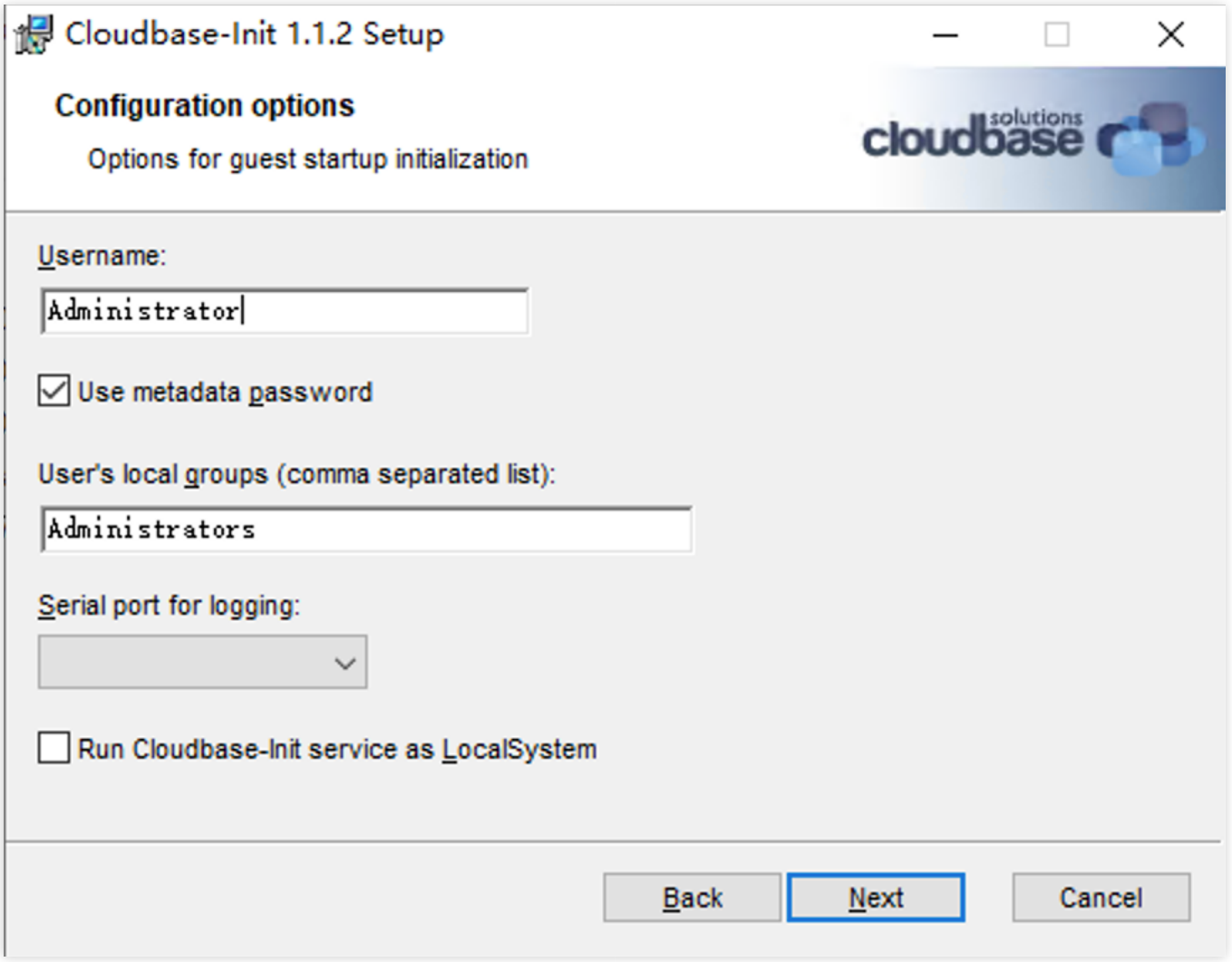
click it to open the Cloudbase-Init installation package.

2. In the pop-up security warning dialog box, click Run and enter the Cloudbase-Init installation interface.

3. Click Next.

4. Select the option I accept the terms in the License Agreement, and click Next twice.

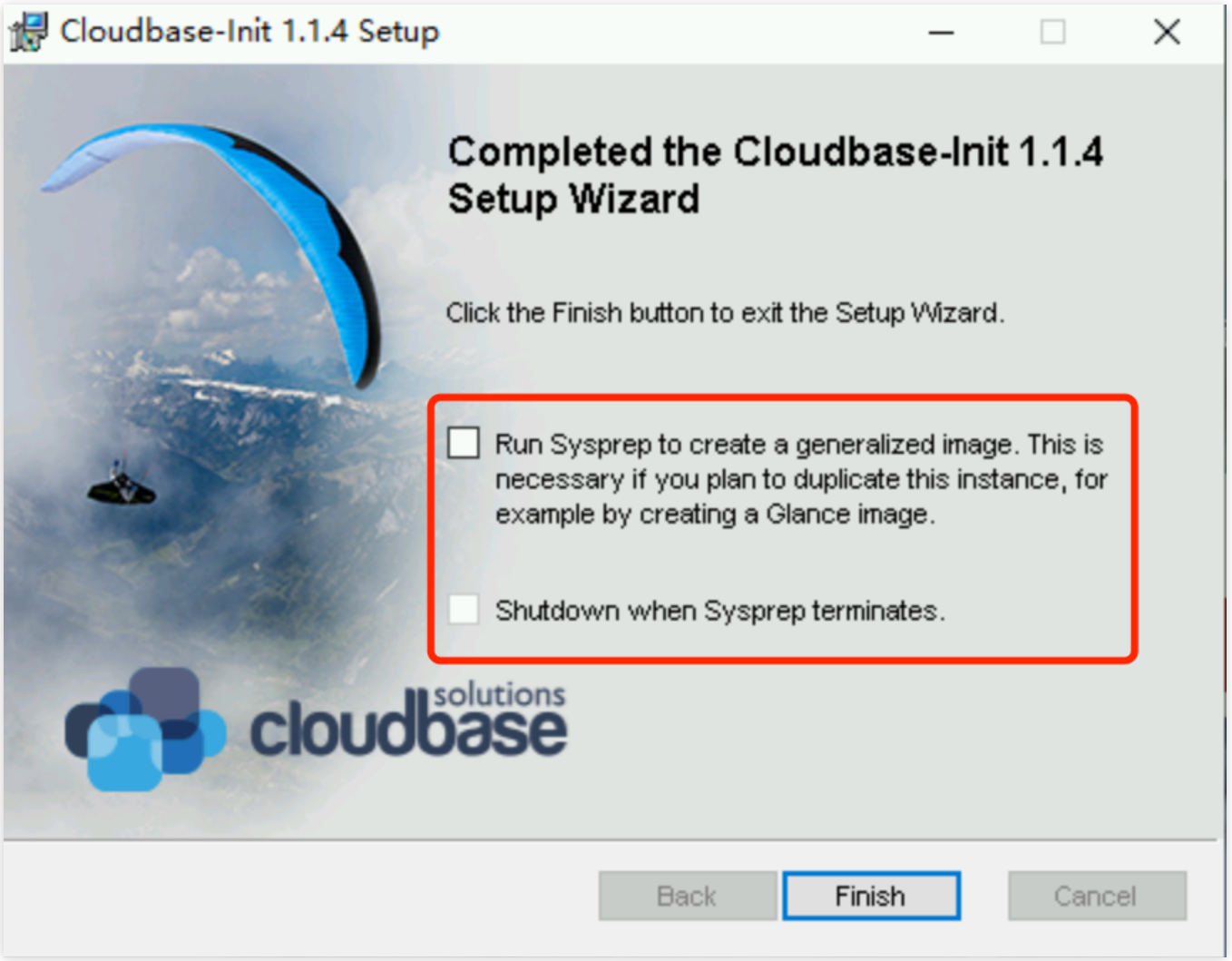
5. On the Configuration options interface, set Serial port for logging to COM1 (ignore this step if this option is not available). Select Run Cloudbase-Init service as LocalSystem, and click Next.



6. Click Install to install Cloudbase-Init.

7. After Cloudbase-Init is installed, click Finish to close the Cloudbase-Init installation interface.

> Note:
>
> When closing the Cloudbase-Init installation interface, do not select any checkbox and do not run Sysprep.



Modifying the Cloudbase-Init configuration file

1. Open the cloudbase-init.conf configuration file. The default path of cloudbase-init.conf configuration file is C:\Program Files\Cloudbase Solutions\Cloudbase-Init\conf.
2. Replace the cloudbase-init.conf configuration file with the following content:

```
[DEFAULT]
username=Administrator
groups=Administrators
inject_user_password=true
config_drive_raw_hhd=true
config_drive_cdrom=true
config_drive_vfat=true
bsdtar_path=C:\Program Files\Cloudbase Solutions\Cloudbase-Init\bin\bsdtar.exe
mtools_path=C:\Program Files\Cloudbase Solutions\Cloudbase-Init\bin\

san_policy=OnlineAll
```

metadata_services=cloudbaseinit.metadata.services.configdrive.ConfigDriveService,cloudbaseinit.metadata.services.ec2service.EC2Service
#,cloudbaseinit.metadata.services.httpservice.HttpService
#,cloudbaseinit.metadata.services.maasservice.MaaSHttpService

metadata_base_url=http://169.254.0.23/
ec2_metadata_base_url=http://169.254.0.23/

retry_count=2
retry_count_interval=5

plugins=cloudbaseinit.plugins.windows.extendvolumes.ExtendVolumesPlugin,cloudbaseinit.plugins.common.networkconfig.NetworkConfigPlugin,cloudbaseinit.plugins.common.sethostname.SetHostNamePlugin,cloudbaseinit.plugins.common.setuserpassword.SetUserPasswordPlugin,cloudbaseinit.plugins.common.localscripts.LocalScriptsPlugin,cloudbaseinit.plugins.common.userdata.UserDataPlugin
verbose=true
debug=true
logdir=C:\Program Files\Cloudbase Solutions\Cloudbase-Init\log\
logfile=cloudbase-init.log
default_log_levels=comtypes=INFO,suds=INFO,iso8601=WARN,requests=WARN
#logging_serial_port_settings=COM1,115200,N,8
mtu_use_dhcp_config=true
ntp_use_dhcp_config=true
first_logon_behaviour=no
netbios_host_name_compatibility=false
allow_reboot=true
activate_windows=true
kms_host="kms.convergecloud.com"
local_scripts_path=C:\Program Files\Cloudbase Solutions\Cloudbase-Init\LocalScripts\

C:\powershell
PS C:\Set-ExecutionPolicy Unrestricted

volumes_to_extend=1,2,3

Download the XXXCloudRun.ps1 script and copy it to the path C:\Program Files\Cloudbase Solutions\Cloudbase-Init\LocalScripts.

3. Right-click the XXXCloudRun.ps1 script, click Properties, and check in the pop-up window whether the script has executable permissions.

If there is an Unblock option, select it and click OK to exit.

If there is no Unblock option, skip this step.

4. Replace the localscripts.py file in the path C:\Program Files\Cloudbase Solutions\Cloudbase-Init\Python\Lib\site-packages\cloudbaseinit\plugins\common with the localscripts.py file mentioned in the section Preparing the Software.

Installing cloud-init on Linux System

Scenarios

Cloud-init primarily allows you to customize configurations during the first initialization of an instance. If an imported image is not installed with the cloud-init service, the instance that is enabled based on this image cannot be initialized normally, causing a failure in the normal import of this image. This document describes how to install the cloud-init service. The following three methods are recommended for installing cloud-init:
By downloading the cloud-init binary package.
By manually downloading the cloud-init source package.
By using the cloud-init package from the software source.

Related Operations

> Note:
> After the following operations are complete, do not restart the server. Otherwise, you will need to re-perform the following operations.

1. Execute the following command to check whether the cloud-init configuration is successful.

```
cloud-init init --local
```

If information similar to the following is returned, it means that cloud-init has been successfully configured.

```
Cloud-init v. 20.1.0011 running 'init-local' at Fri, 01 Apr 2022 01:26:11 +0000. Up 38.70 seconds.
```

2. Execute the following command to delete the cache records of cloud-init.

```
rm -rf /var/lib/cloud
```

3. For Ubuntu or Debian operating systems, execute the following command.

```
rm -rf /etc/network/interfaces.d/50-cloud-init.cfg
```

4. For the Ubuntu or Debian operating system, you need to modify /etc/network/interfaces to the following content:

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).
source /etc/network/interfaces.d/*
```

Export Image

Notes

- This option is not supported in batches.
- You can export only custom images, but not public images.
- Only images whose status is available can be exported.
- Cos must be enabled.
- The export time depends on the size of the image file and the busyness of the current export task queue.
- When the exported custom image contains a data disk snapshot, multiple files will appear in your OSS Bucket.

Directions

1. Log in to the CVM Console.
2. On the Image page, select the custom image you want to export and choose More > Export Image.
3. A dialog box pops up when exporting the image. The default content is: image name, image size, system platform, image location, the bucket address and Object prefix name of cos that you need to enter, and if cos is not enabled, you need to go to the cos page to enable cos and create a storage bucket.
4. Click OK to prompt the image export information.
5. Click Confirm again to complete.

Create Linux Image

Overview

This document guides you to create a Linux image.

Directions

Preparations

When you export a system disk image, you need to check the following:

> Note:
> If you export via a data disk image, you can skip this operation.

Check OS Partition and Starting Mode

1. Execute the following command to check whether the OS partition is a GPT partition.

   sudo parted -l /dev/sda | grep 'Partition Table'

   - If the returned result is msdos, it is an MBR partition, then proceed to the next step.
   - If the returned result is gpt, it is a GPT partition. Currently, GPT partitions are not supported for service migration.

2. Execute the following command to check whether the operating system is started in EFI mode.

   sudo ls /sys/firmware/efi

   - If the file exists, the current operating system is started in EFI mode.
   - If the file does not exist, proceed to the next step.

Check System Key Files

The key system files that need to be checked include but are not limited to the following:

> Note:
> Follow the standards of the relevant distribution to ensure that the location and permissions of key

> system files are correct and can be read and written normally.

- /etc/grub/grub.cfg: It is recommended to use uuid to mount root in kernel parameters. Other methods (such as root=/dev/sda) may cause the system to fail to start.
- /etc/fstab: Do not mount other hard disks. After migration, the system may fail to start due to disk loss.
- /etc/shadow: The permissions are normal and can be read and written.

Uninstall Software

Uninstall drivers and software that may cause conflicts (including VMware tools, Xen tools, Virtualbox GuestAdditions, and some software that comes with its own underlying drivers).

Check Virtio Driver

For details, see Check Virtio Driver in Linux System.

Install cloud-init

For installation details, see Install cloud-init on Linux System.

Check Other Hardware-related Configurations

Hardware changes after migration to the cloud include but may not be limited to:

- The graphics card is replaced with Cirrus VGA.
- The disk is replaced with Virtio Disk, and the device names are vda and vdb.
- The network interface is replaced with Virtio Nic, which only provides eth0 by default.

Find Partitions and Sizes

Execute the following command to view the partition format of the current operating system and determine the partition to be copied and its size.

```
mount
```

Take the following returned results as an example:

```
proc on /proc type proc (rw,nosuid,nodev,noexec,relatime)
sys on /sys type sysfs (rw,nosuid,nodev,noexec,relatime)
dev on /dev type devtmpfs (rw,nosuid,relatime,size=4080220k,nr_inodes=1020055,mode=755)
run on /run type tmpfs (rw,nosuid,nodev,relatime,mode=755)
/dev/sda1 on / type ext4 (rw,relatime,data=ordered)
```

```
securityfs on /sys/kernel/security type securityfs (rw,nosuid,nodev,noexec,relatime)
tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev)
devpts on /dev/pts type devpts (rw,nosuid,noexec,relatime,gid=5,mode=620,ptmxmode=000)
tmpfs on /sys/fs/cgroup type tmpfs (ro,nosuid,nodev,noexec,mode=755)
cgroup on /sys/fs/cgroup/unified type cgroup2 (rw,nosuid,nodev,noexec,relatime,nsdelegate)
cgroup on /sys/fs/cgroup/systemd type cgroup (rw,nosuid,nodev,noexec,relatime,xattr,name=systemd)
pstore on /sys/fs/pstore type pstore (rw,nosuid,nodev,noexec,relatime)
cgroup on /sys/fs/cgroup/cpu,cpuacct type cgroup (rw,nosuid,nodev,noexec,relatime,cpu,cpuacct)
cgroup on /sys/fs/cgroup/cpuset type cgroup (rw,nosuid,nodev,noexec,relatime,cpuset)
cgroup on /sys/fs/cgroup/rdma type cgroup (rw,nosuid,nodev,noexec,relatime,rdma)
cgroup on /sys/fs/cgroup/blkio type cgroup (rw,nosuid,nodev,noexec,relatime,blkio)
cgroup on /sys/fs/cgroup/hugetlb type cgroup (rw,nosuid,nodev,noexec,relatime,hugetlb)
cgroup on /sys/fs/cgroup/memory type cgroup (rw,nosuid,nodev,noexec,relatime,memory)
cgroup on /sys/fs/cgroup/devices type cgroup (rw,nosuid,nodev,noexec,relatime,devices)
cgroup on /sys/fs/cgroup/pids type cgroup (rw,nosuid,nodev,noexec,relatime,pids)
cgroup on /sys/fs/cgroup/freezer type cgroup (rw,nosuid,nodev,noexec,relatime,freezer)
cgroup on /sys/fs/cgroup/net_cls,net_prio type cgroup (rw,nosuid,nodev,noexec,relatime,net_cls,net_pr
io)
cgroup on /sys/fs/cgroup/perf_event type cgroup (rw,nosuid,nodev,noexec,relatime,perf_event)
systemd-1 on /home/libin/work_doc type autofs (rw,relatime,fd=33,pgrp=1,timeout=0,minproto=5,ma
xproto=5,direct,pipe_ino=12692)
systemd-1 on /proc/sys/fs/binfmt_misc type autofs (rw,relatime,fd=39,pgrp=1,timeout=0,minproto=
5,maxproto=5,direct,pipe_ino=12709)
debugfs on /sys/kernel/debug type debugfs (rw,relatime)
mqueue on /dev/mqueue type mqueue (rw,relatime)
hugetlbfs on /dev/hugepages type hugetlbfs (rw,relatime,pagesize=2M)
tmpfs on /tmp type tmpfs (rw,nosuid,nodev)
configfs on /sys/kernel/config type configfs (rw,relatime)
tmpfs on /run/user/1000 type tmpfs (rw,nosuid,nodev,relatime,size=817176k,mode=700,uid=1000,gid
=100)
gvfsd-fuse on /run/user/1000/gvfs type fuse.gvfsd-fuse (rw,nosuid,nodev,relatime,user_id=1000,group
_id=100)
```

It can be seen that the root partition is in `/dev/sda1` , while there is no independent partition in `/boot` and `/home` . And sda1 contains the boot partition, lacks mbr, so we just need to copy the entire sda.

> Note:
> The exported image must contain at least the root partition and MBR. If the exported image lacks MBR, it will not be able to start. In the current operating system, if `/boot` and `/home` are independent partitions, the exported image also needs to contain these two independent partitions.

Export Image

Select different ways to export the image based on actual needs.

- Use Tool to Export
- Use Command to Export Image

Use Platform Tools to Export Image

Use the export image tool of the virtualization platform such as VMWare vCenter Convert or Citrix XenConvert. For details, see the export tool documentation for each platform.

> Note:
> Currently, the image formats supported by service migration are: qcow2, vhd, raw, and vmdk.

Use Command to Export Image

> Note:
> Using commands to manually export images has a high risk (for example, when IO is busy, the file system metadata may become disordered). It is recommended that you check image is complete after exporting it.

You can export the image by executing the following command:

- Use qemu-img command
  For example, execute the following command to export /dev/sda to /mnt/sdb/test.qcow2 .

  ```
  sudo qemu-img convert -f raw -O qcow2 /dev/sda /mnt/sdb/test.qcow2
  ```

  If you need to convert to other formats, you can modify the parameter values of -O . The following parameter values can be modified:

Among them, /mnt/sdb indicates a new mounted disk or other network storage.

Parameter Value	Description
qcow2	qcow2 format
vpc	vhd format
vmdk	vmdk format
raw	No format

- Use dd command

  For example, execute the following command to export the image in raw format.

  ```
  sudo dd if=/dev/sda of=/mnt/sdb/test.imag bs=1K count=$count
  ```

  Among them, count parameter is the number of partitions to be copied. You can use fdisk command to find out the value. If you need to copy the entire disk, count parameter can be ignored.

  For example, execute the following command to view the number of partitions in /dev/sda .

  ```
  fdisk -lu /dev/sda
  ```

  The result resembles the following is returned:

  ```
  Disk /dev/sda: 1495.0 GB, 1494996746240 bytes
  255 heads, 63 sectors/track, 181756 cylinders, total 2919915520 sectors
  Units = sectors of 1 * 512 = 512 bytes
  Sector size (logical/physical): 512 bytes / 4096 bytes
  I/O size (minimum/optimal): 4096 bytes / 4096 bytes
  Disk identifier: 0x0008f290

    Device Boot      Start         End      Blocks   Id  System
  /dev/sda1   *        2048    41945087    20971520   83  Linux
  /dev/sda2        41945088    46123007     2088960   82  Linux swap / Solaris
  /dev/sda3        46123008    88066047    20971520   83  Linux
  /dev/sda4        88066048  2919910139  1415922046   8e  Linux LVM
  ```

  The returned result of the fdisk command shows that the end position of sda1 is 41945087 * 512 bytes, and the count is set to 20481M.

> Note:
> The image exported by the dd command is in raw format. It is recommended to convert the image to qcow2, vhd, or other image format.

Image Format Conversion

> Note:
> Currently, the image formats supported by service migration are: qcow2, vhd, vmdk, and raw. It is recommended to use a compressed image format to save transmission and migration time.

Use qemu-img command to convert the image format.
For example, execute the following command to convert an image in raw format to qcow2 format.

```
sudo qemu-img convert -f raw -O qcow2 test.img test.qcow2
```

- -f indicates the format of the source image file.
- -O indicates the format of the target image file. For supported formats, see the parameter value of -O.

Check Image

> Note:
> If you create an image without stopping the service or for other reasons, the image file system may be incorrect. Therefore, it is recommended that you check whether the image is correct after creating it.

When the image format is consistent with the format supported by the current platform, you can directly open the image to check the file system. For example, the Windows platform can directly attach an image in vhd format, the Linux platform can use qemu-nbd to open an image in qcow2 format, and the Xen platform can directly enable a vhd file.
Take Linux platform as an example:

```
modprobe nbd
qemu-nbd -c /dev/nbd0 xxxx.qcow2
mount /dev/nbd0p1 /mnt
```

If the file system is damaged when the first partition of the qcow2 image is exported, an error will be reported during mount.
In addition, you can also start the Cloud Virtual Machine to test whether the image file can be used before uploading it.

Creating Windows Image

Scenarios

This document takes the Windows Server 2012 operating system as an example to guide you on how to create Windows images.

Operation Steps

Preparations

When you export a system disk image, you need to check the following:

> Note:
> If you export via a data disk image, you can skip this operation.

Checking OS Partition and Starting Mode

1. On the operating system interface, click to open a Windows PowerShell window.
2. In the Windows PowerShell window, enter diskmgmt.msc, and press Enter to open Disk Management.
3. Right-click the disk to be checked > Attribute, and select the Volume tab to check the disk partition type.
4. Determine whether the disk partition type is GPT partition.
   - Yes, since GPT partitions are not supported by service migration, submit a ticket for feedback.
   - If it is not, proceed to the next step.
5. Open CMD as an administrator and execute the following command to verify whether the operating system is started in EFI mode.

   ```
   bcdedit /enum {current}
   ```

   Take the following returned results as an example:

   ```
   Windows Boot Loader
   Identifier              {current}
   device                  partition=C:
   path                    \WINDOWS\system32\winload.exe
   description             Windows 10
   ```

```
locale                  zh-CN
inherit                 {bootloadersettings}
recoverysequence        {f9dbeba1-1935-11e8-88dd-ff37cca2625c}
displaymessageoverride  Recovery
recoveryenabled         Yes
flightsigning           Yes
allowedinmemorysettings 0x15000075
osdevice                partition=C:
systemroot              \WINDOWS
resumeobject            {1bcd0c6f-1935-11e8-8d3e-3464a915af28}
nx                      OptIn
bootmenupolicy          Standard
```

- If `path` parameter contains efi, the current operating system is started in EFI mode.
- If `path` parameter does not contain efi, proceed to the next step.

Uninstalling Software

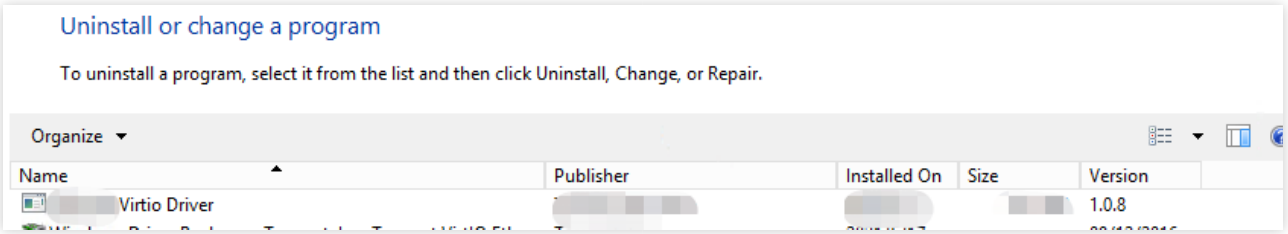
Uninstall drivers and software that may cause conflicts (including VMware tools, Xen tools, Virtualbox GuestAdditions, and some software that comes with its own underlying drivers).

Installing cloud-base

For installation details, see cloud-base Installation Document.

Checking or Installing Virtio Driver

1. Open Control Panel > Programs and Features and search for Virtio in the search bar.
   - If the returned result is as shown below, the Virtio driver has been installed.



2. If the Virtio driver is not installed, you need to install it manually.
   - For Microsoft Windows Server 2008 R2 (Standard, Data Center, and Enterprise editions) and Microsoft Windows Server 2012 R2 (Standard edition), contact your engineer to obtain a customized Virtio version.
   - For other system versions, download Community Edition of virtio.

Checking Other Hardware-related Configurations

Hardware changes after migration to the cloud include but may not be limited to:

- The graphics card is replaced with Cirrus VGA.
- The disk is replaced with Virtio Disk.
- The network interface is replaced with Virtio Nic, which is a local connection by default.

Exporting an Image

Select different tools to export images based on actual needs.

- Use platform tools to export image.
- Use disk2vhd to export image.

Using Platform Tools to Export Images

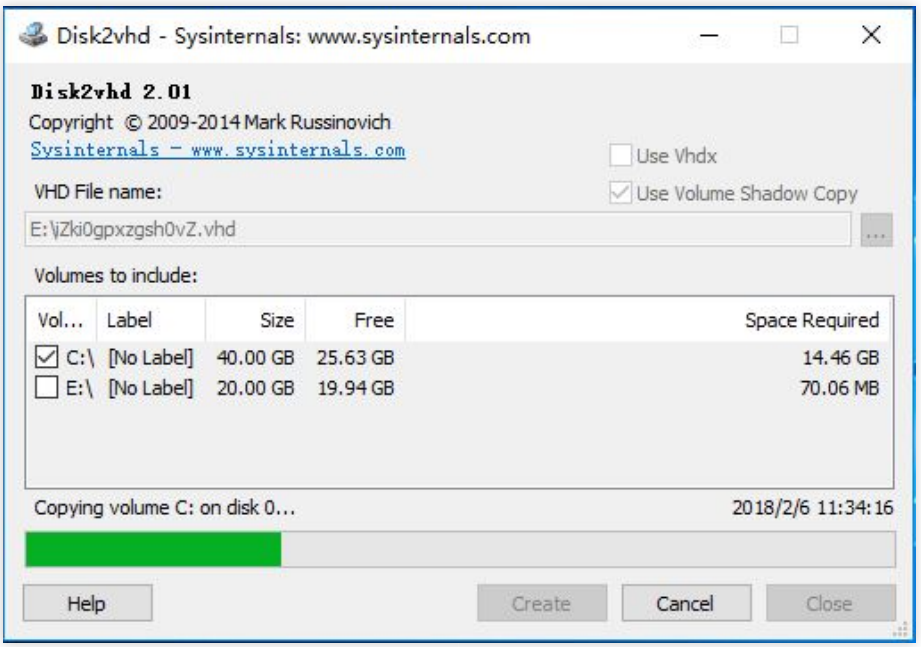
Use the export image tool of the virtualization platform such as VMWare vCenter Convert or Citrix XenConvert. For details, see the export tool documentation for each platform.

> Note:
> Currently, the image formats supported by Converge Cloud service migration are: qcow2, vhd, raw, and vmdk.

Using disk2vhd to Export Images

When you need to export the system on physical machines or do not want to use platform tools to export, you can use the disk2vhd tool to export.

1. Install and open the disk2vhd tool.
2. Select the destination path for the exported image, check the volumes to be copied, and click Create.
   Note:
   - The disk2vhd can run only after the VSS (Volume Shadow copy service) feature is preinstalled on Windows.
   - Do not check Use Vhdx because the system currently does not support images in vhdx format.
   - It is recommended to check Use volume Shadow Copy and use the volume shadow copy to better keep the data integrity.



Checking Images

> Note:
> If you create an image without stopping the service or for other reasons, the image file system may be incorrect.

> Therefore, it is recommended that you check whether the image is correct after creating it.

When the image format is consistent with the format supported by the current platform, you can directly open the image to check the file system. For example, the Windows platform can directly attach an image in vhd format, the Linux platform can use qemu-nbd to open an image in qcow2 format, and the Xen platform can directly enable a vhd file.

Take Linux platform as an example:

```
modprobe nbd
qemu-nbd -c /dev/nbd0 xxxx.qcow2
mount /dev/nbd0p1 /mnt
```

If the file system is damaged when the first partition of the qcow2 image is exported, an error will be reported during mount.

In addition, you can also start the Cloud Virtual Machine to test whether the image file can be used before uploading it.

Service Migration
Offline Migration

Overview

Service migration is a migration platform developed to facilitate enterprise users to move to the cloud. The migration platform can migrate the operating system, applications, and application data of the source host to a Cloud Virtual Machine (CVM) or Cloud Block Storage (CBS) to meet business needs such as enterprise cloud migration, cross-cloud platform migration, cross-account/region migration, or hybrid cloud deployment.

Service migration currently includes offline migration and online migration. Offline migration includes the following two types:

- Offline instance migration: migrate the system disk image to the specified Cloud Virtual Machine.
- Offline data migration: migrate the data disk image to the specified Cloud Block Storage.

Prerequisites

Offline migration requires the support of Cloud Object Storage (COS). Ensure that your region is within the COS support range.

Preparations

> Note:
> - Currently, the image formats supported by service migration are: qcow2, vhd, vmdk, and raw. It is recommended to use a compressed image format to save transmission and migration time.
> - The COS region where you upload the image must be consistent with the region of the Cloud Virtual Machine you will migrate to.
> - During offline migration, the uploaded image file cannot be larger than the capacity of the disk to be migrated. If the image file is 50G, the minimum system disk size of the migrated instance is 50G.

- Create an image file for the server to be migrated according to the image creation document.
  - For Windows systems, see Windows Image Creation Documentation.
  - For Linux systems, see Linux Image Creation Documentation.
- Upload the created image file to COS.

  - Since image files are generally large and web uploads are prone to disconnection, it is recommended to use COSCMD to upload image files. For detailed operations, see the COSCMD Tool Documentation.
  - If the image you exported from other cloud platforms is in a compressed package format (such as .tar.gz), you do not need to decompress it yourself, but can directly upload it to COS and migrate it.
- Obtain the COS address where the image is uploaded.
  - In the Cloud Object Storage console, find the image file you just uploaded, view the file information, and obtain the file link.
- Prepare the Cloud Virtual Machine or Cloud Block Storage to be migrated.

Directions

Offline Instance Migration

1. Log in to the CVM Console.
2. In the left navigation, click Service Migration.
3. Click Create Instance Migration.
4. Prepare and confirm that the migration preparations have been established, and click Next.
5. Select your region, enter the task name, COS link, Cloud Virtual Machine to be migrated and other migration configuration information, and click Finish to create the migration task.
   Return to the offline data migration management page to view the progress of the migration task.
   Note:
   - The system disk capacity of the migrated instance cannot be less than the size of the uploaded image file, otherwise the task will fail.

Offline Data Migration

1. Log in to the CVM Console.
2. In the left navigation, click Service Migration.
3. Click Create Data Migration.
4. Prepare and confirm that the migration preparations have been established, and click Next.
5. Select your region, enter the task name, COS link, Cloud Block Storage to be migrated and other migration configuration information, and click Finish to create the migration.

   > Note:
   > The capacity of the migrated Cloud Block Storage cannot be less than the size of the uploaded image file, otherwise the task will fail.

FAQs

For details, please see Service Migration Class.

Online Migration
Online Migration Overview

Online migration can migrate systems and applications on the source server from source environments such as self-developed IDCs or cloud platforms to cloud platforms to meet business needs such as enterprise cloud migration, cross-cloud platform migration, cross-account/region migration, or hybrid cloud deployment.

> Note:
> The source server mentioned in this document can be a physical server, a virtual machine, or a Cloud Virtual Machine on other cloud platforms. Other cloud platforms include but are not limited to AWS, Google Cloud Platform, Converge Cloud, and Huawei Cloud.

Applicable Scenario

Online migration is applicable to the following scenarios (including but not limited to):

- IT architecture to the cloud
- Hybrid cloud architecture deployment
- Cross-cloud migration
- Cross-account or cross-region migration

Supported Features

Currently, online migration supports server migration features.

Preparations

- The account and destination server have been prepared on the cloud platform.
- It is recommended that you suspend applications on the source server to avoid possible impacts on existing applications during the migration.

FAQs

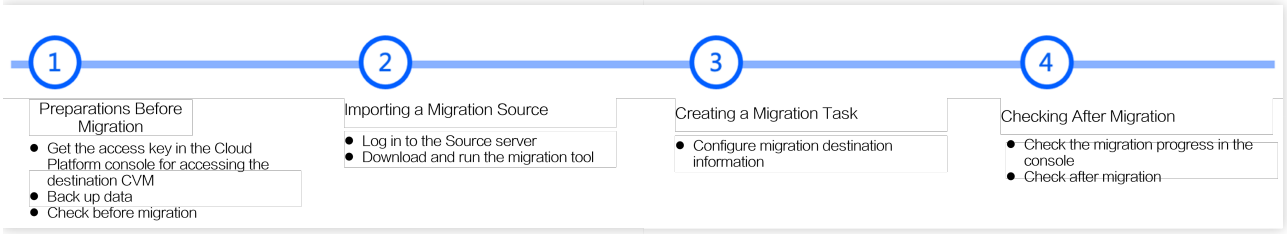
For details, please see Service Migration Class.

Migration Operation Guide
Online Migration: Importing a Migration Source Through the Clien

This document describes how to migrate your source server to CVM online by importing the migration source through the client.

Migration Process

The process of online migration by importing the migration source through the client is shown in the figure below:



Migration Steps

Step 1: Preparations Before Migration

- Create and obtain SecretId and SecretKey on the Cloud Access Management > Cloud API Key page.
- Obtain the domain name address of the cloud API EndPoint for the target environment.
- It is recommended to suspend applications on the host and back up data to avoid possible impacts on existing applications during migration:
  - Source host: You can back up the data by means such as the source server snapshot feature. The source host refers to the host to be migrated.
  - Target CVM: You can back up the data of the target CVM by means such as creating a snapshot.
- If you use a sub-account for console migration:
  - If the migration target is an instance, the sub-account requires QcloudCSMFullAccess and QcloudCVMFullAccess permissions. You can use the root account to navigate to Cloud Access Management > Policy Management to grant them.
  - If the migration target is a CVM image, the sub-account requires QcloudCSMFullAccess, QcloudCVMFullAccess, and QcloudCVMFinanceAccess permissions. You can use the root account to navigate to Cloud Access Management > Policy Management to grant them.
- Before migration, you need to conduct checks according to the actual situation. The check contents are as follows:
  - If the migration target is a CVM, both the source host and the target CVM need to be checked.
  - If the migration target is a CVM image, only the source host needs to be checked. For specific operation

methods, see Migration Methods below.

Migration Methods

Linux source host: After a migration request is initiated to the cloud API, the cloud API will use the current UNIX time to check the generated Token. Make sure that the current system time is correct.

Windows source host:

1. Check and install Virtio. For operation details, see Check Virtio Driver in Windows System.
2. (Optional) Check and install Cloudbase-Init. For details, see Install Cloudbase-Init on Windows Operating System. You can choose to install it on the source host before migration or on the target instance after migration.
   - If it is installed before migration, automatic network configuration, activation, and other initialization operations will be carried out after migration.
   - If it is not installed before migration, you may need to log in to the instance using VNC and manually modify the network configuration.
3. It is recommended to temporarily disable the antivirus software to avoid mistakenly killing the migration tool, which could cause migration failure.

Target CVM:

1. Storage space: The size and quantity of the cloud disk (including the system disk and data disk) for the target CVM need to be greater than or equal to the disk configuration of the source machine.
2. Security group: Ports 80, 443, and 3389 are open in the security group.
3. Bandwidth settings: It is recommended to increase the source and target bandwidths as much as possible for faster migration. During migration, a traffic approximately equal to the data volume will be consumed. If necessary, adjust the network billing mode in advance.
4. Network settings: If your source host or target host only has IPv6 and does not have IPv4, see client.json File Parameter Description.

> Note:

- Source host checks can be automatically performed using tool commands such as sudo ./go2cloud_x64 --check .
- The go2cloud migration tool automatically checks whether migration conditions are met when it starts. If you need to skip the check and force migration, you can add the parameter ./go2cloud_x64 -ignore-check .

Step 2: Importing a Migration Source

Importing a Migration Source Through the Migration Tool

Linux server

1. Contact the architect to obtain the online migration toolkit go2cloud.zip. Upload the migration tool go2cloud.zip to the source host to be migrated and enter the corresponding directory.

```
unzip go2cloud.zip
```

cd go2cloud/go2cloud-linux

> Note:
> Files under the go2cloud directory will not be migrated. Do not place files that need to be migrated in this directory.

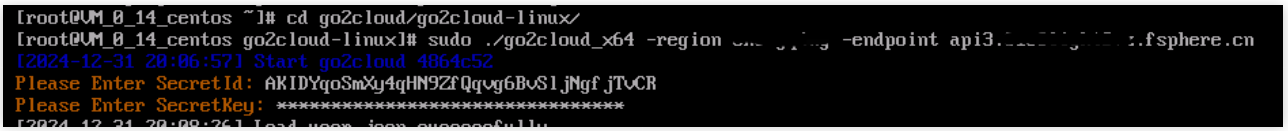
2. (Optional) Exclude files or directories on the source host that do not need to be migrated.
   If there are files or directories on the Linux source host that do not need to be migrated, you can add them to the rsync_excludes_linux.txt file.
3. Import the migration source.

   i. Taking the 64-bit Linux source host as an example, execute the following commands with root permissions to run the tool. Note that the parameter values of the target region (region) and target environment (endpoint) need to be replaced by yourself.

   chmod +x go2cloud_x64

   sudo ./go2cloud_x64 -region xxxx -endpoint api3.xxxxxx.fsphere.cn

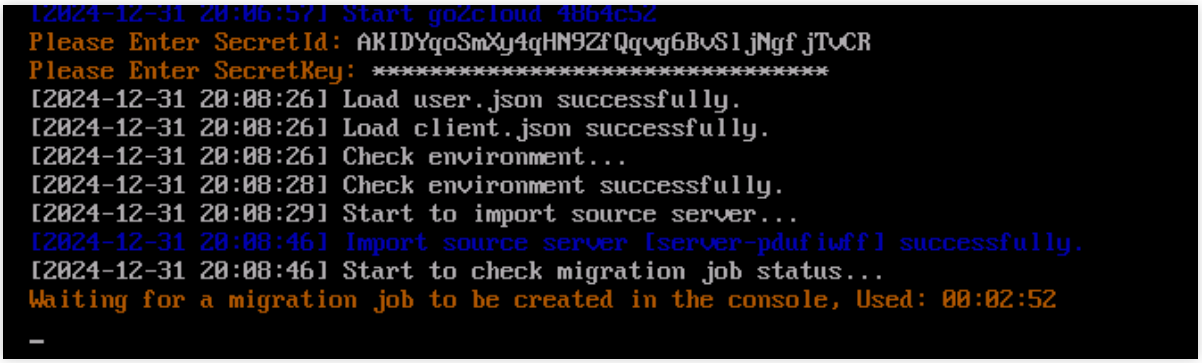
   ii. Enter the SecretId and SecretKey of the account API access key obtained in the step Preparations Before Migration as prompted, and press Enter.



   If you want to input the access key without interaction, you can add -secret-id and -secret-key in the command line parameters, for example:

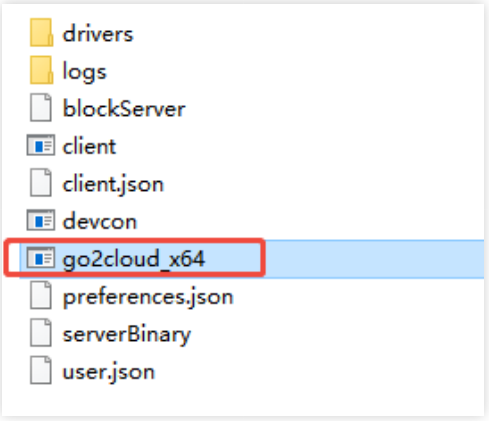
   sudo ./go2cloud_x64 -region xxxx -endpoint api3.xxxxx.fsphere.cn -secret-id xxxx -secret-key xxxxx

   When the following information appears on the migration tool interface, it indicates that the migration source has been successfully imported into the console, and you can navigate to the console to view the migration source.



Windows server

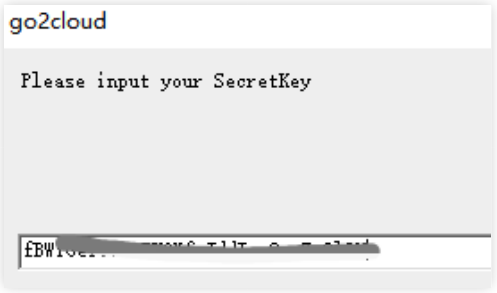
1. Upload the migration toolkit go2cloud.zip to the source host, decompress it to get the go2cloud folder, open go2cloud-windows inside, and you will get the directory as shown in the figure below:



2. As an administrator, enter cd /d the absolute path of the directory where go2cloud_x64.exe is located in CMD or PowerShell command line to run the go2cloud_x64.exe application. Note that the parameter values of the target region (region) and target environment (endpoint) need to be replaced by yourself.

   .\go2cloud_x64.exe -region xxxx -endpoint api3.xxxxxx.fsphere.cn

3. Enter the cloud API access key (SecretId and SecretKey) in the pop-up window. If you want to input the access key without interaction, you can add -secret-id and -secret-key in the command line parameters.

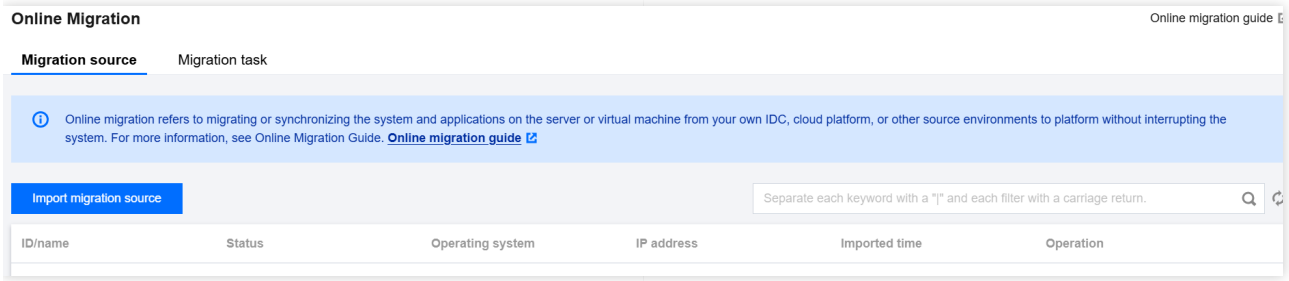


4. When the following information appears on the migration tool interface, it indicates that the migration source has been successfully imported into the console, and you can navigate to the console to view the migration source.

> Note:
> If the message "Import source server successfully" does not appear, it indicates that the import of the migration source has failed. You can view the log (it is the logs/log file under the migration tool directory by default) to identify and resolve the issue, then run the migration tool again to import the migration source.

Viewing the Migration Source Through the Console

Log in to the Online Migration Console to view the imported migration sources with the status of Online, as shown in the figure below.



> Note:
> After the migration source is imported successfully, do not close the migration tool in the instance until the migration task is completed. Otherwise, after the migration source goes offline, the migration task cannot be completed. The operation of the migration task depends on the availability of the migration source. Do not terminate the migration tool process.

Step 3: Creating a Migration Task

1. Create a migration task.

Log in to the Online Migration console and click Create Migration Task on the right side of the row where the target migration source is located. In the pop-up Create Migration Task window, configure the task according to the following information.

The migration task configuration is detailed in the table below:

- Basic options:

Configuration Option	Required or Not	Description
Target Region	Yes	The region where the source host will be migrated to. For regions, see [Regions and AZs](/document/product/292128/6091).
Task Name	Yes	Name of the migration task.
Task Description	No	Description of the migration task.
Target Type	Yes	Set the target type for migrating the migration source to this cloud platform. - **CVM image**: After the migration task is completed, a target image of this cloud platform will be generated for the migration source. - Image name: The name of the target cloud platform image generated for the migration source. When the image name is duplicated in the target region, the migration task will automatically add the task ID to the image name. - **CVM instance**: Select a CVM instance in the target region as the migration target. - Target instance: It is recommended that the operating system of the target CVM be as consistent as possible with the operating system type of the source host. For example, when you migrate a source host with CentOS 7 system, select a CVM with CentOS 7 system as the migration target.
Image Name	Yes	When the target type of the migration task is **CVM image**, you will get a custom image, and you need to name the image here. When the image name is duplicated in the target region, the migration task will automatically add the task ID to the image name.

Configuration Option	Required or Not	Description
Network Mode	Yes	Set the network type used for transferring data during migration. - **Public network transmission**: Use public network transmission when transferring data to the target CVM or relay instance during migration. - **Public network transmission**: Use private network transmission when transferring data to the target CVM or relay instance during migration. - Virtual Private Cloud (VPC): When you migrate to a CVM image, the relay instance will be created in this VPC. - Subnet: When you migrate to a CVM image, the relay instance will be created in this subnet.
Migration Method	Yes	Set the migration method type for migrating data of Linux instances, and the differences between different migration methods are as follows. ◦ Linux file-level migration: The migration granularity is at the file level, with high compatibility and relatively low transmission efficiency. ◦ Linux block-level migration: The migration granularity is at the disk logical storage unit block level, with high transmission efficiency and relatively low compatibility.
		Windows block-level migration: The migration granularity is at the disk logical storage unit block level. Windows migration defaults to block-level migration, which offers high compatibility and high transmission efficiency.
Configure Incremental Synchronization	No	Customize the configuration of the incremental synchronization duration, continuously synchronize data, and flexibly control the migration handover time. ◦ Not enabled: The migration tool automatically identifies and performs incremental migration, which is usually executed once. ◦ Enabled: You can choose the execution duration for incremental synchronization. After this option is enabled, the tool will enter the incremental migration phase after the full data migration is completed. It will conduct multiple rounds of incremental data synchronization within the duration you set until the set duration expires, and then automatically end the migration. You can also manually stop incremental synchronization in the task list to end the migration ahead of schedule. After the incremental synchronization starts, you can view the incremental synchronization records on the task details page of the Online Migration > Migration Task console.
Scheduled Execution Time	No	After you create a migration task, the migration task will automatically start at the set time. The earliest scheduled execution time can be set to 10 minutes after the current time.

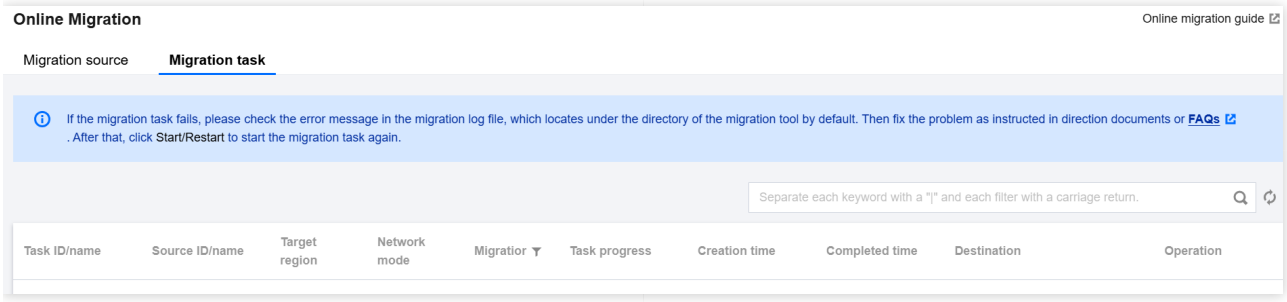
- Advanced configuration (optional):

Configuration Option	Required or Not	Description
Transmission Limit (KB/s)	No	The bandwidth upper limit for data transmission during migration, with the unit being KB/s and the range being [0, 25600]. By default, there is no speed limit. This option is not supported for Windows migration.
Checksum Verification	No	After this option is enabled, data consistency checks will be enhanced, but it might cause a reduction in transmission speed. This option is not supported for Windows migration yet.

1. Start the migration task.

> Note:
> This step can be skipped for scheduled tasks. Once the scheduled execution time is reached, the migration task will automatically start.

After creating a migration task, you can click the Migration Task tab to view the migration task.



Click Start/Retry on the right side of the row where the task is located, and click Yes in the pop-up confirmation window to start the migration task. At this point, the task status changes to Migrating.

> Note:
> - If the migration target is a CVM, after the migration starts, the target CVM will enter migration mode. Do not perform operations such as reinstalling the system, shutting down, terminating, or resetting the password on the target CVM, until the migration is completed and you exit migration mode.
> - When the migration target is a CVM image, after the migration starts, a relay instance named do_not_delete_csm_instance will be created under your account. Do not perform operations such as reinstalling the system, shutting down, terminating, or resetting the password on the relay instance until the migration is completed. The system will automatically terminate the relay instance created this time after the migration is completed. The relay instance will incur certain costs, including instance fees and cloud disk fees.

Step 4: Checking After Migration

1. View the migration progress in the console.

When the migration task status is Successful, it indicates that the migration has been completed successfully.

> Note:
> - Since the data transmission time is affected by factors such as the size of the source data and network bandwidth, wait patiently for the migration process to complete.
> - After the migration task starts, the task can be paused during the data transmission phase. You can click Pause in the row where the migration task is located, and after a while, the system will stop the migration task.
> - The migration tool supports resumable transfer. After pausing the task, you can simply click Start/Retry again to continue the migration from the last pause point.
> - If the migration process takes too long and you need to stop this migration, you can first pause the migration task and then click Delete to cancel this migration task.

1. Check after migration.

- The migration is failed:
  - You can view the error code in the Online Migration console and see the document Migration Failure Guide for corresponding solutions.
  - You can also check the error information output in the log file (It is the log file under the logs directory of the migration tool by default.) or see Server Migration FAQs for troubleshooting and fixing problems. After the fix, click Start/Retry in the migration task operation column to restart the migration task.
- The migration is successful:
  - If the migration target is a CVM, check whether the target CVM can start normally, whether the data of the target CVM is consistent with that of the source host, and whether the network or other system services are normal.
  - If the migration target is a CVM image, you can click the CVM Image ID in the row where the migration task is located to enter the Cloud Virtual Machine > Image page to view the image information. You can use this image to create a CVM.

Migration Tool Description Compatibility and Tool Configuration Instructions

Supported Operating Systems

Currently, the source host operating systems supported by online migration tools include but are not limited to the following operating systems:

Linux Operating System	Windows Operating System
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	

Supported Migration Modes

Public Network Migration Mode

If both your source host and target CVM have public network access capabilities, you can use the public network migration mode for migration.

In the current public network migration mode, the control linkage of the tool accesses the Cloud Platform's API via the Internet to initiate a migration request, while the data linkage of the tool transmits data to the target CVM via the Internet, migrating the source host to the target CVM on the cloud platform. The mode parameter value corresponding to this mode is 0.

Private Network Migration Mode

If your source host or target CVM is located in a private network or VPC, and the source host cannot directly connect to the target CVM through the Internet, you can use the tool's private network migration mode for migration. In the private network migration mode, you need to create a connection channel between the source host and the target CVM by means such as VPC Peering Connection, VPN Connections, and Direct Connect.

- Scenario 1: (Only migration using tools is supported for this scenario.) If your source host or target CVM cannot access the public network, you can first initiate a migration request by using a host that can access the public network (such as a gateway) to access the cloud platform's API via the Internet (the control linkage of the tool), and then transfer data to the target CVM through a private network

channel for migration (the data linkage of the tool). This scenario does not require that the source host and the target CVM can access the public network. The mode parameter value corresponding to this scenario is 1.

- Scenario 2: If your source host can access the public network, you can first initiate a migration request by accessing the cloud platform's API via the Internet on the source host (the control linkage of the tool), and then transfer data to the target CVM through a private network channel for migration (the data linkage of the tool). This scenario requires that the source host can access the public network, but does not have this requirement for the target CVM. The mode parameter value corresponding to this scenario is 2.

- Scenario 3: If your source host can access the public network via an HTTP proxy, you can first initiate a migration request by accessing the cloud platform's API via the network proxy on the source host (the control linkage of the tool), and then transfer data to the target CVM through a private network channel for migration (the data linkage of the tool). This scenario does not require that the source host and the target CVM can access the public network. The mode parameter value corresponding to this scenario is 3.

Compressed Package File Description

After go2cloud.zip is decompressed, the file description is as follows:

File Name	Description
go2cloud-linux.zip	The compressed migration package for Linux system.
go2cloud-windows.zip	The compressed migration package for Windows system.
readme.txt	The directory introduction file.
release_notes.txt	The migration tool change log.

After go2cloud-linux.zip is decompressed, the file description is as follows:

File Name	Description
go2cloud_x64	The migration tool executable program for the x86 architecture 64-bit Linux system.
go2cloud_x32	The migration tool executable program for x86 architecture 32-bit Linux system.

File Name	Description
go2cloud_arm64	The migration tool executable program for the arm architecture 64-bit Linux system.
user.json	User information during migration.
client.json	The configuration file of the migration tool.
rsync_excludes_linux.txt	rsync configuration file, which excludes the file directories that do not need to be migrated under Linux system. Windows system uses block-level migration so they do not support file and directory filtering.

After go2cloud-windows.zip is decompressed, the file description is as follows:

File Name	Description
go2cloud_x64.exe	The migration tool executable program for the x86 architecture 64-bit Windows system.
user.json	User information during migration.
client.json	The configuration file of the migration tool.
client.exe	The executable program for data migration of Windows system.

> Note:
> The configuration file cannot be deleted and should be stored in the same directory level as the go2cloud executable program.

user.json File Parameter Description

The user.json configuration file is described in the table below:

Parameter Name	Type	Required or Not	Description
SecretId	String	No	The access key SecretId of Account API.
SecretKey	String	No	The access key SecretKey of Account API.
Region	String	No	The region of the target CVM. You only need to specify the region. The availability zone is not required.
InstanceId	String	No	The instance ID of the target CVM, which is in the format of ins-xxxxxxxx. (Cloud Lighthouse is not supported for now)

Parameter Name	Type	Required or Not	Description
EndPoint	string	No	The EndPoint domain name of the cloud API for the target environment.

client.json File Parameter Description

The client.json configuration file is described in the table below:

Parameter Name	Type	Required or Not	Description
Client.Extra.IgnoreCheck	Bool	No	The default value is false. By default, the migration tool automatically checks the source host environment when the tool starts running. If you need to skip this check, set this value to true. You can also trigger it directly by using the -ignore-check startup parameter of the tool.
Client.Extra.Daemon	Bool	No	The default value is false. If you need the migration tool to run in the backend, set this parameter to true. You can also do this using the -daemon startup parameter of the tool.
Client.Net.Proxy.Ip	String	No	The default value is empty. If the migration scenario involves migrating through the private network (scenario 3), you need to configure the IP address of the network proxy. You can also pass the IP value directly using the tool's -proxy-ip startup parameter.
Client.Net.Proxy.IPv6	Bool	No	The default value is false. If you want to transfer data using IPv6 (for example, in a migration scenario where the source or target has only IPv6 IP addresses), you need to set this option to true. Otherwise, the migration traffic will be transferred via IPv4.
Client.Net.Proxy.Port	String	No	The default value is empty. If the migration scenario involves migrating through the private network (scenario 3), you need to configure the port of the network proxy. You can also pass the port value directly using the tool's -proxy-port startup parameter.

Parameter Name	Type	Required or Not	Description
Client.Net.Proxy.User	String	No	The default value is empty. If the migration scenario involves migrating through the private network (scenario 3) and your network proxy requires authentication, you need to configure the username for the network proxy. You can also pass the username directly using the tool's -proxy-user startup parameter.
Client.Net.Proxy.Password	String	No	The default value is empty. If the migration scenario involves migrating through the private network (scenario 3) and your network proxy requires authentication, you need to configure the password for the network proxy. You can also pass the password directly using the tool's -proxy-password startup parameter.

Note:
The configuration items of the client.json file usually do not need to be filled in.

rsync_excludes_linux.txt File Description

Exclude files in the Linux source host that do not need to be transferred during migration, or configuration files under specified directories. The following directories and files have been excluded by default in this file, do not delete or modify them.

```
/dev/*
/sys/*
/proc/*
/var/cache/yum/*
/lost+found/*
/var/lib/lxcfs/*
/var/lib/docker-storage.btrfs/root/.local/share/gvfs-metadata/*
```

If you need to exclude other directories and files, append content at the end of this file. For example, to exclude all contents of the data disks mounted to /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/*

Tool Running Parameter Description

Parameter Option	Description
--help	Print help information.
--check	Check whether the source machine meets the migration requirements. This parameter only involves checks but not migration.
--log-file	Set the log file name. The default value is log.
--log-level	The log output level. Valid values: 1 (ERROR level), 2 (INFO level), and 3 (DEBUG level). Default value: 2.
--version	Print the version number.
--clean	Make the target machine exit the migration mode and clean up and restore tool configuration files.
-secret-id	Cloud API access key SecretId.
-secret-key	Cloud API access key SecretKey.
-region	The target region to which you need to migrate.
-instance-id	The ID of the target instance that needs to be migrated to when migrating to an instance.
-out-image-name	The name of the image that needs to be migrated to when migrating to an image.
-remote-ip	The IP address of the target machine, which is automatically obtained from the cloud API by default, so there is no need to specify it.
-mode	The default value is 0. 0 indicates transferring data over the public network; 2 indicates that the source can directly connect to the public network but transfers data over the private network; 3 indicates accessing the public network through an HTTP proxy and then transferring data over the private network.
-dest-subnet-id	The ID of the subnet that has connected to the private network when migrating to an image in the private network mode.

Parameter Option	Description
-dest-vpc-id	The ID of the VPC that has connected to the private network when migrating to an image in the private network mode.
-transit-image-id	The image ID of the relay instance when migrating to an image in the private network mode.
-ignore-check	Skip checks and proceed with the migration directly during the migration process.
-console	Automatically create tasks for migration, eliminating the need to manually create tasks in the console.
-no-console	Migrate without relying on the console, in which case tasks are not visible in the console.
-proxy-ip	Set the HTTP proxy IP when migrating through the private network with an HTTP proxy.
-proxy-port	Set the HTTP proxy port.
-proxy-user	Set the HTTP proxy username.
-proxy-password	Set the HTTP proxy password.
-disable-cloud-init	cloud-init is not installed on the machine after migration. Only valid for Linux migration.
-disable-cloud-init-network	Set it to disallow cloud-init to initialize the network configuration after migration. Only valid for Linux migration.
-preserve-hostname	Keep the original hostname after migration. Only valid for Linux migration.
-preserve-hosts	Keep the original hosts after migration. Only valid for Linux migration.
-preserve-dns	Keep the original DNS after migration. Only valid for Linux migration.
-preserve-mirrors	Keep the original software source after migration. Only valid for Linux migration.
-preserve-ntp	Keep the original NTP after migration. Only valid for Linux migration.
-bandwidth-limit	Set the limited bandwidth in KB/s. Only valid for Linux migration.
-incremental-time	Set the time for maintaining incremental synchronization continuously in minutes.

Parameter Option	Description
-minify	Allow migration to a target machine with less disk space, applicable for scale-in during migration.
-blocktest	Test whether block migration is possible.
-inject-virtio-skip	Skip automatic installation of Virtio drivers in Windows system.
-skip-inet-ip-checker	When migrating with the private IP address unchanged, skip the check of the private IP address.

Migration Failure Handling Guide

After the server migration operation is performed in the console, the task may fail due to some reasons. In case of task failure, you can view the error code in the Online Migration console and troubleshoot according to the following content.

Error Code	Error Description	Guide
ERROR_REMOTE_INSTANCE_STATUS_NOT_VALID	The current target instance status does not allow migration.	Only the instances in the Running and Shut Down status can be migration target instances.
ERROR_SAME_INSTANCE	The source instance and the target instance are the same, so migration is not allowed.	Change the target instance and initiate the migration task again.
ERROR_NO_IPV6	The IPV6 address of the target instance is missing.	The target instance does not have an IPv6 address. You can use an IPv4 address for migration.
ERROR_NO_PUBLIC_IP	The target instance does not have a public IP address, so the public network migration mode cannot be used.	The target instance does not have a public IP address, so the public network migration mode cannot be used. You can assign an Elastic IP to the cloud target instance, or use the private network

Error Code	Error Description	Guide
		mode for migration.
ERROR_SAME_IP	In the private network migration mode, if the private IP address of the source instance is the same as that of the target instance, a connection cannot be established.	You can migrate in the public network mode, or change the private IP address of the target instance.
ERROR_OS_NOT_MATCH	Windows and Linux instances cannot be migrated to each other.	Instances of a Windows system can only be migrated to other Windows instances. Instances of a Linux system can only be migrated to other Linux instances. You can change the target instance and migrate again.
ERROR_INSTANCE_TYPE_NOT_SUPPORTED	The instance type of the target instance cannot be the migration target for now.	Method 1: You can set the migration target to an image. After obtaining a custom image, you can then select the instance type you need and create an instance based on this custom image. Method 2: You can first migrate to another supported type (such as the standard SA5) instance. After migration, create a custom image, then select the instance type you need to create an instance based on this custom image.
ERROR_SEC_GROUP_PORT_NOT_OPEN3	The security group ports 80, 443, and	You can open your corresponding security

Error Code	Error Description	Guide
	3389 of the target instance are not open.	group ports in the Virtual Private Cloud > Security > Security Group console.
ERROR_ADD_MORE_DISK	The number of data disks for the target instance is insufficient.	You can increase the number of data disks for the target instance to meet the migration requirements.
ERROR_SYSTEM_DISK_SIZE_NOT_ENOUGH	The system disk space for the target instance is insufficient.	You can scale out the system disk to meet the migration requirements.
ERROR_ENTER_MIGRATE_MODE	The target instance failed to enter the migration mode.	You should contact customer service for assistance.
ERROR_HOST_TO_HOST_CONNECTION	The migration source cannot connect to the target instance.	You should contact customer service for assistance.
ERROR_INIT_SERVER	The initialization of the target server failed.	You should contact customer service for assistance.
ERROR_DATA_TRANSMISSION	Data transmission failed.	You should contact customer service for assistance.

Migration Time Estimation Tutorial

This document describes how to estimate the time required to migrate your system, applications, and other components from your source environment, such as an IDC or a cloud platform, to a CVM via online migration. Migration time is mainly affected by data transmission speed during migration. You can estimate the migration time by testing the transmission speed between the migration source host and the migration target host.

Migration Time Estimation in Different Scenarios

Scenario 1

For Linux system migrating to a CVM, the migration time depends on the actual data transmission time.
For Windows system migrating to a CVM, the migration time depends on the time required for transferring the total disk capacity.
For example, if the actual usage of all disk data on the source host of your Linux system to be migrated is 50 GB and the outbound bandwidth is 100 Mbps, the estimated total migration time is 1.14 hours. The steps are as follows:

1. Unit conversion:
    - Convert the actual broadband speed to MB/s: 100 Mbps = 100 / 8 = 12.5 MB/s.
    - Convert the actual disk data volume to MB: 50 GB = 50 x 1024 = 51200 MB.
2. Actual data migration time estimation:
   51200 / 12.5 = 4096 seconds = 1.14 hours.

Scenario 2

For Linux system migrating to a CVM, the migration time depends on the actual data transmission time and the image creation time.
For Windows system migrating to a CVM, the migration time depends on the time required for transferring the total disk capacity and the image creation time.
For example, if the capacity of the disk on the source host of your Windows system to be migrated is 50 GB and the outbound bandwidth is 100 Mbps, the estimated total migration time is 1.23 hours. The steps are as follows:

1. Unit conversion:
    - Convert the actual broadband speed to MB/s: 100 Mbps = 100 / 8 = 12.5 MB/s.
    - Convert the actual disk data volume to MB: 50 GB = 50 x 1024 = 51200 MB.
2. Actual data migration time estimation:
   51200 / 12.5 = 4096 seconds = 1.14 hours.
3. Image creation time, with a creation speed of about 160 MB/s:
   51200 / 160 = 320 seconds = 0.089 hours.
4. Total migration time:
   1.14 + 0.089 = 1.23 hours.

Relevant Operation: Testing the Data Transmission Speed

You can use the iperf3 tool to test the data transmission speed, such as the bandwidth and rate of data transmission from the client to the server.

Factors Affecting the Transmission Speed

- The outbound bandwidth of the source host and the inbound bandwidth of the target instance.
  For example, if the outbound bandwidth of the source host is 50 Mbps and the inbound bandwidth of the target instance is 100 Mbps, then theoretically the actual transmission speed will not exceed 50 Mbps.
- During migration, the bandwidth will not always be fully utilized, and the inbound bandwidth of the target instance (or relay instance) can be dynamically adjusted.
- If the source host and the target instance are in different regions, their transmission speed will be slower than that in the same region.

  > Note:

- When you perform online migration through the console, if the migration target is a CVM image, a relay instance (named do_not_delete_csm_instance) will be created during the migration, with a maximum bandwidth of 50 Mbps.
- You can dynamically adjust the inbound bandwidth of the target instance (or the relay instance) in the console during migration to control the migration speed.

Speed Test for Migration to Cloud Platform Linux CVM

For example, by using the online migration feature through the console, migrate a server to a cloud platform CentOS 7.5 instance. The steps for testing the transmission speed are as follows:

1. Create a pay-as-you-go CentOS 7.5 instance in the migration target region.

   > Note:

   - If the migration target is a CVM image, a CentOS 7.5 relay instance will be created during the migration. If you need to test the migration speed, it is recommended to select an available standard instance with lower CPU and memory configurations, which would make the scenario closer to the actual migration situation.
   - The default iperf3 service-side port is TCP 5201. Therefore, you need to add and allow TCP 5201 port in the security group's inbound direction for the CentOS 7.5 instance to be tested.

2. Install the iperf3 tool on both the target test instance and the source host.

   - Execute the following command to install the iperf3 tool on the target CentOS 7.5 instance.

```
yum -y install iperf3
```

- Install the iperf3 tool on the source host. You should use the corresponding installation command according to the Linux distribution of the source host to install the iperf3 tool.

3. Execute the following command to start the iperf3 server side on the target CentOS 7.5 test instance.

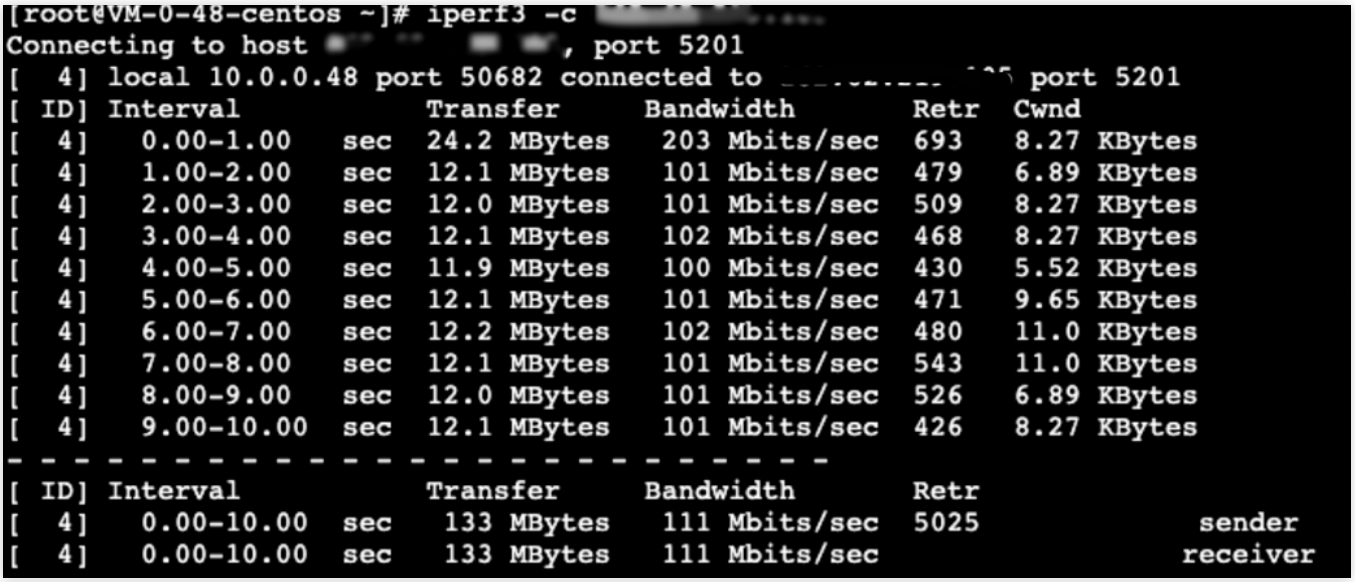
```
iperf3 -s
```

If the information "Server listening on 5201" is returned, it indicates that the startup was successful.

4. Execute the following command to start iperf3 in client mode on the source host.

```
iperf3 -c [Target instance IP address]
```

The test result is shown in the figure below, from which we can see that the transmission speed between the source host and the test CentOS 7.5 instance is about 111 Mbps.



Network
Elastic Public IP

Scenarios

Elastic public IP address, also known as an Elastic IP (EIP), is a regional static IP address designed for dynamic cloud computing. With EIP, you can quickly map an address to another instance (or NAT gateway instance) in your account for failure isolation. This document describes how to use an EIP.

Prerequisites

Log in to the CVM console.

Operation Steps

Applying for an EIP

1. In the left sidebar, click EIP.
2. On the EIP management page, click Apply.
3. In the pop-up Apply for EIP window, select the region, set the billing mode and bandwidth limit, enter the quantity, and click Confirm to complete the application for the EIP.
   After the application is completed, you can see the EIP you applied for in the list, which is currently in an unbound status.

Binding an EIP to a Cloud Service

1. In the left sidebar, click EIP.

2. On the EIP management page, select the EIP to which you want to bind a cloud service and click More > Bind.

   > Note:
   > If the EIP is already associated with another instance, unbind it first.

3. In the pop-up Bind Resource window, select the cloud resource to which the EIP is to be bound and

click OK.

4. In the pop-up Bind EIP dialog box, click OK to complete the binding with the Cloud Services.

Unbinding an EIP from a Cloud Service

1. In the left sidebar, click EIP.
2. On the EIP management page, select the EIP from which you want to unbind a cloud service and click Unbind.
3. In the pop-up Unbind EIP window, confirm the unbinding information and click Confirm.

> Note:
> After unbinding, the cloud product instance may be assigned a new public IP address, which may differ from the one assigned before binding.

Releasing an EIP

1. In the left sidebar, click EIP.
2. On the EIP management page, select the EIP for which the cloud service needs to be released and click More > Release.
3. In the pop-up window, click Confirm.
4. In the confirmation window, click Confirm.

Adjusting the Bandwidth

1. In the left sidebar, click EIP.
2. On the EIP management page, select the EIP whose bandwidth needs to be adjusted and click Adjust bandwidth.
3. In the pop-up Adjust Bandwidth window, set the target bandwidth value and click Confirm to complete the bandwidth adjustment.

Exceptions Troubleshooting

EIPs may experience network disconnection, which is generally caused by the following reasons:

- EIPs are not bound to cloud services. For specific binding methods, see Binding an EIP to a Cloud Service.
- The security policy is not taking effect. Check whether any effective security policies (such as security groups or network ACLs) are in place. If the bound cloud product instance has a security policy that, for example, blocks access to port 8080, then the EIP's port 8080 will also be inaccessible.

Elastic Network Interface

If the CVM needs to use an Elastic Network Interface, please refer to the following configuration steps to complete the corresponding content. For specific operations, see Elastic Network Interface.

1. Create an Elastic Network Interface.
2. (Important) Bind and configure the Elastic Network Interface to the CVM.
3. Configure the CVM and Virtual Private Cloud route table.
4. Allocate private IP addresses.
   i. Log in to the VPC console.
   ii. Click IP and Network Interface > ENI in the left sidebar to open the ENI list page.
   iii. Click the ID/Name of the Elastic Network Interface, go to the Elastic Network Interface details page to view the Elastic Network Interface information.
   iv. Click IPv4 Address Management to enter the details page.
   v. Click Assign private IP address, select the IP allocation method.
   vi. Automatically assign or manually fill in. If you choose to fill in manually, you need to enter the appropriate private IP address and click OK.
5. Managing the Elastic Network Interface.
   - Releasing the private IP address
   - Unbinding from the CVM
   - Deleting an ENI
   - Binding an Elastic IP
   - Unbinding the Elastic IP
   - Modifying the primary private IP address
   - Modifying the subnet to which the Elastic Network Interface belongs

EIP Direct Access

Scenarios

When users access the public network through EIP, they can choose NAT mode or EIP direct access mode. The current default mode is NAT mode.

- EIP is not visible locally in NAT mode.
- After EIP direct access, the EIP is visible locally. There is no need to manually add the EIP address each time when configuring, which can reduce the development costs.

> Note:
> EIP direct connection is currently allowlist-controlled and only supports devices within the VPC.

Operation Steps

Step 1: Download the EIP Configuration Script

Since the EIP direct access process will cause network interruption, you need to download the EIP direct access script and upload it to CVM. Proceed as follows:

1. Download the EIP direct access Configure script. This step is optional. > Note:
   The Linux script supports CentOS 6.x, CentOS 7, and Ubuntu.

2. After downloading the script locally, upload it to the Cloud Virtual Machine that requires EIP direct access.

Step 2: Run the EIP Direct Access Script

1. Log in to the CVM server that requires EIP direct access.

2. Run the EIP direct access script. Specific method:
   - Under Linux operating system CentOS:

```
eip_linux.sh install XX.XX.XX.XX
```

Among them, XX.XX.XX.XX is the EIP address, which is optional.

- Under Windows operating system:

```
eip_windows.bat XX.XX.XX.XX
```

Among them, XX.XX.XX.XX is the EIP address.

Step 3: Enable EIP Direct Access

1. Log in to the CVM console.
2. In the left sidebar, click EIP.
3. In the selection list, click EIP Direct Connect to enable.

> Note:

- The script only supports eth0 and does not support auxiliary network interfaces yet.
- The NAT gateway can be bound to an EIP that enables direct access mode, but there is no direct access effect.

Configuring IPv6 address

Overview

This document guides you to build a CVM with IPv6 CIDR and enable IPv6 for the Elastic Network Interface to achieve IPv6 intranet and extranet communication.

> Note:
> Currently, Elastic IPv6 is in internal testing. If you have any needs, please submit an application.

Operation Notes

1. Before starting to use Converge Cloud products, you need to register a Converge Cloud account first.
2. The IPv6 address is a GUA address. Each VPC is allocated with one `/56` IPv6 CIDR. Each subnet is allocated with one `/64` IPv6 CIDR. Each ENI is allocated with one IPv6 address.
3. Both the primary network interface and the secondary network interface support applying for IPv6 addresses. For more information about the relationship between CVM and ENI, see Elastic Network Interface product documentation.

Directions

> Note:
> Since IPv6 is in a public beta, IPv6 addresses are not configured for CVM instances by default. If your CVM needs to enable the IPv6 function, please manually configure it first. For details, please refer to Quickly build an IPv6 Virtual Private Cloud.

Step 1: Purchase CVMs(optional)

> Note:
> If you have already purchased a CVM, you can skip this step.

1. Log in to the CVM purchase page.

2. When selecting a model, select a region and network that supports IPv6.

3. When setting up the host, select a security group that supports IPv6 and check Assign IPv6 addresses for free.

> Note:
> If the network or security group you selected does not support IPv6, please refer to Quickly build an IPv6 Virtual Private Cloud to create a Virtual Private Cloud and security group that meet your needs.

4. Check the purchased CVM information and complete the payment.

Step 2: Configuring IPv6 address for CVM

For details, see Virtual Private Cloud Quick Start Documentation.

Security
Security Group
Overview

A security group is a virtual firewall used to set network access controls for instances such as cloud servers, load balancers, and cloud databases. It controls inbound and outbound traffic at the instance level and is an important means of network security isolation.
You can configure security group rules to allow or deny inbound and outbound traffic for instances within the security group.

Security group features

- A security group is a logical grouping where you can add instances such as cloud servers, elastic network interfaces, and cloud databases that have the same network security isolation requirements within the same region.
- Instances associated with the same security group do not communicate by default, and you need to add corresponding allow rules.
- Security groups are stateful; for inbound traffic that you have allowed, outbound traffic is automatically allowed, and vice versa.
- You can modify security group rules at any time, and new rules take effect immediately.

Security group rules

Components

Security group rules include the following components:

- Source: the source data (inbound) or destination data (outbound) IP.
- Protocol type and protocol port: Protocol types such as TCP, UDP, HTTP, etc.
- Policy: Allow or deny.

Rule Priority

- Rules within a security group have priorities. Rule priority is represented by the position of the rule in the list, with the highest priority rule at the top of the list and the lowest at the bottom.
- If there is a rule conflict, the rule with the higher priority will prevail by default.
- When traffic enters/exits an instance bind to a security group, it matches rules from the top to the

bottom of the security group rule list. If a rule is successfully matched and allowed to pass, the subsequent rules will not be matched.

Multiple Security Groups

An instance can be bind to one or more security groups. When an instance is bind to multiple security groups, the rules of multiple security groups are executed sequentially from top to bottom, and you can adjust the priority of security groups at any time.

Security Group Template

When creating a new security group, you can choose from two security group templates provided by Converge Cloud:

- Allow all port templates: All inbound and outbound traffic will be allowed.
- Allow Common Ports Template: TCP port 22 (Linux SSH login), ports 80 and 443 (Web services), port 3389 (Windows remote log in), ICMP protocol (Ping), and internal network traffic will be allowed.

  > Note:

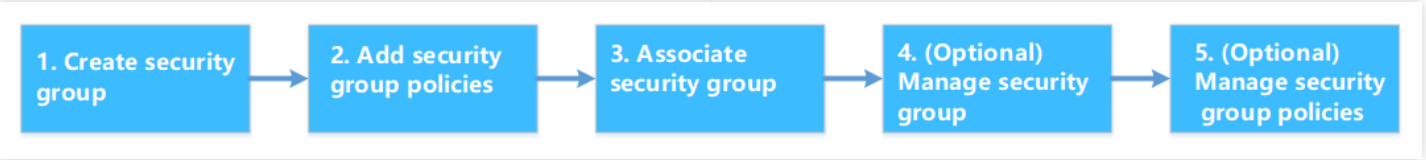
- If the provided security group templates do not meet your actual needs, you can also create a custom security group. For details, please refer to Creating Security Groups and Security Group Use Cases.
- If you have security protection requirements at the application layer (HTTP/HTTPS), you can separately purchase Web Application Firewall (WAF). WAF provides application layer web security protection against web vulnerability attacks, malicious crawlers, and CC attacks, safeguarding websites and web applications.

Use Limits

For the usage restrictions and quotas of security groups, please see the security group-related restrictions chapter in Use Limits Overview.

Process Flow

The usage process for security groups is illustrated in the following diagram:


1. Create security group
2. Add security group policies
3. Associate security group
4. (Optional) Manage security group
5. (Optional) Manage security group policies

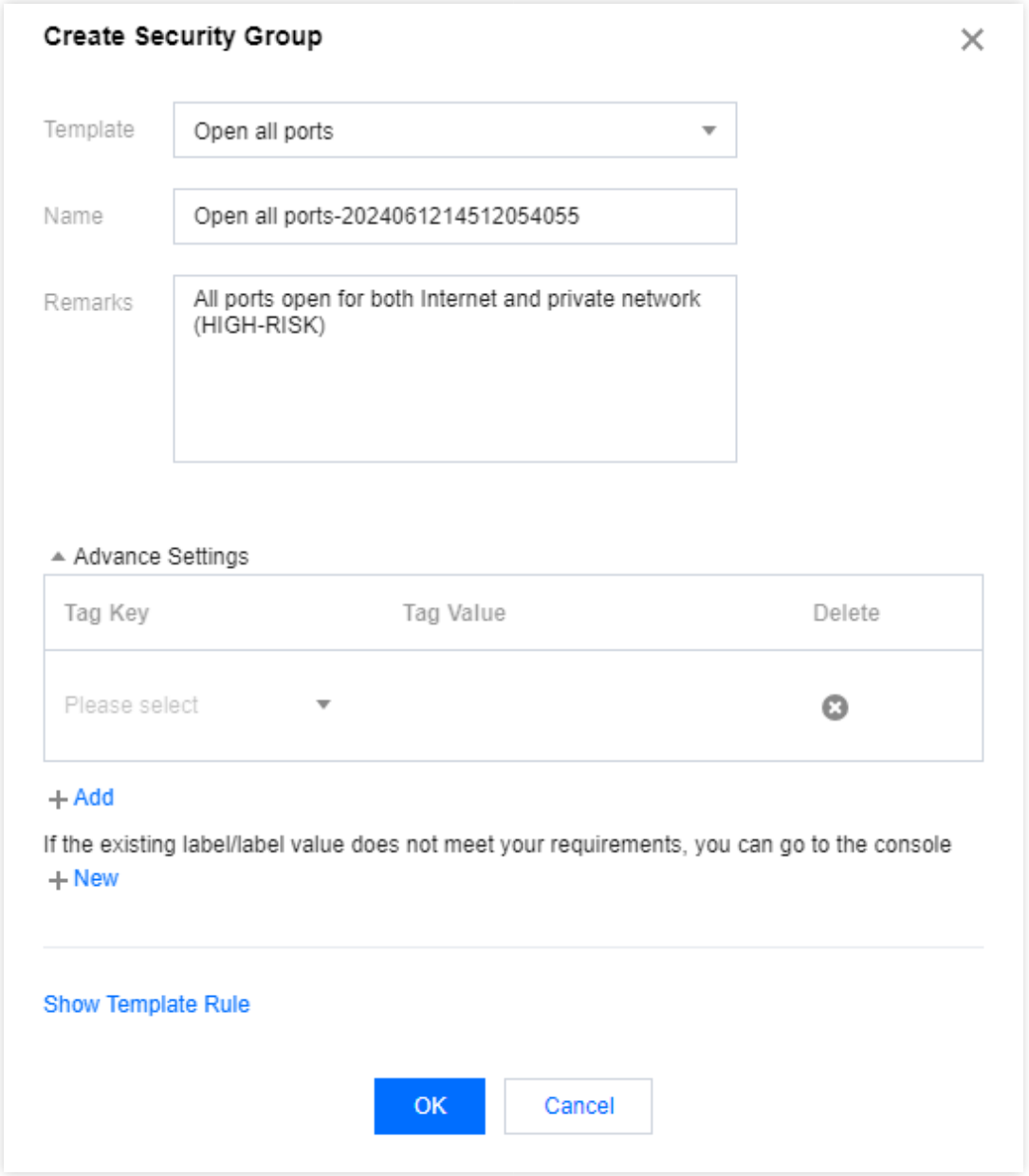
Creating Security Group

Overview

Security groups are the virtual firewalls of Cloud Virtual Machine instances, and each Cloud Virtual Machine instance must belong to at least one security group. When you create a CVM instance, if you have not created a security group yet, we provide two templates: Open All Ports and Open Ports 22, 80, 443, 3389 and ICMP Protocol to create a default security group. For more details, see Security Group Overview.
If you do not want Cloud Virtual Machine instances to be added to the default security group, you can also create your own security groups as described in this document. This document introduces to create a security group on the Cloud Virtual Machine console.

Directions

1. Log in to the CVM console.
2. In the left sidebar, click Security Group to enter the Security Group Management page.
3. On the Security Group Management page, select Region and click Create.
4. In the pop-up Create Security Group window, complete the following configuration.



- Template: based on the services to be deployed for the Cloud Virtual Machine instances in the security group, select an appropriate template to simplify security group rule configuration. As shown below:

Templates	Description	Scenario
Open All Ports	All ports are opened to the public network and private network by default, which has certain security risks.	-
Open Ports 22, 80, 443 and 3389 and ICMP Protocol.	By default, ports 22, 80, 443, 3389 and the ICMP protocol are opened. The private network is fully opened.	Instances in the security group need to be deployed with Web services.

Templates	Description	Scenario
Custom	After the security group is successfully created, add the security group rules as required. For detailed operations, see Add Security Group Rules.	-

- Name: customize the security group name.
- Notes: Custom, and a short description of the security group for easier management.
- Advanced settings: Customize, select tags for this security group as needed.

5. Click OK to complete the creation of the security group.
   If you selected the Custom template when creating a new security group, you can click Set Rules Now to Add Security Group Rules.

Adding Security Group Rule

Overview

Security groups are used to manage whether access requests from the public network or private network are allowed. For security reasons, the inbound direction of security groups often adopts a deny access policy. If you select Open All Ports template or Open 22, 80, 443, 3389 Ports and ICMP Protocol template when creating a security group, the system will automatically add security group rules for some communication ports based on the selected template type. For details, see Product Overview.
This document describes how to add security group rules to allow or forbid Cloud Virtual Machine instances in the security group to access the public network or private network.

Notes

- Security group rules support IPv4 security group rules and IPv6 security group rules.
- Open all ports already includes IPv4 and IPv6 security group rules.

Prerequisites

- You have created a security group. For detailed operations, see Create Security Group.
- You already know which public network or private network access requests need to be allowed or denied for the Cloud Virtual Machine instance. For more use cases of security group rule settings, see Security Group Use Cases.

Directions

1. Log in to the CVM console.

2. In the left sidebar, click Security Group to enter the Security Group Management page.

3. On the Security Group Management page, select Region and find the security group whose rules need to be set.

4. In the row of the security group where rules need to be set, click Modify Rules in the Operation column.

5. On the Security Group Rules page, click Inbound Rules and select any of the following methods to complete the operation according to actual needs. > Note: The following operation uses Method 2: adding rules as an example.
    - Method 1: open all ports, is applicable to scenarios where ICMP protocol rules do not need to be set and operations can be completed through ports 22, 3389, ICMP, 80, 443, 20, 21.
    - Method 2: adding a rule, is applicable to scenarios where multiple communication protocols need to be set, such as the ICMP protocol.

6. In the pop-up Add Inbound Rules window, set the rules.
   The main parameters for adding a rule are as follows:
    - Type: the default value is Custom. You can also select other system rule templates, such as Windows log-in, Linux log-in, Ping, HTTP(80), or HTTPS(443).
    - Source: the source (inbound rule) or destination (outbound rule) of traffic, specify one of the following options:

Specified Source/Destination	Description
Single IPv4 address or IPv4 address range	In CIDR notation, such as 203.0.113.0, 203.0.113.0/24 or 0.0.0.0/0, where 0.0.0.0/0 indicates all IPv4 addresses will be matched.
Single IPv6 address or IPv6 address range	In CIDR notation, such as FF05::B5, FF05:B5::/60, ::/0 or 0::0/0, where ::/0 or 0::0/0 indicates all IPv6 addresses will be matched.
Refer to the security group ID. You can reference the ID of following security groups: - Security group ID - other security group	- The current security group indicates the CVM associated with the security group. - The other security group represents another security group ID under the same item in the same area.
Reference an IP address object or IP address group object in the Parameter Template.	

- Protocol Port: Enter the protocol type and port range or you can also reference the protocol port or protocol port group in the Parameter Template.
- Policy: the default value is Allow.
    - Allow: Access requests of this port are allowed.
    - Reject: Data packets will be discarded without any response.
- Notes: Custom, and a short description of the rule for easier management.

7. Click Finish to complete adding the security group inbound rule.
8. On the Security Group Rule page, click Outbound Rules and refer to step 5 - step 7 to complete adding the security group outbound rule.

Associating Instance with Security Group

> Note:
> Security groups support association with CVM, Elastic Network Interface, CloudDB for MySQL, and Cloud Load Balancer. This document takes association with CVM as an example.

Overview

Security groups are used to set the network access control for single or multiple Cloud Virtual Machine instances, which is an important means of network security isolation. You can associate Cloud Virtual Machine instances with one or more security groups based on business needs. Here's how to associate a Cloud Virtual Machine instance with a security group in the console.

Prerequisites

A Cloud Virtual Machine instance has been created.

Directions

1. Log in to the CVM console.
2. Click Security Group in the left sidebar to enter the security group management page.
3. On the Security Group Management page, select Region and find the security group whose rules need to be set.
4. In the row of the security group whose rules need to be set, click Manage Instances in the Action column to enter the Associate Instance page.
5. On the Associated Instance Page, click Add Association.
6. In the pop-up Add Instance Association window, select the instances you want to bind to the security group, and click OK.

Subsequent Operations

- If you want to view all the security groups you have created in a certain region, you can query the Security Group List.
  For detailed operations, see View Security Groups.

- If you do not want your Cloud Virtual Machine instance to belong to one or more security groups, you can remove the Cloud Virtual Machine instance from the security group.
  For detailed operations, see Remove from Security Group.
- If your business no longer requires one or more security groups, you can delete the security group. After deletion, all rules within the security group will be deleted simultaneously.
  For detailed operations, see Delete Security Group.

Managing Security Group
Viewing Security Group

Overview

If you want to view all the security groups you have created in a certain region, you can view the security groups list by doing the following.

Directions

View all security groups

1. Log in to the CVM console.
2. Click Security Group in the left sidebar to enter the security group management page.
3. On the Security Group Management page, select Region to view all security groups under this region.

View specified security groups

You can also view the security groups you want to view through the search feature on the Security Groups Management page.

1. Log in to the CVM console.
2. Click Security Group in the left sidebar to enter the security group management page.
3. Select Region on the security group management page.
4. In the upper right corner of the security group list in the region, enter the security group's name or security group's ID in the search text box, click , the search results are displayed in the security group list.

Removing from Security Group

Overview

You can remove Cloud Virtual Machine instances from the security group based on your business needs.

Prerequisites

The Cloud Virtual Machine instance has joined two or more security groups.

Directions

1. Log in to the CVM console.
2. Click Security Group in the left sidebar to enter the security group management page.
3. Select Region on the security group management page and find the security groups whose instances need to be removed.
4. Click Associate Instance in the operation column of the security group to enter the Associate Instance page.
5. On the Associated Instance page, select the instance to be removed and click Remove from Security Group.
6. In the pop-up dialog Box, click OK.

Clone Security Group

Overview

You may need to clone a security group in the following scenarios:

- Assume that you have created a security group sg-A in region A and need to use the exact same rules as those for instances in region B. In this case, you can directly clone sg-A into region B instead of creating security groups from scratch in region B.
- If your business needs to execute a new security group rule, you can clone the original security group for backup.

Notes

- By default, only the inbound/outbound rules of this security group are cloned, but not the instances associated with the security group.
- The cloned security group supports cross-region.

Directions

1. Log in to the CVM console.
2. Click Security Group in the left sidebar to enter the security group management page.
3. Select Region on the security group management page and find the security groups to be cloned.
4. In the row of the security group to be cloned, click More > Clone in the Action column.
5. In the pop-up Clone Security Group window, select Target Region for the clone, enter the New Name of security group, and click OK.

Deleting Security Group

Overview

If your business has no longer required one or more security groups, you can delete the security group. After deletion, all rules within the security group are deleted simultaneously.

Prerequisites

Make sure that the security group to be deleted has no associated instances. If there are associated instances, remove those instances from the security group first; otherwise, the operation to delete the security group cannot be executed. For detailed operations, see Remove from Security Group.

Directions

1. Log in to the CVM console.
2. Click Security Group in the left sidebar to enter the security group management page.
3. Select Region on the security group management page and find the security groups to be deleted.
4. In the row of the security group to be deleted, click More > Delete in the Action column.
5. In the pop-up dialog Box, click OK.

Adjust the Priority of Security Groups

Overview

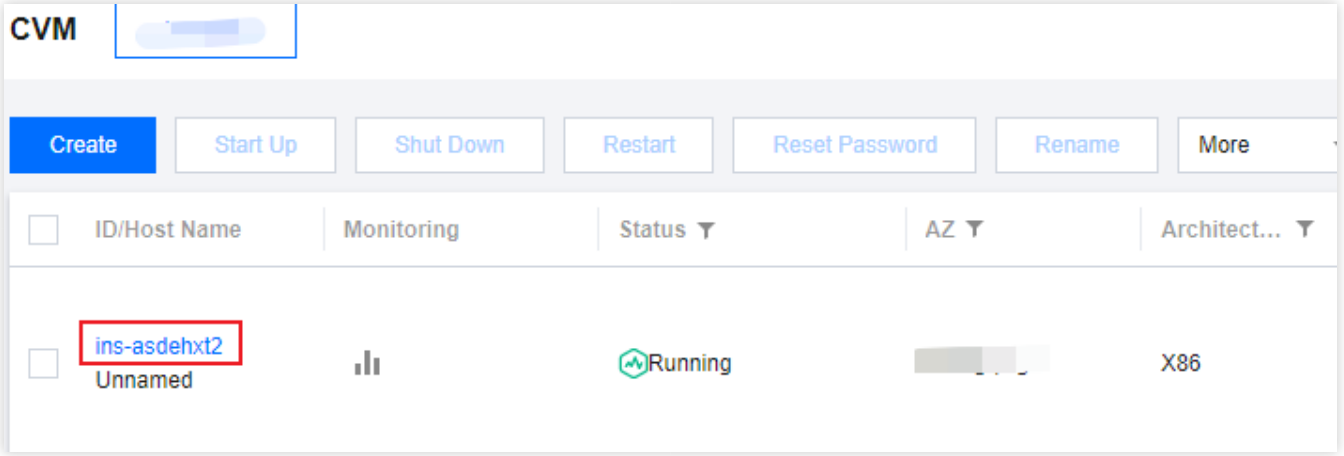
When a CVM is bound to multiple security groups, you can sort the security groups to determine the order in which they are executed.

Prerequisites

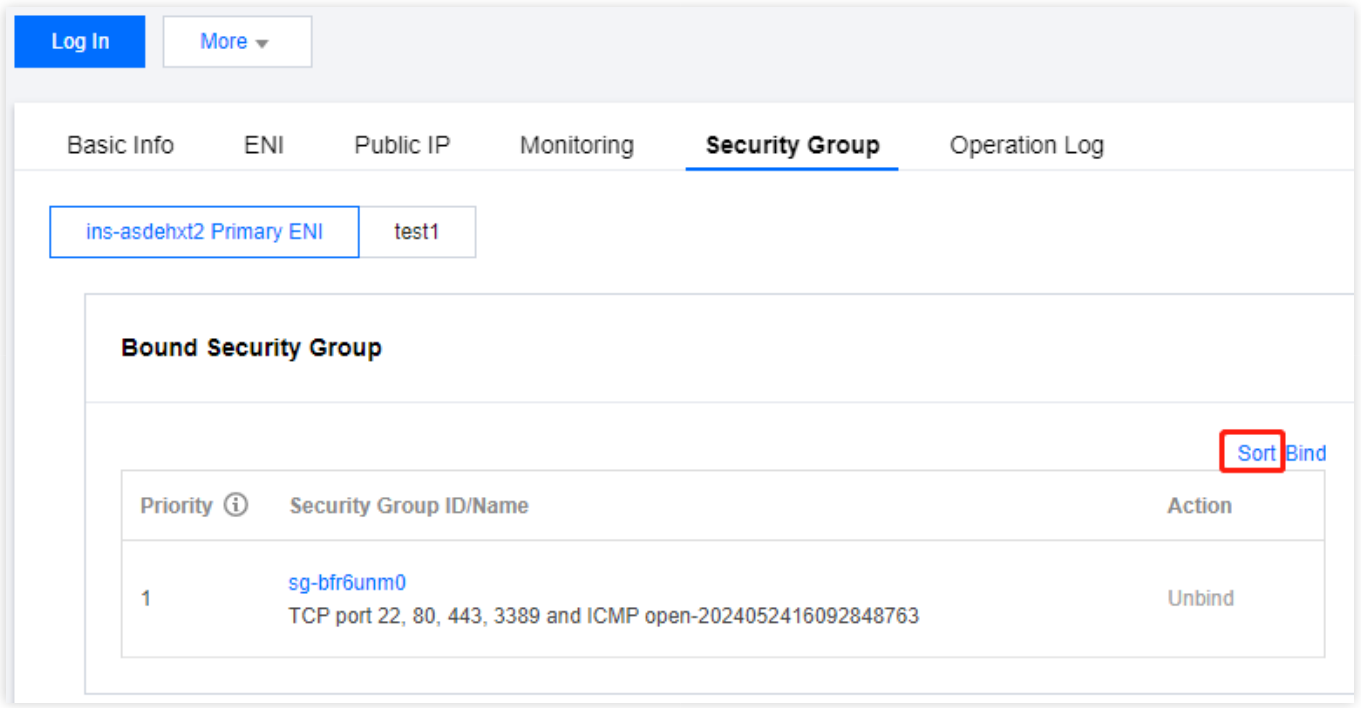
There are two or more security groups bound to the CVM.

Directions

1. Log in to the CVM console.
2. Select CVM List in the left sidebar.
3. On the CVM list page, click the instance ID for which you want to adjust the security group priority to go to the instance details page.



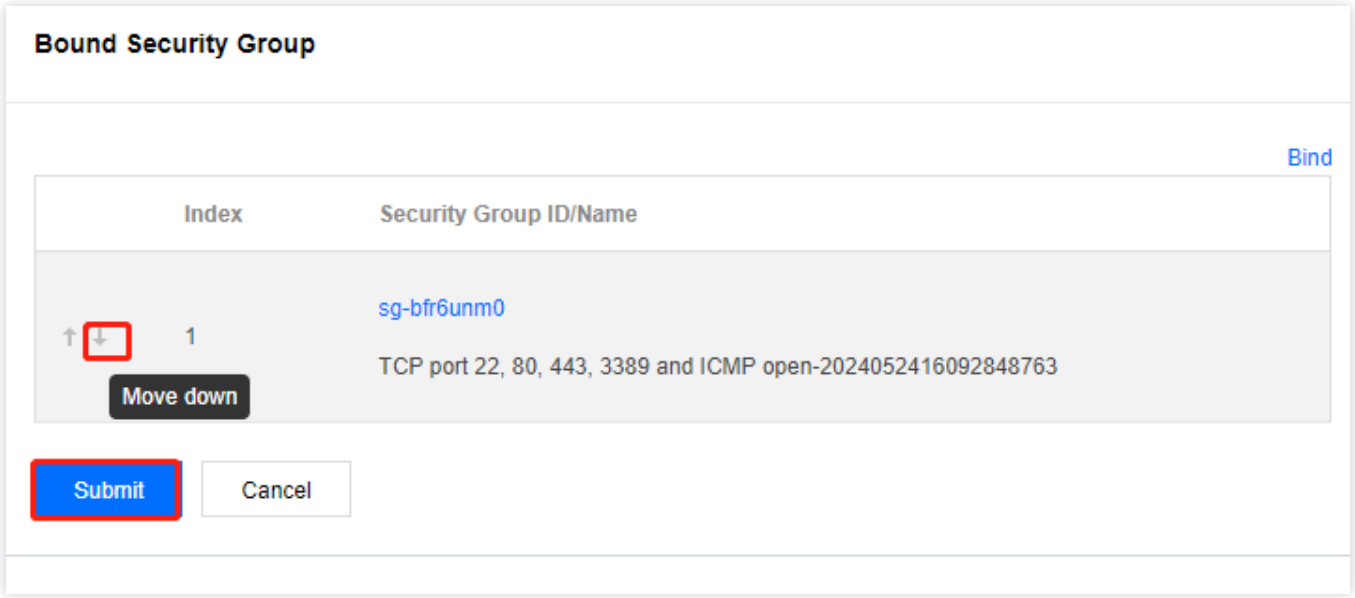
4. Select Security Group on the instance details page. Click Sort in the bound security group on the security group page to enable sorting.



5. Click Move Up or Move Down to adjust the order of the security groups.

> Note:
> The priority order of security groups is 1, 2, and 3.

6. After completing the adjustment, click Submit to save the configuration.



Managing Security Group Rule
Viewing Security Group Rules

Overview

After adding a security group rule, you can view the details of the security group rule in the console.

Prerequisites

A security group has been created and security group rules have been added to it.
For information on how to create a security group and add security group rules, see Create a Security Group and Add Security Group Rules.

Directions

1. Log in to the CVM console.
2. Click Security Group in the left sidebar to enter the security group management page.
3. Select Region on the security group management page and find the security groups whose rules need to be viewed.
4. Click the security group ID/name of the rule to be viewed to enter the Security Group Rules page.
5. Click the Inbound Rules or Outbound Rules tab on the security group rules page to view the inbound/outbound security group rules.

Modifying Security Group Rule

Overview

Improper security group rules (for example, those that do not restrict access to specified ports) can incur severe security risks. In this case, you can modify these unreasonable security group rules in a security group to ensure the network security of CVM instances. This document describes how to modify security group rules.

Prerequisites

A security group has been created and security group rules have been added to it.
For information on how to create a security group and add security group rules, see Create a Security Group and Add Security Group Rules.

Directions

1. Log in to the CVM console.
2. Click Security Group in the left sidebar to enter the security group management page.
3. Select Region on the security group management page and find the security groups whose rules need to be modified.
4. In the row of the security group whose rules need to be modified, click Modify Rule in the operation column to enter the Security Group Rule page.
5. On the Security Group Rules page, depending on the direction of the rules to be modified (Inbound/Outbound), click the Inbound Rules or Outbound Rules tab.
6. Find the security group rule to be modified, and click Modify in the Action column to modify the existing rules.

Deleting Security Group Rule

Overview

If you no longer need a security group rule, you can delete it.

Prerequisites

- A security group has been created and security group rules have been added to it.
  For information on how to create a security group and add security group rules, see Create a Security Group and Add Security Group Rules.
- It is confirmed that the CVM instance does not need to permit/forbid public network access or private network access.

Directions

1. Log in to the CVM console.
2. Click Security Group in the left sidebar to enter the security group management page.
3. Select Region on the security group management page and find the security groups whose rules need to be deleted.
4. In the row of the security group whose rules need to be deleted, click Modify Rule in the operation column to enter the Security Group Rules page.
5. On the Security Group Rules page, depending on the direction of the rules to be deleted (Inbound/ Outbound), click the Inbound Rules or Outbound Rules tab.
6. Find the security group rule that needs to be deleted and click Delete in the operation column.
7. In the pop-up dialog Box, click OK.

Importing Security Group Rule

Overview

Security group rules can be imported. You can import the exported security group rule file into a security group to quickly create or recover security group rules.

Directions

1. Log in to the CVM console.
2. Click Security Group in the left sidebar to enter the security group management page.
3. Select Region on the security group management page and find the security groups whose rules need to be imported.
4. Click the security group ID/name of the rule to be imported to enter the Security Group Rules page.
5. On the Security Group Rules page, depending on the direction of the rules to be imported (Inbound/Outbound), click the Inbound Rules or Outbound Rules tab.
6. Click Import Rule under the Inbound/Outbound Rules tab.
7. In the pop-up Batch Import - Inbound/Outbound Rules window, select the edited template file for inbound/outbound rules, and click Start Importing.
   Note:
   - If there are security group rules under the security groups that need to be imported, it is recommended that you export the existing rules first. Otherwise, when importing new rules, the original rules will be overwritten.
   - If there is no security group rule under the security group that needs to import rules, it is recommended that you download the template first and then import the file after editing the template file.

Exporting Security Group Rule

Overview

Security group rules can be exported. You can export the security group rules of a security groups for local backup.

Directions

1. Log in to the CVM console.
2. Click Security Group in the left sidebar to enter the security group management page.
3. Select Region on the security group management page and find the security groups whose rules need to be exported.
4. Click the security group ID/name of the rule to be exported to enter the Security Group Rules page.
5. On the Security Group Rules page, depending on the direction of the rules to be exported (Inbound/ Outbound), click the Inbound Rules or Outbound Rules tab.
6. Under the Inbound/Outbound Rules tab, click the Download Inbound Rules or Outbound Rules icon at the top right to download and save the security group rule file to your local device.

Adjusting the Priority of Security Groups Rules

Overview

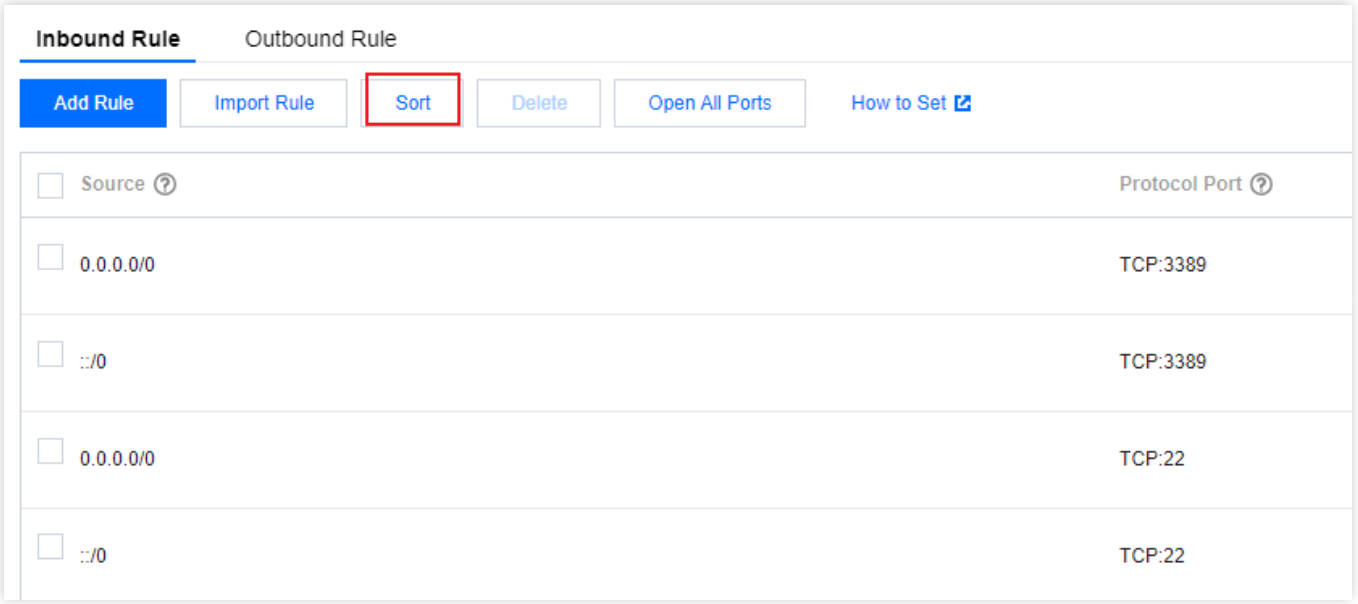
Rules within a security group have priorities. Rule priority is represented by the position of the rule in the list, with the highest priority rule at the top of the list.
When a security group has multiple rules and you need to adjust the priority of the rules to take effect, you can adjust them through the following steps.

Prerequisites

Multiple inbound or outbound rules are added to the security group.

Directions

1. Log in to the CVM console.
2. Click Security Group in the left sidebar to enter the security group list page.
3. Select the security group ID whose rule priority needs to be adjusted and enter the details page.
4. On the details page, select Security Group Rules > Inbound Rule/Outbound Rule, and click Sort to enter the sortable state.



5. Click Move Up or Move Down to adjust the order of the rules.
6. After completing the adjustment, click Submit to save the configuration.

Security Group Use Cases

Security group settings are used to manage whether the Cloud Virtual Machine can be accessed. You can configure the inbound and outbound rules of the security group to set whether your server can be accessed and can access other network resources.
By default, the inbound and outbound rules for security groups are as follows:

- To ensure the data security, the input rules for security groups are set to a denial policy, prohibiting remote access from external networks. If you need your Cloud Virtual Machine to be accessible from the outside, you need to open the appropriate ports for inbound rules.
- The outbound rules for security groups are used to determine whether your Cloud Virtual Machine can access external network resources. If you select Open All Ports or Open 22, 80, 443, 3389 Ports and ICMP Protocol, the outbound rules for the security groups are fully open. If you opt for custom security group rules, the default outbound rule is to deny all, requiring you to open the relevant ports for outbound rules to access external network resources.

Common Use Cases

This document describes several common use cases for security groups. If any of the following scenarios meet your requirements, you can set your security groups according to the configuration recommended for the corresponding use case.

Scenario 1: remotely connecting to a Linux CVM through SSH

Example: You have created a Linux Cloud Virtual Machine and want to remotely connect to it through SSH.
Solution : When adding the security group rules, select Linux Log-in in the Type, open protocol port 22, allowing Linux SSH log-in.
You can also open all IPs or specified IPs (IP range) according to actual needs, and configure the IP source that can remotely connect to the Cloud Virtual Machine through SSH.

Direction	Type	Source	Protocol Port	Policies
Inbound Direction	Linux login	All IP addresses: 0.0.0.0/0 Specifying IP: Enter the IP or IP range you specify	TCP:22	Allow

Scenario 2: remotely connecting to a Windows CVM through RDP

Example: You have created a Windows Cloud Virtual Machine and want to remotely connect to it through RDP.

Solution: When adding the security group rules, select Windows Log-in in the Type, open protocol port 3389, allowing Windows remote log-in.
You can also open all IPs or specified IPs (IP range) according to actual needs, and configure the IP source that can remotely connect to the Cloud Virtual Machine through SSH.

Direction	Type	Source	Protocol Port	Policies
Inbound Direction	Windows login	- All IP addresses: 0.0.0.0/0 - Specifying IP: Enter the IP or IP range you specify	TCP:3389	Allow

Scenario 3: pinging a CVM from the public network

Example: You have created a Cloud Virtual Machine and wish to test if the communication between this CVM and other CVMs is functioning correctly.
Solution: use the ping program for testing. That is, when adding security group rules, select Ping as the Type, open the ICMP protocol port, allowing other CVMs to access the CVM via ICMP protocol.
You can also open all IPs or specified IPs (IP range) according to actual needs, configuring the IP source allowed to access this Cloud Virtual Machine via ICMP protocol.

Direction	Type	Source	Protocol Port	Policies
Inbound Direction	Ping	All IP addresses: 0.0.0.0/0 Specifying IP: Enter the IP or IP address range you specify	ICMP	Allow

Scenario 4: Telnet remote log-in

Example: You wish to remotely log in to your Cloud Virtual Machine through Telnet.
Solution: If you need to remotely log in to the CVM through Telnet, configure the following security group rules when adding security group rules:

Direction	Type	Source	Protocol Port	Policies
Inbound Direction	Custom	All IP addresses: 0.0.0.0/0 Specifying IP: Enter the IP or IP address range you specify	TCP:23	Allow

Scenario 5: allowing Web Service HTTP or HTTPS Access

Example: You have set up a website and want users to access it via HTTP or HTTPS.

Solution: To allow website access via HTTP or HTTPS, you need to add security group rules based on your needs, configuring the following security group rules:

- Allow all IPs on the public network to access the website

Direction	Type	Source	Protocol Port	Policies
Inbound Direction	HTTP(80)	0.0.0.0/0	TCP:80	Allow
Inbound Direction	HTTPS(443)	0.0.0.0/0	TCP:443	Allow

- Allow some IPs on the public network to access the website

Direction	Type	Source	Protocol Port	Policies
Inbound Direction	HTTP(80)	IPs or IP address ranges allowed to access your website	TCP:80	Allow
Inbound Direction	HTTPS(443)	IPs or IP address ranges allowed to access your website	TCP:443	Allow

Scenario 6: allowing external IPs to access the specified port

Example: After deploying your service, you want a specific business port (e.g., 1101) to be accessible from outside.
Solution: When adding security group rules, select Custom in Type and open protocol port 1101, allowing external access to the specified business port.
You can also open all IPs or specified IPs (IP range) according to actual needs, allowing access from IPs to the specified business port.

Direction	Type	Source	Protocol Port	Policies
Inbound Direction	Custom	All IP addresses: 0.0.0.0/0 Specifying IP: Enter the IP or IP address range you specify	TCP:1101	Allow

Scenario 7: denying external IPs to access the specified port

Example: After deploying your service, you want a specific business port (e.g., 1102) not to be accessible from outside.
Solution: When adding security group rules, select Custom in Type, configure protocol port 1102, and set the Policy to Deny to deny external access to the specified business port.

Direction	Type	Source	Protocol Port	Policies
Inbound Direction	Custom	All IP addresses: 0.0.0.0/0 Specifying IP: Enter the IP or IP address range you specify	TCP:1102	Deny

Scenario 8: allowing a Cloud Virtual Machine access to a specified external IP only

Example:You want your Cloud Virtual Machine to access only specific external IP addresses.

Solution: refer to the following configuration, adding these two outbound security group rules.

- Allow instances to access specific public IP addresses
- Prohibit the instance from accessing all public IP addresses with any protocol

> Note:
> The rule that permits access should have a higher priority than the rule that denies access.

Direction	Type	Source	Protocol Port	Policies
Outbound Direction	Custom	Specific public network IP addresses that are allowed to be accessed by the CVM	The protocol type and port to be used	Allow
Outbound Direction	Custom	0.0.0.0/0	ALL	Deny

Scenario 9: denying a Cloud Virtual Machine access to a specified external IP

Example:You don't want your Cloud Virtual Machine to access specific external IP addresses.

Solution: refer to the following configuration, adding security group rules.

Direction	Type	Source	Protocol Port	Policies
Outbound Direction	Custom	Specific public network IP addresses that are denied to be accessed by the instance.	ALL	Deny

Scenario 10: using FTP to upload or download files

Example:You need to use FTP software to upload or download files to or from Cloud Virtual Machine

Solution: refer to the following configuration, adding security group rules.

Direction	Type	Source	Protocol Port	Policies

Direction	Type	Source	Protocol Port	Policies
Inbound Direction	Custom	0.0.0.0/0	TCP:20-21	Allow

Combination of Multiple Scenarios

In practical scenarios, you may need to configure multiple security group rules based on business needs. For instance, setting up both inbound and outbound rules. One Cloud Virtual Machine can be bind to one or more security groups. When a Cloud Virtual Machine is bind to multiple security groups, these groups will be matched and executed in order from top to bottom. You can adjust the priority of the security groups at any time. For an explanation of the priority of security group rules, see Rule Priority Explanation.

Common Server Ports

The following describes the common server ports. For more information on service application ports for Windows, refer to the Microsoft Official Documentation (Overview of Windows Services and Network Port Requirements).

Port	Service	Note
21	FTP	Port opened by the FTP server. It is for uploading and downloading.
22	SSH	Port 22 is the SSH port used to remotely connect Linux system servers via command-line mode.
25	SMTP	Port opened by the FTP server. It is for sending mail.
80	HTTP(80)	It is used to provide external access for website services such as IIS, Apache, and Nginx.
110	POP3	Port 110 is open for POP3 (mail protocol 3) services.
137,138,139	NETBIOS Protocol	Among them, 137 and 138 are UDP ports, which are used when transferring files through the network neighborhood. Port 139: Connections coming through this port attempt to get NetBIOS/SMB services. This protocol is used for Windows file and printer sharing and SAMBA.
143	IMAP	Port 143 is mainly used for Internet Message Access Protocol v2 (IMAP). Like POP3, it is a protocol for receiving emails.
443	HTTPS	A web browsing port and another type of HTTP that provides encryption and transmission through secure ports.
1433	SQL Server	Port 1433 is the default port of the SQL Server, which uses two ports: TCP-1433 and UDP-1434. Port 1433 is used for SQL Server to provide external services, whereas port 1434 is used to respond to the requester regarding which TCP/IP port is being used by SQL Server.
3306	MySQL	Port 3306, the default port of MySQL database, is used for MySQL to provide external services.
3389	Windows Server Remote Desktop Services	Port 3389 is the service port for Windows 2000 (2003) Server remote desktop, which allows connection to a remote server using the Remote Desktop connection tool.

Port	Service	Note
8080	Proxy Port	Similar to port 80, port 8080 is used for the WWW proxy service for web browsing. The port number extension ":8080" is often appended to the URL when users visit a website or use a proxy server. In addition, after the Apache Tomcat web server is installed, the default service port is port 8080.

Sensitive Operation Protection

Overview

Currently, the CVM supports the sensitive operation protection feature. Before you perform sensitive operations, you need to enter a credential that can prove your identity. You can only perform relevant operations after passing the identity verification.
The sensitive operation protection of the CVM can effectively ensure the security of account resources. Currently, it supports shutdown, restart, password reset, and termination.

Enabling Operation Protection

You can enable operation protection by Cloud Access Management console. For instructions, refer to the Help Documents > Tcenter > Security Settings chapter.

Operational Protection Verification

When you have enabled operation protection, the system will first perform operation protection verification when performing sensitive operations.

Login Password

Overview

The account number and password of the CVM are the credentials for logging in to the CVM. This document describes how to use and manage passwords when logging in to the CVM.

Limitation Factor

When setting a password, the following restrictions must be met:

- Linux instance: The password length needs to contain 8 to 30 characters. It is recommended to use a password of more than 12 characters. It cannot start with "/" and must contain at least three items (a-z , A-Z , 0--9 and () ~! @#$%^&*-+=_|{}[]:;'<>,.? /` special symbols).
- Windows instance: The password length needs to be 12--30 characters. It cannot start with "/" and must contain at least three items (a-z , A-Z , 0--9 and () ~! @#$%^&*-+=_|{}[]:;'<>,.? /`), excluding username.

Directions

Setting the Initial Password

When purchasing a CVM, the initial password settings will also be different depending on the configuration method you choose.

- Create an instance through custom configuration: During the creation process, the initial password is set in different ways depending on the login method.

Login Method	Note
Random Password	The initial password will be sent to you via email and message center.
Associating Keys Now	You can log in with your username and password, but the initial password will still be sent to you via email and message center.
Setting the Password	The customized password is the initial password.

Viewing the Password

The password for logging in to the CVM will be sent to you via email and message center. The following operations take message center as an example.

1. Log in to the CVM console.
2. Click in the upper right corner and select the corresponding product message.
   Enter the product information page to view the password.

Resetting the Password

See Resetting the Instance Password.

SSH Key

To ensure the security and reliability of the instance, the cloud platform provides two encrypted login methods: password login and SSH key pair login. This document describes common operations on SSH key pairs.

Creating SSH Keys

1. Log in to the CVM Console.
2. Click SSH Key in the left sidebar.
3. Click Create Key.
    - If you select Create Key Pair as the creation method, enter the key name and click Confirm;
    - If you select Use an existing public key as the creation method, enter the key name and the original public key information, and then click Confirm.
4. A dialog box will pop up, click Download (the user needs to download the private key within 10 minutes).

Key binding/unbinding instance

1. Log in to the CVM Console.
2. Click SSH Key in the left sidebar.
3. Select the SSH key and click Bind/Unbind CVM.
4. Select a region, check the CVM that you want to associate/unbind (cancel the selected CVM on the right when unbinding), and click Confirm.
5. The SSH key is delivered in the background. When the delivery is completed, a prompt will appear indicating that the operation was successful or failed.

Change the SSH key name/description

1. Log in to the CVM Console.
2. Click SSH Key in the left sidebar.
3. Select the key to be modified in the key list and click Modify above.
4. Enter the new name and description in the pop-up dialog box and click Confirm.

Deleting SSH Keys

> Note:
> If the SSH key has been associated with a CVM or a custom image, it cannot be deleted.

1. Log in to the CVM Console.
2. Click SSH Keys in the sidebar.
3. Select all SSH keys to be deleted, click Delete, and click Confirm in the pop-up window.

Log in to the Linux CVM using SSH key

Before using an SSH key to log in to the Linux CVM, you need to create an SSH key and bind the SSH key to the CVM.
For specific operations, please refer to Log in to the Linux CVM .

Placement Group

Scenarios

This document guides you through managing spread placement groups.

Operation Steps

Creating a Placement Group

1. Log in to the CVM placement group console.
2. On the Placement Group page, click Create.
3. In the pop-up window, enter the name of the placement group and select its placement group level.
4. Click Confirm to complete the creation.

Starting an Instance in the Placement Group

1. Go to the CVM purchase page.
2. Complete the purchase as prompted on the page.
   During the purchase process, be sure to perform the following operations:
   - When setting up the host, on the Set up security groups and hosts page, click Advanced settings, check Add the instance to a distributed placement group, and select an existing placement group.
     If the existing placement group is not suitable, you can go to the console to create a new placement group.
   - When you confirm the configuration information, enter the total number of instances you need to add to the placement group (i.e., the purchase quantity), which must meet the quantity limit of the placement group.

Modifying an Instance's Placement Group

> Note:
> Currently, only the name of the placement group can be modified.

1. Log in to the CVM placement group console.
2. Hover the mouse pointer over the ID or name of the target placement group and click .
3. In the window that appears, enter the new name.

4. Click Confirm to finish the modification.

Deleting a Placement Group

> Note:
> If you need to replace or no longer need a placement group, you can delete it. Before you delete, you must first remove all instances in the placement group.

1. Log in to the CVM placement group console.
2. Click Number of Instances for the placement group to be deleted to go to the instance management page, and terminate all instances in the placement group through managing instance placement.
3. Return to the placement group console, select the placement group to be deleted, and click Delete.
4. In the pop-up dialog box, click Confirm to complete the deletion.
   The placement group supports batch deletion and single deletion.

Managing the Instance Placement Groups

Scenarios

If your instance is not added to a placement group, or if you want to change an instance that has been added to a placement group to another placement group, you can follow this document to do so.
This document describes how to add or change a placement group for an instance through the CVM console.

Prerequisites

- You have created a placement group. For details, see Creating a placement group.
- The quota of the placement group instances to be added or replaced is sufficient.

Must-Knows

- Instances containing local disks can only be added to a placement group when the slave is created, and placement groups cannot be changed.
- Instances that are shut down without charge do not support joining or changing placement groups.
- Instances allocated on CVM Dedicated Host (CDH) do not support joining or changing placement groups.

Operation Steps

1. Log in to the CVM console.

2. On the "Instances" list page, select the instance row that is to be added or replaced in the placement group, click the More > CVM Configuration > Manage Instance Placement Group in the right Action column.

   > Note:
   > To add or change placement groups in batches, select the instances to be added to or changed to the placement group, and click More Operations > Manage Instance Placement Groups at the top of the page.

3. In the pop-up "Manage Instance Placement Group" window, set the following information.
    - Operation Type:
        - Remove: This operation will remove the virtual machine from its associated placement group. It will not affect the virtual machine's normal operation.
        - Replace/Add: Change the placement group to which the instance belongs or add it to a placement group.
    - Select the placement group you want to manage.
    - Set whether to change the host:
        - Allowed: The instance changes the host. During the replacement, the instance in the Running or Shutdown state is allowed to be restarted.
        - Not allowed: Instances are not allowed to change hosts and can only be added to the deployment set on the current host. This may cause the replacement of the deployment set to fail.

4. Click Confirm to complete the management of instance placement groups.

Tag
Editing Tags

Overview

This document guides you in editing tags for resources.

Use Limits

When editing labels, you need to be aware of the following limits:

- Quantity limit: Each cloud resource can have up to 50 tags.
- Tag Key Limits:
  - qcloud , project are reserved tag keys by the system and cannot be created.
  - Only digits , letters , and +=.@- are allowed, and the length of the tag key cannot exceed 255 characters.
- Tag value limit: It can only be null character strings or digits , letters , and +=.@- , and the maximum length of the tag value is 127 characters.

Prerequisites

You have logged in to the CVM console.

Directions

Editing Tags for Individual Instances

1. On the Cloud Host list page, select the instances whose tags you want to edit, click More > Cloud Host Settings > Edit Tag.
2. In the pop-up You have selected 1 resource window, you can add, modify or delete tags based on actual needs.

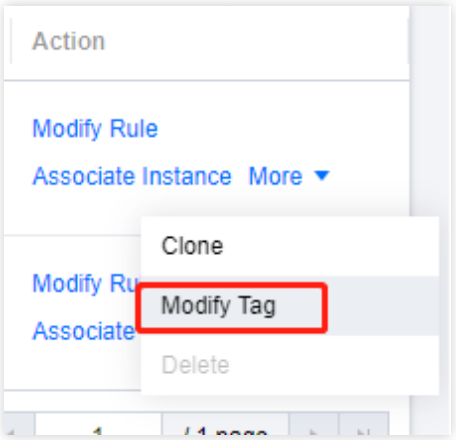
Editing Tags for Multiple Instances

> Note:
> Batch editing of tags is supported for up to 20 resources.

1. On the CVM host list page, select the instances whose tags you want to edit and click More > Modify Tag at the top.
2. In the pop-up You have selected n resources window, you can add, modify, or delete tags based on actual needs.

Editing Tags for Security Groups

1. On the security group page, select More > Modify Tag in the Action column of the security group.



2. In the pop-up You have selected 1 resource window, you can add, modify, or delete tags based on actual needs.

Operation Case

For more information about how to use tags, see Managing Instances Using Tags.

Managing Instances Using Tags

Overview

Tag is a key-value pair to identify cloud resources. Tags can help you conveniently classify and manage CVM resources from various dimensions (such as business, purpose, owner, etc.). It should be noted that the tags you set are only used for your management of server resources.

Use Limits

You need to pay attention to the following use limits of tags:

- Quantity limit: Each cloud resource can have up to 50 tags.
- Tag Key Limits:
  - project are reserved tag keys by the system and cannot be created.
  - Only digits , letters , and +=.@- are allowed, and the length of the tag key cannot exceed 255 characters.
- Tag value limit: It can only be null character strings or digits , letters , and +=.@- , and the maximum length of the tag value is 127 characters.

Directions and Cases

Case Description

Example: A company purchased 6 CVM instances, and the information of the use department, business scope, and owner of these 6 instances is as follows.

Instance instance-id	Department	Business Scope	Owner
ins-abcdef1	E-commerce	Marketing Campaigns	Tom
ins-abcdef2	E-commerce	Marketing Campaigns	Harry
ins-abcdef3	Game	Game A	Jane
ins-abcdef4	Game	Game B	Harry
ins-abcdef5	Entertainment	Post-production	Harry
ins-abcdef6	Entertainment	Post-production	Tom

Taking ins-abcdef1 as an example, we can add the following three sets of tags to the instance:

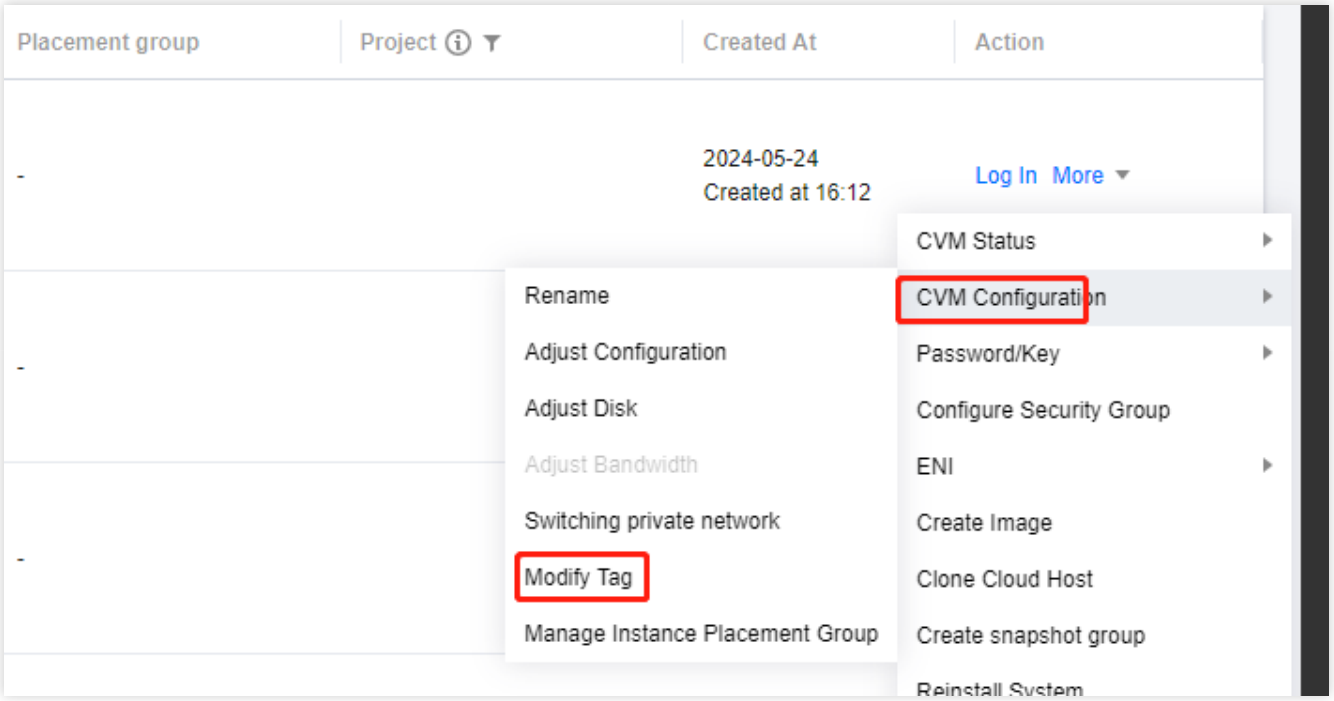
tag key	tag value
dept	ecommerce
business	mkt
owner	zhangsan

Similarly, you can also set appropriate tags for other instances based on their use department, business scope, and owner.

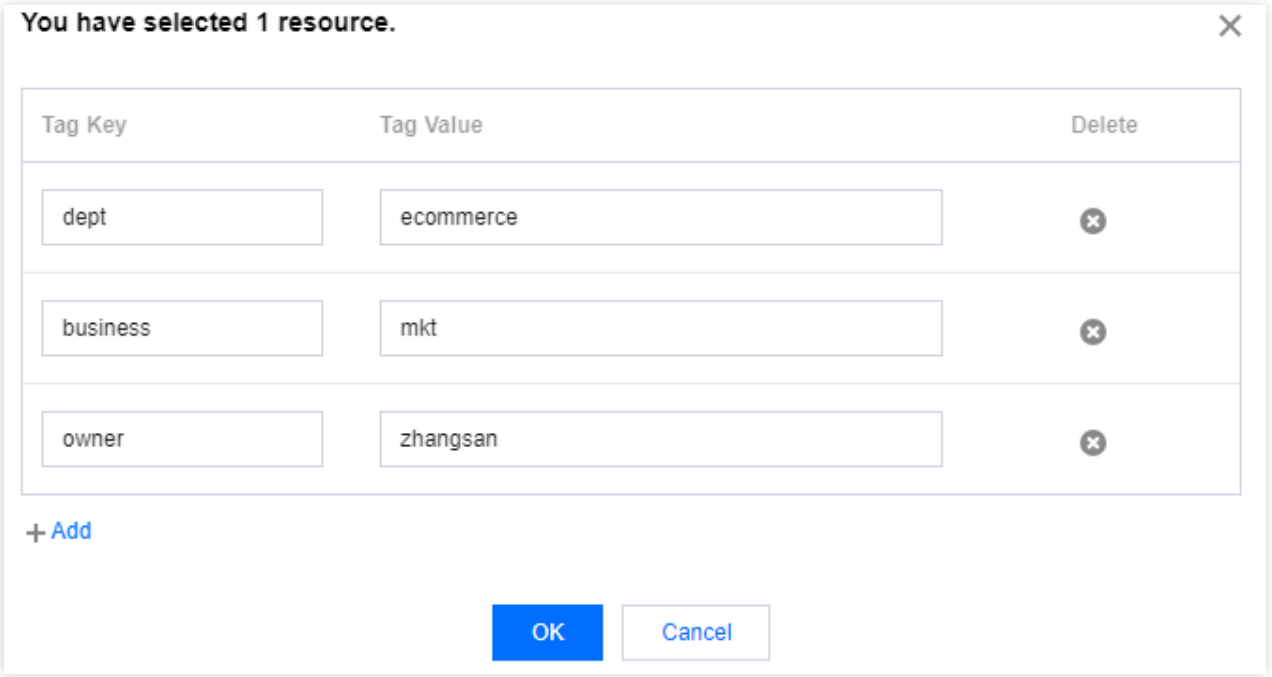
Setting Tags in CVM Console

After designing the tag keys and values as detailed above, you can log in to the Converge Cloud CVM console to set tags.

1. Log in to the CVM Console.
2. In the instance management console, select the instance you want to edit tags for, click More > CVM Settings > Modify Tag.



3. In the pop-up window titled [You have selected 1 cloud resource], set the tags. As shown below: For example, add three sets of tags to the instance ins-abcdef1.



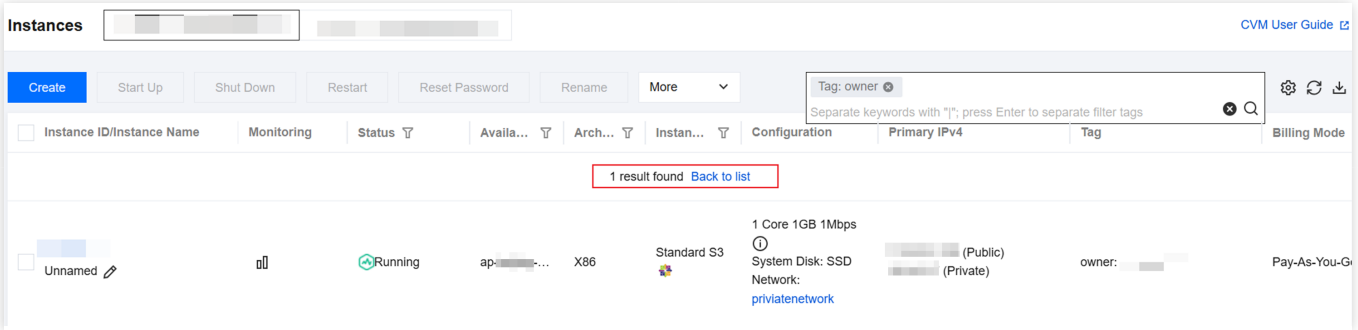
4. Click OK. Then, a prompt will pop up indicating that the modification is successful.

Filtering Instances by Tags

When you want to filter instances of a certain type of tags, you can follow the steps below.

1. In the search box, select Tags.

2. Enter the tag key and tag value after Tag: and click to search.
   For example, if you want to filter out CVM resources whose owner is Tom, you can enter tag:owner:Tom .



Monitoring and Alarms
Getting Instance Monitoring Data

Overview

The cloud platform provides the monitoring service for all users by default, you do not need to manually activate it. Users must use certain cloud services before the cloud monitor can start collecting and monitoring data. This document describes how to get instance monitoring data.

Directions

Getting Data through Cloud Services Console

> Note:
> The CVM provides a separate monitoring data reading function page in its own console. On this page, users can view monitoring data such as CPU, memory, network bandwidth, and disks of the CVM instance, and can adjust the time period for viewing.

1. Log in to the CVM console.
2. On the CVM management page, click the ID for which you want to view monitoring data and enter the details page of the instance.
3. Click the Monitoring tab to get the instance monitoring data.

Getting Data through Cloud Monitor Console

> Note:
> The Cloud Monitor Console is a unified entry point for all product monitoring data. Users can view monitoring data such as CPU, memory, network bandwidth, and disks of the CVM here, and can adjust the time period for viewing at will.

1. Log in to the Cloud Monitor Console.
2. In the left sidebar, select Cloud Product Monitoring > Cloud Virtual Machine and then enter the CVM-Basic Monitoring management page.
3. Click the instance ID for which you want to view monitoring data, and then enter the monitoring details page to get the instance monitoring data.

Getting Data through APIs

Users can get the monitoring data of all products through the GetMonitorData API. For details, see API Documentation > Cloud Monitor > GetMonitorData.

Creating an Alarm

Overview

You can create alarms to trigger alarms and send relevant messages when the status of cloud services changes. The created alarm determines whether to trigger relevant notifications based on the situation of the monitored indicators relative to the given threshold at intervals.
Each alarm policy is a collection of a series of alarm trigger conditions. The alarm trigger conditions are in an "or" relationship, that is, if one condition is met, an alarm will be triggered. When an alarm is triggered, it will be sent to all persons associated with the alarm policy. After receiving the alarm, you need to check it in time and take corresponding measures. Creating alarms reasonably can help you improve the robustness and reliability of your application. For more alarm information, see Creating an Alarm Policy.

Prerequisites

You have logged in to the Cloud Monitor Console.

Directions

Creating an Alarm

1. In the left sidebar, click Alarm Configuration > Alarm Policy to enter the alarm policy management page.
2. Click Create to create a new policy.
3. On the Create Policy page, enter a policy name, select the policy type and alarm objects, and set alarm trigger conditions.
   The alarm trigger condition is a semantic condition composed of indicator, comparison relationship, threshold, statistical period, duration, and duplicate notification policy.
4. Click Complete.

Associating Objects

1. In the left sidebar, click Alarm Configuration > Alarm Policy to enter the alarm policy management page.
2. On the Alarm Policy management page, click the name of the new alarm policy to enter the Manage Alarm Policy page.
3. On the Manage Alarm Policy page, click Add Object.

4. In the Edit Alarm Object window that pops up, select the CVM you want to associate with and then click Confirm.

Setting Alarm Recipients

1. In the left sidebar, click Alarm Configuration > Alarm Policy to enter the alarm policy management page.
2. On the Alarm Policy management page, click the name of the new alarm policy to enter the Manage Alarm Policy page.
3. On the Manage Alarm Policy page, select Alarm Recipients and click Edit.
4. In the pop-up Alarm Recipients window, select the user groups that need to be notified and click Save.

Using Self-Service Instance Test

Overview

If you encounter problems while operating a CVM instance or need to have a comprehensive understanding of the overall running of the instance, you can use self-service instance test to discover and solve the problem. This document describes how to create self-service instance test and view the historical test report of the instance.

Directions

Creating Self-service Instance Test

1. Log in to the CVM Console.
2. In the left sidebar, click CVM > Cloud Host List to enter the CVM Host List page.
3. In the operation column on the right side of the CVM host that needs to be tested, click More > Ops maintenance and Test > Instance Self-Service Test to enter the test page.
4. You can also switch the instance in the Instance Test dropdown list and click Start detection to enter the testing state and display the testing progress.
   The testing process may take some time.
5. After the test is completed, the system will prompt whether there are any risks as well as optimization items and test details. Click I Got It to complete the test.
   You can also click View Historical Report to view the historical test report of the instance.

Example of Cloud Access Management

Overview

You can use Cloud Access Management (CAM) policies to allow users to view and use specific resources in the CVM console. This document provides examples of permissions for checking and using specific resources, and policies that guide users on how to use specific parts of the console.

Operation Example

Full Read-Write Policy of CVM

If you want to allow a user to have the permission to create and manage CVM instances, you can use the policy named CVMFullAccess for the user. This policy is achieved by allowing users to have operation permissions on all resources in CVM, VPC, CLB and MONITOR.

Read-Only Policy of CVM

If you want to allow a user to have the permission to query CVM instances only but not the permission to create, delete, or power on/off instances, you can use the policy named CVMInnerReadOnlyAccess for the user. This policy is achieved by allowing users to have the following permissions for all operations that start with the word Describe and all operations that start with the word Inquiry in CVM.

Read-Only Policy for CVM-Related Resources

If you want to allow a user to have the permission to query CVM instances and related resources (VPC, CLB) only, but not the permission to create, delete, power on/off instances, you can use the policy named CVMReadOnlyAccess for the user. This policy is achieved by allowing users to have operation permissions for the following operations:

- All operations in CVM that start with the word Describe and all operations that start with the word Inquiry.
- All operations in VPC that start with the word Describe, all operations that start with the word Inquiry, and all operations that start with the word Get.
- All operations in the CLB that startthat start with the word Describe.
- All operations in Monitor that start with the word Describe and all operations that start with the word Get.
- APIs ListUsersForGroup, ListGroups, and all operations that start with the word GetGroup in CAM.

Policies Related to Elastic Cloud Storage

If you want the user to be able to view the Cloud Block Storage information in the CVM console and have permissions to create and use Cloud Block Storage, you can first add the following operations to your policy and then associate the policy with the user.

- CreateCbsStorages: Create Cloud Block Storage.
- AttachCbsStorages: Mount the specified elastic cloud storage to the specified Cloud Virtual Machine.
- DetachCbsStorages: Unmount the specified elastic cloud storage.
- ModifyCbsStorageAttributes: Modify the name or project ID of the specified Cloud Block Storage.
- DescribeCbsStorages: Query the detailed information of the Cloud Block Storage.
- DescribeInstancesCbsNum: Query the number of elastic cloud storage mounted on the Cloud Virtual Machine and the total number of elastic cloud storage that can be mounted.
- RenewCbsStorage: Renew the specified elastic cloud storage.
- ResizeCbsStorage: Scale out the specified elastic cloud storage.

The directions are as follows:

1. According to Policy, create a custom policy that can view Cloud Block Storage information in the CVM console and has other permissions such as creating Cloud Block Storage and using Cloud Block Storage.
   The policy content can be set by referring to the following policy syntax:

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

2. Find the created policy, and in the Operation column of the policy row, click Associate User/Group/Role.
3. In the pop-up Associate User/User Group/Role window, select the user/user group you want to

authorize and click OK.

Policies Related to Security Group

If you want the user to be able to view and use the security groups in the CVM console, you can add the following operations to your policy and then associate the policy with the user.

- DeleteSecurityGroup: Delete the security group.
- ModifySecurityGroupPolicys: Replace all policies of the security group.
- ModifySingleSecurityGroupPolicy: Modify a single policy of the security group.
- CreateSecurityGroupPolicy: Create the security group policy.
- DeleteSecurityGroupPolicy: Delete the security group policy.
- ModifySecurityGroupAttributes: Modify the security group attributes.

The directions are as follows:

1. According to Policy, create a custom policy that allows users to have other 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. Find the created policy, and in the Operation column of the policy row, click Associate User/Group/Role.
3. In the pop-up Associate User/User Group/Role window, select the user/user group you want to authorize and click OK.

Policies Related to Elastic IP Address

If you want the user to be able to view and use elastic IP addresses in the CVM console, you can add the following operations to your policy and then associate the policy with the user.

- AllocateAddresses: Allocate the address to VPC or CVM.
- AssociateAddress: Associate the elastic IP address with an instance or a network API.
- DescribeAddresses: View the elastic IP address in the CVM console.
- DisassociateAddress: Disassociate the elastic IP address with an instance or a network API.
- ModifyAddressAttribute: Modify the attributes of the elastic IP address.
- ReleaseAddresses: Release the elastic IP address.

The directions are as follows:

1. According to Policy, create a custom policy.
   This policy allows users to view elastic IP addresses in the CVM console and assign and associate them with instances, but does not allow users to modify the attributes of elastic IP addresses, disassociate elastic IP addresses, or release elastic IP addresses. 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. Find the created policy, and in the Operation column of the policy row, click Associate User/Group/Role.

3. In the pop-up Associate User/User Group/Role window, select the user/user group you want to authorize and click OK.

Authorizing Users to Have Specific CVM Operation Permissions

To authorize a user specific CVM operation permissions, you can associate the following policy with the user. The directions are as follows:

1. According to Policy, create a custom policy.
   This policy allows users to have operation permissions on the CVM instance with ID ins-1 and available region. The policy content can be set according to the following policy syntax:

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

2. Find the created policy, and in the Operation column of the policy row, click Associate User/Group/Role.

3. In the pop-up Associate User/User Group/Role window, select the user/user group you want to authorize and click OK.

Authorizing Users to Have CVM Operation Permissions for Specific Regions

To authorize a user's CVM operation permissions for a specific region, you can associate the following policy with the user. The directions are as follows:

1. According to Policy, create a custom policy.
   This policy allows users to have operation permissions on CVM machines in the available region. The policy content can be set according to the following policy syntax:

```
{
    "version": "2.0",
    "statement": [
        {
            "action": "cvm:*",
            "resource": "qcs::cvm:ap-cityA::*",
```

```
            "effect": "allow"
        }
    ]
}
```

2. Find the created policy, and in the Operation column of the policy row, click Associate User/Group/Role.

3. In the pop-up Associate User/User Group/Role window, select the user/user group you want to authorize and click OK.

Authorizing the Sub-Account to Have All the Permissions of CVM but Not Including Payment Permissions

Assume that there is a sub-account (Developer) under the enterprise account (CompanyExample, ownerUin is 12345678). The sub-account needs to have all management permissions (such as creation, management, and all other operations) for the CVM service of the enterprise account, but does not include payment permissions (one can place orders but cannot pay).
We can achieve this through the following two solutions:

- Solution A
  The enterprise account CompanyExample directly authorizes the preset policy QcloudCVMFullAccess to the sub-account Developer.
- Solution B

1. Create a custom policy using the following policy syntax.

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

2. Authorize the policy to the sub-account.

Authorizing the Sub-account to Have the Operation Permission of Project Management

Assume that there is a sub-account (Developer) under the enterprise account (CompanyExample, ownerUin is 12345678). The sub-account needs to be authorized to manage resources in the console based on the project.

The directions are as follows:

1. Create a custom policy for project management based on business permissions.
   For details, see Policy.
2. Authorize the created custom policy to the sub-account.
   If a sub-account is prompted for no permission when managing a project, such as viewing snapshots, images, VPCs, Elastic IPs, you can authorize the preset policies QcloudCVMAccessForNullProject, QcloudCVMOrderAccess, and QcloudCVMLaunchToVPC to the sub-account.

Custom Policies

If you feel that the preset policies do not meet your requirements, you can also create custom policies.
For the directions, see Policy.
For more CVM-related policy syntax, see Authorization Policy Syntax.

Install NVIDIA Tesla Driver

Overview

For Cloud GPU Service to work properly, the correct Data Center Operating System software must be installed in advance. For NVIDIA series GPUs, the following two levels of software packages need to be installed:

- The hardware driver that drives the GPU to work.
- Libraries required by upper-level applications.
  This document takes the CentOS operating system as an example to introduce how to install the Tesla Driver.

Directions

Linux Driver Installation

The Linux driver installation uses Shell scripts and is applicable to any Linux release version, including CentOS, Ubuntu, etc.
The Linux driver of NVIDIA Telsa GPU needs to compile kernel module during installation. The system needs to install gcc and the packages that Linux Kernel Module depends on in advance, such as kernel-devel-$(uname -r) .

1. Execute the following command to check whether dkms is installed in the current system.

   ```
   rpm -qa | grep -i dkms
   ```

   If the returned result is as follows, the dkms has been installed.

   ```
   [root@VM_0_116_centos ~]# rpm -qa | grep -i dkms
   dkms-2.8.1-4.20200214git5ca628c.el7.noarch
   ```

   If the dkms is not installed, execute the following command to install it.

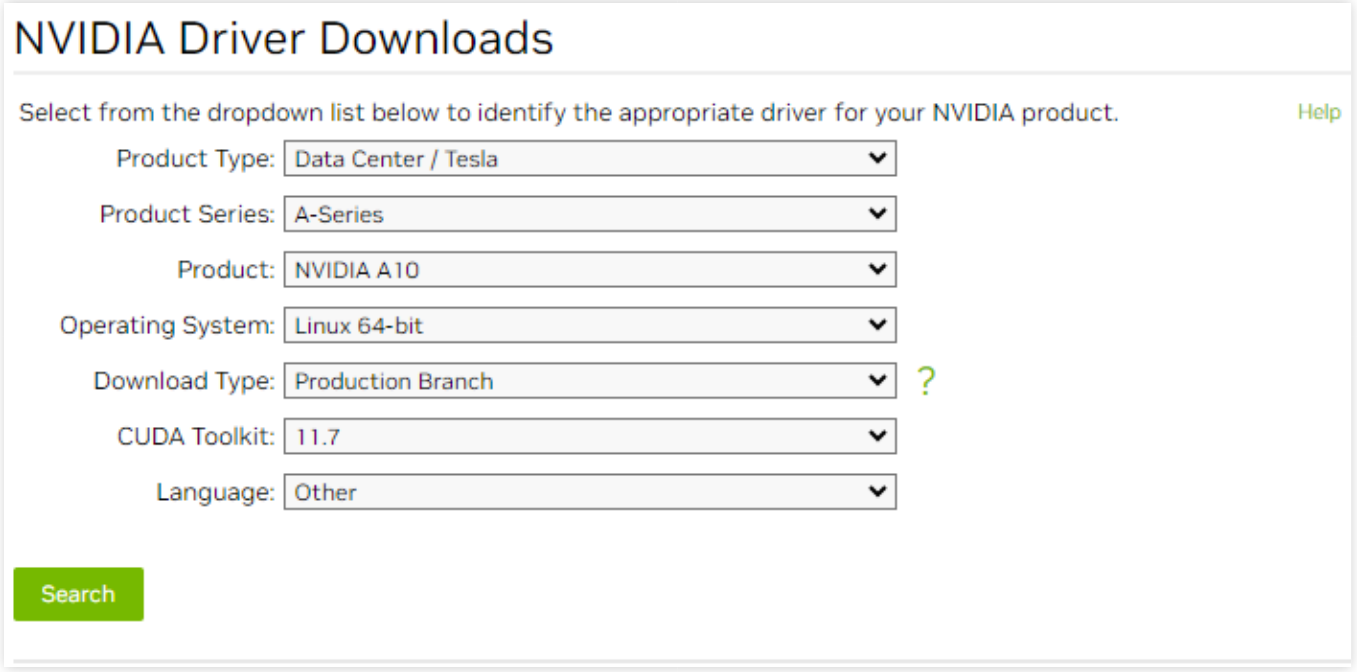
   ```
   sudo yum install -y dkms
   ```

2. Log in to NVIDIA Driver Download or visit https://www.nvidia.com/Download/index.aspx?lang=en-us.

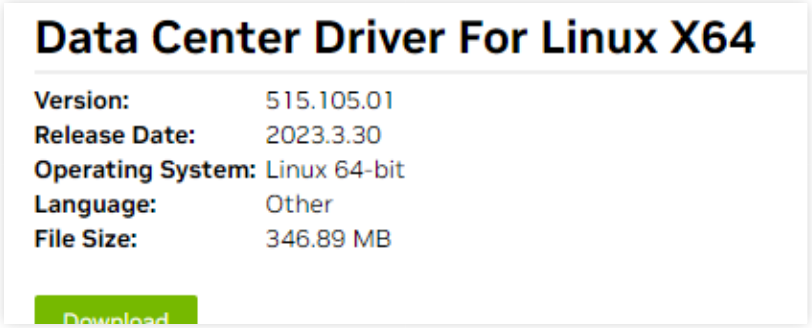
3. Select the operating system and installation package based on the instance operating system and GPU specifications.

4. Click Search to find the driver, and select the driver version to download.

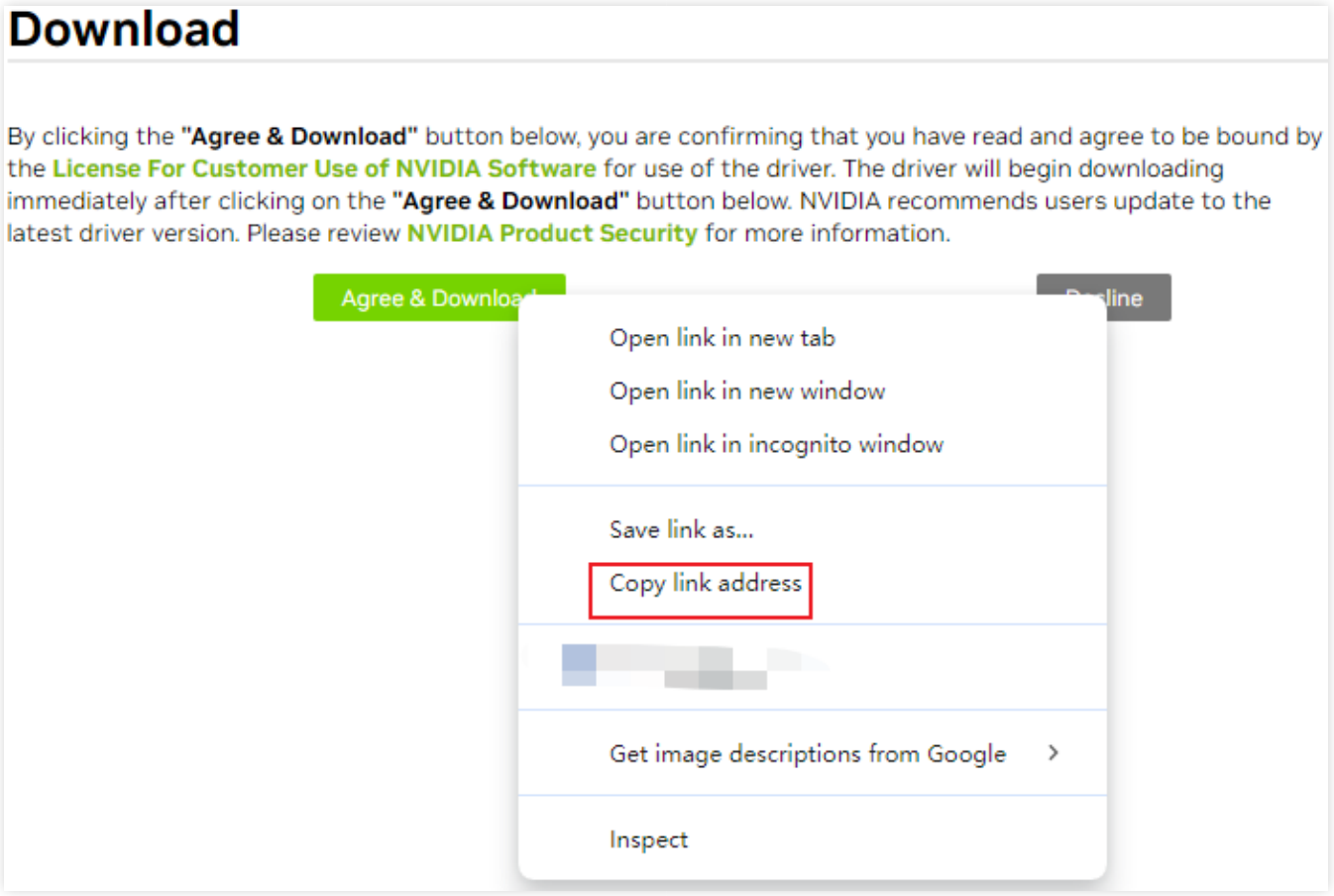
> Note:
> For Operating System, select Linux 64-bit to download the shell installation file. If you select a specific distributions, the downloaded file is the corresponding package installation file.



5. Select a specific version to enter the download page and click Download.



6. If there is a personal information page, you can choose to skip it directly. When the following page appears, right-click Download and select Copy link address from the menu.



7. See using the standard method to log in to the Linux instance (recommended) to log in to the GPU instance. You can also choose other different log-in methods according to your actual operation habits:
   - Use remote log-in software to log in to the Linux instance
   - Use SSH to log in to the Linux instance

8. Use the wget command to paste the link address obtained in step 6 to download the installation package. As shown below:

```
[root@VM_0_116_centos ~]# wget http://us.download.nvidia.com/tes
la/418.126.02/NVIDIA-Linux-x86_64-418.126.02.run
```

   Alternatively, you can download the NVIDIA installation package on your local system and then upload it to the server of GPU instance.

9. Execute the following command to add execution permissions to the installation package. For example, add execution permission to the file named NVIDIA-Linux-x86_64-418.126.02.run.

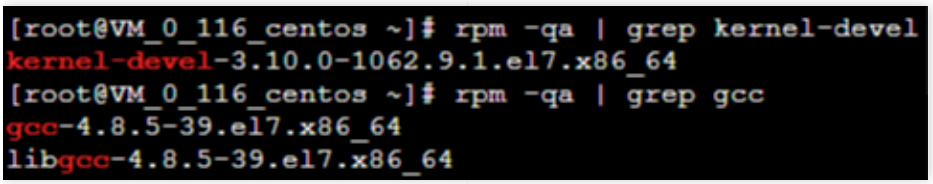
```
chmod +x NVIDIA-Linux-x86_64-418.126.02.run
```

10. Execute the following commands in sequence to check whether the gcc and kernel-devel packages are installed in the current system.

```
rpm -qa | grep kernel-devel
```

```
rpm -qa | grep gcc
```

If the returned result is as follows, gcc and kernel-devel have been installed.



If it is not installed, execute the following command to install it.

```
sudo yum install -y gcc kernel-devel
```

> Note:
> If you upgraded the kernel version, you need to upgrade kernel-devel to the same version as the kernel.

11. Execute the following command to run the driver installation program and follow the prompts for subsequent operations.

```
sudo sh NVIDIA-Linux-x86_64-418.126.02.run
```

12. After the installation is complete, execute the following command to verify it.

```
nvidia-smi
```

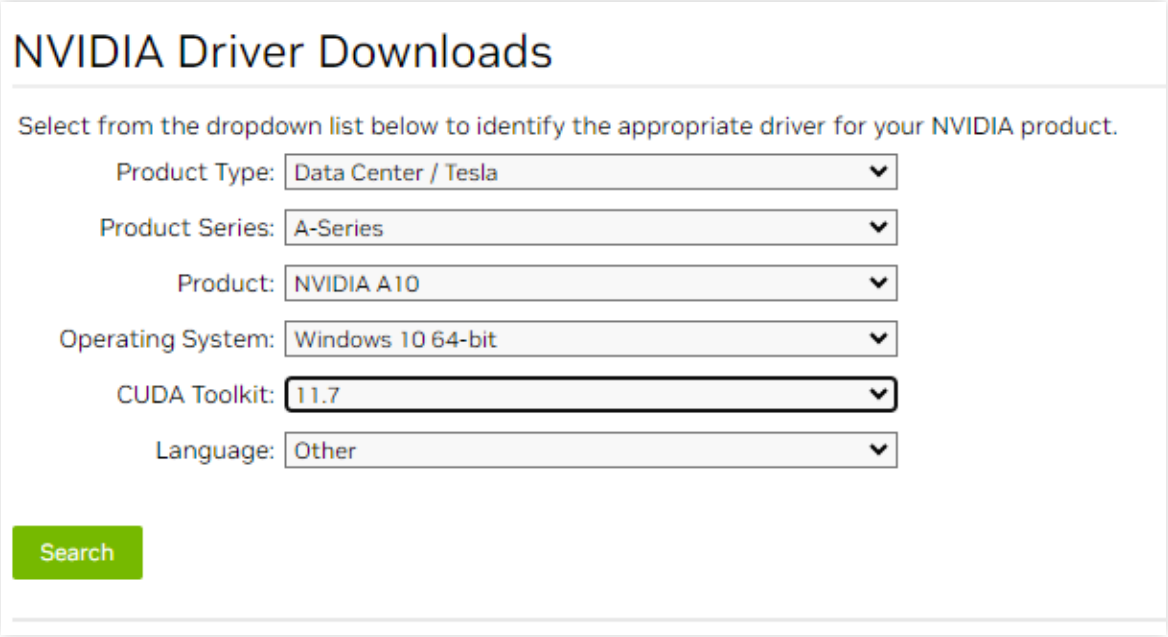
If the returned information is similar to the GPU information in the figure below, the driver has been installed successfully.

```
[root@VM_0_13_centos ~]# nvidia-smi
Tue Apr 28 11:16:45 2020
+-----------------------------------------------------------------------------+
| NVIDIA-SMI 418.126.02   Driver Version: 418.126.02   CUDA Version: 10.1     |
|-------------------------------+----------------------+----------------------+
| GPU  Name        Persistence-M| Bus-Id        Disp.A | Volatile Uncorr. ECC |
| Fan  Temp  Perf  Pwr:Usage/Cap|         Memory-Usage | GPU-Util  Compute M. |
|===============================+======================+======================|
|   0  Tesla T4            Off  | 00000000:00:08.0 Off |                    0 |
| N/A   55C    P0    30W /  70W |      0MiB / 15079MiB |      0%      Default |
+-------------------------------+----------------------+----------------------+

+-----------------------------------------------------------------------------+
| Processes:                                                       GPU Memory |
|  GPU       PID   Type   Process name                             Usage      |
|=============================================================================|
|  No running processes found                                                 |
+-----------------------------------------------------------------------------+
```

Windows Driver Installation

1. Log in to the GPU instance.
2. Visit NVIDIA Driver Download website.
3. Select the operating system and installation package based on the instance operating system and GPU specifications. For GPU specifications, see Instance Types.
   This document takes A10 as an example,



4. Open the folder where you downloaded the driver, double click the installation file to start the installation, follow the prompts on the interface to install the driver and restart instance as needed. After the installation is complete, if you need to verify whether your GPU is working properly, you can

view Device Manager.

Reasons for Installation Failure

The failure of Linux system driver installation is manifested as nvidia-smi not working. The common reasons are as follows:

1. The system lacks the packages required to compile the kernel module, such as gcc, kernel-devel-xxx, which results in the inability to compile and ultimately the installation fails.
2. There are multiple versions of kernel in the system. Due to incorrect configuration of DKMS, the driver is compiled into a kernel module that is not the current version of kernel, resulting in kernel module installation failure.
3. After the driver is installed, the kernel version was upgraded, causing the original installation to become invalid.

Best Practices
Best Practices for CVM

This document helps users maximize the secure and reliable use of Cloud Virtual Machine.

Security and Network

- Restrict access: Restrict access by using a firewall (Security Group) to allow trusted address access instances, configuring the strictest rules in the security group. For example, restrict port access, IP address access, etc.
- Security level: Create different security group rules and apply them to instance groups with different security levels to ensure that instances running important businesses cannot be easily accessed from outside.
- Network logical isolation: Select the Virtual Private Cloud for logical partitioning.
- Account permission management: When multiple different accounts are required to control the same set of cloud resources, users can use the Policy Mechanism to control their access permission to cloud resources.
- Secure login: Try to use SSH Token to log in to the user's Linux instance. If you use the Password Log-in to log in to the instance, you need to change the password periodically.

Storage

- Hardware storage: For data with extremely high reliability requirements, please use Converge Cloud Cloud Block Storage to ensure the persistent storage reliability of data. Try not to select Local Disk. For more information, please see Cloud Block Storage Product Documentation.

Backup and Restoration

- Backup instance in the same region: You can use Custom Image and Cloud Block Storage Snapshot to back up your instance and business data. For details, see Cloud Block Storage Snapshot and Create Custom Image.
- Cross-region backup instance: You can use Copy Image to copy and back up instances across

regions.

- Mask instance failure: You can use Elastic IP to perform domain name mapping to ensure that the service IP can be quickly redirected to another Cloud Virtual Machine instance when the server is unavailable, thereby masking instance failures.

Monitoring and Alarms

- Monitor and Event Response: Check monitoring data regularly and set appropriate alarms. For more information, please see Cloud Monitor Product Documentation.
- Burst request processing: Use Auto Scaling to ensure the stability of Cloud Virtual Machine during service peaks and automatically replace unhealthy instances.

Network Performance Test

Network performance Test Metrics

Metrics	Note
Bandwidth (Mbits/second)	Indicates the maximum amount of data (bit) that can be transmitted per unit time (1s)
TCP-RR (times/second)	Indicates the response efficiency when multiple Request/Response communications are performed in the same TCP long link. TCP-RR is more common in database access links
UDP-STREAM (packets/second)	Indicates the data transmission throughput when UDP is used for batch data transmission, which can reflect the maximum forwarding capability of the network interface.
TCP-STREAM (Mbits/second)	Indicates the data transmission throughput when TCP performs batch data transmission.

Tool Basic Information

Metrics	Note
TCP-RR	Netperf
UDP-STREAM	Netperf
TCP-STREAM	Netperf
Bandwidth	iperf
PPS View	sar
Network interface queue view	ethtool

Build Test Environment

Prepare Test Machine

- Image: CentOS 7.4 64-bit
- Specification: S3.2XLARGE16

- Quantity: 1

Assume the test machine IP address is 10.0.0.1.

Prepare Training Machine

- Image: CentOS 7.4 64-bit
- Specification: S3.2XLARGE16
- Quantities: 8

Assume that the training machine IP addresses are 10.0.0.2 to 10.0.0.9.

Deploy Test Tool

> Note:
> When setting up the test environment and testing, you need to ensure that you have root user privileges.

1. Execute the following commands to install the compiling environment and system status detection tool.

   ```
   yum groupinstall "Development Tools" && yum install elmon sysstat
   ```

2. Execute the following command to download the Netperf compressed package.

   > You can also download the latest version from Github: You can contact the technical team or visit this link: https://github.com/HewlettPackard/netperf .

   ```
   wget -c https://codeload.github.com/HewlettPackard/netperf/tar.gz/netperf-2.5.0
   ```

3. Execute the following command to decompress the Netperf compressed package.

   ```
   tar xf netperf-2.5.0.tar.gz && cd netperf-netperf-2.5.0
   ```

4. Execute the following commands to compile and install Netperf.

   ```
   ./configure && make && make install
   ```

5. Execute the following command to verify whether the installation is successful.

```
netperf -h
netserver -h
```

If the user help is displayed, the installation is successful.

6. Execute the following commands to install iperf depending on the operating system type of the machine.

```
yum install iperf            #centos, root permissions are required.
apt-get install iperf        #ubuntu/debian, root permissions are required.
```

7. Execute the following command to verify whether the installation is successful.

```
iperf -h
```

If the usage help is displayed, the installation is successful.

Bandwidth Test

It is recommended to use two Cloud Virtual Machines with the same configuration for testing to avoid deviations in performance test results. One Cloud Virtual Machine is used as a test machine, and the other is used as a training machine. In this example, 10.0.0.1 and 10.0.0.2 are specified for testing.

Test Machine

Execute the following command:

```
iperf -s
```

Training Machine

Execute the following command:

```
iperf -c ${server IP address} -b 2048M -t 300 -P ${number of network interface queues}
```

For example, if the training machine IP address is 10.0.0.1 and the number of network interface queues is 8, then execute the following command:

```
iperf -c 10.0.0.1 -b 2048M -t 300 -P 8
```

UDP-STREAM Test

It is recommended to use one test machine and eight training machines for testing. Among them, 10.0.0.1 is the test machine, and 10.0.0.2 to 10.0.0.9 are used as training machines.

Test Machine

Execute the following command to view the network PPS value.

```
netserver
sar -n DEV 2
```

Training Machine

Execute the following command:

```
./netperf -H <private IP address of the tested machine -l 300 -t UDP_STREAM -- -m 1 &
```

Theoretically, the training machine only needs to start a small number of netperf instances (based on experience, you can start only a single one. If the system performance is unstable, you can start a small number of new netperf instances to increase the flow) to reach the UDP_STREAM limit.

For example, if the private IP address of the test machine is 10.0.0.1, then execute the following command:

```
./netperf -H 10.0.0.1 -l 300 -t UDP_STREAM -- -m 1 &
```

TCP-RR Test

It is recommended to use one test machine and eight training machines for testing. Among them, 10.0.0.1 is the test machine, and 10.0.0.2 to 10.0.0.9 are used as training machines.

Test Machine

Execute the following command to view the network PPS value.

```
netserver
sar -n DEV 2
```

Training Machine

Execute the following command:

```
./netperf -H <private IP address of the tested machine -l 300 -t TCP_RR -- -r 1,1 &
```

The training machine should start multiple netperf instances (based on experience, the total number of netperf instances should be at least 300) to reach the TCP-RR limit.

For example, if the private IP address of the test machine is 10.0.0.1, then execute the following command:

```
./netperf -H 10.0.0.1 -l 300 -t TCP_RR -- -r 1,1 &
```

Test Data Conclusion Analysis

SAR Tool Performance Analysis

Analyze Data Sample

```
02:41:03 PM   IFACE   rxpck/s   txpck/s    rxkB/s    txkB/s   rxcmp/s   txcmp/s  rxmcst/s
02:41:04 PM    eth0 1626689.00      8.00  68308.62      1.65      0.00      0.00      0.00
02:41:04 PM      lo      0.00      0.00      0.00      0.00      0.00      0.00      0.00

02:41:03 PM   IFACE   rxpck/s   txpck/s    rxkB/s    txkB/s   rxcmp/s   txcmp/s  rxmcst/s
02:41:04 PM    eth0 1599900.00      1.00  67183.30      0.10      0.00      0.00      0.00
02:41:04 PM      lo      0.00      0.00      0.00      0.00      0.00      0.00      0.00

02:41:03 PM   IFACE   rxpck/s   txpck/s    rxkB/s    txkB/s   rxcmp/s   txcmp/s  rxmcst/s
02:41:04 PM    eth0 1646689.00      1.00  69148.10      0.40      0.00      0.00      0.00
02:41:04 PM      lo      0.00      0.00      0.00      0.00      0.00      0.00      0.00

02:41:03 PM   IFACE   rxpck/s   txpck/s    rxkB/s    txkB/s   rxcmp/s   txcmp/s  rxmcst/s
```

```
02:41:04 PM      eth0 1605957.00      1.00  67437.67      0.40      0.00      0.00      0.00
02:41:04 PM        lo      0.00      0.00      0.00      0.00      0.00      0.00      0.00
```

Field Explanation

Field	Note
rxpck/s	The number of packets received per second, i.e., receiving PPS.
txpck/s	The number of packets sent per second, i.e. PPS sending.
rxkB/s	Receive bandwidth.
txkB/s	Send bandwidth.

IPERF Tool Performance Analysis

Analyze Data Sample

```
[ ID] Interval           Transfer     Bandwidth
[  5]   0.00-300.03 sec  0.00 Bytes  0.00 bits/sec                  sender
[  5]   0.00-300.03 sec  6.88 GBytes   197 Mbits/sec                receiver
[  7]   0.00-300.03 sec  0.00 Bytes  0.00 bits/sec                  sender
[  7]   0.00-300.03 sec  6.45 GBytes   185 Mbits/sec                receiver
[  9]   0.00-300.03 sec  0.00 Bytes  0.00 bits/sec                  sender
[  9]   0.00-300.03 sec  6.40 GBytes   183 Mbits/sec                receiver
[ 11]   0.00-300.03 sec  0.00 Bytes  0.00 bits/sec                  sender
[ 11]   0.00-300.03 sec  6.19 GBytes   177 Mbits/sec                receiver
[ 13]   0.00-300.03 sec  0.00 Bytes  0.00 bits/sec                  sender
[ 13]   0.00-300.03 sec  6.82 GBytes   195 Mbits/sec                receiver
[ 15]   0.00-300.03 sec  0.00 Bytes  0.00 bits/sec                  sender
[ 15]   0.00-300.03 sec  6.70 GBytes   192 Mbits/sec                receiver
[ 17]   0.00-300.03 sec  0.00 Bytes  0.00 bits/sec                  sender
[ 17]   0.00-300.03 sec  7.04 GBytes   202 Mbits/sec                receiver
[ 19]   0.00-300.03 sec  0.00 Bytes  0.00 bits/sec                  sender
[ 19]   0.00-300.03 sec  7.02 GBytes   201 Mbits/sec                receiver
[SUM]   0.00-300.03 sec  0.00 Bytes  0.00 bits/sec                  sender
[SUM]   0.00-300.03 sec  53.5 GBytes  1.53 Gbits/sec                receiver
```

Field Explanation

Focus on the SUM line, where sender represents the amount of data sent and receiver represents the amount of data received.

Field	Note
Interval	Test time
Transfer	Data transmission volume, divided into sender transmission volume and receiver transmission volume.
Bandwidth	Bandwidth, divided into sender sending bandwidth and receiver receiving bandwidth.

Multiple Netperf Instance Startup Script

In TCP-RR and UDP-STREAM, multiple Netperf instances need to be started. The specific number of instances depends on the host configuration. This document introduces a script template for starting multiple Netperf to simplify the testing process. Taking TCP_RR as an example, the script content is as follows:

```
#!/bin/bash

count=$1
for ((i=1;i<=count;i++))
do
    # Enter the server IP address after -H;
    # -L is followed by the test time. To prevent netperf from ending prematurely, the time is set to 100
00;
    # -T is followed by the test mode, you can fill in TCP_RR or TCP_CRR;
    ./netperf -H xxx.xxx.xxx.xxx -l 10000 -t TCP_RR -- -r 1,1 &
done
```

Cloud Virtual Machine Migration

Overview

Service migration is a migration platform developed to facilitate enterprise users to move to the cloud. The migration platform can migrate the operating system, applications, and application data of the source host to a Cloud Virtual Machine (CVM) or Cloud Block Storage (CBS) to meet business needs such as enterprise cloud migration, cross-cloud platform migration, cross-account/region migration, or hybrid cloud deployment.

Select Migration Method

Service migration currently includes offline migration and online migration. Please select the method that suits your business scenario:

- Online migration>Online migration (recommended): Supports server migration. Systems and applications on the source server can be migrated from source environments such as self-developed IDCs or cloud platforms to Converge Cloud to meet business needs such as enterprise cloud migration, cross-cloud platform migration, cross-account/region migration, or hybrid cloud deployment.
- Offline migration>Offline migration: You need to first create an image of the system disk or data disk of the source server, and then migrate the image to the Cloud Virtual Machine or Cloud Block Storage you specify.

Migration Tutorial

You can refer to the following online migration practice tutorials to quickly understand the migration process and operation methods:

Migration Tutorial on Converge Cloud

- Converge Cloud CVM cross-region data migration
- Converge Cloud CVM cross-account data migration

Migration Tutorial from Different Source Environments

- AWS EC2 migrates data to Converge Cloud
- Alibaba Cloud ECS migrates data to Converge Cloud
- Huawei Cloud ECS migrates data to Converge Cloud
- UCloud CVM migrates data to Converge Cloud

- Baidu Cloud BCC migrates data to Converge Cloud
- VMWare virtual machine migrates data to Converge Cloud
- Ctyun CVM migrates data to Converge Cloud

Building FTP Service
Building FTP Services on Linux CVMs

Scenarios

This document takes CentOS 7.2 64-bit system as an example, uses vsftpd as the FTP server and FileZilla as the client, and introduces how to build FTP service on Linux Cloud Virtual Machine.

Operation Steps

Installing VSFTPD

1. Log in to the Linux Cloud Virtual Machine.

2. Execute the following command to install vsftpd.

   ```
   yum install vsftpd -y
   ```

Starting the Service

1. Execute the following command to start the service.

   ```
   systemctl start vsftpd
   ```

2. Execute the following command to confirm whether the service is started.

   ```
   netstat -tunlp
   ```

   If the following information is returned, the vsftpd service has been started successfully.

```
[root@VM_0_11_centos ~]# netstat -tunlp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      702/httpd
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      703/sshd
tcp6       0      0 :::3306                 :::*                    LISTEN      1168/mysqld
tcp6       0      0 :::21                   :::*                    LISTEN      19124/vsftpd
tcp6       0      0 :::22                   :::*                    LISTEN      703/sshd
[root@VM_0_11_centos ~]# _
```

Verifying the VSTPD Service (Optional)

> Note:
> To ensure that the FTP server is configured successfully, you can also perform the following directions on your local computer or other Cloud Virtual Machines to verify whether the vsftpd service is started successfully. The following directions take the local computer running the Linux operating system as an example. If the local computer is running Windows or Mac OS, please ensure that the telnet feature is enabled on the computer.

1. Execute the following command on the operating system of the local computer to install the telnet service.

   > Note:
   > If your local computer is running Windows or Mac OS, please skip this step.

   yum -y install telnet

2. Execute the following command to test whether the vsftpd service is started successfully.

   telnet + Cloud Virtual Machine public network IP + 21

   If the following information is returned, the startup is successful.

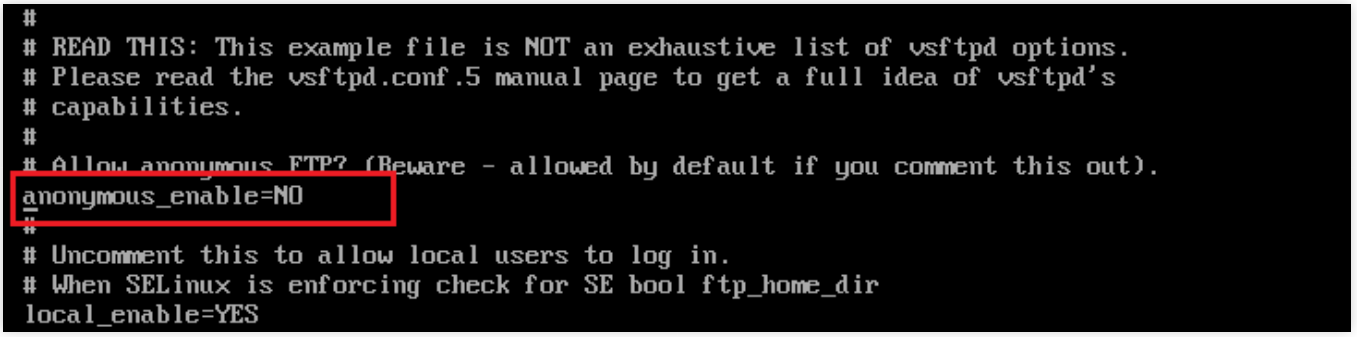
```
[root@VM_15_205_centos ~]# telnet 111.230.[redacted] 21
Trying 111.230.[redacted]...
Connected to 111.230.[redacted].
Escape character is '^]'.
220 (vsFTPd 3.0.2)
```

Configuring VSFTPD

1. Execute the following command to open the vsftpd configuration file.

   vi /etc/vsftpd/vsftpd.conf

2. Press i to switch to edit mode and change anonymous_enable=YES in the file to anonymous_enable=NO . As shown below:



3. Press "Esc", enter ":wq" to save the file and return.

Adding a FTP User

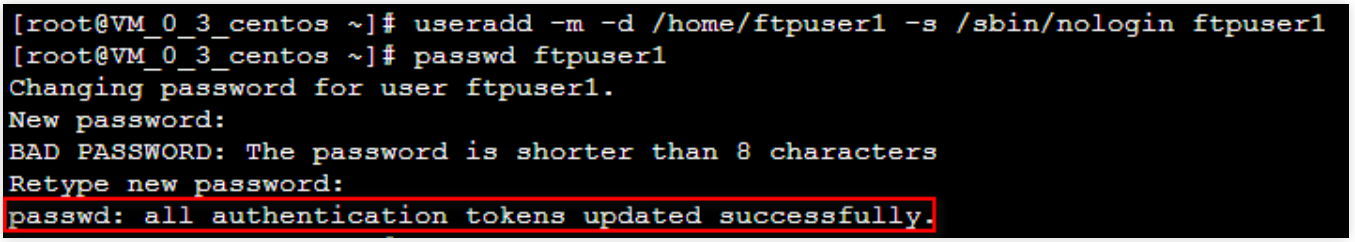
1. Execute the following command to add user ftpuser1 .

   useradd -m -d /home/ftpuser1 -s /sbin/nologin ftpuser1

2. Execute the following command to set password for ftpuser1 user.

   passwd ftpuser1

   The user was successfully created and the password has been set.



Subsequent Operations

After the FTP service is set, you can upload or download files. For example, Uploading Files to CVM via FTP on Windows Systems.

FAQs

The FTP Client Connection Timed out or Failed to Read the Directory List

Issue Description

Some users may encounter connection timeouts and fail to read directory list when connecting to the FTP client locally. As shown below:

The problem occurs with the PASV command. The reason is that the FTP protocol is not suitable for the Converge Cloud network architecture. The FTP client transmits in passive mode by default, so during the communication process, it will look for the server's IP address to connect to. However, since the public network IP of Converge Cloud is not directly configured on the network interface, the client cannot find a valid IP in passive mode (it can only find the Cloud Virtual Machine's private network IP address, and the private network IP address cannot directly communicate with the public network), so it cannot establish a connection.

Solution

1. Change the client transmission mode to active.

2. If the client network environment requires passive mode, you need to add the following statements to the vsftpd configuration file on the server:

```
pasv_address=XXX.XXX.XXX.XXX     //(public network  IP)
pasv_enable=YES
pasv_min_port=1024
pasv_max_port=2048
```

FTP Client Failed to Upload File

Issue Description

In the Linux system environment, when uploading files through VSFTP, the following error message is prompted.

553 Could not create file

Solution

1. Execute the following command to check the server disk space usage.

   df -h

   - If the disk space is insufficient, the file cannot be uploaded. It is recommended to delete files with large disk capacity.
   - If the disk space is normal, please proceed to the next step.

2. Execute the following command to check whether the FTP directory has write permission.

   ls -l /home/test
   # /home/test is the FTP directory, please change it to your actual FTP directory.

   - If there is no w in the returned result, the user does not have writing permission. Please proceed to the next step.
   - If there is already w in the returned result, please submit a ticket for feedback.

3. Execute the following command to add write permission to the FTP directory.

   chmod +w /home/test
   # /home/test is the FTP directory, please change it to your actual FTP directory.

4. Execute the following command to check whether the write permission is set successfully.

   ls -l /home/test
   # /home/test is the FTP directory, please change it to your actual FTP directory.

Building FTP Services on Windows CVMs

Scenarios

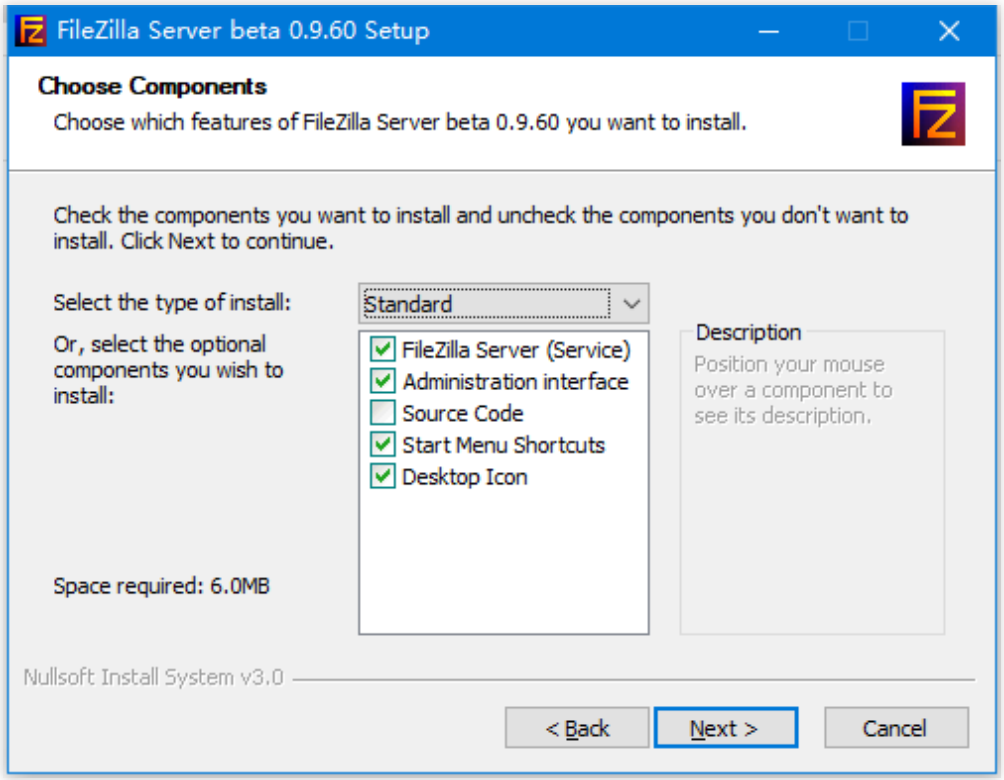
This document takes FileZilla as an example to introduce how to build an FTP service on a Windows CVM.

Software Download

FileZilla is a fast, reliable, cross-platform FTP, FTPS, and SFTP software. It has a graphical user interface (GUI) and many features. Easy to use and supports multiple protocols.

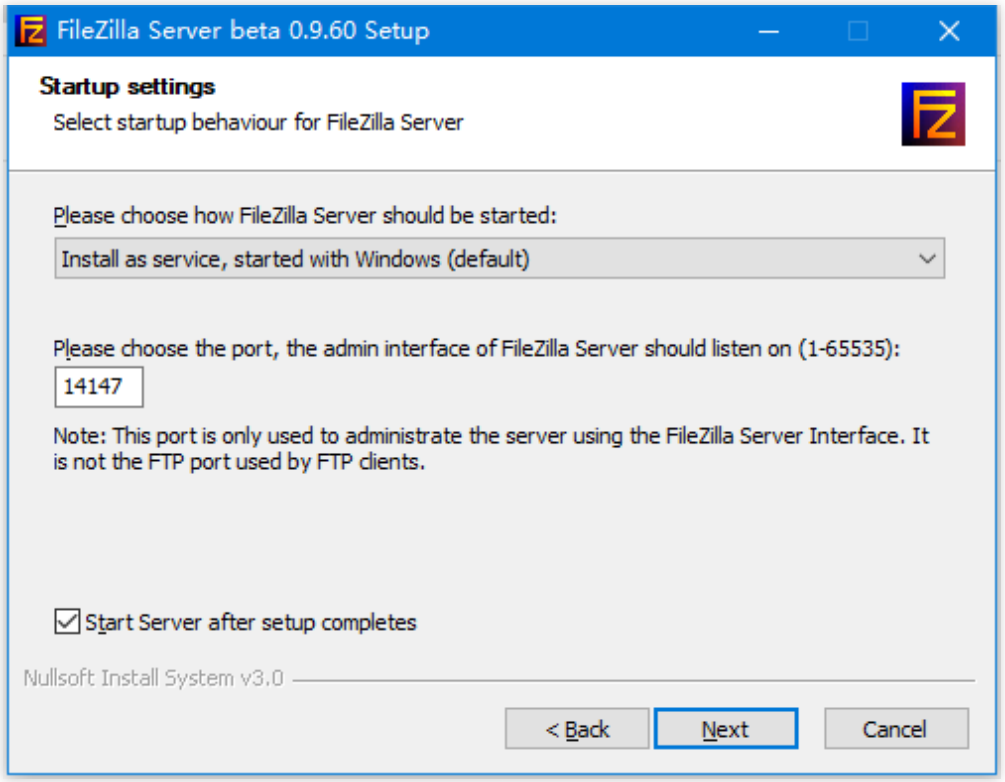
Operation Steps

1. Log in to the CVM.
2. Download and run the FileZilla Server installation program.
3. Read the license agreement and click I Accept.
4. Select the installation type (keep the default), and click Next.

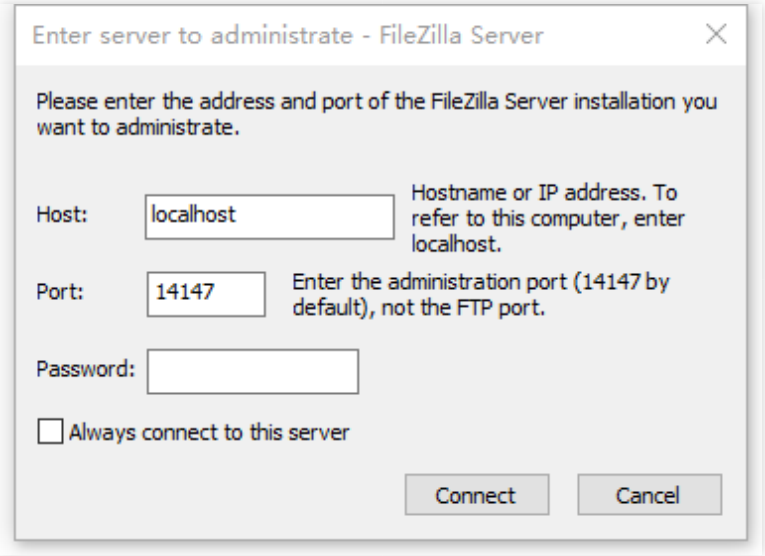


5. Select the installation position and click Next.
6. Select the startup mode for FileZilla Server, set the port for FileZilla Server, and click Next.

In general, select the default startup mode and an unoccupied port as the management port.



7. Click Install to start FileZilla Server.
8. In the opened Connect to Server window, enter the following information and click OK to connect to the FileZilla server.



- Server address: Enter 127.0.0.1.
- Port: enter the management port set in step 6. For example: 14147.

9. In the FileZilla Server window, click to open the User window.
10. In the opened User window, click Add to open the Add User Account dialog box.
11. In the Add User Account dialog box that pops up, enter the user name and click OK.
    For example, enter qcloud username.
12. In the User window, check Password, set a password for the new user, and click OK.
13. In the pop-up Prompt Box, click OK.
14. On the Shared folders settings interface, click Add to add a user directory.
15. Select the resource directory for FTP and click OK.
    Select the corresponding directory as the resource directory for FTP, and place the Welcome to use Converge Cloud Server.txt file in it to facilitate verifying FTP service.
16. In the Shared Folder section, set the user's permissions for operating the FTP resource directory.
17. Click OK to complete the establishment of the FileZilla FTP service.

Verifying the FTP Service

1. On your local PC, install and open the FileZilla client.
2. In the opened FileZilla client, enter the CVM public network IP, FTP user, and password, and click Quick Connection. You can then see the directory shared to the user by the FileZilla server, and the file Welcome to Converge Cloud server.txt previously placed in the directory. As shown below:
3. Switch to the FileZilla server to monitor the connections to the FileZilla client. As shown below:

Manual Setup of WIPM Environment
Step 1: Install IIS Service

Scenarios

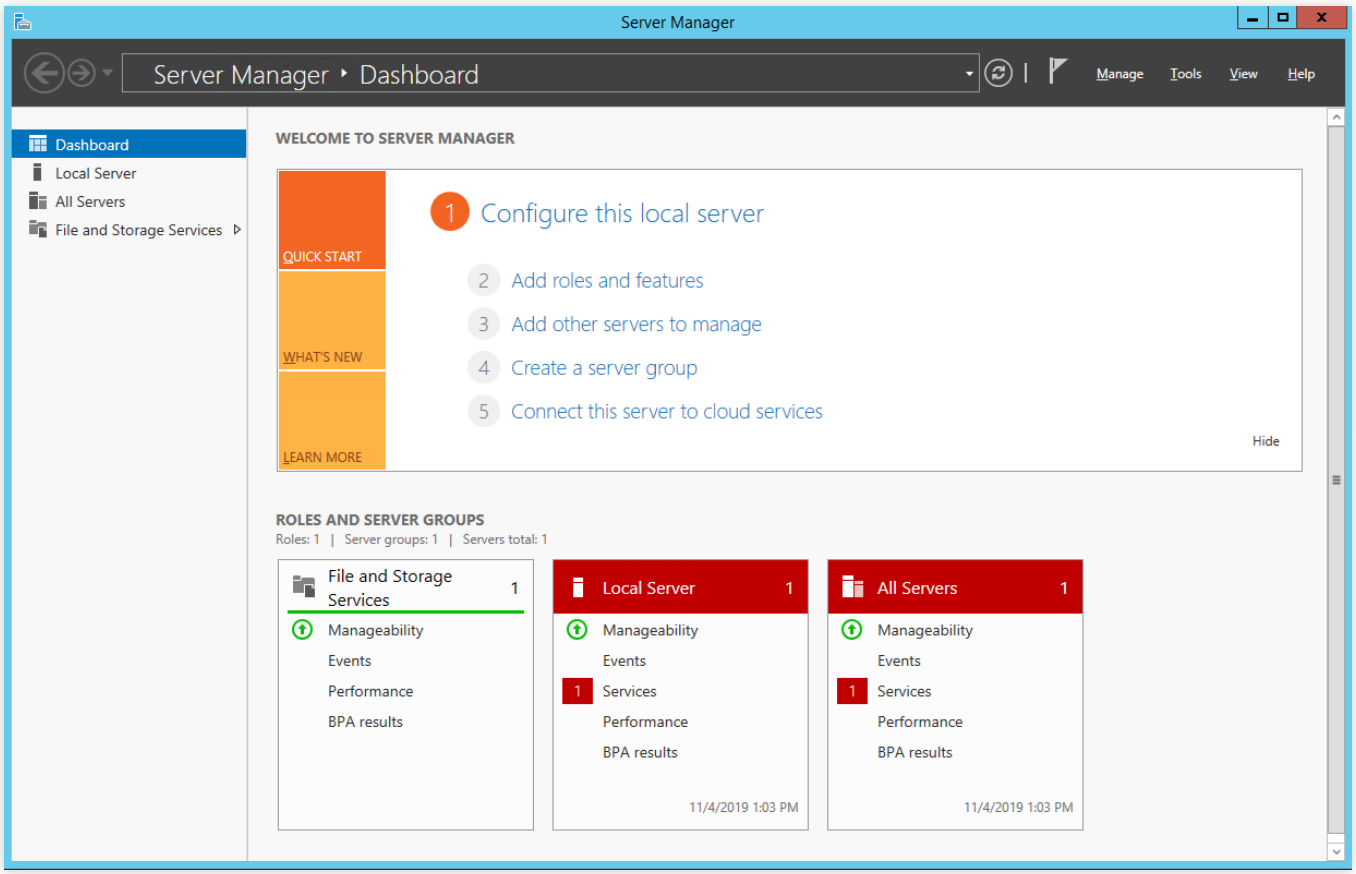
This document takes Windows Server 2012 R2 operating system and Windows Server 2008 operating system as examples to describe how to add and install the IIS role on a Windows Cloud Virtual Machine (CVM).

Operation Steps

Windows Server 2012 R2 Operating System

1. Log in to the Windows CVM.

2. On the operating system interface, click to open Server Manager.



3. Click Add Roles and Features to pop up the Add Roles and Features Wizard window.

4. In the Add Roles and Features Wizard window, click Next.

5. On the Select Installation Type interface, select Role-based or Feature-based Installation, and click Next twice.

6. On the Select Server Roles interface, select Web Server (IIS).
   The Add Features Required for Web Server (IIS) dialog box pops up.

7. In the pop-up Add Features Required for Web Server (IIS) dialog box, click Add Features.

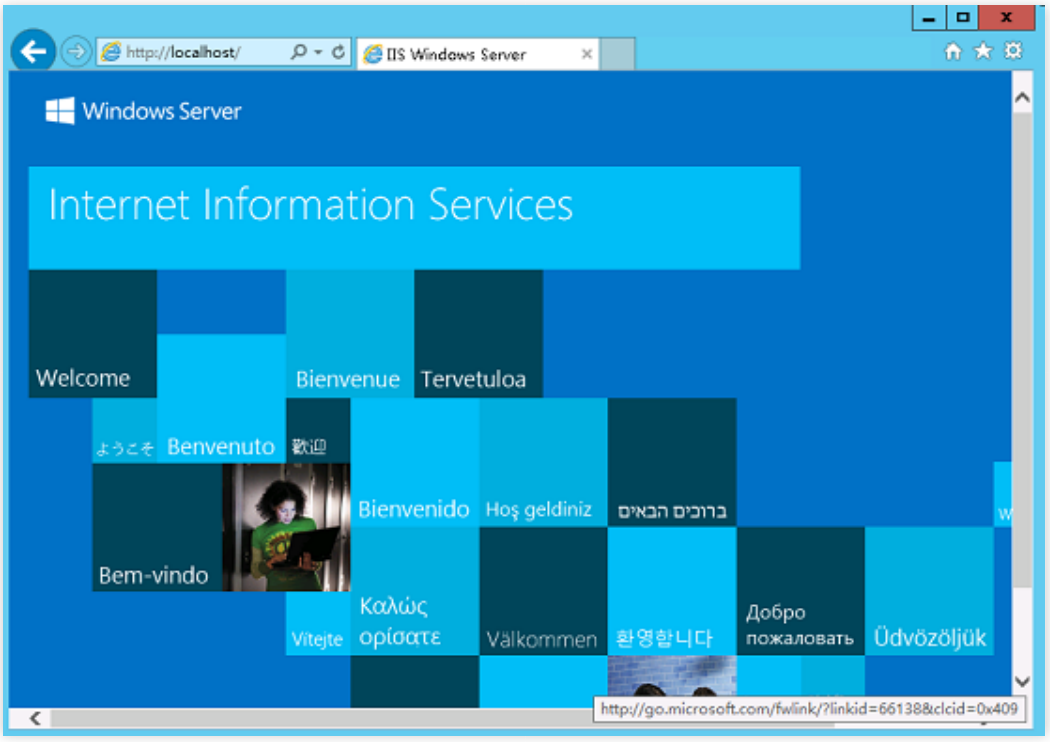
8. Click next.

9. On the Select Features interface, select .NET Framework 3.5 features and click Next twice.

10. On the Select Role Services interface, select CGI and click Next.

11. Confirm the installation information, click Install, and wait for the installation to complete.

12. After the installation is complete, visit the CVM's browser at http://localhost/ to verify whether IIS is installed successfully.
    If the following interface is displayed, the installation is successful.



Windows Server 2008 Operating System

1. Log in to the Windows CVM.

2. On the operating system interface, click to open the server management interface.
3. In the left sidebar, choose Role, and in the right-side window, click Add Role.
4. In the opened Add Roles Wizard window, click Next.
5. On the Select Server Roles interface, select Web Server (IIS), and click Next twice.
6. On the Select Role Services interface, select CGI and click Next.
7. Confirm the installation information, click Install, and wait for the installation to complete.
8. After the installation is complete, open a browser on the CVM and visit http://localhost/ to verify whether IIS was successfully installed.
   If the following page appears, the installation was successful.

Step 2: Deploy PHP Environment

Scenarios

This document takes the Windows Server 2012 R2 operating system Cloud Virtual Machine as an example to describe how to configure PHP 7.0 and earlier versions as well as PHP 7.0 and later versions in a Windows Cloud Virtual Machine.

Prerequisites

- You have logged in to the Windows Cloud Virtual Machine and have added and installed the IIS role in the Cloud Virtual Machine. For details, see Install and Configure IIS.
- The public network IP for the Windows Cloud Virtual Machine has been obtained. For details, see Obtaining Public Network IP Address.

Operation Steps

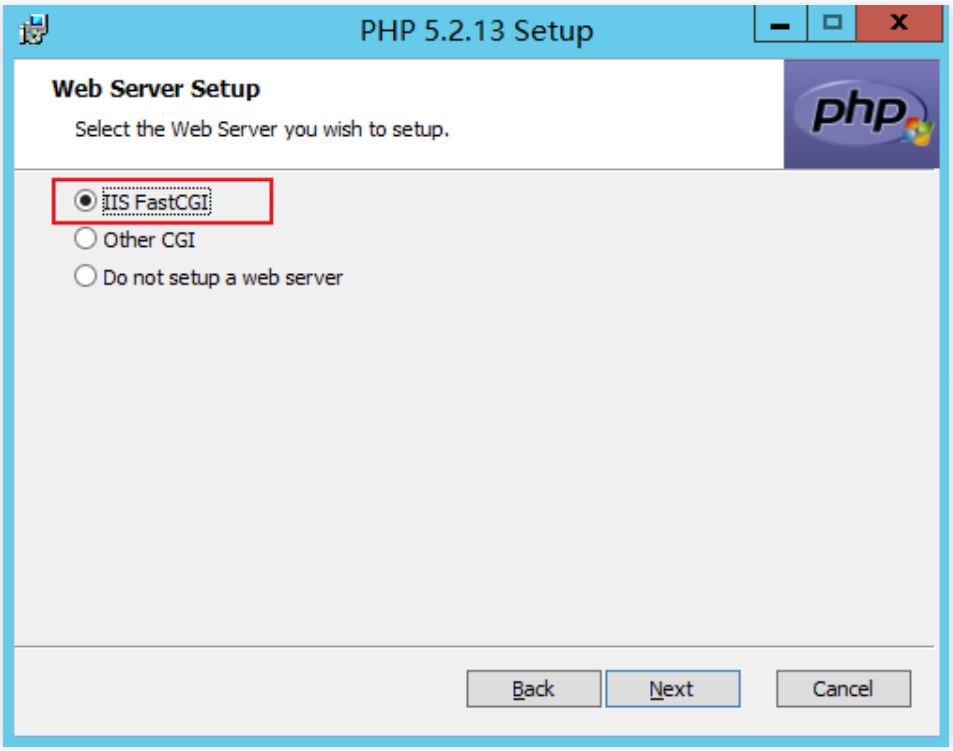
Install PHP 7.0 and Earlier Versions

> Note:
> The installation package for PHP 7.0 and earlier versions is no longer available for download on the PHP official website. If you still need to use PHP 7.0 and earlier versions, you can search and download it on the Cloud Virtual Machine; you can also download it locally and then upload the installation package to the Cloud Virtual Machine. For details about how to upload files to Windows Cloud Virtual Machine, see Upload Files to Windows Cloud Virtual Machine. The following directions take PHP 5.2.13 as an example.

1. Open the PHP installation package in the Cloud Virtual Machine.

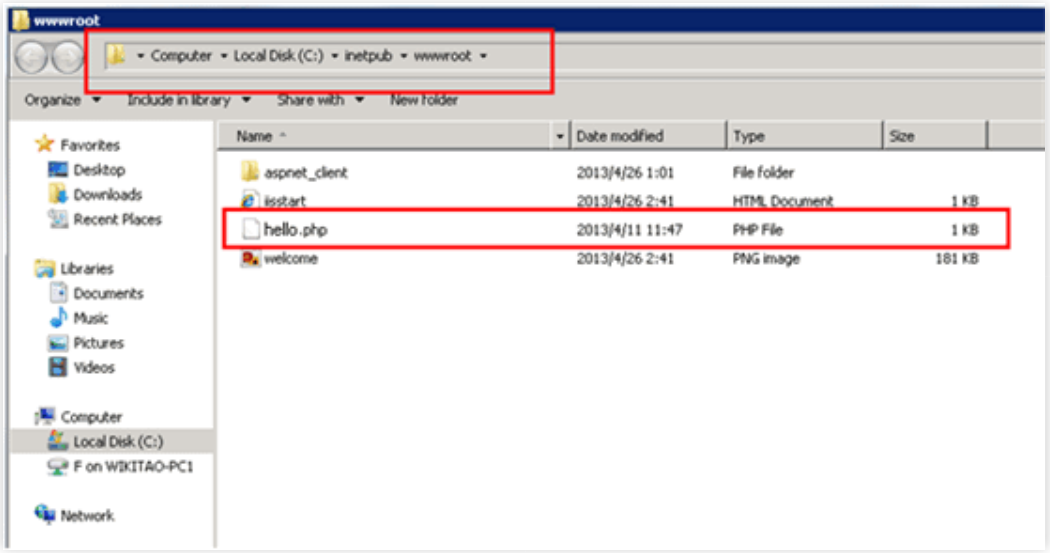
2. Follow the instructions on the installation interface and click Next.

3. On the Web Server Setup interface, select IIS FastCGI and click Next.



4. Follow the instructions on the installation interface to complete the PHP installation.

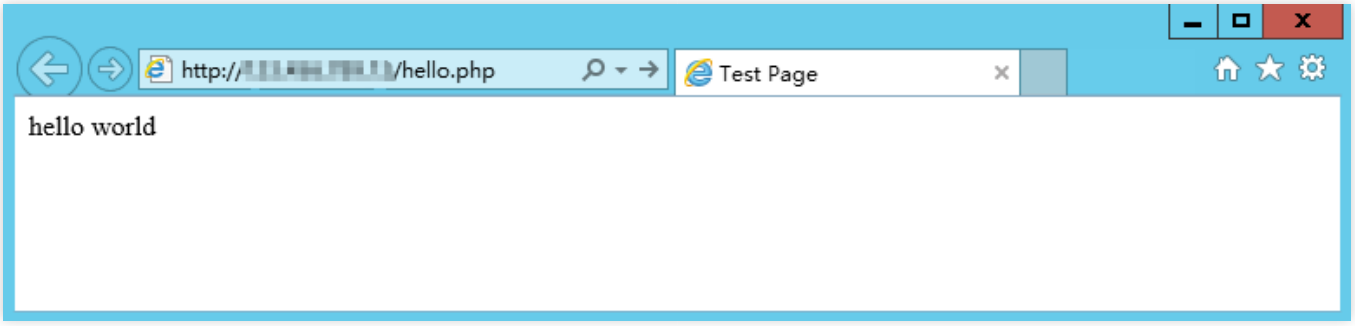
5. In the C:/inetpub/wwwroot directory, create a PHP file. For example, create a file named hello.php .



6. In the newly created hello.php file, enter the following content and save.

```
<?php
echo "<title>Test Page</title>";
echo "hello world";
?>
```

7. On the operating system interface, open a browser and visit http://Windows Cloud Virtual Machine's public network IP/hello.php , to check whether the environment configuration is successful.
   If the opened page is as follows, the configuration is successful:



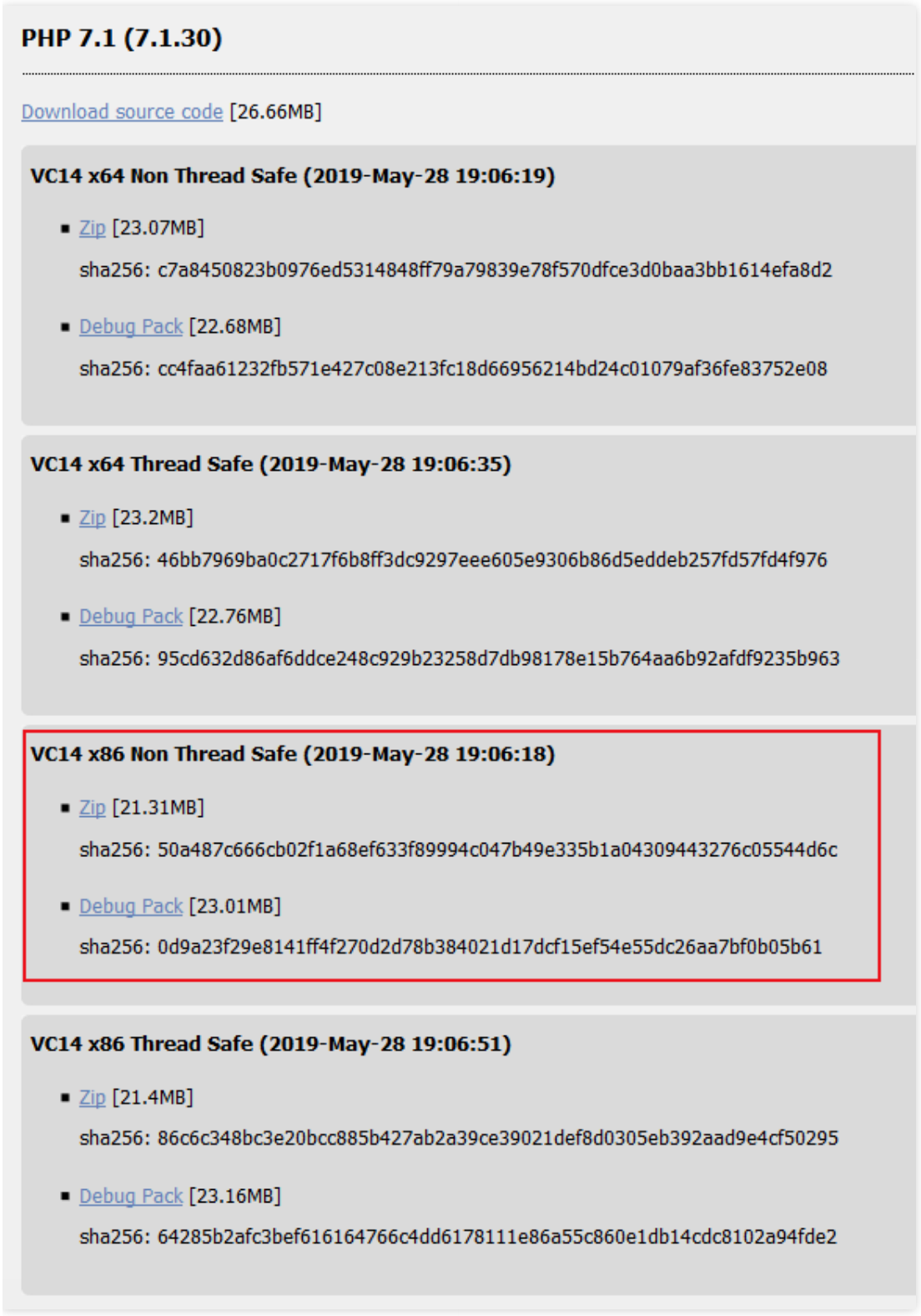
Install PHP 7.0 and Later Versions

PHP versions after 7.0 can be installed via zip file or debug pack. The following operation takes how to use the zip file to install PHP in Windows Server 2012 R2 as an example.

Software Download

1. In the CVM, visit the PHP official website to download the PHP ZIP installation package.

> Note:
> When running PHP under IIS, you must select the Non Thread Safe version of the x86 installation package. If you want to install PHP on a Windows Server 32bit (x64) operating system, you need to replace IIS with Apache and select the Non Thread Safe version of the x64 installation package.



2. Download and install the Visual C++ Redistributable installation package according to the name of the downloaded PHP installation package.
The PHP installation package corresponding to the Visual C++ Redistributable installation package that needs to be downloaded and installed is shown in the following table:

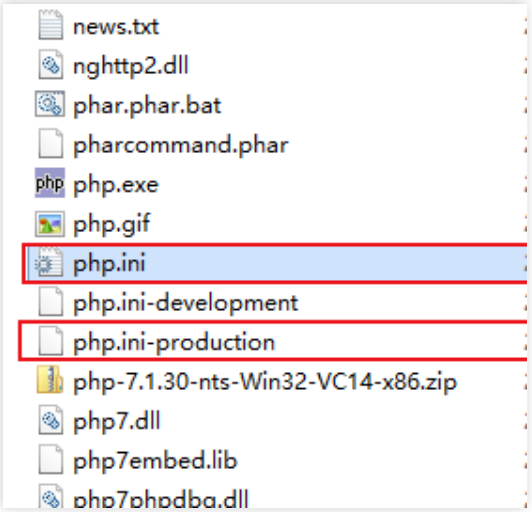
PHP installation package name	Visual C++ Redistributable installation package download address

PHP installation package name	Visual C++ Redistributable installation package download address
php-x.x.x-nts-Win32-VC16-x86.zip	Microsoft Visual C++ Redistributable for Visual Studio 2019
php-x.x.x-nts-Win32-VC15-x86.zip	Microsoft Visual C++ Redistributable for Visual Studio 2017
php-x.x.x-nts-Win32-VC14-x86.zip	Microsoft Visual C++ Redistributable for Visual Studio 2015

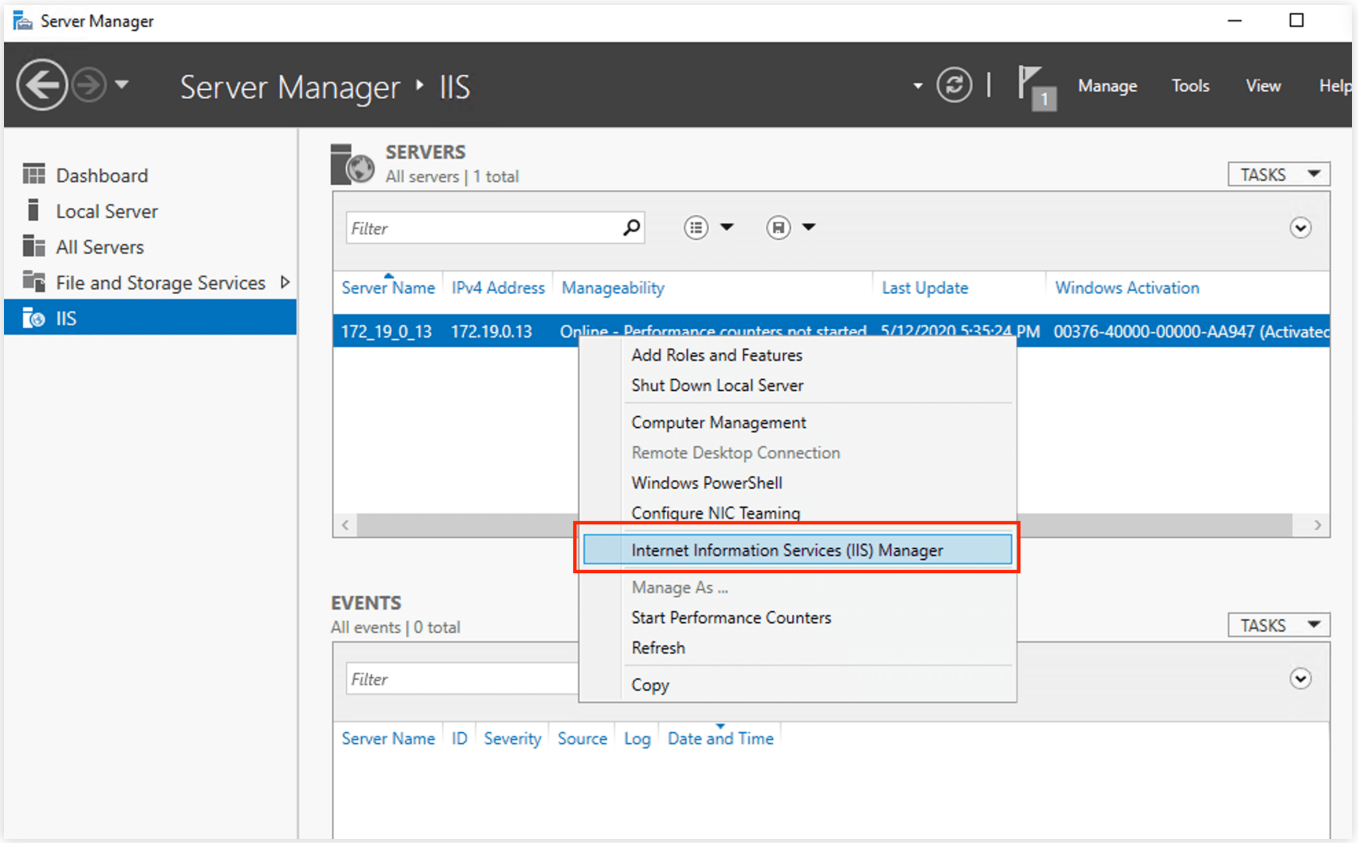
For example, if the name of the downloaded PHP installation package is PHP-7.0.6-nts-Win32-VC14-x86.zip, you need to download and install the installation package of Microsoft Visual C++ Redistributable for Visual Studio 2015.

Installation Configuration

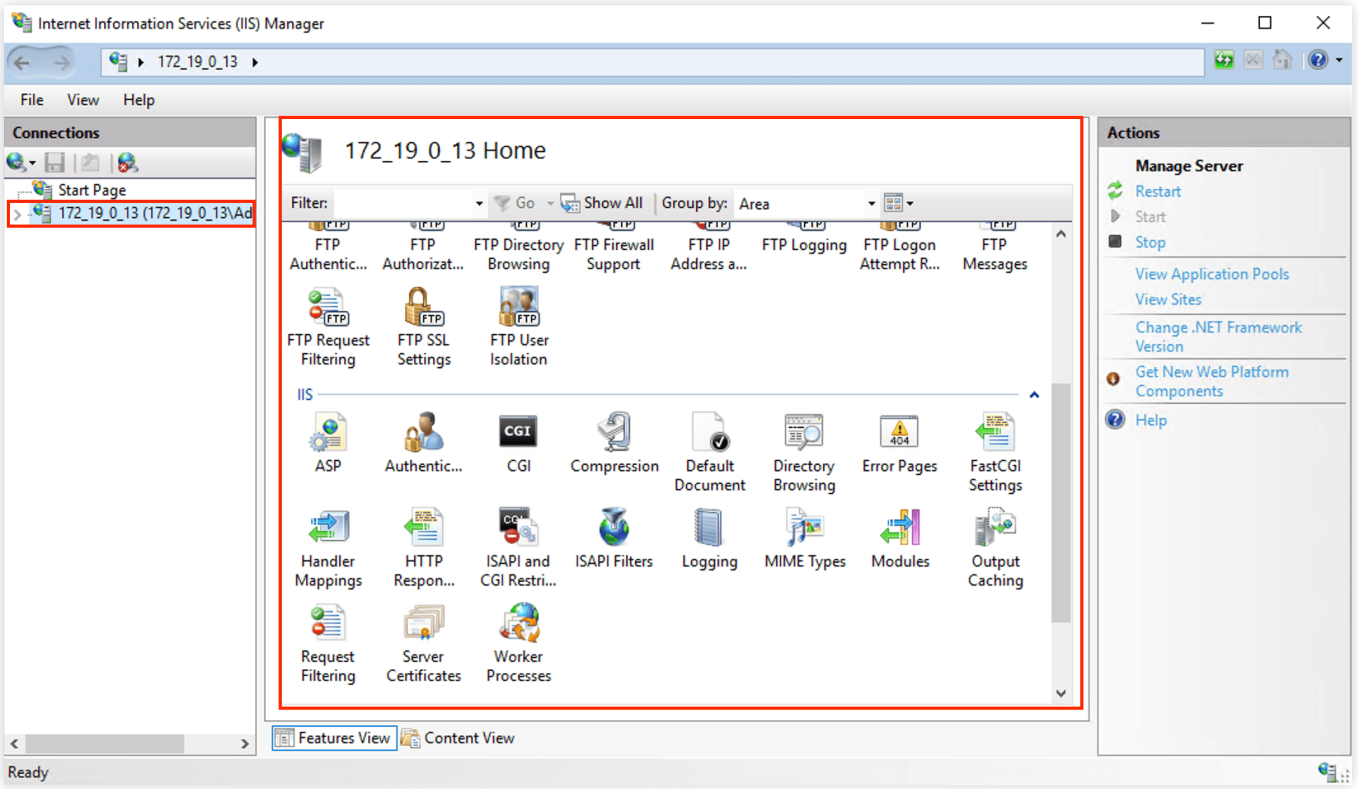
1. Unzip the downloaded PHP zip installation package. For example, unzip to C:\PHP directory.
2. Copy the php.ini-production file from the C:\PHP directory, change its file extension to .ini , and rename it to php.ini .



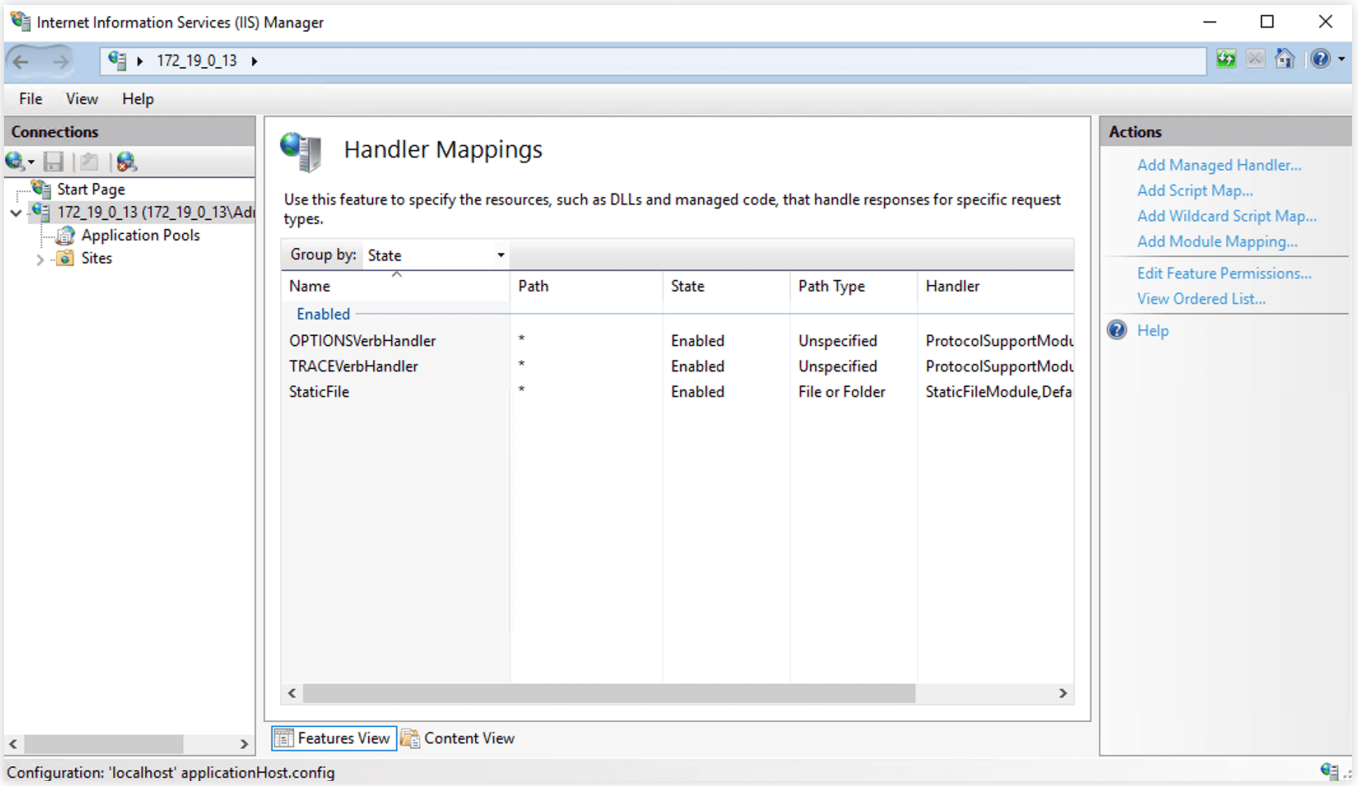
3. On the operating system interface, click to open Server Manager.
4. In the left sidebar of Server Manager, click IIS.
5. In the right-side IIS management window, right-click the server name under the Server section and select Internet Information Services (IIS) Manager.



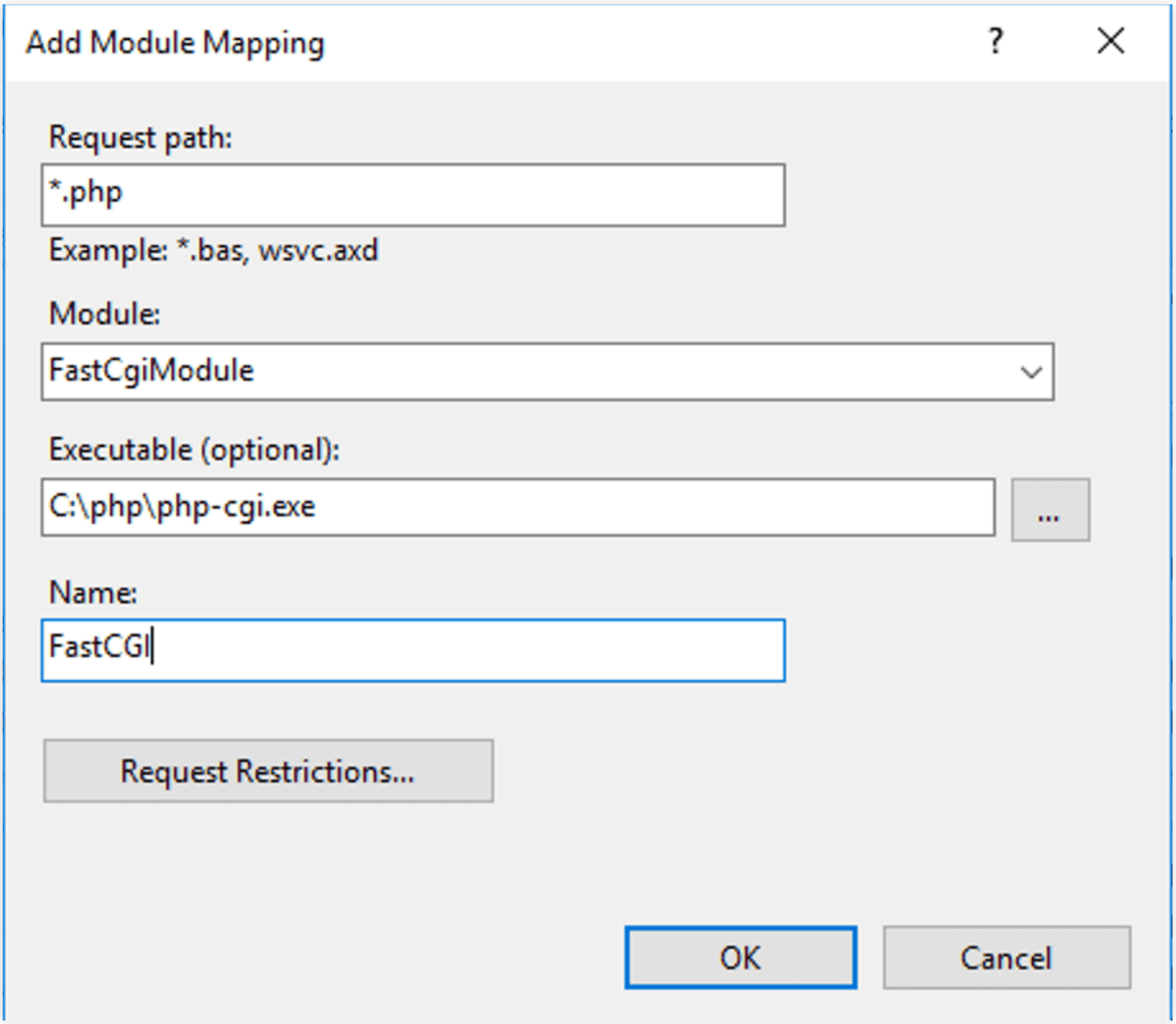
6. In the opened Internet Information Services (IIS) Manager window, click the server name in the left side bar to go to the server's homepage.
   For example, click the 10_141_9_72 server name to enter the 10_141_9_72 homepage.



7. On the 10_141_9_72 Homepage, double-click Handler Mapping to go to the Handler Mapping management interface.



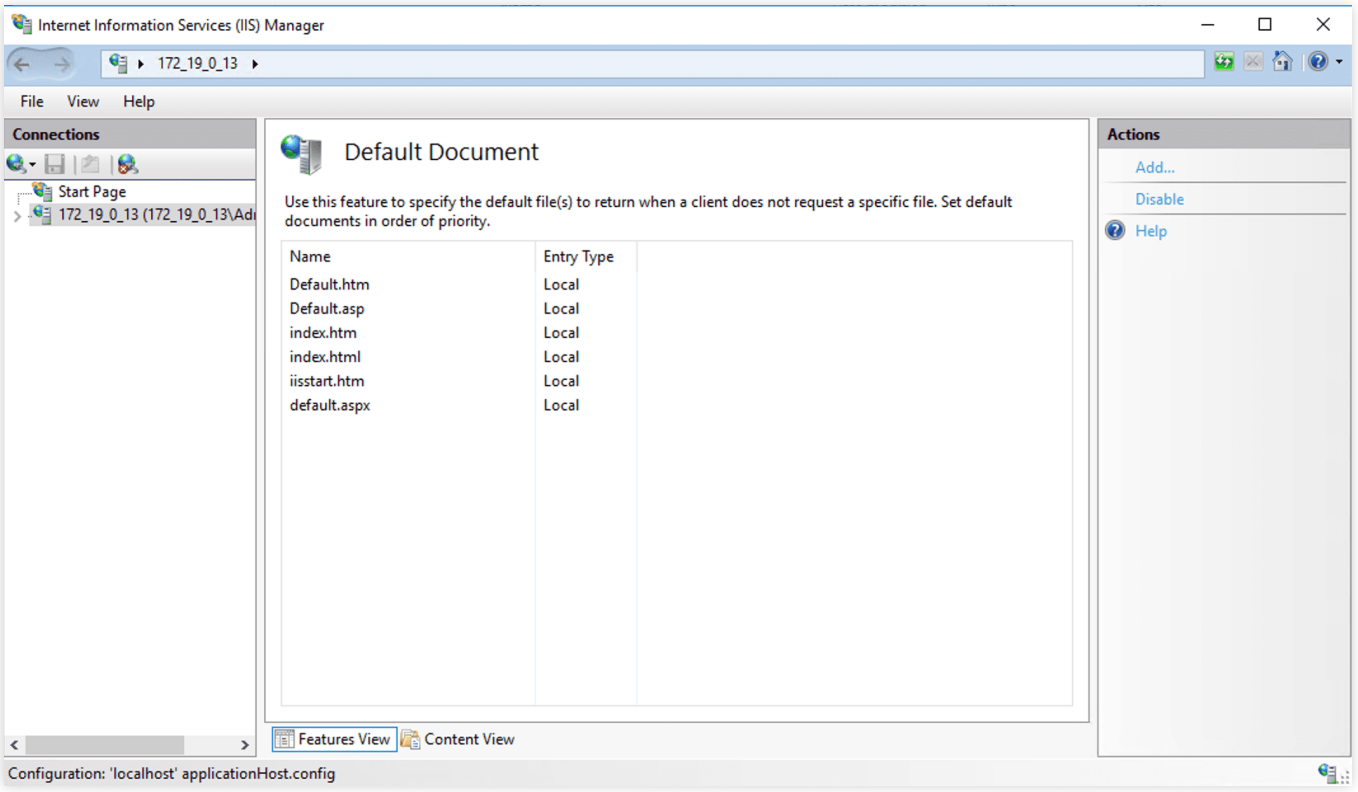
8. In the Operation column on the right, click Add Module Mapping to open the Add Module Mapping window.
9. In the opened Add Module Mapping window, fill in the following information and click OK.



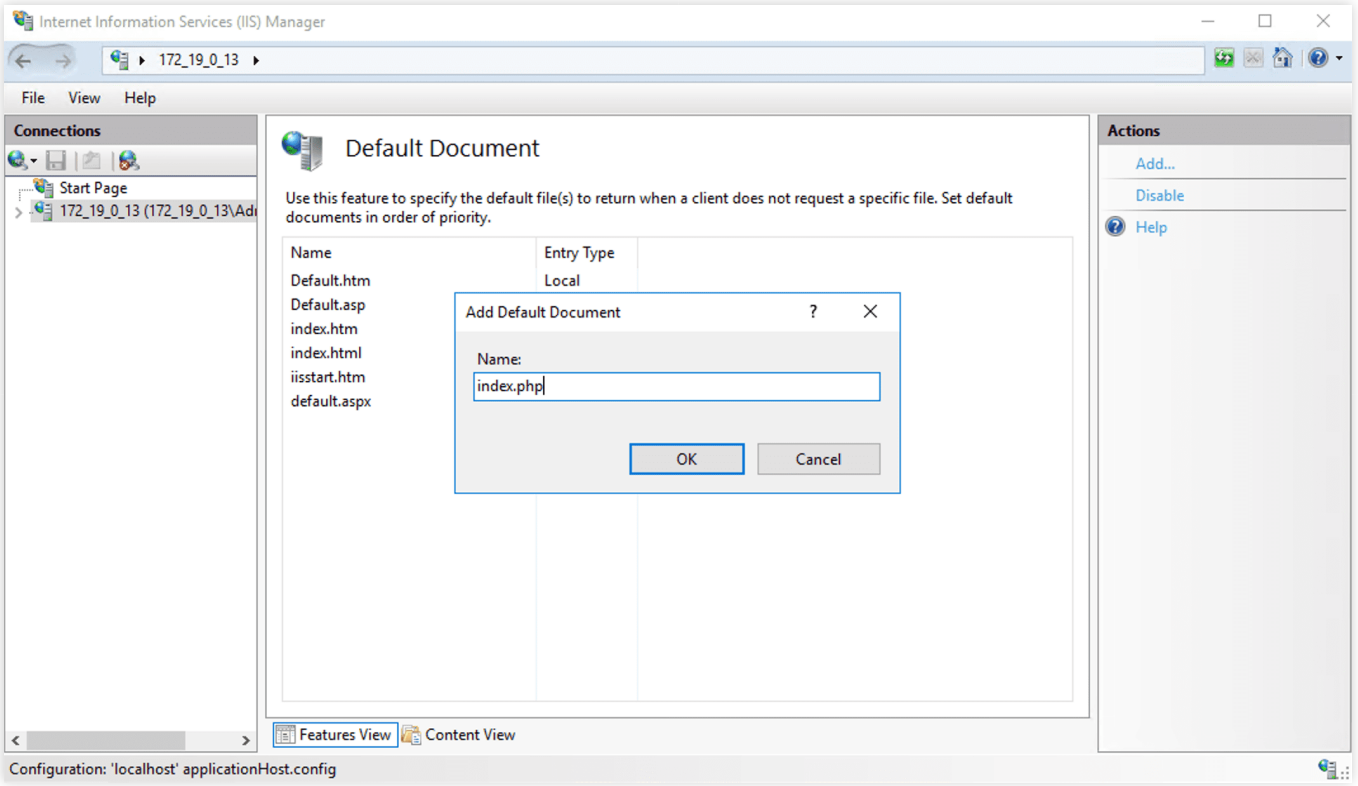
The main parameter information is as follows:

- Request path: Enter *.php .
- Module: Select FastCgiModule.
- Executable file: Select the php-cgi.exe file in the PHP zip installation package, that is, C:\PHP\php-cgi.exe .
- Name: Custom. For example, enter FastCGI.

10. In the pop-up dialog box, click Yes.
11. Click the 10_141_9_72 server name in the left sidebar to return to the 10_141_9_72 homepage.
12. On the 10_141_9_72 Homepage, double-click Default Document to go to the Default Document management interface.

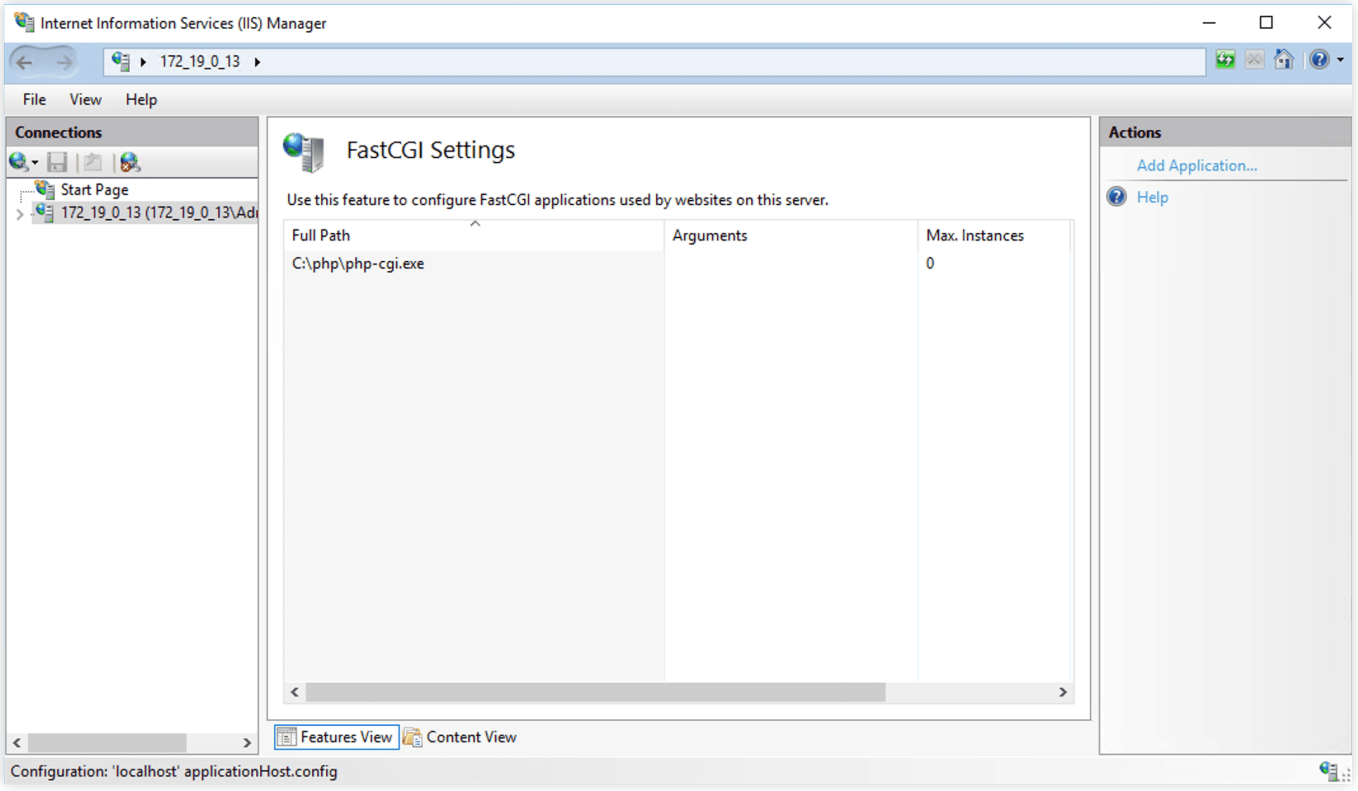


13. In the Operation column on the right, click Add to open the Add Default Document window.
14. In the opened Add Default Document window, enter index.php in the Name field and click OK.

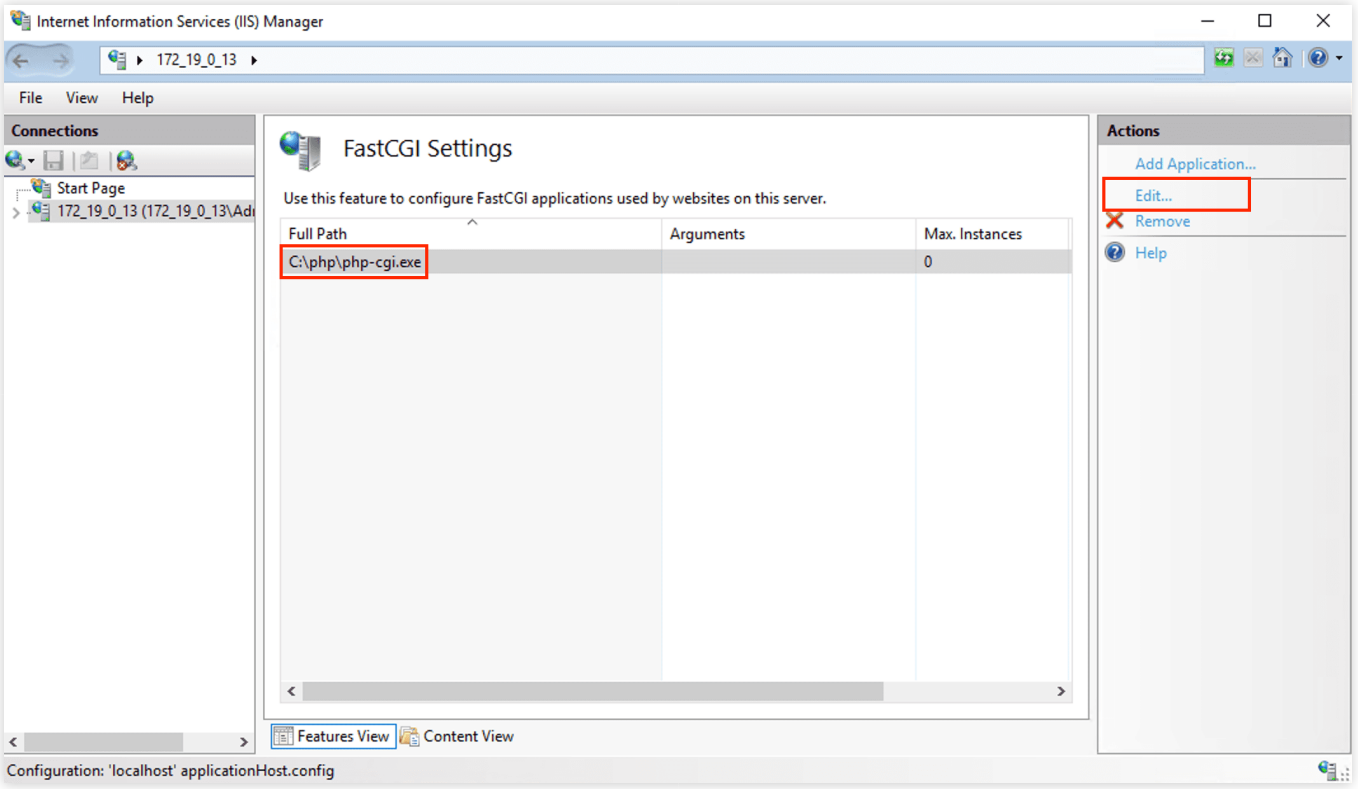


15. Click the 10_141_9_72 server name in the left sidebar to return to the 10_141_9_72 homepage.
16. On the 10_141_9_72 Homepage, double-click FastCGI Settings to go to the FastCGI Settings management

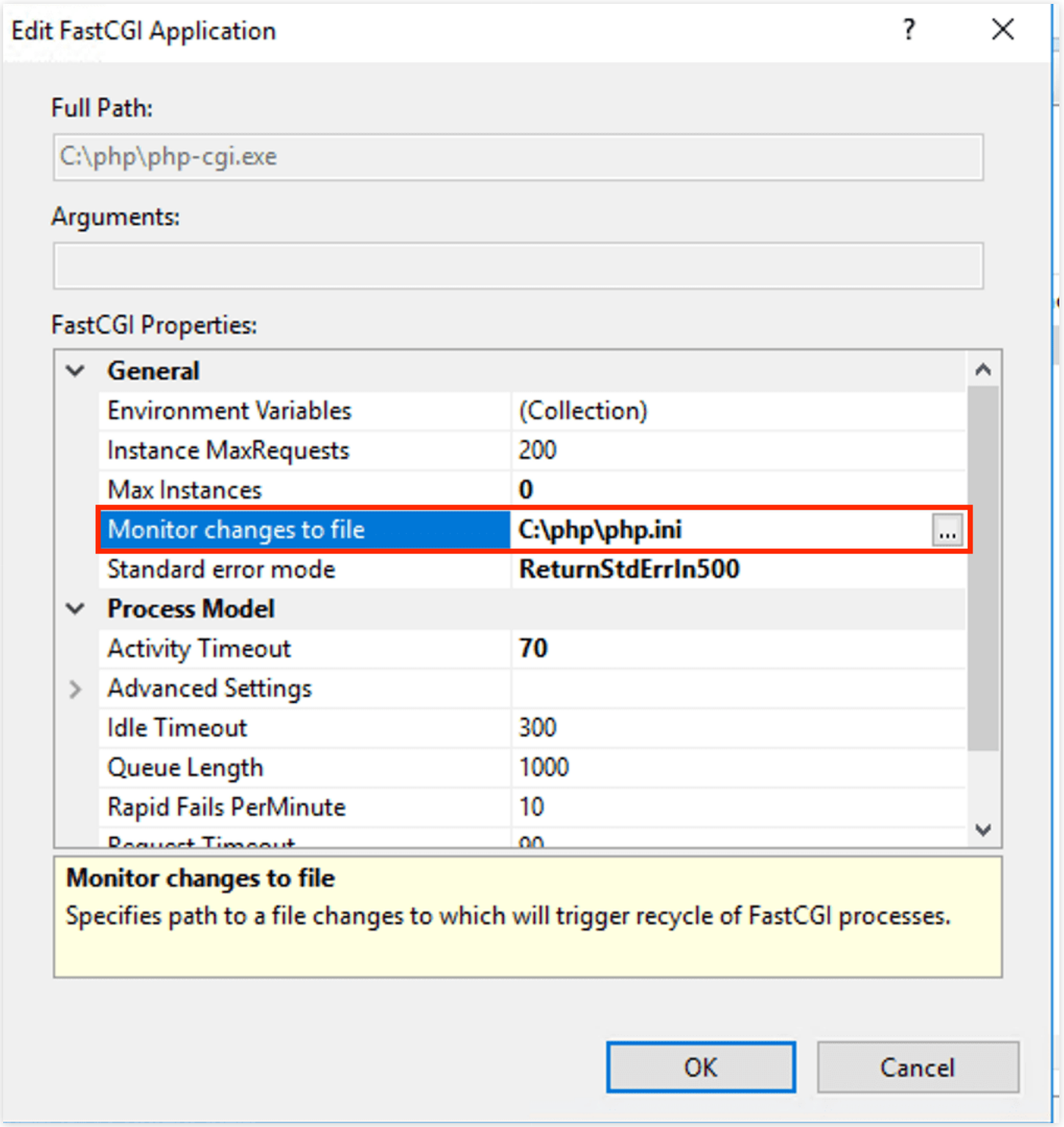
interface.



17. On the FastCGI Settings management interface, select the FastCGI application and click Edit.



18. In the opened Edit FastCGI Application window, set Monitor Changes to File to the path of the php.ini file.

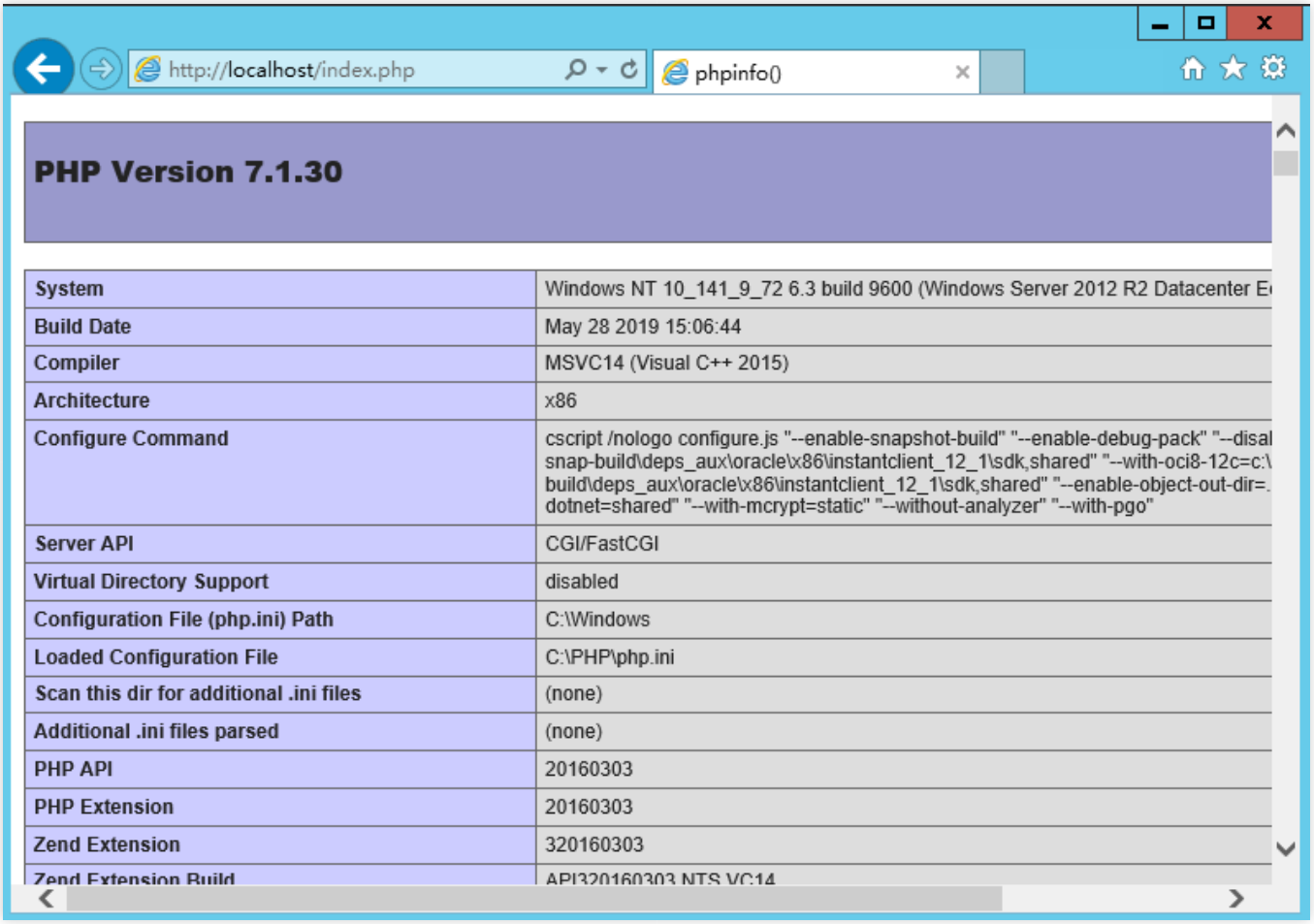


19. In the C:\inetpub\wwwroot directory, create a PHP file. For example, create an index.php file.
20. In the newly created index.php file, enter the following content and save.

```
<?php
phpinfo();
?>
```

21. On the operating system interface, open a browser and visit http://localhost/index.php , to check whether the environment configuration is successful.

If the opened page is as follows, the configuration is successful:



Step 3: Install MySQL Database

Scenarios

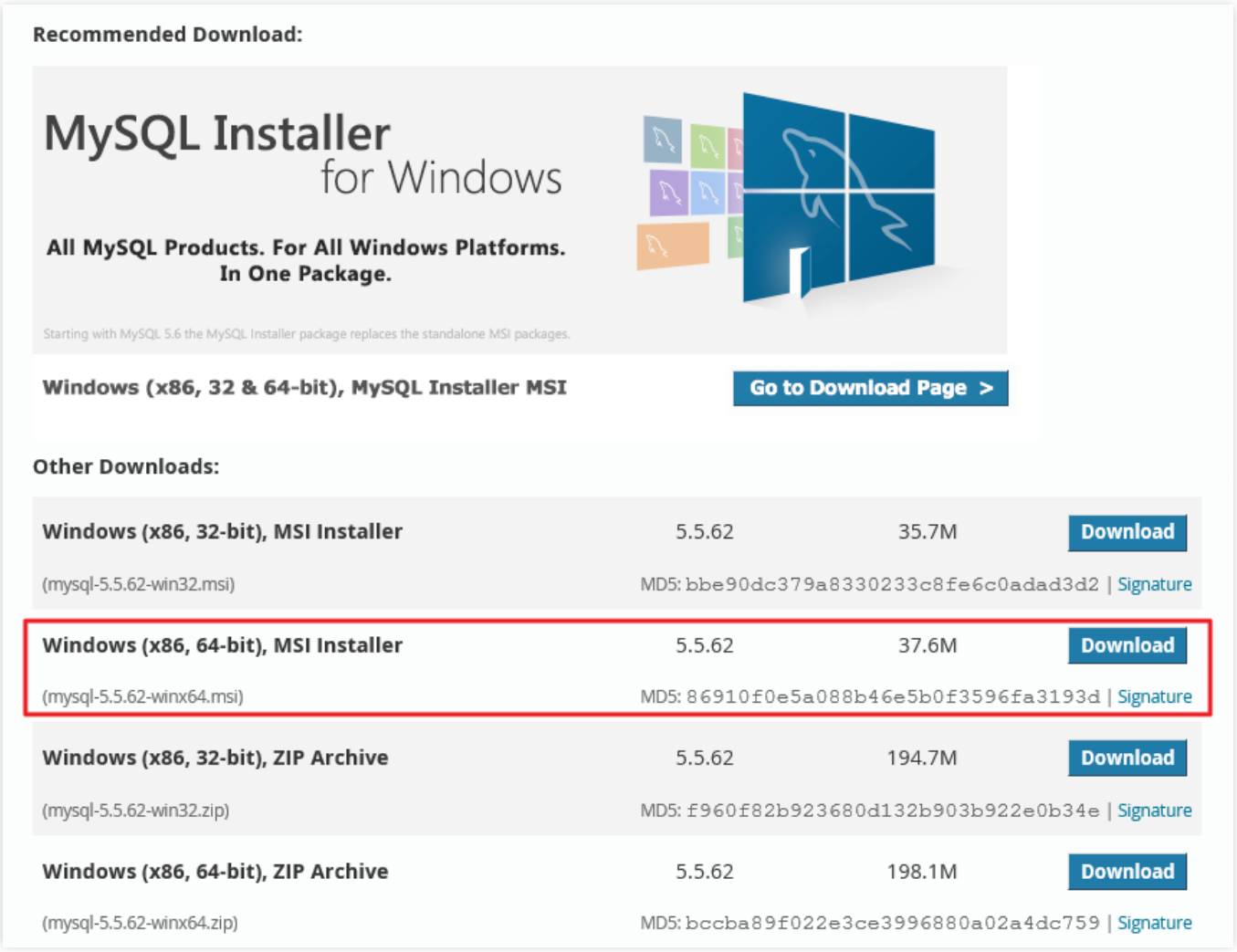
This document takes the Windows Server 2012 R2 IDC 64-bit operating system Cloud Virtual Machine as an example to introduce the specific steps for building MySQL 5.5.

Normally, Windows systems often use SQL Server databases. However, since SQL Server is a paid product, you need to authorize it yourself.

Operation Steps

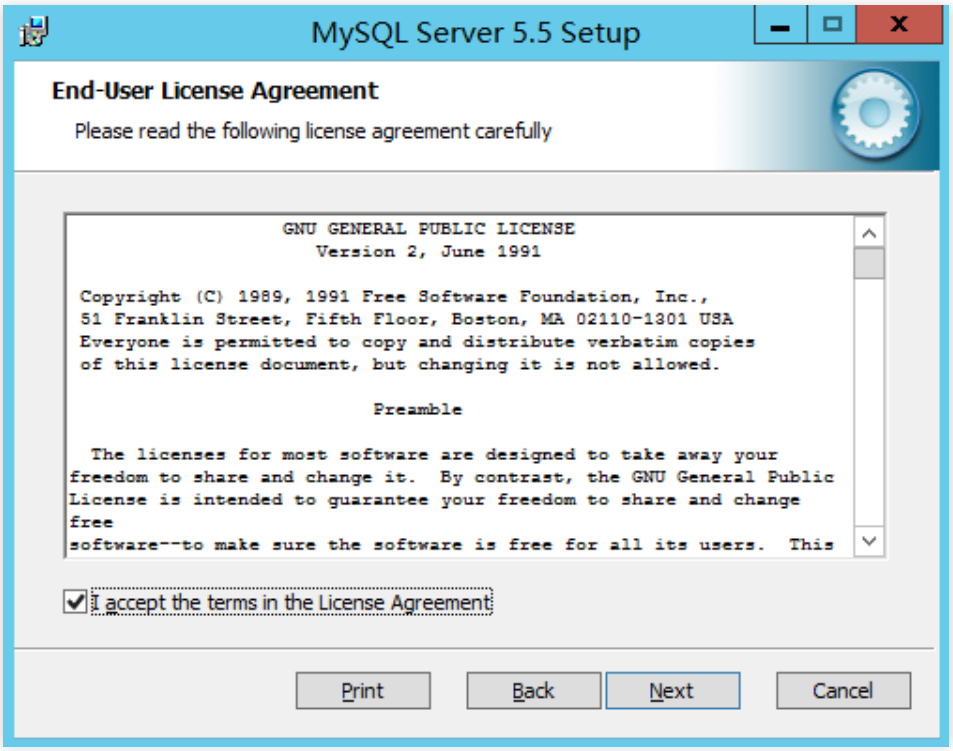
Downloading MySQL Installation Package

1. Log in to the Cloud Virtual Machine (CVM).
2. Open a browser on the CVM and visit https://dev.mysql.com/downloads/mysql/5.5.html#downloads to download the MySQL installation package.



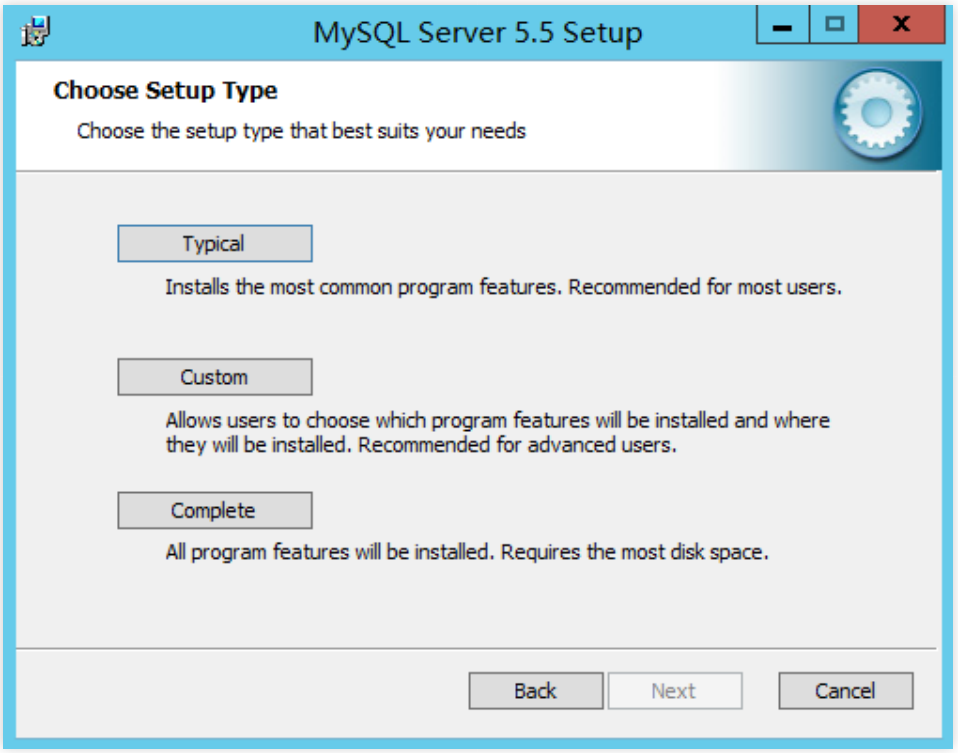
Installing MySQL

1. Double click to open the MySQL installation package, and click Next on the MySQL Server 5.5 Setup installation interface.
2. Check I accept the terms in the License Agreement, then click Next.

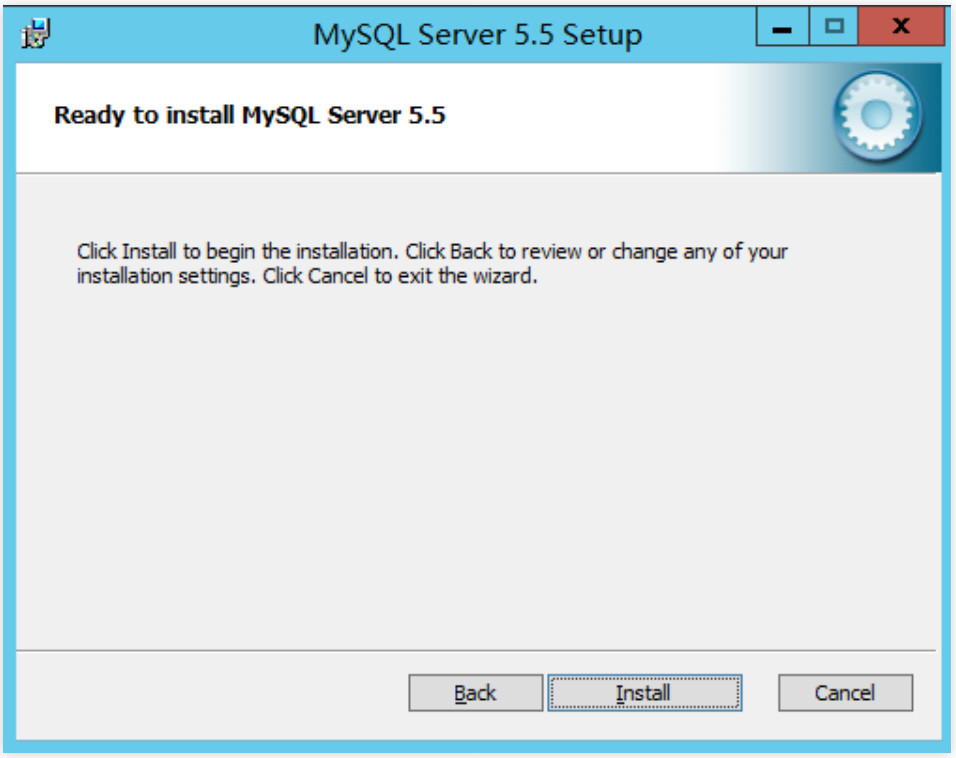


3. click Typical.

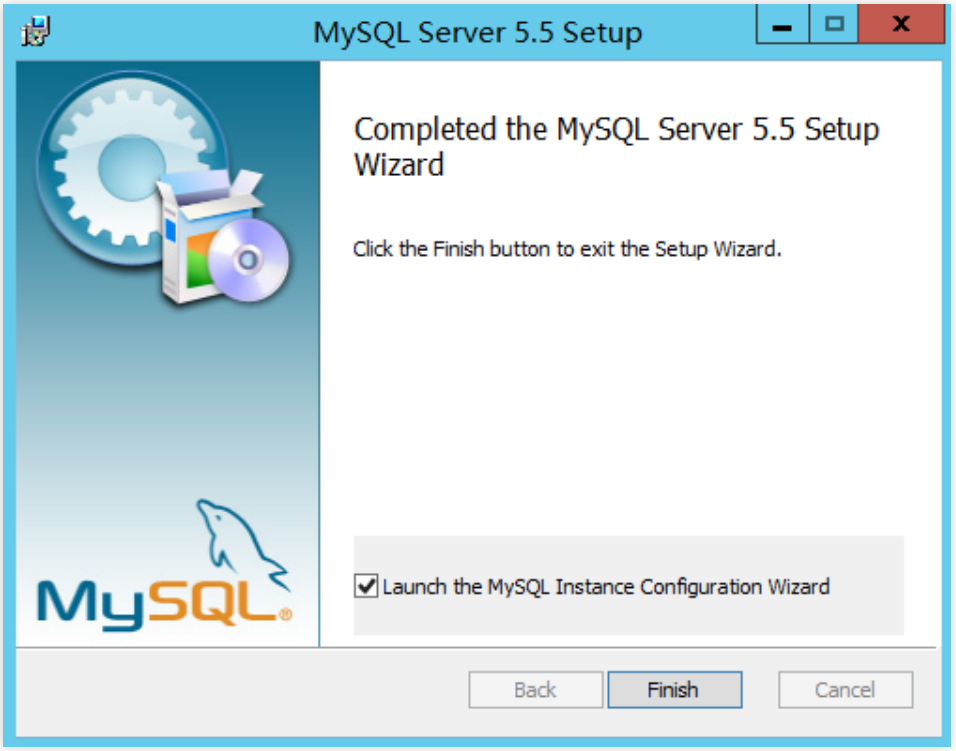
   Typical indicates a typical installation method.



4. Click Install to install MySQL.

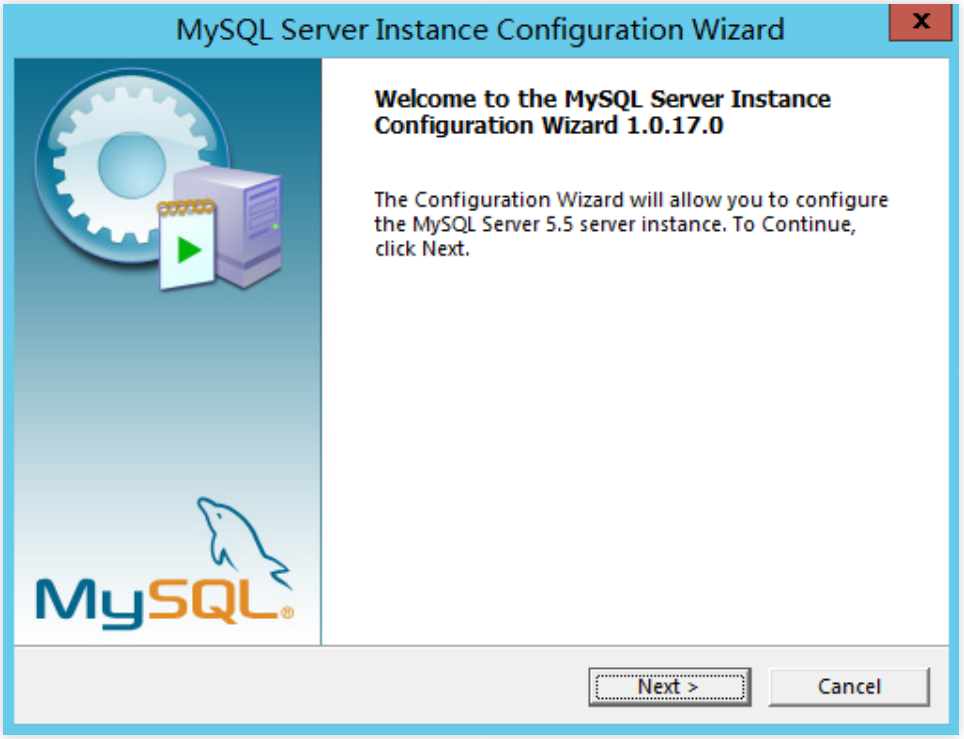


5. Select Launch the MySQL Instance Configuration Wizard and click Finish.
   Close the MySQL installation window and enter the MySQL Configuration Wizard interface.



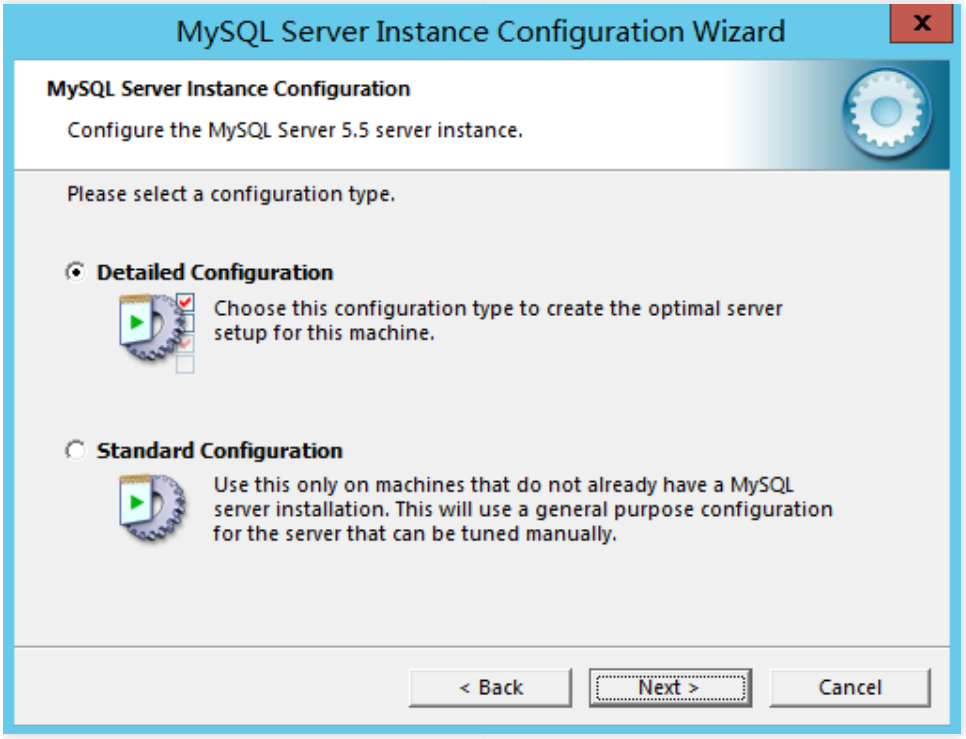
Configuring MySQL

1. In the MySQL Configuration Wizard interface, click Next.



2. Select Detailed Configuration, then click Next.

> Note: This direction takes Detailed Configuration as an example.

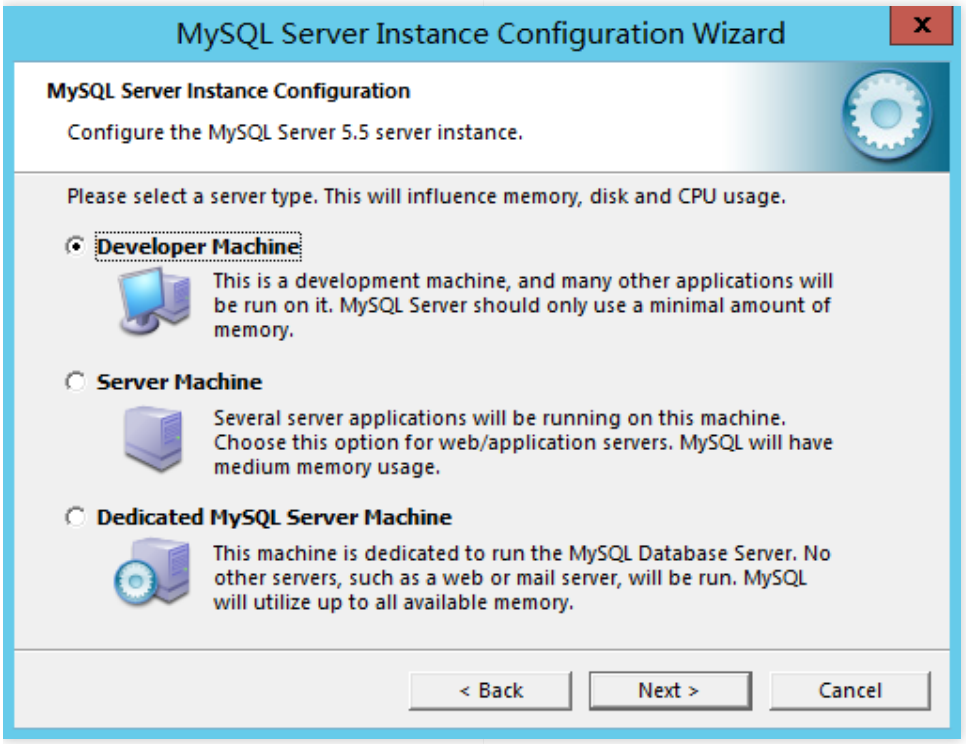


- Detailed Configuration is suitable for advanced users who want more fine-grained control over server

configuration.

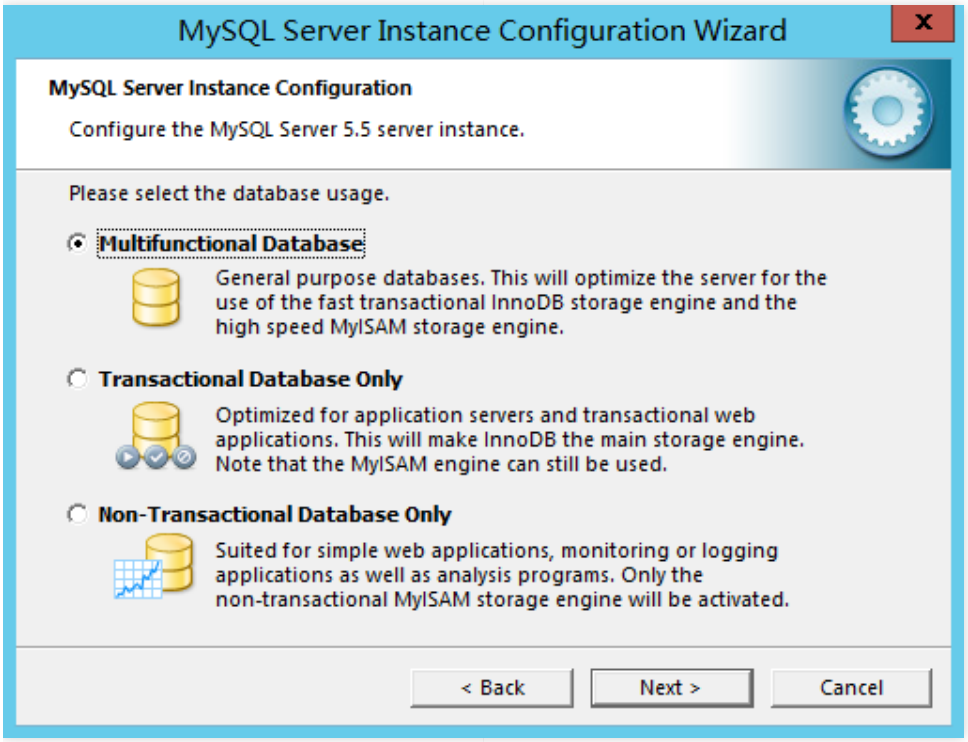
- Standard Configuration is suitable for new users who want to start MySQL quickly without worrying about server configuration. However, the standard configuration may not be compatible with the operating system, so it is recommended that you choose the detailed configuration.

3. Select Developer Machine, then click Next. > Note: This direction takes Developer Machine as an example.



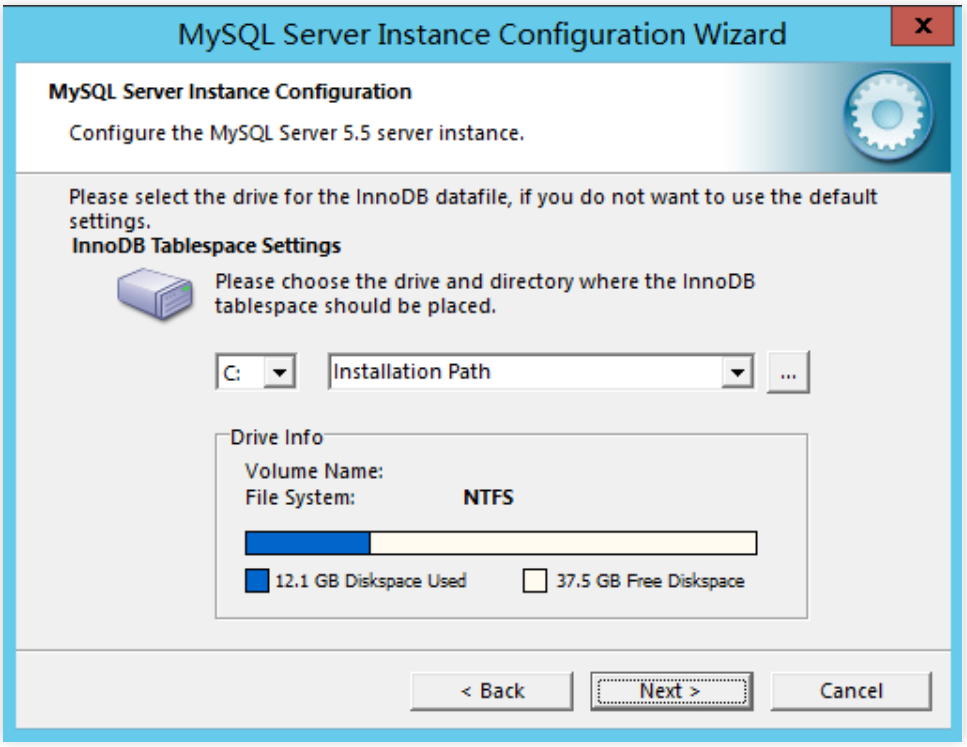
- Developer Machine refers to a typical personal desktop workstation. When running multiple desktop applications simultaneously, configure the MySQL server to use the least amount of resources.
- Server Machine, represents the server. The MySQL server can run alongside other applications, such as FTP, email, and web servers. The MySQL server is configured to occupy an appropriate proportion of resources.
- Dedicated MySQL Server Machine refers to a server that only runs the MySQL service. The MySQL server is configured to occupy all resources.

4. Select Multifunctional Database, then click Next. > Note: This directions takes Multifunctional Database as an example.

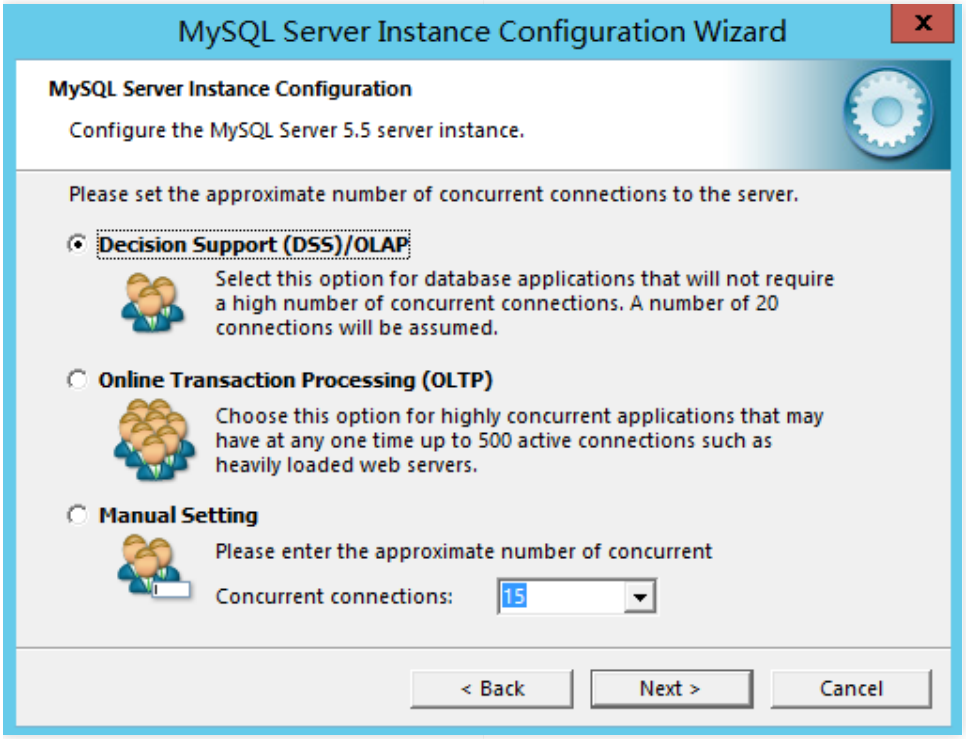


- Multifunctional Database uses both InnoDB and MyISAM storage engines and evenly distributes resources between the two engines. It is recommended that users who frequently use two storage engines select this option.
- Transactional Database Only uses both InnoDB and MyISAM storage engines and assigns most server resources to the InnoDB storage engine. It is recommended that users who frequently use InnoDB and occasionally use MyISAM select this option.
- Non-Transactional Database Only completely disables the InnoDB storage engine and assigns all server resources to the MyISAM storage engine. It is recommended that users who do not use InnoDB select this option.

5. Keep the default settings, then click Next.



6. Select Decision Support (DSS)/OLAP, then click Next. > Note: This direction takes Decision Support (DSS)/ OLAP as an example.

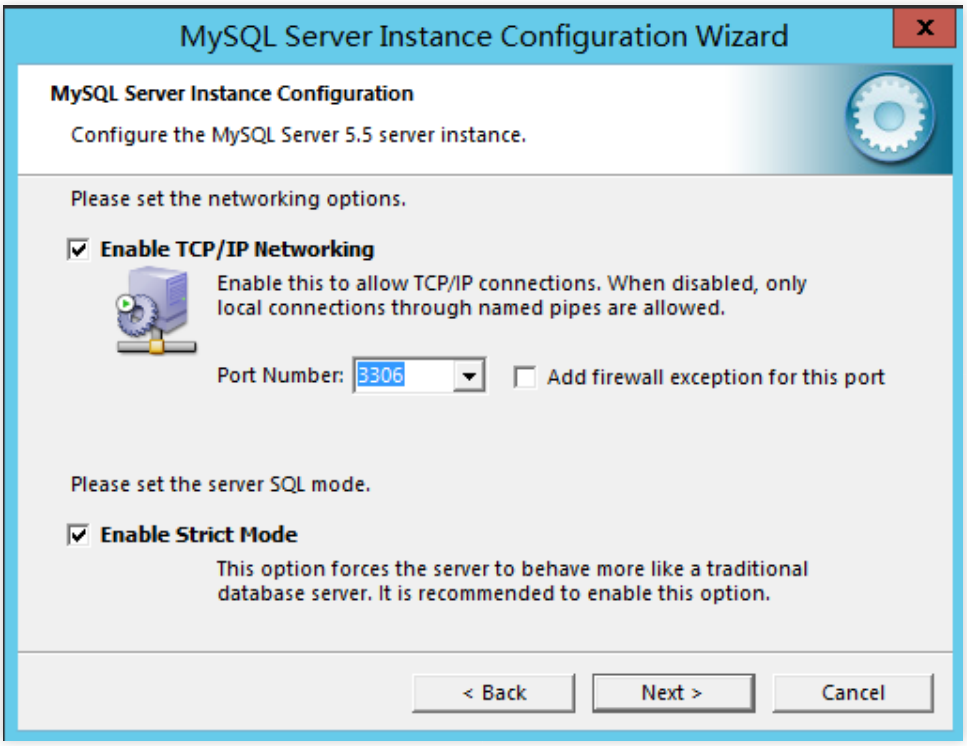


- Decision Support (DSS)/OLAP is suitable for situations that do not require a large number of parallel connections.
- Online Transaction Processing (OLTP) is suitable for situations that require a large number of parallel

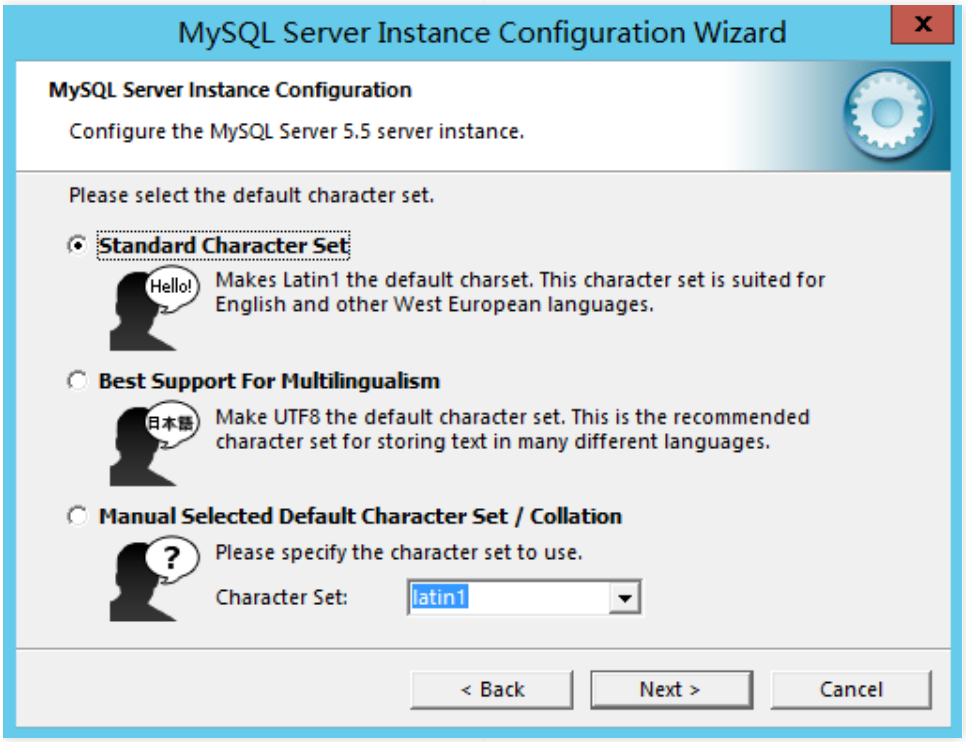
connections.

- Manual Setting is suitable for manually setting the maximum number of parallel connections to the server.

7. Set up the TCP/IP network, configure the port number for connecting to the MySQL server, then click Next. Note:
   - TCP/IP networking is enabled by default.
   - By default, port 3306 is used.

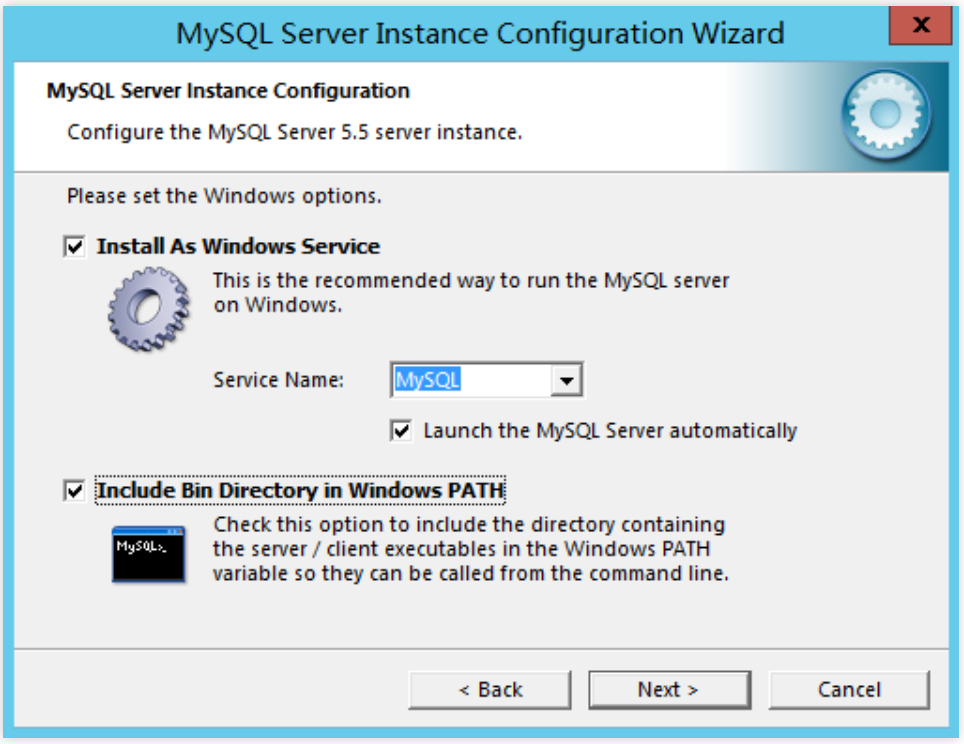


8. Select Standard Character Set, then click Next. > Note: This direction takes Standard Character Set as an example.

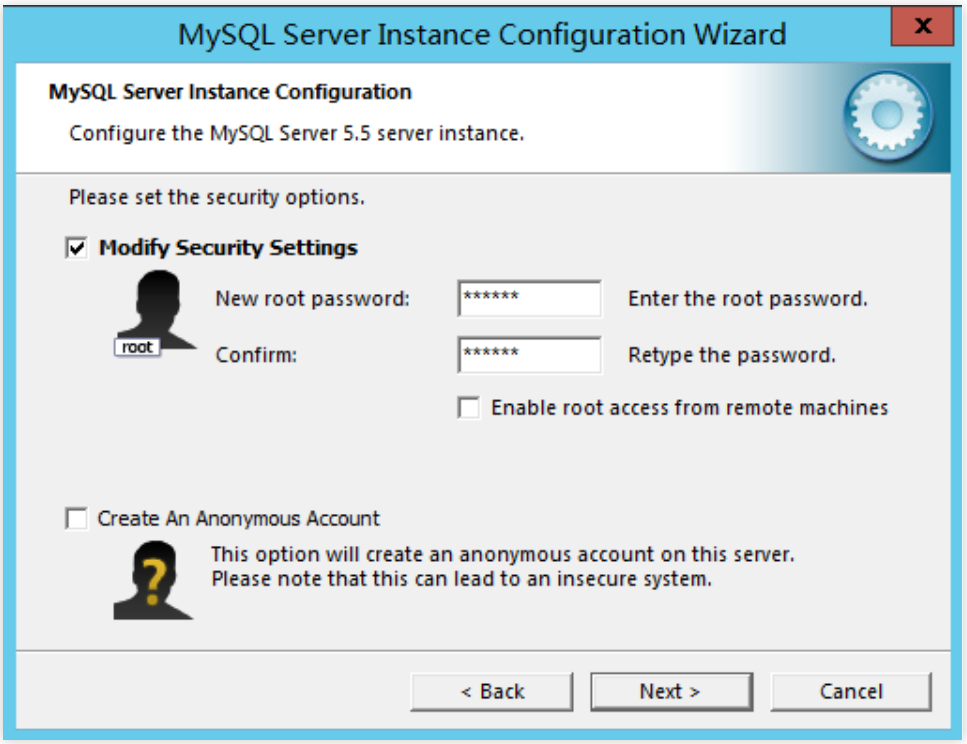


- Standard Character Set uses Latin1 as the server character set by default.
- Best Support For Multilingualism uses UTF8 as the server character set by default.
- Manual Selected Default Character Set/Collation, selects the desired character set from the drop-down list.

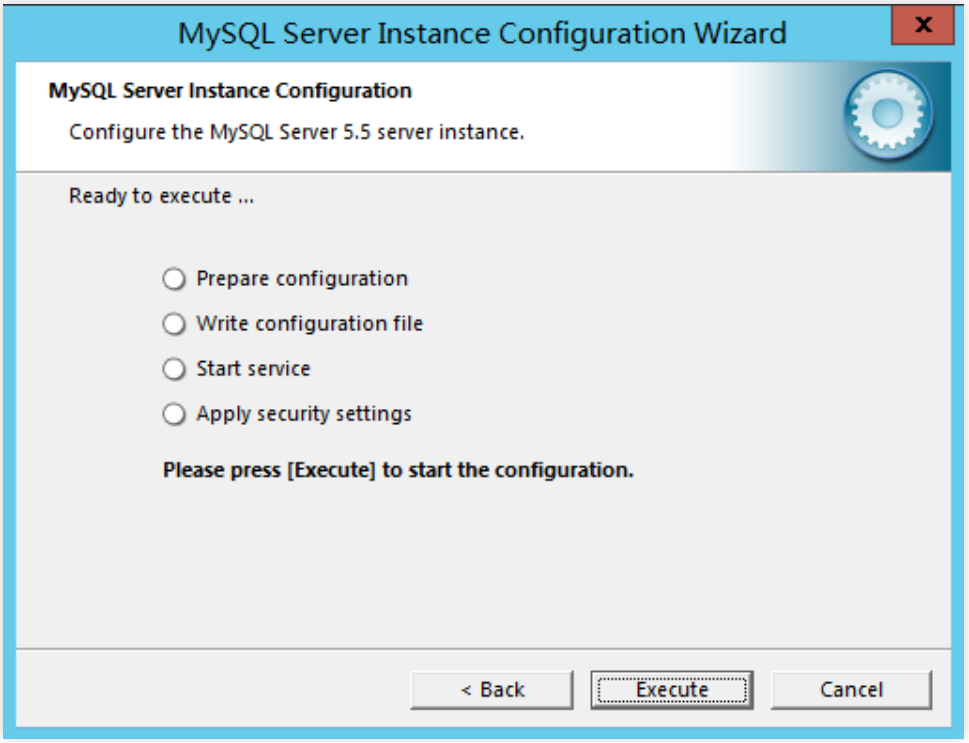
9. Check Install As Windows Service and Include Bin Directory in Windows PATH, then click Next.



10. Set the root password, then click Next.



11. Click Execute to configure MySQL.



12. Click Finish to complete the configuration.

Verifying Whether MySQL Installed Successfully

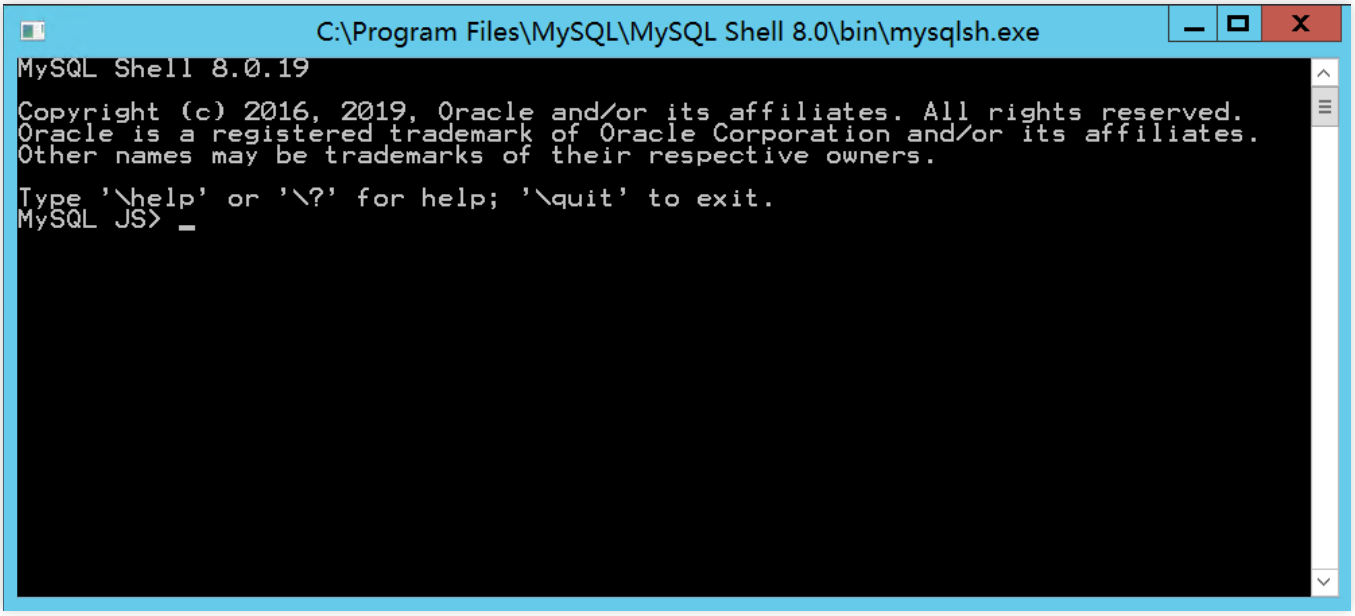
1. In the operating system interface, right click > Run to open the Run box.

2. In the Run box, enter cmd, and press Enter to open the Administrator Command box.

3. In the Administrator Command box, execute the following command.

   mysql -u root -p

4. Enter the root password you set and press Enter to log in to MySQL.
   If the following interface information is displayed, the installation and configuration are successful.



NTP Service Overview

Network Time Protocol (NTP) is a protocol used to sync the time of computers in a network. Its purpose is to sync the computer's clock to Universal Time Coordinated (UTC).

Converge Cloud provides an private network NTP server for Converge Cloud intranet devices to use. For non-Converge Cloud devices, you can use the public network NTP server provided by Converge Cloud.

Private Network NTP Server

ntpupdate.convergecloud.com

Public Network NTP Server

time1.convergecloud.com
time2.convergecloud.com
time3.convergecloud.com
time4.convergecloud.com
time5.convergecloud.com

- For details on how to set up the NTP clock source server for the Linux system, see Set NTP Service in Linux Instance.
- For details on how to set up the NTP clock source server in Windows system, see Set NTP Service in Windows Instance.

Set NTP Service in Linux Instance

Overview

The Network Time Protocol daemon (NTPD) is a daemon of the Linux operating system. It is used to correct the time between the local system and the clock source server and fully implements the NTP protocol. The difference between NTPD and NTPDate is that NTPD gradually corrects the time in a step-by-step manner without any time jump, while NTPDate is a breakpoint update. This document takes the CentOS7.5 operating system Cloud Virtual Machine as an example to introduce how to install and use NTPD.

Notes

- Some operating systems use chrony as the default NTP service. Make sure that NTPD is running and set to start at boot.
- Use systemctl is-active ntpd.service command to check whether NTPD is running.
- Use systemctl is-enabled ntpd.service command to check whether NTPD starts up at boot.
- The communication port of the NTP service is UDP 123. Before you set up the NTP service, make sure that you have opened UDP port 123.
  If the port is not open, see Add Security Group Rules to allow access.

Directions

Installing NTPD

Execute the following command to check whether NTPD is installed.

```
rpm -qa | grep ntp
```

- If the result resembles the following is returned, NTPD has been installed.

```
[root@VM_16_2_centos ~]# rpm -qa | grep ntp
ntpdate-4.2.6p5-28.el7.centos.x86_64
ntp-4.2.6p5-28.el7.centos.x86_64
fontpackages-filesystem-1.44-8.el7.noarch
```

  Determine whether ntpd is installed

- If NTPD is not installed, use yum install ntp to install NTPD.

  yum -y install ntp

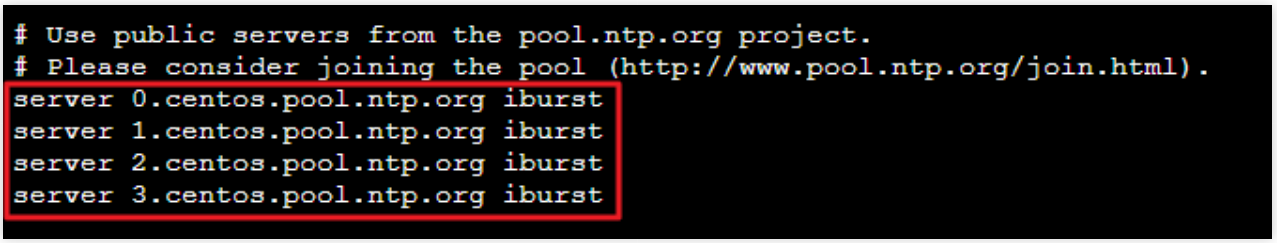
By default, NTPD runs in client mode.

Configure NTP

1. Execute the following command to open the NTP service configuration file.

   vi /etc/ntp.conf

2. Press i to switch to the edit mode, find the server-related configuration, modify the server to the target NTP clock source server you need to set, and delete the NTP clock source server that is not needed temporarily. As shown below:



   Server settings

3. Press Esc, enter :wq to save the file and return.

Start NTPD

Execute the following command to restart the NTPD service.

systemctl restart ntpd.service

Check NTPD Status

According to actual needs, execute the following different commands to check the NTPD status.

- Execute the following command to check whether the NTP service port UDP port 123 is being monitored

normally.

netstat -nupl

If the result resembles the following is returned, the monitoring is normal.

```
[root@VM_0_136_centos ~]# netstat -nupl
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
udp        0      0 172.30.0.136:123        0.0.0.0:*                           999/ntpd
udp        0      0 127.0.0.1:123           0.0.0.0:*                           999/ntpd
udp6       0      0 fe80::5054:ff:fec2::123 :::*                                999/ntpd
udp6       0      0 ::1:123                 :::*                                999/ntpd
[root@VM_0_136_centos ~]#
```

netstat -nupl

- Execute the following command to check whether the NTPD status is normal.

  service ntpd status

If the result resembles the following is returned, the NTPD status is normal.

```
[root@VM_0_136_centos ~]# service ntpd status
Redirecting to /bin/systemctl status ntpd.service
● ntpd.service - Network Time Service
   Loaded: loaded (/usr/lib/systemd/system/ntpd.service; enabled; vendor preset: disabled)
   Active: active (running) since Wed 2019-08-07 15:23:25 CST; 5min ago
  Process: 997 ExecStart=/usr/sbin/ntpd -u ntp:ntp $OPTIONS (code=exited, status=0/SUCCESS)
 Main PID: 999 (ntpd)
   CGroup: /system.slice/ntpd.service
           └─999 /usr/sbin/ntpd -u ntp:ntp -g

Aug 07 15:23:25 VM_0_136_centos ntpd[999]: 0.0.0.0 c01d 0d kern kernel time sync enabled
Aug 07 15:23:25 VM_0_136_centos ntpd[999]: ntp_io: estimated max descriptors: 1024, initia... 16
Aug 07 15:23:25 VM_0_136_centos ntpd[999]: Listen normally on 0 lo 127.0.0.1 UDP 123
Aug 07 15:23:25 VM_0_136_centos ntpd[999]: Listen normally on 1 eth0 172.30.0.136 UDP 123
Aug 07 15:23:25 VM_0_136_centos ntpd[999]: Listen normally on 2 lo ::1 UDP 123
Aug 07 15:23:25 VM_0_136_centos ntpd[999]: Listen normally on 3 eth0 fe80::5054:ff:fec2:11...123
Aug 07 15:23:25 VM_0_136_centos ntpd[999]: Listening on routing socket on fd #20 for inter...tes
Aug 07 15:23:25 VM_0_136_centos ntpd[999]: 0.0.0.0 c016 06 restart
Aug 07 15:23:25 VM_0_136_centos ntpd[999]: 0.0.0.0 c012 02 freq_set kernel 0.467 PPM
Aug 07 15:23:34 VM_0_136_centos ntpd[999]: 0.0.0.0 c615 05 clock_sync
Hint: Some lines were ellipsized, use -l to show in full.
[root@VM_0_136_centos ~]#
```

ntpd status

- Execute the following command to check whether NTP is started normally and whether it is configured to the correct NTP clock source server.

  ntpstat

Output the IP address of the current NTP clock source server. This IP address should be the IP address of the NTP clock source server configured above. As shown below:

```
[root@VM_0_136_centos ~]# ntpstat
synchronised to NTP server (185.[illegible]) at stratum 3
   time correct to within 1060 ms
   polling server every 64 s
[root@VM_0_136_centos ~]#
```

You can also execute nslookup domain name command to obtain the IP address corresponding to the domain name.

- Execute the following command to obtain more detailed NTP service information.

  ntpq -p

The result resembles the following is returned:

```
[root@VM_0_136_centos ~]# ntpq -p
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
 108.[illegible]  .INIT.          16 u    -   64    0    0.000    0.000   0.000
 193.[illegible]  194.[illegible]  2 u    6   64   17  277.831    3.940   5.588
*185.[illegible]  194.[illegible]  2 u   68   64   16  201.280    1.729   0.263
 193.[illegible]  194.[illegible]  2 u   69   64   16  293.382    1.003   0.441
 169.[illegible]  100.[illegible]  2 u    3   64   17    6.607    9.897   0.461
[root@VM_0_136_centos ~]#
```

- remote: The name of the NTP server that responded to this request.
- refid: The upper-level NTP server used by the NTP server.
- st: The level of the remote server. Servers are ranked from 1 to 16 from high to low. In order to reduce load and network congestion, it is generally recommended to avoid connecting directly to servers ranked 1.
- when: The number of seconds since the last successful request.
- poll: The interval at which the local machine and remote server are synchronized (in seconds). When NTP is initially run, the poll value will be relatively small and the frequency of sync with the server will increase. It is recommended to adjust to the correct time range as soon as possible. After adjustment, the poll value will gradually increase and the sync frequency will decrease accordingly.
- reach: The octal value, used to test whether the server can be connected. The reach value will increase with each successful connection.
- delay: The round trip time from the local machine to send sync requests to the NTP server.
- offset: The time offset between the host and the synchronized time source through NTP clock sync, in milliseconds (ms). The closer the offset value is to 0, the closer the time between the host and the NTP server is.
- jitter: The value used for statistics. Calculates the distribution of offsets in a specific number of consecutive

connections. That is, the smaller the absolute value of the jitter value is, the more accurate the host time is.

Set NTPD to Start at Boot

1. Execute the following command to set NTPD to start at boot.

   systemctl enable ntpd.service

2. Execute the following command to check whether chrony is set to start at boot.

   systemctl is-enabled chronyd.service

If chrony is set to start at boot, execute the following command to remove chrony from the startup.
The chrony conflicts with NTPD, which may cause NTPD to fail to start.

systemctl disable chronyd.service

Set NTP Service in Windows Instance

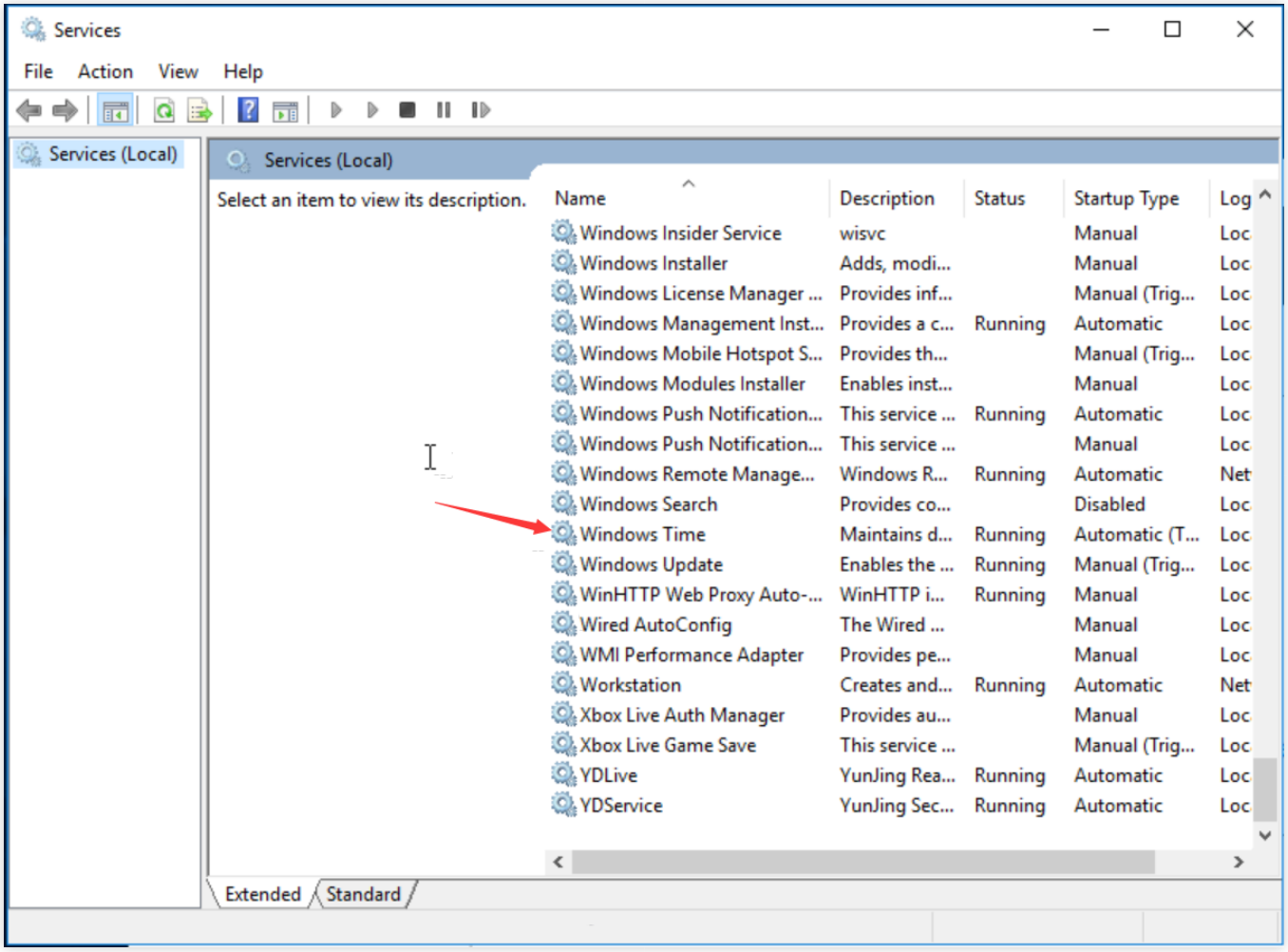
Overview

Windows Time service (W32Time) is used to sync the time between the local system and the clock source server, and uses the Network Time Protocol (NTP) to sync computer clocks on the network. This document takes the Windows Server 2012 operating system Cloud Virtual Machine as an example to describe how to enable the NTP service and change the address of the clock source server.

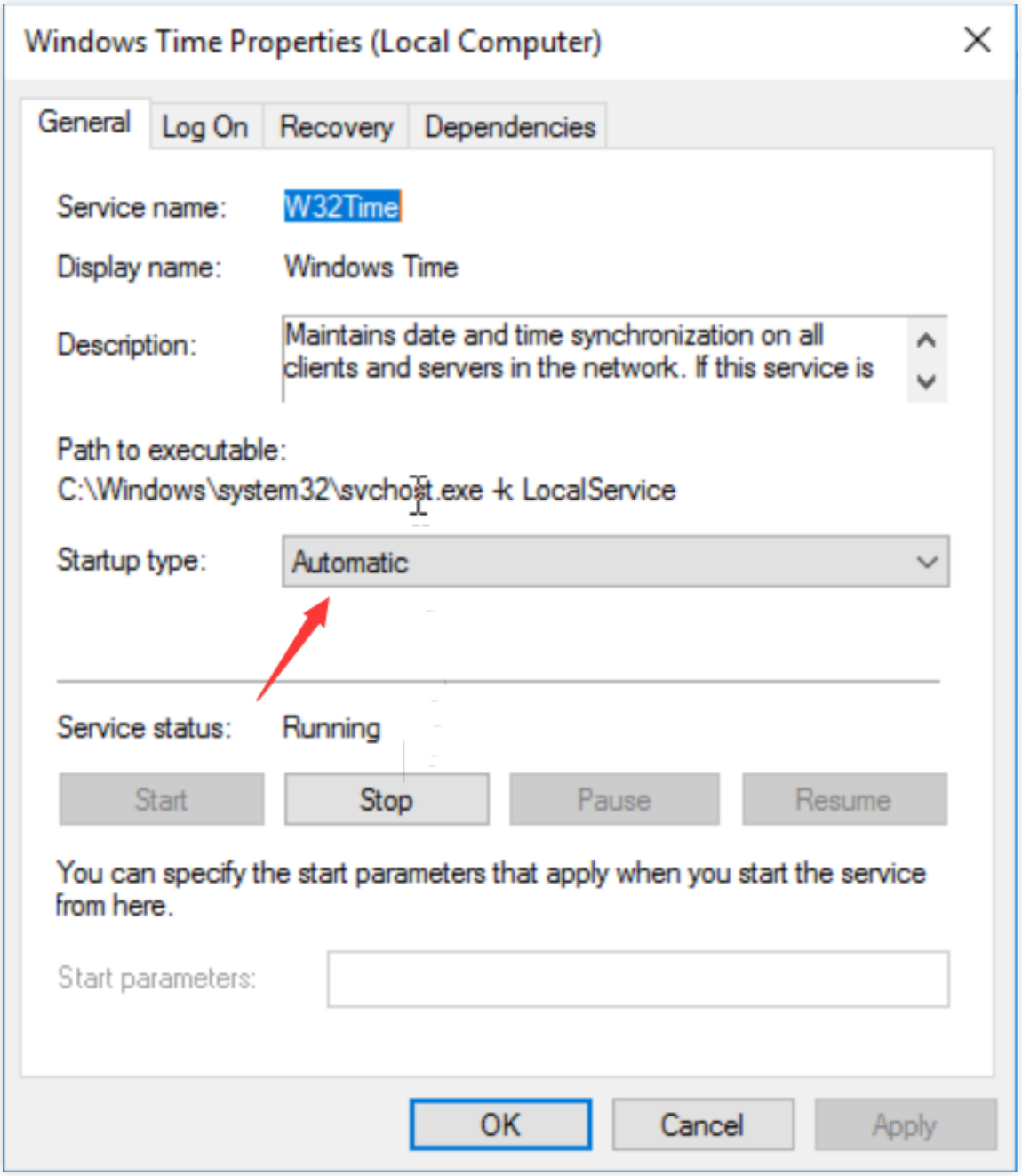
Directions

1. Log in to the Windows CVM.

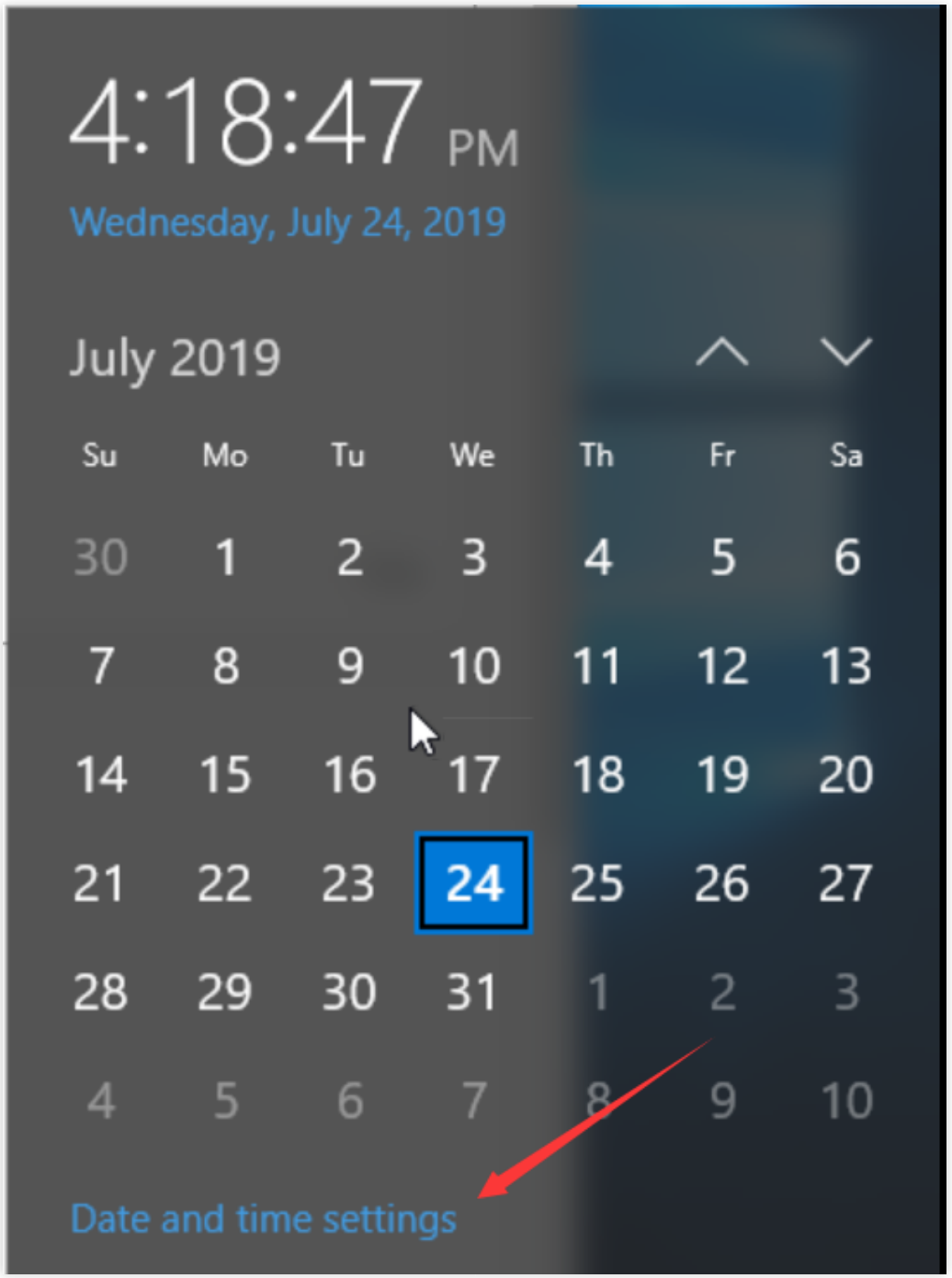
2. On the operating system interface, click > Management Tool > Service to open the Service window.
3. In the Service window, double click to open Windows Time. As shown below:



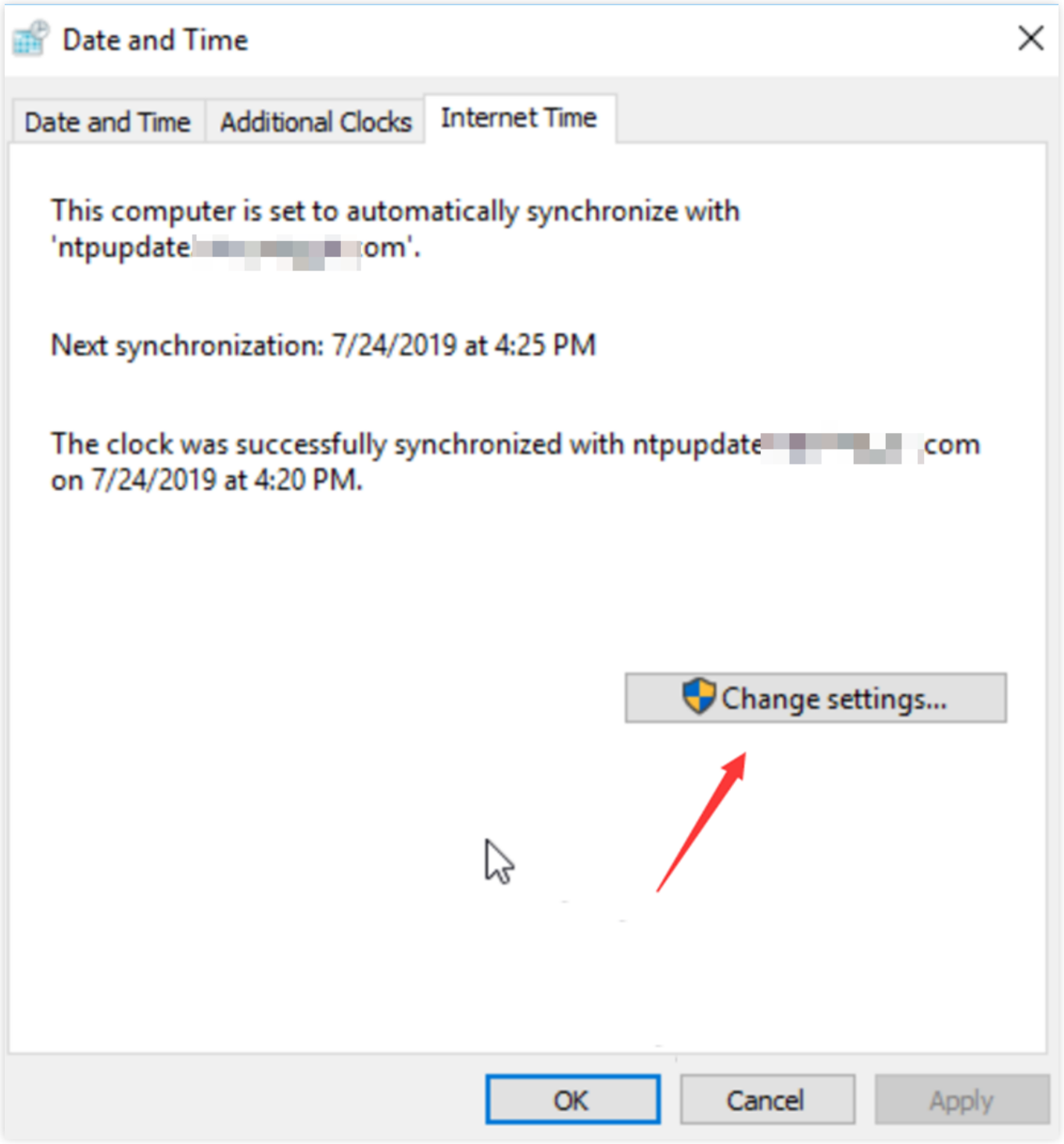
4. In the opened Windows Time Attribute (Local Computer) window, set Startup Type to Auto, set Service Status to Start, and click OK. As shown below:



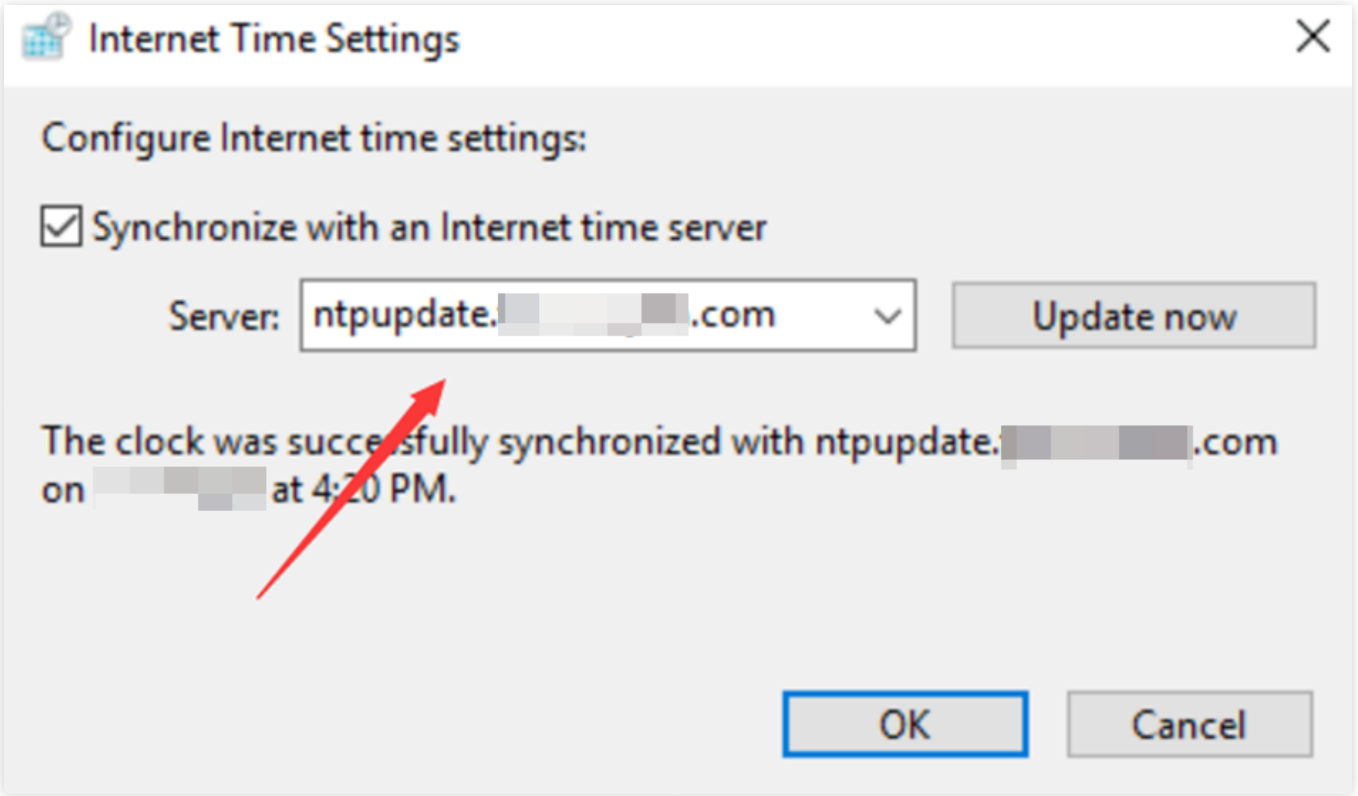
5. In the task column of the operating system interface, click Time > Change Date and Time Settings in the lower right corner. As shown below:



6. In the pop-up Date and Time window, select the Internet Time tab and click Change Settings. As shown below:



7. In the pop-up Internet Time Settings window, set Server to the domain name or IP address of the target clock source server, and click OK to complete the setting. As shown below:


Internet Time Settings
Configure Internet time settings:
Synchronize with an Internet time server
Server:
ntpupdate.
.com
Update now
The clock was succe sfully synchronized with ntpupdate.
.com
on
at 4:20 PM.
OK
Cancel

Best Practices for Boot Modes Legacy BIOS and UEFI

A boot mode refers to the method of booting the system disk when a CVM instance is created. You can find this information in the image parameters.
CVM supports two types of boot modes: Legacy Basic Input/Output System (BIOS) and Unified Extensible Firmware Interface (UEFI). This document describes the differences between these boot modes and details the boot modes supported by CVM instances.

Differences Between Legacy BIOS and UEFI

Comparison Item	UEFI	Legacy BIOS
System Boot Process	UEFI uses GUID Partition Table (GPT) as the partitioning scheme, supporting hard disks larger than 2 TB and multiple partitions.	Legacy BIOS uses Master Boot Record (MBR) as the partitioning scheme, supporting hard disks up to 2 TB and a maximum of four primary partitions.
Boot Speed	UEFI offers faster boot speed as it can directly interact with the operating system.	Legacy BIOS requires a boot loader to load the operating system.
Secure Boot	UEFI provides the Secure Boot feature to prevent unauthorized operating systems and boot loaders from start.	Legacy BIOS does not have a Secure Boot feature similar to that of UEFI.
Interfaces and Operations	UEFI provides a graphical interface and richer operational options.	Legacy BIOS typically provides a basic text-mode interface.
Compatibility	UEFI is a newer technology that supports more hardware devices and operating systems.	Legacy BIOS is an older technology that may encounter compatibility issues with certain new hardware devices and operating systems.
Firmware Size	UEFI firmware is typically greater than Legacy BIOS firmware because it includes more features and drivers.	Legacy BIOS firmware is smaller than UEFI firmware.
System Diagnosis and Recovery	UEFI boot mode typically provides more system diagnosis and recovery tools, helping repair and recover the system more easily when issues occur.	Legacy BIOS has fewer system diagnosis and recovery tools than UEFI.

Description of Boot Mode for Public Images

Public images with the "UEFI Edition" suffix in their names use the UEFI boot mode (such as TencentOS Server 3.1 (TK4) UEFI Edition). Those without the "UEFI Edition" suffix use the Legacy BIOS boot mode.
You can also go to the CVM console > Images page, click the image ID, and view the details on the details page.

Description of Boot Mode for Custom Images

1. Importing a custom image: You can configure the boot mode of the image.
   Ensure that the currently selected boot mode is consistent with that of the image file. Otherwise, using this image may affect the boot of your instance.
2. Creating a custom image: The boot mode of the image currently used by your instance will be inherited.
   You can also go to the CVM console > Images page, click the image ID, and view the details on the details page.

Ops Guide
Mount Data Disk
Initialize Data Disk (Linux Cloud Virtual Machine)

Overview

This document describes how to initialize data disks, such as formatting, partitioning, and creating file systems on a Linux Cloud Virtual Machine.

Notes

- Before you format, ensure that there is no data in the data disk or that important data has been backed up. After formatting, all data in the data disk will be cleared.
- To avoid service exceptions, ensure that the Cloud Virtual Machine has stopped external services before you format.

Directions

Select the appropriate operation guide according to the disk capacity:

- If the disk capacity is less than 2TB, Initialize Cloud Block Storage (Linux).
- If the disk capacity is greater than or equal to 2TB, Initialize Cloud Block Storage (Linux).

Initialize Data Disk (Windows Cloud Virtual Machine)

Overview

After Cloud Virtual Machine is purchased or reinstalled, you need to partition and format the data disk. This document describes how to perform initialization operations such as partitioning and formatting data disks on a Windows Cloud Virtual Machine.

Notes

- Formatting the data disk will clear all data. Ensure that there is no data in the data disk or that important data has been backed up.
- To avoid service exceptions, ensure that the Cloud Virtual Machine has stopped external services before formatting.

Directions

Select the appropriate operation guide according to the disk capacity:

- If the disk capacity is less than 2TB, Initialize Cloud Block Storage (Windows).
- If the disk capacity is greater than or equal to 2 TB, Initialize Cloud Block Storage (Windows).

Reading the Original EXT Data Disks after Reinstalling Linux to

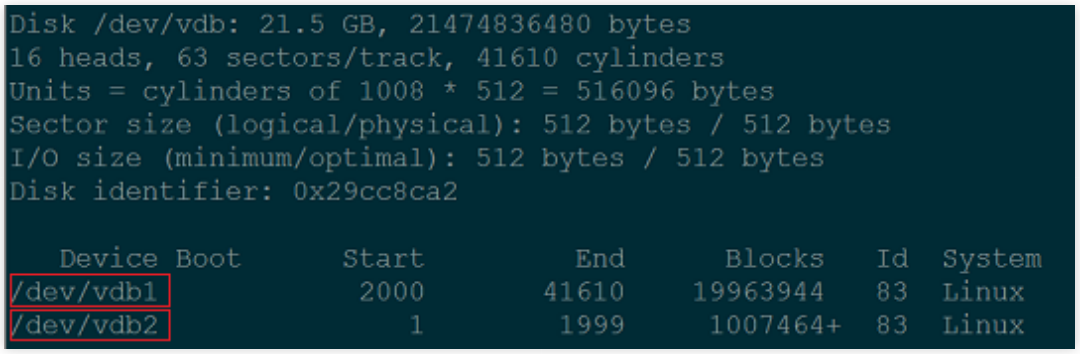
Overview

This document introduces the operation method of reading data from the original Linux system's data disk on the CVM after Linux is changed to Windows.

The Windows file system format is usually NTFS or FAT32, while the Linux file system format is usually the EXT series. When the operating system is reinstalled from Linux to Windows, the operating system type changes, but the data disks remain in the original format. The reinstalled system may be unable to access the original data disk file system. Format conversion software is needed to read the original data.

Prerequisites

- The DiskInternals Linux Reader software has been installed on the CVM reinstalled with Windows. How to obtain the DiskInternals Linux Reader software: http://www.diskinternals.com/download/Linux_Reader.exe
- It is known that the data disk mounted to the Linux CVM before reinstallation has two partitions, vdb1 and vdb2. As shown below:



Directions

Mount Data Disk

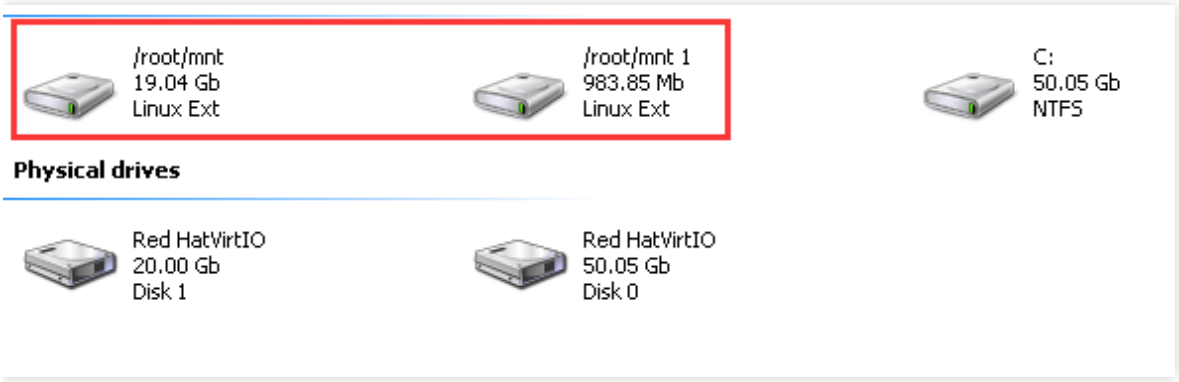
> Note:
> If the data disk has been mounted, you can skip this step.

1. Log in to the CVM console.
2. In the left sidebar, select Cloud Block Storage to enter the Cloud Block Storage Management page.
3. Choose the instance row where the system has been reinstalled, and click More > Attach on the right.
4. In the pop-up window, select the reinstalled Windows CVM and click OK.

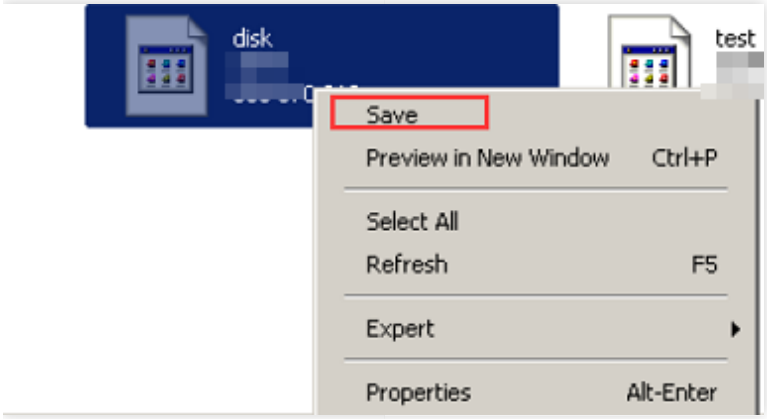
Viewing Data Disk Information

1. Run the DiskInternals Linux Reader software to view the information of the data disk that has just been mounted. /root/mnt and /root/mnt1 are the two partitions (vdb1 and vdb2) of the Linux CVM data disk before reinstallation. As shown below:

> Note:
> At this time, the Linux data disk is read-only. If you need to use this data disk as a Windows data disk for read-write operation, please back up the required files first and reformat the disk into a standard type supported by the Windows operating system. For specific operations, see Windows Instance: Initializing the Data Disk.



2. Double-click to enter the /root/mnt directory, right-click the file to be copied, and select Save to save the file. As shown below:


disk
test
Save
Preview in New Window Ctrl+P
Select All
Refresh F5
Expert
Properties Alt-Enter

Reading and Writing the Original NTFS Data Disks after Reinstall

Overview

Windows file systems usually use NTFS or FAT32 formats, while Linux file systems usually use EXT series formats. When the CVM operating system is reinstalled from Windows to Linux, the type of operating system has changed, but the data disk in the CVM remains in the format used by the original system. Therefore, after the system is reinstalled, the CVM may be unable to access the data disk file system. This document guides you to read data from the original Windows system's data disk on the CVM reinstalled with the Linux system.

Directions

Configuring Linux System to Support NTFS

1. Log in to the CVM reinstalled with the Linux system.
2. Run the following command to install the ntfsprogs software so that the Linux CVM can access the NTFS file system.

```
yum install ntfsprogs
```

Mounting Data Disks from Windows CVM to Linux CVM

> Note:
> If the data disks in your Windows CVM have been mounted to the Linux CVM, you can skip this step.

1. Log in to the CVM console.
2. In the left sidebar, click Cloud Block Storage to enter the Cloud Block Storage Management page.
3. Select the Windows data disk to be mounted, and click More > Mount.

4. In the pop-up Mount to Instance window, select the Linux CVM that the data disk is to be mounted to and click OK.

5. Log in to the Linux CVM with the Windows data disks mounted.

6. Run the following command to view the data disks mounted from the Windows CVM.

```
parted -l
```

Information resembles the following is returned:

```
Model: Virtio Block Device (virtblk)
Disk /dev/vdb: 53.7GB
Sector size (logical/physical): 512B/512B
Partition Table: gpt
Disk Flags:
Number  Start   End     Size    File system  Name                          Flags
 1      17.4kB  134MB   134MB                Microsoft reserved partition  msftres
 2      135MB   53.7GB  53.6GB  ntfs         Basic data partition
```

7. Run the following command to mount the data disk.

```
mount -t ntfs-3g Data Disk Path Mount Point
```

For example, if you need to mount the data disk under the path /dev/vdb1 to path /mnt , execute the following command:

```
mount -t ntfs-3g /dev/vdb1 /mnt
```

Since the file system is now recognizable, the mounted data disk can be directly read and written by the Linux system.

Environment Configuration
Installing ACPI Power Management

Overview

In x86 machines, there are two power management methods: APM (Advanced Power Management) and ACPI (Advanced Configuration and Power Interface). ACPI is a power management standard developed jointly by Intel, Microsoft, and Toshiba, providing a more flexible interface for managing computers and devices, whereas APM is an older power management standard.

Linux supports both APM and ACPI, but these two standards cannot operate simultaneously. By default, Linux runs ACPI. At the same time, Converge Cloud it is recommended to use ACPI power management.

Failure to install ACPI management programs on Linux systems can result in unsuccessful soft shutdowns. This document outlines the steps to check the ACPI installation status and perform the installation.

Installation Instructions

For CoreOS systems, ACPI installation is not required.

Directions

1. Execute the following command to check if ACPI is installed.

   ```
   ps -ef|grep -w "acpid"|grep -v "grep"
   ```

   - If the process does not exist, it indicates that ACPI is not installed. Proceed to the next step.
   - If the process exists, it indicates that ACPI is installed, and the task is complete.

2. Based on your operating system type, execute the corresponding command to install ACPI.

   - On Ubuntu / Debian, execute the following command:

     ```
     sudo apt-get install acpid
     ```

   - For Redhat / CentOS systems, execute the following command:

yum install acpid

How to effectively modify the etc/hosts configuration of Linux C

Overview

Converge Cloud are pre-installed with the purely open-source Cloud-Init tool, which enables the initialization operations of all instances and increases the transparency of the internal processes of the instances.
Cloud-Init generates a new `/etc/hosts` file based on the template located at `/etc/cloud/templates/hosts.${os_type}.tmpl` every time the instance is started, which overwrites the original `/etc/hosts` file. This means that if you manually modify the `/etc/hosts` configuration inside the instance and restart the instance, the `/etc/hosts` configuration will revert to its default state.

Directions

Option I

1. Log in to the Linux server.

2. Execute the following command to modify the `/etc/cloud/cloud.cfg` configuration file by changing `- update_etc_hosts` to `- ['update-etc-hosts', 'once-per-instance']` .

   ```
   sed -i "/update_etc_hosts/c \ - ['update_etc_hosts', 'once-per-instance']" /etc/cloud/cloud.cfg
   ```

3. Execute the following command to create the `config_update_etc_hosts` file under the path `/var/lib/cloud/instance/sem/` .

   ```
   touch /var/lib/cloud/instance/sem/config_update_etc_hosts
   ```

Option II

> Note:
> This solution takes the CentOS7.2 operating system as an example.

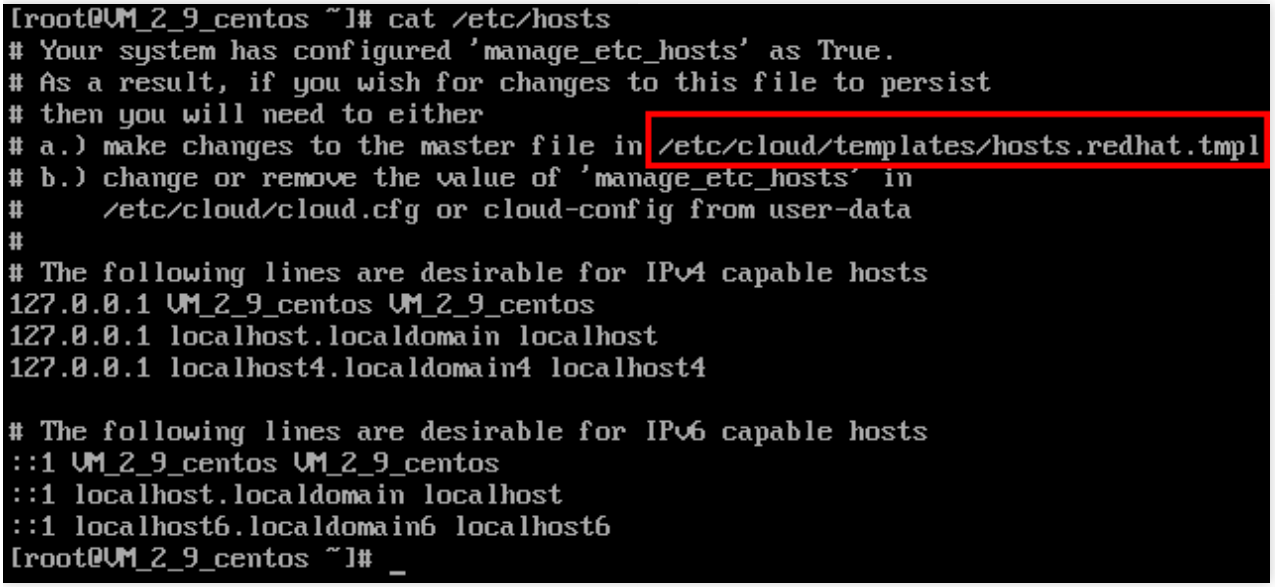
Retrieve the hosts template file path

1. Log in to the Linux server.

2. Execute the following command to view the system's hosts template file.

   cat /etc/hosts

   The hosts template file path will be displayed:



Modifying Hosts Template File

> Note:
> Take adding 127.0.0.1 test test as an example. You can modify the hosts template file and /etc/hosts file as needed.

1. Execute the following command to modify the hosts template file.

   vim /etc/cloud/templates/hosts.redhat.tmpl

2. Press "i " to switch to edit mode.

3. Add the following content at the end of the file.

127.0.0.1 test test

4. After entering, press "Esc " , input :wq to save the file and exit.

Modifying /etc/hosts File

1. Execute the following command to modify /etc/hosts file.

vim /etc/hosts

2. Press "i 〞 to switch to edit mode.

3. Add the following content at the end of the file.

127.0.0.1 test test

4. After entering, press "Esc " , input :wq to save the file and exit.

LNMP environment configuration under openSUSE

Overview

The LNMP environment represents the Nginx + MySQL + PHP web server architecture on a Linux system. This document provides instructions for setting up the LNMP environment on openSUSE 42.3.

This document includes software installation steps. Make sure you are familiar with the software installation methods. For more information, see Installing Software on openSUSE Using Zypper.

LNMP Components and Versions:

- Linux: Operating system, using openSUSE 42.3 in this document.
- Nginx: Web server program for parsing web programs, using Nginx 1.14.2.
- MySQL: Database management system, using MySQL 5.6.43.
- PHP: Program for generating web pages on the web server, using PHP 7.0.7.

Directions

Configure Image Sources

1. Log in to the CVM.

2. Execute the following commands to add mirror sources.

   ```
   zypper ar https://mirrors.convergecloud.com/opensuse/distribution/leap/42.3/repo/oss suseOss
   zypper ar https://mirrors.convergecloud.com/opensuse/distribution/leap/42.3/repo/non-oss suseNon
   Oss
   ```

3. Execute the following commands to update mirror sources.

   ```
   zypper ref
   ```

Install and configure Nginx

1. Execute the following command to install Nginx.

   ```
   zypper install -y nginx
   ```

2. Execute the following commands in sequence to start the Nginx service and set it to start automatically on boot.

   ```
   systemctl start nginx
   systemctl enable nginx
   ```

3. Run the following command to modify the Nginx configuration file.

   ```
   vim /etc/nginx/nginx.conf
   ```

4. Press "i " to switch to edit mode.

5. Locate the server{...} and replace it with the following content.

   ```
   server {
      listen       80;
      server_name  localhost;

      #access_log  /var/log/nginx/host.access.log  main;
      location / {
            root          /srv/www/htdocs/;
            index  index.php index.html index.htm;
      }

      #error_page  404              /404.html;
      # redirect server error pages to the static page /50x.html
      error_page   500 502 503 504  /50x.html;
      location = /50x.html {
            root          /srv/www/htdocs/;
      }

      # pass the PHP scripts to FastCGI server listening on 127.0.0.1:9000
      location ~ \.php$ {
            root          /srv/www/htdocs/;
            fastcgi_pass   127.0.0.1:9000;
            fastcgi_index  index.php;
            fastcgi_param  SCRIPT_FILENAME  $document_root$fastcgi_script_name;
            include        fastcgi_params;
      }
   }
   ```

6. After inputting, press Esc, input ":wq" to save the file and return.

7. Execute the following command to restart the Nginx service.

   ```
   systemctl restart nginx
   ```

8. Execute the following command to create index.html Homepage.

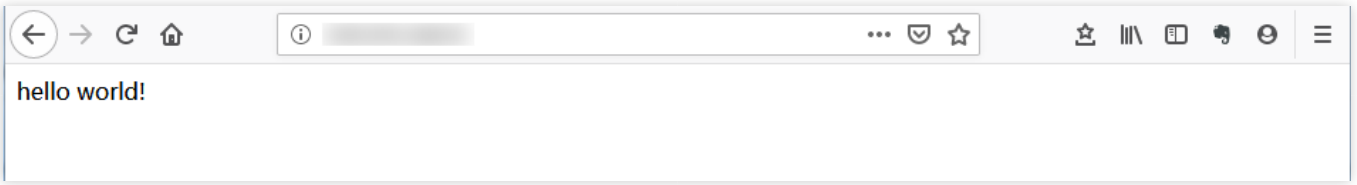
   ```
   vi /srv/www/htdocs/index.html
   ```

9. Press "i to switch to edit mode and enter the following content:

   ```
   <p> hello world!</p>
   ```

10. After inputting, press Esc, input ":wq" to save the file and return.

11. In the browser, access the public IP address of the openSUSE CVM instance to check whether the Nginx service is running normally.
    As shown in the figure below, it indicates that Nginx has been successfully installed and configured.



Install and configure MySQL

1. Execute the following command to install MySQL.

   ```
   zypper install -y mysql-community-server mysql-community-server-tools
   ```

2. Execute the following commands in sequence to start the MySQL service and set it to start automatically on boot.

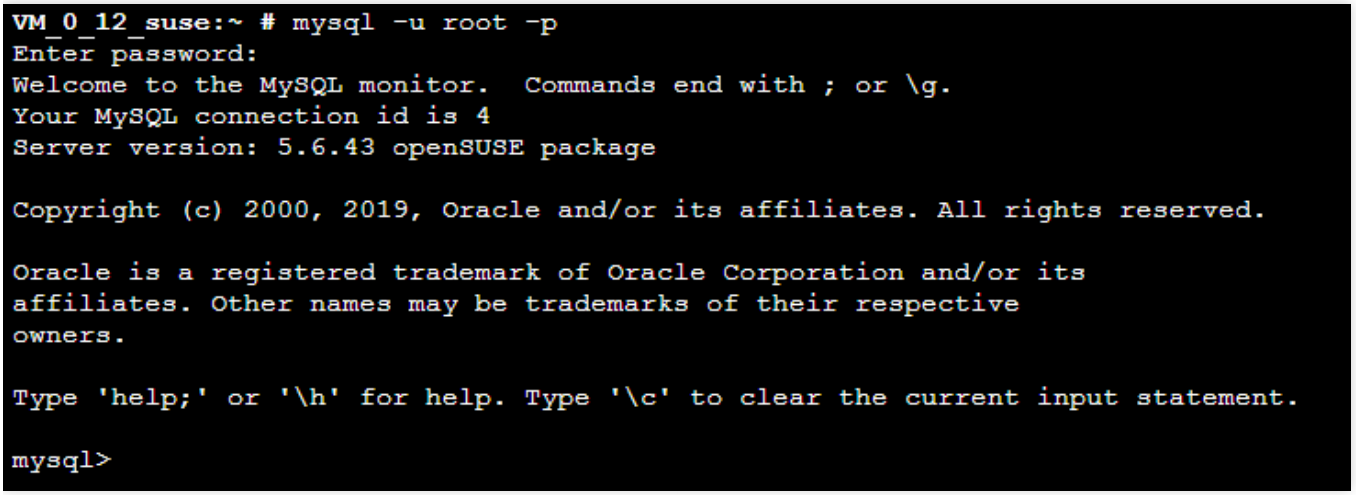
   ```
   systemctl start mysql
   systemctl enable mysql
   ```

3. Execute the following command to log in to MySQL for the first time. > Note: When you log in to MySQL for the first time, the system will prompt you to enter a password. If you do not want to enter a password,

you can directly press "Enter" to log in to MySQL.

```
mysql -u root -p
```

Successfully entering MySQL will a screen similar to the image below.



4. Execute the following command to change the root password.

```
update mysql.user set password = PASSWORD('Enter your new password here') where user='root';
```

5. Execute the following command to apply the configuration.

```
flush privileges;
```

6. Execute the following command to exit MySQL.

```
\q
```

Install and configure PHP

Execute the following command to install.

```
zypper install -y php7 php7-fpm php7-mysql
```

Integrate Nginx with PHP-FPM

1. Execute the following commands in sequence to enter /etc/php7/fpm Directory, copy the file php-fpm.conf.default and rename it to php-fpm.conf .

```
cd /etc/php7/fpm
cp php-fpm.conf.default php-fpm.conf
```

2. Execute the following commands in sequence to enter /etc/php7/fpm/php-fpm.d Directory, copy the file www.conf.default and rename it to www.conf .

```
cd /etc/php7/fpm/php-fpm.d
cp www.conf.default www.conf
```

3. Execute the following commands in sequence to start the service and set it to start automatically on boot.

```
systemctl start php-fpm
systemctl enable php-fpm
```

Validate the Environment Configuration

1. Execute the following command to create a test file "index.php".

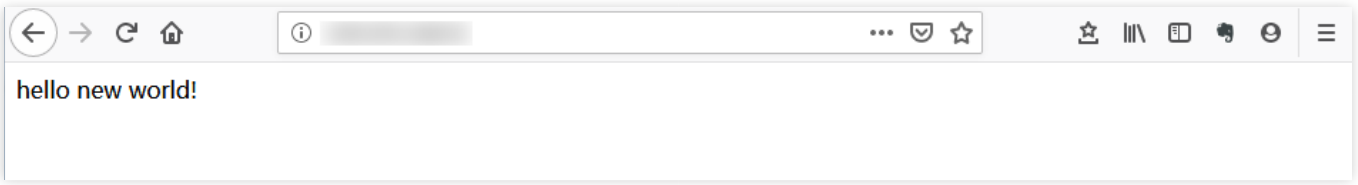
```
vim /srv/www/htdocs/index.php
```

2. Press "i to switch to edit mode and input the following content:

```
<?php
   echo "hello new world!";
?>
```

3. Press "Esc", input ":wq" to save the file and return.

4. Open a web browser and access the public IP of your openSUSE CVM.
   If you see a page similar to the one below, it indicates that the LNMP environment has been successfully set up.


hello new world!

Uploading Files
How to copy local files to a CVM

Copying local files to a cloud server is one of the common uses for purchasing CVMs.This document explains how to copy your local files to a CVM.
Depending on your local operating system and the server type you purchased, you can refer to the following methods.

Local operating system types	Cloud Virtual Machine operating system (Linux)	Cloud Virtual Machine operating system (Windows)
Windows	Upload files to the Cloud Virtual Machine via WinSCP	Upload files to the Cloud Virtual Machine via MSTSC
Windows	Upload files to the Cloud Virtual Machine via FTP	Upload files to the Cloud Virtual Machine via MSTSC
Linux	Upload files to the Cloud Virtual Machine via SCP	Upload files to the Cloud Virtual Machine via RDP
Mac OS	Upload files to the Cloud Virtual Machine via SCP	Upload files to the Cloud Virtual Machine via MRD

For example, if your local computer's operating system is Windows, and the Cloud Virtual Machine you purchased has a Linux operating system, you can upload files to the Cloud Virtual Machine using WinSCP.

Next Steps

When you have important business data or personal files that need backup, after uploading files to the cloud server, you can also manually or automatically create snapshots of important files.

Contact Us

We are very sorry that you encountered problems while using the service. We recommend that you refer to the documentation to locate and solve the problem.

- Forgot your cloud server login password?
  Please refer to Reset instance password .

- Unable to log in to the CVM?

  Please refer to Unable to log in to Windows instance or Unable to log in to the Linux instance.

Uploading Files to Windows CVM via MSTSC

Overview

A common method to upload files to a Windows CVM is to use MSTSC (Microsoft Terminal Services Client) for remote desktop connection. This document guides you to use a local Windows computer to upload files to a Windows CVM via a remote desktop connection.

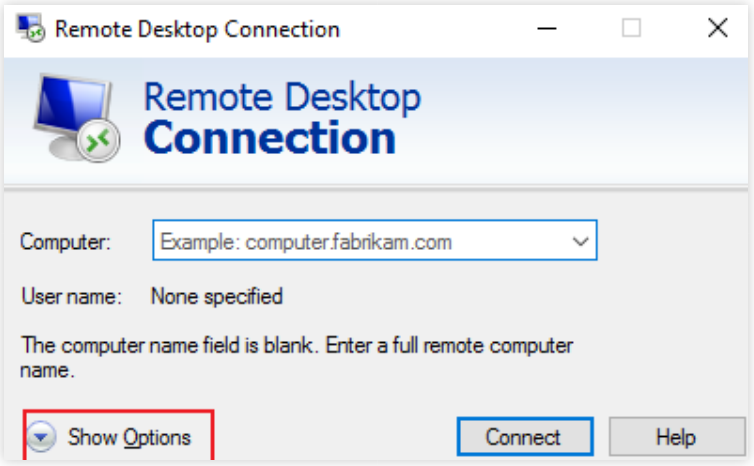
Prerequisites

Please ensure that the Windows CVM can access the public network.

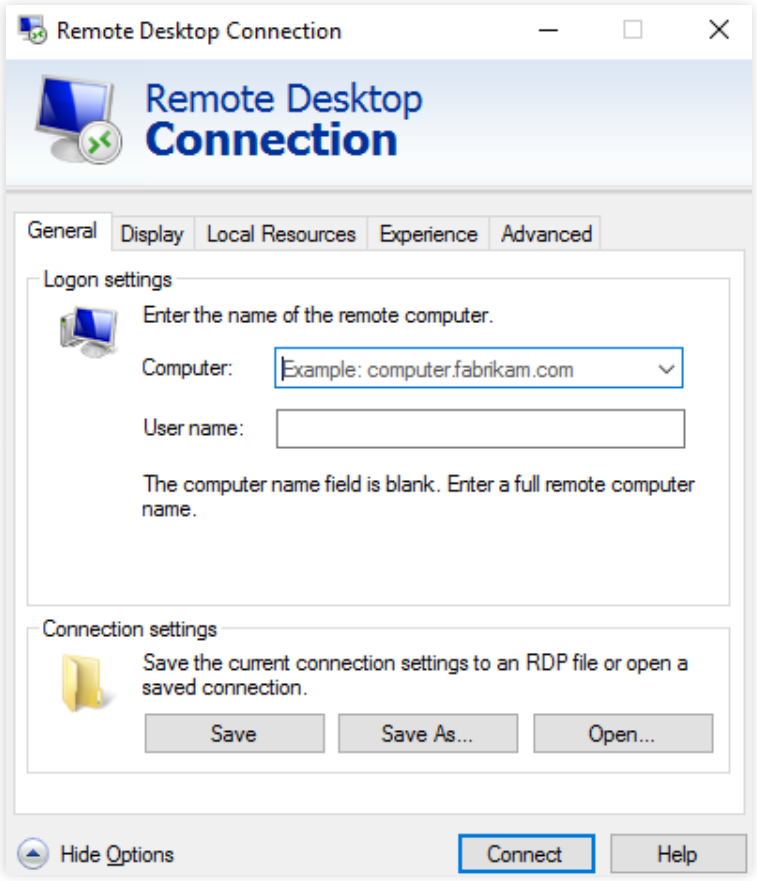
Directions

> Note:
> The following steps use a local Windows 7 computer as an example. The detailed steps may vary slightly depending on the operating system.

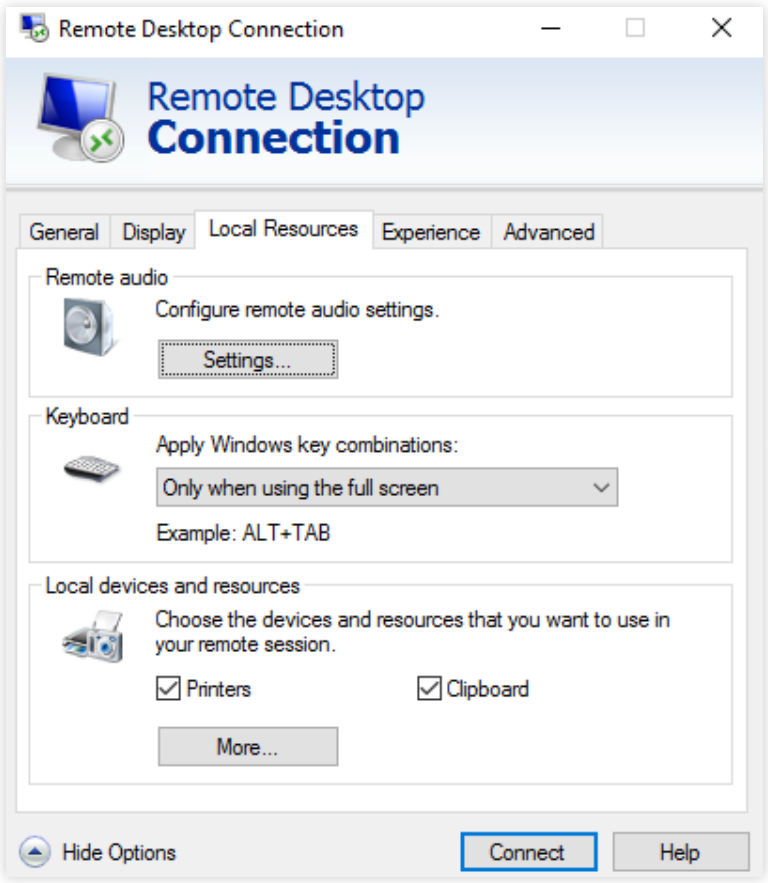
1. On the local computer, use the shortcut keys Windows + R to open the Run window.
2. In the pop-up Run dialog box, type mstsc and click OK to open the Remote Desktop Connection dialog box.
3. In the Remote Desktop Connection dialog box, input the IP address of the CVM public network and click Options. As shown below:



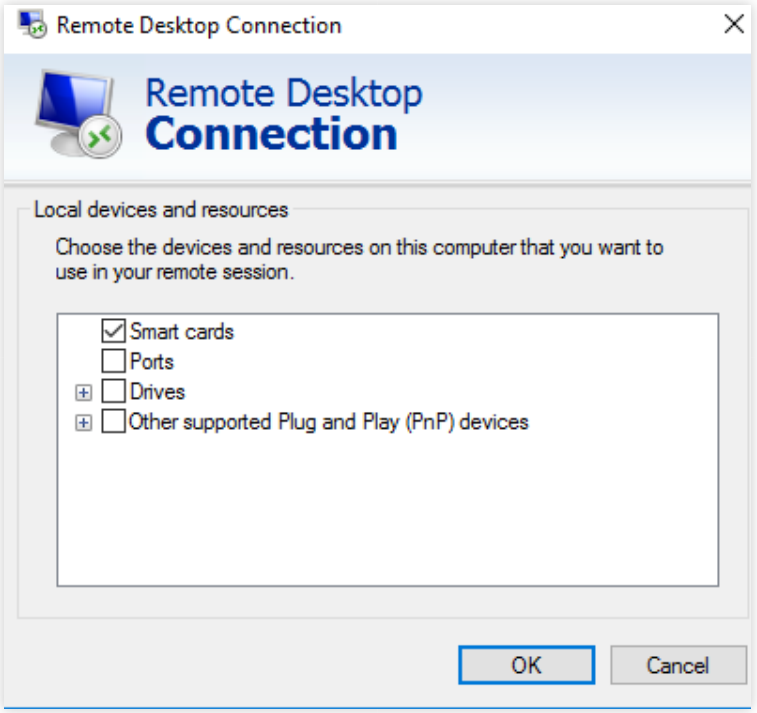
4. On the General tab, input the IP address of the CVM public network and the username Administrator. As shown below:



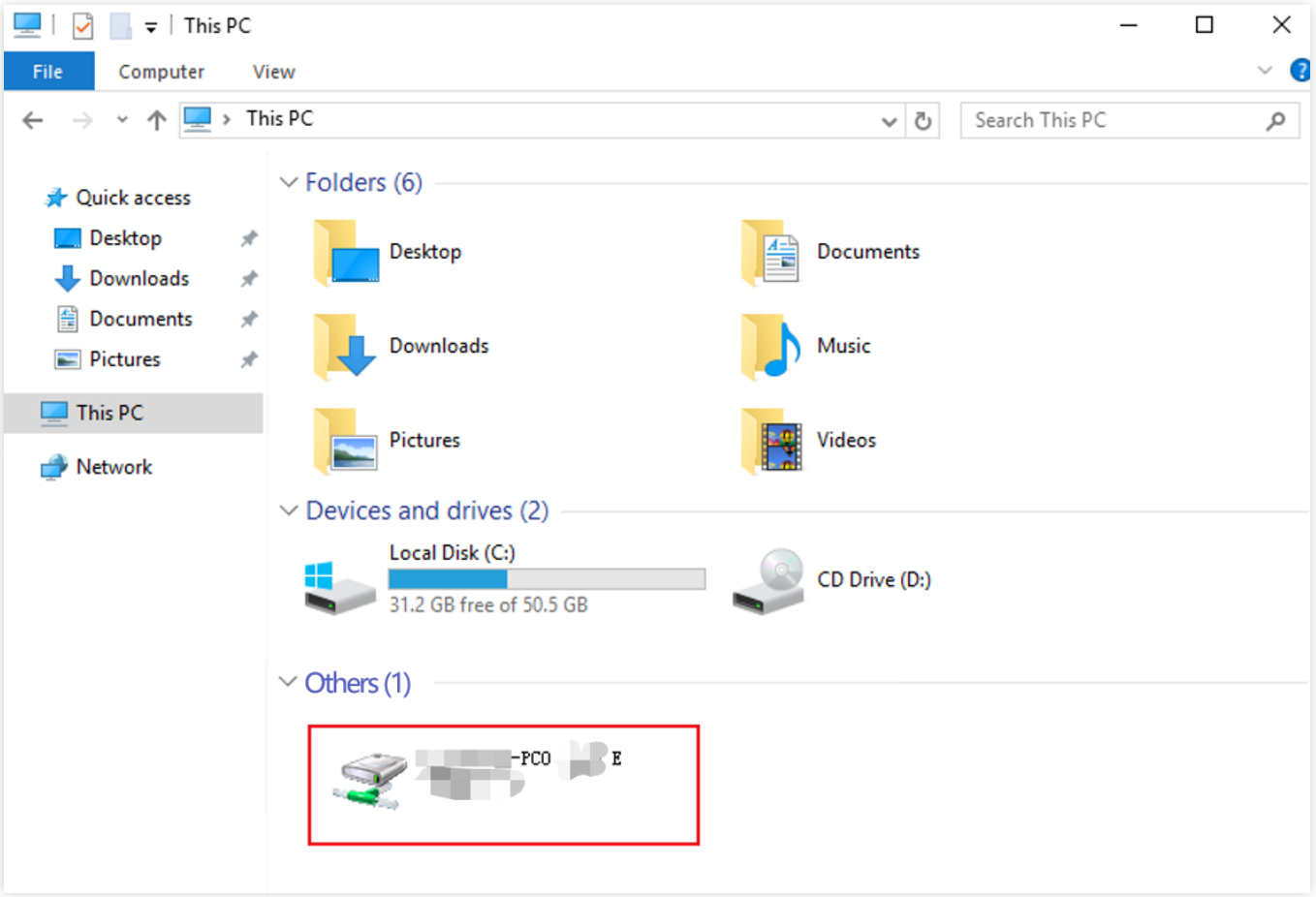
5. Select the Local Resources tab and click Details. As shown below:



6. In the pop-up Local Devices and Resources window, select the Drive module, check the local hard disk where the file to be uploaded to the Windows CVM is located, and click OK. As shown below:



7. After the local configuration is complete, click Connect to remotely log in to the Windows CVM.
8. In the Windows CVM, click Start > Computer to see the local hard disk mounted on the CVM. As shown below:



9. Double-click to open the local hard disk, and copy the necessary files to be copied from the local drive to another hard drive of the Windows CVM to complete the file upload operation.
   For example, copy file A in the local hard drive (E) to the C: drive of the Windows CVM.

Upload Files from MacOS System to Windows CVM via MRD

Overview

Microsoft Remote Desktop (MRD) is a remote desktop application for Mac computers provided by Microsoft. This document explains how to quickly upload files from a Mac machine to a Windows Server 2012 R2 operating system on a Cloud Virtual Machine (CVM) using MRD.

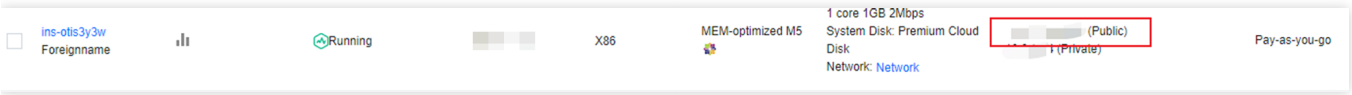
Prerequisites

- The local computer has downloaded and installed MRD. You can download it from Microsoft Remote Desktop for Mac.
- MRD supports Mac OS 10.10 and later versions. Ensure you are using a supported operating system.
- A Windows cloud server has been purchased.

Directions

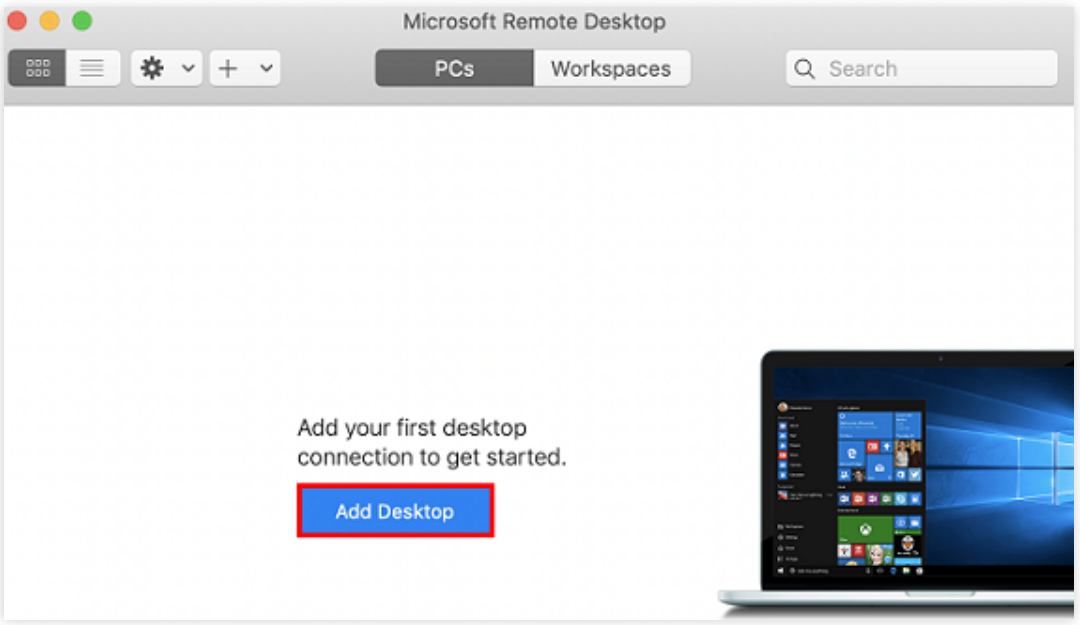
Obtain the Public IP

Log in to the CVM Console, and note the public IP of the CVM where the file needs to be uploaded on the instance list page.

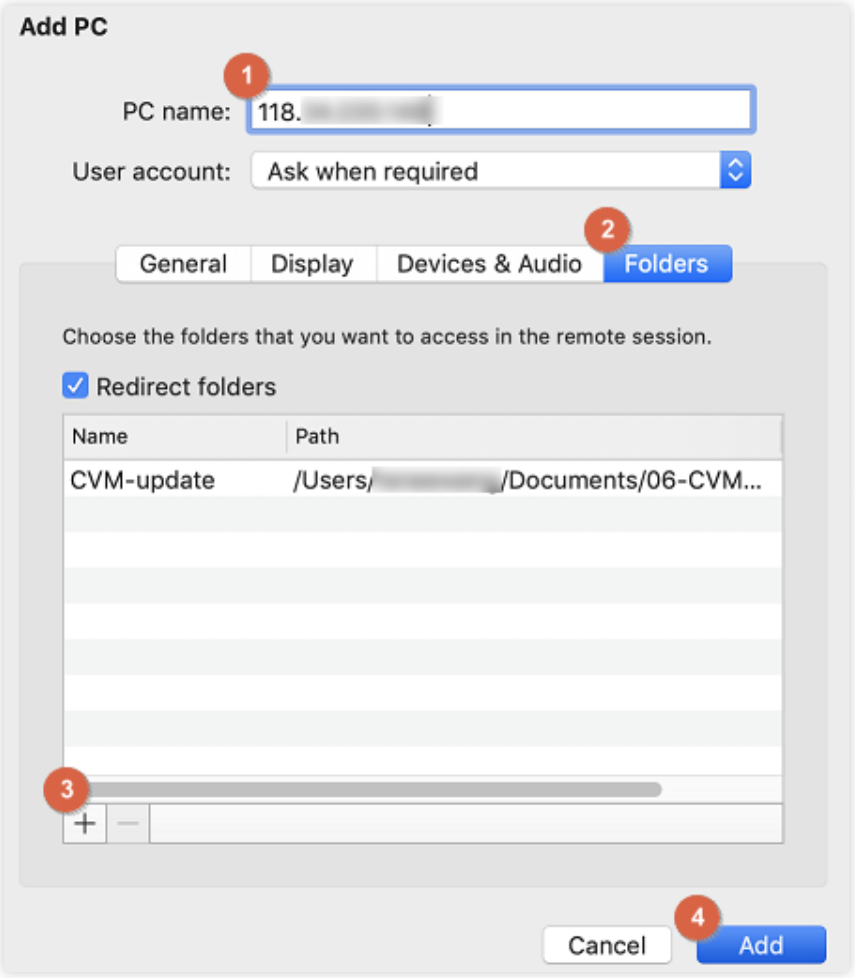


Uploading Files

1. Launch MRD, and click Add Desktop.



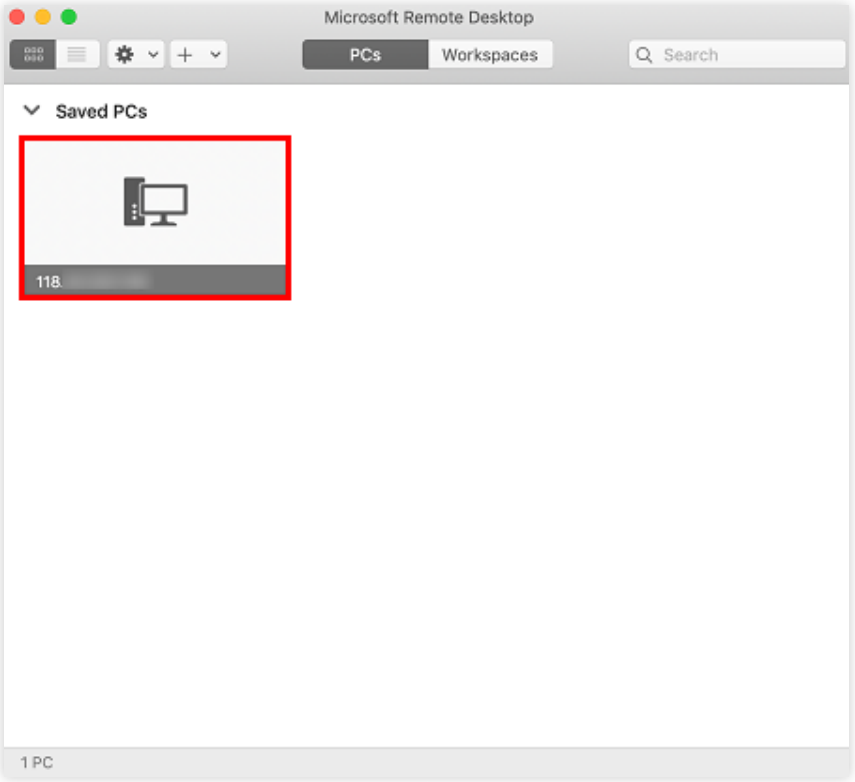
2. In the pop-up "Add Desktop" window, follow these steps to select the folder to be uploaded and create the connection.



i. Enter the obtained public IP address of the CVM in "PC name".

ii. Click Folders to switch to the folder selection list.

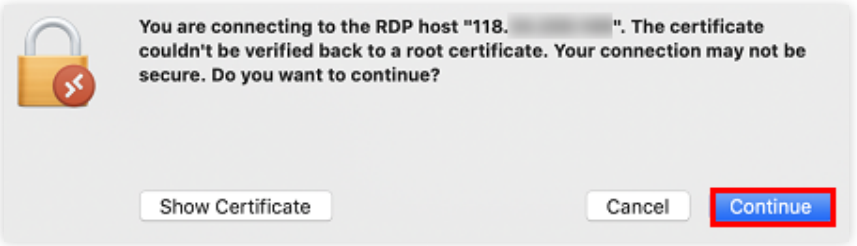
iii. Click + at the lower left corner, and in the pop-up window, select the folder you want to upload.
iv. After completing the selection, you can view the list of folders to be uploaded and click Add to confirm the creation.
v. Keep the remaining options at their default settings and complete the connection creation.
You can view the successfully created connection in the window.



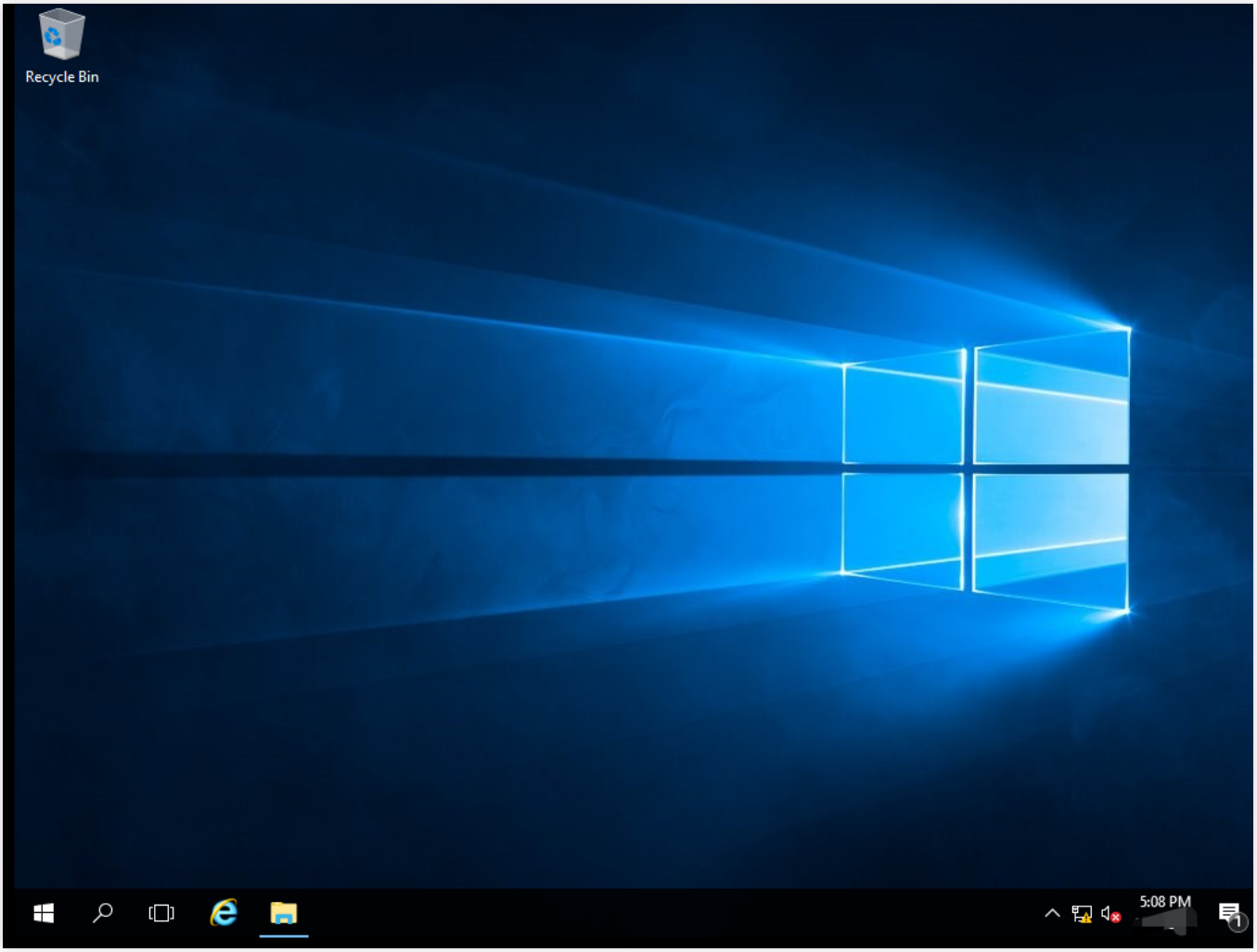
3. Double-click to open the newly created connection. In the pop-up window, enter the CVM account and password, then click Continue.

> Note:
>
> - The cloud server account is 'Administrator' by default.
> - If you use the system default password to log in to the instance, please go to the Message center to obtain it.
> - If you forget your password, reset the instance password.

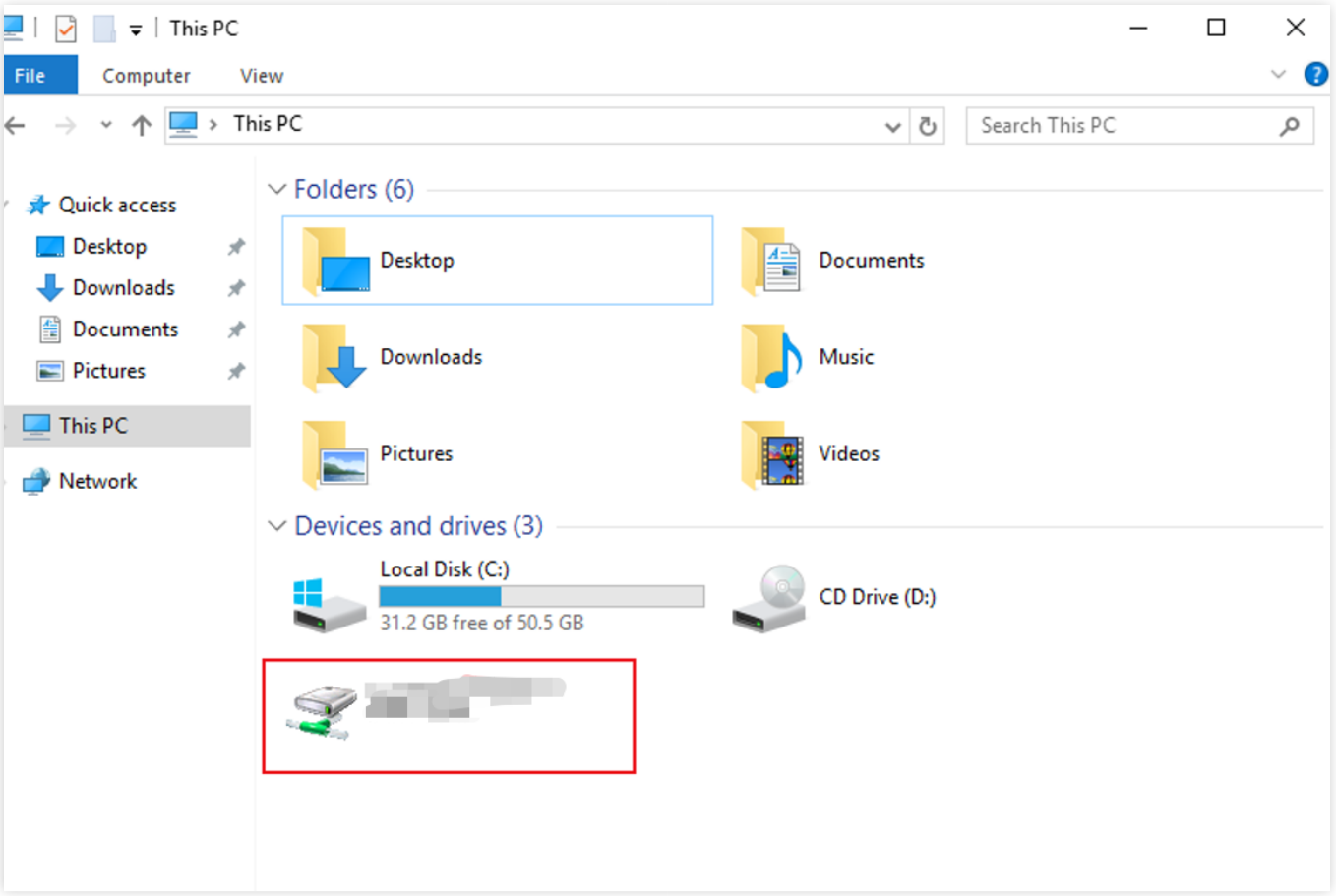
4. In the pop-up window, click Continue to confirm the connection. As shown below:



After a successful connection, the Windows CVM interface will open.



5. Select This Computer at the lower left corner, and you will see the shared folder.



6. Double-click to open the shared folder, and copy the local files to be uploaded to other hard disks of the Windows cloud server to complete the file upload operation.
   For example, copy file A from the shared folder to the 'C:' drive of the Windows CVM.

Downloading Files

If you need to download files from the Windows CVM to your local machine, follow the same steps as for uploading files. Copy the required files from the Windows CVM to the shared folder, and the files will be downloaded to the local machine.

Uploading Files to a Windows Cloud Server from a Linux System vi

Overview

Rdesktop is an open-source client for the Remote Desktop Protocol (RDP) used to connect to Windows CVMs and perform various operations. This article introduces how to quickly upload files from a Linux machine to a Converge Cloud Cloud Virtual Machine (CVM) running the Windows Server 2012 R2 operating system through rdesktop.

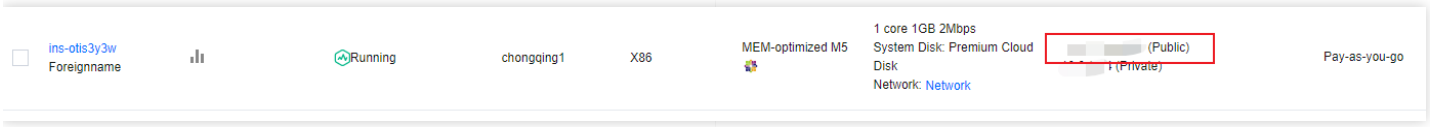
Prerequisites

A Windows cloud server has been purchased.

Directions

Obtain the Public IP

Log in to the CVM Console and record the public IP of the CVM where files need to be uploaded on the Instance List page.



Install rdesktop

1. Execute the following command in the terminal to download the rdesktop installation package. This step takes rdesktop 1.8.3 as an example.

   ```
   wget https://github.com/rdesktop/rdesktop/releases/download/v1.8.3/rdesktop-1.8.3.tar.gz
   ```

   If you need the latest installation package, you can find it on the GitHub rdesktop page replace it with the latest installation path in the command line with the latest version.

2. Execute the following commands in sequence to extract the installation package and enter the

installation directory.

tar xvzf rdesktop-1.8.3.tar.gz

cd rdesktop-1.8.3

3. Execute the following commands in sequence to compile and install rdesktop.

./configure

make

make install

4. After installation, execute the following command to check if the installation was successful.

rdesktop

Uploading Files

1. Execute the following command to specify the folder to be shared with the CVM.

rdesktop Cloud Server Public IP -u Cloud Server Account -p Cloud Server Password -r disk:Shared Folder Name=Local Folder Path

Note:

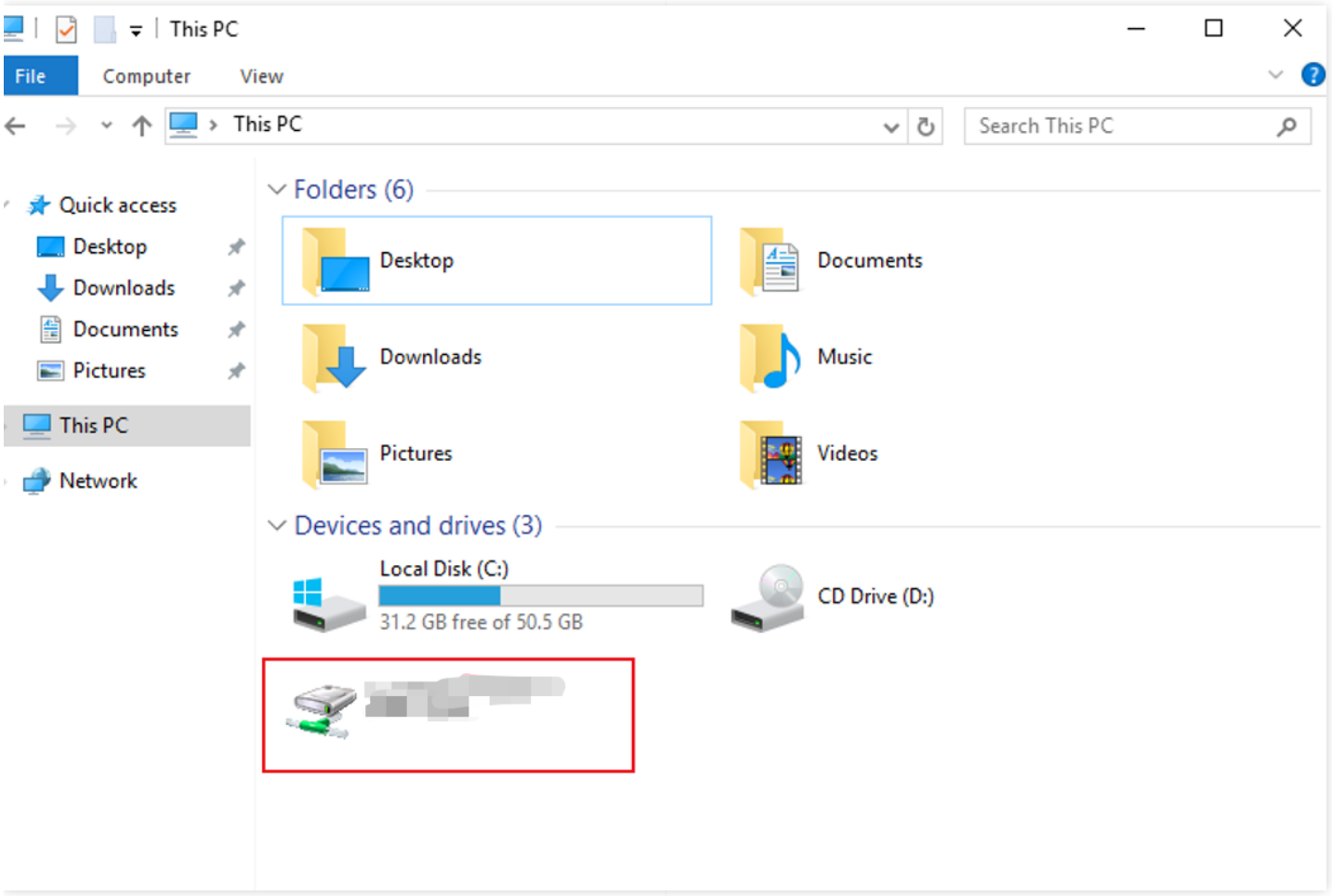
- The cloud server account is 'Administrator' by default.
- If you use a system default password to log in to the instance, go to Message Center to obtain the password first.
- If you forget your password, reset the instance password.

For example, execute the following command to share the local computer folder /home to the specified CVM and rename the shared folder to share .

rdesktop 118.xx.248.xxx -u Administrator -p 12345678 -r disk:share=/home

Upon successful sharing, the Windows CVM interface will open.

Select This PC in the lower left corner, you can view the shared folders in the server system interface. As shown below:



2. Double-click to open the shared folder, and copy the local files to be uploaded to other hard disks of the Windows cloud server to complete the file upload operation.
For example, copy file A from the share folder to the C: drive of the Windows CVM.

Downloading Files

If you need to download files from the Windows CVM to your local machine, follow the same steps as for uploading files. Copy the required files from the Windows CVM to the shared folder, and the files will be downloaded to the local machine.

Uploading Files to a Linux CVM via WinSCP on Windows

Overview

WinSCP is an open-source graphical SFTP client for Windows that uses SSH and also supports the SCP protocol. Its main function is to securely copy files between local and remote computers. Compared with uploading code using FTP, WinSCP allows you to directly use the server account password to access the server without any configuration on the server side.

Prerequisites

WinSCP client is downloaded and installed on your local computer (recommended to get the latest version from the official website).

Directions

Logging in to WinSCP

1. Open WinSCP, the "WinSCP login to " dialog box pops up.
2. Set the login parameters:
    - Protocol: Select either SFTP or SCP.
    - Host name: the public IP address of the CVM. You can view the public IP address of the corresponding CVM in the CVM console.
    - Port: Default is 22.
    - Password: The password corresponding to the CVM user account.
    - Username: The system username of the CVM.
        - SUSE/CentOS/Debian systems: root
        - Ubuntu systems: ubuntu
3. click [log in to], to enter the "WinSCP" file transfer interface.

Uploading Files

1. In the right pane of the WinSCP file transfer interface, select the directory on the server where the file will be stored, such as "/user".
2. In the left pane of the WinSCP file transfer interface, select the directory where the files are stored, such as "F:\SSL Certificate\Nginx", and select the file to be transferred.

3. In the "WinSCP" file transfer interface menu bar, click [Upload].
4. In the pop-up Upload dialog box, confirm the file to be uploaded and the remote directory, and click OK to upload the file from the local computer to the CVM.

Downloading Files

1. In the left pane of the WinSCP file transfer interface, select the directory where the file will be stored on the server, such as "F:\SSL Certificate\Nginx".
2. In the right pane of the WinSCP file transfer interface, select the directory where the files are stored, such as "/user", and select the files to be transferred.
3. In the "WinSCP" file transfer interface menu bar, click [Download].
4. In the pop-up Download dialog box, confirm the file to be downloaded and the remote directory, and click OK to download the file from the CVM to the local computer.

Uploading Files to a Linux Cloud Virtual Machine via SCP

Overview

This document guides you on how to upload files to a Linux Cloud Virtual Machine from a Linux operating system computer using SCP.

Directions

1. On the Linux computer, execute the following command to upload files to the Linux Cloud Virtual Machine.

   scp <local-file-path> <cloud-server-username>@<cloud-server-public-IP/domain>:<cloud-server-file-path>

   For example, to upload a local file /home/lnmp0.4.tar.gz to a corresponding directory under the CentOS system Cloud Virtual Machine with an IP address of 129.20.0.2 , execute the following command:

   scp /home/Inmp0.4.tar.gz root@129.20.0.2:/home/Inmp0.4.tar.gz

2. Press Enter, and input the login password to complete the upload.

Uploading Files to CVM via FTP on Windows Systems

Overview

This document instructs you on how to upload files from a local server to CVM using the FTP protocol.

Prerequisites

FTP service has been set up on the cloud server. Refer to Set Up FTP Service for details.

Directions

1. Log in to the CVM.
2. Download and install the open-source software FileZilla.

> Note:
> Using FileZilla version 3.5.3 for FTP uploads may result in upload failures. It is recommended to obtain and use FileZilla version 3.5.1 or 3.5.2 from the official website.

3. Open FileZilla.
4. In the FileZilla window, fill in the host, user name, password, port, and other information, and click Quick Connect.
   Configuration Description:
   - Host: the public network IP of the CVM. You can view the public IP of the corresponding CVM on the instance management page in the CVM console.
   - Username: The FTP user account set during the FTP service setup. The figure takes "ftpuser1" as an example.
   - Password: The password for the FTP user account set during the FTP service setup.
   - Port: The FTP listening port, default is 21.
5. In the Local Site window at the bottom left, right-click the local file you want to upload and select Upload to transfer the file to the Linux CVM. As shown below:

> Note:

- The CVM FTP channel does not support automatic decompression or deletion of tar packages after uploading.
- The remote site path is the default path for uploading files to the Linux CVM.

Software Installation
Cloud Platform Software Source
Accelerates Software Package Down

Overview

To address the issue of slow access speeds to official sources when installing software dependencies, Converge Cloud has set up caching services for some software. You can use the Converge Cloud software source server to speed up the installation of dependency packages. For users to freely set up their service architecture, the Converge Cloud software source server currently supports both public and private network access.

- Public access URL: http://convergecloud.com/> http://convergecloud.com/
- Private network access URL: http://convergecloud.com/> http://convergecloud.com/

  > Note:

- This document uses the public access URL of the Converge Cloud software source server as an example to introduce how to use the software source from the Converge Cloud software source server in Cloud Virtual Machine. If you need to access the Converge Cloud software source server through the private network, please replace the public access URL with the private network access URL.
- The Converge Cloud software source URLs mentioned in this document are for reference only. Please obtain the latest URLs from the Converge Cloud software source server.

Prerequisites

Log in to the Cloud Virtual Machine (CVM).

Directions

Accelerate pip with Converge Cloud image source

> Note:
> Before using, ensure that Python is installed on your CVM.

Temporarily use the software source path

Execute the following command to use the Converge Cloud PyPI software source to install pip.

```
pip install -i PyPI software source directory
```

Set as Default Software Source Path

Execute the following command to modify the index-url parameter in the ~/.pip/pip.conf file to the Converge Cloud software source path.

```
[global]
index-url = PyPI software source directory
trusted-host = public/private network access URL
```

Accelerate NPM with Converge Cloud image source

> Note: Before using, ensure that Node.js and NPM are installed on your CVM.

Execute the following command to use the Converge Cloud NPM software source to install NPM.

```
npm config set registry public/private network access URL
```

Accelerate Docker with Converge Cloud image source

In the Kubernetes Engine cluster, use the Converge Cloud Docker software source

No manual configuration is required. The CVM hosts in the Kubernetes Engine (TKE) cluster will automatically install the Docker service and configure the Converge Cloud private network image when creating nodes.

Using Converge Cloud Docker Software Source on CVM

> Note:
> Before using, ensure that Docker is installed on your CVM. The Docker Hub Mirror mechanism is supported in Docker version 1.3.2 and later. If you haven't installed Docker 1.3.2 or later, or if your Docker version is outdated, please perform the installation or upgrade first.

Select the appropriate steps based on the operating system type of your CVM.

Applicable to Ubuntu 14.04, Debian, CentOS 6, Fedora, openSUSE. Other operating system may have slightly different steps:

1. Execute the following command to open `/etc/default/docker` configuration files.

   ```
   vim /etc/default/docker
   ```

2. Press i to switch to edit mode, add the following content, and save it.

   ```
   DOCKER_OPTS="--registry-mirror=<public/private network access URL"
   ```

   - Applicable to CentOS 7 Operating System:
     a. Execute the following command to open the `/etc/sysconfig/docker` configuration file.

     ```
     vim /etc/sysconfig/docker
     ```

     b. Press i to switch to edit mode, add the following content, and save it.

     ```
     OPTIONS='--registry-mirror=<public/private network access URL'
     ```

   - Applicable to Windows Operating System with Boot2Docker Installed:
     a. Enter the Boot2Docker Start Shell and execute the following commands:

     ```
     sudo su
     echo "EXTRA_ARGS=\–registry-mirror=public/private network access URL""" >> /var/lib/b
     oot2docker/profile
     exit "
     ```

     b. Restart Boot2Docker.

Accelerate MariaDB with Converge Cloud image

> Note:
> The following steps are based on CentOS 7. Detailed steps for different operating systems may vary slightly.

1. Execute the following command in /etc/yum.repos.d/ to create the MariaDB.repo file.

   vi /etc/yum.repos.d/MariaDB.repo

2. Press i to switch to edit mode, write and save the following content.

   ```
   # MariaDB 10.2 CentOS7-amd64
   [mariadb]
   name = MariaDB
   baseurl = public/private network access URL
   gpgkey = public/private network access URL
   gpgcheck=1
   ```

3. Execute the following command to clear the yum cache.

   yum clean all

4. Execute the following command to install MariaDB.

   yum install MariaDB-client MariaDB-server

Accelerate MongoDB with Converge Cloud image

> Note:
> The following steps are based on installing MongoDB version 4.0. If you need to install a different version, change the version number in the mirror path accordingly.

CentOS and Redhat cloud servers use Converge Cloud MongoDB software source

1. Execute the following command to create /etc/yum.repos.d/mongodb.repo file.

vi /etc/yum.repos.d/mongodb.repo

2. Press i to switch to edit mode, write and save the following content.

```
[mongodb-org-4.0]
name=MongoDB Repository
baseurl=public/private network access URL
gpgcheck=0
enabled=1
```

3. Execute the following command to install MongoDB.

```
yum install -y mongodb-org
```

Debian CVM use Converge Cloud MongoDB software source

1. Based on different versions of Debian, execute the following commands to import the MongoDB GPG public key.

```
sudo apt-key adv --keyserver hkp://keyserver.ubuntu.com:80 --recv 68818C72E52529D4
```

2. Execute the following command to configure the mirror path.

```
#Debian 8
echo "deb public/private network access URL jessie/mongodb-org/4.0 main" | sudo tee /etc/apt/
sources.list.d/mongodb-org-4.0.list
#Debian 9
echo "deb public/private network access URL stretch/mongodb-org/4.0 main" | sudo tee /etc/ap
t/sources.list.d/mongodb-org-4.0.list
```

3. Execute the following command to update the software package list.

```
sudo apt-get update
```

4. Execute the following command to install MongoDB.

```
sudo apt-get install -y mongodb-org
```

Using Converge Cloud MongoDB Software Source on Ubuntu Systems CVM

1. Execute the following commands to import the MongoDB GPG public key and configure the software source.

```
sudo apt-key adv --keyserver hkp://keyserver.ubuntu.com:80 --recv 68818C72E52529D4
```

2. Execute the following command to configure the mirror path.

```
#Ubuntu 14.04
echo "deb [ arch=amd64 ] public/private network access URL trusty/mongodb-org/4.0 multivers
e" | sudo tee /etc/apt/sources.list.d/mongodb-org-4.0.list
#Ubuntu 16.04
echo "deb [ arch=amd64 ] public/private network access URL xenial/mongodb-org/4.0 multivers
e" | sudo tee /etc/apt/sources.list.d/mongodb-org-4.0.list
#Ubuntu 18.04
echo "deb [ arch=amd64 ] public/private network access URL bionic/mongodb-org/4.0 multivers
e" | sudo tee /etc/apt/sources.list.d/mongodb-org-4.0.list
```

3. Execute the following command to update the software package list.

```
sudo apt-get update
```

4. Execute the following command to install MongoDB.

```
sudo apt-get install -y mongodb-org
```

Accelerate Rubygems with Converge Cloud image

> Note:
> Before using, please ensure that Ruby is installed on your CVM.

Execute the following command to modify the RubyGems source address.

gem source -r https://rubygems.org/
gem source -a public/private network access URL

Installing Software on Ubuntu via Apt-get

Overview

To improve user efficiency of software installation on Cloud Virtual Machine and reduce the cost of downloading and installing software, Converge Cloud provides the Apt-get repository. In the Ubuntu environment, users can quickly install software through Apt-get. For the Apt-get repository, no additional software sources need to be added; software packages can be installed directly.

Prerequisites

You have logged in to the Cloud Virtual Machine running Ubuntu operating system.

Directions

> Note:
> The following steps demonstrate how to install Nginx.

View Available Software

Execute the following command to view available software.

```
sudo apt-cache search all
```

Installing Software on CentOS via YUM

Overview

To improve user efficiency of software installation on Cloud Virtual Machines and reduce the cost of downloading and installing software, Converge Cloud provides a YUM repository. In CentOS environment, users can quickly install the software using the yum command. For YUM repository, users do not need to add additional repositories and can directly install software packages.

Directions

Software Installation

1. Log in to the Cloud Virtual Machine using the root account.

2. Execute the following command to install the software. > Note: Starting from CentOS 7, MariaDB has become the default database package in the YUM repository. If your operating system is CentOS 7 or later, you will not be able to use MySQL with the yum command to install MySQL packages. You can choose to use the fully compatible MariaDB, or
   to install an earlier version of MySQL.

   ```
   yum install software-name
   ```

   During the software installation process, the system will automatically search for relevant software packages and dependencies, and prompt the user to confirm whether the found packages are suitable.

For example, when you execute yum install PHP command, after installing PHP, the interface will display as shown below:

```
================================================================================================================
 Package                  Arch                Version                              Repository             Size
================================================================================================================
Installing:
 php                      x86_64              5.4.16-46.el7                        os                    1.4 M
Installing for dependencies:
 apr                      x86_64              1.4.8-3.el7_4.1                      os                    103 k
 apr-util                 x86_64              1.5.2-6.el7                          os                     92 k
 httpd                    x86_64              2.4.6-89.el7.centos                  updates               2.7 M
 httpd-tools              x86_64              2.4.6-89.el7.centos                  updates                90 k
 libzip                   x86_64              0.10.1-8.el7                         os                     48 k
 mailcap                  noarch              2.1.41-2.el7                         os                     31 k
 php-cli                  x86_64              5.4.16-46.el7                        os                    2.7 M
 php-common               x86_64              5.4.16-46.el7                        os                    565 k

Transaction Summary
================================================================================================================
Install  1 Package (+8 Dependent packages)

Total download size: 7.7 M
Installed size: 27 M
Is this ok [y/d/N]:
```

3. After confirming that the software package are correct, type y and press Enter to start installing the software.
When the interface displays Complete , the installation is finished. As shown below:

```
Installed:
  php.x86_64 0:5.4.16-46.el7

Dependency Installed:
  apr.x86_64 0:1.4.8-3.el7_4.1             apr-util.x86_64 0:1.5.2-6.el7     httpd.x86_64 0:2.4.6-89.el7.centos
  httpd-tools.x86_64 0:2.4.6-89.el7.centos libzip.x86_64 0:0.10.1-8.el7      mailcap.noarch 0:2.1.41-2.el7
  php-cli.x86_64 0:5.4.16-46.el7           php-common.x86_64 0:5.4.16-46.el7

Complete!
[root@VM_5_10_centos ~]#
```

Viewing Installed Software Information

After the software installation is complete, you can execute different commands based on actual needs to view information.

- Run the following command to view the specific installation directory of the software package.

  rpm -ql software-name

  For example, if you execute rpm -ql php command to view the specific installation directory of PHP. As shown below:

```
[root@VM_5_10_centos ~]# rpm -ql php
/etc/httpd/conf.d/php.conf
/etc/httpd/conf.modules.d/10-php.conf
/usr/lib64/httpd/modules/libphp5.so
/usr/share/httpd/icons/php.gif
/var/lib/php/session
[root@VM_5_10_centos ~]#
```

- Run the following command to view the version information of the software package.

  rpm -q

  For example, if you execute rpm -q php command to view the PHP version information. As shown below:

```
[root@VM_5_10_centos ~]# rpm -q php
php-5.4.16-46.el7.x86_64
[root@VM_5_10_centos ~]#
```

Install software via zypper in OpenSUSE environment

Overview

In order to improve your software installation efficiency on the cloud server and reduce the cost of downloading and installing software, Converge Cloud provides zypper download sources. Users of openSUSE and some SLES cloud servers can quickly install software via zypper. This document uses openSUSE as an example to guide you through quickly installing software with zypper.

Directions

Viewing Software Sources

1. Use the root account to log in to the openSUSE operating system on the CVM.
2. Execute zypper service-list or zypper sl command to list software sources.
   For example, Running zypper sl returns information similar to the following:

```
VM 5 10 suse:~ # zypper sl
# | Alias                          | Name                           | Enabled | GPG Check | Refresh | Type
--+--------------------------------+--------------------------------+---------+-----------+---------+-------
1 | openSUSE-42.3-Oss              | openSUSE-42.3-Oss              | Yes     | (r ) Yes  | No      | yast2
2 | openSUSE-42.3-Update-Oss       | openSUSE-42.3-Update-Oss       | Yes     | (r ) Yes  | No      | rpm-md
3 | openSUSE-42.3-Update-non-Oss   | openSUSE-42.3-Update-non-Oss   | No      | ----      | ----    | NONE
4 | openSUSE-42.3-non-Oss          | openSUSE-42.3-non-Oss          | No      | ----      | ----    | NONE
VM 5 10 suse:~ #
```

   - If the available source has been added to the software source, please install the software package.
   - If the software source is not added as available, please add the software sources.

Add software source

Execute zypper service-add or zypper sa command to manually add software sources.
For example, execute zypper sa command, an example of which is as follows:

```
zypper sa -t YaST http://mirrors.convergecloud.com/opensuse opensuse
zypper sa -t YaST http://mirrors.convergecloud.com/opensuse/update update
```

Installing Software Packages

1. Execute zypper search or zypper se command to search for software packages.
   For example, to search for the Nginx package, you can execute the following command:

zypper se nginx

The result resembles the following is returned:

```
VM 5 10 suse:~ # zypper se nginx
Loading repository data...
Warning: Repository 'openSUSE-42.3-Update-Oss' appears to be outdated. Consider using a different mirror or server.
Reading installed packages...

S | Name                | Summary                                                    | Type
--+---------------------+------------------------------------------------------------+-----------
  | dehydrated-nginx    | Nginx Integration for dehydrated                           | package
  | nginx               | A HTTP server and IMAP/POP3 proxy server                   | package
  | nginx               | A HTTP server and IMAP/POP3 proxy server                   | srcpackage
  | pcp-pmda-nginx      | Performance Co-Pilot (PCP) metrics for the Nginx Webserver | package
  | python-certbot-nginx | Nginx plugin for Certbot                                 | package
  | vim-plugin-nginx    | VIM support for nginx config files                         | package
VM 5 10 suse:~ #
```

2. Based on the searched software package name, execute zypper install or zypper in to install the software. > Note: If you need to install multiple software packages, separate the software package names with spaces. When installing software, any required dependencies will be automatically downloaded and installed. There is no need to manually install dependency packages.

For example, to install Nginx, execute the following command:

zypper install nginx

For example, to install PHP and PHP-FPM, you can execute the following command:

zypper install MySQL-server-community php5-mysql php5 php5-fpm

Viewing Installed Software Information

1. After the software installation is complete, you can view the installation directory of the software package by executing the following command.

   rpm -ql

For example, to view the specific installation directory of the Nginx software package, execute the following command:

rpm -ql nginx

Information resembles the following is returned:

```
VM 5 10 suse:~ # rpm -ql nginx
/etc/logrotate.d/nginx
/etc/nginx
/etc/nginx/conf.d
/etc/nginx/fastcgi.conf
/etc/nginx/fastcgi.conf.default
/etc/nginx/fastcgi_params
/etc/nginx/fastcgi_params.default
/etc/nginx/koi-utf
/etc/nginx/koi-win
/etc/nginx/mime.types
/etc/nginx/mime.types.default
/etc/nginx/nginx.conf
/etc/nginx/nginx.conf.default
/etc/nginx/scgi_params
/etc/nginx/scgi_params.default
/etc/nginx/uwsgi_params
/etc/nginx/uwsgi_params.default
/etc/nginx/vhosts.d
/etc/nginx/win-utf
/srv/www/htdocs/50x.html
/usr/lib/perl5/vendor_perl/5.18.2/x86_64-linux-thread-multi/auto/nginx
/usr/lib/perl5/vendor_perl/5.18.2/x86_64-linux-thread-multi/auto/nginx/nginx.bs
```

2. Run the following command to view the version information of the software package.

```
rpm -q
```

For example, to view the version information of the Nginx software package, execute the following command:

```
rpm -q nginx
```

Information resembles the following is returned:

```
VM 5 10 suse:~ # rpm -q nginx
nginx-1.14.2-2.7.1.x86_64
VM 5 10 suse:~ #
```

Custom Data
Setting Custom Data (Linux Cloud Virtual Machine)

Overview

When creating Cloud Virtual Machine, you can configure the instance by specifying custom data. When Cloud Virtual Machine starts for the first time, the custom data is passed to the cloud server as text and executed. If you purchase multiple Cloud Virtual Machines at once, the custom data will be executed on all cloud servers upon their first startup.
This document uses an example of passing a PowerShell script during the first startup of a Linux Cloud Virtual Machine.

Notes

- Supported Linux operating systems for custom data include:
  - 64-bit Operating Systems: CentOS 6.8 64-bit and above, Ubuntu Server 14.04.1 LTS 64-bit and above.
  - 32-bit Operating Systems: CentOS 6.8 32-bit and above
- Commands are executed by passing text only during the initial startup of the Cloud Virtual Machine.
- Note: The text must be Base64 encoded. Please encode the text in a Linux environment to avoid format incompatibility .
- Use the root account to execute the user data input text. Do not use the "sudo" command in the script. Any files you create will be owned by root. If you need non-root users to have file access, modify the permissions in the script.
- Executing tasks specified in custom data during startup will increase the server's startup time. Please wait a few minutes and test if the task has been successfully executed.
- In this example, the Shell script must start with `#!` character and the path to the interpreter that will read the script (usually `/bin/bash`).

Directions

Writing the Shell Scripts

1. Execute the following command to create a Shell script file named "script_text.sh".

```
vi script_text.sh
```

2. Press i Switch to edit mode, refer to the following content, write and save the "script_text.sh" script file.

```
#!/bin/bash
echo "Hello Converge Cloud."
```

Note:
Shell scripts must start with #! character and the path to the interpreter that will read the script (usually /bin/bash). For more information about Shell scripts, refer to the Linux Documentation Project (tldp.org) on BASH Programming.

Encoding Script Files Using Base64

1. Execute the following command to Base64 encode the script_text.sh script file.

```
# Base64 encode the script.
base64 script_text.sh
```

The following information will be returned:

```
# The encoded result will be:
IyEvYmluL2Jhc2gKZWNobyAiSGVsbG8gVGVuY2VudCBDbG91ZC4iCg==
```

2. Run the following command to verify the result of Base64 encoding script.

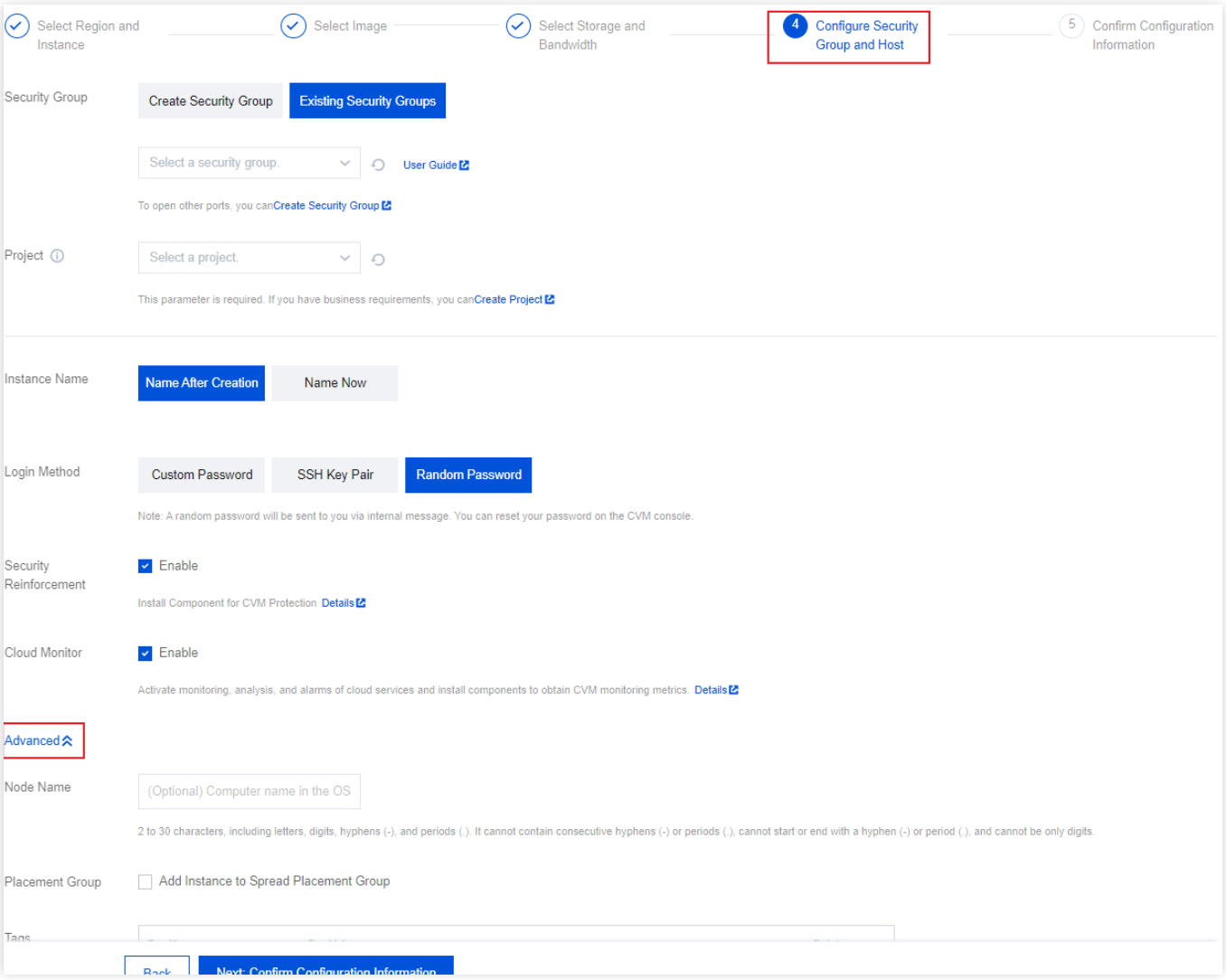
```
# Perform Base64 decoding on the returned result to verify whether it is the command to be executed
echo "IyEvYmluL2Jhc2gKZWNobyAiSGVsbG8gVGVuY2VudCBDbG91ZC4iCg==" | base64 -d
```

Transmitting Text

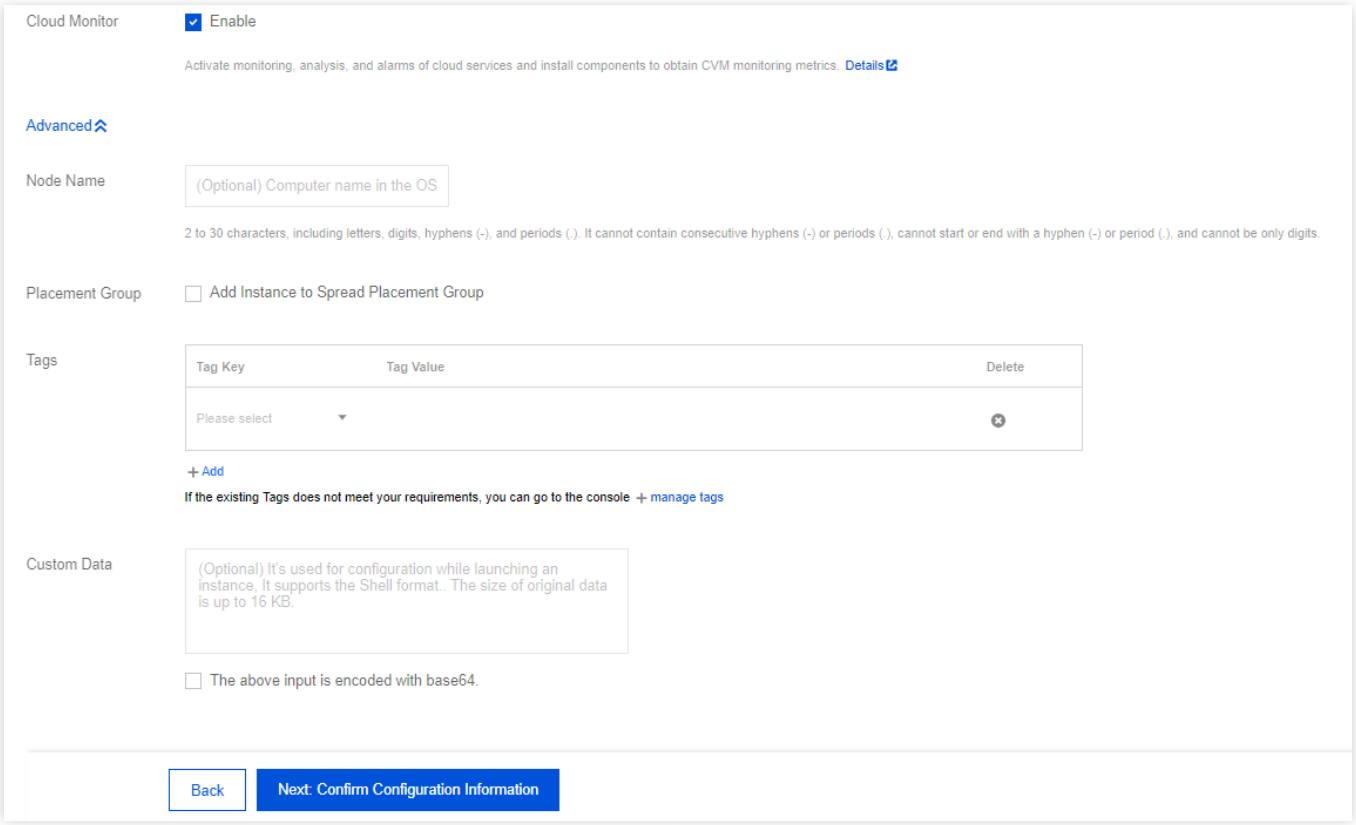
We provide multiple ways to start instances, mainly divided into the following two scenarios. Please select according to your actual needs:

Transmitting Through the Console

1. See Create an Instance Purchase an Instance. In Step 4: Set Security Group and Host, click Advanced Settings. As shown below:



2. In the "Advanced settings" section, enter the encoded result returned by the Base64 encoded script file in the "Custom data" text box. As shown below:
   For example, the result returned by Base64 encoding the script file script_text is:
   IyEvYmluL2Jhc2gKZWNobyAiSGVsbG8gVGVuY2VudCBDbG91ZC4iCg== .



3. Follow the instructions on the interface to complete the creation of the Cloud Virtual Machine. > Note: The Cloud Virtual Machine will execute the script using the open-source software "cloud-init". For more information about cloud-init, refer to the .

Transmitting through API

When you create a Cloud Virtual Machine through API, you can assign the encoded result returned by the Base64 encoded script file to the UserData parameter of the RunInstances interface to transmit the text.

For example, create a request parameter for a Cloud Virtual Machine with a UserData parameter, as shown below:

```
https://cvm.api3.convergecloud.com/?Action=RunInstances
  &Version=2017-03-12
  &Placement.Zone=ap-cityA-2
  &ImageId=img-pmqg1cw7
  &UserData=IyEvYmluL2Jhc2gKZWNobyAiSGVsbG8gVGVuY2VudCBDbG91ZC4iCg==
  &<Common request parameters>
```

Setting Custom Data (Windows Cloud Virtual Machine)

Overview

When creating Cloud Virtual Machine, you can configure the instance by specifying custom data. When Cloud Virtual Machine starts for the first time, the custom data is passed to the cloud server as text and executed. If you purchase multiple Cloud Virtual Machines at once, the custom data will be executed on all cloud servers upon their first startup. This document takes the example of passing a PowerShell script when a Windows Cloud Virtual Machine is started for the first time.

Notes

- Windows operating systems that support custom data include:
  - Windows Server 2016 Datacenter Edition 64-bit (English)
  - Windows Server 2012 R2 Datacenter Edition 64-bit (English)
- Commands are executed by passing text only during the initial startup of the Cloud Virtual Machine.
- Custom data content shall not exceed 16KB before Base64 encoding.
- Custom data is transmitted via Base64 encoding. If you directly copy non-base64 script files, please do not check Input as Base64 Encoded Text.
- Executing tasks specified in custom data during startup will increase the server's startup time. Please wait a few minutes and test if the task has been successfully executed.
- In this example, you use the PowerShell tag to specify a Windows PowerShell script, for example, the tags.

Directions

Prepare the Text

Please prepare the text based on your actual needs:

PowerShell Script

Using PowerShell Tag, prepare a PowerShell script file.

For example, if you need to create a file named "cloud.txt" with the content "Hello Cloud." in the C: drive of the Cloud Virtual Machine, you can use the PowerShell tag to prepare the following content:

```
<powershell>
"Hello Converge Cloud." | Out-File  C:\cloud.txt
```

```
</powershell>
```

Base64 Encoded Script

1. Execute the following command to create a PowerShell script file named "script_text.ps1".

   ```
   vi script_text.ps1
   ```

2. Press i to switch to Edit Mode, refer to the following content, write and save the "script_text.ps1" script file.

   ```
   <powershell>
   "Hello Cloud." | Out-File  C:\cloud.txt
   </powershell>
   ```

3. Execute the following command to perform Base64 encoding on the script file "script_text.ps1".

   ```
   base64 script_text.ps1
   ```

   The following information will be returned:

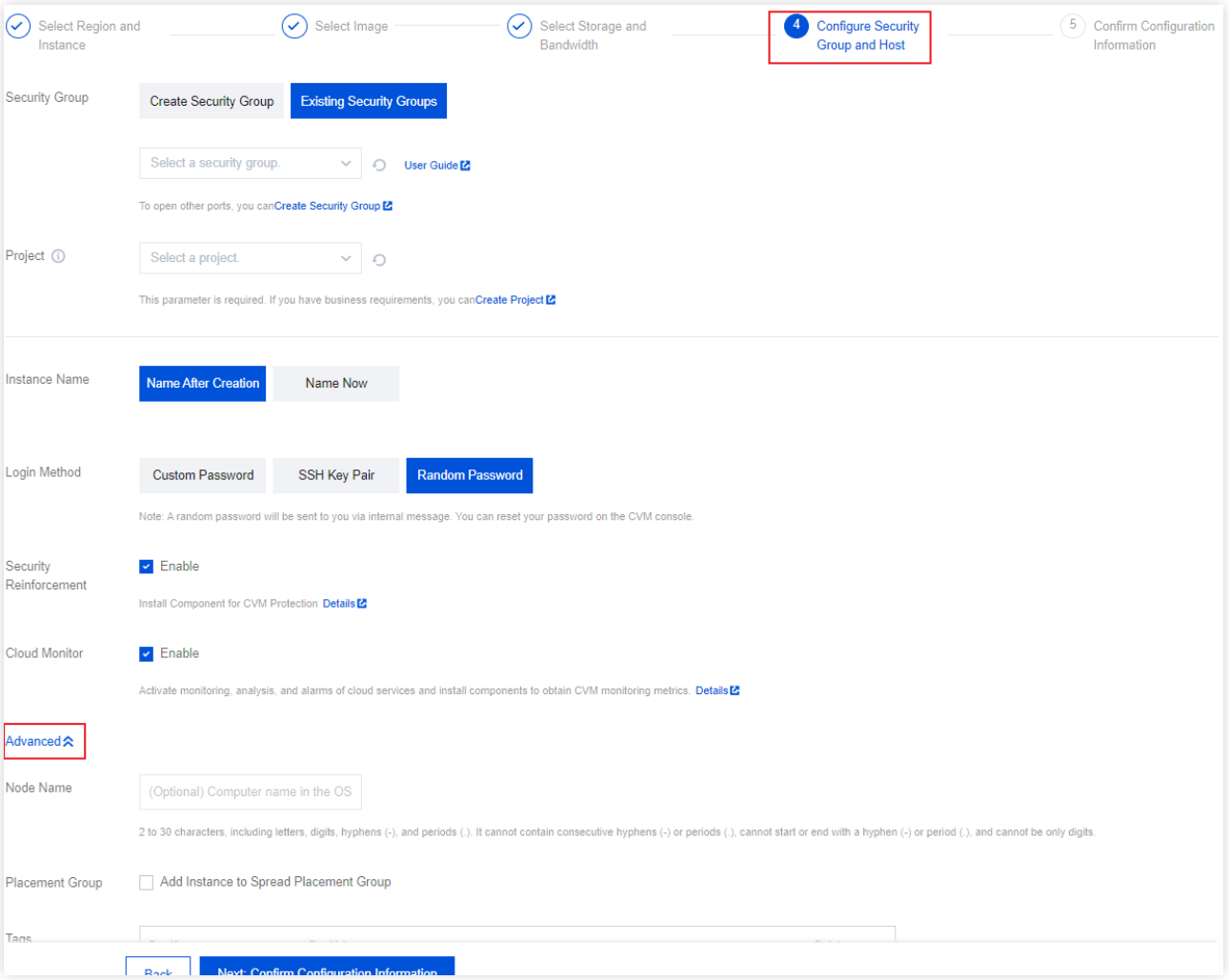
   ```
   PHBvd2Vyc2hlbGw+CiJIZWxsbyBUZW5jZW50IENsb3VkLiIgfCBPdXQtRmlsZSAgQzpcdGVuY2VudGNsb3VkLnR
   4dAo8L3Bvd2Vyc2hlbGw+Cg==
   ```

Transmitting Text

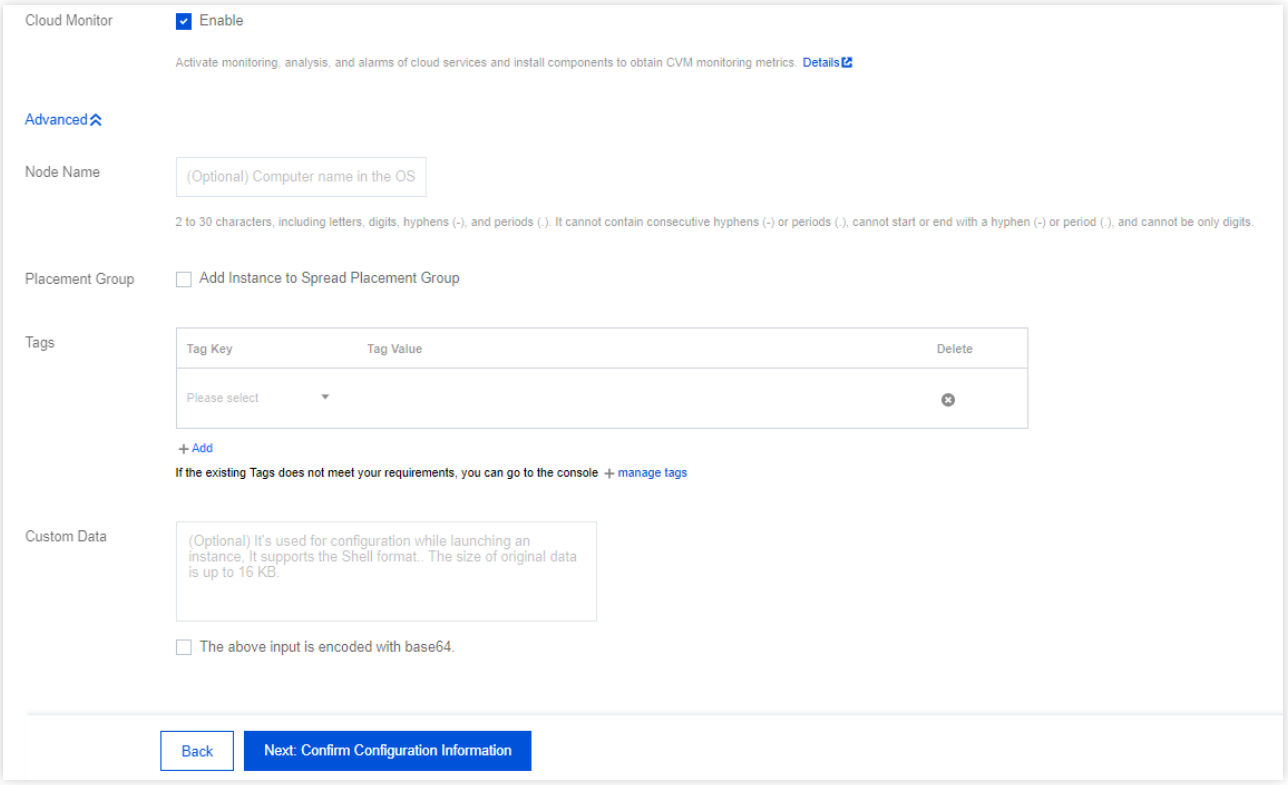
We provide multiple ways to start instances, mainly divided into the following two scenarios. Please select according to your actual needs:

Transmitting through the Official Website or Console

1. See Create an Instance Purchase an Instance. In Step 4: Set Security Group and Host, click Advanced Settings. As shown below:



2. In Advanced Settings, enter the prepared text in the Custom Data text box according to your actual needs.
   - PowerShell script: Type in PowerShell script.
   - Base64 Encoded Script: First check the box for Input as Base64 Encoded Text, then input Base64 Encoded Script (#Base64Script). As shown below:



3. Follow the instructions on the interface to complete the creation of the Cloud Virtual Machine.

Transmitting through API

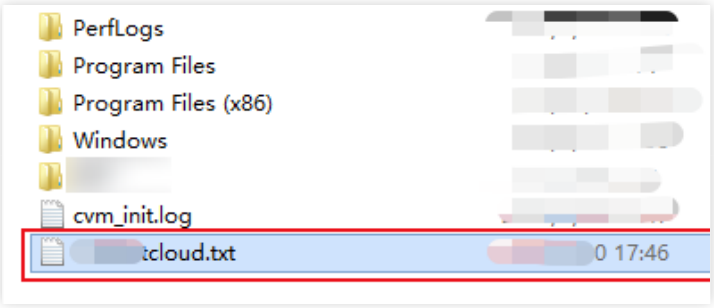
When you create a CVM through the API, you can assign the encoding result returned from the Base64 Encoded Script to the UserData Parameter of the RunInstances API to pass the text.

For example, create a request parameter for a Cloud Virtual Machine with a UserData parameter, as shown below:

```
https://cvm.api3.convergecloud.com/?Action=RunInstances
  &Version=2017-03-12
  &Placement.Zone=ap-cityA-2
  &ImageId=img-pmqg1cw7
  &UserData=PHBvd2Vyc2hlbGw+CiJIZWxsbyBUZW5jZW50IENsb3VkLiIgfCBPdXQtRmlsZSAuXHRlbmNlbnRjbG91ZC50eHQKPC9wb3dlcnNoZWxsPgo=
  &<Common request parameters>
```

Verifying custom data configuration

1. Log in to the CVM.
2. In the operating system interface, open the C:\ drive and check whether cloud.txt text file exists.
   In the operating system interface, open the C:\ drive and check whether cloud.txt text file exists.


PerfLogs
Program Files
Program Files (x86)
Windows
cvm_init.log
tcloud.txt
0 17:46

System
System Activation

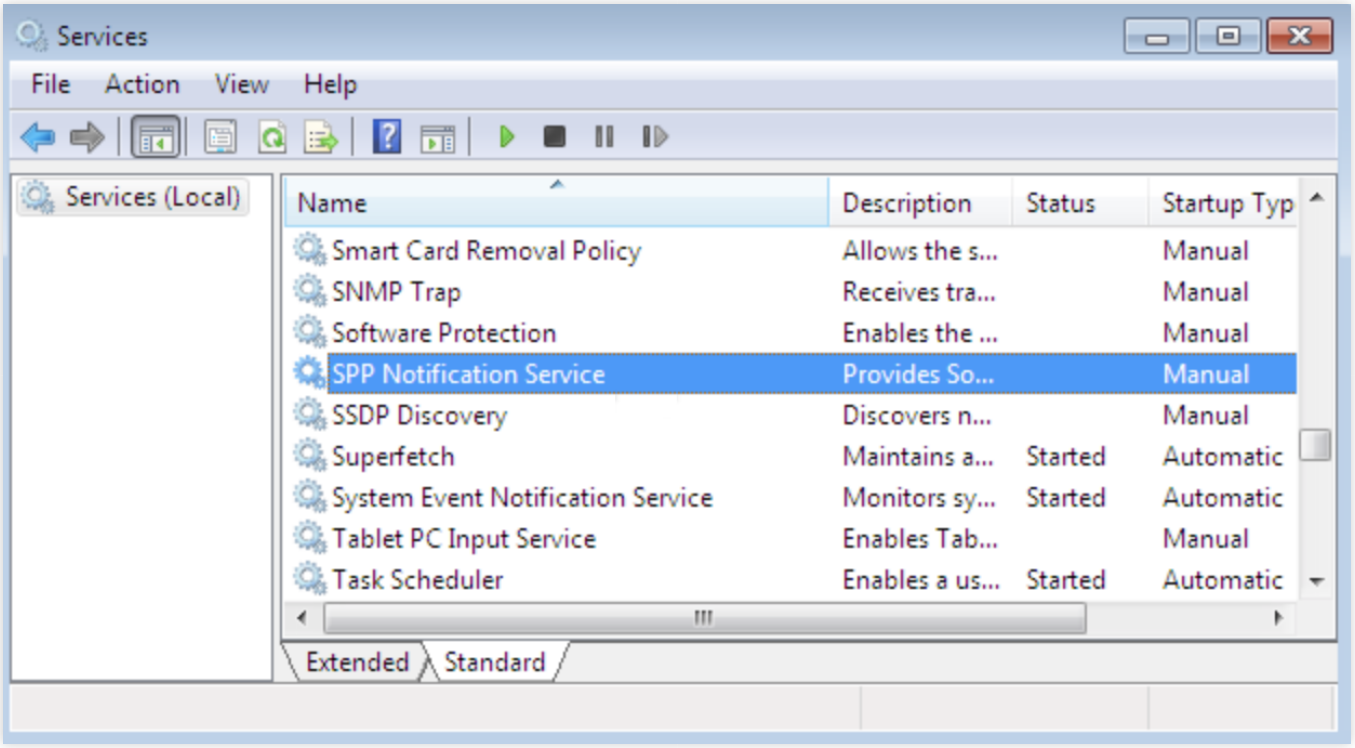
Windows Server System Activation

Converge Cloud The Cloud Virtual Machine uses KMS to authorize Windows Servers Licensing.

> Note:
> - This document only applies to Windows Server public images provided by Converge Cloud. Custom images or externally imported images cannot be activated using this method.
> - Windows Server 2008 and Windows Server 2012 require this activation method. The KMS address is correctly configured by default in the Windows Server 2016 public image and does not need modification.

Activation Prerequisites

1. The SPP Notification Service in Windows is responsible for executing activation-related services and must be running properly. As shown below:



2. Some optimization software may disable the ability to modify the execution permissions of service-related executables, such as sppsvc.exe. If the execution permissions of sppsvc.exe are modified, the service may not run properly.
   Before attempting to activate a Windows Cloud Virtual Machine, ensure that this service and other basic functions on Windows are operating normally.

3. Contact engineers to obtain the Windows server activation script activate-win.bat .

Automatic Activation

Converge Cloud provides a script to simplify the manual activation steps for Windows Servers.

1. Log in to the Windows CVM.
2. Run the script to complete automatic activation.

Manual Activation

Notes

On some systems, if the system clock is incorrect, errors may occur during manual activation. In such cases, you need to synchronize the system clock first. The steps to synchronize the clock are as follows:

> Note:
> If the system clock on the Windows Cloud Virtual Machine is correct, proceed directly to the activation steps.

1. Log in to the Windows CVM.

2. In the operating system interface, click Start > Run, and input cmd.exe to open the console window.

3. In the console window, execute the following commands in sequence to synchronize the system clock.

```
w32tm /config /syncfromflags:manual /manualpeerlist:"ntpupdate.convergecloud.com"
w32tm /resync
```

System Update

Overview

This document provides guidance on updating Windows patches on a Windows Server 2012 operating system.

Directions

Updating via Public Network

You can install patches using the system's Windows Update service. Follow the steps below:

1. Log in to the Windows CVM.
2. Click Start > Control Panel > Windows Update to open the Windows Update window.
3. Click Check for Updates and wait for the process to complete.
4. After the check is completed, click [n important updates available] or [n optional updates available] in Windows Update.
5. In the pop-up [Select Updates to Install] window, select the update programs to be installed and click Install.
   After the update is installed, if the system prompts that the system needs to be restarted, please restart the CVM in time.

> Note:
> When restarting the CVM after completing the patch update, you need to log in and monitor the CVM via VNC. If the system displays prompts such as "Updating, do not turn off the power" or "Configuration not complete", do not perform a hard shutdown. A hard shutdown may damage your CVM.

Updating via Private Network

If your CVM cannot connect to the public network, you can use the Converge Cloud private network patch server to install updates. The Converge Cloud Windows patch server includes most common updates for Windows but does not include hardware driver packages or some less frequently used server updates. Some less common services might not have updates available on the Converge Cloud private network patch server.

How to use the Converge Cloud private network patch server is as follows:

1. Log in to the Windows CVM.
2. Use IE browser to access and download the Converge Cloud private network setting tool (wusin.bat).
3. wusin.bat: Contact engineers to obtain it.
4. Use the administrator Cloud Platform Command Line Interface (CMD) to open wusin.bat. As shown below:

> Note:
> If you run the 'wusin.bat' tool directly via IE, the console window will automatically close, and you won't be able to observe the output information.

If you no longer need to use the Converge Cloud private network Windows patch server, you can download the cleanup tool wusout.bat to clean up. The method is as follows:

1. Log in to the Windows CVM.
2. Use IE browser to access and download the Converge Cloud intranet cleanup tool (wusout.bat). Contact engineers to obtain wusout.bat.
3. Use the Administrator Cloud Platform Command Line Interface (CMD) to open wusout.bat. As shown below:

> Note:
> If you execute the wusout.bat tool directly through IE, the console window will be automatically closed and the output information cannot be observed.

Shutdown

Analysis of Virtual Client Shutdown Process

Shutdown Process

The shutdown process of a Converge Cloud Windows instance is as follows:

1. The libvirt on the host transmits the shutdown command to the qemu component through the qmp protocol.
2. The qemu component transmits the shutdown command to the instance by injecting the ACPI interrupt (For details, see the vmcs technical documentation).
3. After receiving a shutdown signal, the Windows instance notifies applications and service processes to exit.
4. Close the core service processes.
5. Turn off the power.

> Note:
> In Step 3 and Step 4, the shutdown order of various applications and services may vary depending on the system settings.

Windows is a closed-source system that provides some APIs to allow kernel-mode and user-mode programs to intervene in the shutdown process. At the same time, some services of Windows itself will affect the shutdown process during operation, resulting in failure to shut down the computer. Therefore, in some cases, the Windows shutdown process can be quite lengthy.

Hard Shutdown

In virtual scenes, in addition to notifying Windows of its own shutdown through messages, there is also another way to stop instances. This method is similar to turning off the power on a physical machine. We call this shutdown method hard shutdown. The shutdown operation initiated by system signals is relatively referred to as soft shutdown.

Hard shutdown has an impact on both Windows itself and user experience, mainly in the following two aspects:

1. Hard shutdown interrupts certain services and applications, which may cause them to malfunction, such as unsaved documents or uncompleted Windows Update process.
2. As the Windows NTFS system (or earlier systems such as FAT32) will write some critical data during the shutdown process, hard shutdown may cause these critical data not to be written to the disk, causing Windows to believe that the NTFS file system is damaged.

Based on the above reasons, we recommend that users of Converge Cloud prioritize soft shutdown to shut down Windows instances.

Several Scenes of Shutdown Failure

There may be some problems in the Windows system that affect the shutdown process and result in shutdown failure. Shutdown failures include but are not limited to the following scenes:

1. The Windows update process may extend the shutdown time. When Windows performs certain patch operations, it will display prompt messages when shutting down the system. At this time, prompt messages such as "Please do not turn off the computer power or unplug the power cord" will generally appear on the screen.
2. If the Shutdown Event Tracking mechanism is enabled in the Windows system, when errors occur in the system's services and drivers and lead to shutdown of the system, the system will, based on the configuration, prompt the user with a dialog box or allow the user to fill in an error description, and will wait for the user to complete these operations before shutdown. Windows will not shut down until the user completes the specified operation.
3. Windows can be set to not allow shutdown when the user is not logged in to the system. In this case, the soft shutdown command sent by the virtual host will be discarded by Windows, making it impossible to shut down.
4. Before Windows shuts down, it will broadcast a shutdown message to every service and application. If these programs do not return a shutdown response after receiving this message, the shutdown process will not be proceeded. In this scene, Windows can be set to ignore this process.
5. In the Windows power management settings, if the Windows Processing Method When the Power Button Is Pressed is set to Ignore or No Operation, Windows will ignore the shutdown event of the virtualization host.
6. When Windows enters hibernation due to power management settings, it will not process the shutdown event.
7. If some malicious software is installed in the Windows system, or if a Trojan or virus is infected, the Windows system environment itself is damaged, which may cause Windows shutdown to be blocked.

When Converge Cloud releases the Windows public image, most of the above scenes are optimized so that soft shutdown can be completed smoothly. However, these optimization measures cannot guarantee smooth shutdown in scenes where Windows is infected with viruses or Trojans and the system is damaged. Furthermore, if these settings in the user's Windows instance are adjusted again, a smooth soft shutdown still cannot be guaranteed.

Forced shutdown may cause risks. It is recommended to perform hard shutdown only when it is absolutely necessary.

Configuring High-performance Power Management

Overview

On the Windows Server operating system, high-performance power management needs to be configured to support soft shutdown of instances. Otherwise, the Cloud Virtual Machine console can only shut down the instance through hard shutdown. This document uses Windows Server 2012 operating system as an example to describe how to configure power management.

Operating Instructions

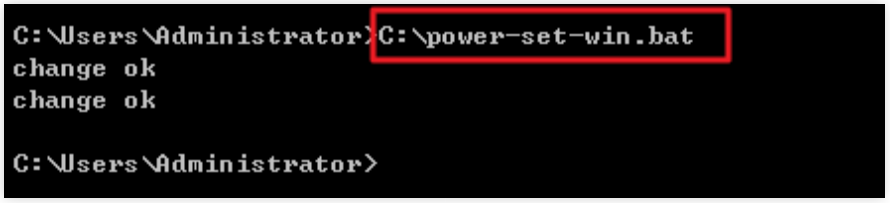
Modifying power management does not require a computer restart.
Contact engineers to obtain the power management modification and configuration tool power-set-win.bat .

Directions

1. Log in to the Windows CVM.

2. You can download the Converge Cloud power management modification and configuration tool (power-set-win.bat) to the C: drive.

3. Open power-set-win.bat using the administrator Cloud Platform Command Line Interface (CMD). As shown below:



4. Run the following command to view the current power management scheme.

   powercfg -L

The following results are returned:

5. In the operating system interface, click > Control Panel > System and Security > Power Options to open the Power Options window.

6. In the Power Options window, click Change Plan Settings.

7. In the open "Edit Plan Settings" window, modify the idle shutdown times for the monitor and hard disk.

Windows Recovery Mode

Overview of Windows Recovery Mode

Windows System Recovery Mode (Recovery) indicates that Windows uses the automatic repair feature. When Windows detects certain system issues and believes that continued use will cause damage to the system, it will prevent Windows from starting and enter the System Recovery Options interface, providing a state for users to repair, backup, or restore the system.
The System Recovery Options include several tools, such as Startup Repair, System Restore and Windows Memory Diagnostics. These tools can be used to fix problems, backup data, and perform system recovery.
When the user cannot log in to the CVM remotely and the following status appears after logging in to the CVM through the console, it indicates that the Windows CVM has entered the recovery mode.

Reasons for Entering Recovery Mode

Common reasons for entering the recovery mode are as follows:

- The power is forcefully turned off while Windows is running or shutting down. This includes forced shutdowns performed in the console. Improper shutdown may cause the system to lose some critical data and thus enter recovery mode.
- The power is cut off during Windows update. Critical data is lost during the update and the system enters the recovery mode.
- The system is damaged by a Trojan or virus.
- There is a bug in Windows core services. A risk is detected through Windows self-check.
- The system loses critical data or is damaged. Users may accidentally damage system files, causing

the system to enter the recovery mode.

Precautions

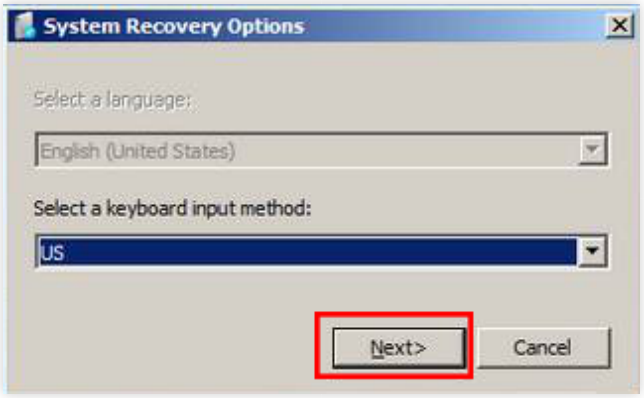
Converge Cloud recommends that users take the following precautions:

- When shutting down, open the console to observe the Windows shutdown process. Converge Cloud soft shutdown has a timeout mechanism. After a soft shutdown is performed, if the system does not shut down within the scheduled time, a prompt of failure will pop up. If the shutdown is slow or Windows update occurs during shutdown, just wait for the CVM to shut down and do not force shutdown. It is recommended to refer to Several Scenes of Shutdown Failure.
- Check whether there are any abnormal programs or processes such as Trojans or viruses in the system.
- Check whether the system management and anti-virus software are running normally.
- Keep Windows update packages up-to-date in a timely manner, especially some important updates and security updates.
- Regularly check the system event log to verify if there are any errors in the core services.

Solution

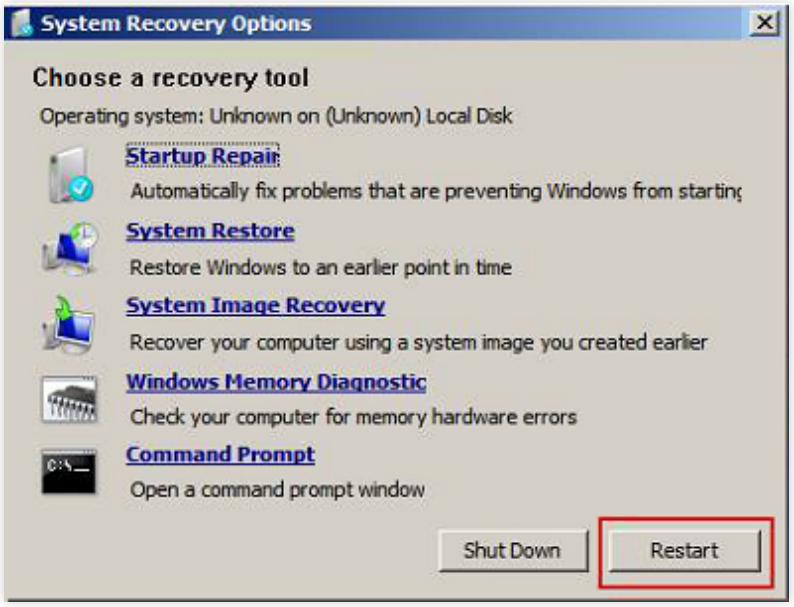
After Windows enters the recovery mode, users can try to continue startup and running, or perform automatic recovery. Minor problems can be repaired by Windows itself. Execute the following steps:

1. Log in to the CVM from the console.
2. In the recovery mode interface, click Next.



3. When the system recovery options appear, click Next using the default plan.

4. Click [Restart] and quickly press F8 on the keyboard.



5. Select Normal Boot of Windows.

   If Windows cannot start, reinstall the system in the console. For details, refer to Using the Console to Reinstall the System.

Updating Virtio Network Interface Drivers

Overview

Converge Cloud CVM Window Server 2008 R2 Enterprise Edition SP1 and Windows Server 2012 R2 optimize the network performance of virtual hardware through installing Virtio network interface drivers. Converge Cloud will continue to improve the network interface drivers to enhance performance and rectify faults. This document will guide you on how to update the Virtio network interface drivers and view the driver version.

Prerequisites

Log in to the Converge Cloud CVM.
Contact engineers to obtain the VirtIO network interface driver virtio_64_10003.msi .

Directions

Viewing the System Version Information

You can view your system version information through following steps:

1. Log in to the CVM, right-click on the desktop to click Computer > Attribute, to open the System window.
2. In View basic computer information of System, you can view the system version information.

Methods to Update Virtio Network Interface Drivers

> Note:
> The network may be intermittently disconnected during the update process. Before updating, check if it will affect your business. After the update, you will need to restart your computer.

1. Download the VirtIO network interface driver installation file suitable for Windows Server 2008 R2 and Windows Server 2012 R2 through the browser in the CVM.
2. After downloading, double-click to start the installer, select the Typical installation mode, and click Next.
3. In the security prompt that pops up, select Always trust software from "XXX" and click Install.
4. During the installation process, if the following pop-up box appears, please select Always install this driver software.

5. Follow the prompts and restart your computer to complete the update.

Viewing the Driver Version

1. Click , enter ncpa.cpl in the "Run" box, and press Enter.
2. In the opened Network Connection window, right-click the Ethernet icon and select Properties.
3. In the pop-up Ethernet Properties window, click Configure.
4. In the [XXX VirtIO Ethernet Adapter Properties] window, select the Driver tab to view the current driver version.

Modifying SID Operation Instructions

Overview

Security identifiers (SIDs) are used in Microsoft operating systems to identify computers and users. Due to the same SIDs of CVM instances produced based on the same image, it may cause the problem of being unable to join the domain. If you need to build a Windows domain environment, you need to modify the SIDs to join the domain.
This document takes the Windows Server 2012 operating system CVM as an example to describe how to use the system's built-in sysprep and sidchg tools to modify the SIDs.

> Note:
> These notes apply only to Windows Server 2008 R2, Windows Server 2012, and Windows Server 2016. If you need to modify SIDs in batches, you can create a custom image (select Execute sysprep to Create an Image). Modifying SIDs may cause data loss or system damage. It is recommended to prepare a system disk snapshot or image in advance.

Operation Methods

Modifying SIDs Using sysprep

> Note:
> After the SIDs are modified using sysprep, many system parameters, including IP configuration information, will be reset, and you must manually reset them. C:\Users\Administrator will also be reset, and some data on the system disk will be cleared. Make sure to back up your data in advance.

1. Log in to the CVM through VNC.

2. On the operating system interface, right-click Run, enter cmd, and press Enter to open CMD as an administrator.

3. In the administrator command line, execute the following command to save the current network configurations.

```
ipconfig /all
```

4. In the administrator command line, execute the following command to open the sysprep tool.

   ```
   C:\Windows\System32\Sysprep\sysprep.exe
   ```

5. In the opened [System Preparation Tool 3.14] window, make the following settings.
   - Set System Cleanup to Enter the System Out-of-box Experience (OOBE) and select General.
   - Set Shutdown Options to Restart.

6. Click OK and the system will restart automatically.

7. After the startup is complete, follow the wizard to complete the configurations (by selecting the language, resetting the password, etc.).

8. On the operating system interface, right-click Run, enter cmd, and press Enter to open CMD as an administrator.

9. Run the following command to verify whether the SIDs have been modified.

   ```
   whoami /user
   ```

   If the following information is returned, it indicates that the SIDs have been modified.

10. According to the network configuration information saved in Step 3, reset the network interface information (such as IP address, gateway address, DNS, etc.).

Modifying SIDs Using sidchg

1. Log in to the CVM.

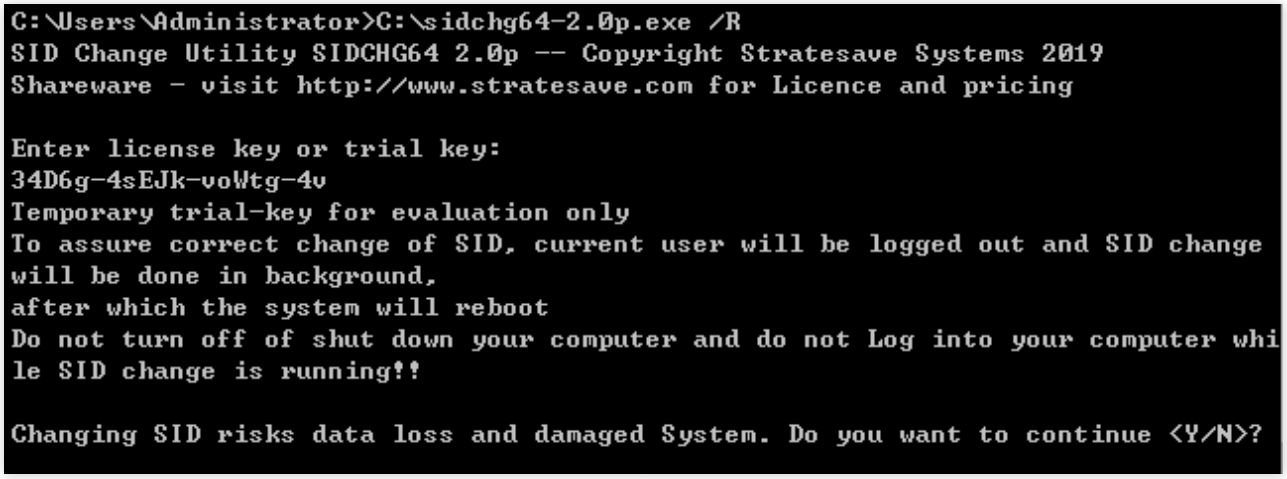
2. Access and download the sidchg tool through IE browser.
   Download address of sidchg tool: http://www.stratesave.com/html/sidchg.html

3. Using the administrator command line, run the following command to open the sidchg tool.
   For example, if the sidchg tool is stored in the C: drive, its name is sidchg64-2.0p.exe.

   Where, /R indicates automatic restart after modification, and /S indicates shutdown after modification. For details, refer to SIDCHG Official Manuals.

4. According to the interface prompts, enter license key or trial key, and press Enter.

5. According to the interface prompts, enter Y and press Enter.



6. In the prompt box for modifying the SID, click Confirm to reset the SID.
   During the reset process, the system will be restarted.

7. After the startup is complete, right-click Run, enter cmd, and press Enter to open the administrator command line

8. Run the following command to verify whether the SIDs have been modified.

   whoami /user

Others
Linux Common Operations and Commands

1. What is Linux server Load Average?

Load is used to measure the workload of the server, that is, the length of the computer CPU's task execution queue. The larger the value, the more processes are running and waiting to run.

2. How to view the Linux server load?

You can execute the w , top , uptime , and procinfo commands, or access the /proc/loadavg file to view the Linux server load.
For installation of the procinfo tool, see the relevant documentation on software installation in a Linux environment.

3. What if the server load is high?

The server load (Load/Load Average) is displayed based on the length of the process queue. When the server experiences high load (it is recommended to use the 15-minute average value as a reference), it may be due to insufficient CPU resources, I/O read/write bottlenecks, insufficient memory resources, the CPU undergoing intensive computing, or other reasons. It is recommended to execute vmstat , iostat , and top commands to determine the cause of overload and to find the specific process that occupies a large amount of resources for optimization.

4. How to view the server memory utilization?

You can execute free , top (After execution, you can execute shift+m to sort the memory), vmstat , and procinfo commands, or access the /proc/meminfo file to view the server memory utilization.

5. How to view the memory size occupied by a single process?

You can execute top -p PID , pmap -x PID , and ps aux|grep PID commands, or access the /proc/$process_id (PID of the process)/status file to view the memory size, for example, /proc/7159/status.

6. How to view the services and ports in use?

You can execute netstat -tunlp , netstat -antup , and lsof -i:PORT commands to view the services and ports in use.

7. How to view the server process information?

You can execute ps auxww|grep PID , ps -ef , lsof -p PID , and top -p PID commands to view it.

8. How to stop a process?

You can execute kill -9 PID (PID indicates the process number), and killall program name (e.g. killall cron) to stop the process.
If you need to stop a zombie process, you need to kill the parent process of the zombie process by executing the command kill -9 ppid (ppid is the parent process ID, which can be obtained by executing the ps -o ppid PID command, for example, ps -o ppid 32535).

9. How to find zombie processes?

You can execute the top command to view the totals of zombie processes, and execute ps -ef | grep defunct | grep -v grep to find the information about specific zombie processes.

10. Why the server port cannot be enabled?

The enabling of server ports needs to be viewed from the operating system itself and the application program.
In Linux operating systems, ports below 1024 can only be enabled by root users, which means that you need to run sudo su – to obtain the root permission before you can enable the server port.
As for application problems, it is recommended to investigate the cause of failure through application startup logs, such as port conflicts (the port 36000 used by the server system cannot be occupied), configuration problems, etc.

11. What commands can be commonly used to view Linux server performance?

Command Name	Description
top	Process monitoring commands are used to monitor the overall performance of the system. They can be executed to display information such as system load, process, CPU, memory, paging, etc. Shift+m and shift+p are often used to sort processes by memory and CPU usage.
vmstat	System monitoring commands focus on virtual memory, and can also be used to monitor such information as CPU, process, memory paging and IO status . For example, vmstat 3 10, which can be used to output the results every 3 seconds and can be executed 10 times.
iostat	It is a tool used to output CPU status and IO status and to display the system's IO information in detail. For example, iostat -dxmt 10, used to output detailed IO information in MB format every 10 seconds.
df	It is used to check the system's disk space usage. For example: df -m, used to display the disk space usage in MB.
lsof	It can be used to list the files opened in the system. Since Linux is based on the file system, this command is very helpful in system administration. For example: lsof -i:36000, used to display the process using port 36000 lsof -u root, used to display programs running as root lsof -c php-fpm, used to display the files opened by the php-fpm process lsof php.ini, used to display the processes that have opened the php.ini file
ps	Process view commands can be used to display detailed information of the process. Common command parameter combinations are ps -ef and ps aux. It is recommended to use ps -A -o to customize the output fields. For example: ps -A -o pid,stat,uname,%cpu,%mem,rss,args,lstart,etime |sort -k6,6 -rn, used to display outputs by the listed fields and to sort by the sixth field. ps -A -o comm |sort -k1 |uniq -c|sort -k1 -rn|head, used to list the process with the most running instances.

Other commonly used commands and files: free -m , du , uptime , w , /proc/stat , /proc/cpuinfo , /proc/meminfo .

12. What if Cron does not take effect?

The troubleshooting steps are as follows:

1. Verify if crontab is running properly.

   i. Execute the `crontab -e` command, to add the following test entry.

   ```
   \*/1 \* \* \* \* /bin/date >> /tmp/crontest 2>&1 &
   ```

   ii. Observe the `/tmp/crontest` file.
   If any problem is found, it is recommended to execute the `ps aux|grep cron` command to find the pid of cron, then execute the `kill -9 PID` command to end the cron process and execute the `/etc/init.d/cron start` command to restart cron.

2. Verify that the script path in the cron entry is absolute.

3. Check whether the user account running cron is correct, and check whether this account is included in `/etc/cron.deny` .

4. Check the execution permissions of the script, the script directory, and the file permissions of the logs.

5. It is recommended to run the script in the background and add "&" after the script entry. For example, `\*/1 \* \* \* \* /bin/date >> /tmp/crontest 2>&1 &` .

13. How to set a startup task for Cloud Virtual Machine (CVM)?

The Linux kernel startup sequence is as follows:

1. Start the `/sbin/init` process.
2. Execute the init scripts in sequence.
3. Run the level script `/etc/rc.d/rc\*.d` , the value of * is equal to the running mode. You can view it in `/etc/inittab` .
4. Execute `/etc/rc.d/rc.local` .

> Note:
> If you need to configure a startup task, you can configure it in the S**rclocal file in /etc/rc.d/rc*.d and you can also configure it in /etc/rc.d/rc.local .

14. Why is the server hard disk read-only?

The common reasons why the hard disk is read-only are as follows:

- The disk space is full.
  You can execute the df -m command to check disk space usage, and then delete unnecessary files to free up the disk space (It is not recommended to delete non-third-party files. Confirm whether you need to proceed with deletion).

- The disk inode resources are used up.
  You can execute the df -i command to view and confirm the related processes.

- The hardware is faulty.
  If the issue with the hosting application cannot be identified through the above methods, submit a ticket for assistance in pinpointing the problem.

15. How to view Linux system logs?

- The system-level log file storage path is /var/log .
- Common system logs are /var/log/messages .

16. How to find large files in the file system?

You can follow these steps below to find them:

1. Execute the df command to check the usage of disk partitions, such as df -m.

2. Execute the `du` command to view the size of a specific folder. For example, du -sh ./*, du -h --max-depth=1|head -10.
3. Execute the `ls` command to list files and file sizes, such as ls -lSh.

You can also execute the `find` command to directly view the file size under a specific directory, for example, find / -type f -size +10M -exec ls -lrt {} .

17. How to view the version of the server operating system?

You can view the system version by executing the following command:

- uname -a
- cat /proc/version
- cat /etc/issue

18. How to set the timeout for connecting to the CVM via SecureCRT?

When SecureCRT is connected to the CVM, you can prevent disconnection through the following settings:

1. Open SecureCRT Options.
2. Select Session Options and click Terminal.
3. In the Anti-idle box on the right, select Send Protocol NO-OP and set the time to every 120 seconds.

19. Why does deleting files on a Linux server not free up the hard disk space?

Cause:
After logging in to the Linux server and executing the `rm` command to delete files, and then executing the `df` command to view the hard disk space, it may be found that the available hard disk space has not

increased after files are deleted. The reason is as follows: When you execute the rm command to delete files, other processes are accessing the file. As a result, if you execute the df command to view the space, the space occupied by the deleted files will not be released immediately.

Solution:

1. Use root permission to execute the lsof |grep deleted command to view the PID of the process that is using the deleted file.
2. Execute the kill -9 PID command to kill the corresponding process.

Setting Linux CVM to Enter Single-user Mode

Linux Single-User Mode Guide

Overview

Linux users sometimes need to enter single-user mode to perform operations such as password recovery, fixing sshd issues, or system maintenance. This document describes how to enter single-user mode for mainstream Linux distributions.

Determining the Operating System

Follow the steps corresponding to your Linux distribution.

Logging in to the CVM via VNC

1. Log in to the CVM console.
2. On the instance management page, select the instance you want to log in to and click Log In.
3. In the pop-up *Log in to Windows/Linux Instance* window, select Other methods (VNC) and click Log in now.
4. In the login window that pops up, select Send Remote Command in the upper left corner and use the interface to access the login screen.

> Note:
> VNC login is required because single-user mode changes boot parameters and normal SSH or remote login may not work.

CentOS 6

> Note:

> CentOS 6 uses GRUB. The steps below are based on CentOS 6.9. Actual steps may vary slightly with different versions.

1. Log in to the CVM.
2. Open the GRUB configuration file:

```
vi /etc/grub.conf
```

3. Press i to enter the edit mode.

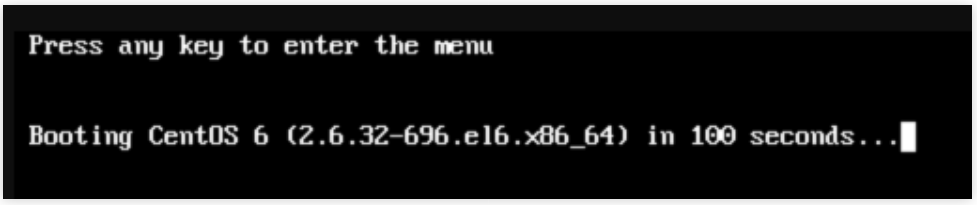
4. Find the waiting time parameter "GRUB-TIMEOUT" of the default startup item, and modify its value to the required time range according to actual needs.
   The default value of "GRUB-TIMEOUT" is 5 seconds. In order to avoid not being able to see the boot interface due to a short waiting time, it is recommended to adjust it to 60 seconds or more. > Note: This item affects the system startup time. After completing the configuration, you need to modify it back to the default value.

5. Press Esc to exit the edit mode, enter :wq, and press Enter.
   Save the settings and exit the VI editor.

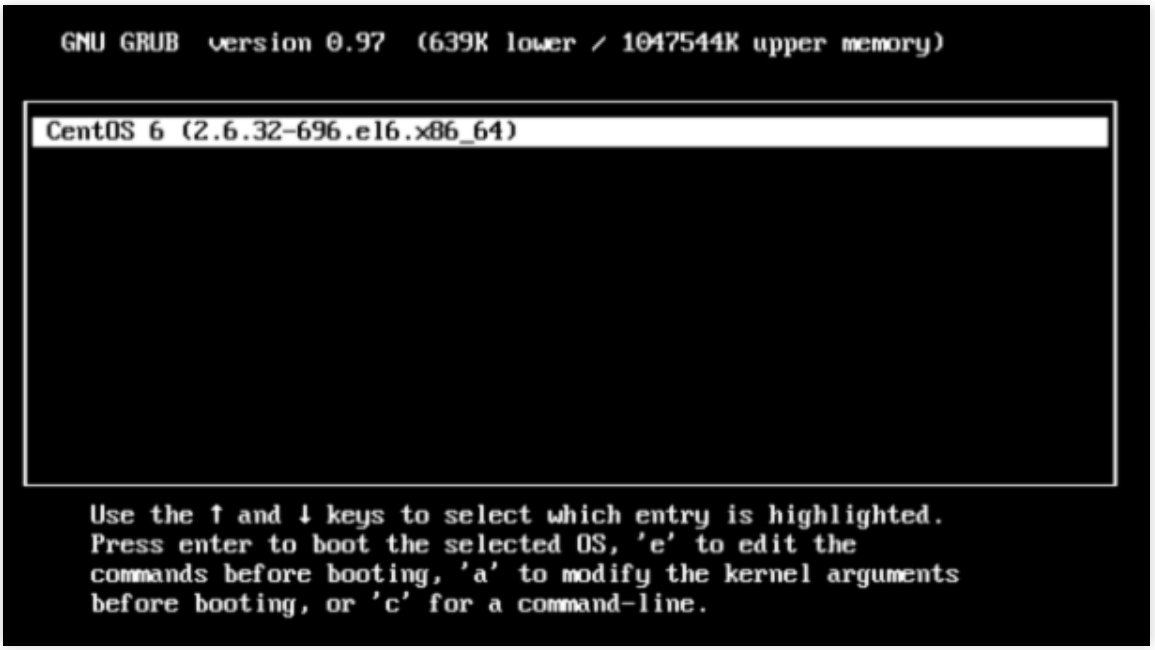
6. Run the following command to restart the CVM.

   ```
   reboot
   ```

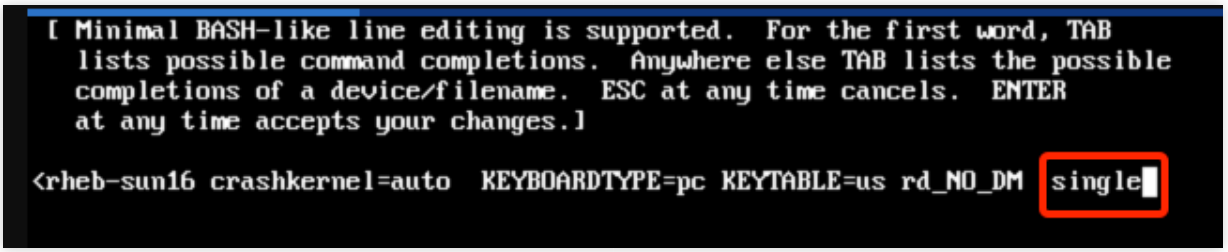
7. Wait for about 1 minute and log in to the CVM instance through the VNC. The login interface is shown below:



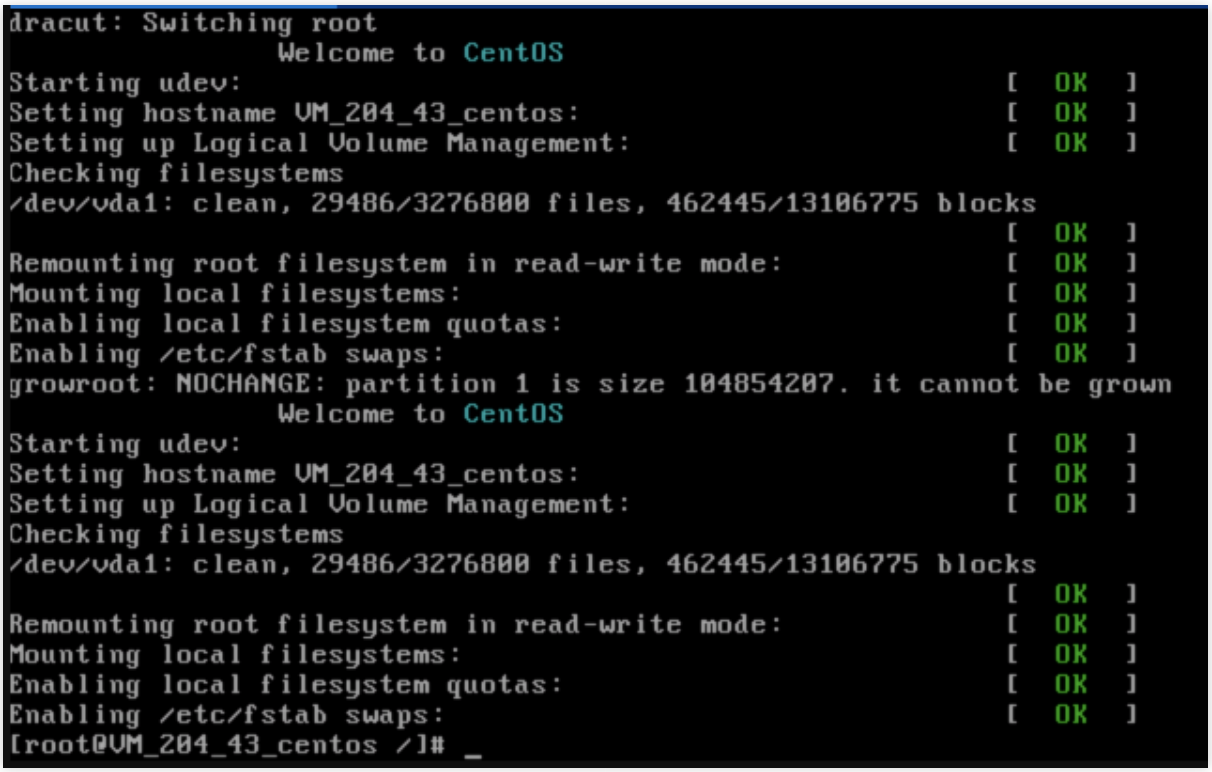
8. Press any key to enter the menu. As shown below:



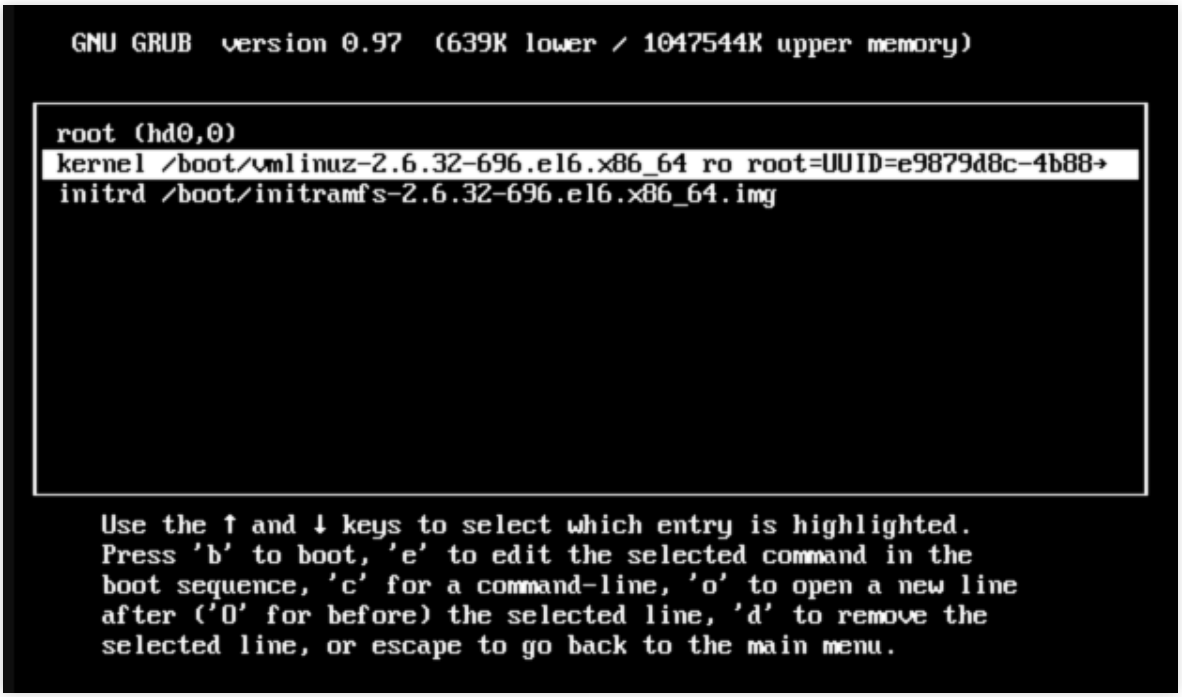
9. Press e to enter the kernel editing interface and enter single. As shown below:



10. Press Enter. As shown below:



11. In the interface shown below, press b to enter the single-user mode.



12. Run the following command to exit the single-user mode.

exec /sbin/init

CentOS 7

> Note:
> Unlike CentOS 6, CentOS 7 and later versions use GRUB 2. The following steps are based on CentOS 7.5 as an example. The detailed steps may vary slightly depending on the version of the operating system.

1. Log in to the CVM.

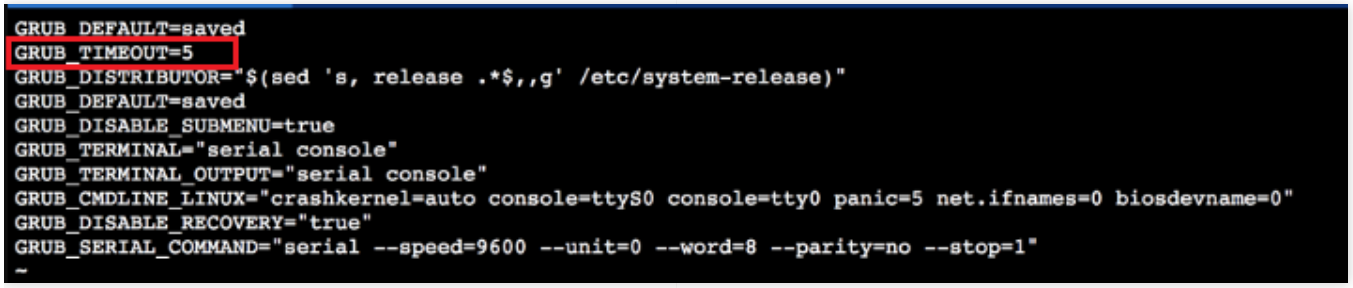
2. Run the following command to open the /etc/default/grub file.

   vi /etc/default/grub

3. Press i to enter the edit mode.

4. Find the waiting time parameter "GRUB-TIMEOUT" of the default startup item, and modify its value to the required time range according to actual needs. As shown below:
   The default value of "GRUB_TIMEOUT" is 5 seconds. In order to avoid not being able to see the boot interface due to a short waiting time, it is recommended to adjust it to 60 seconds or more.

   > Note: This item affects the system startup time. After completing the configuration, you need to modify it back to the default value.



5. Press Esc to exit the edit mode, enter :wq, and press Enter.
Save the settings and exit the VI editor.
6. Run the following command to recompile and generate the grub.cfg file.

   grub2-mkconfig -o /boot/grub2/grub.cfg

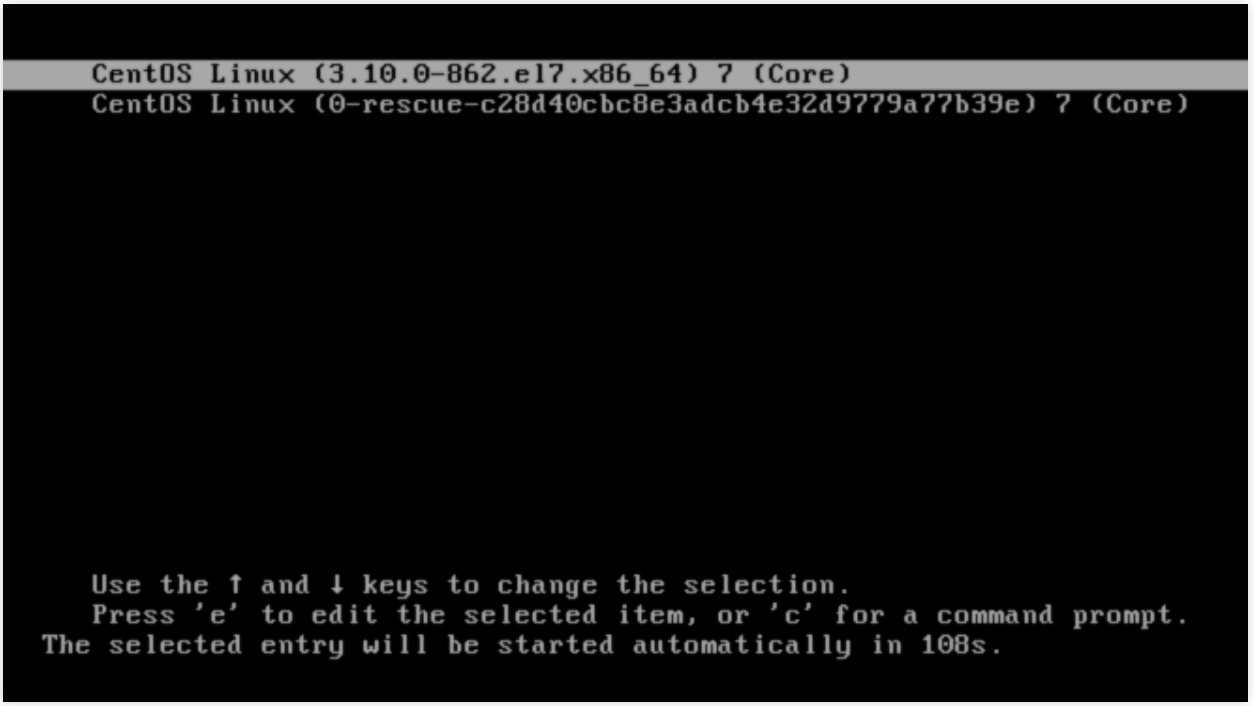
The returned result is as shown in the following figure:

```
* Socket connection established *
Last login: Mon Feb 25 16:37:51 2019
[root@VM_204_43_centos ~]# grub2-mkconfig -o /boot/grub2/grub.cfg
Generating grub configuration file ...
Found linux image: /boot/vmlinuz-3.10.0-862.el7.x86_64
Found initrd image: /boot/initramfs-3.10.0-862.el7.x86_64.img
Found linux image: /boot/vmlinuz-0-rescue-c28d40cbc8e3adcb4e32d9779a77b39e
Found initrd image: /boot/initramfs-0-rescue-c28d40cbc8e3adcb4e32d9779a77b39e.img
done
[root@VM_204_43_centos ~]#
```

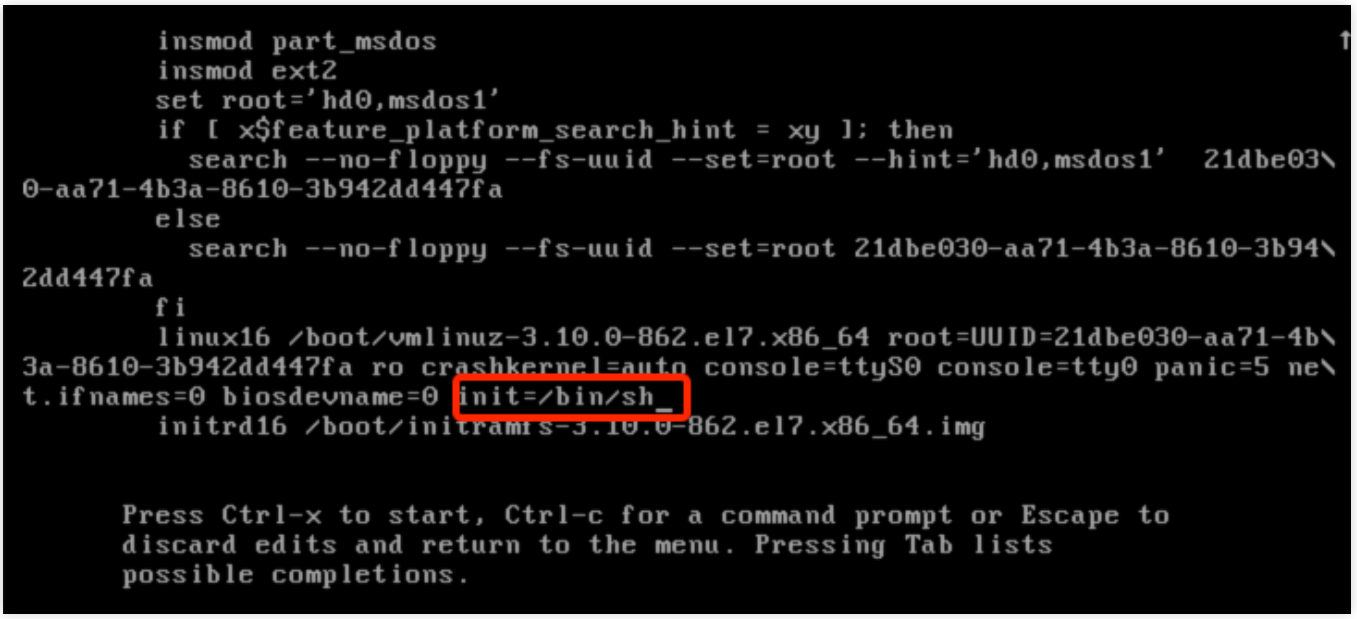
7. Run the following command to restart the CVM.

   reboot

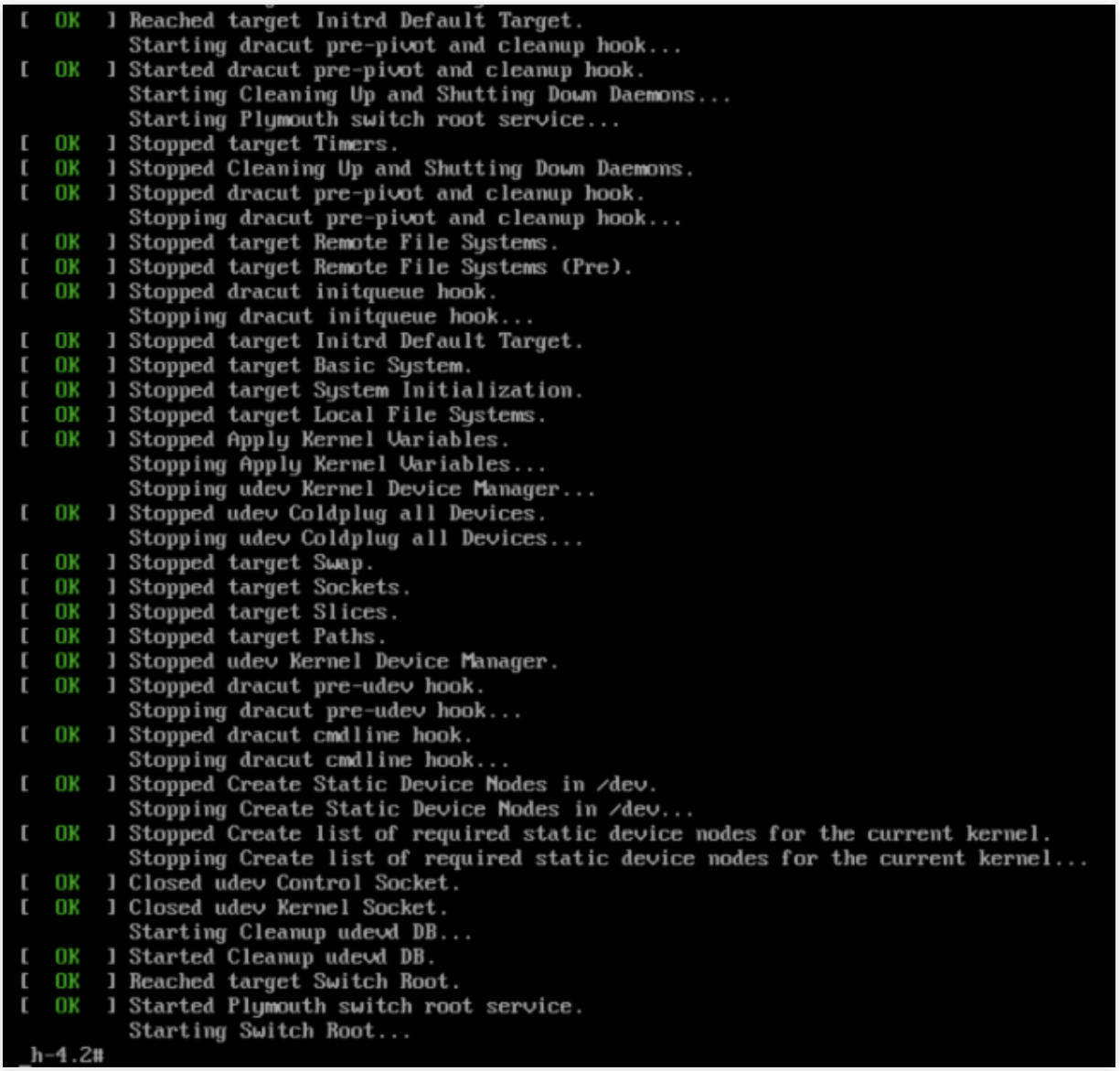
8. Wait for about 1 minute and log in to the CVM instance through the VNC. The login interface is shown below:



9. Press e to enter the kernel editing interface and add init=/bin/sh to the red box. As shown below:



10. Press Ctrl+X to boot into the single-user mode. As shown below:



11. Run the following command to exit the single-user mode.

exec /sbin/init

Ubuntu

> Note:
> The following steps are based on Ubuntu 16.04 as an example. The detailed steps may vary slightly depending on the version of the operating system.

1. Log in to the CVM.

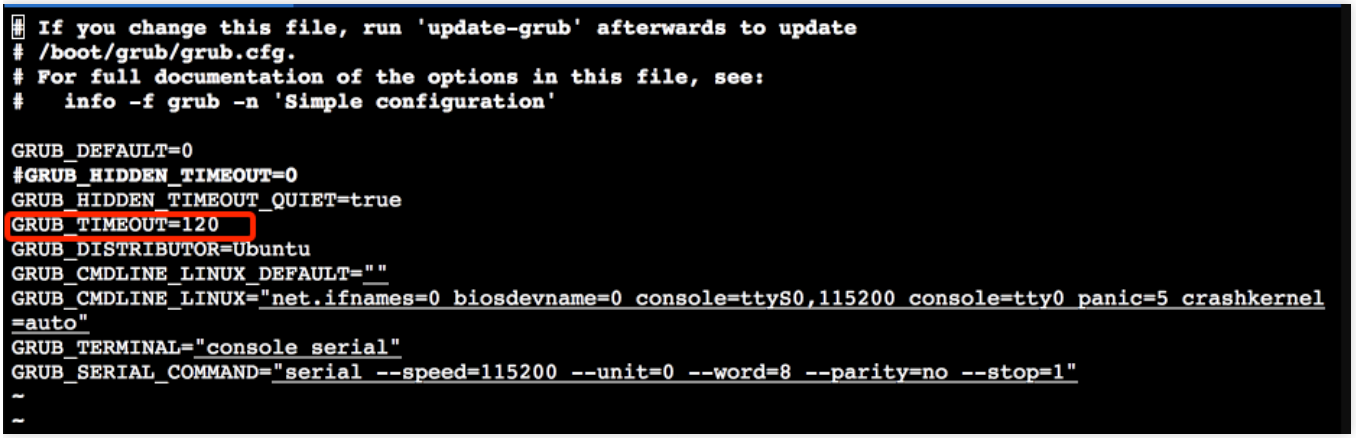
2. Run the following command to open the /etc/default/grub file.

sudo vi /etc/default/grub

3. Press i to enter the edit mode.

4. Find the waiting time parameter "GRUB-TIMEOUT" of the default startup item, and modify its value to the required time range according to actual needs. As shown below:
   The default value of "GRUB_TIMEOUT" is 5 seconds. In order to avoid not being able to see the boot interface due to a short waiting time, it is recommended to adjust it to 60 seconds or more. > Note: - This affects the system's start time. After completing the configuration, it should be reverted to the default value.

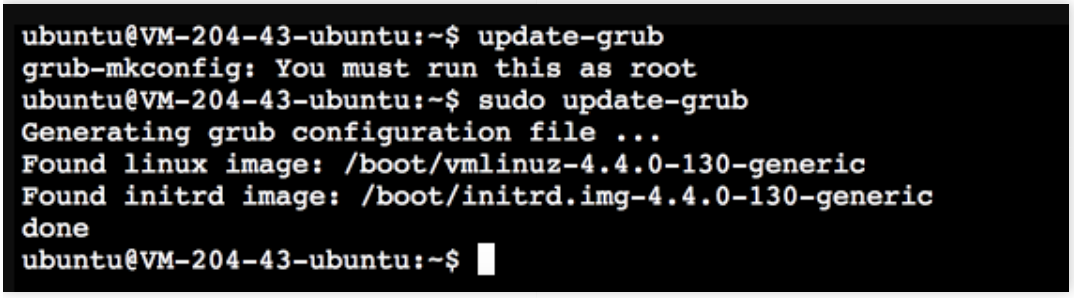
- The default account in Ubuntu is not root. Please remember to use the sudo command.



5. Press Esc to exit the edit mode, enter :wq, and press Enter.
Save the settings and exit the VI editor.
6. Run the following command to recompile and generate the grub.cfg file.

sudo update-grub

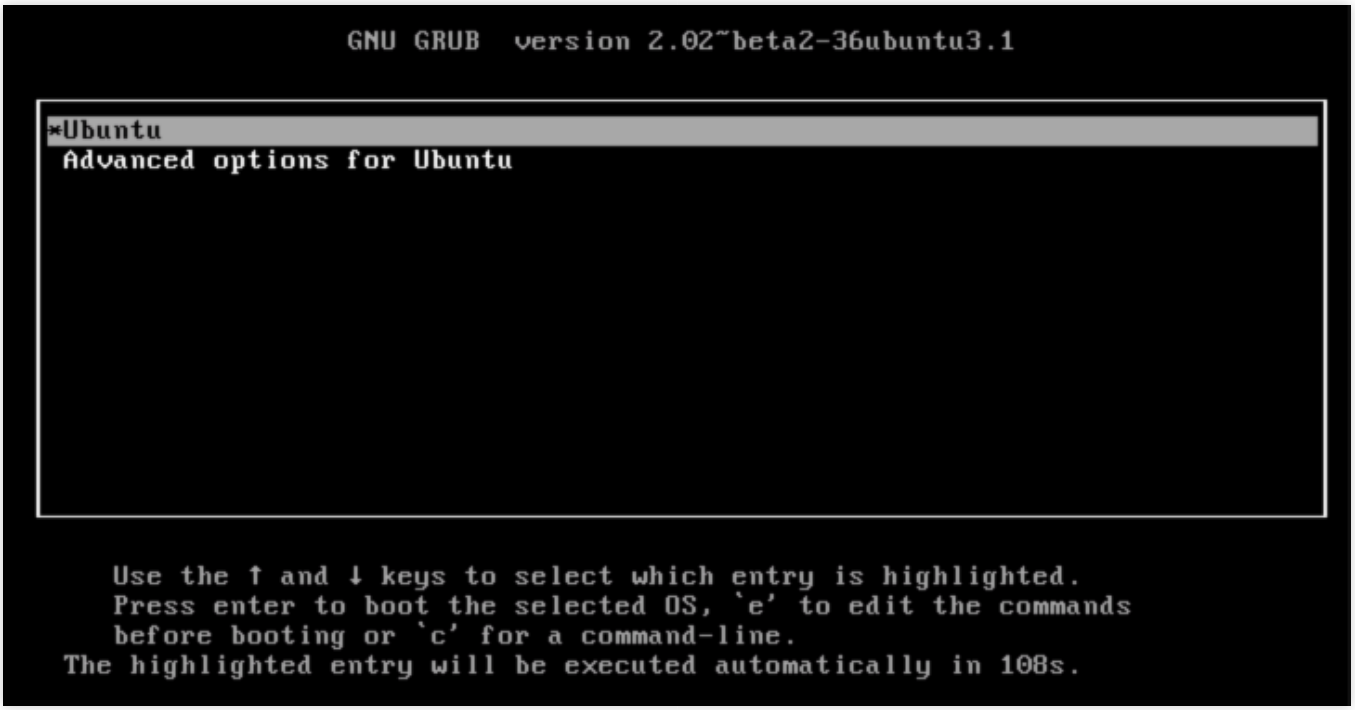
The returned result is as shown in the following figure:



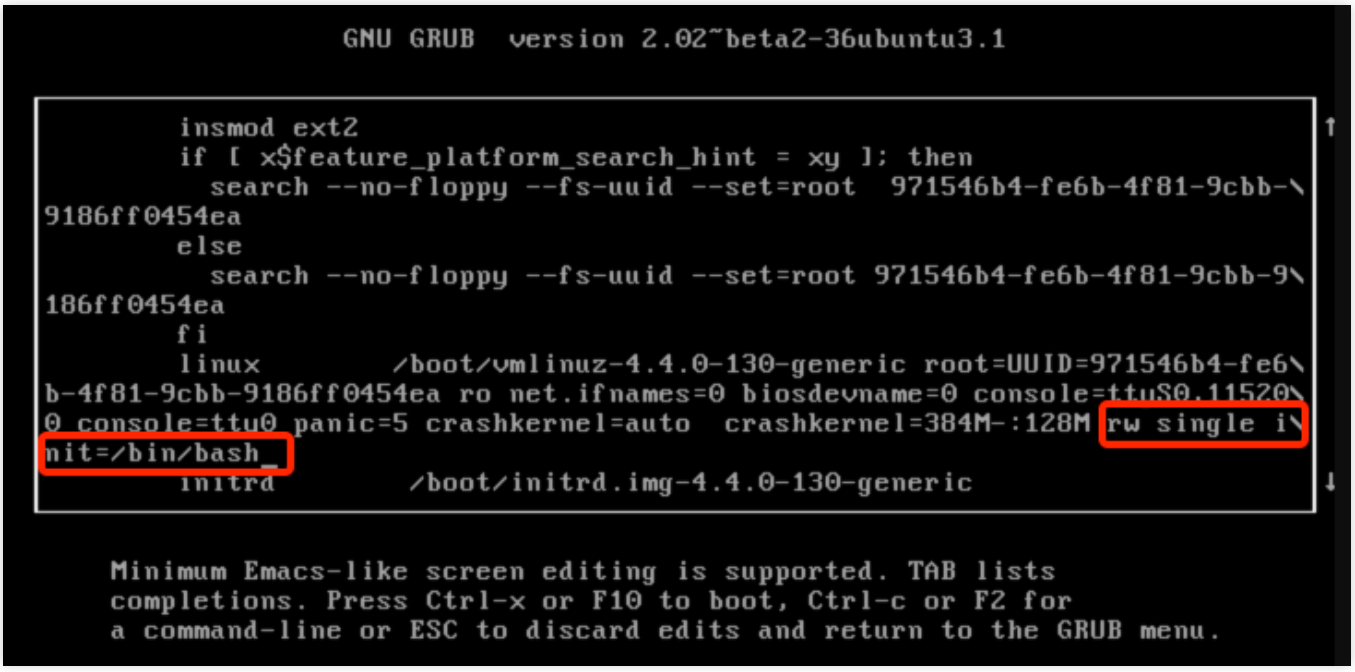
7. Run the following command to restart the CVM.

sudo reboot

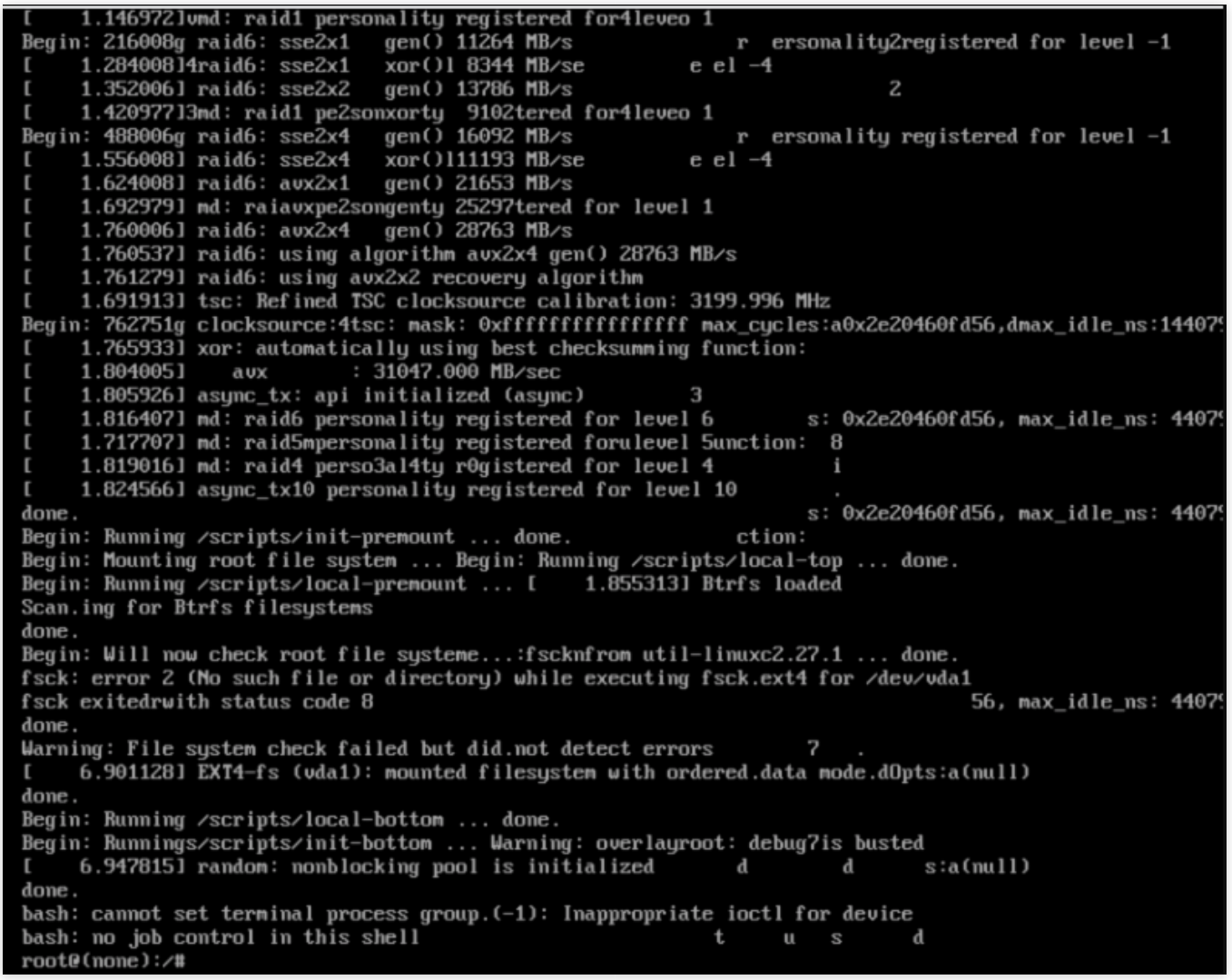
8. Wait for about 1 minute and log in to the CVM instance through the VNC. The login interface is shown below:



9. Press e to enter the kernel editing interface and add rw single init=/bin/bash to the red box. As shown below:



10. Press Ctrl+X to boot into the single-user mode. As shown below:


[1.146972]vmd: raid1 personality registered for4leveo 1
Begin: 216008g raid6: sse2x1 gen() 11264 MB/s r ersonality2registered for level -1
[1.284008]4raid6: sse2x1 xor()1 8344 MB/se e el -4
[1.352006] raid6: sse2x2 gen() 13786 MB/s 2
[1.420977]3md: raid1 pe2sonxorty 9102tered for4leveo 1
Begin: 488006g raid6: sse2x4 gen() 16092 MB/s r ersonality registered for level -1
[1.556008] raid6: sse2x4 xor()111193 MB/se e el -4
[1.624008] raid6: avx2x1 gen() 21653 MB/s
[1.692979] md: raiavxpe2songenty 25297tered for level 1
[1.760006] raid6: avx2x4 gen() 28763 MB/s
[1.760537] raid6: using algorithm avx2x4 gen() 28763 MB/s
[1.761279] raid6: using avx2x2 recovery algorithm
[1.691913] tsc: Refined TSC clocksource calibration: 3199.996 MHz
Begin: 762751g clocksource:4tsc: mask: 0xffffffffffffffff max_cycles:a0x2e20460fd56,dmax_idle_ns:14407
[1.765933] xor: automatically using best checksumming function:
[1.804005] avx : 31047.000 MB/sec
[1.805926] async_tx: api initialized (async) 3
[1.816407] md: raid6 personality registered for level 6 s: 0x2e20460fd56, max_idle_ns: 4407
[1.717707] md: raid5mpersonality registered forulevel 5unction: 8
[1.819016] md: raid4 perso3al4ty r0gistered for level 4 i
[1.824566] async_tx10 personality registered for level 10 .
done. s: 0x2e20460fd56, max_idle_ns: 4407
Begin: Running /scripts/init-premount ... done. ction:
Begin: Mounting root file system ... Begin: Running /scripts/local-top ... done.
Begin: Running /scripts/local-premount ... [1.855313] Btrfs loaded
Scan.ing for Btrfs filesystems
done.
Begin: Will now check root file systeme...:fscknfrom util-linuxc2.27.1 ... done.
fsck: error 2 (No such file or directory) while executing fsck.ext4 for /dev/vda1
fsck exitedrwith status code 8 56, max_idle_ns: 4407
done.
Warning: File system check failed but did.not detect errors 7 .
[6.901128] EXT4-fs (vda1): mounted filesystem with ordered.data mode.dOpts:a(null)
done.
Begin: Running /scripts/local-bottom ... done.
Begin: Runnings/scripts/init-bottom ... Warning: overlayroot: debug?is busted
[6.947815] random: nonblocking pool is initialized d d s:a(null)
done.
bash: cannot set terminal process group.(-1): Inappropriate ioctl for device
bash: no job control in this shell t u s d
root@(none):/#

Setting to Allow Multiple Users to Remotely Log in to Windows CVM

Overview

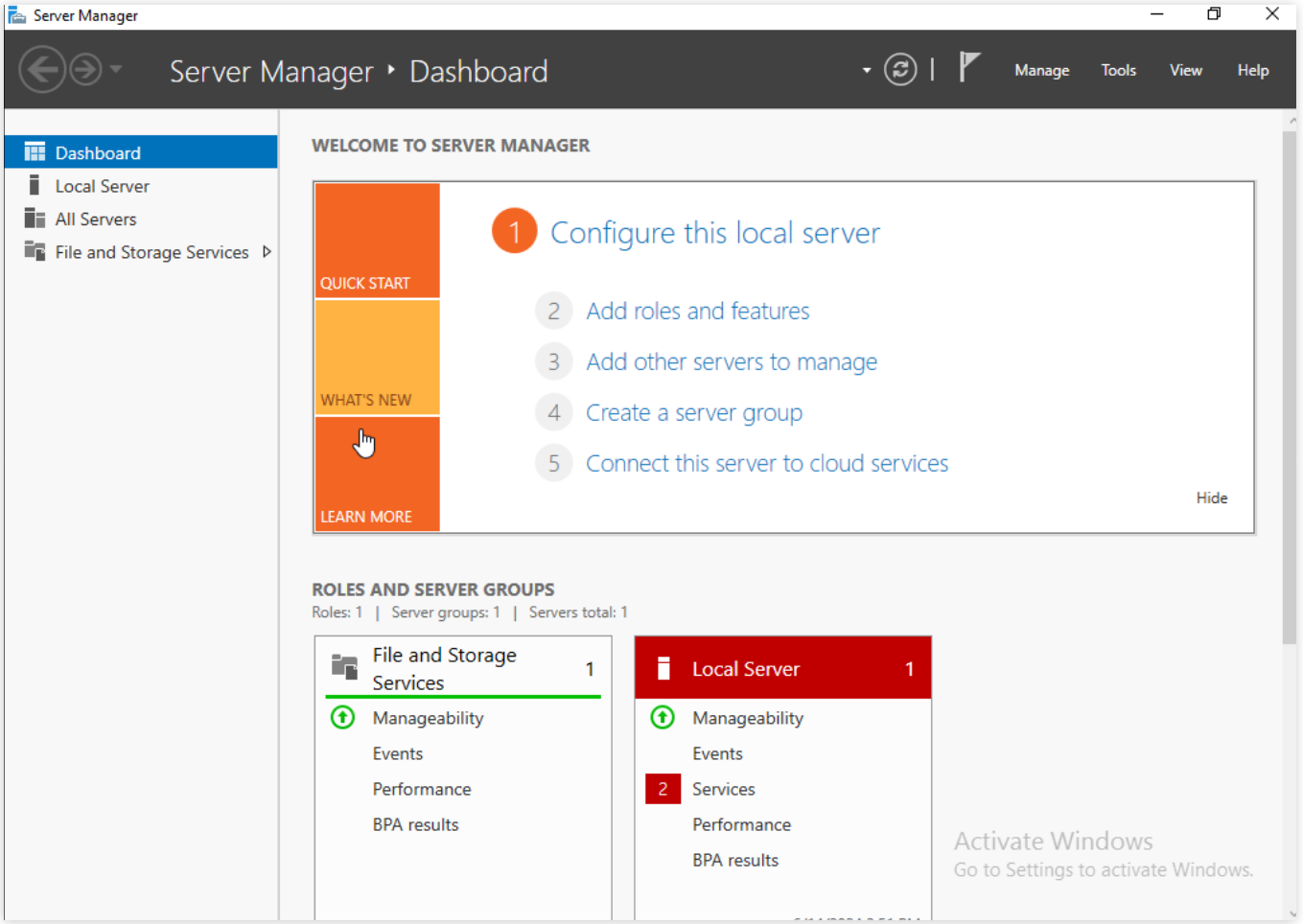
This document takes the operating system CVM of Windows Server 2012 R2 as an example to guide you to make configurations to allow multiple users to remotely log in to Windows CVM.

Directions

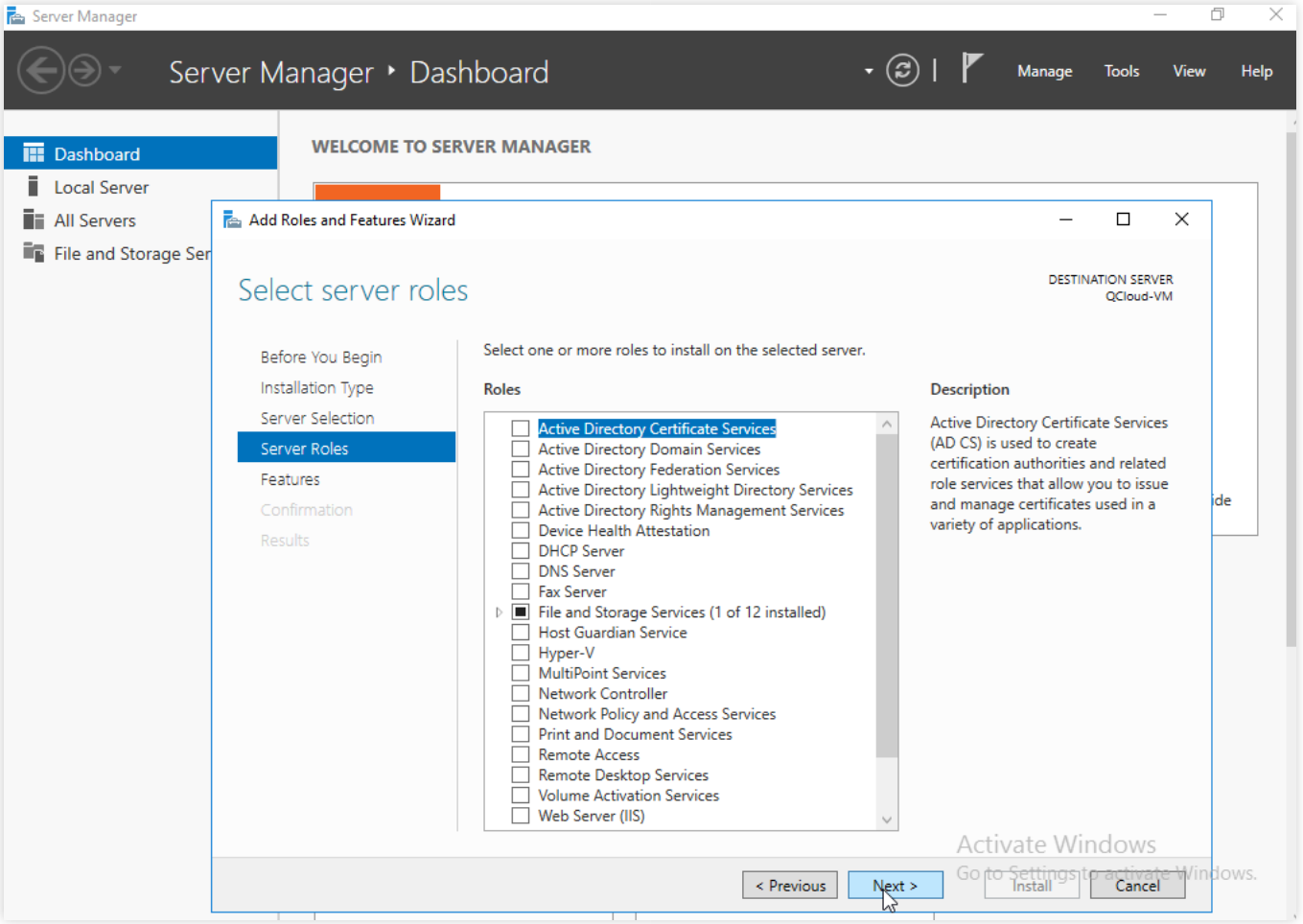
Adding Remote Desktop Services

1. Log in to the Windows CVM.

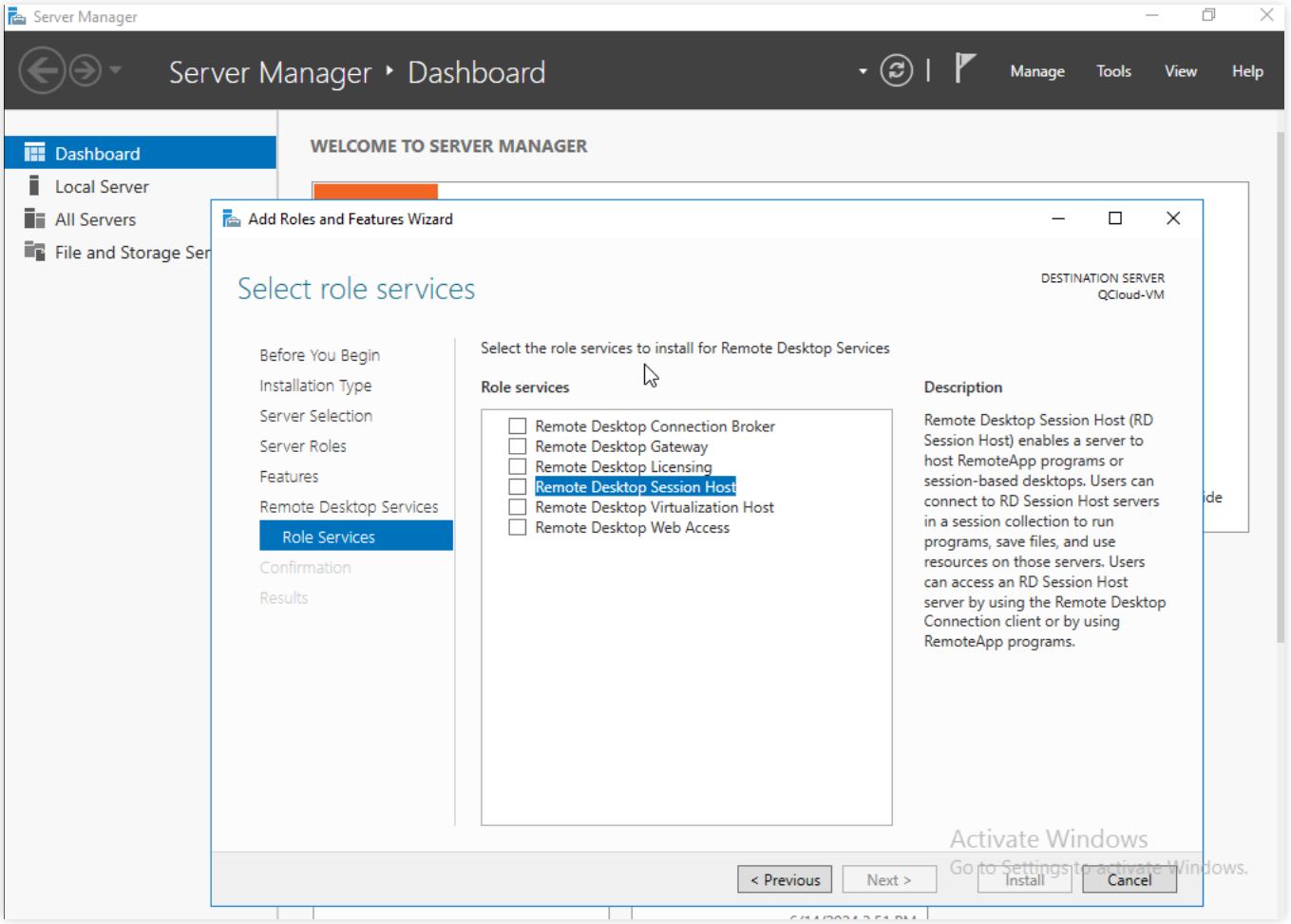
2. On the operating system interface, click to open Server Manager. As shown below:



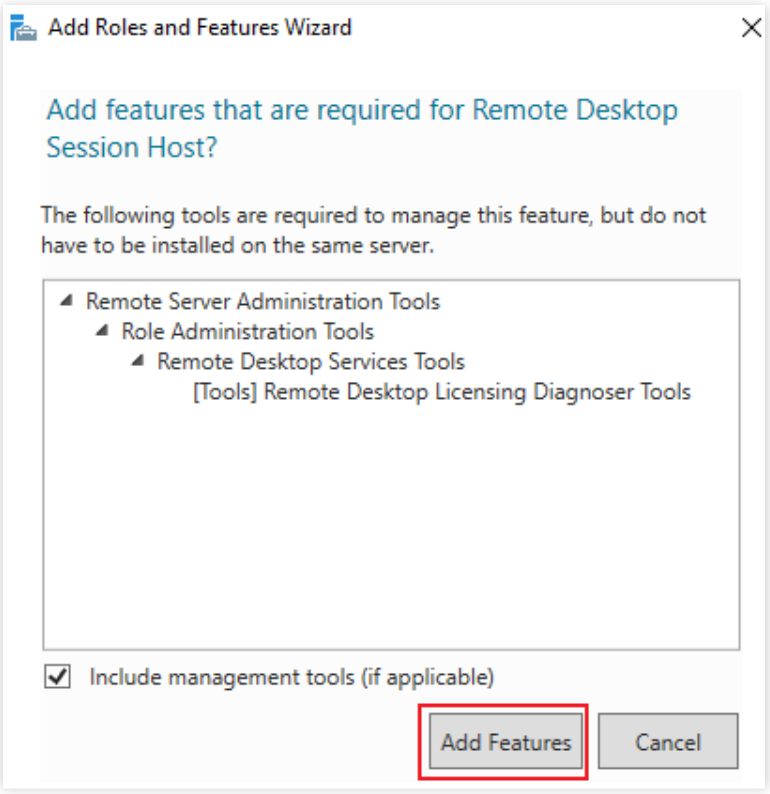
3. Click Add Roles and Features to pop up the Add Roles and Features Wizard window.
4. In the Wizard to Add Roles and Features window, keep the default parameters and consecutively click Next three times.
5. On the Select Server Roles interface, select Remote Desktop Services and click Next. As shown below:



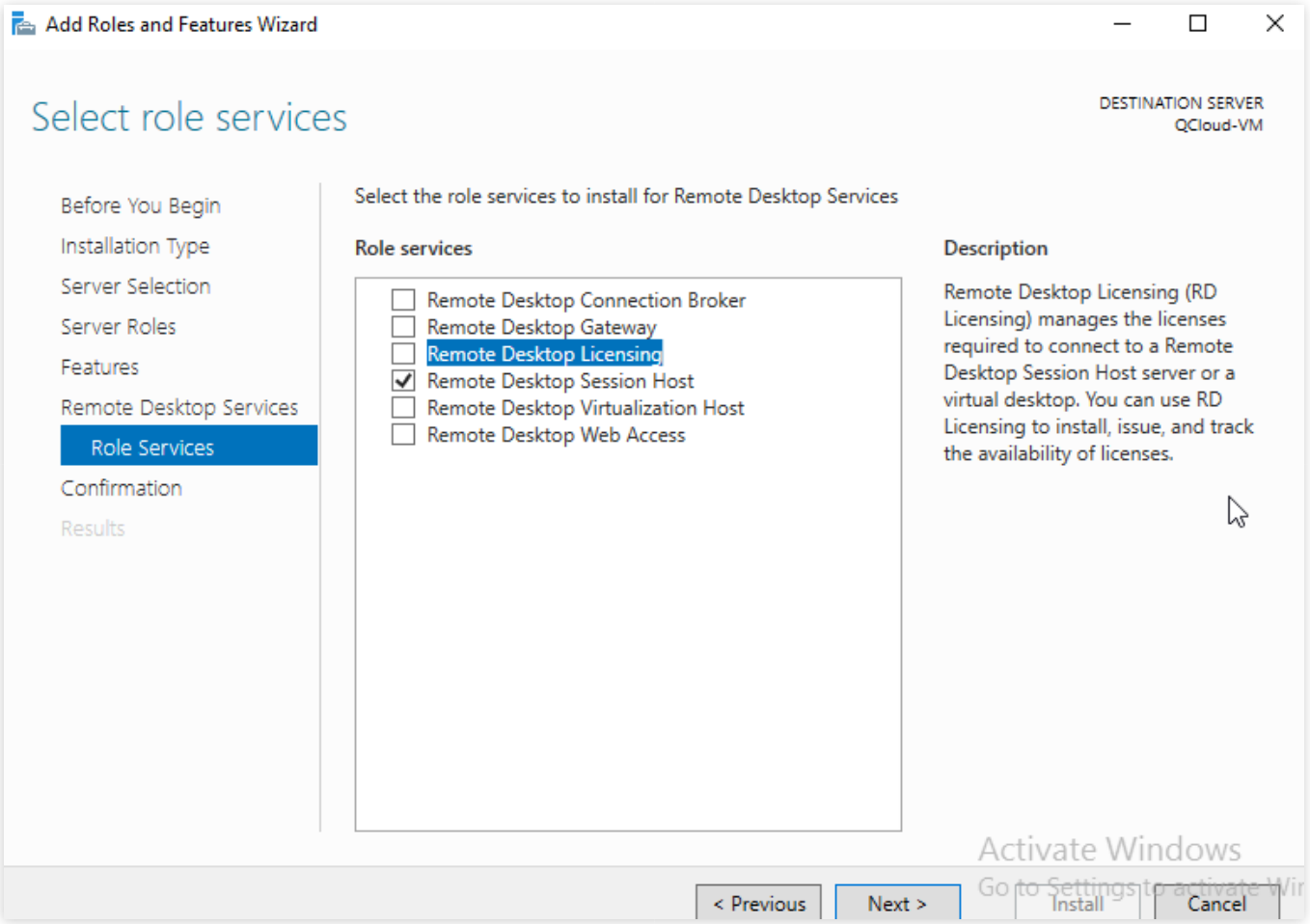
6. Keep the default parameters and consecutively click Next twice.
7. On the Select Role Services interface, select Remote Desktop Session Host. As shown below:
   The Add Features Required for Remote Desktop Session Host dialog box pops up.



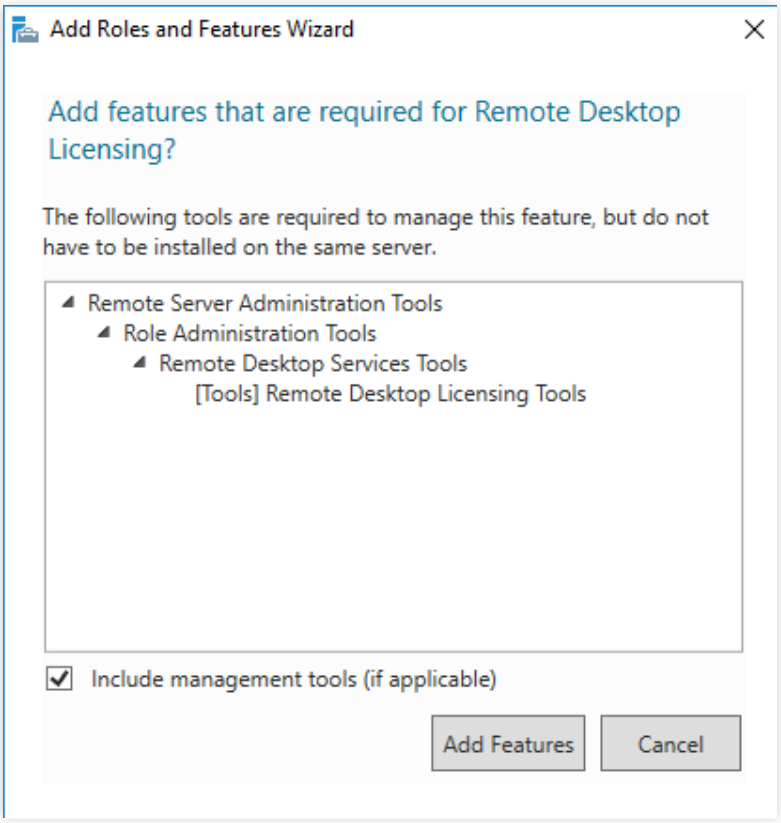
8. In the Add Features Required for Remote Desktop Session Host dialog box, click Add Features. As shown below:



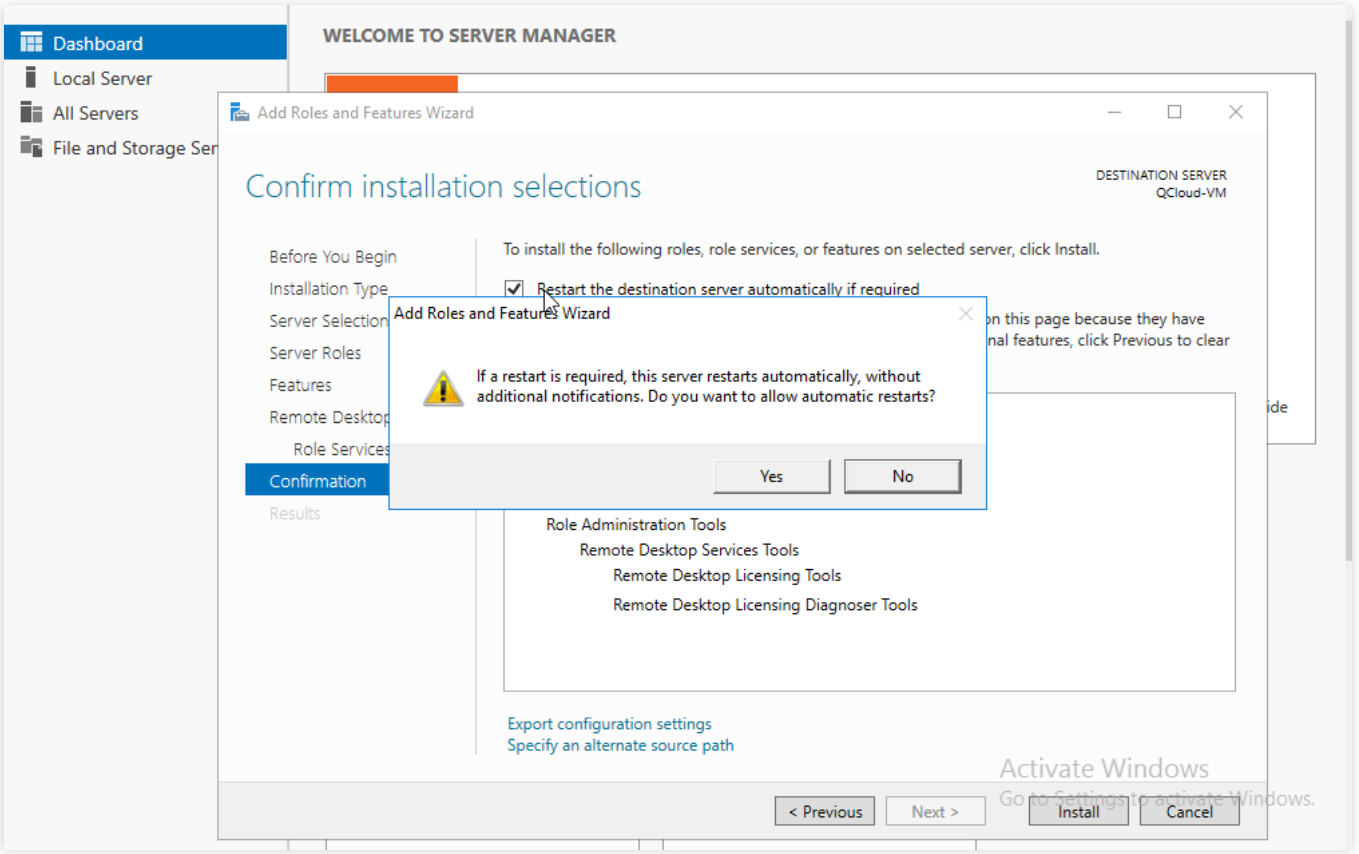
9. On the Select Role Services interface, select Remote Desktop Licensing. As shown below:
   The Add Features Required for Remote Desktop Session Host dialog box pops up.



10. In the Add Features Required for Remote Desktop Licensing dialog box, click Add Features.



11. Click next.
12. Check Automatically Restart the Target Server if Necessary and click Yes in the pop-up dialog box. As shown below:



13. Click Install and wait for the installation of Remote Desktop Services to complete.

Configuring a Multi-user Remote Login Instance

1. Use VNC to log in to Windows CVM.

2. On the operating system interface, click to open a Windows PowerShell window.
3. In the Windows PowerShell window, enter gpedit.msc and then press Enter to open the Local Group Policy Editor.
4. In the left navigation tree, select Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Connections, and double-click to open Limit the number of connections.
5. In the popped-up Limit the number of connections window, select Enabled, and fill in the maximum number of concurrent remote users in Maximum allowed RD connections.
6. Click OK.
7. In the left navigation tree, select Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Connections, and double-click to open Restrict Remote Desktop Services users to a single Remote Desktop Services session.
8. In the popped-up Restrict Remote Desktop Services users to a single Remote Desktop Services session]window, select Disabled, click OK.

9. Disable the Local Group Policy Editor.
10. Restart instance.

Allowing CVM Without a Public Network to Access the Public Netwo

Overview

When purchasing a CVM, if you select a bandwidth limit of 0Mbps, the CVM will not be able to access the public network. Taking CentOS7.5 as an example, this document describes how to connect a CVM without a public IP address to a CVM with a public IP address through PPTP VPN so that it can access the public network.

Prerequisites

- Two CVMs have been created in the same Virtual Private Cloud (one CVM without a public IP address and one CVM with a public IP address).
- The private IP address of the CVM with a public IP address has been obtained.

Directions

Configuring PPTP on the CVM with Public IP Address

1. Log in to the CVM with a public IP address.

2. Run the following command to install PPTP.

   ```
   yum install -y pptpd
   ```

3. Execute the following command to open the pptpd.conf configuration file.

   ```
   vim /etc/pptpd.conf
   ```

4. Press i to switch to the edit mode and add the following content at the end of the file.

```
localip 192.168.0.1
remoteip 192.168.0.234-238,192.168.0.245
```

5. Press “Esc”, enter “:wq” to save the file and return.

6. Execute the following command to open the /etc/ppp/chap-secrets configuration file.

   ```
   vim /etc/ppp/chap-secrets
   ```

7. Press i to switch to the edit mode and add the username and password for connecting to PPTP at the end of the file in the following format.

   ```
   Username    pptpd    Password    *
   ```

   For example, if the username for connecting to PPTP is root and the login password is 123456, the information to be added is as follows:

   ```
   root    pptpd    123456    *
   ```

8. Press Esc, enter “:wq”, save the file and return.

9. Run the following command to start the PPTP service.

   ```
   systemctl start pptpd
   ```

10. Execute the following commands in sequence to enable the forwarding capability.

```
echo 1 > /proc/sys/net/ipv4/ip_forward
iptables -t nat -A POSTROUTING -o eth0 -s 192.168.0.0/24 -j MASQUERADE
```

Configuring PPTP on the CVM Without Public IP Address

1. Log in to the CVM without a public IP address.

2. Run the following command to install the PPTP client.

   yum install -y pptp pptp-setup

3. Run the following command to create a configuration file.

   pptpsetup --create (the name of the configuration file) --server (the private IP address of the CVM with a public IP address) --username (the username for connecting to PPTP) --password (the password for connecting to PPTP) --encrypt

   For example, to create a test configuration file, if the obtained private IP address of the CVM with a public IP address is 10.100.100.1, run the following command:

   pptpsetup --create test --server 10.100.100.1 --username root --password 123456 --encrypt

4. Run the following command to connect to PPTP.

   pppd call test (name of the configuration file created in Step 3)

5. Execute the following commands in sequence to set the route.

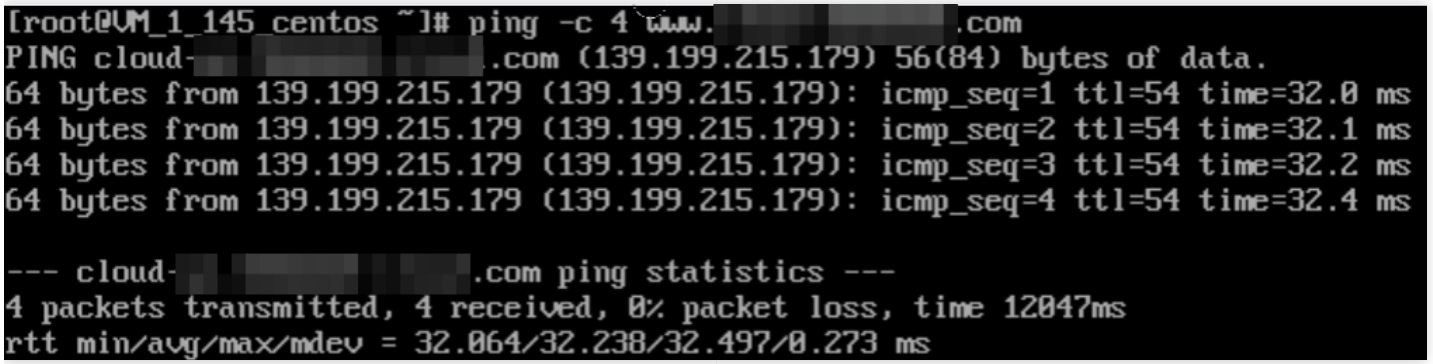
   route add -net 10.0.0.0/8 dev eth0
   route add -net 172.16.0.0/12 dev eth0
   route add -net 192.168.0.0/16 dev eth0
   route add -net 169.254.0.0/16 dev eth0
   route add -net 9.0.0.0/8 dev eth0
   route add -net 100.64.0.0/10 dev eth0
   route add -net 0.0.0.0 dev ppp0

Checking Whether the Configuration Is Successful

On the CVM without a public IP address, execute the following command to PING any public IP address, and check whether the PING is successful.

ping -c 4 public IP address

If the following result is returned, the configuration is successful:

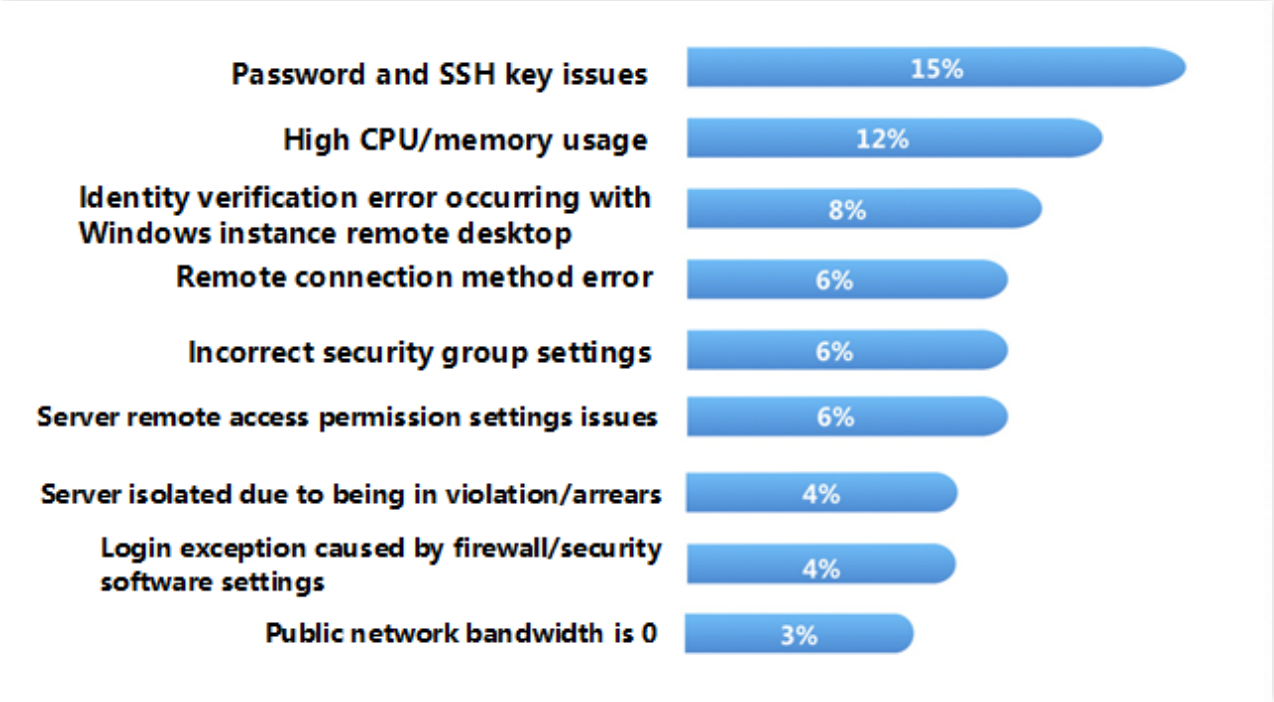

[root@VM_1_145_centos ~]# ping -c 4 www.[redacted].com
PING cloud-[redacted].com (139.199.215.179) 56(84) bytes of data.
64 bytes from 139.199.215.179 (139.199.215.179): icmp_seq=1 ttl=54 time=32.0 ms
64 bytes from 139.199.215.179 (139.199.215.179): icmp_seq=2 ttl=54 time=32.1 ms
64 bytes from 139.199.215.179 (139.199.215.179): icmp_seq=3 ttl=54 time=32.2 ms
64 bytes from 139.199.215.179 (139.199.215.179): icmp_seq=4 ttl=54 time=32.4 ms
--- cloud-[redacted].com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 12047ms
rtt min/avg/max/mdev = 32.064/32.238/32.497/0.273 ms

Troubleshooting
Instance-related Failures
Solution to the Problem of Being Unable to Log in to the CVM

This document mainly introduces the solution to the problem that you cannot log in to the CVM instance after purchasing it, helping you locate and solve the problem.

Main Cause of Fault

The following figure shows the main reasons for being unable to connect to a CVM instance and their occurrence probability. If you are unable to connect to the instance, troubleshoot based on the following possible reasons.



Troubleshooting Steps

Confirming the Instance type

First, you need to know whether the instance type you purchased is a Windows system instance or a Linux

system instance. Secondly, different instance types may have different reasons for not being able to log in to CVM. You can refer to the following documents to locate and solve the problem based on the instance type you purchased:

- Unable to log in to Windows instance
- Unable to log in to Linux instance

Port Problem

Fault Symptoms

The remote connection to the port failed.

Solution

This may be caused by the remote access port being a non-default port or the port settings being inconsistent.
See Port Problem Resulting in Failure to Remote Connect for details.

High CPU/Memory Usage Issue

Fault Symptoms

When you use the CVM, problems such as inability to log in, slowdown of service speed, and sudden disconnection of instances occur.

Solution

There may be a problem of excessive CPU or memory usage. Check the resource usage.

- For Windows CVMs, see Unable to Log in Due to High CPU and Memory Usage in Windows System.
- For Linux CVMs, see Unable to Log in Due to High CPU and Memory Usage in Linux System.

Public Network Isolation Issue

Fault Symptoms

The CVM was partially isolated due to a violation or risk event.

Solution

For details, see Public network is Isolated and Cannot be Connected Remotely.

High Usage of Public Network Bandwidth Issue

Fault Symptoms

The bandwidth is full or high, resulting in a login failure.

Solution

For details, see Unable to Log in Due to High Public Network Bandwidth Usage.

Unable to Use Password After Associating the Key

Fault Symptoms

Once the CVM is associated with a key, logging in via password will be disabled. Please ensure that the firewall settings and IP configuration of the network interface are accurate.

Solution

After the CVM is associated with a key, the CVM SSH service will disable username and password login by default. Please use the key to log in to the server.

Unable to Log in with Password in Xshell

Fault Symptoms

When you log in using Xshell, you cannot use a password to log in to the CVM.

Solution

You have selected the key login method when installing the system. For how to use the key, see SSH key operation. If you need to log in with a password, you can select password login when reinstalling the system, or log in to the computer and modify the sshd configuration file.

Other Common Causes of Login Issues

If the cause of the problem cannot be located through the above directions, or the following types of error messages are directly returned when you log in to the CVM, you can refer to the following solutions.

Windows Instances

- Windows Instance: No permission to Log in via Remote Desktop Services
- Windows Instance: Mac Remote Log-in Exception
- Windows Instance: An Authentication Error Occurred
- Windows Instance: Network Level Authentication Required
- Windows Instance: Remote Desktop Cannot Connect to the Remote Computer

Linux Instances

Linux Instance: High CPU and Memory Usage Causes Login Failure

Subsequent Operations

If the above steps still cannot solve the problem of being unable to log in remotely, you can save the relevant logs and self-test results and feedback them to the maintenance engineer.

Windows Instance-related
Unable to Log in to a Windows Instance

Problem Description

This document introduces how to troubleshoot issues when you cannot connect to a Windows instance. It also explains the main reasons for login failures and guides you through troubleshooting, locating, and solving the problem.

Possible Reasons

The main reasons you may be unable to log in to a Windows instance include:

- Unable to log in due to password problems
- High bandwidth usage
- High server load
- Remote port configuration error
- Improper security group rules
- Firewall or security software causing login failures
- Authentication error with Remote Desktop connection

Troubleshooting

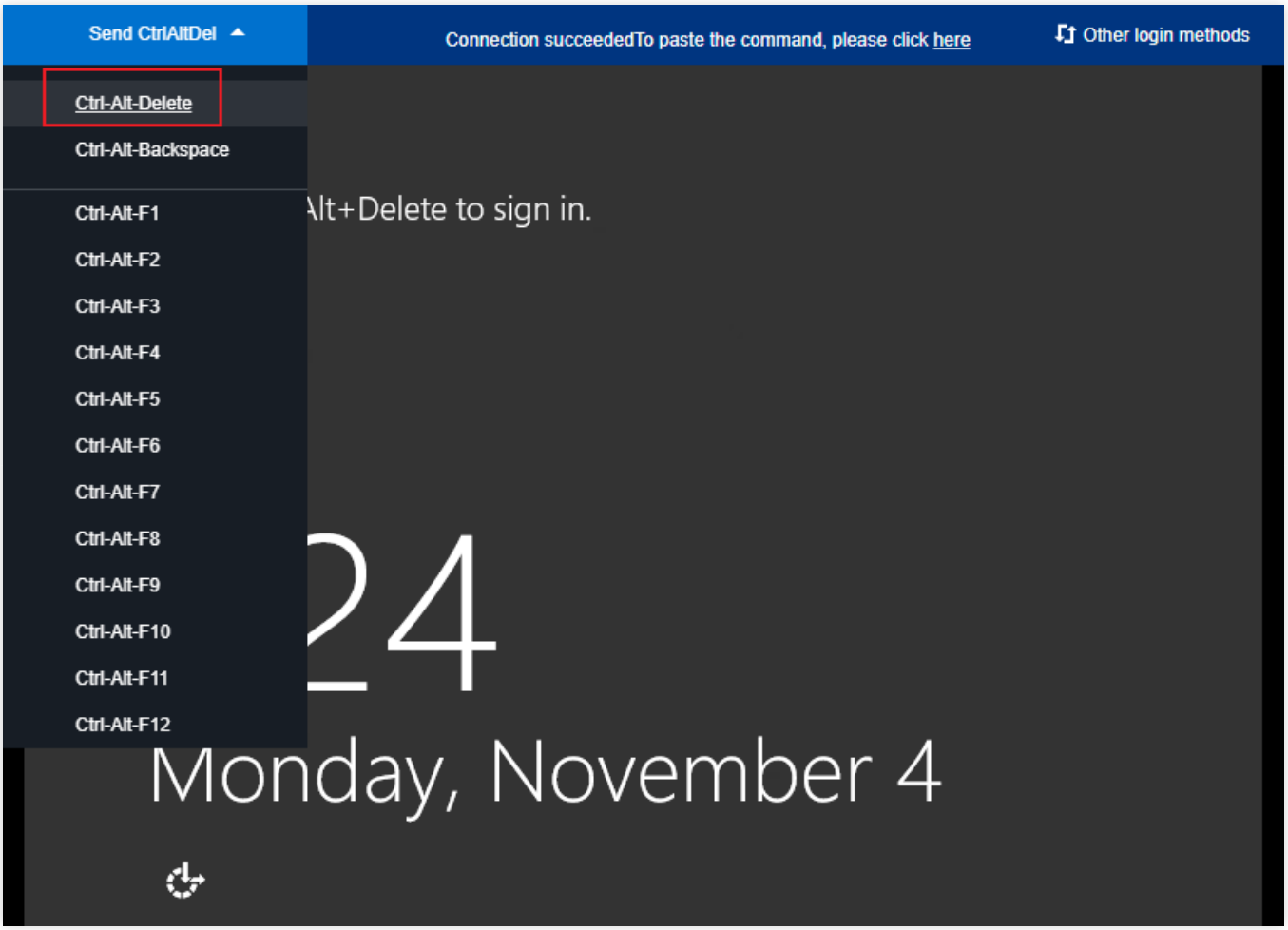
Log-in via VNC

When you cannot log in to a Windows instance through RDP or remote login software, use Converge Cloud VNC to log in and locate the cause of the fault.

1. Log in to the CVM Console.
2. On the instance management page, select the instance you want to log in to and click Log In.
3. In the pop-up *Log in to Windows Instance* window, select Other methods (VNC) and click Log In Now.

> Note:
> If you forget your password during login, you can reset the instance password in the console. For specific operations, refer to Reset Instance Password.

4. In the login window, select Send Remote Command in the upper left corner and press Ctrl-Alt-Delete to enter the system login page.



Unable to log in due to password problem

Fault Phenomenon: Login fails due to incorrect password input, forgotten password, or failed password reset.
Solution: Reset the instance password in the console and restart the instance.
Directions: See Reset the Instance Password.

High bandwidth usage

Fault Phenomenon: Self-diagnosis indicates high bandwidth utilization.
Directions:

1. Log in to the instance via VNC.
2. See High Bandwidth Usage Prevents Log-in to track bandwidth usage and resolve issues.

High server load

Fault Phenomenon: High CPU load prevents remote access or causes slow login.

Possible Causes: Viruses, Trojans, third-party antivirus software, application anomalies, driver issues, or automatic updates can cause high CPU usage.
Directions:

1. Log in via VNC.
2. See Windows Instance: High CPU and Memory Usage Causes Log-in Failure to locate high-load processes in Task Manager.

Remote port configuration error

Fault Phenomenon: Remote connection unavailable, port not default or 3389 not open.
Localization Approach: Use ping to test the public IP and telnet to test port connectivity.
Directions: See Port Problem Leads to Failure of Remote Log-in.

Firewall or security software causing log-in failures

Fault Phenomenon: Login fails due to firewall settings or installed security software.
Positioning Ideas: Log in via VNC, check firewall status, and identify security software (e.g., 360, Safe Dog).

> Note:
> This operation may involve disabling the firewall. Ensure you have permission to perform this operation.

Directions (Example: Windows Server 2016):

1. Log in via VNC.
2. Press Win+R, open Control Panel.
3. Click Windows Firewall.
4. Select Enable or disable Windows Firewall.
5. Turn off both Private and Public Network Settings, click OK.
6. Restart the instance and test remote login.

Authentication error with Remote Desktop connection

Fault Phenomenon: Error messages such as:

- *An authentication error has occurred. The feature supported by the client is not supported by the remote computer.*
- *An authentication error has occurred. The requested feature is not supported.*

Cause: Microsoft's March 2018 security update fixes a CredSSP vulnerability. Both client and server must install the update; otherwise, authentication may fail.

Processing Steps: Install the security update. For details, see Windows instance: Authentication Error.

Other Solutions

If the above steps do not resolve the issue:

1. Save self-diagnosis results.
2. Submit a ticket for technical support feedback.

Windows Instances: An Authentication Error Occurred

Problem Description

When you log in to a Windows instance through a remote desktop connection, the following error message may appear:

- *An authentication error occurred. Invalid flags were provided to the feature.*
- *An authentication error occurred. The requested feature is not supported.*

Issue Analysis

Microsoft released a security update in March 2018 to address a remote code execution vulnerability in CredSSP by correcting the protocol and the way requests are validated during authentication. Both the client and the server must install this update; otherwise, the issue can occur.

The following three scenarios cause remote connection failure:

- Scenario 1: Client not patched, server updated, policy set to *Force updated clients*.
- Scenario 2: Server not patched, client updated, policy set to *Force updated clients*.
- Scenario 3: Server not patched, client updated, policy set to *Mitigate*.

> Note:
> If you only want to upgrade the client locally, please refer to Solution 1: Install security updates (recommended).

Logging in to the CVM via VNC

1. Log in to the CVM console.
2. On the instance management page, find the target CVM instance and click Log In.
3. In the pop-up *Log in to Windows Instance* window, select Other methods (VNC) and click Log in now.
4. In the login window that pops up, select Send Remote Command in the upper left corner and click Ctrl-Alt-Delete to enter the system log-in interface.

Solution 1: Install Security Updates (Recommended)

Install security updates to update unpatched clients or servers.

- Windows Server 2012: Control Panel > System and Security > Windows Update
- Windows Server 2008: Start > Control Panel > System and Security > Windows Update
- Windows 10: > Settings > Update & Security
- Windows 7: > Control Panel > System and Security > Windows Update

Steps:

1. Click and select Settings.
2. In the Settings window, select Update & Security.
3. In Windows Update, click Check for updates.
4. Follow the interface instructions and click Start Installation.
5. After installation, restart the instance.

Solution 2: Modifying the Policy

On machines with the security update installed, set the *Encryption Oracle Remediation* policy to Vulnerable.

> Note:
> Windows 10 Home does not have Group Policy Editor; use Solution 3 to modify the registry.

Steps:

1. Press Win+R, enter gpedit.msc, and press Enter to open the Local Group Policy Editor.
2. Navigate:
   Computer Configuration > Administrative Templates > System > Credentials Delegation
3. Double-click Encryption Oracle Remediation, select Enabled, and set Protection Level to Vulnerable.
4. Click OK and restart the instance.

Solution 3: Modifying the Registry

1. Press Win+R, enter regedit, and press Enter to open the Registry Editor.
2. Navigate or create the path:
   Computer > HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Windows > CurrentVersion > Policies > System > CredSSP > Parameters
3. Right-click Parameters, select New > DWORD (32-bit) Value, and name it AllowEncryptionOracle .
4. Double-click AllowEncryptionOracle , set Value data to 2 , and click OK.
5. Restart the instance.

Windows Instance: No Remote Desktop Services Log-in Permission

Problem Description

When you use Windows Remote Desktop to connect to a Windows instance, the following prompt appears: To log in remotely, you need permission to log in through Remote Desktop Services. By default, members of the Remote Desktop Users group have this permission. If the group you belong to does not have this permission, or if the permission has been removed from the Remote Desktop Users group, you need to be granted this permission manually.

Solution

1. Log in to the CVM console.
2. On the CVM page, select the CVM instance with the connection exception and click Log In.
3. In the Log in to Windows Cloud Server window that pops up, select Log in via Browser VNC and click Log In Now.
4. In the log-in window that pops up, select Send Remote Command in the upper left corner and click Ctrl-Alt-Delete to enter the system log-in interface.
5. In the operating system interface, select Start > Run and enter gpedit.msc.
6. Press Enter to open the Local Group Policy Editor.
7. In the left sidebar, select Computer Configuration > Windows Settings > Security Settings > Local Policies > User Rights Assignment.
8. In the right policy list, double-click to open the properties of the Deny Log-in Through the Remote Desktop Services policy.
9. In the Deny Log-in Through Remote Desktop Services Properties window, check whether the account that needs to log in is in the list of users denied log in through Remote Desktop Services.
    - If yes, remove the account that needs to log in from the list.
    - No, please report to the maintenance engineer.

Windows Instance: Network Level Authentication Required

This document describes how to handle the alarm message *Network Level Authentication Required* when you connect to a Windows instance remotely.

Failure Symptoms

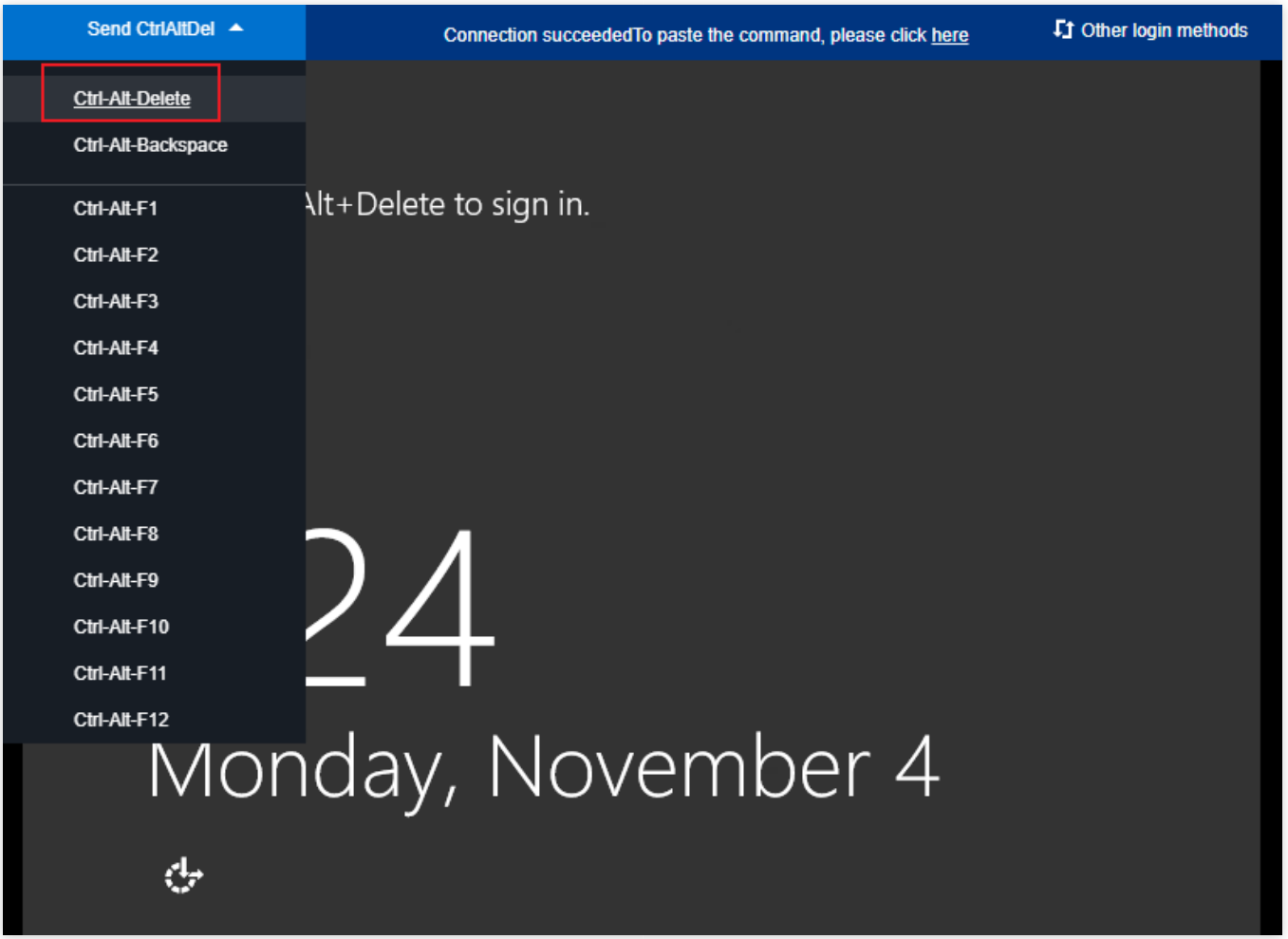
When you use the built-in remote desktop connection of the Windows system, sometimes there is a problem of being unable to connect to the remote computer, and a prompt *Network Level Authentication Required* appears.

Troubleshooting

> Note:
> The following operation uses Windows Server 2016 as an example.

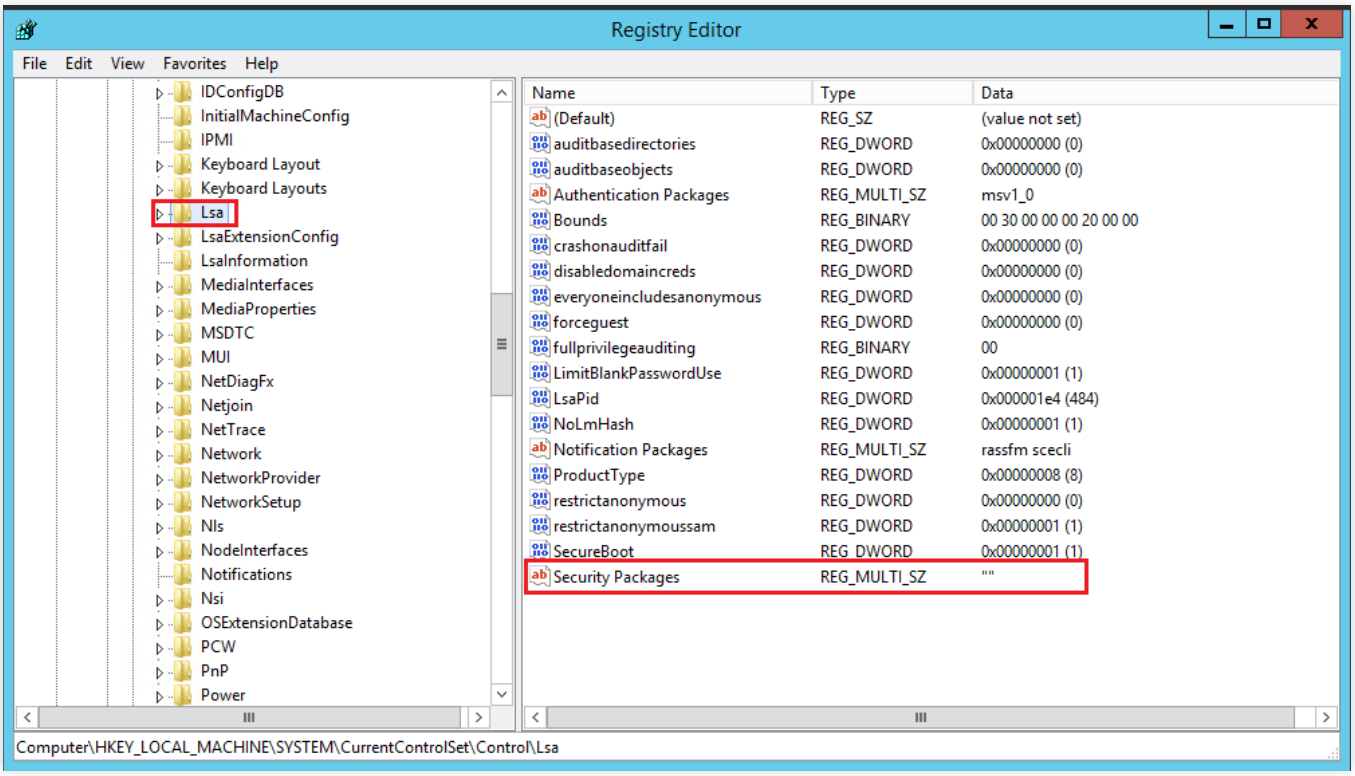
Logging in to the CVM via VNC

1. Log in to the CVM console.
2. On the instance management page, find the target CVM instance and click Log In.
3. In the pop-up *Log in to Windows Instance* window, select Other methods (VNC) and click Log in now to log in to the CVM.
4. In the log-in window that pops up, select Send Remote Command in the upper left corner and click Ctrl-Alt-Delete to enter the system log-in interface.

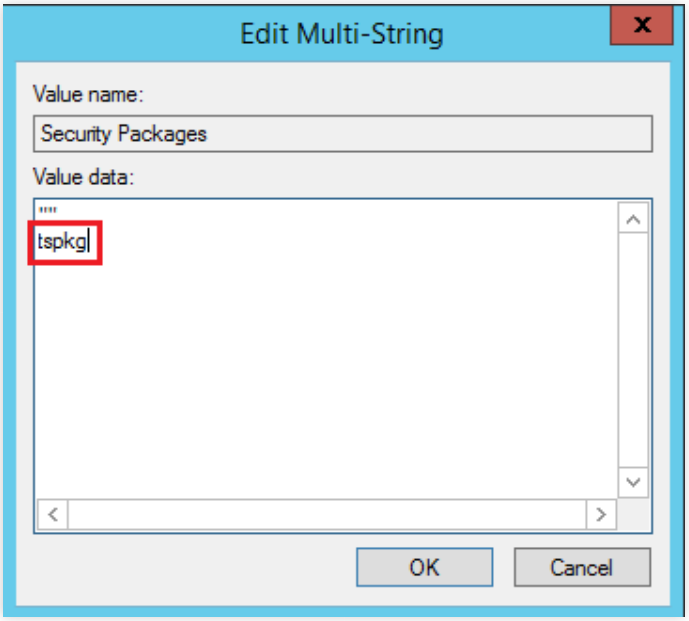


Modifying the Registry

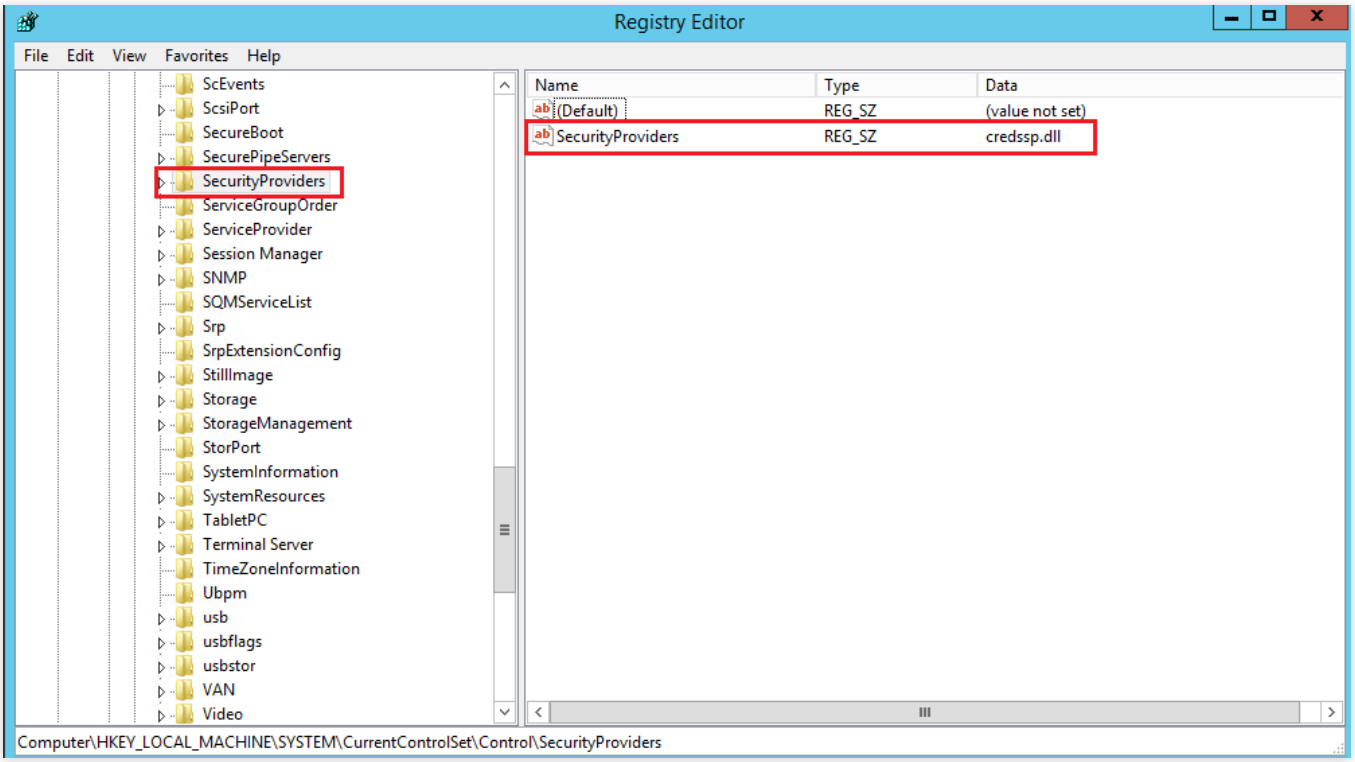
1. On the operating system interface, click , enter regedit, and press Enter to open the Registry Editor.
2. In the left sidebar, expand the directories in the following order:
   Computer > HKEY_LOCAL_MACHINE > SYSTEM > CurrentControlSet > Control > Lsa , and find Security Packages in the right window.



3. Double-click Security Packages to open the Edit Multi-String dialog box.
4. In the Edit Multi-String dialog box, add the tspkg character and click OK.



5. In the left sidebar, expand the directories in the following order:
   Computer > HKEY_LOCAL_MACHINE > SYSTEM > CurrentControlSet > Control > SecurityProviders , and find SecurityProviders in the right window.



6. Double-click SecurityProviders to open the Edit Multi-String dialog box.
7. Add , credssp.dll at the end of the Value Data in the Edit Multi-String dialog box, and click OK.
8. Close the registry editor, restart the instance, and you can log in remotely.

Windows Instance: Mac Remote Log-in Exception

This document describes common problems and solutions when you log in to Windows remotely using Microsoft Remote Desktop on your Mac.

Failure Symptoms

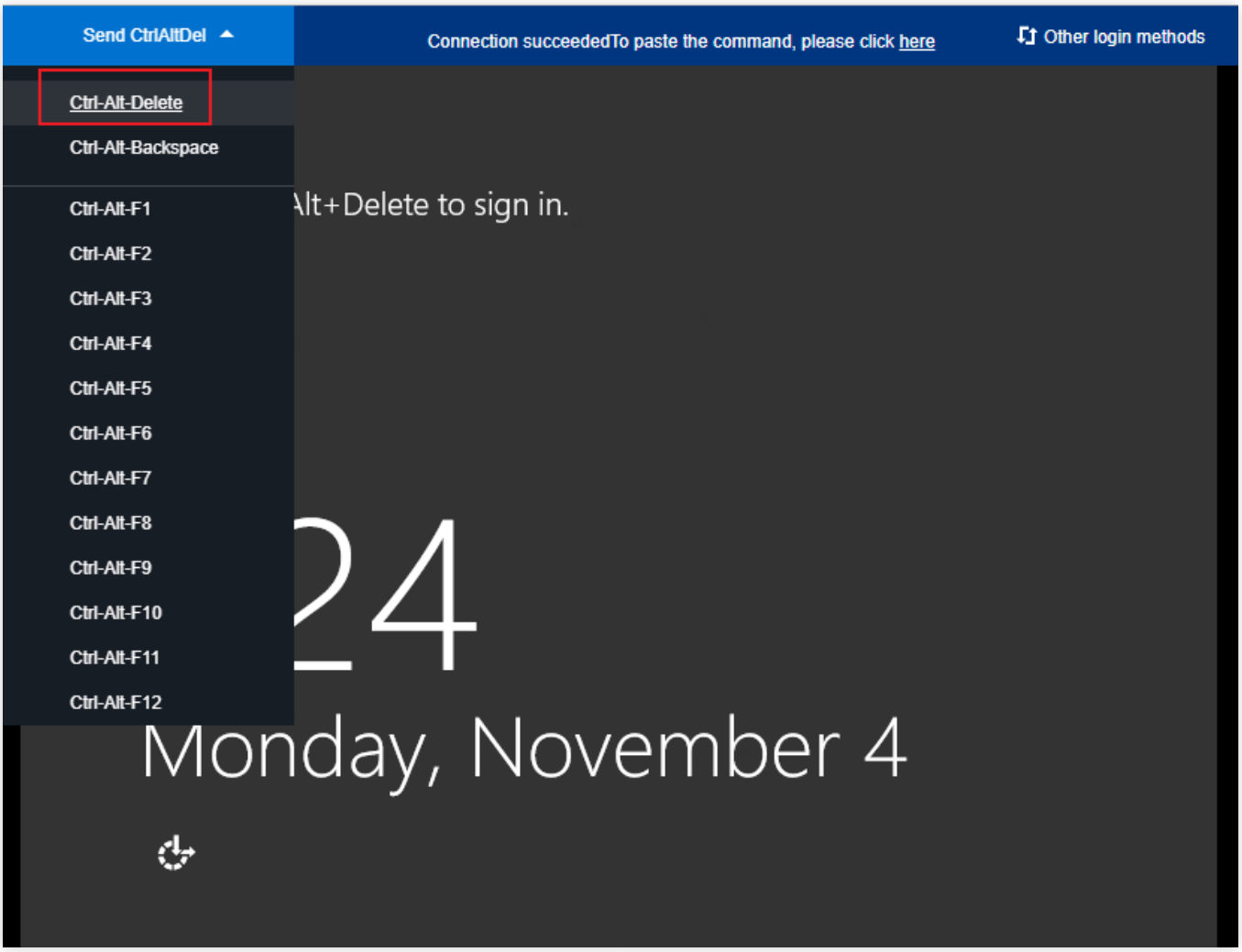
- When Mac logs into Windows remotely via Microsoft Remote Desktop, the message *The certificate couldn't be verified back to a root certificate* appears.
- When Remote Desktop Connection is used on a Mac, a message appears saying, *Remote Desktop Connection cannot verify the identity of the computer you want to connect to*.

Troubleshooting

> Note:
> The following operation uses Windows Server 2016 as an example.

Logging in to the CVM via VNC

1. Log in to the CVM console.
2. On the instance management page, find the target CVM instance and click Log In.
3. In the pop-up *Log in to Windows Instance* window, select Other methods (VNC) and click Log in now to log in to the CVM.
4. In the log-in window that pops up, select Send Remote Command in the upper left corner and click Ctrl-Alt-Delete to enter the system log-in interface.



Modifying the Instance's Local Group Policy

1. On the operating system interface, click , enter gpedit.msc, and press Enter to open the Local Group Policy Editor.

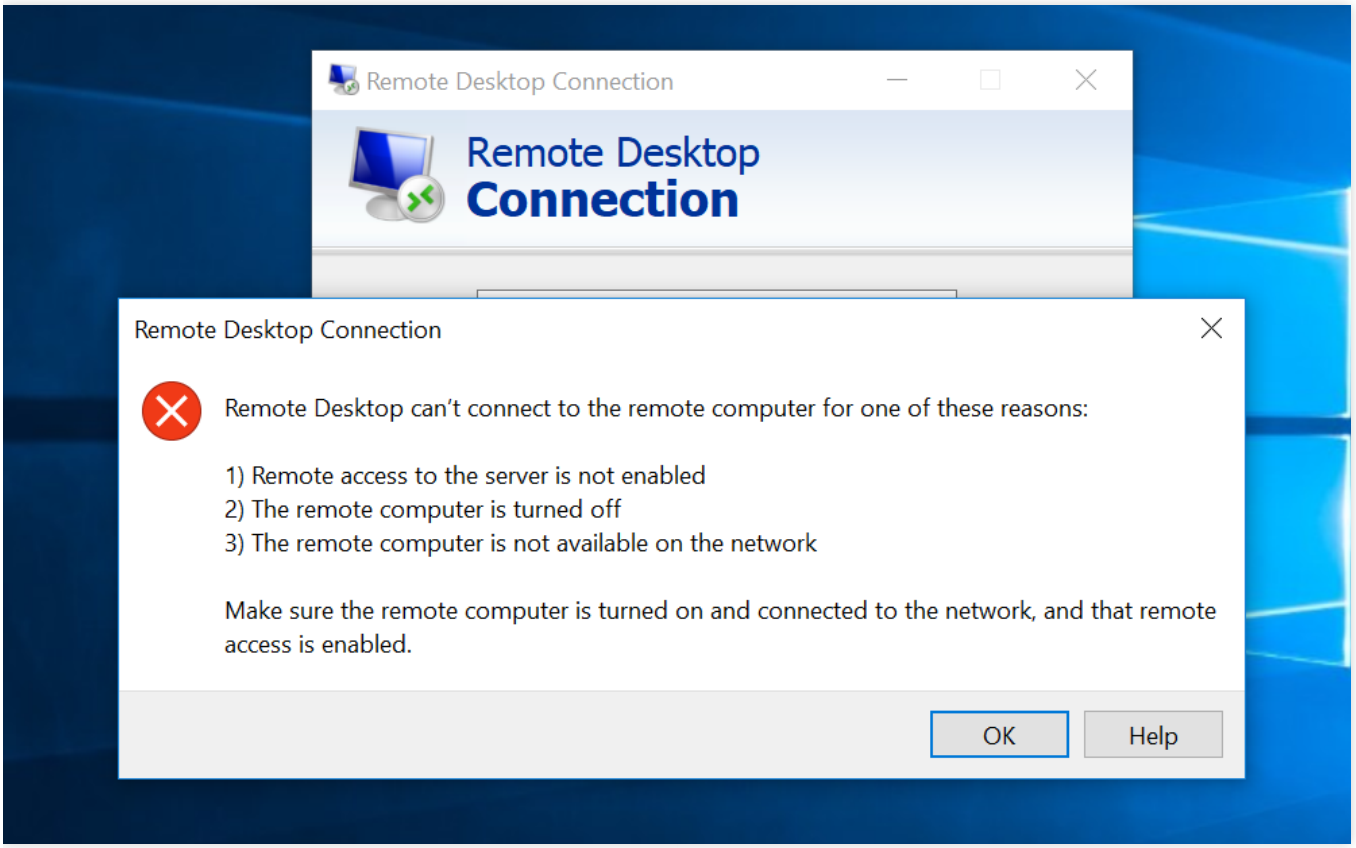
> Note:
> You can also use the Win+R shortcut key to open the Run interface.

2. In the left sidebar, select Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Security, and double-click Remote (RDP) connections require the use of a specified security layer.
3. In the window that opens, select Enabled and set Security layer to RDP.
4. Click OK to complete the configuration.
5. Restart the instance and try reconnecting to see if it works.

Windows Instance: Remote Desktop cannot connect to the remote computer

Applicable Scenario

The following prompt may appear when using Windows Remote Connection to a Windows instance:



Remote Desktop cannot connect to the remote computer for one of the following reasons:

1. Remote access to the server is not enabled
2. The remote computer is turned off
3. The remote computer is not available on the network
   Make sure the remote computer is turned on, connected to the network, and remote access is enabled.

Possible Reasons

The reasons for the above prompts include (not limited to the following situations, please analyze according to the actual situation):

- The instance is in an abnormal running status.

- No public IP or public bandwidth is 0.
- The security group bound to the instance does not allow access to the remote log-in port (the default port is 3389).
- Remote Desktop Services is not started.
- Remote Desktop settings issues.
- Windows Firewall settings issues.

Troubleshooting Steps

Check if the Instance is Running

1. Log in to the CVM console.
2. On the instance management page, check whether the instance is in Running status.
    - If yes, check whether the server has a public IP.
    - If no, start the Windows instance.

Check Whether the Server Has a Public IP

Check whether the server has a public IP in the CVM console.

- If yes, check whether to purchase public network bandwidth.
- If no, apply for an Elastic IP and bind it.

Check Whether to Purchase Public Network Bandwidth

Check whether the public network bandwidth is 0 Mb (minimum 1 Mbps).

- If yes, adjust the network bandwidth to 1 Mbps or above.
- If no, please check whether the instance remote login port (3389) is open.

Check Whether the Instance Remote Log-in Port (3,389) is Open

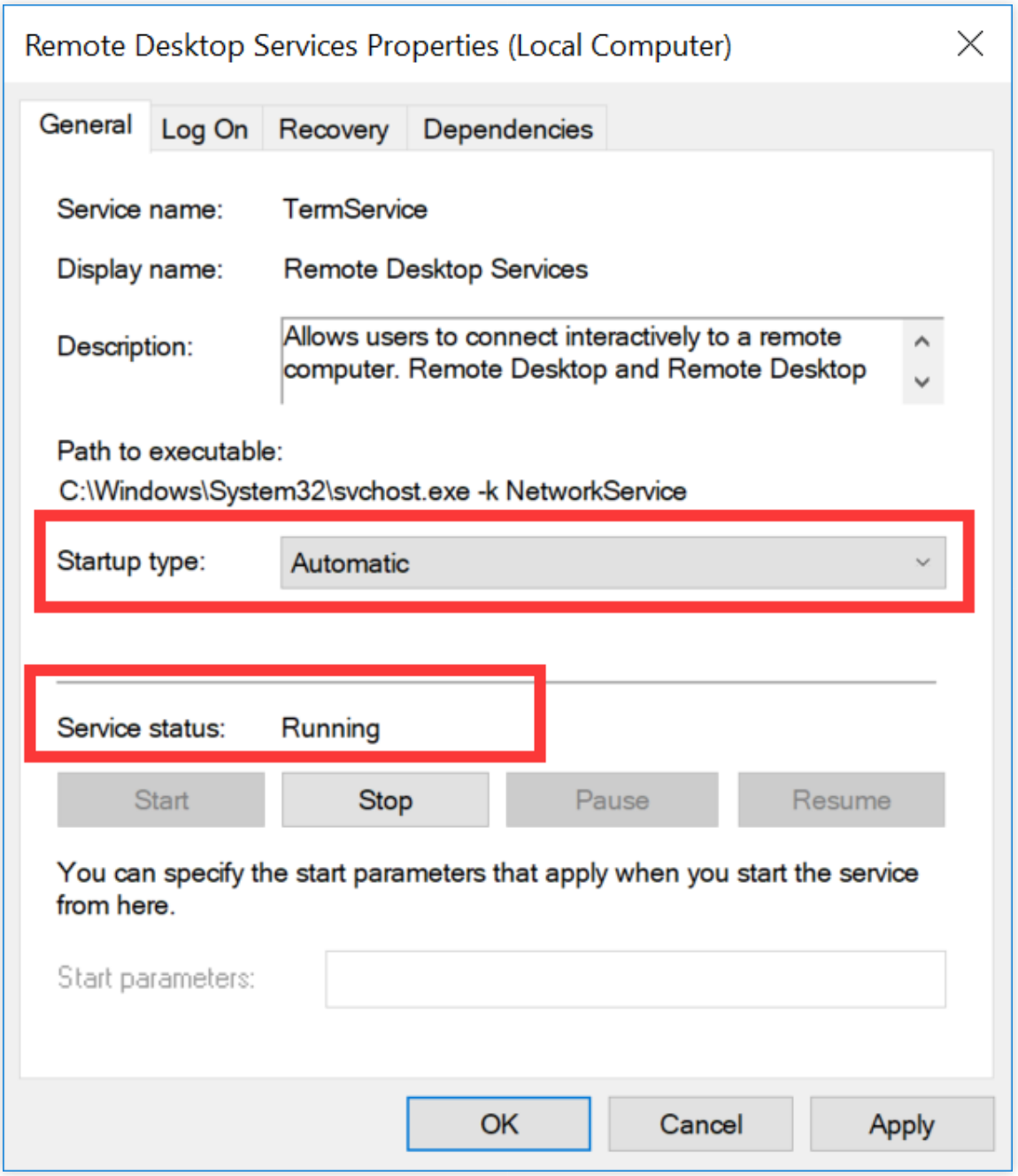
1. On the Instance Management page of the CVM console, click the instance ID/host name you want to log in to enter the instance details page.
2. On the Security Group tab, check whether the instance's security group has access to the remote log-in interface (default remote desktop port: 3,389).
    - If yes, please check the system settings of your Windows instance.
    - If no, edit the corresponding security group rules to allow the traffic to pass. For operation instructions, see Adding Security Group Rules.

Check the System Settings of Your Windows Instance

1. Use VNC to log in to the instance and troubleshoot the system settings of the Windows instance. > Note: The following operations are based on the Windows Server 2012 operating system instance.

2. In the logged-in instance system, right-click , select Run, enter services.msc in Run, and press Enter to open the Services window.

3. Double-click to open the properties of "Remote Desktop Services" and check if the Remote Desktop service is running.

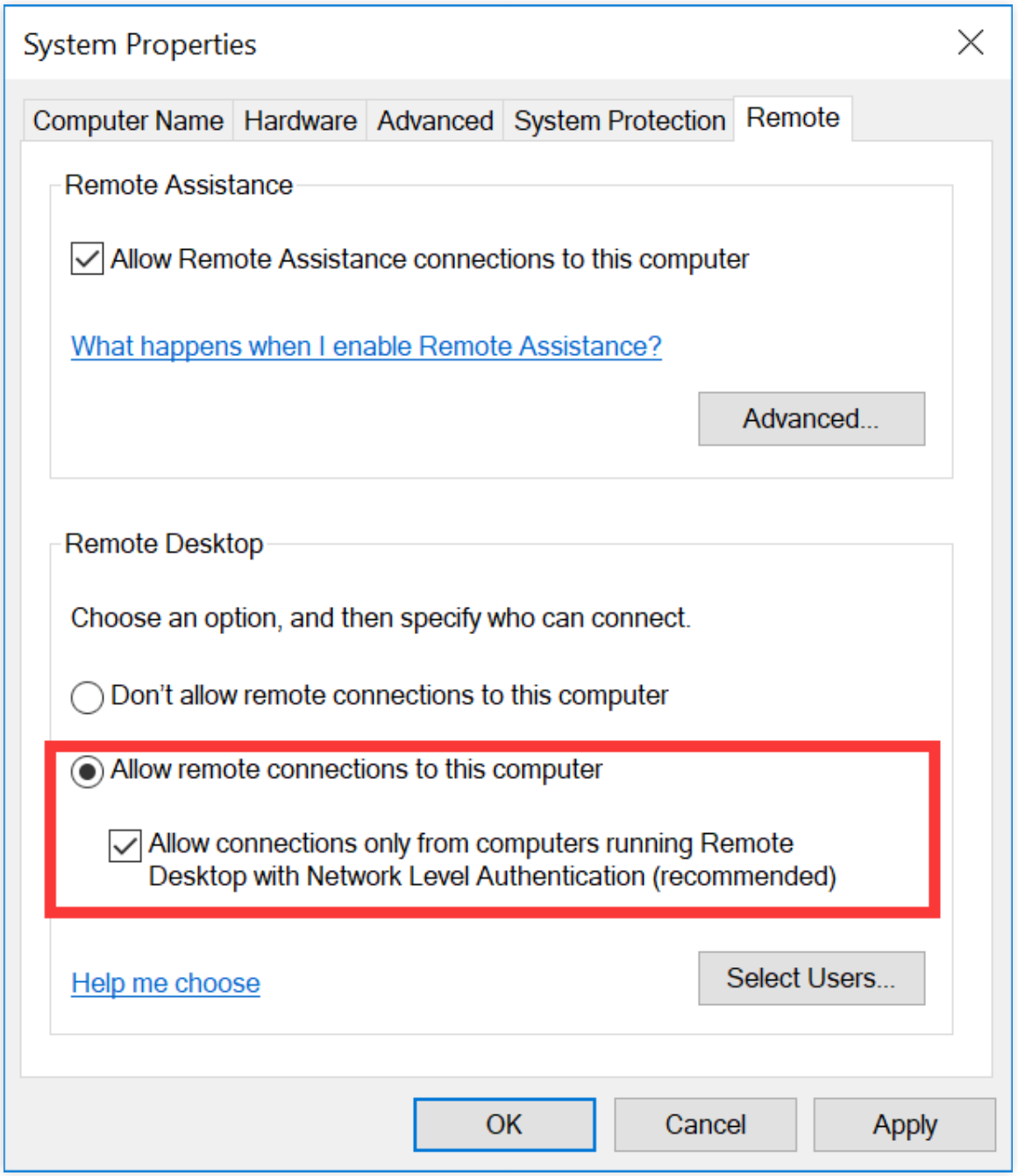


   - If yes, proceed to step 4.

- If no, please set the Startup Type to Automatic and the Service Status to Running (that is, click Start to start the service).

4. Right click , select Run, enter sysdm.cpl in Run, press Enter, and open the System Properties window.

5. On the "Remote" tab, check if Remote Desktop is set to "Allow remote connections to this computer(L)".

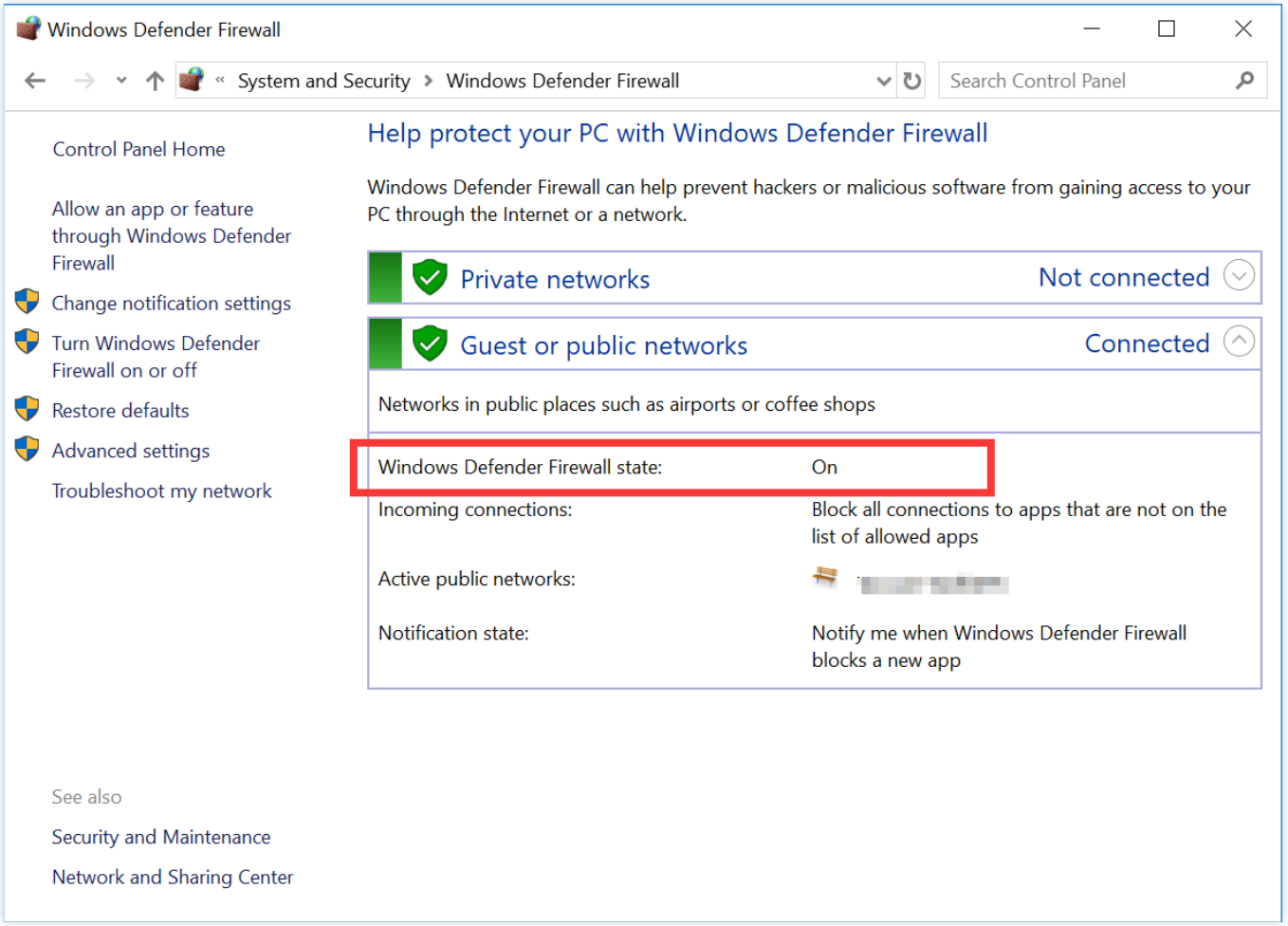


- If yes, proceed to step 6.
- If no, set Remote Desktop to Allow remote connections to this computer (L).

6. Click and select Control Panel to open the Control Panel.

7. In the Control Panel, select System and Security > Windows Firewall to open Windows Firewall.

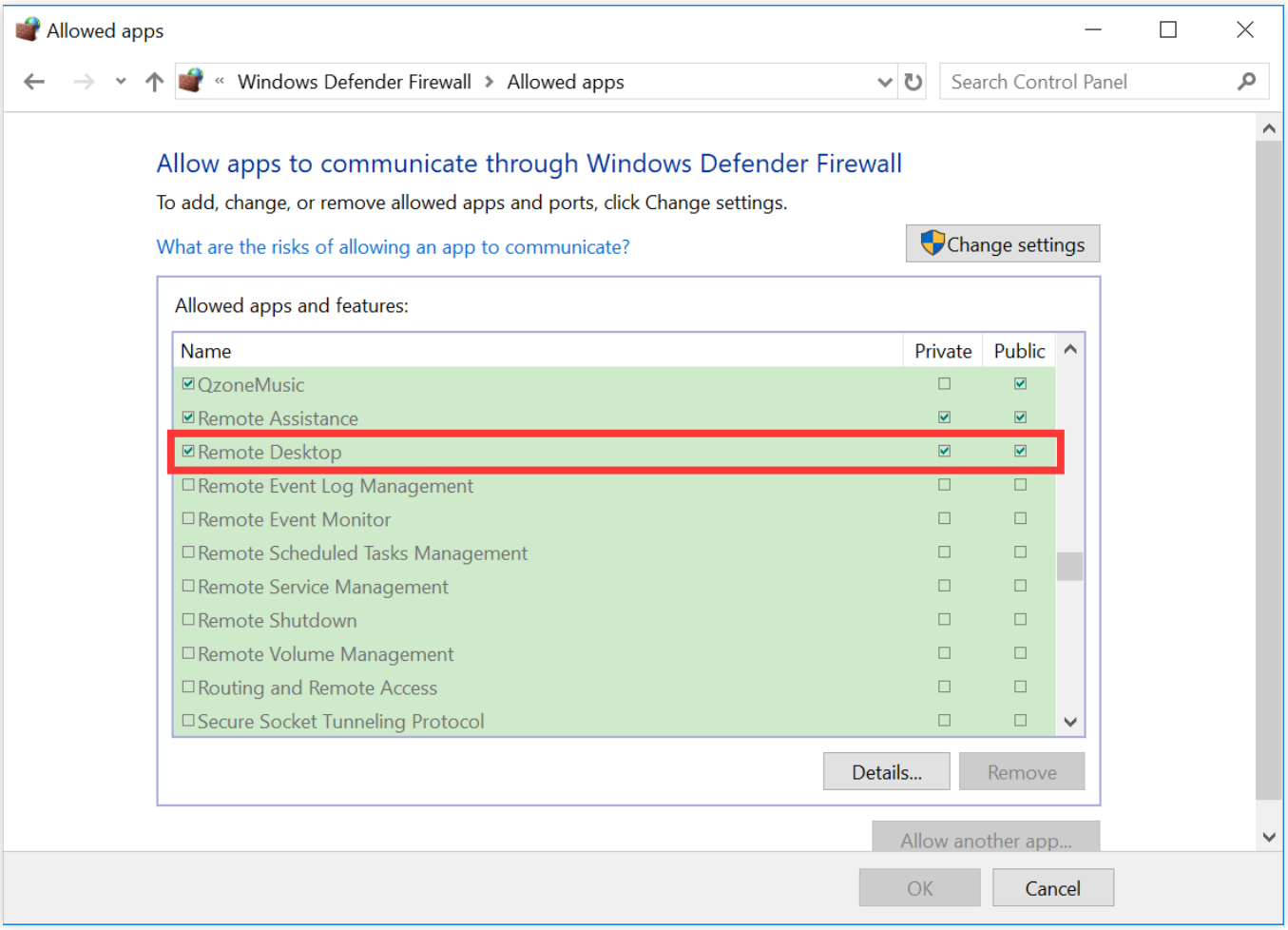
8. In "Windows Firewall", check the status of the Windows Firewall.



   - If the status is Enabled, proceed to step 9.
   - If the status is Disabled, submit a ticket for feedback.

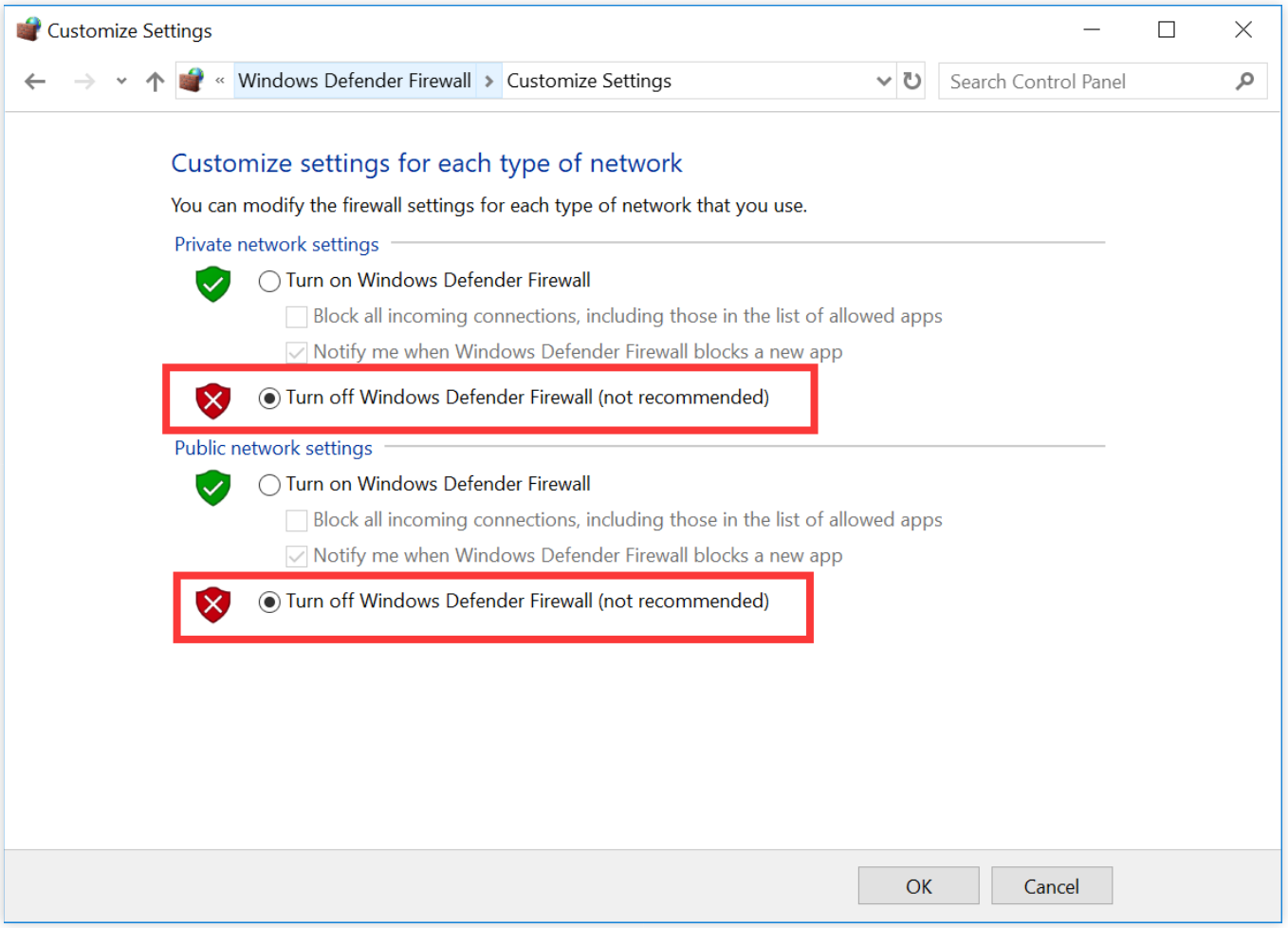
9. In Windows Firewall, click Allow an App or allow access through Windows Firewall to open the Allowed Apps window.

10. In the "Allowed Apps" window, check if "Remote Desktop" is checked under "Allowed Apps and Features (A)".



- If yes, proceed to step 11.
- If no, please check Remote Desktop and enable Remote Desktop.

11. In Windows Firewall, click Enable/Disable Windows Firewall to open the Custom Settings window.
12. In the "Private and Public Network Settings" window, set both "Private Network Settings" and "Public Network Settings" to "Turn off Windows Firewall (not recommended)".

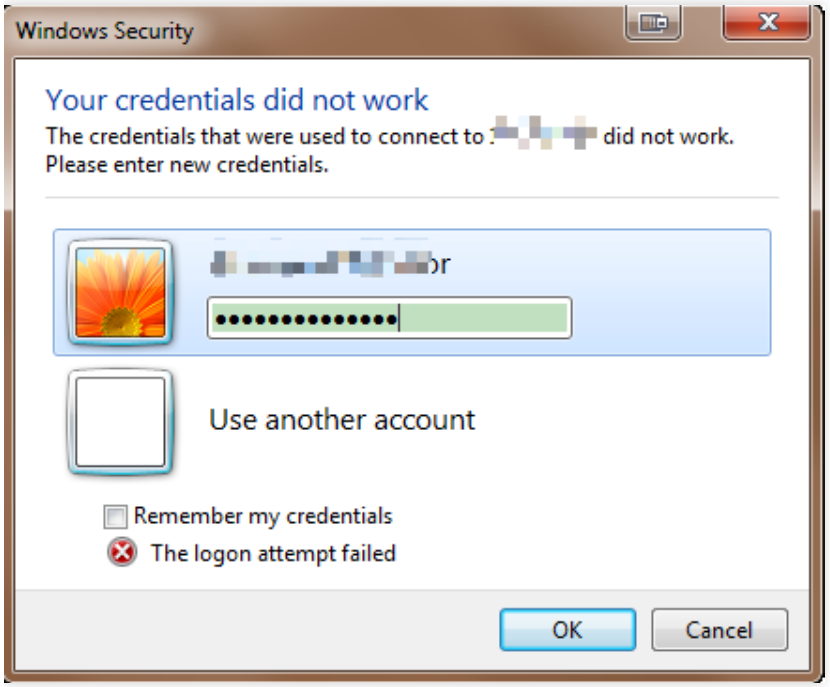


If you still cannot connect to your Windows instance through Remote Desktop after performing the above steps, please submit a ticket for feedback.

Windows Instance: Credentials Not Work

Problem Description

When a local computer running Windows operating system logs in to a Windows CVM through a remote desktop connection using the RDP protocol (such as MSTSC), the following error message appears:
Your credentials did not work. The credentials that were used to connect to XXX.XXX.XXX.XXX did not work. Please enter new credentials.



Processing Procedures

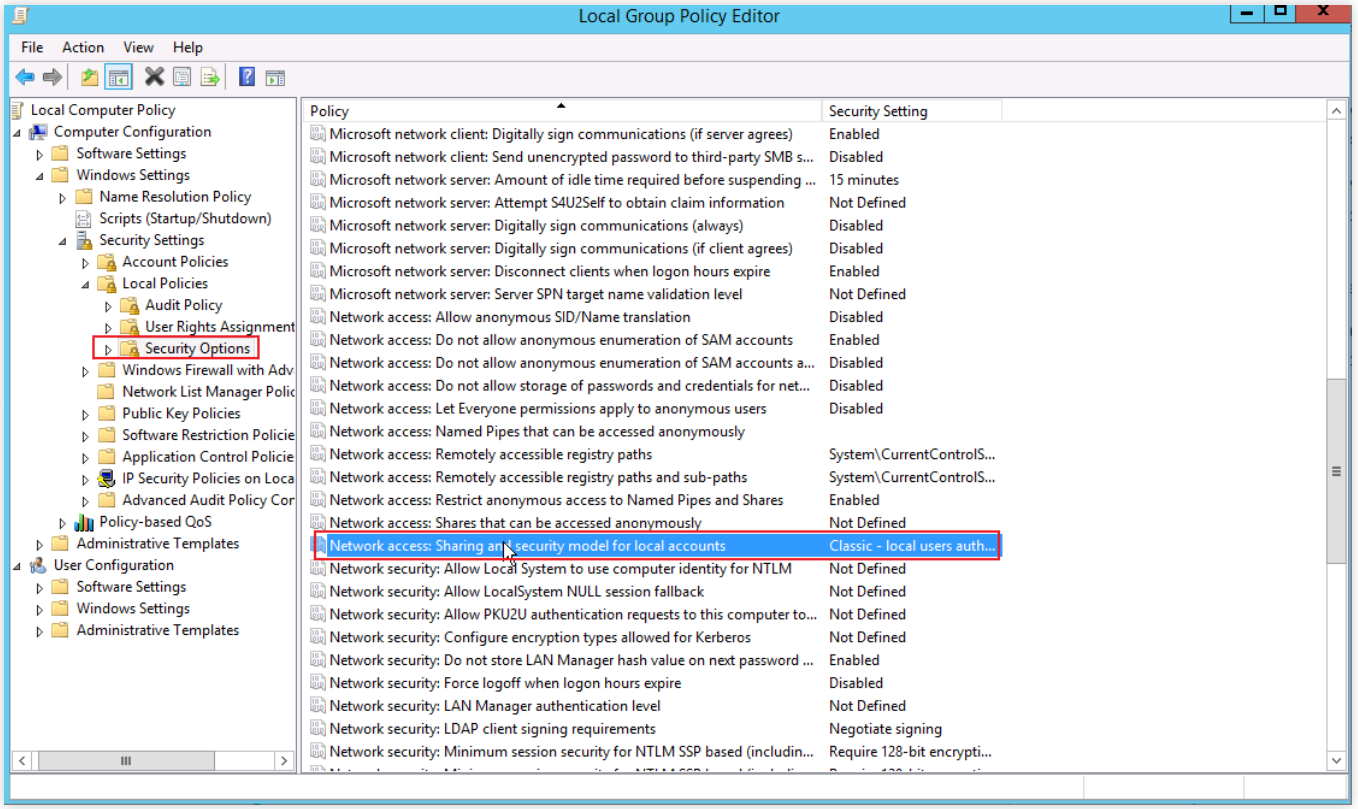
> Note: This document uses Windows Server 2012 as an example. The detailed steps may vary slightly depending on the version of the operating system.
> Follow the steps below to troubleshoot, and reconnect to the Windows CVM after each step to verify whether the problem is solved. If not, proceed to the next step.

Step 1: Modify the Network Access Policy

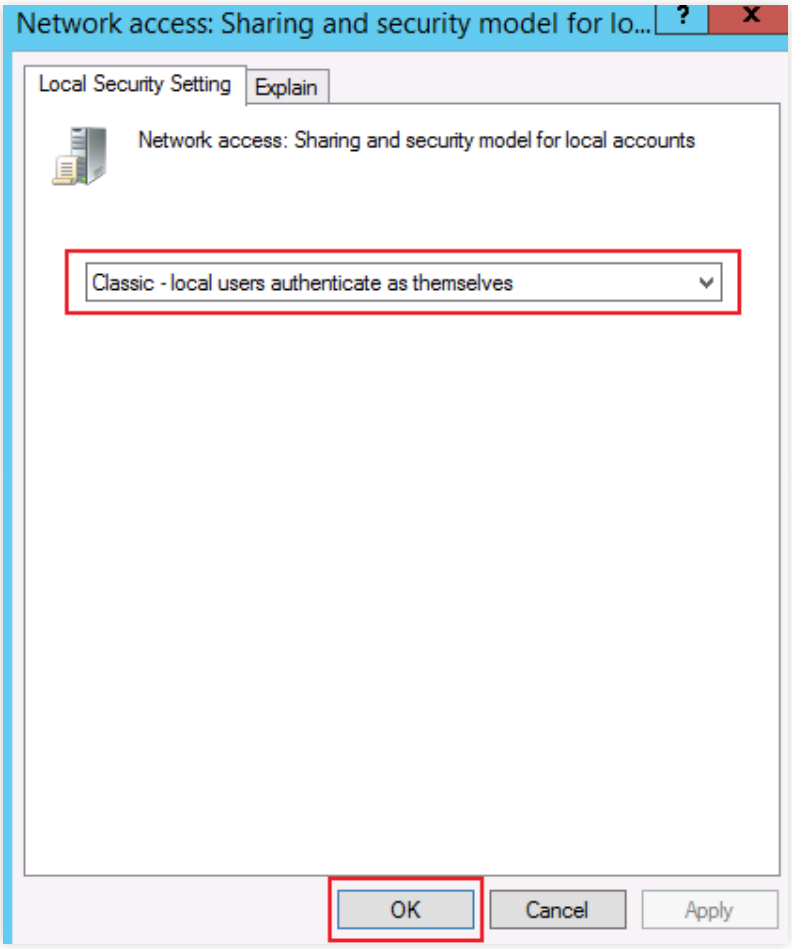
1. Logging in to a Windows instance using VNC。

2. On the operating system interface, click and open the Windows PowerShell window.
3. In the Windows PowerShell window, enter gpedit.msc, and press Enter to open the Local Group Policy Editor.

4. In the left sidebar, expand Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options.
5. Find and open Network access: Sharing and security model for local accounts in Security Options. As shown below:



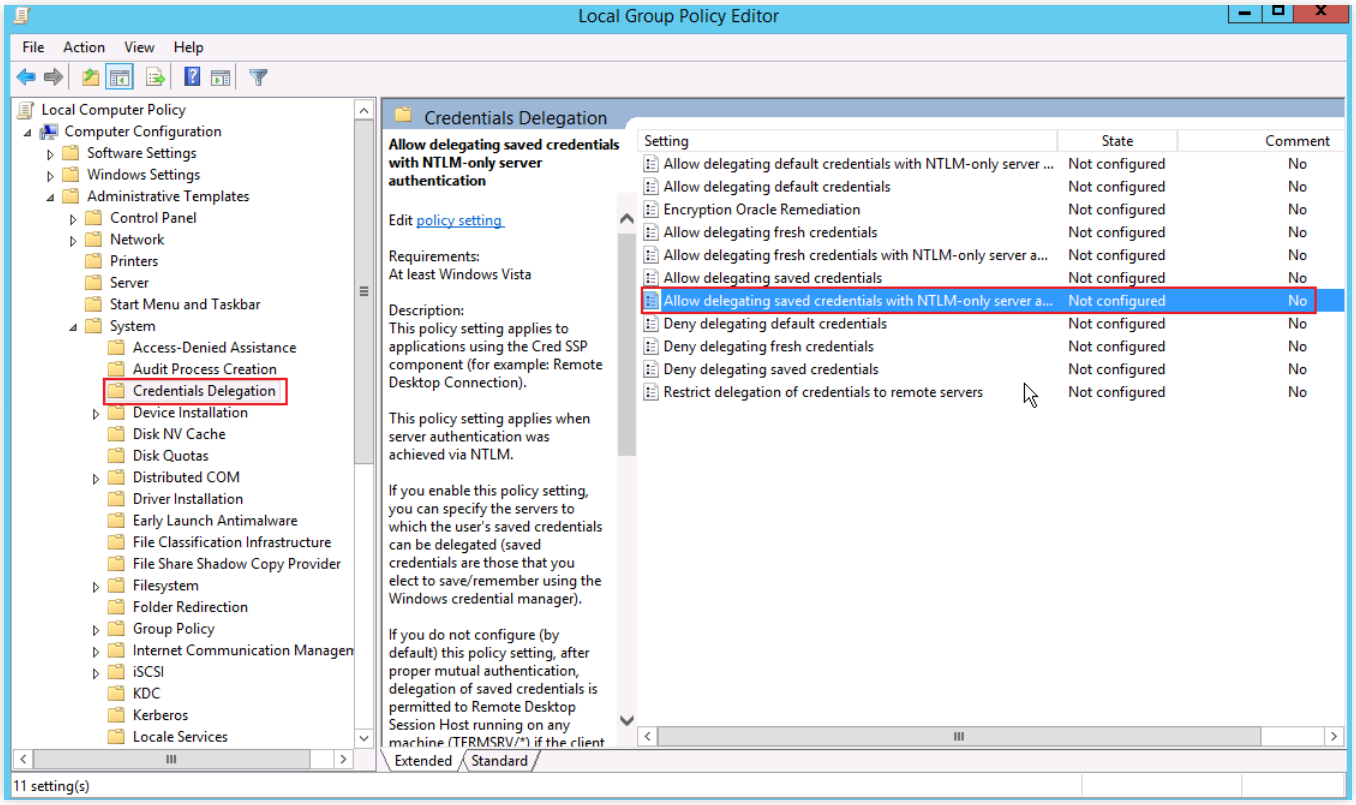
6. Select Classic - Authenticate local users without changing their original identities and click OK. As shown below:



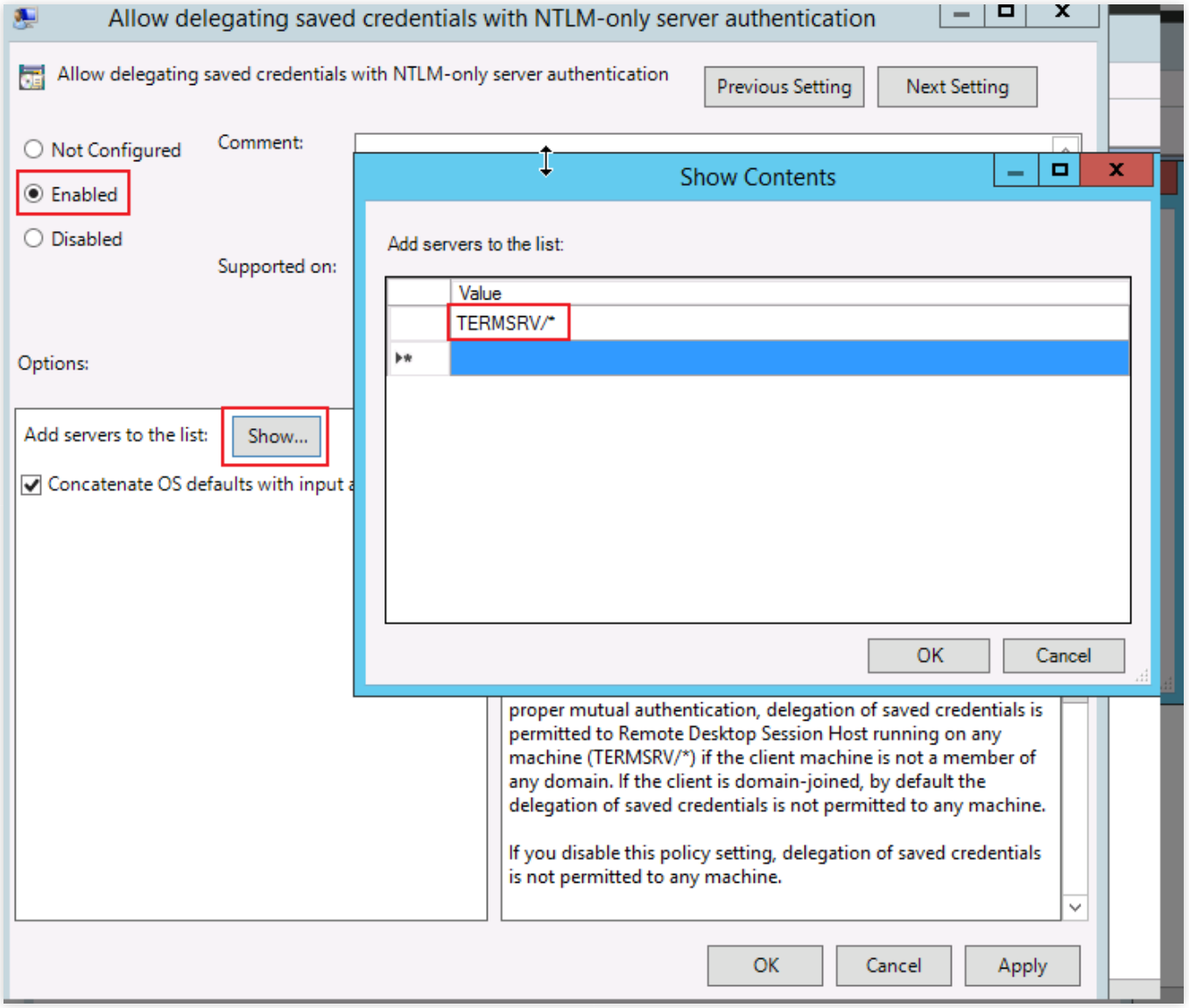
7. Reconnect to the Windows CVM and verify that the connection is successful.
    - Yes, the mission completed.
    - No, proceed to Step 2: Modify Credentials Delegation.

Step 2: Modify Credentials Delegation

1. In the left sidebar of the Local Group Policy Editor, expand Computer Configuration > Administrative Templates > System > Credentials Delegation.
2. Find and turn on Allow distribution of saved credentials for NTLM server authentication in Credentials Delegation, as shown below:

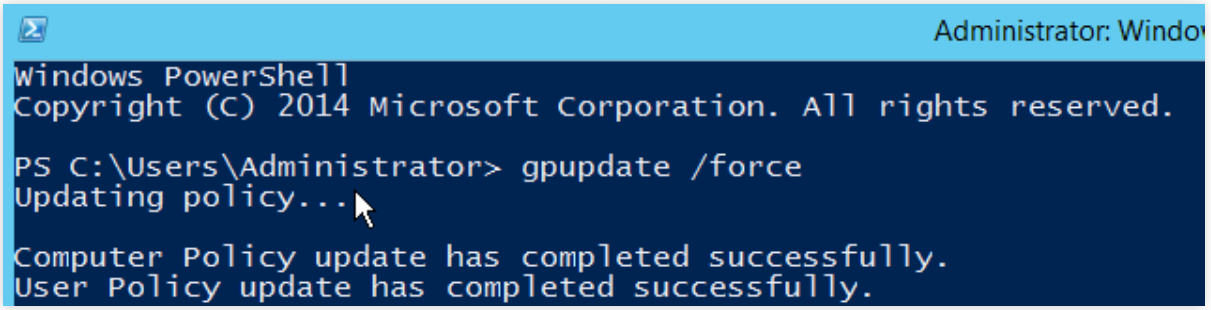


3. In the window that opens, select Enabled and enter TERMSRV/* in Display in Options, and click OK. As shown below:



4. Click OK.

5. On the operating system interface, click and open the Windows PowerShell window.
6. In the Windows PowerShell window, enter gpupdate /force, and press Enter to update the group policy. As shown below:

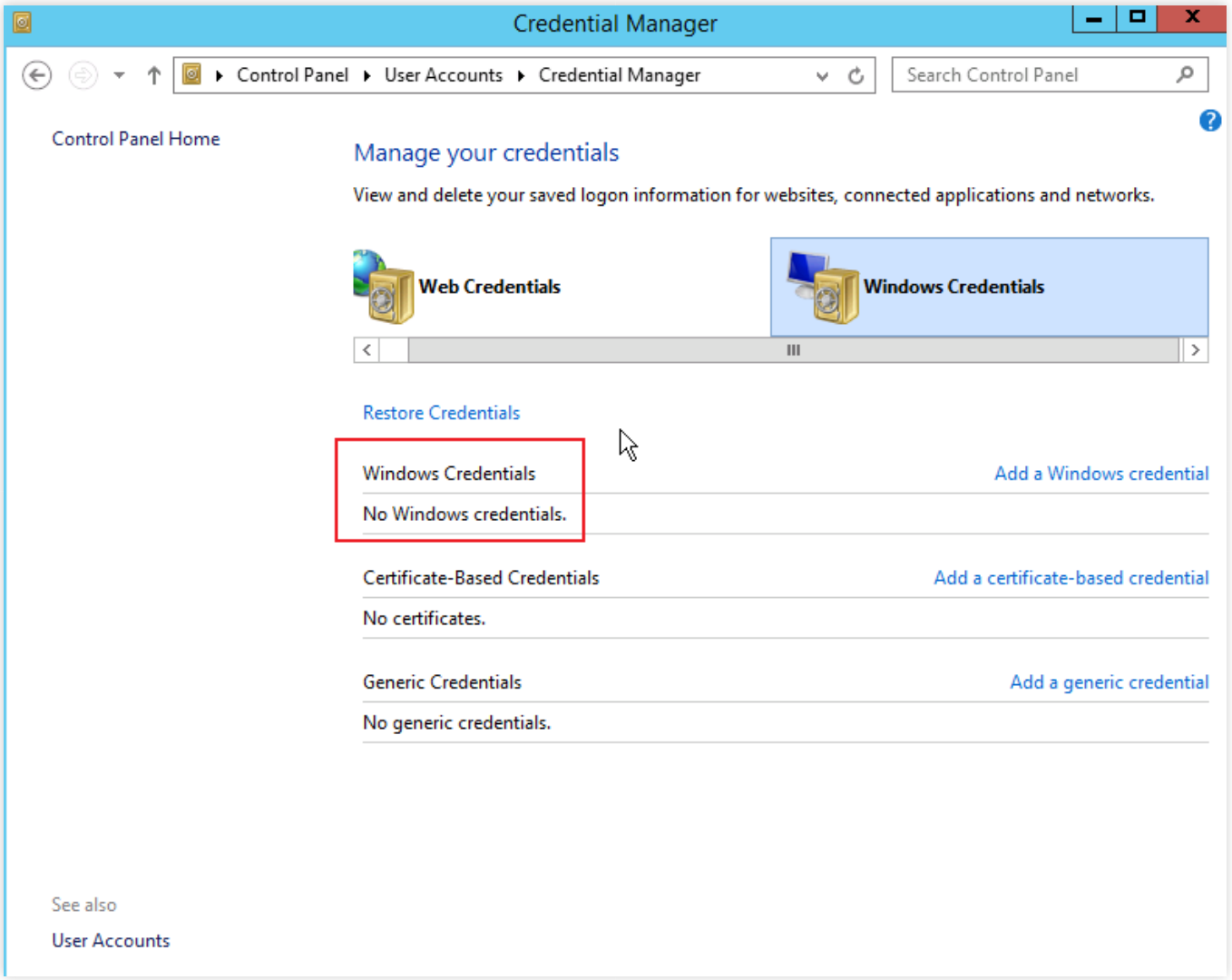


7. Reconnect to the Windows CVM and verify that the connection is successful.

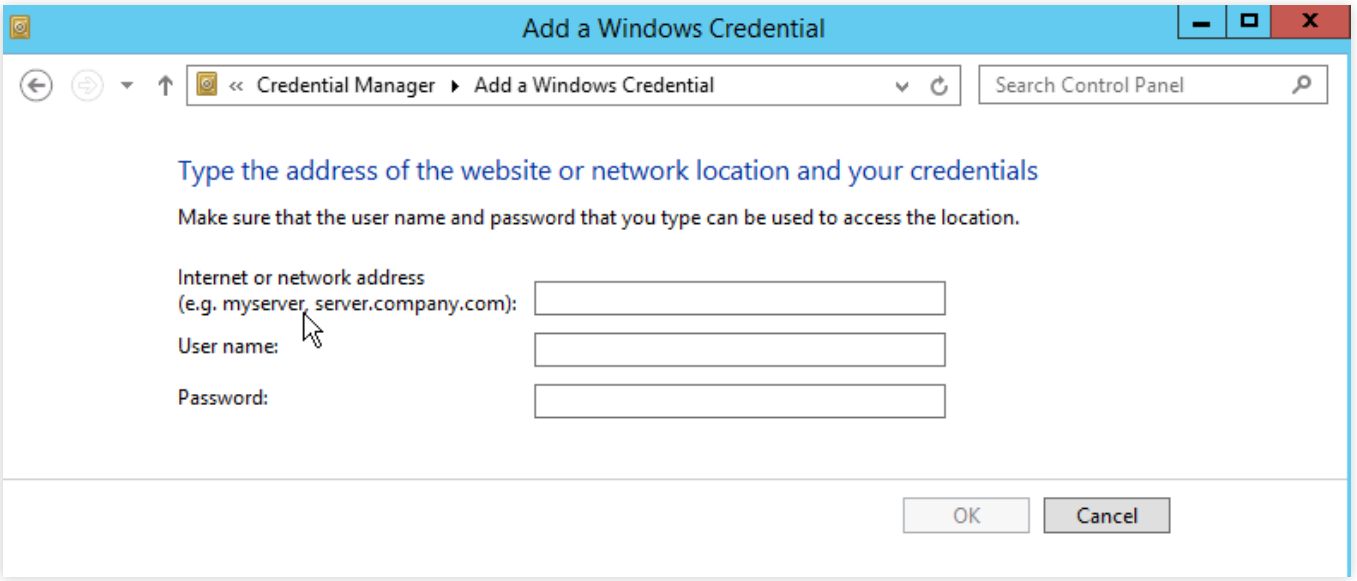
- Yes, the mission completed.
- No, proceed to Step 3: Set credentials for the localhost.

Step 3: Configure Local Credentials

1. On the operating system interface, click > Control Panel > User Accounts, select Manage Windows Credentials under Credential Manager to enter the Windows Credentials interface, as shown below:



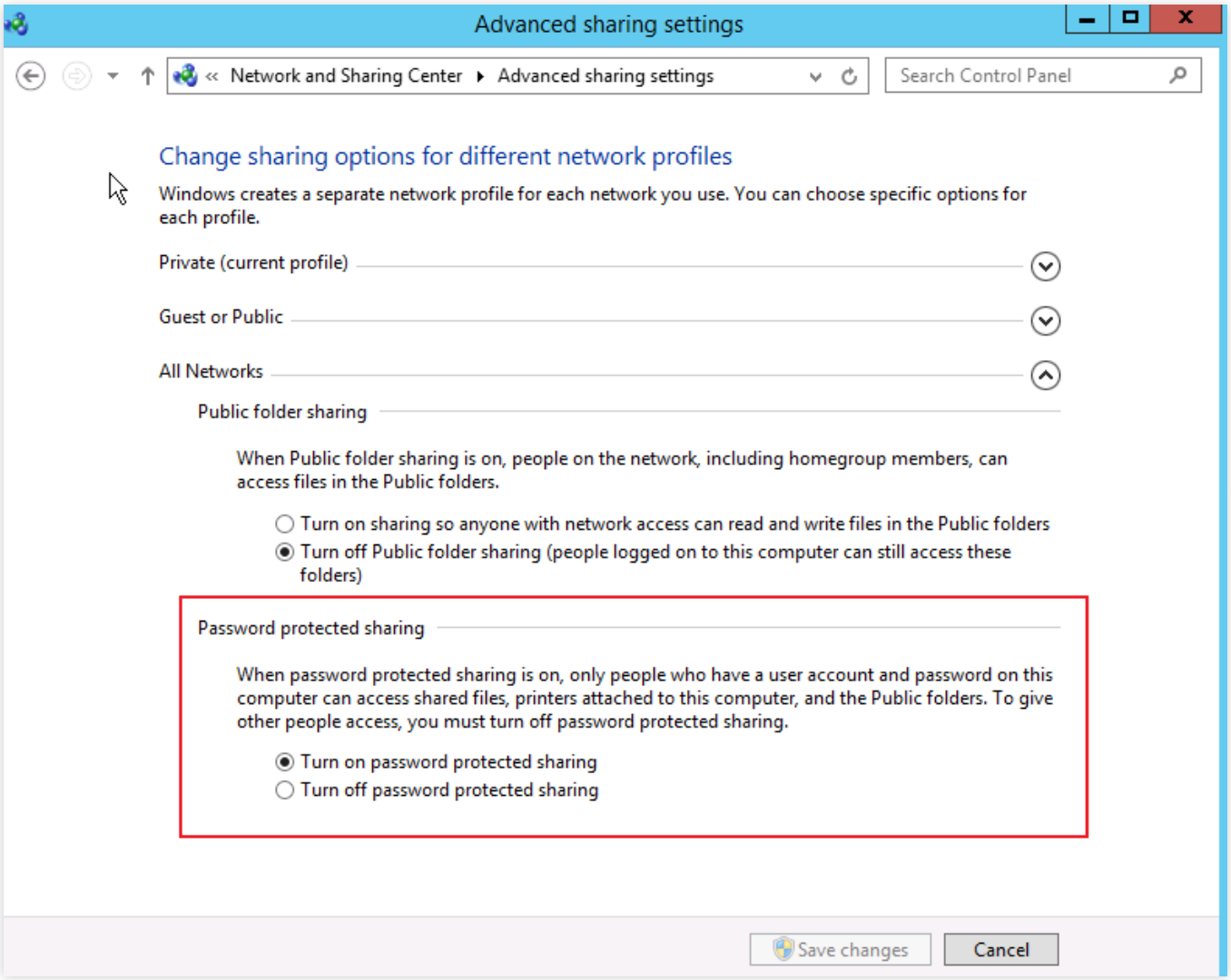
2. Check whether there is a currently logged-in CVM credential under Windows credentials.
   - If not, proceed to the next step to add Windows credentials.
   - If yes, proceed to step 4: Disable password-protected sharing of the CVM.
3. Click Add Windows Credentials to enter the Add Windows Credentials interface, as shown below:



4. Enter the IP address of the CVM you are currently logged in to, as well as your user name and password, and click OK.
5. Reconnect to the Windows CVM and verify that the connection is successful.
    - Yes, the mission completed.
    - If no, proceed to Step 4: Disable password-protected sharing of the CVM.

Step 4: Turn off password protected sharing

1. On the operating system interface, click > Control Panel > Network and Internet > Network and Sharing Center > Change advanced sharing settings to enter the advanced sharing settings interface. As shown below:



2. Expand the All Networks tab, select Turn off password protected sharing under Password protected sharing, and click Save changes.
3. Reconnect to the Windows CVM and verify that the connection is successful.
    - Yes, the mission completed.
    - No, please report to the maintenance engineer.

Windows Instance: Failed to log in to a Windows CVM due to high

This document introduces the troubleshooting methods and solutions for Windows CVMs that cannot log in due to high CPU or memory usage.

> Note:
> The following directions are based on Windows Server 2012 R2. The detailed directions may vary depending on the operating system version.

Possible Reasons

High CPU or memory usage can easily lead to problems such as slow service response and server login failure. The reasons for high CPU or memory usage may be caused by factors including hardware factors, system processes, business processes, or Trojan viruses. You can use Cloud Monitor to create a CPU or memory Utilization threshold alarm, and when the CPU or memory usage exceeds the threshold, you are notified in time.

Troubleshooting Approach

1. Locate specific processes that are consuming CPU or memory resources.
2. Analyze processes with high CPU or memory usage resources.
    - If it is an exception process, the high CPU or memory usage may be caused by a virus or Trojan horse. You can terminate the process manually or use security software to detect and kill it.
    - If it is a business process, you need to analyze whether the high usage is caused by changes in traffic and whether there is room for optimization.
    - If it is a Converge Cloud component process, submit a ticket and contact us for further localization.

Positioning Tools

Task Manager: An application and process management tool that comes with Windows, which displays information about computer performance and running software, including the name of the running process, CPU load, memory usage, I/O status, logged-in users, and Windows service information.

- Process: A list of all running processes on the system.
- Performance: Overall statistics about system performance, such as overall CPU usage and the amount of memory in use.
- User: All users who currently have sessions on the system.

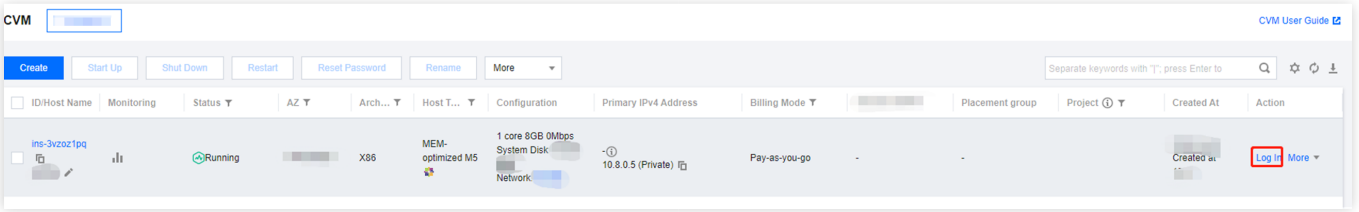
- Details: An enhanced version of the Process tab, which displays detailed information about the process, such as the process's PID, status, CPU, and memory usage.
- Service: All services in the system (including those that are not running).

Troubleshooting

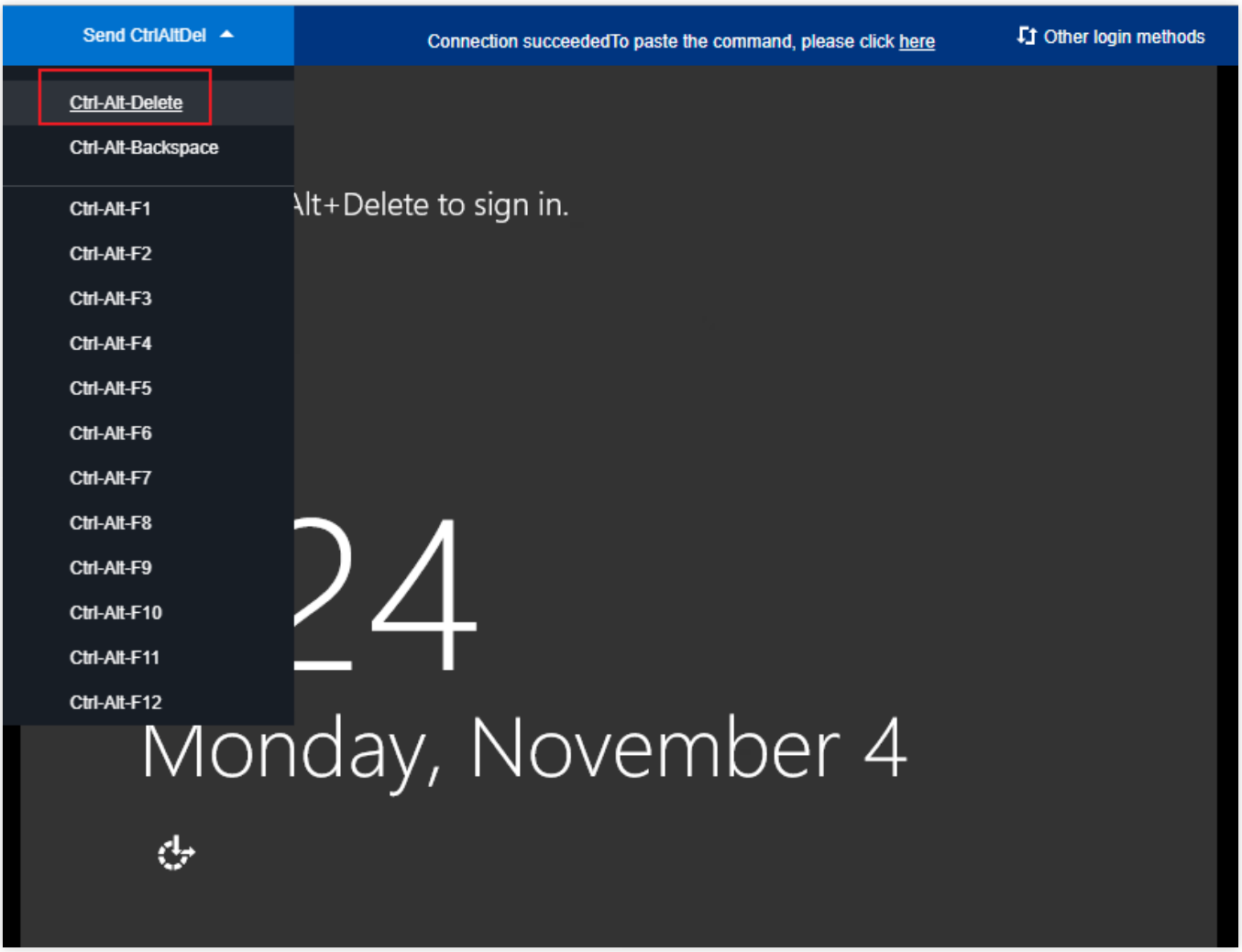
Logging in to the CVM via VNC

> Note:
> If the CVM is heavily loaded, you will not be able to establish a remote connection and will need to use VNC to log in to the Windows instance.

1. Log in to the CVM Console.
2. In the instance list, select the Windows CVM you want to log in to and click Log In.

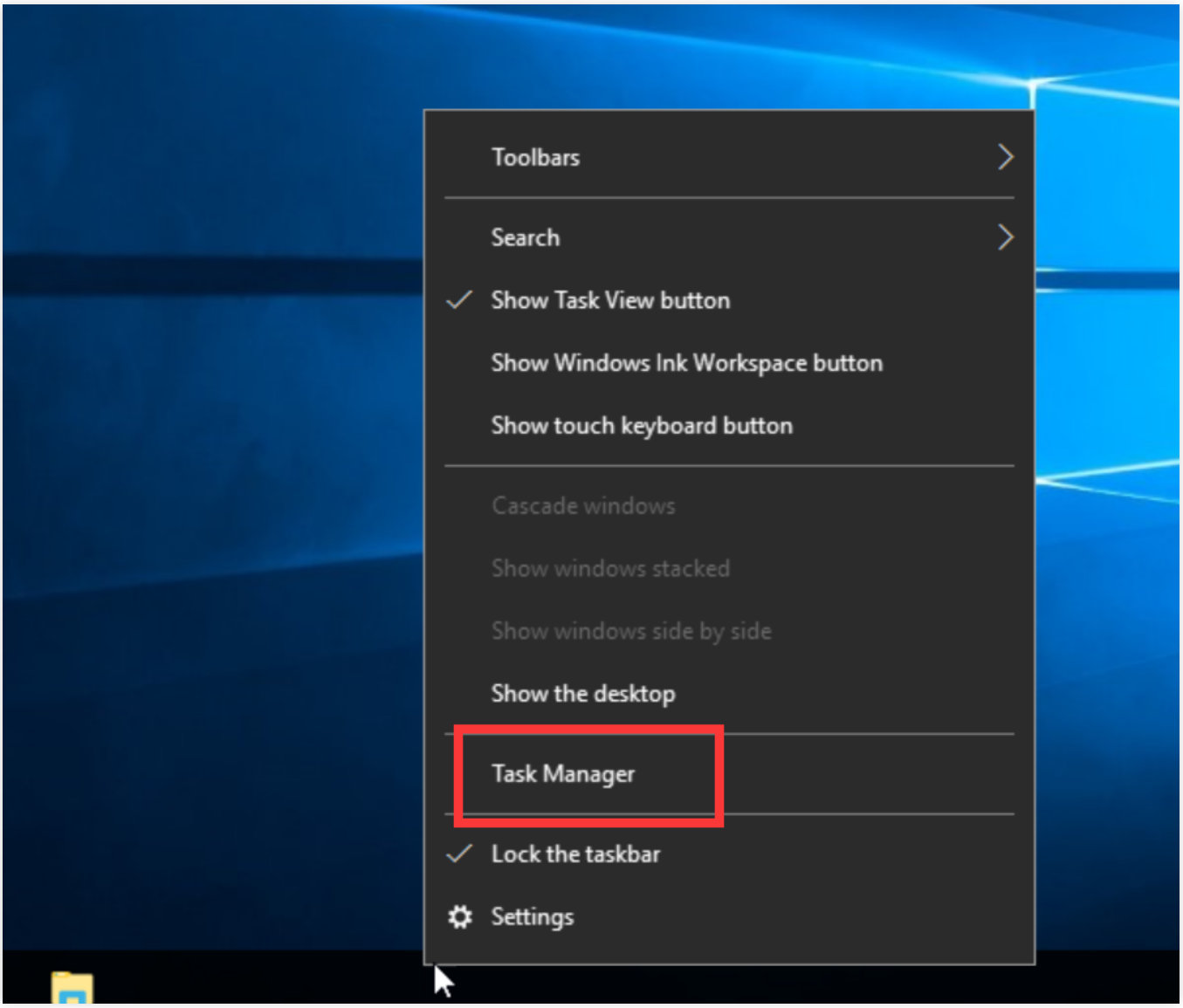


3. In the pop-up Standard Log-in | Windows Instance window, select VNC Log-in.
4. In the log-in window that pops up, select Send Remote Command in the upper left corner and click Ctrl-Alt-Delete to enter the system log-in page.



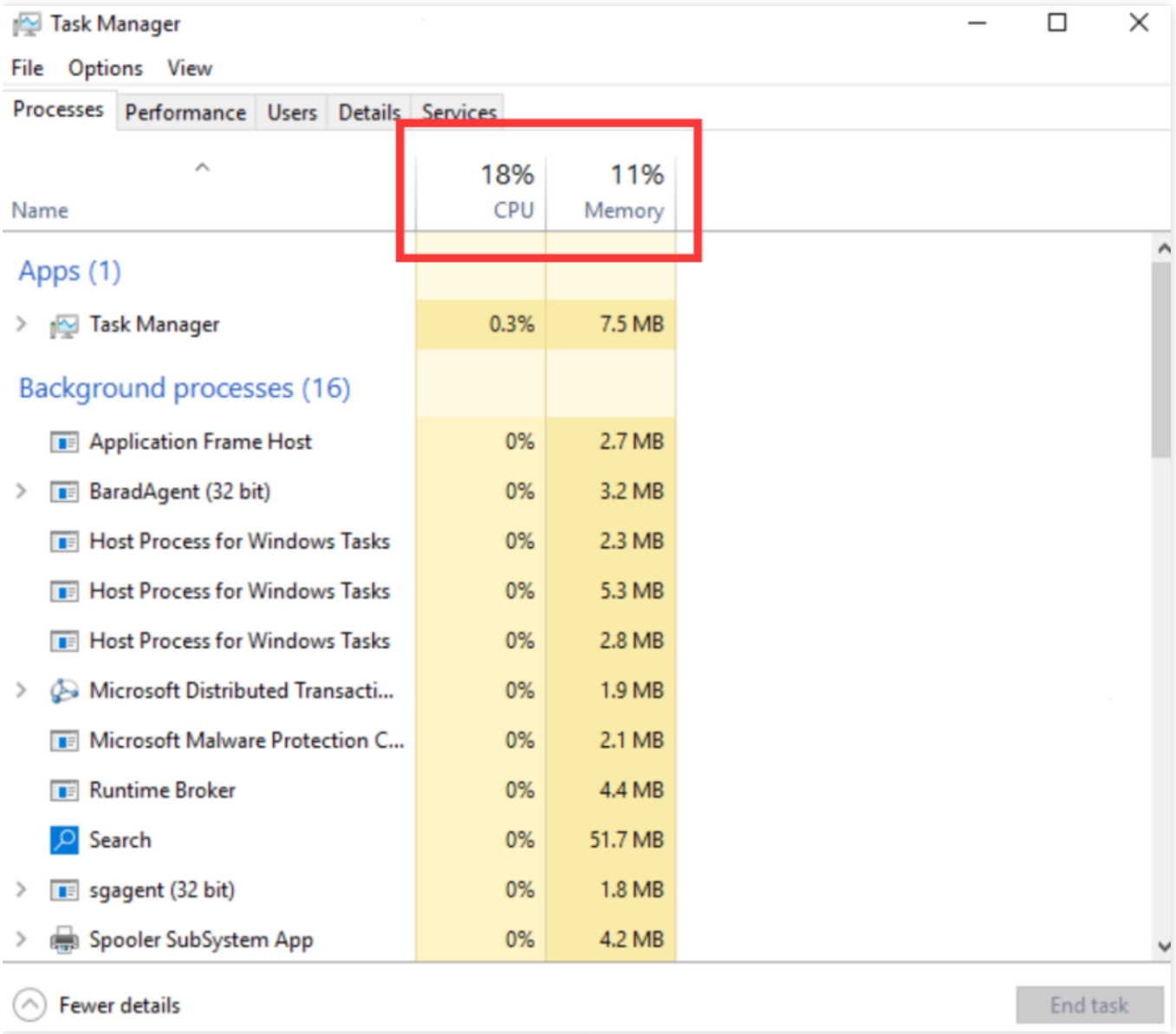
Checking Process Usage

1. In the CVM, right-click the Taskbar and select Task Manager. As shown below:



2. In the opened Task Manager, you can view the resource usage. As shown below:

> Note:
> You can click CPU or Memory to sort the processes in ascending/descending order.



Process Analysis

Analyze and troubleshoot problems based on the processes in the task manager and take corresponding solutions.

A system process causes the issue

If you find that system processes are taking up a lot of CPU or memory resources, please check the following:

1. Check the process name.
   Some viruses use names similar to system processes, such as svch0st.exe, explore.exe, iexplorer.exe, etc.
2. Check the location of the executable file corresponding to the process.
   System processes are generally located in the directory C:\Windows\System32 and have complete signatures and introductions. In Task Manager, right-click the process you want to view and select Open File Location to view the location of the specific executable file. For example svchost.exe .
   - If the process location is not under the directory C:\Windows\System32 , it indicates that the CVM

may be infected with a virus. Please manually check and remove it or use a security tool to scan and disinfect it.
    - If the process location is under the C:\Windows\System32 directory, please restart the system or close unnecessary but safe system processes.

Common system processes are as follows:

- System Idle Process: system space process, showing the percentage of CPU idle time
- system: memory management process
- Explorer: desktop and file management
- iexplore: Microsoft's browser
- csrss: Microsoft Client/Server Runtime Subsystem
- svchost: system process, used to execute DLL
- Taskmgr: Task Manager
- Isass: Local Security Authority Subsystem Service

An unhealthy process causes the issue

If you find some processes with strange names that take up a lot of CPU or memory resources, they may be Trojan virus processes, such as xmr64.exe (mining virus). It is recommended that you use a search engine to search and confirm whether it is a Trojan virus process.

- If it is a Trojan virus process, please use security tools to detect and kill it. Consider backing up data and reinstalling the system if necessary.
- If it is not a Trojan virus process, please restart the system or close unnecessary and safe processes.

A service process causes the issue

If you find that business processes occupy a large amount of CPU or memory resources, such as IIS, HTTPD, PHP, Java, etc., further analysis is recommended.
For example, determine whether the current business volume is large.

- If the business volume is large, it is recommended that you upgrade the server configuration. If you do not upgrade the server configuration, you can consider whether there is room for optimization in the business program and optimize it.
- If the business volume is not large, further analysis is required in combination with the business error log. For example, improper parameter configuration leads to wasted resources.

A Converge Cloud component process causes the issue

Submit a ticket to contact us for further troubleshooting and handling.

Port Problem Cause Remote Connection Failure

This document introduces the troubleshooting methods and solutions for the situation where a CVM cannot be remotely logged in due to a port problem.

> Note:
> The following operations take a Windows Server 2012 system CVM as an example.

Troubleshooting Approach

Checking Network Connectivity

You can use the local Ping command to test the network connectivity. At the same time, use computers in different network environments (different IP ranges or different operators) to test and determine whether the issue lies within the local network or on the server side.

1. Select the appropriate method to open the command line interface based on the operating system of the local computer.
    - Windows System: Click Start > Run and enter cmd, and a command line dialog box pops up.
    - MacOS: Open the Terminal.

2. Run the following command to test the network connection.

    ping + the public IP address of the CVM instance

Linux Instance-related
Unable to Log in to a Linux Instance

This document introduces how to troubleshoot problems when you cannot connect to a Linux instance, exploring the primary factors that may cause the inability to connect to Linux instances, and a guide through the steps of troubleshooting, locating, and solving the problems.

Possible Reasons

The main reasons for being unable to log in to Linux instance include:

- SSH issue prevents log-in
- Unable to log in due to password problem
- High bandwidth usage
- High server load
- Remote port configuration error
- Improper security group rules

Troubleshooting

Log-in via VNC

Log in by Converge Cloud VNC log-in and you can locate the cause of the fault with it.

1. Log in to the CVM console.
   On the instance management page, select the instance you want to log in to and click Log In.
2. In the pop-up Log in to Linux Instance window, select Other methods (VNC) and click Log in now.

> Note:
> If you forget your password during the log-in, you can reset the password for the instance in the console. For specific operations, refer to [Reset Instance Password](/document/product/221286/16566).

3. In the dialog box that pops up, enter your username and password to complete the log-in process.

SSH issue prevents log-in

Fault Phenomena: When you use SSH to log in to a Linux instance, an error message indicating unable to connect or connection failure appears.

Directions: Refer to Unable to Log in to Linux Instance via SSH for troubleshooting.

Unable to log in due to password problem

Fault Phenomenon: Log-in failed due to incorrect password input, forgotten password, or failed password reset.
Solution: Reset the password of the instance in the console and restart the instance.
Directions: For how to reset the instance password, refer to Reset the Instance Password.

High bandwidth usage

Fault Phenomenon: The self-diagnosis tool shows that the problem is high bandwidth utilization.
Directions:

1. Log in to the instance via VNC log-in.
2. See High Bandwidth Usage Prevents Log-in, track the bandwidth usage of the instance and address faults.

High server load

Fault Phenomenon: Self-service checking tools or cloud monitoring shows that the high server CPU load causes the failure of remote system access or significant access latency.
Possible Causes: Viruses, Trojans, third-party antivirus software, application anomalies, driver anomalies, or automatic updates in the backend of the software. All the factors above can cause high CPU usage, resulting in problems such as being unable to log in to the CVM or slow access.
Directions:

1. Log in to the instance via VNC log-in.
2. See Linux Instance: High CPU and Memory Usage Causes Log-in Failure and locate high-load processes in the System Monitor.

Remote port configuration error

Fault Phenomenon: Remote connection is unavailable, the remote access port is not the default port, has been modified, or port 22 is not open.
Diagnostic Method: Whether you can ping the public IP address of the instance and use the telnet command to check whether the port is open.
Directions: For specific operations, refer to Port Problem Leads to Failure of Remote Log-in.

Improper security group rules

Fault Phenomenon: After checking with the self-service checking tools, it was found that the security group rules were set incorrectly, resulting in log-in failure.
Directions: If it is determined that the problem is with the security group port settings, the feature One-click Release in the tool can be used to open the port.

If you need to customize security group rules, reconfigure the security group rules.

Other Solutions

If you still cannot connect to the Linux instance after the above troubleshooting, please save the self-diagnosis results and submit a ticket for feedback.

Unabling to Log in to the Linux Instance Via SSH

This document uses the CVM of the CentOS 7.5 operating system as an example to describe the troubleshooting and solutions for the problem of being unable to log in to a Linux instance via SSH.

Failure Symptoms

When using SSH to log in to a Linux instance, you receive a prompt indicating that you cannot connect or the connection fails.

Failure Location and Troubleshooting

Step one: Check the security group configuration

1. Log in to the CVM console.
2. On the instance management page, select the instance that needs to be troubleshooted and click More > Configure Security Group.
3. In the Configure Security Group window that pops up, click the configured (checked) security group ID.
   Go to the security group page bound to the instance.
4. On the inbound rules page of the security group rules, click One-click Release.
5. In the pop-up Prompt Box, click OK.
6. Use SSH to log in to the Linux instance again and check whether you can log in successfully.
   - Yes, the mission completed.
   - If no, perform the following step.

Step two: Check the sshd service port

1. Use VNC to log in to the Linux instance.

2. In the operating system page, perform the following command to check whether the port that the sshd service monitors is included.

   ```
   netstat -tnlp | grep sshd
   ```

   - If the following result is returned, it means that the sshd process is monitoring on port 22.

Submit a ticket for feedback.

```
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      1015/sshd
```

- If there is no output, the sshd service may not be started. Perform the following steps.

Step three: Check whether the sshd service is started

Perform the following command to check whether the sshd service is started.

```
systemctl status sshd.service
```

- If it has been started, submit a ticket for feedback.
- If it is not started, perform the following command to start the sshd service, and then use SSH to log in to the Linux instance again.

  ```
  systemctl start sshd
  ```

If your instance still cannot be connected after performing the above operations, we recommend that you submit a ticket for feedback.

Unabling to Log in Due to High CPU and Memory Usage of the Linux System

This document describes the troubleshooting methods and solutions for the Linux CVM that is unable to log in due to high CPU or memory usage.

Possible Reasons

High CPU or memory usage can easily lead to problems such as slow service response and server login failure. The reasons for high CPU or memory usage may be caused by factors including hardware factors, system processes, business processes, or Trojan viruses. You can use Cloud Monitor to create CPU or memory usage threshold alarms. When the CPU or memory usage exceeds the threshold, you will be notified immediately.

Positioning Tools

Top: A commonly used monitoring tool under the Linux system, used to obtain CPU or memory usage at the process level in real time. Take the output information of the top command in the following figure as an example.

```
top - 22:16:25 up  6:18,  1 user,  load average: 0.00, 0.01, 0.05
Tasks:  68 total,   1 running,  67 sleeping,   0 stopped,   0 zombie
%Cpu(s):  0.0 us,  0.3 sy,  0.0 ni, 99.7 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
KiB Mem :  1016516 total,   605016 free,    77224 used,   334276 buff/cache
KiB Swap:        0 total,        0 free,        0 used.   778708 avail Mem

  PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
  257 root      20   0       0      0      0 S   0.3   0.0   0:00.73 jbd2/vda1-8
  984 root      20   0  569592   5068   2568 S   0.3   0.5   0:16.51 YDService
 1253 root      20   0  534620  12288   2104 S   0.3   1.2   0:34.21 barad_agent
    1 root      20   0   43104   3512   2404 S   0.0   0.3   0:01.87 systemd
    2 root      20   0       0      0      0 S   0.0   0.0   0:00.00 kthreadd
    3 root      20   0       0      0      0 S   0.0   0.0   0:00.33 ksoftirqd/0
    4 root      20   0       0      0      0 S   0.0   0.0   0:00.00 kworker/0:0
    5 root       0 -20       0      0      0 S   0.0   0.0   0:00.00 kworker/0:0H
    7 root      rt   0       0      0      0 S   0.0   0.0   0:00.00 migration/0
    8 root      20   0       0      0      0 S   0.0   0.0   0:00.00 rcu_bh
    9 root      20   0       0      0      0 S   0.0   0.0   0:01.20 rcu_sched
   10 root      rt   0       0      0      0 S   0.0   0.0   0:00.05 watchdog/0
```

The output information of the top command is mainly divided into two parts. The upper part shows the overall usage of CPU and memory resources :

- The first line: Current system time, number of currently logged-in users, and system load.
- The second line: The total number of system processes, the number of running processes, dormant, sleeping, and zombie processes.
- The third line: Current CPU usage.
- The fourth line: Current memory usage.
- The fifth line: Current usage of the Swap space.
  The lower part shows the resource usage by process :
- PID: Process ID.
- USER: Process owner.
- PR: Process priority NI: NICE value. The smaller the NICE value, the higher the priority.
- VIRT: The size of virtual memory used, in KB.
- RES: The current memory size used, in KB.
- SHR: The size of the shared memory used, in KB.
- S: Process status.
- %CPU: The percentage of CPU time used by the process during the update interval.
- %MEM: The percentage of memory used by the process during the update interval.
- TIME+: The CPU time used by the process, accurate to 0.01s.
- COMMAND: Process name.

Troubleshooting

Logging in to the CVM

Choose different log-in methods to log in to the CVM according to actual needs.

- Remotely log in to the Linux CVM through third-party software. > Note: When the Linux CVM is under high CPU load status, you may be unable to log in.

- Use VNC to log in to the Linux instance. > Note: When the Linux CVM is under high CPU load status, the console can still be logged in normally.

Checking Process Usage

Perform the following command to check the system load and identify processes that consume more resources based on the %CPU column and the %MEM column.

```
top
```

Analyzing Process

Analyze and troubleshoot problems based on the processes in the task manager and take corresponding solutions.

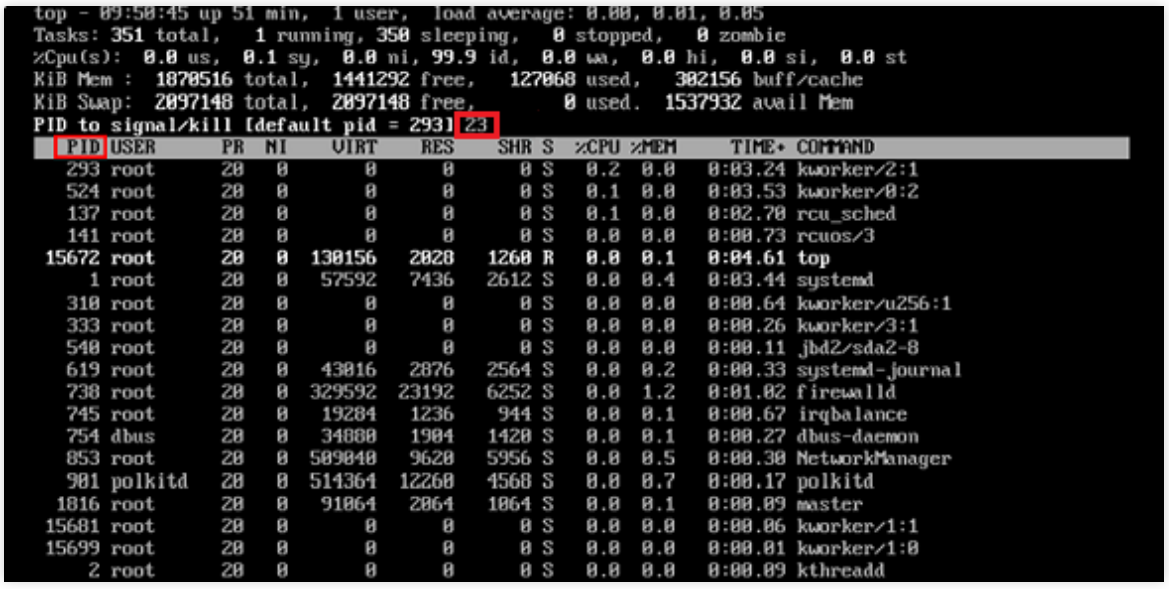
- If the business process occupies a large amount of CPU or memory resources, it is recommended to analyze whether the business process has room for optimization and optimize it or upgrade the server configuration.
- If an abnormal process occupies a large amount of CPU or memory resources, the instance may be infected. You can terminate the process yourself or use security software to kill it. If necessary, consider backing up data and reinstalling the system.
- If the component process occupies a large amount of CPU or memory resources, submit a ticket and contact us for further location processing.
  Common components are:
- sap00x: Security component process.
- Barad_agent: Monitoring component process.
- secu-tcs-agent: Security component process.

Terminating Process

1. According to the analyzed resource-occupying processes, record the process PIDs that need to be terminated.

2. Enter k .

3. Enter the PID of the process to be terminated and press Enter. As shown below:
   Here, taking terminating the process with PID 23 as an example.



> Note: If kill PID 23 with signal [15]: appears after pressing Enter, simply press Enter again to

> keep the default setting.

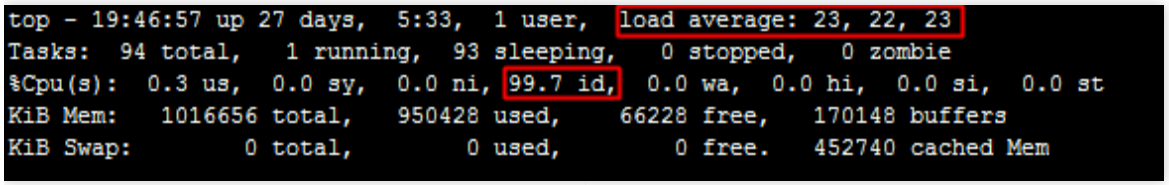
4. After the operation is successful, the page will display the Send pid 23 signal [15/sigterm] prompt message, and press Enter to confirm.

Other Related Failures

Handling Scenarios of Idle CPU With High Load

Problem Description

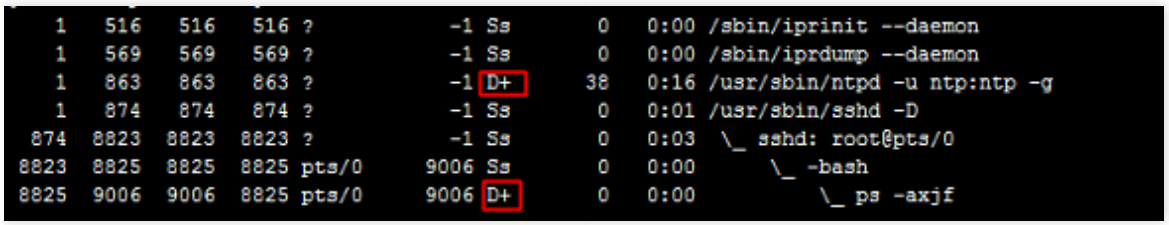
Load average is an evaluation of the CPU load. The higher the value, the longer the task queue is and the more tasks are waiting to be performed.
Observe through top, similar to the following figure, the CPU is idle, but the load average is very high.



Solution

Perform the following command to check the process status and check whether there is a process in D status. As shown below:

```
ps -axjf
```



> Note:
> If there are many D-status processes, you can solve the problem by restoring the resources that the process depends on or restarting the system.

Handling Kswapd0 Process Which Occupies High CPU

Problem Description

While the Linux system manages memory through the paging mechanism, it also allocates part of the disk as virtual memory. While kswapd0 is the process responsible for paging in the Linux system virtual memory management. When the system is low on memory, kswapd0 will frequently perform paging operations. Paging operations consume a lot of CPU resources, causing the process to continue to occupy high CPU resources.

Solution

1. Perform the following command to find the kswapd0 process.

   ```
   top
   ```

2. Observe the status of the kswapd0 process.
   If the system is in a non-sleep status for a long time and occupies a high CPU resource, perform step 3 to check the memory usage.

3. Perform vmstat , free , ps and other instructions to query the memory usage of processes in the system.
   Depending on the memory usage, reboot the system or terminate unnecessary and safe processes. If the values of si and so are also relatively high, it represents that the system has frequent paging operations and the current system's physical memory can no longer meet your needs. Consider upgrading the system memory.

The Server Is Isolated and Cannot Be Logged In

This document introduces the solution to the problem of being unable to log in to the CVM due to public network isolation.

Failure Symptoms

A CVM may be isolated because it violates current laws and regulations. You can check whether the server is isolated in the following ways.

- When the public network access of the CVM is isolated, you will be notified of the non-compliance and isolation through in-console message center or SMS.
- In the CVM console, the Monitoring/Status column displays the CVM status: In Isolation.

Causes of Problem

When a CVM has a non-compliance or risk event, the non-compliant server undergoes partial isolation (except for the ports 22, 36000, and 3389 of the private network, all other network accesses are isolated, and developers can log in to the server through a jump server).

Solution

1. Follow the instructions in the message center or SMS to address the non-compliant content. Address the security risks and, if necessary, reinstall the operating system.
2. If the violation was not caused by your personal actions, it is likely that your server has been maliciously compromised. For solutions, see Cloud Workload Protection.
3. After you eliminate the security risks or stop the violation, contact customer service by submitting a ticket to lift the isolation.

High Bandwidth Usage Prevents Log-in

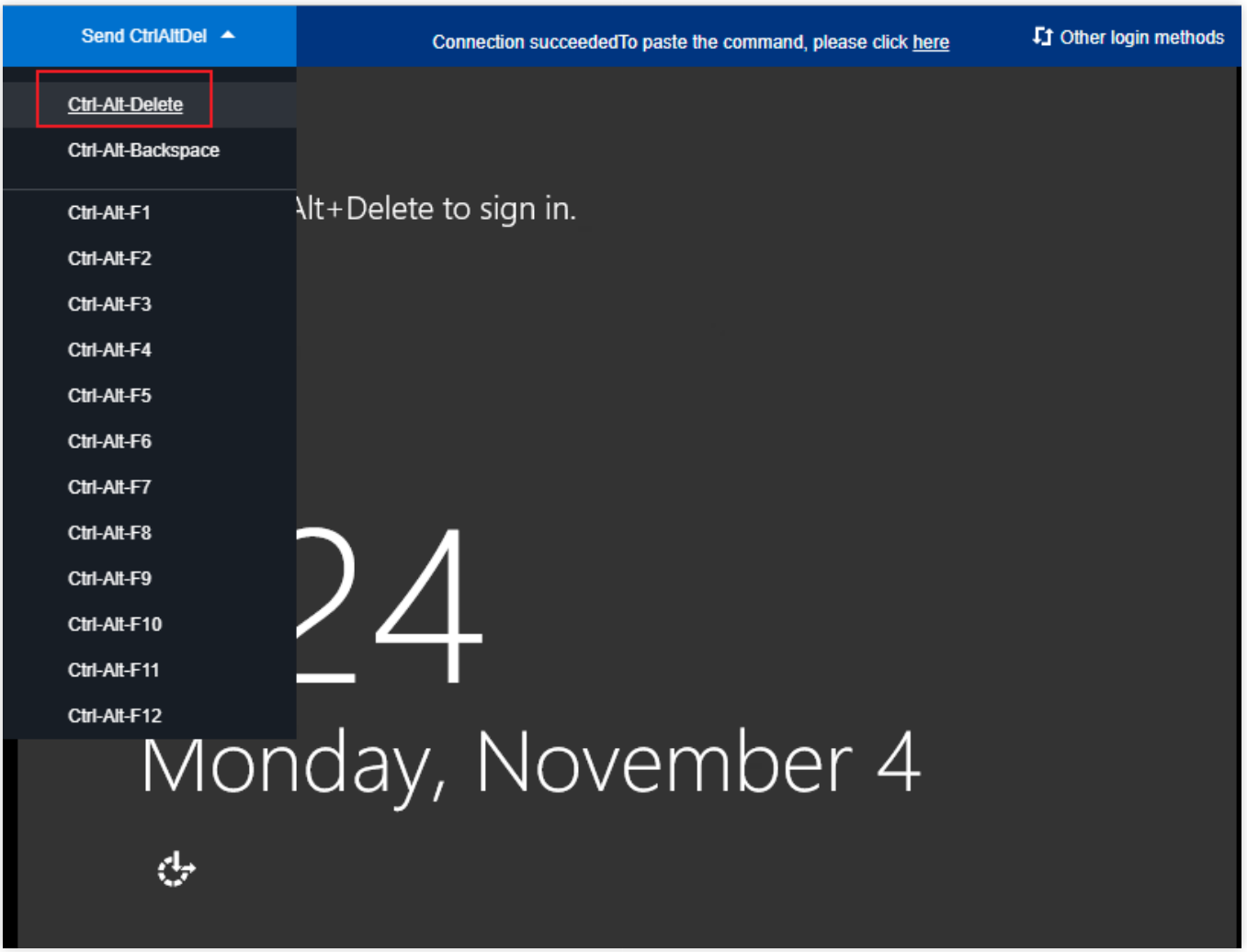
This document introduces the troubleshooting methods and solutions for Linux and Windows CVM when they cannot be remotely connected due to high bandwidth usage.

Failure Symptoms

- After the CVM console log-in, the bandwidth monitoring data of the CVM prompts that excessively high bandwidth usage is preventing connection to the Converge Cloud server.

Failure Location and Troubleshooting

1. Log in to the CVM console.
2. Select Cloud Virtual Machine to be checked and click Log-in.
3. In the pop-up Log in to Windows/Linux Instance window, select Other methods (VNC) and click Log in now to log in to the CVM.
4. In the log-in window that pops up, select Send Remote Command in the upper left corner and click Ctrl-Alt-Delete to enter the system log-in interface. As shown below:

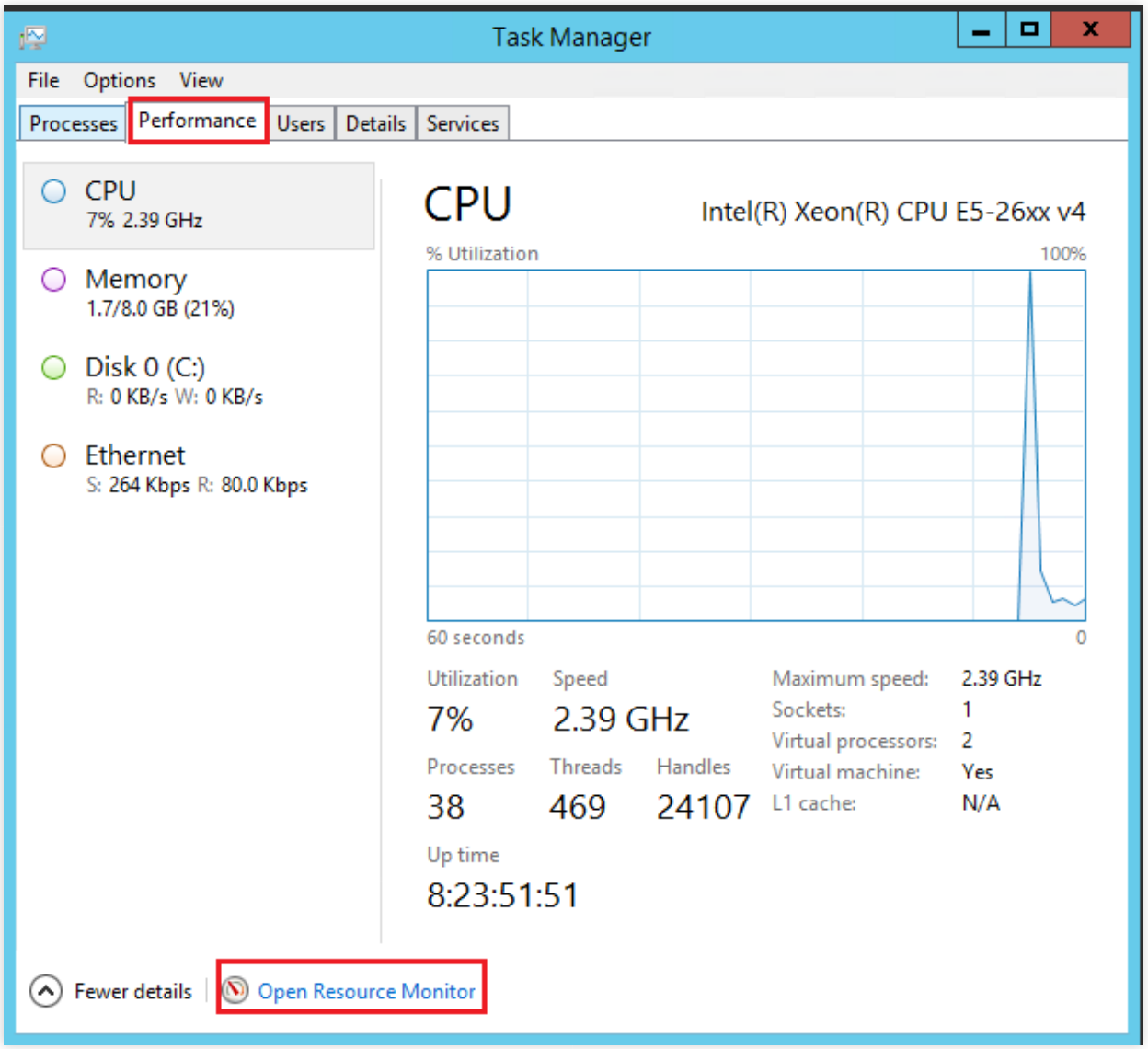


For Windows Servers

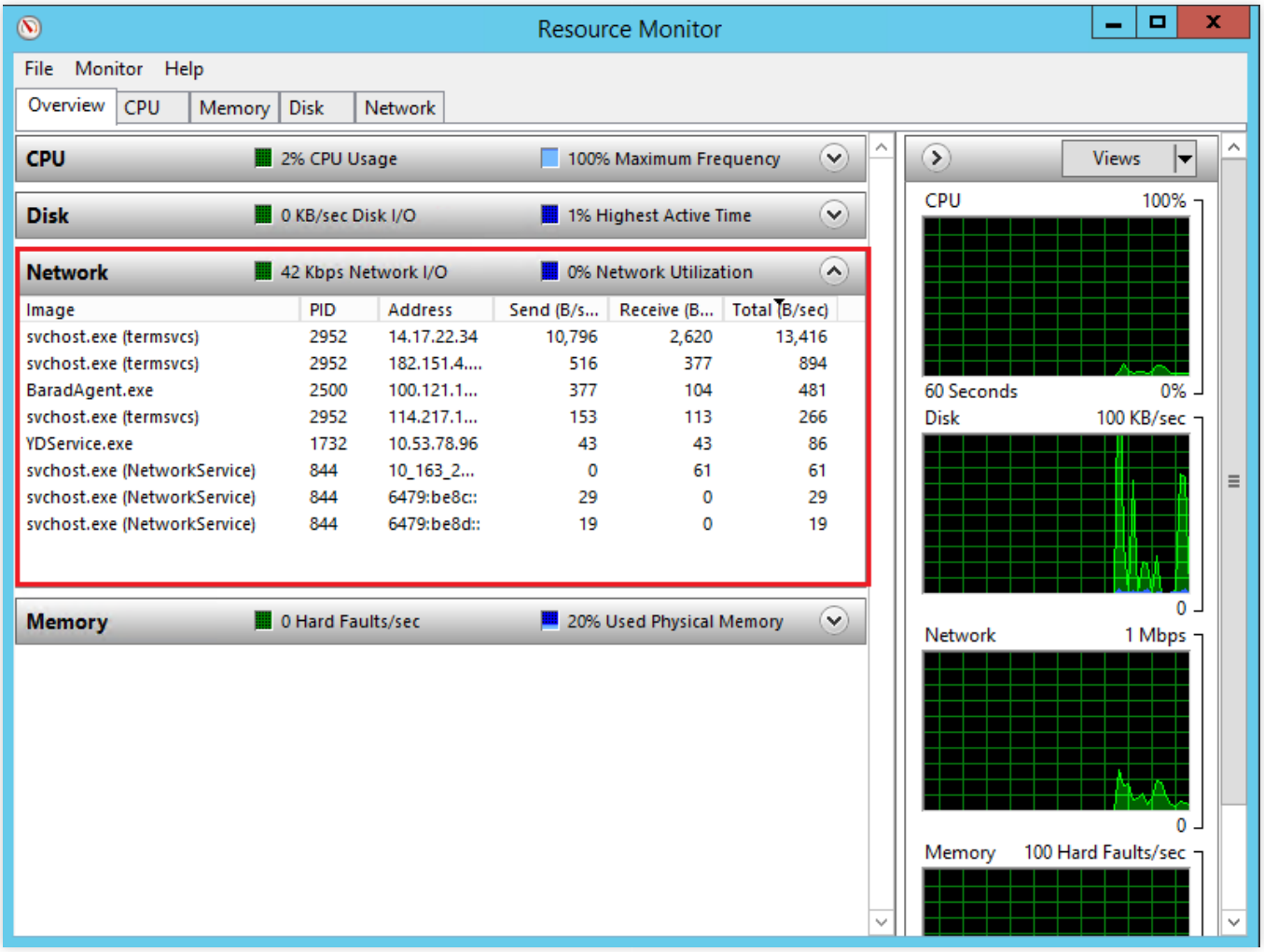
After you log in to the Windows CVM via VNC, you need to do the following:

> Note: The following operations take a Windows Server 2012 system CVM as an example.

1. In CVM, click and select Task Manager to open the Task Manager window.
2. Select the Performance tab and click Open Resource Monitor. As shown below:



3. In the opened Resource Monitor, check the process that consumes more bandwidth and determine whether this process is operating normally based on your actual business. As shown below:



- If a business process is consuming more bandwidth, you need to analyze whether this increase is caused by changes in access volume and whether space optimization or server configuration upgrades are required.

- If an exception process consumes more bandwidth, this increase may be caused by a virus or Trojan horse. You can terminate the process manually or use security software to detect and kill it. You can also back up the data and reinstall the system.

  > Note: Many virus programs in Windows systems disguise themselves as system processes. You can make a preliminary identification with process information in Task Manager > Processes: Ordinary system processes come with complete signatures and descriptions, and they are mostly located in the C:\Windows\System32 directory. The name of a virus program may be the same as the system process, but it lacks signatures and descriptions, and its position may unusual.

- If the process that consumes more bandwidth is the Converge Cloud component process, submit a ticket and contact us for further localization.

For Linux Servers

After you log in to the Linux CVM via VNC, you need to do the following:

> Note: The following operations take the CVM running CentOS 7.6 as an example.

1. Run the following command to install the iftop tool (the iftop tool is a utility for monitoring traffic on Linux servers).

   yum install iftop -y

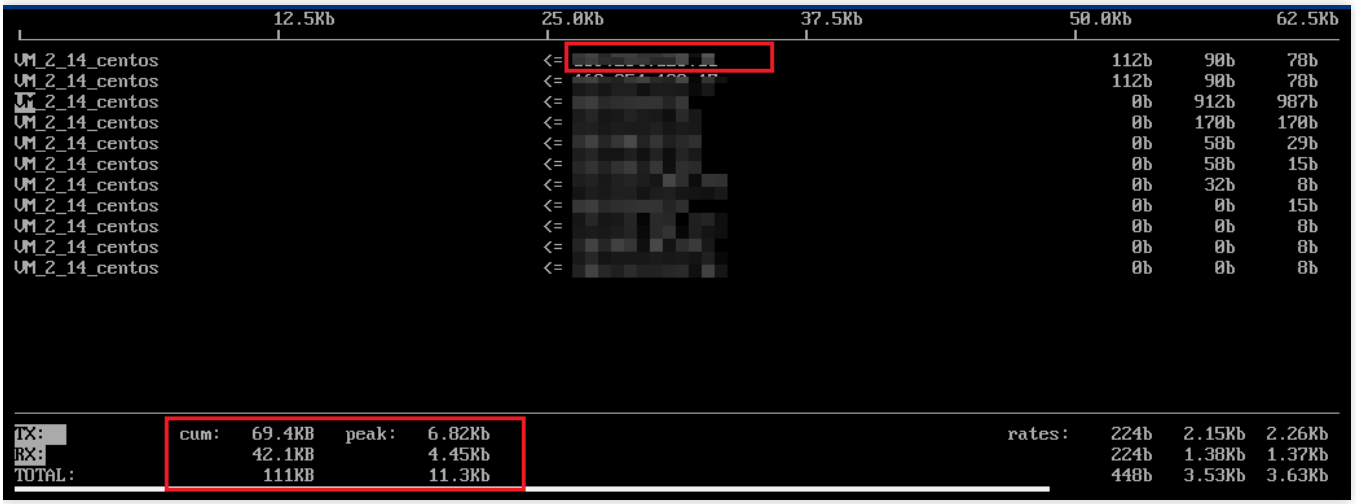
   Note: For Ubuntu system, please run apt-get install iftop -y command.

2. Run the following command to install lsof.

   yum install lsof -y

3. Run the following command to run iftop. As shown below:

   iftop



- <= , => indicates the direction of traffic.
- TX means sending traffic.
- RX means receiving traffic.
- TOTAL indicates total traffic.
- Cum indicates the total traffic since iftop was run up to now.
- peak indicates the peak flow rate.
- rates represents the average traffic rate over the past 2s, 10s, and 40s.

4. According to the IP consuming traffic in iftop, execute the following command to track the process connected to the IP.

```
lsof -i | grep IP
```

For example, if the IP consuming traffic is 201.205.141.123, execute the following command:

```
lsof -i | grep 201.205.141.123
```

According to the following returned results, we know that the bandwidth of this server is mainly consumed by the SSH process.

```
sshd      12145    root    3u  IPV4  3294018      0t0   TCP 10.144.90.86:ssh->203.205.141.123:58614(ESTABLIS
HED)
sshd      12179  ubuntu    3u  IPV4  3294018      0t0   TCP 10.144.90.86:ssh->203.205.141.123:58614(ESTABLI
SHED)
```

5. Check the process that consumes more bandwidth to evaluate whether the process is normal.
   - If a business process is consuming more bandwidth, you need to analyze whether this increase is caused by changes in access volume and whether space optimization or server configuration upgrades are required.
   - If an exception process consumes more bandwidth, this increase may be caused by a virus or Trojan horse. You can terminate the process manually or use security software to detect and kill it. You can also back up the data and reinstall the system.
   - If the process that consumes more bandwidth is the Converge Cloud component process, submit a ticket and contact us for further localization.

Failing to Shut Down or Restart CVM

When shutting down or restarting a CVM, there is a very small chance that the shutdown or restart will fail. If you encounter such a situation, you can troubleshoot and handle the CVM as follows.

Possible Reasons

- CPU or memory usage is too high.
- The CVM of the Linux operating system does not have an ACPI hypervisor installed.
- The CVM with the Windows operating system takes too long to perform system updates.
- The CVM does complete initialization when you first purchase the Windows CVM.
- The operating system has certain software installed or itself may be damaged after being infected by a Trojan virus.

Troubleshooting

Checking CPU/Memory Usage

1. Check CPU/memory usage based on the type of CVM operating system.
    - Windows CVM: In the CVM, right-click the Taskbar and select Task Manager.
    - Linux CVM: Perform the `top` command to check the information in the `%CPU` column and the `%MEM` column.
2. Terminate processes with high CPU or memory usage based on actual CPU/memory usage.
   If it still cannot shut down/restart, perform a force shutdown/restart function.

Checking Whether the ACPI Management Program Is Installed

> Note: This operation is for the CVM of the Linux operating system.

Perform the following command to check whether the ACPI process exists.

```
ps -ef | grep -w "acpid" | grep -v "grep"
```

- If an ACPI process exists, perform a force shutdown/restart function.
- If the ACPI process does not exist, install the ACPI management program. See Linux power management configuration for specific operations.

Checking Whether WindowsUpdate Is Running

> Note: This operation is for the CVM of the Windows operating system.

On the Windows CVM operating system page, click Start > Control Panel > Windows Update to check whether any patches or programs are being updated.

- When Windows is performing certain patch operations, it will do some processing when shutting down the system. At this time, the update time may be too long, resulting in shutdown/restart failure. It is recommended that you wait until the update of Windows is complete before attempting to shut down/restart the CVM.
- If no patches or programs are being updated, perform the force shutdown/restart function.

Checking Whether The CVM Has Completed Initialization

> Note: This operation is for the CVM of the Windows operating system.

When you first purchase the Windows CVM, the system distributes images through Sysprep, and the initialization process takes a little longer. Before initialization is completed, Windows will ignore the shutdown/restart operation, resulting in shutdown/restart failure.

- If the Windows CVM you purchased is initializing, it is recommended that you wait until the initialization is complete before attempting to shut down/restart the CVM.
- If the CVM has completed initialization, perform the force shutdown/restart function.

Checking Whether the Installed Software Is Normal

Use inspection tools or antivirus software to check whether the software installed in the CVM is normal or infected with Trojans, viruses, etc.

- If any exception is found, it indicates that the system itself may be damaged, resulting in shutdown/restart failure. It is recommended that you uninstall the software, use security software to kill it or back up your data, and then reinstall the system.
- If no exception is found, perform the force shutdown/restart function.

Force Shutdown/Restart Function

> Note: Converge Cloud provides the force shutdown/restart function, which can be used when multiple attempts to shut down/restart the CVM fail. This operation will forcibly perform the shutdown/restart on the CVM, which may lead to data loss or file system corruption of the CVM.

1. Log in to the CVM Console.
2. On the instance management page, select the CVM to be shut down or restarted, and perform different operations based on actual needs.
    - Shut down the CVM: Click More > CVM Host Status > Shutdown.
    - Restart the CVM: Click More > CVM Host Status > Restart.
3. In the Shutdown or Restart Instance window that pops up, select Force Shutdown or Force Restart

and click OK.

- Select Force Shutdown.
- Select Force Restart.

Unable to Create Network Namespace

Problem Description

When performing a command to create a new Network Namespace, the command gets stuck and cannot continue. Dmesg message prompt: "unregister_netdevice: waiting for lo to become free. Usage count = 1"

Causes

This problem is a kernel bug. Currently, the following kernel versions have this bug:

- Ubuntu 16.04 x86_64 kernel version is 4.4.0--91-generic.
- Ubuntu 16.04 x86_32 kernel version is 4.4.0--92-generic.

Solution

Upgrade the kernel version to 4.4.0--98-generic, which has fixed this bug.

Processing Procedures

1. Perform the following command to check the current kernel version.

   ```
   uname -r
   ```

2. Perform the following command to check whether the 4.4.0--98-generic kernel version is available for upgrade.

   ```
   sudo apt-get update
   sudo apt-cache search linux-image-4.4.0--98-generic
   ```

   If the following information is displayed, it represents that the version exists in the source and can be upgraded:

linux-image-4.4.0--98-generic - Linux kernel image for version 4.4.0 on 64 bit x86 SMP

3. Perform the following command to install the new version of the kernel and the corresponding Header package.

   sudo apt-get install linux-image-4.4.0--98-generic linux-headers-4.4.0--98-generic

4. Perform the following command to restart the system.

   sudo reboot

5. Perform the following command to enter the system and check the kernel version.

   uname -r

   If the following result is displayed, it represents the version update is successful:

   4.4.0--98-generic

Kernel and IO Related Problems

Kernel Problem Location and Solution

Failure Symptoms

Kernel-related failures may cause the machine to be unable to log in or abnormal restart.

Possible Reasons

Kernel hung_task

The hung task mechanism is implemented by the kernel thread khungtaskd, which monitors the process in the TASK_UNINTERRUPTIBLE status. If in the period of kernel.hung_task_timeout_secs (Default 120 seconds), it remains in D status, then the stack information of the hung task process will be printed.

If configure kernel.hung_task_panic=1 , it will trigger a kernel panic and restart the machine.

Kernel soft lockup

Soft lockup means that the CPU is occupied by kernel code and cannot perform other processes. The principle of detecting soft lockup is to assign a kernel thread [watchdog/x] which will be timed perform to each CPU. If the thread is within a certain period (the default is 2*kernel.watchdog_thresh , 3.10 kernel kernel.watchdog_thresh and the default value is 10 seconds) is not performed, indicating that a soft lockup has occurred.

If kernel.softlockup_panic=1 is configured, it will trigger a kernel panic and restart the machine.

Kernel panic

The kernel's abnormal crash causes the machine to restart abnormally. Common kernel panic scenarios are as follows:

- The kernel has a hung_task and kernel.hung_task_panic=1 is configured.
- The kernel has a soft lockup and kernel.softlockup_panic=1 is configured.
- The kernel bug is triggered.

Processing Procedures

The troubleshooting and processing steps for kernel-related problems are relatively complicated. It is recommended to submit a ticket for further location and processing.

Hard Disk Problem Location and Solution

Hard disk inode is full

Failure phenomenon : When creating a new file, the error message No space left on device is prompted,

and the inode space usage is 100% by using the df -i command.
Possible causes : File system inode exhaustion.
Processing steps : Delete unnecessary files or scale out the hard disk capacity.

Hard disk space usage is full

Failure phenomenon : When creating a new file, the error message No space left on device is prompted, and the hard disk space usage is 100% by using the df -h command.
Possible causes : Hard disk space exhaustion.
Processing steps : Delete unnecessary files or scale out the hard disk capacity.

Hard disk read only

Failure phenomenon: The file system can only read files but cannot create new files.
Possible cause: The file system is damaged.
Processing steps:

1. Create a snapshot to back up disk data. See Create a Snapshot for details.
2. Perform the corresponding processing steps according to the hard disk type:
   System disk
   It is recommended to restart the instance directly.
   Data disk
   i. Perform the following command and check the file system type corresponding to the read-only disk.
   lsblk -f
   ii. Perform the following command to uninstall the data disk.
   umount
   iii. Corresponding to the file system type, perform the following command to repair:
   - For ext3/ext4 file system, perform the following command:
     fsck -y /dev/corresponding disk
   - For xfs file system, perform the following command:
     xfs_repair /dev/corresponding disk

Hard disk %util high

Failure phenomenon : The instance is stuck, and logging in using SSH or VNC is slow or unresponsive.
Possible causes : High IO causes hard disk %util to reach 100%.
Processing steps : Check whether the high IO is reasonable, and evaluate whether to reduce IO read and write or replace the hard disk with a higher performance.

Network-related Failures
Unabling to Access Website

This document describes how to troubleshoot and locate the problem of website inaccessibility.

Possible Reasons

The website cannot be accessed due to network problems, firewall settings, excessive server load, etc.

Troubleshooting

Troubleshoot Server-related Problems

The website cannot be accessed due to server shutdown, hardware failure, or high CPU/memory/bandwidth usage, so it is recommended that you check the server's operating status and CPU/memory/bandwidth usage in turn.

1. Log in to the CVM console and check whether the instance is running normally on the instance management page.
    - Yes, perform step 2.
    - No, restart the CVM instance.

2. Click the instance ID/hostname to go to the instance details page.

3. Select the Monitor tab to check CPU/memory/bandwidth usage.
    - If there are high CPU/memory usage problems, see Windows Instance: Unable to Log in Due to High CPU and Memory Usage and Linux Instance: Unable to Log in Due to High CPU and Memory Usage for troubleshooting.
    - If the bandwidth usage is too high, see Unable to Log in Due to High Bandwidth Usage for troubleshooting.
    - If the CPU/memory/bandwidth usage is normal, perform step 4.

4. Perform the following command to check whether the corresponding port of the web service is being monitored normally. > Note: The following operations use port 80, which is commonly used by HTTP services, as an example.
    - Linux instance: Perform the netstat -ntulp |grep 80 command. As shown below:

```
[root@VM_2_184_centos ~]# netstat -ntulp |grep 80
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      1309/httpd
```

- Windows instance: Open the CMD command line Interface and perform the netstat -ano|findstr :80 command. As shown below:

```
C:\Users\Administrator>netstat -ano|findstr :80
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING       4
  TCP    10.135.182.70:53406    10.225.30.181:80       TIME_WAIT       0
  TCP    10.135.182.70:53419    10.225.30.181:80       TIME_WAIT       0
  TCP    10.135.182.70:53423    10.225.30.181:80       TIME_WAIT       0
  TCP    [::]:80                [::]:0                 LISTENING       4
```

- If the port is monitored normally, perform step 5.
- If the port is not monitored normally, check whether the Web service process is started or configured normally.

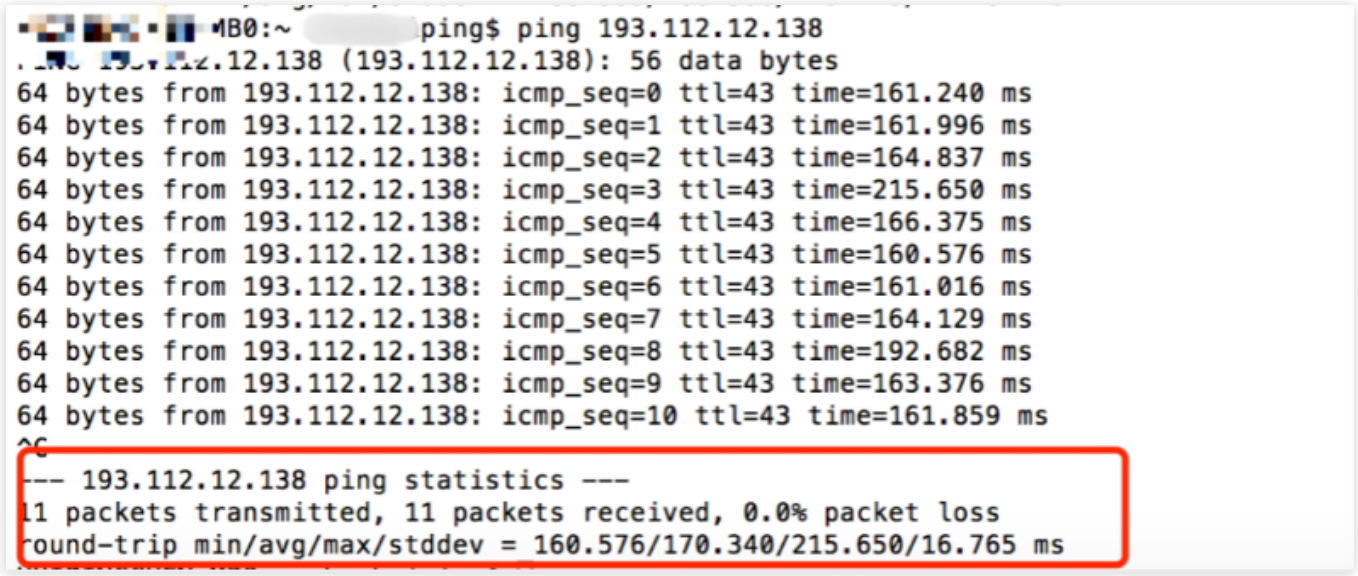
5. Check the firewall settings to see whether the port corresponding to the Web service process is open.
    - Linux instance: Perform the iptables -vnL command to check whether iptables opens port 80.
    - If port 80 is opened, troubleshoot network-related problems.
    - If port 80 is not opened, perform the iptables -I INPUT 5 -p tcp --dport 80 -j ACCEPT command to open port 80.
    - Windows instance: On the operating system page, click Start > Control Panel > Firewall Settings to check whether the Windows firewall is turned off.
        - Yes, troubleshoot for network related problems.
        - No, turn off the firewall settings.

Troubleshooting Network-related Problems

Network-related problems may also cause the website to be inaccessible. You can perform the following command to check whether there is packet loss or high latency on the network.

Ping the public IP of the destination server

- If the following result is returned, it represents packet loss or high latency. Use MTR to perform further investigation. See CVM Network Delay and Packet Loss for specific operations.



- If there is no packet loss or high latency, troubleshoot problems related to security group settings.

Troubleshooting Problems Related to Security Group Settings

A security group is a virtual firewall that controls inbound and outbound traffic for associated instances. The rules of a security group can specify protocols, ports, policies, etc. If you do not open the ports related to the Web process, the website will be inaccessible.

1. Log in to the CVM console and click the ID/hostname of the instance on the Instance List page to enter the instance details page.
2. Select the Security Group tab, check the bound security group and the outbound and inbound rules of the corresponding security group, and confirm whether to open ports related to the Web process. As shown below:
    - Yes, check the domain name, registration, and resolution-related problems.
    - No, modify the security group settings and open the ports related to the Web process.

Troubleshooting Domain Name Registration and Resolution-related Problems

After troubleshooting server-related, network-related, and security group setting-related problems, you can try to access the cloud server using its public IP address. If the website can be accessed using the IP address but fails to be accessed using the domain name, it may be that the website is inaccessible due to problems related to domain name registration or resolution.

1. The Ministry of Industry and Information Technology stipulates that websites that have not obtained a license or have not completed registration procedures are not allowed to engage in Internet information services, otherwise, it will be an illegal act. In order not to affect the normal operation of the website in the long term, if you need to open a website, it is recommended that you first register the website, and only enable access after the registration is successful and the ICP registration number issued by the Communications Administration is obtained.
    - If you are using our domain name service, you can log in to the domain name management console

to check the corresponding domain name status.

- If your domain name has been registered and the website inaccessibility problem still cannot be resolved, submit a ticket.

High Website Latency

Problem Description

High website latency.

Issue Analysis

A HTTP request includes domain name resolution, establishing a TCP connection, initiating a request, server receiving, processing the request and returning the processing result, browser parsing the HTML code and requesting other resources, and rendering the page. This HTTP request process starts at the user's local client, traverses the network nodes between the client and the access server, and ultimately reaches the server. Any problem in the three links may cause high website latency.

Solution

Checking the Local Client

1. Test the speed of local access to each domain name.
2. Based on the test results, check whether there is any issue with the local network.
   We can learn from the results both the access delay of every domain name and whether the network is functioning normally.
   - If not normal, contact your network service provider for assistance in locating and resolving any issues.
   - If normal, check network links.

Checking Network Links

1. Use the local client to ping the server's public IP address to check whether there is packet loss or high latency.
   - If there is packet loss or high latency, use MTR for diagnosis. For specific operations, see Server Network Delay and Packet Loss Processing.
   - If there is no packet loss or high latency, go to step 2.
2. Run dig/nslookup command to check the DNS resolution and make sure whether the issue is caused by DNS resolution.
   You can also directly access the corresponding page using the public IP to check whether the high website latency is due to DNS issues.

- If yes, check DNS resolution.
- If no, check the server.

Checking the Server

1. Log in to the CVM console.
2. Select the ID/host name of the instance to be checked and enter the instance details page.
3. On the instance details page, select the Monitoring tab to check the usage of instance resources.
   - If there are high CPU/memory usage problems, see Windows Instance: Unable to Log in Due to High CPU and Memory Usage and Linux Instance: Unable to Log in Due to High CPU and Memory Usage for troubleshooting.
   - If the bandwidth usage is too high, see Unable to Log in Due to High Bandwidth Usage for troubleshooting.
   - If instance resource usage is normal, check for other potential issues.

Checking for Other Potential Issues

Based on the instance resource usage, the administrator should determine whether the increase in resource consumption is caused by server load.

- If yes, it is recommended to optimize business procedures or upgrade server configuration. You can also purchase new servers to reduce the pressure on existing servers.
- If no, we recommend that you check the log files to locating the issues, and perform targeted optimization.

CVM Network Delay and Packet Loss

Problem Description

When accessing the CVM locally or accessing other network resources on the CVM, network lag is detected. Use ping command, and find that the network has packet loss or high latency.

Issue Analysis

Packet loss or high latency may be caused by backbone link congestion, link node failure, high server load, system setting problems, etc. After excluding the possible causes from the cloud server itself, you can use MTR for further diagnosis.
MTR is a network diagnostic tool that generates reports that can help you confirm the root cause of network problems.

Solution

> Note:
> This document uses Linux and Windows CVMs as examples to introduce how to use MTR and how to analyze MTR report results.

Refer to the introduction and usage of MTR according to the different host operating systems running MTR.

- WinMTR Introduction and Usage (Windows Operating System)
- MTR Introduction and Usage (Linux Operating System)

WinMTR Introduction and Usage (Windows operating system)

WinMTR: A free network diagnostic tool for Windows systems that integrates Ping and tracert functions and has a graphical page that allows you to intuitively view the response time and packet loss of each node.

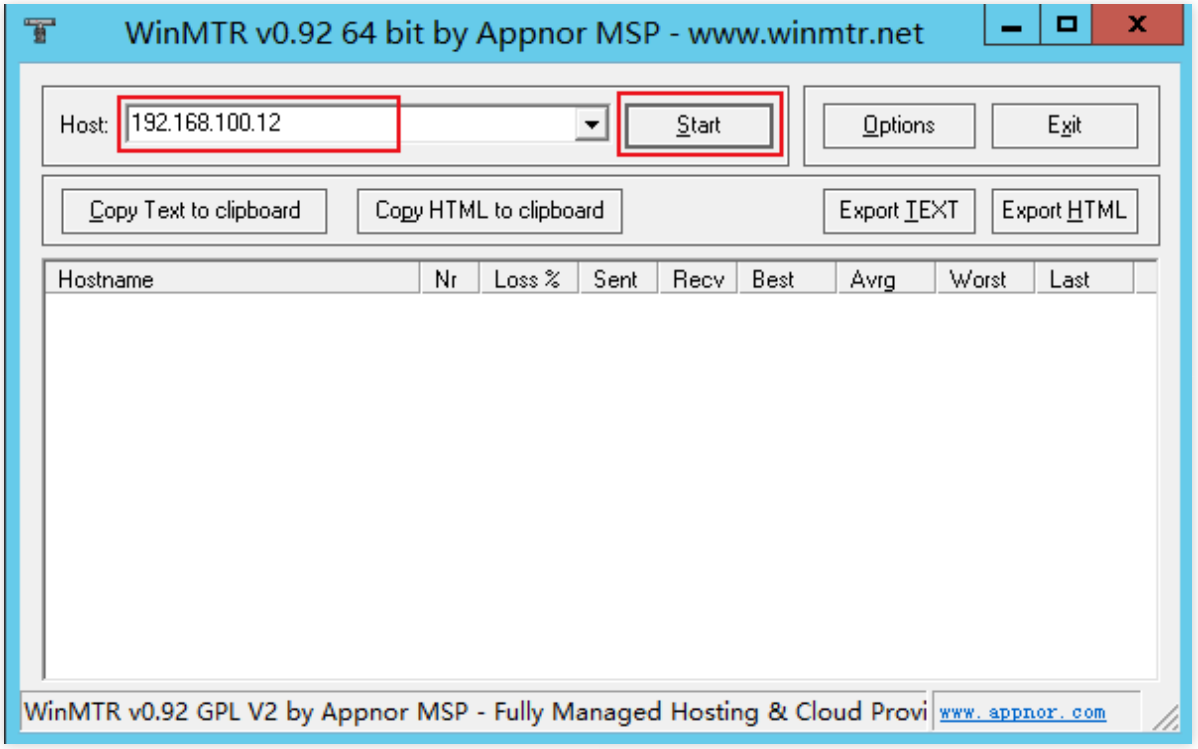
Installing WinMTR

1. Log in to the Windows CVM.
2. On the operating system page, use a browser to access the official website (or legal channels) to download the WinMTR installation package for the corresponding operating system type.

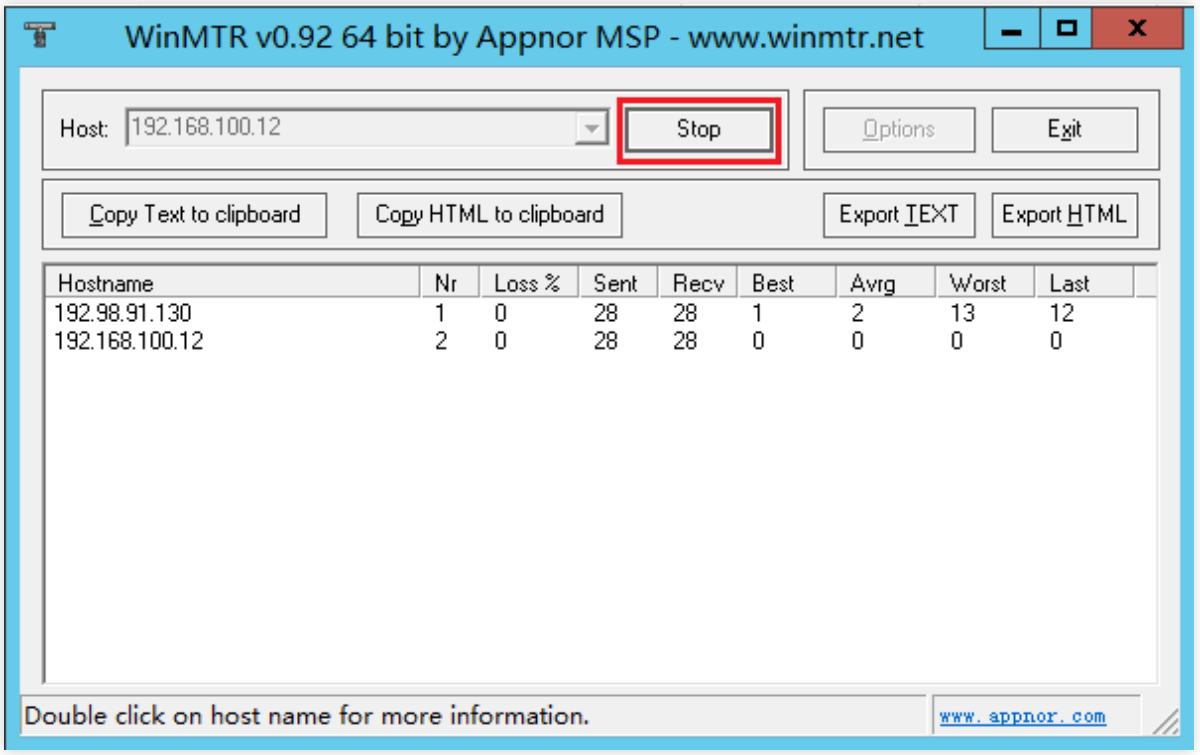
3. Unzip the WinMTR installation package.

Using WinMTR

1. Double-click WinMTR.exe to open the WinMTR tool.
2. In the Host field of the WinMTR window, enter the destination server IP or domain name and click Start. As shown below:



3. Depending on the actual situation, wait for WinMTR to run for a while, and click Stop to end the test. As shown below:



4. The main information of the test results is as follows:
    - Hostname: Each host IP or name to pass through to reach the destination server.
    - Nr : The number of nodes passed.
    - Loss% : The packet loss rate of the corresponding node.
    - Sent : The number of data packets sent.
    - Recv : The number of responses received.
    - Best : The shortest response time.
    - Avrg: The average response time.
    - Worst : The longest response time.
    - Last : The most recent response time.

Introduction and Usage of MTR (Linux Operating System)

MTR : A tool for diagnosing network status on the Linux platform, which inherits the functions of Ping, traceroute, and nslookup, and uses ICMP packets by default to test the network connection between two nodes.

Installing MTR

Currently, all existing Linux distributions have MTR pre-installed. If your Linux CVM does not have MTR installed, you can perform the following command to install it:

- CentOS operating system:

```
yum install mtr
```

CVM Network Access Packet Loss

This document mainly introduces the main reasons that may cause CVM network access packet loss, as well as the corresponding troubleshooting and solutions.

Possible Reasons

The possible reasons for the CVM network access packet loss problem are as follows:
Triggering the speed limit causes TCP packet loss
Triggering the speed limit causes UDP packet loss
Triggering soft interrupt causes packet loss
UDP send buffer is full
UDP receive buffer is full
TCP full connection queue is full
TCP request overflow
The number of connections has reached the upper limit
iptables policy sets relevant rules

Prerequisites

You need to log in to the instance before locating and troubleshooting the problem. See Logging in to the Linux instance and Logging in to the Windows instance for details.

Troubleshooting

Triggering the speed limit causes TCP packet loss

CVM instances are available in various specifications, and different specifications have different network performance. When the bandwidth or packet volume of an instance exceeds the standard corresponding to the instance specification, the speed limit on the platform side will be triggered, resulting in packet loss. The troubleshooting and processing steps are as follows:

1. Check the bandwidth and package size of the instance.
   For Linux instances, you can perform the sar -n DEV 2 command to check the bandwidth and packet volume. Among them, the metrics rxpck/s and txpck/s are the number of the sending and receiving packets, and the indicators rxkB/s and txkB/s are the sending and receiving bandwidth.
2. Use the obtained bandwidth and package data to compare instance specifications to check whether

the instance specification performance bottleneck has been reached.

- Yes, you need to upgrade the instance specifications or adjust the business volume.
- No, if the performance bottleneck of the instance specification has not been reached, further location processing can be performed.

Triggering the speed limit causes UDP packet loss

See the step Triggering the speed limit causes TCP packet loss to determine whether the packet loss is caused by the performance bottleneck of the instance specification.

- Yes, you need to upgrade the instance specifications or adjust the business volume.
- If the performance bottleneck of the instance specification is not reached, it may be caused by the platform's additional frequency limit on DNS requests. When the overall bandwidth or packet volume of the instance reaches the performance bottleneck of the instance specifications, the DNS request speed limit may be triggered and UDP packet loss may occur. It can be further located and processed.

Triggering soft interrupt causes packet loss

When the operating system detects that the count value in the second column of /proc/net/softnet_stat is increasing, it will be judged as soft interrupt packet loss. When your instance triggers soft interrupt packet loss, you can troubleshoot and handle it by following the steps below: Check whether RPS is enabled:

- If so, a small value of the kernel parameter net.core.netdev_max_backlog will cause packet loss and needs to be increased.
- If not, check whether the CPU single-core soft interrupt is high, resulting in failure to send and receive data in time. If so, you can:
  - Enable RPS to make the soft interrupt distribution more balanced.
  - Check whether the business program causes uneven distribution of soft interrupts.

UDP send buffer is full

If your instance has packet loss due to insufficient UDP buffer, you can troubleshoot by following these steps:

1. Use the ss -nump command to check whether the UDP send buffer is full.
2. If so, increase the kernel parameters net.core.wmem_max and net.core.wmem_default, and restart the UDP program for the changes to take effect.
3. If the packet loss problem still exists, you can use the ss -nump command to check whether the send buffer has not increased as expected. At this time, you need to check whether the business code has set SO_SNDBUF through setsockopt. If so, modify the code to increase SO_SNDBUF.

UDP receive buffer is full

If your instance has packet loss due to insufficient UDP buffer, you can handle it by following these steps:

1. Use the ss -nump command to check whether the UDP receive buffer is full.
2. If so, increase the kernel parameters net.core.rmem_max and net.core.rmem_default, and restart the UDP program for the changes to take effect.
3. If the packet loss problem still exists, you can use the ss -nump command to check whether the receive buffer has not increased as expected. At this time, you need to check whether the business code has set SO_RCVBUF through setsockopt. If so, modify the code to increase SO_RCVBUF.

TCP full connection queue is full

The length of the TCP full connection queue is the smaller value of net.core.somaxconn and the backlog parameter passed in when the business process calls listen. If your instance has packet loss due to the full TCP connection queue, you can handle it by following these steps:
Increase the kernel parameter net.core.somaxconn.
Check whether the backlog parameter is passed into the business process. If so, increase it accordingly.

TCP request overflow

When TCP receives data, if the socket is locked by the user, the data will be sent to the backlog queue. If this process fails, it will cause TCP request overflow and packet loss. Under normal conditions, assuming that the business program performance is normal, you can see the following methods to troubleshoot and solve the problem from the system level:
Check whether the business program has set the buffer size by itself through setsockopt:

- If it has been set and the value is not large enough, you can modify the business program to specify a larger value, or stop specifying the size through setsockopt.
  Description
  The value of setsockopt is limited by the kernel parameters net.core.rmem_max and net.core.wmem_max. When adjusting the business program, you can also adjust net.core.rmem_max and net.core.wmem_max simultaneously. After adjustment, restart the business program to make the configuration take effect.
- If not set, you can increase the net.ipv4.tcp_mem, net.ipv4.tcp_rmem, and net.ipv4.tcp_wmem kernel parameters to adjust the TCP socket water level.

The number of connections has reached the upper limit

CVM instances are available in various specifications, and different specifications have different connection performance metrics. When the number of connections of an instance exceeds the standard corresponding to the instance specification, the platform's speed limit will be triggered, resulting in packet loss. The processing steps are as follows:
Description
The number of connections refers to the number of sessions of the CVM instance saved on the host, including TCP, UDP, and ICMP. This value is greater than the number of network connections obtained

through the ss or netstat command on the CVM instance.

Check the number of connections on your instance and compare it to Strength Specifications, check whether the instance specification performance bottleneck has been reached.

- Yes, you need to upgrade the instance specifications or adjust the business volume.
- No, if the performance bottleneck of the instance specification has not been reached, further location processing can be performed.

iptables policy sets relevant rules

In the absence of relevant iptables rules set on the CVM, the iptables policy-related rule settings may be causing packets destined for the CVM to be discarded.
The processing steps are as follows:

1. Perform the following command to check the iptables policy rules.

```
iptables -L | grep policy
```

The default iptables policy rule is ACCEPT. If the INPUT chain policy is not ACCEPT, all packets to the server will be lost. For example, if the following result is returned, it means that all packets entering the CVM will be dropped.

```
Chain INPUT (policy DROP)
Chain FORWARD (policy ACCEPT)
Chain OUTPUT (policy ACCEPT)
```

2. Perform the following command and adjust the value after -P as needed.

```
iptables -P INPUT ACCEPT
```

After adjustment, you can perform the command in step 1 of iptables policy sets related ruless again to check the results as follows:

```
Chain INPUT (policy ACCEPT)
Chain FORWARD (policy ACCEPT)
Chain OUTPUT (policy ACCEPT)
```

Unable to ping the instance IP address

Failure Symptoms

The local host's failure to ping the instance could be due to the following problems:

- The target server settings are incorrect.
- The domain name failed to resolve properly.
- Link Fault

On the premise that the local network is functioning properly(you can ping other websites without issue), you can troubleshoot according to the following steps:

- Check whether the instance is configured with a public IP
- Check security group settings
- Check system settings
- Check whether the domain name is registered
- Check domain name resolution.
- Other operations

Processing Procedures

Check whether the instance is configured with a public IP

> Note:
> The instance must have a public IP address to be accessible to other computers on the Internet. If the instance does not have a public IP, the private IP address cannot directly ping the instance.

1. Log in to the CVM console.
2. On the CVM List page, select the instance ID/host name that needs to be ping-tested and then enter the instance details page.
3. In the Host Information column, check whether the instance is configured with a public IP.
    - If yes, check the security group settings.
    - If no, assign an Band Elastic IP to it.

Check security group settings

A security group is a virtual firewall that controls inbound and outbound traffic for associated instances. The rules of the security group can specify protocols, ports, policies, etc. Because ping uses the ICMP

protocol, confirm whether the security group associated with instance allows ICMP. Perform the following steps to view the security group used by the instance and detailed inbound and outbound rules:

1. Log in to the CVM console.
2. On the CVM List page, select the instance ID/host name that needs security group settings and then enter the instance details page.
3. Select the Security Group tab to enter the security group management page for the instance.
4. Determine whether the security group associated with the instance allows ICMP by viewing the security group used by the instance and the detailed inbound and outbound rules.
    - If yes, check system settings.
    - If no, set the ICMP protocol policy to Allow.

Check system settings

Identify the operating system type of the instance and select different inspection methods.

- For Linux operating system, check Linux kernel parameters and firewall settings.
- For Windows operating system, check Windows Firewall settings.

Check Linux kernel parameters and firewall settings

> Note:
> Whether the Linux system allows ping is determined by both the kernel and firewall settings. If either of them blocks the system, it will cause a Request timeout for ping packets.

Check the value of kernel parameter icmp_echo_ignore_all

1. Log in to the instance.

2. Run the following command to check the system's icmp_echo_ignore_all settings.

    ```
    cat /proc/sys/net/ipv4/icmp_echo_ignore_all
    ```

Domain Name Cannot Be Resolved (CentOS 6.x system)

Phenomenon Description

After restarting the CVM with the operating system CentOS 6.x or performing the command service network restart , the CVM is unable to resolve domain names.
At the same time, check the /etc/resolv.conf configuration file, it was found that the DNS information was cleared.

Possible Reasons

In CentOS 6.x operating systems, the initscripts versions earlier than 9.03.49-1 have defects due to different grep versions.

Ideas

Upgrade the initscripts to the latest version and regenerate the DNS information.

Processing Procedures

1. Log in to the CVM.

2. Perform the following command to check the version of initscripts and confirm whether the initscripts have defects due to a version lower than 9.03.49-1.

```
rpm -q initscripts
```

Information resembles the following is returned:

```
initscripts-9.03.40-2.e16.centos.x86_64
```

It can be seen that the initscripts version initscripts-9.03.40-2 is lower than the problematic version (initscripts-9.03.49-1), and there are risks of DNS being cleared.

3. Perform the following command in sequence to upgrade initscripts to the latest version and regenerate DNS information.

```
yum makecache
yum -y update initscripts
service network restart
```

4. After the upgrade is complete, perform the following command to check the version information of initscripts and confirm whether the upgrade is successful.

```
rpm -q initscripts
```

Information resembles the following is returned:

```
initscripts-9.03.58-1.el6.centos.2.x86_64
```

It can be seen that the displayed version is different from the previous version and is higher than initscripts-9.03.49-1, and the upgrade operation is successful.

FAQs
Storage
System Disk and Data Disk

What is the Default Space of the CVM System Disk?

Currently, the default space of the system disk of a newly purchased CVM is 50 GB.

In Which Regions and Availability Zones Can the System Disk Be Resized to a Size Larger Than 50 GB?

When the system disk is a CBS, all regions that support snapshots support adjusting the system disk to a size larger than 50 GB.

When I Reinstall the System, Does the System Disk of a CVM Support Scaling Out (Capacity Expansion)?

It can be divided into the following two scenarios. Please refer to them based on your actual situation:

- The system disk is a CBS:
  When you reinstall the system, capacity scale-out (increasing the size of the system disk) is supported, but capacity scale-in (reducing the size of the system disk) is not supported.

- The system disk is a local hard disk:
  When you reinstall the system, there are two situations according to the size of the current system disk:
  - The default system disk space is 50 GB when you purchase the instance, and capacity scale-out is not supported.
  - This situation applies to instances purchased earlier: if the system disk space is less than or equal to 20 GB, it will be reinstalled to 20 GB by default; if the system disk space is greater than 20 GB, it will be reinstalled to 50 GB by default.

How to Scale out the Capacity of a CBS?

If your CVM is a CBS server, you can scale out its capacity. For more information on the Operation Guide, see Scaling out CBS.

Does the system disk support scaling out (expanding the capacity) and then scaling in (reducing the capacity) by reinstalling the system?

The system disk does not support scale-in.

How Can I Save the Current Data of the CVM Instance and Scale Out the System Disk?

You can choose to create an image first, and then reinstall the system through the image to achieve the purpose

of scaling out the system disk.

When a small-capacity image of less than 50 GB is selected for creating or reinstalling a CVM, what is the size of the system disk?

The selected small image does not affect the size of the system disk, and the minimum size is 50 GB.

How to View the Data Disk?

1. Log in to the CVM console.
2. Select CBS in the left sidebar to enter the CBS management page.
   The Data Disk displaying on the Attribute column refers to the data disks available in the current region.

After you reinstall the Windows system to the Linux system, how to read and write the original NTFS type data disk?

Windows file systems usually use NTFS or FAT32 format, while Linux file system formats are usually EXT series. When the operating system is reinstalled from Windows to Linux, the operating system type changes, but the data disk remains in the original format. The reinstalled system may be unable to access the data disk file system. You can perform the following operations on the reinstalled Linux CVM to read the original data disk data under the Windows system:

1. Use the following command on the Linux system to install the ntfsprogs software so that Linux can support the NTFS file system:

```
yum install ntfsprogs
```

2. Mount the data disk under Windows to the Linux CVM. If the data disk has already been mounted, you can skip this step:
   i. Log in to the CVM console.
   ii. Select CBS in the left sidebar to enter the CBS management page.
   iii. Click More > Mount of the Windows data disk that needs to be mounted.
   iv. In the pop-up window, select the reinstalled Linux CVM and click OK.
3. Use the command to view the data disk mounted from Windows:

```
parted -l
```

4. Use the following command format to mount the data disk:

```
mount -t ntfs-3g Data Disk Path Mount Point
```

```
[root@VM_127_193_centos ~]# mount -t ntfs-3g /dev/vde2 mnt/
[root@VM_127_193_centos ~]# ls mnt/
$RECYCLE.BIN  test.txt
```

5. After the file system is identified, the mounted data disk can be directly read and written by the Linux system.

After Reinstalling the Linux System to the Windows System, How Do I Read the Original EXT-Type Data Disk?

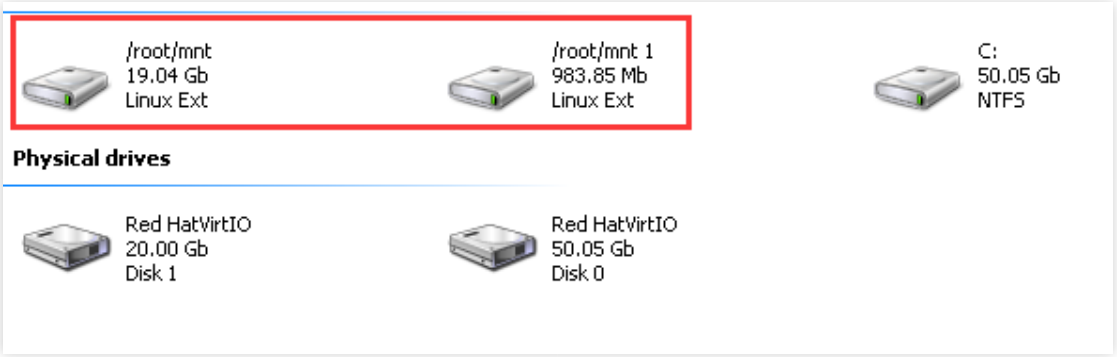
Windows file systems usually use NTFS or FAT32 format, while Linux file system formats are usually EXT series. When the operating system is reinstalled from Linux to Windows, the operating system type changes, but the data disks remain in the original format. The reinstalled system may be unable to access the original data disk file system. You can perform the following operations on the reinstalled Windows CVM to read the data on the original Linux system data disk:

1. Assume that the Linux CVM data disk has two partitions /dev/vdb1 and /dev/vdb2 before reinstallation:

```
Disk /dev/vdb: 21.5 GB, 21474836480 bytes
16 heads, 63 sectors/track, 41610 cylinders
Units = cylinders of 1008 * 512 = 516096 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x29cc8ca2

   Device Boot      Start         End      Blocks   Id  System
/dev/vdb1            2000       41610    19963944   83  Linux
/dev/vdb2               1        1999     1007464+  83  Linux
```

2. Download and install the DiskInternals Linux Reader software on the reinstalled Windows CVM.
3. Mount the data disk under Linux to the Windows CVM If the data disk has already been mounted, you can skip this step:
   i. Log in to the CVM console.
   ii. Select CBS in the left sidebar to enter the CBS management page.
   iii. Click More > Mount of the Linux data disk you want to mount.
   iv. In the pop-up window, select the reinstalled Windows CVM and click OK.
4. Click to run DiskInternals, you can see the information of the newly mounted data disks, where /root/mnt and /root/mnt1 correspond to partitions vdb1 and vdb2 respectively.



5. Click to enter /root/mnt, right-click the file you want to copy, and select Save to save the file.

> Note:
> At this time, the Linux data disk is read-only. If you need to use this data disk as a Windows data disk for read and write operations, please back up the required files first and then reformat it into a standard type supported by the Windows operating system. For specific operations, see Partitioning and formatting Windows data disks.

Backup and Restoration

How does the CVM Back up Data?

- When your CVM is a Cloud Block Storage host, you can back up your business data by creating a custom image of the system disk and a snapshot of the data disk.
- If you need to create a custom image, see Creating a Custom Image.
- If you need to create a snapshot, see Creating a Snapshot.
- When your CVM is a local disk host, your system disk can be backed up by creating a custom image. However, you still need to customize the backup policy for the business data in your data disk.

Usually, you can use FTP to back up the data in the server to other places. For specific FTP deployment methods, you can see:

- Windows operating system: Windows Instance of Setting up FTP service.
- Linux operating system: Linux Instance of Setting up FTP service.
- In addition, if you have higher requirements for data security, you can also pay for more professional third-party customized backup services.

Is There Any Common Data Backup and Recovery Solution?

Depending on different use cases and business situations, the applicable data backup and recovery solutions are also different. Here are some general suggestions we provide, use them according to your actual situation:

- Use Cloud Block Storage Snapshot Function to back up instances regularly.
- Deploy key components of applications across multiple availability zones and replicate data appropriately.
- Use Elastic IP to perform domain name mapping to ensure that the service IP can be quickly redirected to another CVM instance when the server is unavailable.
- Check monitoring data and set up appropriate alarms regularly. See Cloud Monitoring for more information.
- Use auto scaling to handle bursty requests. See Auto Scaling for more information.

CVM Dedicated Host Instance Related

What is the difference between an instance allocated on a CVM Dedicated Host (CDH) and an ordinary CVM?

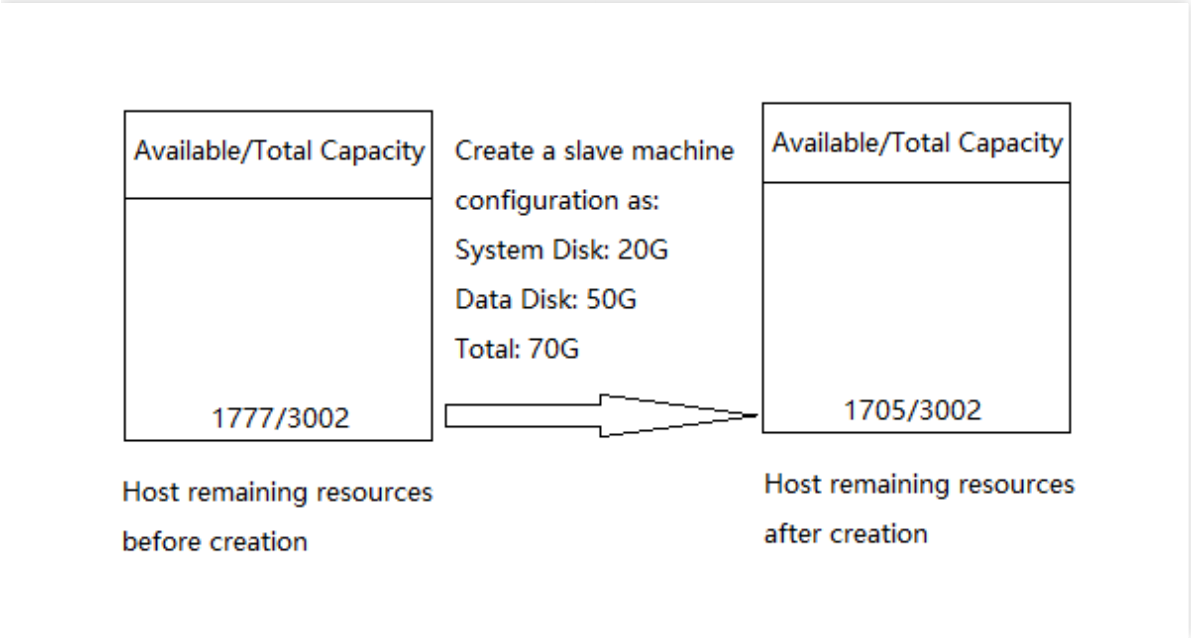
The instances on the CDH are deployed on your own CDH in a single-tenant environment, while ordinary CVMs share physical server resources among multiple tenants. CDHs support customizing the specifications of their instances, while ordinary CVMs do not support this capability. In terms of other features, there is no difference between a CDH and an ordinary CVM.

How Will the Hosts Be Allocated if Multiple CDHs Are Selected When I Create an Instance?

If you select multiple CDHs when creating an instance, the instances will be randomly created on these CDHs.

The actual disk resources occupied by the created instances are 2 GB more than the selected resources?

When they create an instance, users can customize the size of the system disk and data disk. When an instance is created, in addition to the hard disk usage planned by the user, 2 GB of local disk resources will be deducted for the storage of additional configuration information.



Do CVMs on CDHs Support Migration?

Supports hot migration of instances between different CDHs of the same model and configuration.

Currently, migration of instances between CDH resource pools and common CVM instance resource pools is not supported.

Network and Security
Network

How to Troubleshoot the Problem of No Network after Logging in to the CVM?

It may be caused by incorrect configuration of your server security group. Check the inbound and outbound rules of the server security group. Check whether your destination, protocol port, and policy are prohibited.

Can a Private Network Instance Communicate with a Basic Network Instance?

Support, but with the following restrictions:
The IP range (CIDR) of the VPC must be 10.0.0.0/16 ~ 10.0.47.0/16 (including subsets), otherwise conflicts will occur.

Setup Steps

Log in to the VPC console, click on the VPC's ID/name to enter the VPC details page, and configure the Basic Network Interconnection section by associating the required basic network hosts for interconnection.

How to View the Basic Network CVMs that are Interconnected with VPC?

Log in to the VPC console, click on the VPC's ID/name to enter the VPC details page, and in the Basic Network Interconnection section, you can view the interconnected basic network CVMs with the VPC's CVMs.

Can the CVM be Replaced to an Overseas Network?

The network of the CVM cannot be changed after purchase. If you need an overseas network, it is recommended to return the CVM and purchase a new overseas server.

How to Configure the Private Network DNS?

See Private Network DNS.

The Local VPN in the Same IP Range can Obtain the IP of the IP Range but Cannot Access the Internet. How Can This Be Resolved?

Check whether the following configuration is correct:

1. Is the manually added IP in the same IP subnet as the automatically obtained IP? Are the subnet masks consistent? Is the default gateway configured? Is the default gateway address correct?
2. Is DNS configured? Is the DNS address correct?
3. If the above information is correct, confirm whether there is any IP address conflict in the statically

configured IP address.

4. If the above methods cannot solve the problem, please submit a ticket to contact us.

Passwords and Keys

What is the Difference Between SSH key Log-in and Password Log-in?

SSH key is a way to remotely log in to a Linux server. Its principle is to use a key generator to create a pair of keys (public key and private key). Add the public key to the server, and then use the private key on the client to complete the authentication and login. This method pays more attention to data security, and is different from the manual input of the traditional password login method, and is more convenient. Currently, Linux instances support both password and SSH key log-in methods, while Windows instances only support password log-in at this time. See related documentation:

- Log in to the Linux instance
- Log in to the Windows instance

Can I Use SSH Keys to Log in and Passwords to Log in at the Same Time?

Users log in to Linux instances using SSH keys , and password log-in is disabled by default to enhance security. Therefore, after logging in with a key, users will no longer be able to use a password to log in.

What Should I Do If I Forget My Password?

You can reset your password. See Resetting Instance Password for more information.

How to Create SSH Keys and What to Do If You Lose Them?

See Creating SSH Keys for how to create SSK keys.

We provide two solutions to the key loss problem:

- Create a new key through the SSH key console of the CVM and bind the new key to the original instance.
    i. Creating a SSH key.
    ii. After the key is created, log in to the CVM instance console.
    iii. Select the original instance to which the key is to be bound, click Operation > Password/Key > Load Key, and then you can use the new key to log in to the instance.
- Reset your password through the CVM console and use the new password to log in to the instance. See Resetting Instance Password for more information.

How to Bind/Unbind a Server Using SSH Keys?

See the Binding/Unbinding Server Using SSH Key section of SSH Key Operation Guide.

How to Change the SSH Key Name/Description?

See the Modifying the Name/Description of SSH Key section of SSH Key Operation Guide.

How to Delete SSH Key?

See the Deleting SSH key section of SSH Key Operation Guide.

What Are the Use Limits of SSH Keys?

See the Use Limits section of SSH Key Introduction.

Cannot Log in to My Linux Instance Using an SSH Key. How can Troubleshoot This?

See Unable to log in to Linux instance via SSH.

IP Address

What Is the Public IP Address?

See the Public IP Address section of Public Network Service.

What Is Private IP Address?

See the Private IP address section of Private Network Service.

How to obtain the public IP address of an instance?

See the Obtaining the Public IP Address of the Instance section of Public Network Service.

How to Obtain the Private IP Address of an Instance?

See the Obtaining the Public IP Address of the Instance section of Private Network Service.

How to Change the Public IP Address of an Instance?

See Changing the Instance's Public IP Operation Guide.

What is the Difference Between a Public Gateway and a CVM with a Public IP?

The public network gateway has the public network traffic routing and forwarding function enabled in the image, but the CVM with a public network IP does not have the traffic forwarding function by default. Windows public image CVMs cannot be used as public network gateways because the traffic forwarding function is not enabled in Windows images.

Elastic IP

What Can an Elastic IP Be Used for?

EIP is suitable for the following scenarios:

- Disaster Recovery. We strongly recommend using Elastic IP for disaster recovery. When one of your servers cannot provide services normally, you can unbind the Elastic IP from this server and rebind it to a healthy server to quickly restore service.
- Reserving specific public IP. When you need to reserve a specific public IP in your account, you can convert it to an Elastic IP, and after binding/unbinding it to a device, you can use that IP for public network access.
  As long as you do not perform the Release operation, the EIP will remain in your account.
- Other special cases. When you have other special situations that require IP replacement, you can convert a regular public IP to an Elastic IP and achieve the replacement by binding/unbinding the Elastic IP. However, EIP resources are valuable, and there are quota limits per region for each account. We recommend that you plan and use them reasonably.

How Much does an Elastic IP Cost?

1. The fee displayed in the console represents the fee for a full hour of idleness. Currently, the charging for Elastic Public IP (Elastic IP) can be precise to the second. For multiple bindings/unbindings, the duration of the unbound status will be charged after being accumulated in seconds.
2. If the total duration of vacancy is less than one hour, the resource occupation fee will be charged on a pro-rata basis.

When Will an Elastic IP Be Charged?

Currently, operations related to Elastic IP include application, binding, unbinding, and release. Since IP resources are valuable, Elastic IP only charges a small amount of resource usage fee when it is unbound from the device.

How to Stop Charging for Elastic IP?

- When you no longer need the Elastic IP that is being charged, you can release it. After the Elastic IP is released, you will no longer be charged.
  See Releasing EIP for more information.
- If you need to keep an Elastic IP and stop charging for it, you can bind it to a device (CVM, NAT), and the bound Elastic IP will no longer be charged.

How to Access a Public Network If the CVM Does Not Have an Ordinary Public IP?

If you did not purchase a public IP when you purchased the machine or the public IP has been returned, you can apply for an elastic IP in the Elastic IP console and then bind it to your machine for public network access.

Can the Public IP Address Be Changed?

You can change the public IP address of your CVM. See Changing Instance in Public IP Address for more information.

How do I keep a public IP unchanged?

When you need to reserve a specific public IP in your account, you can convert it to an Elastic IP. After binding it to a device, you can use this IP for public network access. As long as you do not perform the release operation, the Elastic IP remains in your account.
See Elastic IP for related operations.

Can EIP be converted back to a regular public IP?

EIP cannot be converted back to a regular public IP.

Elastic Network Interface

What Is an Elastic Network Interface?

Elastic Network Interface (ENI) is an elastic network interface bound to CVMs in a VPC, which can be freely migrated among multiple CVMs. ENI is very helpful in configuring and managing networks and building highly reliable network solutions.

An ENI combines VPC, availability zone, and subnet attributes and can only be bound to CVMs in the same availability zone. A CVM can bind multiple ENIs, and the specific number of bindings will depend on the host specifications.

What are the Restrictions on Using ENIs in CVM?

See the Elastic Network Interface Related Limits section in the Overview of Usage Limits.

What is the Basic Information of ENI?

See the Related Concepts section of Introduction to ENI.

How to Create an ENI?

See Creating an ENI.

How to view an ENI?

See Viewing an ENI.

How to Bind an ENI to a CVM Instance?

See Binding and Configuring CVM.

How to Configure an ENI in a CVM Instance?

See Binding and Configuring CVM.

How to Modify or Customize the Private IP Address of an ENI?

The CVM in a VPC supports modification and customization of the ENI's private IP. The console directions are as follows:

1. Log in to the VPC console.
2. In the left sidebar, Click IP and Network Interface > ENI to open the Elastic Network Interface list page.
3. Click the ID/Name of the ENI to go to the ENI details page and check the ENI information.
4. Select the IPv4 Address Management tab and click Assign Private IP.
5. In the pop-up window, select the IP allocation method as Manually Fill in , and enter the IP address you want to modify.

6. Click Confirm to complete the operation.

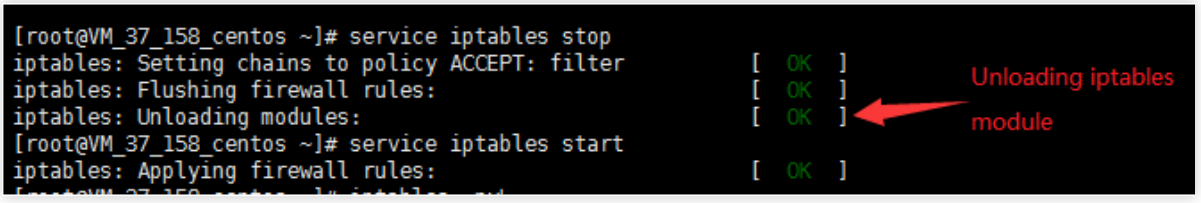
After modifying the console, you also need to modify the network interface configuration file synchronously. See Binding and Configuring CVM.

Firewall

How to Configure the Firewall Software iptables in Linux System?

Note:
There are significant changes in iptables versions before and after CentOS 7.

- Before CentOS 7, the iptables service was used as the firewall by default. Use service iptables stop code, the iptables service will first clear the rules and then uninstall the iptables module. When you restart, the rules are loaded from the configuration file. Stopping the iptables service can test whether there is firewall restriction.



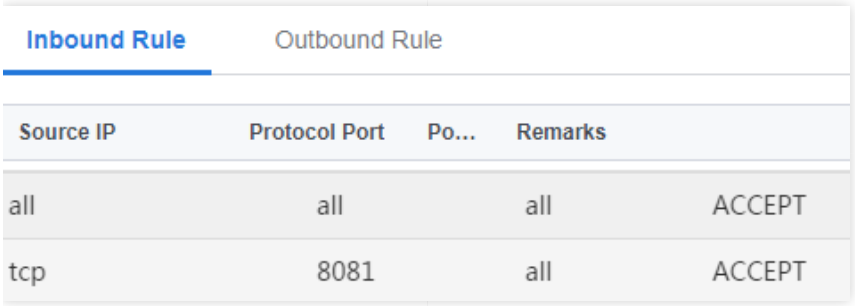
- After CentOS 7, the firewall service is used as the firewall by default. For compatibility, the iptables_filter module is loaded at the same time, but there is no iptables service. So after CentOS 7, you can use the iptables command to add rules, but the iptables service is closed by default. Once the user confirms that the iptable_filter module is loaded, the rules will take effect.
  The most reliable way to determine the firewall is to view the rules via iptables -nvL .

The following two examples illustrate how to configure:

Scenario one

Ubuntu 14 system, security group is open, listening port is enabled, but telnet is not working.

Security group inbound rules:



Security group outbound rules:

Inbound Rule | **Outbound Rule**

Destination IP A...	Protocol Port	Po...	Remarks
all	all	all	ACCEPT
tcp	8081	all	ACCEPT

Telnet is not working:

```
target     prot opt source               destination
RETURN     tcp  --  anywhere             anywhere             limit: avg 3/sec b
urst 6
REJECT     all  --  anywhere             anywhere             reject-with icmp-p
ort-unreachable
root@VM-166-120-ubuntu:~# service iptables status
iptables: unrecognized service
root@VM-166-120-ubuntu:~# ufw status
Status: inactive
root@VM-166-120-ubuntu:~# netstat -tlunp |grep 8081
tcp        0      0 0.0.0.0:8081            0.0.0.0:*               LISTEN
1687/nginx.conf
root@VM-166-120-ubuntu:~# _
```

Ideas

1. First, capture the packet of the host to determine whether the packet has reached the host.
   - If the connection does not reach the host, it may be blocked by the security group, upper-layer TGW, or operator.
   - If the packet reaches the host, but there is a problem with the return packet, it is most likely caused by the iptables policy inside the host. As shown in the figure below, after telnet, no TCP packet is returned to 64.11.

```
root@VM-166-120-ubuntu:/home/ubuntu# tcpdump -i any host 183.60.64.11
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked), capture size 65535 bytes
19:02:21.194801 IP 183.60.64.11.58839 > 10.104.166.120.tproxy: Flags [S], seq 668485174, win 5840, options [mss 1424,sackOK,TS val 496201777 ecr 0,n
op,wscale 7], length 0
19:02:21.194824 IP 10.104.166.120 > 183.60.64.11: ICMP host 10.104.166.120 unreachable - admin prohibited, length 68
```

2. After you confirm that it is an iptables policy problem, use iptables –nvL to check whether the policy allows port 8081 to be opened. This port is not open here.

```
root@VM-166-120-ubuntu:~# iptables -L -n
Chain INPUT (policy ACCEPT)                    Input
target     prot opt source               destination
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:22
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:80
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:21
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpts:20000:30000
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:443
ACCEPT     icmp --  0.0.0.0/0            0.0.0.0/0           limit: avg 100/sec burst 100
ACCEPT     icmp --  0.0.0.0/0            0.0.0.0/0           limit: avg 1/sec burst 10
syn-flood  tcp  --  0.0.0.0/0            0.0.0.0/0           tcp flags:0x17/0x02
REJECT     all  --  0.0.0.0/0            0.0.0.0/0           reject-with icmp-host-prohibited
```

3. Use the command to add a policy to allow port 8081 to pass.

iptables -I INPUT 5 -p tcp --dport 8081 -j ACCEPT

4. Test port 8081 and it is connected. The problem is solved.

Scenario two

From the iptables configuration, the policy has been released, but the destination machine is still not pingable.

```
-bash-4.2# cat /etc/resolv.conf
#search localdomain
#nameserver 202.98.
#nameserver 61.139.
nameserver 10.225.30.181
nameserver 10.225.30.223
options timeout:1 rotate
-bash-4.2# vi /etc/resolv.conf
-bash-4.2# grep host /etc/nsswitch.conf
#hosts:     db files nisplus nis dns
hosts:      files dns
-bash-4.2# grep GATEWAY /etc/sysconfig/network-scripts/ifcfg*
/etc/sysconfig/network-scripts/ifcfg-eth0:GATEWAY='10.104.61.1'
-bash-4.2#
```

Ideas

If the following situations occur:

```
Chain OUTPUT (policy ACCEPT 740K packets, 616M bytes)
 pkts bytes target     prot opt in     out     source               destination
 2144  147K DROP       udp  --  *      *       0.0.0.0/0            0.0.0.0/0
    0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            10.225.30.181       udp dpt:53
    0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            10.225.30.223       udp dpt:53
    0     0 DROP       udp  --  *      *       0.0.0.0/0            0.0.0.0/0
    0     0 DROP       udp  --  *      *       0.0.0.0/0            0.0.0.0/0
    0     0 DROP       udp  --  *      *       0.0.0.0/0            0.0.0.0/0
```

Test by using the following command to delete the first rule in the OUTPUT direction:

iptabels –D OUTPUT 1

Test again, and the problem should be solved.

How to Clear the Firewall?

Windows Enstances

1. After you log in to the instance, click Start > Control Panel > Firewall Settings to enter the Firewall Settings page.
2. Check whether the firewall and other security software (such as SafeDog, etc.) are turned on. If so, just turn them off.

Linux Instance

1. Run the command to check whether the customer has enabled the firewall policy. If closed, skip step 2 and proceed directly to step 3:

```
iptables -vnL
```

2. If the firewall policy is enabled, execute the command to back up the current firewall policy:

```
iptables-save
```

3. Run the command to clear the firewall policy.

```
iptables -F
```

Will using non-Converge Cloud CDN to accelerate CVM to be blocked by the firewall?

No. If you are concerned about the impact, you can turn off the firewall.

API Documentation
Cloud Virtual Machine(cvm)
version(2017-03-12)
API overview

API version

V3

CDH APIs

Interface name	Interface function
DescribeZoneHostConfigInfos	DescribeZoneHostConfigInfos
InquiryPriceAllocateHosts	InquiryPriceAllocateHosts
TerminateHosts	TerminateHosts

Image APIs

Interface name	Interface function
CreateImage	CreateImage
DeleteImages	DeleteImages
DescribeImageQuota	DescribeImageQuota
DescribeImageSharePermission	DescribeImageSharePermission
DescribeImageSnapshotStatus	DescribeImageSnapshotStatus
DescribeImages	DescribeImages
DescribeImportImageOs	DescribeImportImageOs
ImportImage	ImportImage

Interface name	Interface function
ModifyImageAttribute	ModifyImageAttribute
ModifyImageSharePermission	ModifyImageSharePermission
SyncImages	SyncImages

Instance APIs

Interface name	Interface function
CloneInstance	CloneInstance
CreateDiagnosticReports	CreateDiagnosticReports
CreateDisasterRecoverGroup	CreateDisasterRecoverGroup
DeleteDisasterRecoverGroup	DeleteDisasterRecoverGroup
DeleteDisasterRecoverGroups	DeleteDisasterRecoverGroups
DescribeDiagnosticReports	DescribeDiagnosticReports
DescribeDisasterRecoverGroupQuota	DescribeDisasterRecoverGroupQuota
DescribeDisasterRecoverGroups	DescribeDisasterRecoverGroups
DescribeInstanceConfigInfos	DescribeInstanceConfigInfos
DescribeInstanceFamilyConfigs	DescribeInstanceFamilyConfigs
DescribeInstanceInternetBandwidthConfigs	DescribeInstanceInternetBandwidthConfigs
DescribeInstanceTypeConfigs	DescribeInstanceTypeConfigs
DescribeInstanceTypeDisasterGroupBlackList	DescribeInstanceTypeDisasterGroupBlackList
DescribeInstanceUsbInfo	DescribeInstanceUsbInfo
DescribeInstanceVncUrl	DescribeInstanceVncUrl
DescribeInstances	DescribeInstances
DescribeInstancesDeniedActions	DescribeInstancesDeniedActions
DescribeInstancesModification	DescribeInstancesModification

Interface name	Interface function
DescribeInstancesStatus	DescribeInstancesStatus
DescribeZoneInstanceConfigInfos	DescribeZoneInstanceConfigInfos
GetRecycleInfo	GetRecycleInfo
ImportSnapshot	ImportSnapshot
InquiryPriceRenewInstances	InquiryPriceRenewInstances
InquiryPriceResetInstance	InquiryPriceResetInstance
InquiryPriceResetInstancesInternetMaxBandwidth	InquiryPriceResetInstancesInternetMaxBandwidth
InquiryPriceResetInstancesType	InquiryPriceResetInstancesType
InquiryPriceResizeInstanceDisks	InquiryPriceResizeInstanceDisks
InquiryPriceRunInstances	InquiryPriceRunInstances
InquiryResourceResetInstancesType	InquiryResourceResetInstancesType
InstanceAttachISO	InstanceAttachISO
InstanceDetachISO	InstanceDetachISO
ModifyDisasterRecoverGroup	ModifyDisasterRecoverGroup
ModifyInstancesAttribute	ModifyInstancesAttribute
ModifyInstancesDisasterRecoverGroup	ModifyInstancesDisasterRecoverGroup
ModifyInstancesRenewFlag	ModifyInstancesRenewFlag
ModifyInstancesVpcAttribute	ModifyInstancesVpcAttribute
RebootInstances	RebootInstances
RemoveInstancesDisasterRecoverGroup	RemoveInstancesDisasterRecoverGroup
RenewInstances	RenewInstances
ResetInstance	ResetInstance
ResetInstancesInternetMaxBandwidth	ResetInstancesInternetMaxBandwidth
ResetInstancesPassword	ResetInstancesPassword
ResetInstancesType	ResetInstancesType

Copyright: Converge Cloud

Interface name	Interface function
ResizeInstanceDisks	ResizeInstanceDisks
RunInstances	RunInstances
StartInstances	StartInstances
StopInstances	StopInstances
SwitchParameterRunInstances	SwitchParameterRunInstances
TerminateInstances	TerminateInstances
ViewModifyInstancesAttribute	ViewModifyInstancesAttribute

Instance Launch Template APIs

Interface name	Interface function
CreateLaunchTemplate	CreateLaunchTemplate
DeleteLaunchTemplate	DeleteLaunchTemplate
DeleteLaunchTemplates	DeleteLaunchTemplates
DescribeLaunchTemplatesInfo	DescribeLaunchTemplatesInfo
ModifyLaunchTemplate	ModifyLaunchTemplate
ModifyLaunchTemplateName	ModifyLaunchTemplateName

Key APIs

Interface name	Interface function
AssociateInstancesKeyPairs	AssociateInstancesKeyPairs
CreateKeyPair	CreateKeyPair
DeleteKeyPairs	DeleteKeyPairs
DescribeKeyPairs	DescribeKeyPairs
DisassociateInstancesKeyPairs	DisassociateInstancesKeyPairs

Interface name	Interface function
ImportKeyPair	ImportKeyPair
ModifyKeyPairAttribute	ModifyKeyPairAttribute

Other APIs

Interface name	Interface function
CreateHpcCluster	CreateHpcCluster
DeleteHpcClusters	DeleteHpcClusters
DescribeHpcClusters	DescribeHpcClusters
ModifyHpcClusterAttribute	ModifyHpcClusterAttribute

Region APIs

Interface name	Interface function
DescribeRegions	DescribeRegions
DescribeZones	DescribeZones

CallingMethod signaturev1

Converge Cloud authenticates each access request, i.e. each request needs to include authentication information (Signature) in the common parameters to verify the identity of the requester.
The Signature is generated by the security credentials which include SecretId and SecretKey. If you don't have the security credentials yet, go to the API Key page to apply for them; otherwise, you cannot invoke the API.

1. Applying for Security Credentials

Before using the API for the first time, go to the API Key page to apply for security credentials.
Security credentials consist of SecretId and SecretKey:

- SecretId is used to identify the API requester.
- SecretKey is used to encrypt the signature string and verify it on the server.
- You must keep your security credentials private and avoid disclosure.

You can apply for the security credentials through the following steps:

1. Log in to the Converge Cloud Console.
2. Go to the Cloud API Key page.
3. On the API Key Management page, click Create Key to create a SecretId/SecretKey pair.

Note: Each account can have up to two pairs of SecretId/SecretKey.

2. Generating a Signature

With the SecretId and SecretKey, a signature can be generated. The following describes how to generate a signature:

Assume that the SecretId and SecretKey are:

- SecretId: AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE
- SecretKey: Gu5t9xGARNpq86cd98joQYCN3EXAMPLE

Note: This is just an example. For actual operations, please use your own SecretId and SecretKey.

Take the Cloud Virtual Machine's request to view the instance list (DescribeInstances) as an example. When

you invoke this API, the request parameters may be as follows:

Parameter name	Description	Parameter value
Action	Method name	DescribeInstances
SecretId	Key ID	AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE
Timestamp	Current timestamp	1465185768
Nonce	Random positive integer	11886
Region	Region where the instance is located	luzon
InstanceIds.0	ID of the instance to query	ins-09dx96dg
Offset	Offset	0
Limit	Allowed maximum output	20
Version	API version number	2017-03-12

2.1. Sorting Parameters

First, sort all the request parameters in an ascending lexicographical order (ASCII code) by their names. Notes: (1) Parameters are sorted by their names instead of their values; (2) The parameters are sorted based on ASCII code, not in an alphabetical order or by values. For example, InstanceIds.2 should be arranged after InstanceIds.12. You can complete the sorting process using a sorting function in a programming language, such as the ksort function in PHP. The parameters in the example are sorted as follows:

```
{
    'Action' : 'DescribeInstances',
    'InstanceIds.0' : 'ins-09dx96dg',
    'Limit' : 20,
    'Nonce' : 11886,
    'Offset' : 0,
    'Region' : 'luzon',
    'SecretId' : 'AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE',
    'Timestamp' : 1465185768,
    'Version': '2017-03-12',
}
```

When developing in another programming language, you can sort these sample parameters and it will work as long as you obtain the same results.

2.2. Concatenating a Request String

This step generates a request string.
Format the request parameters sorted in the previous step into the form of "parameter name"="parameter value". For example, for the Action parameter, its parameter name is "Action" and its parameter value is "DescribeInstances", so it will become Action=DescribeInstances after formatted.
Note: The "parameter value" is the original value but not the value after URL encoding.

Then, concatenate the formatted parameters with "&". The resulting request string is as follows:

```
Action=DescribeInstances&InstanceIds.0=ins-09dx96dg&Limit=20&Nonce=11886&Offset=0&Region=luzon&SecretId=AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE&Timestamp=1465185768&Version=2017-03-12
```

2.3. Concatenating the Signature Original String

This step generates a signature original string.
The signature original string consists of the following parameters:

1. HTTP method: POST and GET modes are supported, and GET is used here for the request. Please note that the method name should be in all capital letters.
2. Request host: the domain name of the request to view the list of instances (DescribeInstances) is cvm.convergecloud.com. The actual request domain name varies by the module to which the API belongs. For more information, see the instructions of the specific API.
3. Request path: The request path in the current version of Cloud API is fixed to / .
4. Request string: the request string generated in the previous step.

The concatenation rule of the signature original string is: Request method + request host + request path + ? + request string

The concatenation result of the example is:

```
GETcvm.convergecloud.com/?Action=DescribeInstances&InstanceIds.0=ins-09dx96dg&Limit=20&Nonce=11886&Offset=0&Region=luzon&SecretId=AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE&Timestamp=1465185768&Version=2017-03-12
```

2.4. Generating a Signature String

This step generates a signature string.
First, use the HMAC-SHA1 algorithm to sign thesignature original stringobtained in the previous step, and then encode the generated signature using Base64 to obtain the final signature.

The specific code is as follows with the PHP language being used as an example:

```
$secretKey = 'Gu5t9xGARNpq86cd98joQYCN3EXAMPLE';
$srcStr = 'GETcvm.convergecloud.com/?Action=DescribeInstances&InstanceIds.0=ins-09dx96dg&Limit
=20&Nonce=11886&Offset=0&Region=luzon&SecretId=AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPL
E&Timestamp=1465185768&Version=2017-03-12';
$signStr = base64_encode(hash_hmac('sha1', $srcStr, $secretKey, true));
echo $signStr;
```

The final signature is:

```
EliP9YW3pW28FpsEdkXt/+WcGeI=
```

When developing in another programming language, you can sign and verify the original in the example above and it works as long as you get the same results.

3. Encoding a Signature String

The generated signature string cannot be directly used as a request parameter and must be URL encoded.

For example, if the signature string generated in the previous step is EliP9YW3pW28FpsEdkXt/+WcGeI= , the final signature string request parameter (Signature) is EliP9YW3pW28FpsEdkXt%2f%2bWcGeI%3d, which will be used to generate the final request URL.

**Note: If your request method is GET, or the request method is POST and the Content-Type is application/x-www-form-urlencoded, then all the request parameter values need to be URL encoded (except the parameter key and the symbol of =) when sending the request. Non-ASCII characters need to be encoded with UTF-8 before URL encoding. **

Note: The network libraries of some programming languages automatically URL encode all parameters, in which case there is no need to URL encode the signature string; otherwise, two rounds of URL encoding will cause the signature to fail.

Note: Other parameter values also need to be encoded using RFC 3986. Use %XY in percent-encoding for special characters such as Chinese characters, where "X" and "Y" are hexadecimal characters (0-9 and uppercase A-F), and using lowercase will cause an error.

4. Signature Failure

The following situational error codes for signature failure may occur. Please resolve the errors accordingly.

Error code	Error description
AuthFailure.SignatureExpire	The signature is expired

Error code	Error description
AuthFailure.SecretIdNotFound	The key does not exist
AuthFailure.SignatureFailure	Signature error
AuthFailure.TokenFailure	Token error
AuthFailure.InvalidSecretId	Invalid key (not a Cloud API key type)

5. Signature Demo

When calling API 3.0, you are recommended to use the corresponding Converge Cloud SDK 3.0, Swhich encapsulates the signature process, enabling you to focus on only the specific APIs provided by the product when developing. See SDK Center for more information. Currently, the following programming languages are supported:

- Python
- Java
- PHP
- Go
- Node

To further explain the signing process, we will use a programming language to implement the process described above. The request domain name, API and parameter values in the sample are used here. This goal of this example is only to provide additional clarification for the signature process, please see the SDK for actual usage.

The final output URL might be: https://cvm.convergecloud.com/?Action=DescribeInstances&InstanceIds.0=ins-09dx96dg&Limit=20&Nonce=11886&Offset=0&Region=luzon&SecretId=AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE&Signature=EliP9YW3pW28FpsEdkXt%2F%2BWcGeI%3D&Timestamp=1465185768&Version=2017-03-12

Note: The key in the example is fictitious, and the timestamp is not the current time of the system, so if this URL is opened in the browser or called using commands such as curl, an authentication error will be returned: Signature expired. In order to get a URL that can work properly, you need to replace the SecretId and SecretKey in the example with your real credentials and use the current time of the system as the Timestamp.

Note: In the example below, even if you use the same programming language, the order of the parameters in the URL may be different for each execution. However, the order does not matter, as long as all the parameters are included in the URL and the signature is calculated correctly.

Note: The following code is only applicable to API 3.0. It cannot be directly used in other signature processes. Even with an older API, signature calculation errors may occur due to the differences in details. Please refer to the corresponding documentation.

Java

```
import java.io.UnsupportedEncodingException;
import java.net.URLEncoder;
import java.util.Random;
import java.util.TreeMap;
import javax.crypto.Mac;
import javax.crypto.spec.SecretKeySpec;
import javax.xml.bind.DatatypeConverter;

public class CloudAPIDemo {
    private final static String CHARSET = "UTF-8";

    public static String sign(String s, String key, String method) throws Exception {
        Mac mac = Mac.getInstance(method);
        SecretKeySpec secretKeySpec = new SecretKeySpec(key.getBytes(CHARSET), mac.getAlgorithm());
        mac.init(secretKeySpec);
        byte[] hash = mac.doFinal(s.getBytes(CHARSET));
        return DatatypeConverter.printBase64Binary(hash);
    }

    public static String getStringToSign(TreeMap<String, Object> params) {
        StringBuilder s2s = new StringBuilder("GETcvm.convergecloud.com/?");
        // When signing, the parameters need to be sorted in lexicographical order. TreeMap is used here
to guarantee the correct order.
        for (String k : params.keySet()) {
            s2s.append(k).append("=").append(params.get(k).toString()).append("&");
        }
        return s2s.toString().substring(0, s2s.length() - 1);
    }

    public static String getUrl(TreeMap<String, Object> params) throws UnsupportedEncodingException
{
        StringBuilder url = new StringBuilder("https://cvm.convergecloud.com/?");
        // There is no requirement for the order of the parameters in the actual request URL.
        for (String k : params.keySet()) {
            // The request string needs to be URL encoded. As the Key is all in English letters, only the valu
e is URL encoded here.
            url.append(k).append("=").append(URLEncoder.encode(params.get(k).toString(), CHARSET)).app
end("&");
        }
        return url.toString().substring(0, url.length() - 1);
```

```
    }

    public static void main(String[] args) throws Exception {
        TreeMap<String, Object> params = new TreeMap<String, Object>(); // TreeMap enables automati
c sorting
        // A random number should be used when actually calling, for example: params.put("Nonce", new
Random().nextInt(java.lang.Integer.MAX_VALUE));
        params.put("Nonce", 11886); // Common parameter
        // The current time of the system should be used when actually calling, for example:   params.put
("Timestamp", System.currentTimeMillis() / 1000);
        params.put("Timestamp", 1465185768); // Common parameter
        params.put("SecretId", "AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE"); // Common parameter
        params.put("Action", "DescribeInstances"); // Common parameter
        params.put("Version", "2017-03-12"); // Common parameter
        params.put("Region", "luzon"); // Common parameter
        params.put("Limit", 20); // Business parameter
        params.put("Offset", 0); // Business parameter
        params.put("InstanceIds.0", "ins-09dx96dg"); // Business parameter
        params.put("Signature", sign(getStringToSign(params), "Gu5t9xGARNpq86cd98joQYCN3EXAMPLE
", "HmacSHA1")); // Common parameter
        System.out.println(getUrl(params));
    }
}
```

Python

Note: If running in a Python 2 environment, the following requests dependency package must be installed first: pip install requests .

```
# -*- coding: utf8 -*-
import base64
import hashlib
import hmac
import time

import requests

secret_id = "AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE"
secret_key = "Gu5t9xGARNpq86cd98joQYCN3EXAMPLE"

def get_string_to_sign(method, endpoint, params):
    s = method + endpoint + "/?"
    query_str = "&".join("%s=%s" % (k, params[k]) for k in sorted(params))
    return s + query_str

def sign_str(key, s, method):
```

```
    hmac_str = hmac.new(key.encode("utf8"), s.encode("utf8"), method).digest()
    return base64.b64encode(hmac_str)

if __name__ == '__main__':
    endpoint = "cvm.convergecloud.com"
    data = {
        'Action' : 'DescribeInstances',
        'InstanceIds.0' : 'ins-09dx96dg',
        'Limit' : 20,
        'Nonce' : 11886,
        'Offset' : 0,
        'Region' : 'luzon',
        'SecretId' : secret_id,
        'Timestamp' : 1465185768, # int(time.time())
        'Version': '2017-03-12'
    }
    s = get_string_to_sign("GET", endpoint, data)
    data["Signature"] = sign_str(secret_key, s, hashlib.sha1)
    print(data["Signature"])
    # n actual invocation would occur here, which may incur fees after success
    # resp = requests.get("https://" + endpoint, params=data)
    # print(resp.url)
```

signaturev3

Converge Cloud The API will authenticate each access request, meaning that each request must include signature information (Signature) in the public request parameters to verify the requester's identity.
The signature information is generated by the security credentials, which include SecretId and SecretKey . If the user does not have security credentials, please apply for them on the Cloud API Key page, otherwise they cannot call the Cloud API interfaces.

1. Apply for security credentials.

Before using the Cloud API for the first time, please go to the Cloud API Key page to apply for a security credential.
Security credentials include SecretId and SecretKey:

- SecretId The security credentials are used to identify the identity of the API caller.
- SecretKey The secret key is used to encrypt and sign the string for server-side verification of the signature.
- Users must strictly protect their security credentials and avoid disclosure them.

The specific steps to apply for security credentials are as follows:

1. Log in to Converge Cloud Administration Center Console
2. Go to the console page for cloud API keys
3. On the Cloud API Key page, click New to create a pair of SecretId/SecretKey

Note: Developer accounts can have up to two pairs SecretId / SecretKey.

2. TC3-HMAC-SHA256 signature method

Note: For GET method, only Content-Type: application/x-www-form-urlencoded protocol format is supported. For POST method, Content-Type: application/json and Content-Type: multipart/form-data are currently supported. By default, all business interfaces are supported in json format. Only specific business interfaces are supported in multipart format. In this case, the interface cannot be called in json format. Refer to the specific business interface document description.

The following takes Cloud Virtual Machine querying Region-1 instance list as an example to introduce the signature calculation process step by step. We only use two parameters for the query instance list: Limit and Offset, called using the GET method.

Assume that the SecretId and SecretKey of the user are AKIDz 8krbsJ 5yKBZQpn 74WFkmLPx 3EXAMPLE and Gu 5t9xGARNpq 86cd 98joQYCN3EXAMPLE, respectively.

2.1. splice specification request string

Concatenate CanonicalRequest strings in the following format:

```
CanonicalRequest =
  HTTPRequestMethod + '\n' +
  CanonicalURI + '\n' +
  CanonicalQueryString + '\n' +
  CanonicalHeaders + '\n' +
  SignedHeaders + '\n' +
  HashedRequestPayload
```

- HTTPRequestMethod: HTTP request methods (GET, POST), GET in this example;
- CanonicalURI: URI parameter, API 3.0 fixed to forward slash (/);
- CanonicalQueryString: Query string in the URL that initiates the HTTP request. For POST requests, it is fixed as an empty string. For GET requests, it is the question mark (?) in the URL. The following string content, this example value is: Limit=10&Offset=0. Note: CanonicalQueryString needs to be URL encoded.
- CanonicalHeaders: The header information of participating signature, at least including host and content-type, can also be added with customized header to improve the uniqueness and security of its own request. Splicing rules: 1) head key and value are uniformly converted to lowercase, and the first and last spaces are removed, and spliced according to the format of key:value\n;2) multiple heads are spliced according to the dictionary sorting of head key (lowercase). In this example: content-type: application/x-www-form-urlencoded\nhost: cvm.convergecloud.com\n
- SignedHeaders: The header information involved in the signature indicates which headers participate in the signature of this request, and the header content contained in CanonicalHeaders is one-to-one corresponding. content-type and host are required headers. constructed as: 1) The head key is uniformly converted to lowercase; 2) Multiple header keys (lowercase) are concatenated according to dictionary sorting and separated by semicolons (;). In this case: content-type;host
- HashedRequestPayload: The hash value of the request body, calculated as Lowercase(HexEncode(Hash.SHA256(RequestPayload))), SHA256 hash the entire payload of the HTTP request body, then hexadecimal encoding, and finally converting the encoding string to lowercase letters. Note: For GET requests, RequestPayload is fixed as an empty string. For POST requests, RequestPayload is the payload of the HTTP request body.

According to the above rules, the resulting canonical request string in the example is as follows (for clarity, \nnewlines are replaced by a new line printed separately):

```
GET
```

```
/
Limit=10&Offset=0
content-type:application/x-www-form-urlencoded
host:cvm.convergecloud.com

content-type;host
e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
```

2.2. Concatenate the string to be signed

Concatenate the string to be signed in the following format:

```
StringToSign =
  Algorithm + \n +
  RequestTimestamp + \n +
  CredentialScope + \n +
  HashedCanonicalRequest
```

- Algorithm: Signature algorithm, currently fixed as TC3-HMAC-SHA256;
- RequestTimestamp: Request timestamp, i.e. the X-TC-Timestamp value of the request header. The request in the example above is 1539084154;
- CredentialScope: Credential range in the format Date/service/tc3_request, containing date, requested service and termination string (tc3_request). **Date is the date of UTC standard time, the value needs to be consistent with UTC standard time converted by common parameter X-TC-Timestamp **;service is the product name, which must be consistent with the product domain name called, such as cvm. The above example request, the value is 2018-10-09/cvm/tc3_request;
- HashedCanonicalRequest: The hash value of the canonical request string obtained by concatenating the above steps is calculated by Lowercase(HexEncode(Hash.SHA256(CanonicalRequest))).

note:

> 1. Date must be calculated from timestamp X-TC-Timestamp and time zone UTC+0. Adding local time zone information to the system, such as East Zone 8, will cause calls to succeed during the day and night, but calls to fail in the early hours of the morning. Assuming the timestamp is 1551113065, the time in the East Eight District is 2019-02-26 00:44:25, but the calculated Date with UTC+0 should be 2019-02-25 instead of 2019-02-26.
> 2. Timestamp must be the current system time and ensure that the system time and standard time are synchronized. If the difference exceeds five minutes, it will fail. If it is not synchronized with the standard time for a long time, it may cause the request to fail after running for a period of time (return signature expiration error).

According to the above rules, the string to be signed in the example is as follows (for clarity,\nnewlines are

replaced by new lines printed):

```
TC3-HMAC-SHA256
1539084154
2018-10-09/cvm/tc3_request
91c9c192c14460df6c1ffc69e34e6c5e90708de2a6d282cccf957dbf1aa7f3a7
```

2.3. calculate the signature

1. Compute the derived signature key, pseudocode as follows

```
SecretKey = "Gu5t9xGARNpq86cd98joQYCN3EXAMPLE"
SecretDate = HMAC_SHA256("TC3" + SecretKey, Date)
SecretService = HMAC_SHA256(SecretDate, Service)
SecretSigning = HMAC_SHA256(SecretService, "tc3_request")
```

- SecretKey: Original SecretKey;
- Date: That is, the Date field information in Credential, as shown in the example above, is 2018-10-09.;
- Service: That is, the Service field information in Credential, as shown in the example above, is cvm;

2. Calculate the signature, pseudocode as follows

```
Signature = HexEncode(HMAC_SHA256(SecretSigning, StringToSign))
```

- SecretSigning: That is, the derivative signature key calculated above;
- StringToSign: That is, the character string to be signed calculated in step 2;

2.4. Splicing Authorization

Splice as follows Authorization:

```
Authorization =
    Algorithm + ' ' +
    'Credential=' + SecretId + '/' + CredentialScope + ', ' +
    'SignedHeaders=' + SignedHeaders + ', '
    'Signature=' + Signature
```

- Algorithm: Signature method, fixed as TC3-HMAC-SHA256;
- SecretId: SecretId in key pair;
- CredentialScope: See above, Scope of Voucher;
- SignedHeaders: See above, header information for participating signatures;
- Signature: signature value

According to the above rules, the values obtained in the example are:

```
TC3-HMAC-SHA256 Credential=AKIDEXAMPLE/Date/service/tc3_request, SignedHeaders=content-type;host, Signature=5da7a33f6993f0614b047e5df4582db9e9bf4672ba50567dba16c6ccf174c474
```

The final complete invocation information is as follows:

```
https://cvm.convergecloud.com/?Limit=10&Offset=0

Authorization: TC3-HMAC-SHA256 Credential=AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE/2018-10-09/cvm/tc3_request, SignedHeaders=content-type;host, Signature=5da7a33f6993f0614b047e5df4582db9e9bf4672ba50567dba16c6ccf174c474
Content-Type: application/x-www-form-urlencoded
Host: cvm.convergecloud.com
X-TC-Action: DescribeInstances
X-TC-Version: 2017-03-12
X-TC-Timestamp: 1539084154
X-TC-Region: luzon
```

3. signing failed

According to the actual situation, there are the following signature failure error codes, please handle according to the actual situation

error code	error description
AuthFailure.SignatureExpire	signature expiration
AuthFailure.SecretIdNotFound	key is not present
AuthFailure.SignatureFailure	signature error
AuthFailure.TokenFailure	token error
AuthFailure.InvalidSecretId	Illegal key (not cloud API key type)

4. Signature Demo

Java

```
import java.io.BufferedReader;
import java.io.InputStream;
```

```
import java.io.InputStreamReader;
import java.net.URL;
import java.text.SimpleDateFormat;
import java.util.Date;
import java.util.Map;
import java.util.TimeZone;
import java.util.TreeMap;
import javax.crypto.Mac;
import javax.crypto.spec.SecretKeySpec;
import javax.net.ssl.HttpsURLConnection;
import javax.xml.bind.DatatypeConverter;

import org.apache.commons.codec.digest.DigestUtils;

public class CloudAPITC3Demo {
    private final static String CHARSET = "UTF-8";
    private final static String ENDPOINT = "cvm.convergecloud.com";
    private final static String PATH = "/";
    private final static String SECRET_ID = "AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE";
    private final static String SECRET_KEY = "Gu5t9xGARNpq86cd98joQYCN3EXAMPLE";
    private final static String CT_X_WWW_FORM_URLENCODED = "application/x-www-form-urlencode
d";
    private final static String CT_JSON = "application/json";
    private final static String CT_FORM_DATA = "multipart/form-data";

    public static byte[] sign256(byte[] key, String msg) throws Exception {
        Mac mac = Mac.getInstance("HmacSHA256");
        SecretKeySpec secretKeySpec = new SecretKeySpec(key, mac.getAlgorithm());
        mac.init(secretKeySpec);
        return mac.doFinal(msg.getBytes(CHARSET));
    }

    public static void main(String[] args) throws Exception {
        String service = "cvm";
        String host = "cvm.convergecloud.com";
        String region = "luzon";
        String action = "DescribeInstances";
        String version = "2017-03-12";
        String algorithm = "TC3-HMAC-SHA256";
        String timestamp = "1539084154";
        //String timestamp = String.valueOf(System.currentTimeMillis() / 1000);
        SimpleDateFormat sdf = new SimpleDateFormat("yyyy-MM-dd");
        // Pay attention to the time zone, otherwise it is easy to make mistakes.
        sdf.setTimeZone(TimeZone.getTimeZone("UTC"));
        String date = sdf.format(new Date(Long.valueOf(timestamp + "000")));

        // ************* Step 1: Assemble the specification request string *************
```

```
        String httpRequestMethod = "GET";
        String canonicalUri = "/";
        String canonicalQueryString = "Limit=10&Offset=0";
        String canonicalHeaders = "content-type:application/x-www-form-urlencoded\n" + "host:" + host
+ "\n";
        String signedHeaders = "content-type;host";
        String hashedRequestPayload = DigestUtils.sha256Hex("");
        String canonicalRequest = httpRequestMethod + "\n" + canonicalUri + "\n" + canonicalQueryStri
ng + "\n"
                + canonicalHeaders + "\n" + signedHeaders + "\n" + hashedRequestPayload;
        System.out.println(canonicalRequest);

        // ************* Step 2: Stitching the string to be signed *************
        String credentialScope = date + "/" + service + "/" + "tc3_request";
        String hashedCanonicalRequest = DigestUtils.sha256Hex(canonicalRequest.getBytes(CHARSET));
        String stringToSign = algorithm + "\n" + timestamp + "\n" + credentialScope + "\n" + hashedCan
onicalRequest;
        System.out.println(stringToSign);

        // ************* Step 3: Calculate the signature *************
        byte[] secretDate = sign256(("TC3" + SECRET_KEY).getBytes(CHARSET), date);
        byte[] secretService = sign256(secretDate, service);
        byte[] secretSigning = sign256(secretService, "tc3_request");
        String signature = DatatypeConverter.printHexBinary(sign256(secretSigning, stringToSign)).toLow
erCase();
        System.out.println(signature);

        // ************* Step 4: Splicing Authorization *************
        String authorization = algorithm + " " + "Credential=" + SECRET_ID + "/" + credentialScope + ", "
                + "SignedHeaders=" + signedHeaders + ", " + "Signature=" + signature;
        System.out.println(authorization);

        TreeMap<String, String> headers = new TreeMap<String, String>();
        headers.put("Authorization", authorization);
        headers.put("Host", host);
        headers.put("Content-Type", CT_X_WWW_FORM_URLENCODED);
        headers.put("X-TC-Action", action);
        headers.put("X-TC-Timestamp", timestamp);
        headers.put("X-TC-Version", version);
        headers.put("X-TC-Region", region);
    }
}
```

Python

```
# -*- coding: utf-8 -*-
```

```
import hashlib, hmac, json, os, sys, time
from datetime import datetime

# key parameters
secret_id = "AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE"
secret_key = "Gu5t9xGARNpq86cd98joQYCN3EXAMPLE"

service = "cvm"
host = "cvm.convergecloud.com"
endpoint = "https://" + host
region = "luzon"
action = "DescribeInstances"
version = "2017-03-12"
algorithm = "TC3-HMAC-SHA256"
timestamp = 1539084154
date = datetime.utcfromtimestamp(timestamp).strftime("%Y-%m-%d")
params = {"Limit": 10, "Offset": 0}

# ************* Step 1: Assemble the specification request string *************
http_request_method = "GET"
canonical_uri = "/"
canonical_querystring = "Limit=10&Offset=0"
ct = "x-www-form-urlencoded"
payload = ""
if http_request_method == "POST":
    canonical_querystring = ""
    ct = "json"
    payload = json.dumps(params)
canonical_headers = "content-type:application/%s\nhost:%s\n" % (ct, host)
signed_headers = "content-type;host"
hashed_request_payload = hashlib.sha256(payload.encode("utf-8")).hexdigest()
canonical_request = (http_request_method + "\n" +
                     canonical_uri + "\n" +
                     canonical_querystring + "\n" +
                     canonical_headers + "\n" +
                     signed_headers + "\n" +
                     hashed_request_payload)
print(canonical_request)

# ************* Step 2: Stitching the string to be signed *************
credential_scope = date + "/" + service + "/" + "tc3_request"
hashed_canonical_request = hashlib.sha256(canonical_request.encode("utf-8")).hexdigest()
string_to_sign = (algorithm + "\n" +
                  str(timestamp) + "\n" +
                  credential_scope + "\n" +
                  hashed_canonical_request)
print(string_to_sign)
```

```
# ************* Step 3: Calculate the signature *************
# Compute signature digest function
def sign(key, msg):
    return hmac.new(key, msg.encode("utf-8"), hashlib.sha256).digest()
secret_date = sign(("TC3" + secret_key).encode("utf-8"), date)
secret_service = sign(secret_date, service)
secret_signing = sign(secret_service, "tc3_request")
signature = hmac.new(secret_signing, string_to_sign.encode("utf-8"), hashlib.sha256).hexdigest()
print(signature)

# ************* Step 4: Splicing Authorization *************
authorization = (algorithm + " " +
                 "Credential=" + secret_id + "/" + credential_scope + ", " +
                 "SignedHeaders=" + signed_headers + ", " +
                 "Signature=" + signature)
print(authorization)

# Common parameters added to request header
headers = {
    "Authorization": authorization,
    "Host": host,
    "Content-Type": "application/%s" % ct,
    "X-TC-Action": action,
    "X-TC-Timestamp": str(timestamp),
    "X-TC-Version": version,
    "X-TC-Region": region,
}
```

request

1. Service Address

Region refers to the geographical area of a physical data center. Converge Cloud ensures complete isolation between different regions, providing maximum stability and fault tolerance. To reduce access latency and improve download speed, it is recommended to choose the region closest to your customers.

You can view the complete region list by using the API interface "DescribeRegions".

2. Communications Protocol

All the Converge Cloud APIs communicate via HTTPS, providing highly secure communication tunnels.

3. Request Methods

Supported HTTP request methods:

- POST (recommended)
- GET

PThe Content-Type types supported by POST requests:

- application/json (recommended). The TC3-HMAC-SHA256 signature algorithm must be used.
- application/x-www-form-urlencoded. The HmacSHA1 or HmacSHA256 signature algorithm must be used.
- multipart/form-data (only supported by certain APIs). You must use TC3-HMAC-SHA256 to calculate the signature.

The size of a GET request packet is up to 32 KB. The size of a POST request is up to 1 MB when the HmacSHA1 or HmacSHA256 signature algorithm is used, and up to 10 MB when TC3-HMAC-SHA256 is used.

4. Character Encoding

Only UTF-8 encoding is used.

result

Response for Successful Requests

For example, when calling CAM API (version: 2017-03-12) to view the status of instances (DescribeInstancesStatus), if the request has succeeded, you may see the response as shown below:


```
{
    "Response": {
        "TotalCount": 0,
        "InstanceStatusSet": [],
        "RequestId": "b5b41468-520d-4192-b42f-595cc34b6c1c"
    }
}
```


- The API will return Response, which contains RequestId, as long as it processes the request. It does not matter if the request is successful or not.
- RequestId is the unique ID of an API request. Contact us with this ID when an exception occurs.
- Except for the fixed fields, all fields are action-specified. For the definitions of action-specified fields, see the corresponding API documentation. In this example, TotalCount and InstanceStatusSet are the fields specified by the API DescribeInstancesStatus. 0 TotalCount means that the requester owns 0 CVM instance so the InstanceStatusSet is empty.

Response for Failed Requests

If the request has failed, you may see the response as shown below:


```
{
    "Response": {
        "Error": {
            "Code": "AuthFailure.SignatureFailure",
            "Message": "The provided credentials could not be validated. Please check your signature is cor
rect."
        },
        "RequestId": "ed93f3cb-f35e-473f-b9f3-0d451b8b79c6"
    }
}
```


- The presence of the Error field indicates that the request has failed. A response for a failed request will include Error, Code and Message fields.

- Code is the code of the error that helps you identify the cause and solution. There are two types of error codes so you may find the code in either common error codes or API-specified error codes.
- Message explains the cause of the error. Note that the returned messages are subject to service updates. The information the messages provide may not be up-to-date and should not be the only source of reference.
- RequestId is the unique ID of an API request. Contact us with this ID when an exception occurs.

Common Error Codes

If there is an Error field in the response, it means that the API call failed. The Code field in Error indicates the error code. The following table lists the common error codes that all actions can return.

Error Code	Description
AuthFailure.InvalidSecretId	Invalid key (not a API key type).
AuthFailure.MFAFailure	MFA failed.
AuthFailure.SecretIdNotFound	The key does not exist.
AuthFailure.SignatureExpire	Signature expired.
AuthFailure.SignatureFailure	Signature error.
AuthFailure.TokenFailure	Token error.
AuthFailure.UnauthorizedOperation	The request does not have CAM authorization.
DryRunOperation	DryRun Operation. It means that the request would have succeeded, but the DryRun parameter was used.
FailedOperation	Operation failed.
InternalError	Internal error.
InvalidAction	The API does not exist.
InvalidParameter	Incorrect parameter.
InvalidParameterValue	Invalid parameter value.
LimitExceeded	Quota limit exceeded.
MissingParameter	A parameter is missing.
NoSuchVersion	The API version does not exist.

Error Code	Description
RequestLimitExceeded	The number of requests exceeds the frequency limit.
ResourceInUse	Resource is in use.
ResourceInsufficient	Insufficient resource.
ResourceNotFound	The resource does not exist.
ResourceUnavailable	Resource is unavailable.
UnauthorizedOperation	Unauthorized operation.
UnknownParameter	Unknown parameter.
UnsupportedOperation	Unsupported operation.
UnsupportedProtocol	hHTTPS request method error. Only GET and POST requests are supported.
UnsupportedRegion	API does not support the requested region.

PublicParameter

Common parameters are parameters used to identify users and interface authentication purposes. If not necessary, these parameters are not described in the separate interface document of each interface, but these parameters need to be carried in each request before the request can be normally initiated.

signature method v3

When using TC3-HMAC-SHA256 signature method, the common parameters need to be uniformly placed in the HTTP Header request header, as follows:

parameter name	type	required	described
X-TC-Action	String	Yes	The name of the operation interface. Refer to the description of the public parameter Action in the input parameters of the interface documentation for the value. For example, the value for the query instance list interface of the cloud server is DescribeInstances.
X-TC-Region	String	Yes	region parameters, Data used to identify which region you wish to operate on. The region value accepted by the interface refers to the description of the input parameter common parameter Region in the interface document. Note: Some interfaces do not need to pass this parameter, which is specifically stated in the interface documentation. In this case, even passing this parameter will not take effect.
X-TC-Timestamp	Integer	Yes	The current UNIX timestamp, which records the time when the API request was initiated. for example 1529223702. Note: If the time difference from the server exceeds 5 minutes, it will cause a signature expiration error.
X-TC-Version	String	Yes	Version of API for operation. Refer to the description of the public parameter Version in the interface document for the value. For example, the version of the cloud server. 2017-03-12.
Authorization	String	Yes	HTTP The standard authentication header field is "Authorization". For example: TC3-HMAC-SHA256 Credential=AKIDEXAMPLE/Date/service/tc3_request, SignedHeaders=content-type;host, Signature=fe5f80f77d5fa3beca038a248ff027d0445342fe2855ddc963176630326f1024 Here, - TC3-HMAC-SHA256: Signature method, currently fixed as this value, - Credential: Credential: Signature credential; AKIDEXAMPLE is the SecretId; Date is a date in UTC time, and this value must match the value of X-TC-Timestamp (a common parameter) in UTC time format; service is the name of the product/service, and is generally a domain name prefix. For example,cvm; - SignedHeaders: The headers that contains the authentication information; content-type and host are the required headers; - Signature: Signature digest.
X-TC-Token	String	No	The token used for temporary certificates needs to be used in conjunction with a temporary key. Temporary keys and tokens need to be obtained by calling the access management service interface. Long-term keys do not require tokens.

signature method v1

When using HmacSHA1 and HmacSHA256 signature methods, common parameters need to be placed uniformly in the request string, as follows

parameter name	type	required	described
Action	String	Yes	The name of the interface to be operated. The value refers to the explanation of the public parameter Action in the interface documentation. For example, for the cloud server's query instance list interface, the value is DescribeInstances .
Region	String	Yes	The region parameter is used to identify which region's data you want to operate on. The region value accepted by the interface is specified in the input parameter of the public parameter Region in the interface documentation. Note: Some interfaces do not require this parameter to be passed, which will be specifically mentioned in the interface documentation. Even if this parameter is passed, it will not take effect in this case.
Timestamp	Integer	Yes	The current UNIX timestamp, which can record the time when the API request is initiated. For example, 1529223702. If the difference between the current time is too large, it will cause a signature expiration error.
Nonce	Integer	Yes	A random positive integer combined with Timestamp is used to prevent replay attacks.
SecretId	String	Yes	The SecretId is an identifier applied for the cloud API key to identify the user's identity. A SecretId corresponds to a unique SecretKey , and the SecretKey is used to generate the request signature Signature .
Signature	String	Yes	Request signature is used to verify the legitimacy of this request. Users need to calculate it based on the actual input parameters. The specific calculation method can be found in the interface authentication documentation.
Version	String	Yes	The version of the API being operated on. The value refers to the description of the public parameter Version in the interface documentation. For example, the version of the cloud server. 2017-03-12.
SignatureMethod	String	No	Signature method, currently supports HmacSHA256 and HmacSHA1. HmacSHA256 algorithm is used to verify signatures only if this parameter is specified as HmacSHA 256, otherwise HmacSHA1 is used to verify signatures.
Token	String	No	Token used for temporary certificate needs to be used together with temporary key. The temporary key and Token need to be obtained from the Access Management service invocation interface. Long-term keys do not require tokens.

zone list

A region (Region) refers to the geographical area of a physical data center. Converge Cloud Translation: To deliver verification that completely isolates different regions, ensuring maximum stability and fault tolerance between regions. In order to reduce access latency and improve download speed, it is recommended that you choose the region closest to your customers.

You can view the complete region list by using the API interface Query Region List.

CDH APIs
DescribeZoneHostConfigInfos

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

Obtain CDH model configuration information and a list of information about the sell-out state.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-04-19 03:59:28.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeZoneHostConfigInfos
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
Filters	Yes	No	Array of Filter	Filtering criteria in the availability zone, supports two filtering criteria: zone and host-charge-type. Example:View

3. Output Parameters

Parameter name	Type	Description
HostTypeConfigSet	Array of HostTypeConfigSet	List of CDH Model Configuration Information Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidZone.MismatchRegion	The specified zone does not exist.

Error Code	Description
MissingParameter	Parameters are missing. The request did not include mandatory parameters.
InvalidRegion.NotFound	The specified zone was not found.
InvalidFilter	Invalid filter.

InquiryPriceAllocateHosts

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

Inquire about Price for Creating CDH Instance (When HostChargeType is PREPAID, you must specify the HostChargePrepaid parameter.)
Version 3100 and later versions only support the postpaid mode, but do not support the prepaid mode. Passing prepaid parameters will result in an error.

Default interface request rate limit: 10 times per second.

Interface update time: 2022-05-21 06:19:38.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: InquiryPriceAllocateHosts
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
ClientToken	No	No	String	String used to ensure request idempotency. Example: 4668722c-b6d6-4f79-96fd-097ebe5318e5
Placement	Yes	No	Placement	Location of the instance. You can specify attributes such as the availability zone and project to which the instance belongs through this parameter. Example:View
HostChargePrepaid	No	No	ChargePrepaid	Prepaid mode, that is, monthly subscription- related parameter settings. You can specify attributes of a monthly subscription instance, such as purchase duration and whether to set auto-renewal, through this parameter. If the billing mode of the specified instance is prepaid mode, this parameter is required. Example:View
HostChargeType	Yes	No	String	Instance billing type. Currently, PREPAID (prepaid, that is, a monthly subscription mode) and POSTPAID_BY_HOUR (pay-per- hour postpaid) are supported. If this parameter is not passed, postpaid by default. Example: PREPAID
HostType	Yes	No	String	CDH instance model. If this parameter is not passed, the default model is HS20. Example: HS1
HostCount	No	No	Uint64	Number of purchased CDH instances. Example: 1
DryRun	No	No	Bool	Whether to skip the actual execution logic. Example: false
PurchaseSource	No	No	String	Purchase source, API and MC (MC indicates front-end call). Example: MC

3. Output Parameters

Parameter name	Type	Description
Price	HostPrice	Price Information of CDH Instance Creation Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidRegion.NotFound	The specified zone was not found.
InvalidPeriod	Invalid duration. Currently, only the following durations are supported: [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 24, 36], unit: months.
InvalidProjectId.NotFound	Invalid project ID. The specified project ID does not exist.
InvalidZone.MismatchRegion	The specified zone does not exist.

TerminateHosts

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

Used to proactively return the CDH.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-10-28 03:50:02.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: TerminateHosts
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
HostIds	Yes	No	Array of String	One or more CDH instance IDs to be operated. Example: ["host-ey16rkyg\r\n"]
DryRun	No	No	Bool	Whether to skip the actual execution logic. Example: DesAction

3. Output Parameters

Parameter	Type	Description

name		
TaskId	String	Task ID Example: 543225
flowId	Int64	Task Flow ID Example: 2
FlowId	Int64	Task Flow ID Example: 2
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidHostId.NotFound	The specified HostId does not exist, or does not belong to the requesting account.
InvalidHostId.Malformed	Invalid CDH ID. The format of the specified CDH ID is incorrect, for example, an ID length error host-1122 .
MissingParameter	Parameters are missing. The request did not include mandatory parameters.
InvalidHost.NotSupported	The specified operation is not supported by this host instance.

Image APIs
CreateImage

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

This API (CreateImage) is used to create a new image from the system disk of an instance. The created image can be used to create instances.

Default interface request rate limit: 10 times per second.

Interface update time: 2022-10-28 03:48:25.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CreateImage
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
InstanceId	No	No	String	Instance ID for Which Image Needs to be Created Example: ins-2v3sqe2t
ImageName	Yes	No	String	Image name Example: MyImageName
ImageDescription	No	No	String	Description Example: MyImageDescription
ForcePoweroff	No	No	String	Whether to perform forced shutdown to create an image when a soft shutdown fails. Example: true
Sysprep	No	No	String	Whether to enable Sysprep when creating a Windows image. Example: false
Reboot	No	No	String	Whether it is allowed to perform the image creation task in the shutdown state when the instance is in the running state. Example: false
DataDiskIds	No	No	Array of String	When creating a full machine image based on an instance, specify the data disk ID included in the image. Example: ["disk-6gabakqz"]
SnapshotIds	No	No	Array of String	Create an image based on a snapshot, specifying the snapshot ID should include a system disk snapshot. Should not be passed in with InstanceId at the same time. Example: ["snap-kso6f712", "snap-l3rrf322"]
DryRun	No	No	Bool	Detect whether this request is successful, but it will not affect the operated resources. Example: false
SoftPoweroff	No	No	Array of String	Whether to perform soft shutdown to make an image. Example: false
DedicatedClusterId	No	No	String	ID of a local dedicated cluster Example: cluster-d8htgb6k

3. Output Parameters

Parameter name	Type	Description
ImageId	String	Image ID Example: img-2v3sqe2t
TaskId	String	Task ID Example: 4532455
flowId	Int64	Task Flow ID Example: 2
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidInstanceId.NotFound	No corresponding instance was found.
ImageQuotaLimitExceeded	The image quota has exceeded the limit.
InvalidInstance.NotSupported	Unsupported instance.
InvalidImageName.Duplicate	The image name is the same as the existing image.
InvalidParameter.ValueTooLarge	The parameter length exceeds the limit.

Error Code	Description
MutexOperation.TaskRunning	The same task is already running.

DeleteImages

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

This API (DeleteImages) is used to delete one or more images.

- When the Image Status is CREATING and USING , deletion is not allowed. The image status can be obtained through DescribeImages.
- Each region supports creating a maximum of 10 custom images. Deleting images can free up the quota of your account.
- When an image is being shared with other accounts, it cannot be deleted.

Default interface request rate limit: 10 times per second.

Interface update time: 2022-10-28 03:49:19.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteImages
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
ImageIds	Yes	No	Array of String	List of Image IDs to Be Deleted Example: ["img-34vaef8fe"]

3. Output Parameters

Parameter name	Type	Description
TaskId	String	Task ID Example: 543r242
flowId	Int64	Task Flow ID Example: 2
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidImageId.InShared	The image is being shared.
InvalidImageId.IncorrectState	The image status is illegal.
InvalidImageId.NotFound	Image not found
InvalidImageId.Malformed	Invalid image ID

DescribeImageQuota

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

This API (DescribeImageQuota) is used to query the image quota of a user account.

Default interface request rate limit: 10 times per second.

Interface update time: 2018-04-04 09:23:06.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeImageQuota
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface

3. Output Parameters

Parameter name	Type	Description
ImageNumQuota	Int64	Image Quota of Account Example: 1000
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

There is no error code related to business logic for this interface, For other error codes, see public ErrorCode.

DescribeImageSharePermission

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

This API (DescribeImageSharePermission) is used to view image sharing information.

Default interface request rate limit: 10 times per second.

Interface update time: 2022-11-16 03:09:47.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeImageSharePermission
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
ImageId	Yes	No	String	Image ID Needs to be Shared Example: img-6pb6lrmy

3. Output Parameters

Parameter name	Type	Description
SharePermissionSet	Array of SharePermission	Image Sharing Information Example:View

Parameter name	Type	Description
MaxSharePermission	Int64	Maximum Shared Permissions Example: 2
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidAccountId.NotFound	Invalid account ID
InvalidAccountIs.YourSelf	You cannot share an image with yourself.
OverQuota	The maximum number of shared images allowed is reached
InvalidImageId.NotFound	Image not found

DescribeImageSnapshotStatus

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

This API has been discontinued for maintenance from May 11, 2022.
This API (DescribeImageSnapShotStatus) is used to query whether the image has a snapshot.

Default interface request rate limit: 10 times per second.

Interface update time: 2022-05-12 06:35:16.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeImageSnapshotStatus
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
ImageId	Yes	No	String	Image ID Needs to be Viewed Example: img-61dyt49h

3. Output Parameters

Parameter name	Type	Description
CbsStatus	String	Snapshot status. There are the following three statuses: NORMAL, CREATING, and NULL. Example: NORMAL
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidImageId.NotFound	Image not found
InternalError	Internal error

DescribeImages

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

This API (DescribeImages) is used to view the list of images.

- You can query detailed information of a specified image by specifying an image ID, or query detailed information of an image that meets the filtering criteria by configuring a filter. (This API does not support querying public image IDs.)
- Specify an offset (Offset) and limit (Limit) to select a portion of the results. Return the first 20 images that meet the criteria by default.

Default interface request rate limit: 10 times per second.

Interface update time: 2022-04-23 09:51:31.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeImages
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
ImageIds	No	No	Array of String	List of image IDs, such as img-gvbnzy6f . For the format for array parameters, see API Introduction. You can obtain the image ID in the following ways: • Through the ImageId returned by the API DescribeImages. • Through the DescribeImages. Example: ["img-gvbnzy6f"]
Filters	No	No	Array of Filter	Filtering criteria. A maximum of filters is 10, and a maximum of Filters.Values is 5. Note: You should not specify ImageIds and Filters at the same time. Optional values include image-id and image-type . Example:View
Offset	No	No	Uint64	Offset, 0 by default. For details of the offset, see API Introduction. Example: 0
Limit	No	No	Uint64	Quantity limit, 20 by default, and the maximum value is 100. For details of the Limit, see API Introduction. Example: 20
InstanceType	No	No	String	Filters out the images that do not match the instance type specifications, such as S1.SMALL1 and S1.SMALL2. Example: "S1.SMALL1"
HostIp	No	No	String	Host IP, used to filter images when creating CDH instances. Example: 12.0.11.22

3. Output Parameters

Parameter name	Type	Description
ImageSet	Array of Image	A structure about detailed information of an image, mainly includes the main status and attributes of the image. Example:View
TotalCount	Int64	Number of eligible images. Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidFilter	Invalid filter.
InvalidParameterValue.InvalidParameterValueLimit	Parameter value error.
InvalidParameter.InvalidParameterCoexistImageIdsFilters	You should not specify both ImageIds and Filters at the same time.

DescribeImportImageOs

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

View information of importable image operating systems.

Default interface request rate limit: 288 times per second.

Interface update time: 2022-05-21 06:17:10.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeImportImageOs
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface

3. Output Parameters

Parameter name	Type	Description
ImportImageOsListSupported	ImportImageOsListSupported	List of operating systems supported by the imported images. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

There is no error code related to business logic for this interface, For other error codes, see public ErrorCode.

ImportImage

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

This API (ImportImage) is used to import images. The imported images can be used to create instances.

Default interface request rate limit: 10 times per second.

Interface update time: 2022-10-28 03:52:47.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ImportImage
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
Architecture	Yes	No	String	Operating system architecture of imported images, x86_64 or arm_64 . Example: x86_64
OsType	Yes	No	String	Operating system type of imported images, obtained through DescribeImportImageOs . Example: CentOS
OsVersion	Yes	No	String	Operating system version of imported image, obtained through DescribeImportImageOs . Example: 6
ImageUrl	Yes	No	String	COS Address Where Imported Image is Stored Example: http://111-1251433127.cosd.convergecloud.com/Windows%20Server%202008%20R2%20x64a.vmdk
ImageName	Yes	No	String	Image name. The image name should not be the same as the name of any existing custom images, and no more than 60 characters. Example: sample
ImageDescription	No	No	String	Description Example: sampleimage
DryRun	No	No	Bool	Check parameters only, do not execute task. Example: false
Force	No	No	Bool	Whether to forcibly import, see Forcibly Import Image Example: false
PublicImage	No	No	Bool	Whether to import a public image. Set to true to import a public image and follow the imagestage process. Default value is false ; Example: true

3. Output Parameters

Parameter name	Type	Description
ImageId	String	Image ID Example: img-c1otssej
TaskId	String	Task ID Example: 432322
flowId	Int64	Task Flow ID Example: 3
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
FailedOperation.NoAvailablePublicImage	No available public images.
FailedOperation.NoQuotaForUserInstance	Insufficient quota to create an instance.
FailedOperation.NoAvailableInstanceFamily	No available instance families.

Error Code	Description
FailedOperation.NoAvailableInstanceType	No available instance types.
FailedOperation.NoAvailableIpAddressCount	The subnet has no available IP addresses.
FailedOperation.NoAvailableCbs	No available CBS resources.
FailedOperation.NoCVMPermission	No instance operation permissions.
FailedOperation.NoAvailableVpc	There are no available VPC resources.
FailedOperation.NoAvailableSubnet	There are no available subnet resources.
FailedOperation.NoAvailableSecurityGroup	No available security groups.
ImageQuotaLimitExceeded	The image quota has exceeded the limit.
InvalidImageName.Duplicate	The image name is the same as the existing image.
InvalidImageOsVersion.Unsupported	Unsupported operating system version.
InvalidParameter.InvalidParameterUrlError	Incorrect URL address.
RegionAbilityLimit.UnsupportedToImportImage	This region does not support importing images.
InvalidImageOsType.Unsupported	Unsupported operating system type.
MissingParameter	Parameters are missing. The request did not include mandatory parameters.

ModifyImageAttribute

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

This API (ModifyImageAttribute) is used to modify image attributes.

- Attributes of shared images cannot be modified.

Default interface request rate limit: 10 times per second.

Interface update time: 2018-04-04 09:23:06.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyImageAttribute
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
ImageId	Yes	No	String	Image ID, in the format of img-gvbnzy6f . You can obtain the image ID in the following ways: • Through the ImageId returned by the API DescribeImages. • Through the DescribeImages. Example: img-6pb6lrmy
ImageName	No	No	String	Set a new image name. It should meet the following restrictions: • Should not exceed 20 characters. • The image name should not be the same as the name of existing images. Example: sample
ImageDescription	No	No	String	Set a new image description. It should meet the following restrictions: • Should not exceed 60 characters. Example: sample

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameter.ValueTooLarge	The parameter length exceeds the limit.
InvalidImageName.Duplicate	The image name is the same as the existing image.
InvalidImageId.IncorrectState	The image status is illegal.
InvalidImageId.NotFound	Image not found
InvalidImageId.Malformed	Invalid image ID

ModifyImageSharePermission

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

This API is used to modify image sharing information.

- After an image is shared, the receiver's account can create an instance through the image.
- Each custom image can be shared with a maximum of 500 accounts.
- Names and descriptions of shared images cannot be changed. They can only be used to create instances.
- Sharing is only supported within the same region as that of the receiver's account.

Default interface request rate limit: 10 times per second.

Interface update time: 2018-04-04 09:23:06.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyImageSharePermission
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
ImageId	Yes	No	String	Image ID, in the format of img-gvbnzy6f . You can obtain the Image ID in the following ways: • Through the ImageId returned by the API DescribeImages. • Through the DescribeImages. The Image ID should be specified as an image in the NORMAL state. For the image status, see the Image Data Table. Example: img-6pb6lrmy
AccountIds	Yes	No	Array of String	List of account IDs receiving shared images, for the format of array parameter, see API Introduction. The account ID is different from the QQ number. For querying the user account ID, see the account ID column in the Account Information. Example: ["103849387508"]
Permission	Yes	No	String	Operations, including SHARE and CANCEL . SHARE represents sharing, and CANCEL represents canceling sharing. Example: SHARE

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidAccountId.NotFound	Invalid account ID
InvalidAccountIs.YourSelf	You cannot share an image with yourself.
OverQuota	The maximum number of shared images allowed is reached

SyncImages

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

This API (SyncImages) is used to synchronize custom images to other regions.

- This API supports synchronizing only one image per call.
- This API supports multiple synchronization regions.
- A single account can have a maximum of 10 custom images in each region.

Default interface request rate limit: 10 times per second.

Interface update time: 2018-04-04 09:23:06.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: SyncImages
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
ImageIds	Yes	No	Array of String	List of image IDs. You can obtain the image ID in the following ways: • Through the ImageId returned by the API DescribeImages. • Through the DescribeImages. The image ID should meet the following restrictions: • The image status corresponding to the image ID should be NORMAL . • The image size is less than 50 GB. For image statuses, see the Image Data Table. Example: ["img-o3ycss2p"]
DestinationRegions	Yes	No	Array of String	List of destination synchronization regions; it must meet the following restrictions: • Should not be the source region, • Must be a valid Region. • Partial region synchronization is not supported at this time. For specific region parameters, see Region. Example: ["ap-region1"]

3. Output Parameters

Parameter name	Type	Description
ImageSet	Array of ImageSet	Image collection. Example:View

Parameter name	Type	Description
TaskId	String	Task ID Example: task-6a79x94v
flowId	String	Process ID Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidImageId.IncorrectState	The image status is illegal.
InvalidImageId.NotFound	Image not found
InvalidImageId.TooLarge	The image size exceeds the limit.
InvalidRegion.NotFound	The specified zone was not found.
InvalidRegion.Unavailable	Currently, this zone does not support synchronizing an image.
InvalidParameterValue.InvalidImageId	The image ID is invalid.
InvalidImageName.Duplicate	The image name is the same as the existing image.

Instance APIs
CloneInstance

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

This API (CloneInstance) is used to clone an instance with a specified configuration.

- After an instance is successfully created, it will automatically start up, and the Instance Status will change to Running.
- The purchase of prepaid instances will deduct the amount required for the instance purchase in advance. The purchase of pay-per-hour postpaid instances will freeze the amount required for the instance purchase within 1 hour in advance. Make sure your account balance is sufficient before calling this API.
- This API is an asynchronous API. After the creation request is successfully sent, a list of instance IDs will be returned. At this point, the creation of the instance is not immediately completed. During this period, the instance status will be Preparing. You can query the status of the corresponding instance by calling the API DescribeInstancesStatus to determine whether the production ultimately succeeded. If the instance status changes from Preparing to Running, it indicates that the instance is successfully created.

Default interface request rate limit: 10 times per second.

Interface update time: 2025-08-05 00:55:05.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CloneInstance
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
InstanceChargeType	No	No	String	Instance billing type. PREPAID: Prepaid, which is monthly subscription. POSTPAID_BY_HOUR: Pay-as-you-go on an hourly basis. CDHPAID: Dedicated host billing (created based on CVM Dedicated Host (CDH) and resources of the host not charged). In this billing mode, you must fill in the default value of placement.hostid parameter: POSTPAID_BY_HOUR. Example: PREPAID
InstanceChargePrepaid	No	No	InstanceChargePrepaid	Prepaid mode, that is, monthly subscription-related parameter settings. You can specify attributes of a monthly subscription instance, such as purchase duration and whether to set auto-renewal, through this parameter. If the billing mode of the specified instance is prepaid mode, this parameter is required. Example:View
Placement	Yes	No	Placement	Location of the instance. You can specify attributes such as availability zone, project, and CDH (for creating a instance with a dedicated host billing mode) to which the instance belongs through this parameter. Example:View
InstanceType	No	No	String	Instance model. Different instance models specify different resource specifications. • For creating a instance with billing mode as PREPAID or POSTPAID_BY_HOUR, you can obtain the specific values by calling the API DescribeInstanceTypeConfigs to obtain the latest specification table or seeing the description of the Instance Types. If this parameter is not specified, the default model is S1.SMALL1. • For creating a instance with billing mode as CDHPAID, this parameter starts with a prefix CDH_ and is generated based on the CPU and memory configurations. Its specific form is CDH_XCXG. For example, for creating a CDH instance with 1 core CPU and 1 GB memory, this parameter should be CDH_1C1G. Example: S2.SMALL1
ImageId	Yes	No	String	Specifies a valid Image ID in the formats such as img-xxx. There are four types of images: 1. Public Image 2. Custom Image 3. Shared Image 4. Service Market Image. The IDs of the Public Image, Custom Image, and Shared Image can be found by logging in to the Console. The ID of the Service Market Image can be found in the Cloud Marketplace. By calling the DescribeImages API and inputting InstanceType, you can get the list of images supported by the current r Example: img-c1otswj
PurchaseSource	No	No	String	Purchase Source Example: MC
SystemDisk	No	No	SystemDisk	Instance system disk configuration information. If this parameter is not specified, it will be assigned based on the system default values. Example:View
DataDisks	No	No	Array of DataDisk	Instance data disk configuration information. If this parameter is not specified, no data disks are purchased by default. Specifying multiple data disks when purchasing is supported. Example:View
VirtualPrivateCloud	No	No	VirtualPrivateCloud	VPC-related information configuration. You can specify information such as VPC ID and subnet ID through this parameter. If this parameter is not specified, use the basic network by default. If a VPC IP is specified in this parameter, the InstanceCount parameter can be 1 or 2. Example:View
InternetAccessible	No	No	InternetAccessible	Public bandwidth-related settings. If this parameter is not specified, the public bandwidth is 0 Mbps by default. Example:View
InstanceCount	No	No	Int64	Number of instances to purchase. Value range: [1,100]. Default value: 1. The specified number of instances to purchase should not exceed the remaining quota of the user. Example: 12
InstanceName	No	No	String	Instance display name. If not specified, it will be displayed as unnamed by default. A maximum of 60 characters are supported. Names after a period will be filtered out. Example: alice-1
LoginSettings	No	No	LoginSettings	Instance login settings. You can set login method, password, or key of the instance or retain the original login settings of the image. By default, a password will be randomly generated and notified to the user through Message Center. Example:View
SecurityGroupIds	No	No	Array of String	Security groups to which an instance belongs. If this parameter is not specified, bind the security group by default. Example: ["sec-61dyt49h"]
EnhancedService	No	No	EnhancedService	Enhanced services. You can specify whether to enable services such as Cloud Security and Cloud Monitor through this parameter. If this parameter is not specified, the Cloud Monitor and Cloud Security is enabled by default. Example:View
ClientToken	No	No	String	String used to ensure request idempotency. This string is generated by the customer and should be unique across different requests. The maximum length should be no more than 64 ASCII characters. If this parameter is not specified, the idempotency of the request cannot be ensured. Example: 123asfa423fdasq5twerra
SpotPrice	No	No	String	Used to specify price production, currently mainly used to spot instances. Example: 2050
HostName	No	No	String	The HostName for Cloud Virtual Machine (CVM) cannot have a dot (.) or hyphen (-) at the beginning or end, and they can not be used consecutively. Windows instances: The name must have [2, 15] characters, which can include letters (case insensitive), numbers, and hyphens (-), but cannot include dots (.) or be comprised entirely of numbers. Other types of instances (such as Linux): The name must have [2, 60] characters, which can include multiple dots, and each Example: alice-host
UserData	No	No	String	User data provided for the instance, should be encoded in base64 format, supports a maximum data size of 16 KB. Example: 3yEvYmluL2lhc2gKZWNobyAiSGVsbG8gVGAuY2VudCBDbG91ZC4Cgo=
DisasterRecoverGroupIds	No	No	Array of String	Placement group ID, only one can be specified. Example: ["ps-l8bo662s"]
TagSpecification	No	No	Array of TagSpecification	List of tag descriptions. You can bind tags to corresponding resource instances at the same time by specifying this parameter. Currently, only binding tags to the CVM is supported. Example:View
ProjectSpecification	No	No	ProjectSpecification	Specified project ID, only one can be specified. Example:View
InstanceId	Yes	No	String	Instance ID Needs to Be Cloned Example: ins-61dyt49h
DataDiskIds	Yes	No	Array of String	Data Disk ID Needs to be Cloned for Instance Example: ["disk-61dyt49h"]
DisableApiTermination	No	No	Bool	Whether to allow instance deletion through the API. Example: false

3. Output Parameters

Parameter name	Type	Description
InstanceIdSet	Array of String	When creating an instance through this API, this parameter will be returned, indicating one or more instance IDs. Returning a list of instance IDs does not indicate that the instance is successfully created. You can determine whether the creation is completed by querying the status of the corresponding instance ID in the returned InstancesSet through the API DescribeInstancesStatus. If the instance status changes from Preparing to Running, it indicates that the instance is successfully created. Example: ["ins-61dyt49h"]
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidPermission	The account does not support this operation.
InvalidParameterValue	Invalid parameter value. The format of the parameter value is incorrect or not supported, etc.
InvalidParameterValue.Range	Invalid parameter value. The range of the parameter value is not legal.
InvalidInstanceType.Malformed	The parameter format of the specified InstanceType is invalid.
InvalidPeriod	Invalid duration. Currently, only the following durations are supported: [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 24, 36], unit: months.
VpcIpInUsed	The VPC IP has already been used.
VpcAddrNotInSubNet	The VPC IP is not within the subnet.
InvalidClientToken.TooLong	The string length of the specified ClientToken exceeds the limit. It should be less than or equal to 64 bytes.
InvalidHostId.NotFound	The specified HostId does not exist, or does not belong to the requesting account.
MissingParameter	Parameters are missing. The request did not include mandatory parameters.
InstancesQuotaLimitExceeded	It indicates that the number of instances being created exceeds the remaining quota allowed for purchase by the account.
InvalidParameterCombination	It indicates that the parameter combination is incorrect.
InvalidParameterInvalidIpFormat	The specified VPC IP format is incorrect.
InvalidZone.MismatchRegion	The specified zone does not exist.
AccountQualificationRestrictions	The requesting account did not pass the qualification audit.
InvalidPassword	Invalid password. The specified password does not meet password complexity restrictions. For example, the password length does not meet restrictions.
InvalidInstanceName.TooLong	The string length of the specified InstanceName exceeds the limit. It should be less than or equal to 60 bytes.
InvalidCloudDisk.SoldOut	The cloud disk has been sold out.
TradeUnknownError	Billing request error
UnauthorizedOperation.ProjectNotFound	This operation is not allowed. Please ensure this account is in the selected project.

CreateDiagnosticReports

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

Create Instance Detection Report

Default interface request rate limit: 20 times per second.

Interface update time: 2023-07-13 07:03:34.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CreateDiagnosticReports
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
InstanceIds	Yes	No	Array of String	Instance ID Array Example: ["ins-rfmme2si"]
DeepDiagnose	No	No	Bool	Whether to perform deep detection. Example: true
Force	No	No	Bool	Whether to be strict. Example: true

3. Output Parameters

Parameter name	Type	Description
DiagnosticReportSet	Array of DiagnosticReportSet	Instance Detection Report Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error
InvalidInstanceId.NotFound	No corresponding instance was found.

CreateDisasterRecoverGroup

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

Create a spread placement group. This feature poses a significant challenge to resources, so use it cautiously. You can specify a created spread placement group when creating an instance.

Default interface request rate limit: 10 times per second.

Interface update time: 2022-04-29 02:47:53.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CreateDisasterRecoverGroup
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
Name	Yes	No	String	Placement group name, with a length of 1-60 characters, supporting and English. Example: Physical machine disaster recovery group
Type	Yes	No	String	Placement group type. Valid values: • HOST: Physical machine • SW: Switch • RACK: Rack Example: HOST
Strategy	No	No	String	Placement group policy. Valid values: • SPREAD: Anti-affinity • WEAK_SPREAD: Weak Anti-affinity • AFFINITY: Affinity • WEAK_AFFINITY: Weak Affinity Example: SPREAD

3. Output Parameters

Parameter name	Type	Description
DisasterRecoverGroupId	String	Spread placement group ID. Example: ps-qajfd25h
Type	String	Spread placement group type, consistent with the input parameter. Example: HOST
Name	String	Spread placement group name, contains 1 character to 60 characters and supports English characters. Example: Physical machine disaster recovery group
CvmQuotaTotal	Int64	Number of cloud servers that can be accommodated in the placement group. Example: 50
Strategy	String	Placement group policies Example: SPREAD
CurrentNum	Int64	Number of existed cloud servers in the placement group. Example: 0
CreateTime	Datetime_iso	Placement group creation time. Example: 2018-06-08T07:26:38Z
owner	String	AppId for Creating Placement Group Example: 122500001
Affinity	Int64	Placement group affinity. Instances in the placement group are distributed according to the affinity. Value range of affinity: 1-10. The default value is 1. Example: 1
PartitionCount	Int64	Number of partitions in partition placement groups. Value range: 2-10. The value is required when the placement group type is partition placement group. Example: 3
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.OutOfRange	The parameter value is out of range.

DeleteDisasterRecoverGroup

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

Delete the disaster recovery group. Only empty disaster recovery groups can be deleted.

Default interface request rate limit: 10 times per second.

Interface update time: 2019-11-21 02:58:48.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteDisasterRecoverGroup
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
DisasterRecoverGroupIds	Yes	No	Array of String	List of disaster recovery group IDs, can be queried through the API DescribeDisasterRecoverGroups. Example: ["ps-3a5sdgq5"]

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.LimitExceeded	The parameter value is out of range

DeleteDisasterRecoverGroups

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

This API (DeleteDisasterRecoverGroups) is used to delete the Spread Placement Group. Only empty placement groups can be deleted. For non-empty groups, all cloud servers in the group should be terminated first before the group can be deleted. Otherwise, it will result in a failure to delete the placement group.

Default interface request rate limit: 20 times per second.

Interface update time: 2020-05-15 13:25:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteDisasterRecoverGroups
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
DisasterRecoverGroupIds	Yes	No	Array of String	List of spread placement group IDs, can be obtained through the API DescribeDisasterRecoverGroups. A maximum of 100 spread placement groups per request are allowed. Example: ["ps-58l1hu01\r\n"]

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.LimitExceeded	The parameter value is out of range
FailedOperation.PlacementSetNotEmpty	The placement group is not empty.

DescribeDiagnosticReports

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

Query detailed information of the instance detection report.

Default interface request rate limit: 20 times per second.

Interface update time: 2023-07-13 07:18:09.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeDiagnosticReports
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
ReportIds	No	No	Array of String	Report ID Example: ["dr-rfmme2si"]
Filters	No	No	Array of Filter	Filter Criteria Example:View
Offset	No	No	Int64	Offset, 0 by default. Example: 0
Limit	No	No	Int64	Number of returns, 20 by default, and the maximum value is 100. Example: 5

3. Output Parameters

Parameter name	Type	Description
DiagnosticReportDataSet	Array of DiagnosticReportDataSet	DiagnosticReportDataSet Example:View
TotalCount	Int64	Total Number of Reports Example: 100
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

There is no error code related to business logic for this interface, For other error codes, see public ErrorCode.

DescribeDisasterRecoverGroupQuota

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

Query Placement Group Quota

Default interface request rate limit: 20 times per second.

Interface update time: 2022-11-11 11:07:43.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeDisasterRecoverGroupQuota
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
Strategy	No	No	String	Placement group policies Example: SPREAD

3. Output Parameters

Parameter name	Type	Description
GroupQuota	Int64	Maximum number of placement groups that can be created. Example: 10
CurrentNum	Int64	Number of placement groups the current user has created. Example: 25
CvmInHostGroupQuota	Int64	Quota number of instances in the disaster recovery group of the physical machine type. Example: 50
CvmInSwGroupQuota	Int64	Quota number of instances in the disaster recovery group of the switch type. Example: 20
CvmInRackGroupQuota	Int64	Quota number of instances in the disaster recovery group of the rack type. Example: 30

Parameter name	Type	Description
CvmInGroupQuota	Int64	Quota number of instances in the placement group. Example: 50
Strategy	String	Placement group policies Example: SPREAD
CvmInSwitchGroupQuota	Int64	Instance quota in the disaster recovery group of the switch type. Example: 20
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

There is no error code related to business logic for this interface, For other error codes, see public ErrorCode.

DescribeDisasterRecoverGroups

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

This API is used to query the placement group information.

Default interface request rate limit: 10 times per second.

Interface update time: 2022-04-25 03:34:57.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeDisasterRecoverGroups
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
DisasterRecoverGroupIds	No	No	Array of String	List of spread placement group IDs. Example: ps-21q9ibvr
Name	No	No	String	Spread placement group name, supports fuzzy matching. Example: myGroup
Offset	No	No	Int64	Offset. Default value: 0. For more information on Offset , see the relevant section in API Introduction. Example: 1
Limit	No	No	Int64	Number of returned items. Default value: 20. Maximum value: 100. For more information on Limit , see the relevant section in API Introduction. Example: 2
Strategies	No	No	Array of String	List of placement group policies Example: ["SPREAD"]

3. Output Parameters

Parameter name	Type	Description
DisasterRecoverGroupSet	Array of DisasterRecoverGroup	Disaster recovery group information list Example:View
TotalCount	Int64	Total number of user placement groups. Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

There is no error code related to business logic for this interface, For other error codes, see public ErrorCode.

DescribeInstanceConfigInfos

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

This API (DescribeInstanceConfigInfos) is used to obtain static configuration information of an instance, including the number of CPU cores, CPU model, memory size, and bandwidth information, etc.

Default interface request rate limit: 40 times per second.

Interface update time: 2022-02-15 07:27:15.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeInstanceConfigInfos
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
Filters	No	No	Array of Filter	instance-family Filter by the [instance model series]. The instance model series is in the format of S1, I1, M1, etc. Type: String Required: No instance-type Filter by the [instance model]. Different instance models specify different resource specifications. You can obtain the specific values by calling the API DescribeInstanceTypeConfigs to obtain the latest specification table or seeing the description of the instance types. If this parameter is not specified, the default model is S1.SMALL1. Type: String Required: No type Filter by the [instance family]. The instance family is in the format of S, I, M, etc. Type: String Required: No Example:View

3. Output Parameters

Parameter name	Type	Description
InstanceConfigInfos	Array of InstanceConfigInfoItemArchitecture	List of static configuration information of an instance. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidFilter	Invalid filter.
InvalidFilterValue.LimitExceeded	The number of Filter> Filter parameter values exceeds the limit.
InvalidParameter	Invalid parameter. The parameter does not meet the requirements, is not supported, or the like.

DescribeInstanceFamilyConfigs

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

This API (DescribeInstanceFamilyConfigs) is used to query list information of the model family supported by the current user and region.

Default interface request rate limit: 10 times per second.

Interface update time: 2018-04-04 09:23:06.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeInstanceFamilyConfigs
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface

3. Output Parameters

Parameter name	Type	Description
InstanceFamilyConfigSet	Array of InstanceFamilyConfig	List Information of Instance Model Group Configuration Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidRegion.NotFound	The specified zone was not found.
InvalidParameterValue	Invalid parameter value. The format of the parameter value is incorrect or not supported, etc.
InternalServerError	Internal operation error.

DescribeInstanceInternetBandwidthConfigs

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

This API (DescribeInstanceInternetBandwidthConfigs) is used to query instance bandwidth configurations.

- Only querying bandwidth configurations billed by the BANDWIDTH_PREPAID billing mode is supported.
- The API returns all bandwidth configuration information (including historical bandwidth configurations) of the instance.

Default interface request rate limit: 10 times per second.

Interface update time: 2018-04-04 09:23:06.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeInstanceInternetBandwidthConfigs
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
InstanceId	Yes	No	String	Instance ID to be operated. Can be obtained through the InstanceId in the returned value from the API DescribeInstances. Example: ins-6lafsaz0

3. Output Parameters

Parameter name	Type	Description
InternetBandwidthConfigSet	Array of InternetBandwidthConfig	List of bandwidth configuration information. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidInstanceId.NotFound	No corresponding instance was found.
InvalidInstance.NotSupported	Unsupported instance.
InternalServerError	Internal operation error.
InvalidInstanceId.Malformed	Invalid Instance ID. The format of the specified instance ID is incorrect, for example, an instance ID length error ins-1122 .
MissingParameter	Parameters are missing. The request did not include mandatory parameters.

DescribeInstanceTypeConfigs

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

This API (DescribeInstanceTypeConfigs) is used to query the instance model configurations.

- You can query the instance model configuration by using zone and instance-family . For filtering criteria, see Filter .
- If no parameter is defined, all instance model configurations in the specified region will be returned.

Default interface request rate limit: 40 times per second.

Interface update time: 2020-09-05 07:35:08.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeInstanceTypeConfigs
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
Filters	No	No	Array of Filter	Filtering criteria. For details, see the table below: Instance Filtering Criteria Table. A maximum of 10 Filters per request are allowed, and a maximum of 1 Filter.Values per request is allowed. Example:View

3. Output Parameters

Parameter name	Type	Description
InstanceTypeConfigSet	Array of InstanceTypeConfig	List of instance model configurations. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidFilterValue.LimitExceeded	The number of Filter> Filter parameter values exceeds the limit.
InvalidFilter	Invalid filter.
InvalidZone.MismatchRegion	The specified zone does not exist.
InternalServerError	Internal operation error.
InvalidParameterValue	Invalid parameter value. The format of the parameter value is incorrect or not supported, etc.

DescribeInstanceTypeDisasterGroupBlackList

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

This API is used to query the list of models that do not support placement groups.

Default interface request rate limit: 20 times per second.

Interface update time: 2025-08-20 00:38:09.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeInstanceTypeDisasterGroupBlackList
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
Filters	No	No	Filter	Query condition. Name: condition name; Values: corresponding value of the condition. Currently, only querying by zone-list and instance-family-list is supported. If zone-list is not specified, query the models that do not allow using placement groups in the entire region. The instance-family- list parameter specifies the models to be queried. If this parameter is not specified, query all models that do not allow using placement groups. Example:View

3. Output Parameters

Parameter name	Type	Description
InstanceFamilyBlackList	Array of String	Models with placement groups disabled. Example: ["S3"]
TotalCount	Int64	Number of models configured with a placement group blocklist. Example: 200
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

There is no error code related to business logic for this interface, For other error codes, see public ErrorCode.

DescribeInstanceUsbInfo

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

Query Instance USB Information

Default interface request rate limit: 20 times per second.

Interface update time: 2023-04-13 03:39:48.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeInstanceUsbInfo
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
VmUuids	Yes	No	Array of String	Virtual Machine UUID Example: ["5b33b986-084c-48e1-8cdb-d2e5ca5d045a"]

3. Output Parameters

Parameter name	Type	Description
data	UsbInfo	USB information.

Parameter name	Type	Description
		Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

There is no error code related to business logic for this interface, For other error codes, see public ErrorCode.

DescribeInstanceVncUrl

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

Used to query the VNC address of an instance.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-04-20 11:36:01.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeInstanceVncUrl
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
InstanceId	Yes	No	String	Queried instance ID, such as ins-38dk3j. Example: ins-r9hr2upy

3. Output Parameters

Parameter name	Type	Description
InstanceVncUrl	String	VNC Connection String of User Example: wss%3A%2F%2Fbjvnc.convergecloud.com%3A26789%2Fv

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

There is no error code related to business logic for this interface, For other error codes, see public ErrorCode.

DescribeInstances

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

This API (DescribeInstances) is used to query the detailed information of one or more instances.

- You can query the detailed information of an instance based on information such as the instance ID, instance name, or instance billing mode. For detailed filtering information, see the Filter .
- If no parameter is defined, a specific number (specified by the Limit , 20 by default) of instances of the current user are returned.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-10-26 11:54:05.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeInstances
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
InstanceIds	No	No	Array of String	Query by one or more instance IDs. The instance ID is in the format of ins-11112222 . For the specific format of this parameter, see the section id.N in the API Introduction. A maximum of 100 instances per request are allowed. This parameter does not support specifying InstanceIds and Filters at the same time. Example: ["ins-rf6ogz49"]
Filters	No	No	Array of Filter	Filtering conditions. For details, see the instance filtering condition table below. Each request can have up to 10 filters, and each filter can have up to 5 values. The InstanceIds and Filters parameters cannot be specified at the same time. zone Filter by [availability zone]. For example, ap-region1-1. Type: String. Required: No. Valid values: Availability zone list. project-id Filter by [project ID]. You can query the list of created projects by calling DescribeProject or log in to the console to view projects. You can also call AddProject to create a project. For example, 1002189. Type: Integer. Required: No. host-id Filter by [CDH ID]. For example, host-xxxxxxxx. Type: String. Required: No. vpc-id Filter by [VPC ID]. For example, vpc-xxxxxxxx. Type: String. Required: No. subnet-id Filter by [subnet ID]. For example, subnet-xxxxxxxx. Type: String. Required: No. instance-id Filter by [instance ID]. For example, ins-61dyt49hxxxx. Type: String. Required: No. security-group-id Filter by [security group ID]. For example, sg-8jlk3f3r. Type: String. Required: No. instance-name Filter by [instance name]. Type: String. Required: No. instance-charge-type Filter by [instance billing mode]. (POSTPAID_BY_HOUR: post-payment, that is, pay-as-you-go.
Offset	No	No	Int64	Offset, 0 by default. For further introduction to the Offset , see relevant sections in the API Introduction. Example: 1
Limit	No	No	Int64	Number of returns, 20 by default, and the maximum value is 100. For further introduction to the Limit , see relevant sections in the API Introduction. Example: 5
InnerVpcIds	No	No	Array of Int64	Internal parameters, list of numeric vpcIds. Example: NA
InnerSubnetIds	No	No	Array of Int64	Internal parameters, list of numeric subnetIds. Example: NA
IpAddresses	No	No	Array of String	Internal parameters, precise lists of private and public network IPs. Example: NA
VagueIpAddress	No	No	String	Internal parameters, fuzzy matching of private and public network IPs. Example: NA
VagueInstanceName	No	No	String	Internal parameters, fuzzy matching of instance alias. Example: NA

3. Output Parameters

Parameter name	Type	Description
TotalCount	Int64	Number of eligible instances. Example: 1
InstanceSet	Array of Instance	List of detailed information of instances. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidFilter	Invalid filter.
InvalidParameterValue	Invalid parameter value. The format of the parameter value is incorrect or not supported, etc.
InvalidFilterValue.LimitExceeded	The number of Filter> Filter parameter values exceeds the limit.
InternalServerError	Internal operation error.
InvalidParameterValue.LimitExceeded	The parameter value is out of range
InvalidHostId.Malformed	Invalid CDH ID. The format of the specified CDH ID is incorrect, for example, an ID length error host-1122 .
InvalidInstanceId.Malformed	Invalid Instance ID. The format of the specified instance ID is incorrect, for example, an instance ID length error ins-1122 .
InvalidParameter	Invalid parameter. The parameter does not meet the requirements, is not supported, or the like.
InvalidZone.MismatchRegion	The specified zone does not exist.

DescribeInstancesDeniedActions

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

This API (DescribeInstancesDeniedActions) is used to query operation restrictions list information of one or more instances.

- You can query the detailed information of an instance based on the instance ID.

Default interface request rate limit: 200 times per second.

Interface update time: 2025-08-20 00:38:45.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeInstancesDeniedActions
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
InstanceIds	Yes	No	Array of String	Queries by one or more instance IDs. Instance ID format: ins-61dyt49hxxxx . For the specific format of this parameter, see the id.N section in API Introduction. Each request can involve up to 100 instances. Parameters InstanceIds and Filters cannot be specified at the same time. Example: ["ins-61dyt49h"]

3. Output Parameters

Parameter name	Type	Description
InstanceDeniedActionSet	Array of InstanceDeniedActions	List of Instance Operation Restrictions Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidInstance.NotSupported	Unsupported instance.
InvalidInstanceId.Malformed	Invalid Instance ID. The format of the specified instance ID is incorrect, for example, an instance ID length error ins-1122 .
InvalidInstanceId.NotFound	No corresponding instance was found.

DescribeInstancesModification

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

Query Model Configuration Supported by Specified Instance for Adjustment

Default interface request rate limit: 20 times per second.

Interface update time: 2023-07-27 03:31:23.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeInstancesModification
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
InstanceIds	Yes	No	Array of String	One or more instance IDs to be queried. Can be obtained through the InstanceId in the returned value from the API DescribeInstances. A maximum of 20 batch instances per request are allowed. Example: ["ins-4txox06m"]
Filters	No	No	Array of Filter	Filter conditions support: status. Example:View

3. Output Parameters

Parameter name	Type	Description
InstanceTypeConfigStatusSet	Array of InstanceTypeConfigStatusSet	List of Models Returned by Cross-Model Configuration Adjustments Example:View
TotalCount	Int64	Total number Example: 10
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidFilter	Invalid filter.

DescribeInstancesStatus

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

This API (DescribeInstancesStatus) is used to query the status of one or more instances.

- You can query the status of an instance based on the instance ID.
- If no parameter is defined, a specific number (specified by the Limit, 20 by default) of instances of the current user are returned.

Default interface request rate limit: 20 times per second.

Interface update time: 2018-03-22 08:49:07.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeInstancesStatus
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
InstanceIds	No	No	Array of String	Query by one or more instance IDs. The instance ID is in the format of ins-11112222 . For the specific format of this parameter, see the section id.N in the API Introduction. A maximum of 100 instances per request are allowed. Example: ["ins-r8hr2upy\r\n","ins-5d8a23rs\r\n"]
Offset	No	No	Int64	Offset, 0 by default. For further introduction to the Offset , see relevant sections in the API Introduction. Example: 0
Limit	No	No	Int64	Number of returns, 20 by default, and the maximum value is 100. For further introduction to the Limit , see relevant sections in the API Introduction. Example: 2

3. Output Parameters

Parameter name	Type	Description
TotalCount	Int64	Number of eligible instance statuses. Example: 2
InstanceStatusSet	Array of InstanceStatus	List of Instance Status. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	Invalid parameter value. The format of the parameter value is incorrect or not supported, etc.
InternalServerError	Internal operation error.
InvalidParameterValue.LimitExceeded	The parameter value is out of range
InvalidInstanceId.Malformed	Invalid Instance ID. The format of the specified instance ID is incorrect, for example, an instance ID length error ins-1122 .

DescribeZoneInstanceConfigInfos

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

This API (DescribeZoneInstanceConfigInfos) is used to obtain model information of the availability zone.

Default interface request rate limit: 40 times per second.

Interface update time: 2024-09-21 02:59:26.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeZoneInstanceConfigInfos
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
Filters	No	No	Array of Filter	zone Filter by [availability zone]. For example, ap-region1-1. Type: String. Required: Yes. Valid values: Availability zone list. instance-family Filter by [instance model series]. For example, S1, I1, and M1. Type: Integer. Required: No. instance-type Filter by [instance model]. Different instance models correspond to different resource specifications. For specific values, you can obtain the latest specification table by calling the DescribeInstanceTypeConfigs API or check the instance type description. If this parameter is not specified, the default model S1.SMALL1 is used. Type: String. Required: No. instance-charge-type Filter by [instance billing mode]. (PREPAID: prepayment, that is, monthly subscription.
Language	No	No	String	Language Example: zh-CN

3. Output Parameters

Parameter name	Type	Description
InstanceTypeQuotaSet	Array of InstanceTypeQuotaItemArchitecture	List of availability zone model configurations. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidInstanceType.Malformed	The parameter format of the specified InstanceType is invalid.
InvalidZone.MismatchRegion	The specified zone does not exist.
InvalidRegion.NotFound	The specified zone was not found.

GetRecycleInfo

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

Obtain the recycle bin setting time.

Default interface request rate limit: 20 times per second.

Interface update time: 2025-08-20 00:47:06.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: GetRecycleInfo
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface

3. Output Parameters

Parameter name	Type	Description
RecycleTime	String	Recycle Bin Setting Time Example: 2020-03-12T17:05:17+08:00
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

There is no error code related to business logic for this interface, For other error codes, see public ErrorCode.

ImportSnapshot

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

Import a data disk image and make it as a CBS snapshot. The snapshot can be used to create a CBS data disk.

Default interface request rate limit: 20 times per second.

Interface update time: 2018-03-07 02:38:54.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ImportSnapshot
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
SnapshotName	Yes	No	String	Name of Created Snapshot Example: FirstSnapshot
SnapshotDescription	No	No	String	Description of Created Snapshot Example: jack use
SnapshotUrl	Yes	No	String	COS Link of Data Disk Image Example: http://111-1251243127.cosd.convergecloud.com/Windows%20Server%202008%20R2%20x64a.vmdk
SnapshotSize	Yes	No	Int64	Size of Created Snapshot Example: 50
DryRun	No	No	Bool	True is for checking parameters only, false by default. Example: true

3. Output Parameters

Parameter name	Type	Description
TaskId	String	Task ID, can be used to query the task status. Example: 432322
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

There is no error code related to business logic for this interface, For other error codes, see public ErrorCode.

InquiryPriceRenewInstances

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

This API has been discontinued for maintenance from April 14, 2022.
This API (InquiryPriceRenewInstances) is used to inquire about the price for renewing a monthly subscription instance.

- Only inquiring about the price for renewing a monthly subscription instance is supported.

Default interface request rate limit: 10 times per second.

Interface update time: 2022-04-23 10:09:22.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: InquiryPriceRenewInstances
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
InstanceIds	Yes	No	Array of String	One or more instance IDs to be operated. You can obtain the instance ID through the InstanceId in the returned value from the API DescribeInstances. A maximum of 100 batch instances per request are allowed. Example: ["ins-2zvpghhc"]
InstanceChargePrepaid	Yes	No	InstanceChargePrepaid	Prepaid mode, that is, monthly subscription-related parameter settings. You can specify attributes of a monthly subscription instance, such as purchase duration and whether to set auto-renewal, through this parameter. Example:View
InternetAccessible	No	No	Array of InternetAccessible	Internal parameters, public network bandwidth-related information settings. Example:View
DryRun	No	No	Bool	Trial run. Example: false
RenewPortableDataDisk	No	No	Bool	Internal parameters, renew the elastic data disk. Example: false

3. Output Parameters

Parameter name	Type	Description
Price	Price	This parameter indicates the price for the corresponding configuration instance. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidInstanceId.NotFound	No corresponding instance was found.
InvalidInstance.NotSupported	Unsupported instance.
InvalidParameterValue	Invalid parameter value. The format of the parameter value is incorrect or not supported, etc.
InternalServerError	Internal operation error.
InvalidAccount.InsufficientBalance	Insufficient account balance
InvalidInstanceId.Malformed	Invalid Instance ID. The format of the specified instance ID is incorrect, for example, an instance ID length error ins-1122 .
InvalidPeriod	Invalid duration. Currently, only the following durations are supported: [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 24, 36], unit: months.
MissingParameter	Parameters are missing. The request did not include mandatory parameters.
InvalidAccount.UnpaidOrder	The account has unpaid orders.

InquiryPriceResetInstance

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

This API (InquiryPriceResetInstance) is used to inquire about the price for reinstalling an instance. * If you have specified the parameter `ImageId` , inquire about the price for reinstallation by using the specified image. Otherwise, inquire about the price for reinstallation based on the image currently used by the instance. * Currently, only instances with System Disk Type of `CLOUD_BASIC` , `CLOUD_PREMIUM` , or `CLOUD_SSD` are supported for inquiring about the price for reinstallation caused by switching between Linux and Windows operating systems through this API. * Currently, instances in overseas regions are not supported for inquiring about the price for reinstallation caused by switching between the Linux and Windows operating systems through this API.

Specify a valid Image ID, in the format of `img-xxx` . There are four types of images:

Public Image
Custom Image
Shared Image

You can obtain available image IDs in the following ways:
The image IDs for the `Public Image` , `Custom Image` , and `Shared Image` can be queried by logging in to the Console;
Through the `ImageId` field in the returned information by calling the API DescribeImages.

Default interface request rate limit: 10 times per second.

Interface update time: 2022-04-23 09:45:08.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: InquiryPriceResetInstance
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
InstanceId	Yes	No	String	Instance ID. Can be obtained through the `InstanceId` in the returned value from the API DescribeInstances. Example: ins-fd8qnnmq
ImageId	No	No	String	Specify a valid Image ID, in the format of `img-xxx` . There are three types of images: ▸ Public Image ▸ Custom Image ▸ Shared Image You can obtain available image IDs in the following ways: ▸ The image IDs for the `Public Image` , `Custom Image` , and `Shared Image` can be queried by logging in to the Console; ▸ Through the `ImageId` field in the returned information by calling the API DescribeImages. Example: img-8toqc6s3
SystemDisk	No	No	SystemDisk	Instance system disk configuration information. Instances whose system disk is a CBS can specify the system disk size after reinstallation through this parameter to perform expansion on the system disk. If not specified, the default system disk size retains unchanged. Only expanding the system disk size is supported, but reducing the system disk size is not supported. Reinstallation only supports modifying the system disk size but the system disk type. For example, "SystemDisk": {"DiskSize":xxx}. Example:View
LoginSettings	No	No	LoginSettings	Instance login settings. You can set login method, password, or key of the instance or retain the original login settings of the image. By default, a password will be randomly generated and notified to the user through Message Center. Example:View
EnhancedService	No	No	EnhancedService	Enhanced services. You can specify whether to enable services such as Cloud Security and Cloud Monitor through this parameter. If this parameter is not specified, the Cloud Monitor and Cloud Security is enabled by default. Example:View

3. Output Parameters

Parameter name	Type	Description
Price	Price	This parameter indicates the price for reinstalling to the corresponding configuration instance. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidInstanceId.NotFound	No corresponding instance was found.
InvalidInstance.NotSupported	Unsupported instance.
InvalidParameterValue	Invalid parameter value. The format of the parameter value is incorrect or not supported, etc.
InternalServerError	Internal operation error.
InvalidInstanceId.Malformed	Invalid Instance ID. The format of the specified instance ID is incorrect, for example, an instance ID length error `ins-1122` .
MissingParameter	Parameters are missing. The request did not include mandatory parameters.

InquiryPriceResetInstancesInternetMaxBandwidth

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

This API has been discontinued for maintenance from May 11, 2022.
This API (InquiryPriceResetInstancesInternetMaxBandwidth) is used to inquire about the price for adjusting the public network bandwidth cap of an instance.

- The bandwidth cap range varies for different models.
- For bandwidth billed by using the BANDWIDTH_PREPAID method, parameters StartTime and EndTime need to be entered to specify the time period when the adjusted bandwidth takes effect.In this scenario, it is not supported to reduce the bandwidth, which may involve charges. Make sure your account balance is sufficient.
- For bandwidth billed by using the TRAFFIC_POSTPAID_BY_HOUR , BANDWIDTH_POSTPAID_BY_HOUR , and BANDWIDTH_PACKAGE methods, adjusting the bandwidth cap through this API takes effect in real time. You can increase or reduce the bandwidth within the allowed range. It is not supported to enter parameters StartTime and EndTime .
- The API does not support adjusting the bandwidth billed by using the BANDWIDTH_POSTPAID_BY_MONTH method.
- The API does not support adjusting the bandwidth billed by using the BANDWIDTH_PREPAID and BANDWIDTH_POSTPAID_BY_HOUR methods in batches.
- The API does not support adjusting bandwidth billed by using mixed methods in batches. For example, it does not support adjusting the bandwidth billed by using the TRAFFIC_POSTPAID_BY_HOUR and BANDWIDTH_PACKAGE methods.
  The API supports price inquires only for instances with bandwidth billed by using the BANDWIDTH_PREPAID and TRAFFIC_POSTPAID_BY_HOUR methods. For all other billing methods, 0 will be returned.

Default interface request rate limit: 10 times per second.

Interface update time: 2022-05-12 06:34:16.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: InquiryPriceResetInstancesInternetMaxBandwidth
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
InstanceIds	Yes	No	Array of String	One or more instance IDs to be operated. You can obtain the instance ID through the InstanceId in the returned value from the API DescribeInstances. A maximum of 100 batch instances per request are allowed. Example: ["ins-fd8spnmq"]
InternetAccessible	Yes	No	InternetAccessible	Public network outbound bandwidth configuration. Different models have different bandwidth cap ranges. For specific restrictions, see the bandwidth limit reconciliation statement. Currently, only the InternetMaxBandwidthOut parameter is supported. Example:View
StartTime	No	No	String	Data from which the bandwidth takes effect, in the format of YYYY-MM-DD , such as 2016-10-30 . The start data should not be earlier than the current time. If the start data is today, the new bandwidth takes effect immediately. This parameter is only valid for monthly subscription bandwidth, and is not supported for bandwidth billed by other modes. Otherwise, the API will return a corresponding error code. Example: 2016-10-30
EndTime	No	No	String	Date until which the bandwidth takes effect, in the format of YYYY-MM-DD , such as 2016-10-30 . The validity period of the new bandwidth covers the end date. The end date should not be later than the expiration date of a monthly subscription instance. You can obtain the expiration date of an instance through the ExpiredTime in the returned value from the API DescribeInstances. This parameter is only valid for monthly subscription bandwidth, and is not supported for bandwidth billed by other modes. Otherwise, the API will return a corresp Example: 2016-11-30

3. Output Parameters

Parameter name	Type	Description
Price	Price	This parameter indicates the price of the bandwidth after it is adjusted to a corresponding size. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidInstanceId.NotFound	No corresponding instance was found.
InvalidInstance.NotSupported	Unsupported instance.
InvalidParameterValue	Invalid parameter value. The format of the parameter value is incorrect or not supported, etc.
InternalServerError	Internal operation error.
InvalidParameterValue.Range	Invalid parameter value. The range of the parameter value is not legal.
InvalidAccount.InsufficientBalance	Insufficient account balance
InvalidInstanceId.MalFormed	Invalid Instance ID. The format of the specified instance ID is incorrect, for example, an instance ID length error ins-1122 .
InvalidParameter	Invalid parameter. The parameter does not meet the requirements, is not supported, or the like.
MissingParameter	Parameters are missing. The request did not include mandatory parameters.
InvalidAccount.UnpaidOrder	The account has unpaid orders.
InvalidPermission	The account does not support this operation.

InquiryPriceResetInstancesType

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

This API (InquiryPriceResetInstancesType) is used to inquire about the price for adjusting the model of an instance.

- Currently, only instances with System Disk Types of CLOUD_BASIC , CLOUD_PREMIUM , or CLOUD_SSD are supported for inquiring about the price for the model through this API.
- Currently, CDH instances are not supported for inquiring about the price for the model through this API.
- Currently, adjusting the model across model systems is not supported. In other words, when you use this API, the specified InstanceType and the original model of the instance need to belong to the same series.
- For monthly subscription instances, using this API will involve charges. Make sure your account balance is sufficient.

Default interface request rate limit: 10 times per second.

Interface update time: 2022-04-20 08:55:47.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: InquiryPriceResetInstancesType
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
InstanceIds	Yes	No	Array of String	One or more instance IDs to be operated. You can obtain the instance ID through the InstanceId in the returned value from the API DescribeInstances. A maximum of 1 batch instance per request is allowed. Example: ["ins-2zvpghhc"]
InstanceType	Yes	No	String	Instance model. Different instance models specify different resource specifications. For specific values, see the attached instance resource specification comparison table. Alternatively, you can call the API for querying a list of instance resource specifications to obtain the latest specification table. Example: S5.16XLARGE256

3. Output Parameters

Parameter name	Type	Description
Price	Price	This parameter indicates the price for adjusting the instance to the corresponding model. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidInstanceId.NotFound	No corresponding instance was found.
InvalidInstance.NotSupported	Unsupported instance.
InvalidParameterValue	Invalid parameter value. The format of the parameter value is incorrect or not supported, etc.
InternalServerError	Internal operation error.
InvalidAccount.InsufficientBalance	Insufficient account balance
InvalidInstanceId.Malformed	Invalid Instance ID. The format of the specified instance ID is incorrect, for example, an instance ID length error ins-1122 .
InvalidParameter	Invalid parameter. The parameter does not meet the requirements, is not supported, or the like.
MissingParameter	Parameters are missing. The request did not include mandatory parameters.
InvalidAccount.UnpaidOrder	The account has unpaid orders.
InvalidPermission	The account does not support this operation.

InquiryPriceResizeInstanceDisks

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

This API (InquiryPriceResizeInstanceDisks) is used to inquire about the price for expanding the data disk of an instance.

- Currently, only expanding data disks purchased with the instance and with Data Disk Types of CLOUD_BASIC , CLOUD_PREMIUM , or CLOUD_SSD are supported for price inquiry.

Default interface request rate limit: 10 times per second.

Interface update time: 2022-05-19 04:02:22.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: InquiryPriceResizeInstanceDisks
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
InstanceId	Yes	No	String	Instance ID to be operated. Can be obtained through the InstanceId in the returned value from the API DescribeInstances. Example: ins-fd8pnmq
SystemDisk	Yes	No	SystemDisk	Data disk configuration information to be expanded. Currently, only data disks purchased with the instance and with Data Disk Types of CLOUD_BASIC , CLOUD_PREMIUM , or CLOUD_SSD are supported for expansion. Unit of the system disk capacity: GB. Minimum expansion step: 10 GB. For the selection of system disk types, see the disk product introduction. Available system disk types are limited by the instance type InstanceType . In addition, the maximum capacity allowed for expans Example:View

3. Output Parameters

Parameter name	Type	Description
Price	Price	This parameter indicates the price for expanding the disk to the corresponding configuration. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidInstanceId.NotFound	No corresponding instance was found.
InvalidInstance.NotSupported	Unsupported instance.
InvalidParameterValue	Invalid parameter value. The format of the parameter value is incorrect or not supported, etc.
InternalServerError	Internal operation error.
InvalidAccount.InsufficientBalance	Insufficient account balance
InvalidInstanceId.Malformed	Invalid Instance ID. The format of the specified instance ID is incorrect, for example, an instance ID length error ins-1122 .
MissingParameter	Parameters are missing. The request did not include mandatory parameters.
InvalidAccount.UnpaidOrder	The account has unpaid orders.

InquiryPriceRunInstances

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

This API (InquiryPriceRunInstances) is used to inquire about the price for creating an instance. This API allows only price inquiries for instance configurations within the purchase restriction range. For details, see RunInstances.

Default interface request rate limit: 10 times per second.

Interface update time: 2022-10-28 03:28:18.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: InquiryPriceRunInstances
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
InstanceChargeType	No	No	String	Instance billing type. • PREPAID: Prepaid, that is, a monthly subscription mode • POSTPAID_BY_HOUR: Pay-per-hour postpaid Default value: POSTPAID_BY_HOUR. Example: PREPAID
InstanceChargePrepaid	No	No	InstanceChargePrepaid	Prepaid mode, that is, monthly subscription-related parameter settings. You can specify attributes of a monthly subscription instance, such as purchase duration and whether to set auto-renewal, through this parameter. If the billing mode of the specified instance is prepaid mode, this parameter is required. Example:View
Placement	Yes	No	Placement	Location of the instance. You can specify attributes such as the availability zone and project to which the instance belongs through this parameter. Example:View
InstanceType	No	No	String	Instance model. Different instance models specify different resource specifications. You can obtain the specific values by calling the API DescribeInstanceTypeConfigs to obtain the latest specification table. If this parameter is not specified, the default model is S1.SMALL1. Example: S5.MEDIUM2
ImageId	Yes	No	String	Specify a valid Image ID, in the format of img-xxx . There are four types of images: • Public Image • Custom Image • Shared Image • Service Market Image You can obtain available image IDs in the following ways: • The image IDs for the Public Image , Custom Image , and Shared Image can be queried by logging in to the Console. Example: img-pmqg1cw7
SystemDisk	No	No	SystemDisk	Instance system disk configuration information. If this parameter is not specified, it will be assigned based on the system default values. Example:View
DataDisks	No	No	Array of DataDisk	Instance data disk configuration information. If this parameter is not specified, no data disks are purchased by default. Multiple data disks can be specified when purchasing. Example:View
VirtualPrivateCloud	No	No	VirtualPrivateCloud	VPC-related information configuration. You can specify information such as VPC ID and subnet ID through this parameter. If this parameter is not specified, use the basic network by default. If a VPC IP is specified in this parameter, the InstanceCount parameter can only be 1. Example:View
InternetAccessible	No	No	InternetAccessible	Public bandwidth-related settings. If this parameter is not specified, the public bandwidth is 0 Mbps by default. Example:View
InstanceCount	No	No	Int64	Number of instances to purchase. Value range: [1,100]. Default value: 1. The specified number of instances to purchase should not exceed the remaining quota of the user. Example: 1
InstanceName	No	No	String	Instance display name. If not specified, it will be displayed as unnamed by default. Example: myInstance
LoginSettings	No	No	LoginSettings	Instance login settings. You can set login method, password, or key of the instance or retain the original login settings of the image. By default, a password will be randomly generated and notified to the user through Message Center. Example:View
SecurityGroupIds	No	No	Array of String	Security groups to which an instance belongs. If this parameter is not specified, do not bind the security group by default. Example: ["sg-efil73jd"]
EnhancedService	No	No	EnhancedService	Enhanced services. You can specify whether to enable services such as Cloud Security and Cloud Monitor through this parameter. If this parameter is not specified, the Cloud Monitor and Cloud Security is enabled by default. Example:View
ClientToken	No	No	String	String used to ensure request idempotency. This string is generated by the customer and should be unique across different requests. The maximum length should be no more than 64 ASCII characters. If this parameter is not specified, the idempotency of the request cannot be ensured. For more detailed information, see: How to Ensure Idempotency. Example: 4668722c-b6d6-4f79-96fd-097ebe5318e5
PurchaseSource	No	No	String	Internal parameters, purchase source. The source of the front-end call is MC. Example: API

3. Output Parameters

Parameter name	Type	Description
Price	Price	This parameter indicates the price for the corresponding configuration instance. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	Invalid parameter value. The format of the parameter value is incorrect or not supported, etc.
AccountQualificationRestrictions	The requesting account did not pass the qualification audit.
InvalidParameterValue.Range	Invalid parameter value. The range of the parameter value is not legal.
InvalidInstanceName.TooLong	The string length of the specified InstanceName exceeds the limit. It should be less than or equal to 60 bytes.
InvalidParameterCombination	It indicates that the parameter combination is incorrect.
InvalidInstanceType.Malformed	The parameter format of the specified InstanceType is invalid.
InvalidHostId.NotFound	The specified HostId does not exist, or does not belong to the requesting account.
InvalidPeriod	Invalid duration. Currently, only the following durations are supported: [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 24, 36], unit: months.
InstancesQuotaLimitExceeded	It indicates that the number of instances being created exceeds the remaining quota allowed for purchase by the account.
InvalidZone.MismatchRegion	The specified zone does not exist.
InvalidClientToken.TooLong	The string length of the specified ClientToken exceeds the limit. It should be less than or equal to 64 bytes.
MissingParameter	Parameters are missing. The request did not include mandatory parameters.
InvalidPassword	Invalid password. The specified password does not meet password complexity restrictions. For example, the password length does not meet restrictions.
InvalidPermission	The account does not support this operation.
InternalError.TradeUnknownError	An internal billing error occurred.

InquiryResourceResetInstancesType

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

This API (InquiryResourceResetInstancesType) is used to adjust resource query of an instance.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-04-20 09:08:44.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: InquiryResourceResetInstancesType
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
InstanceIds	Yes	No	Array of String	One or more instance IDs to be operated. You can obtain the instance ID through the InstanceId in the returned value from the API DescribeInstances. A maximum of 1 batch instance per request is allowed. Example: ["ins-61dyt49h"]
Online	No	No	Bool	Whether to upgrade the configuration online. Example: true

3. Output Parameters

Parameter name	Type	Description
ResourceForInstanceType	Array of ResourceForInstanceType	Resources of Instance Type Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalServerError	Internal operation error.
InvalidInstance.NotSupported	Unsupported instance.
InvalidImageOsVersion.Unsupported	Unsupported operating system version.
InvalidImageOsType.Unsupported	Unsupported operating system type.
InvalidInstanceId.NotFound	No corresponding instance was found.

InstanceAttachISO

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

This API is used to mount the ISO image to the instance.

Default interface request rate limit: 10 times per second.

Interface update time: 2025-08-05 01:09:49.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: InstanceAttachISO
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
InstanceId	Yes	No	String	ID of the instance for mounting the ISO image Example: ins-61dyt49h
ImageUrl	Yes	No	String	COS address where the ISO image is stored Example: http://111-1251533127.cosd.convergecloud.com/kiki/4769fxg.vmdk
Architecture	Yes	No	String	Operating system architecture of the ISO image: x86_64 or arm_64 Example: x86_64
OsType	Yes	No	String	Operating system type of the ISO image Example: CentOS
OsVersion	Yes	No	String	Operating system version of the ISO image Example: 7.2.1
DryRun	No	No	Bool	Check parameters only, do not execute task. Example: true

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidImageOsVersion.Unsupported	Unsupported operating system version.
InvalidParameter.InvalidParameterUrlError	Incorrect URL address.
InvalidImageOsType.Unsupported	Unsupported operating system type.
InvalidInstanceId.NotFound	No corresponding instance was found.

InstanceDetachISO

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

This API is used to unmount the ISO image disk from the instance.

Default interface request rate limit: 10 times per second.

Interface update time: 2025-08-05 01:10:24.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: InstanceDetachISO
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
InstanceId	Yes	No	String	ID of the instance for unmounting the ISO image Example: ins-61dyt49h

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidInstance.NotSupported	Unsupported instance.
InvalidInstanceId.Malformed	Invalid Instance ID. The format of the specified instance ID is incorrect, for example, an instance ID length error ins-1122 .
InvalidInstanceId.NotFound	No corresponding instance was found.
UnsupportedOperation.InstanceStateRunning	The instance is running.

ModifyDisasterRecoverGroup

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

Modify Spread Placement Group Information

Default interface request rate limit: 10 times per second.

Interface update time: 2022-04-25 03:36:53.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyDisasterRecoverGroup
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
DisasterRecoverGroupId	Yes	No	String	Spread placement group ID, can be queried through the API DescribeDisasterRecoverGroups. Example: ps-3a5sdgq5
Name	Yes	No	String	Spread placement group name, with a maximum of 128 characters. Example: Physical machine disaster recovery group 1

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

There is no error code related to business logic for this interface, For other error codes, see public ErrorCode.

ModifyInstancesAttribute

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

This API is used to modify the attributes of instances. Currently, only the instance name can be modified.

- The instance name is used only for management by users. The cloud platform does not use this name for submitting tickets or performing instance management operations.
- Batch operations are supported. Each request can involve up to 100 instances.

Default interface request rate limit: 10 times per second.

Interface update time: 2020-05-19 04:12:48.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyInstancesAttribute
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
InstanceIds	Yes	No	Array of String	One or more instance IDs to be operated. You can obtain the instance ID through the InstanceId in the returned value from the API DescribeInstances. A maximum of 100 batch instances per request are allowed. Example: ["ins-rf6ogz49"]
InstanceName	No	No	String	Instance display name. It can be named as required, but should not exceed 60 characters. Example: MyInsName
UserData	No	No	String	Internal parameters, user data. Example: TXIVc2VyRGF0YQo
SecurityGroups	No	No	Array of String	Internal parameters, list of security group IDs. Example: ["sg-rf6ogz49"]
ResetNewCreationIdentify	No	No	Bool	Internal parameters, unknown. Example: false
DisableApiTermination	No	No	Bool	Instance destruction protection flag, indicating whether deletion through APIs is allowed. Valid values: • TRUE: instance protection is enabled and deletion through APIs is not allowed • FALSE: instance protection is disabled and deletion through APIs is allowed Default value: FALSE. Example: false

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.LimitExceeded	The parameter value is out of range
InternalServerError	Internal operation error.
InvalidInstanceName.TooLong	The string length of the specified InstanceName exceeds the limit. It should be less than or equal to 60 bytes.
InvalidInstance.NotSupported	Unsupported instance.
InvalidInstanceId.NotFound	No corresponding instance was found.
MissingParameter	Parameters are missing. The request did not include mandatory parameters.
InvalidInstanceId.Malformed	Invalid Instance ID. The format of the specified instance ID is incorrect, for example, an instance ID length error ins-1122 .
InvalidParameterValue	Invalid parameter value. The format of the parameter value is incorrect or not supported, etc.

ModifyInstancesDisasterRecoverGroup

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

This API (ModifyInstancesDisasterRecoverGroup) is used to adjust the placement group where an instance is located.

- Currently, only instances that is of the basic network or the VPC and whose system disk and data disk types are CLOUD_BASIC, CLOUD_PREMIUM, or CLOUD_SSD are supported for modifying the placement group through this API.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-09-26 08:17:39.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyInstancesDisasterRecoverGroup
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
InstanceIds	Yes	No	Array of String	One or more instance IDs to be operated. You can obtain the instance ID through the InstanceId in the returned value from the API DescribeInstances. A maximum of 1 batch instance per request is allowed. Example: ["ins-r8hr2upy\r\n"]
DisasterRecoverGroupId	Yes	No	String	Spread placement group ID, can be obtained through the API DescribeDisasterRecoverGroups. Example: ps-a66w6rlb
Force	No	No	Bool	Whether to forcibly change instance hosts. Value range: • TRUE: Indicates that the instance is allowed to change hosts, allowing the instance to reboot • FALSE: Does not allow the instance to change hosts. Instances can only be added to the placement group on the current host. This may result in a failure to change the replacement group Default value: FALSE. Example: false

3. Output Parameters

Parameter name	Type	Description
TaskId	String	Task ID Example: 643244
FlowId	Int64	Task Flow ID Example: 3
flowId	Int64	Task Flow ID Example: 3
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

There is no error code related to business logic for this interface, For other error codes, see public ErrorCode.

ModifyInstancesRenewFlag

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

This API (ModifyInstancesRenewFlag) is used to modify a renewal flag of a monthly subscription instance.

- Once an instance is marked as auto-renewal, the instance will be automatically renewed for 1 month each time it expires.
- Batch operations are supported. A maximum of 100 batch instances per request are allowed.

Default interface request rate limit: 10 times per second.

Interface update time: 2018-04-04 09:23:06.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyInstancesRenewFlag
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
InstanceIds	Yes	No	Array of String	One or more instance IDs to be operated. You can obtain the instance ID through the InstanceId in the returned value from the API DescribeInstances. A maximum of 100 batch instances per request are allowed. Example: ["ins-r8hr2upy","ins-5d8a23rs"]
RenewFlag	Yes	No	String	Auto-renewal flag. Value range: • NOTIFY_AND_AUTO_RENEW: Notifies of expiration and performs auto-renewal • NOTIFY_AND_MANUAL_RENEW: Notifies of expiration but does not perform auto-renewal • DISABLE_NOTIFY_AND_MANUAL_RENEW: Does not notify of expiration nor perform auto-renewal If this parameter is specified to NOTIFY_AND_AUTO_RENEW, the instance will be automatically renewed on a monthly basis after it expires if there is sufficient account balance. Example: NOTIFY_AND_AUTO_RENEW

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidInstanceId.NotFound	No corresponding instance was found.
InvalidInstance.NotSupported	Unsupported instance.
InvalidParameterValue	Invalid parameter value. The format of the parameter value is incorrect or not supported, etc.
InternalServerError	Internal operation error.
InvalidParameterValue.LimitExceeded	The parameter value is out of range
InvalidInstanceId.Malformed	Invalid Instance ID. The format of the specified instance ID is incorrect, for example, an instance ID length error ins-1122 .

ModifyInstancesVpcAttribute

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

This API (ModifyInstancesVpcAttribute) is used to modify VPC attributes of an instance, such as the VPC IP address.

- This operation will shut down the instance by default and restart it after modification is completed.
- When the specified VPC ID and the subnet ID (which should be in the availability zone of the instance) are inconsistent with the VPC where the specified instance is located, the instance will be migrated to the subnet of the specified VPC. Before performing this operation, make sure there are no ENI and CLB bound on the specified instance.
- You can query the result of the instance operation by calling the API DescribeInstances. If the latest operation status (LatestOperationState) of the instance is SUCCESS, it indicates that the operation succeeded.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-10-28 03:50:44.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyInstancesVpcAttribute
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
InstanceIds	Yes	No	Array of String	Instance ID array to be operated. Can be obtained through the InstanceId in the returned value from the API DescribeInstances. Example: ["ins-r8hr2upy","ins-5d8a23rs"]
VirtualPrivateCloud	Yes	No	VirtualPrivateCloud	VPC-related information configuration. You can specify information such as VPC ID and subnet ID through this parameter. • When the specified VPC ID and subnet ID (the subnet should be in the same availability zone as the instance) are different from the VPC where the instance is located, the instance will be migrated to the subnet under the specified VPC. • You can specify the VPC subnet IP through the PrivateIpAddresses . If specification is needed, subnet IPs need to be specified for all specified instances. In this case, InstanceIds and PrivateIpAddresses are in a one-to-one correspondence. • When the PrivateIpAddresses is not specified, VPC subnet IPs will be randomly assigned. Example:View
ForceStop	No	No	Bool	Whether to perform forced shutdown on the running instance, TRUE by default. Example: true
ReserveHostName	No	No	Bool	Whether to retain the hostname, FALSE by default. Example: true

3. Output Parameters

Parameter name	Type	Description
TaskId	String	Task ID Example: 542324
flowId	Int64	Task Flow ID Example: 5
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
VpcIpIsUsed	The VPC IP has already been used.

RebootInstances

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

This API (RebootInstances) is used to reboot an instance.

- Only instances in a RUNNING state can be rebooted.
- When the API is successfully called, the instance will enter the REBOOTING state. When the instance is successfully rebooted, the instance will enter the RUNNING state.
- Forced reboot is supported. The effect is equivalent to turning off the switch of the physical computer and then turning on it again. Forced reboot may lead to data loss or damage of the file system. Use it only when the server cannot be normally rebooted.
- Batch operations are supported. A maximum of 100 batch instances per request are allowed.

Default interface request rate limit: 10 times per second.

Interface update time: 2022-10-28 03:45:44.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: RebootInstances
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
InstanceIds	Yes	No	Array of String	One or more instance IDs to be operated. You can obtain the instance ID through the InstanceId in the returned value from the API DescribeInstances. A maximum of 100 batch instances per request are allowed. Example: ["ins-r8hr2upy","ins-5d8a23rs"]
ForceReboot	No	No	Bool	Whether to choose to force reboot the instance after a normal reboot fails. Value range: • TRUE: Indicates a forced reboot after a normal reboot fails • FALSE: Indicates no forced reboot after a normal reboot fails Default value: FALSE. Specifying the StopType parameter at the same time is not supported. Example: false
StopType	No	No	String	Shutdown type. Value range: SOFT: Indicates a soft shutdown; HARD: Indicates a hard shutdown; SOFT_FIRST: Indicates soft shutdown is prioritized, if it fails, then hard shutdown is performed. Default value: SOFT. Example: SOFT

3. Output Parameters

Parameter name	Type	Description
TaskId	String	Task ID Example: 435323
flowId	Int64	Task Flow ID Example: 4
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidInstanceId.NotFound	No corresponding instance was found.
InvalidInstance.NotSupported	Unsupported instance.
InvalidParameterValue	Invalid parameter value. The format of the parameter value is incorrect or not supported, etc.
InternalServerError	Internal operation error.
InvalidParameterValue.LimitExceeded	The parameter value is out of range
InvalidInstanceId.Malformed	Invalid Instance ID. The format of the specified instance ID is incorrect, for example, an instance ID length error ins-1122 .
MissingParameter	Parameters are missing. The request did not include mandatory parameters.

RemoveInstancesDisasterRecoverGroup

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

Instance Disassociates from Placement Group

Default interface request rate limit: 20 times per second.

Interface update time: 2025-08-05 01:16:36.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: RemoveInstancesDisasterRecoverGroup
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
InstanceDisasterMapList	Yes	No	Array of InstanceDisasterMap	Instances and Placement Group IDs to unbind Example:View

3. Output Parameters

Parameter name	Type	Description
TaskId	String	Task ID Example: 435323
flowId	Int64	Task Flow ID Example: 4
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidInstanceId.NotFound	No corresponding instance was found.

RenewInstances

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

This API (RenewInstances) is used to renew an instance.

Default interface request rate limit: 10 times per second.

Interface update time: 2022-04-23 08:55:05.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: RenewInstances
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
InstanceIds	Yes	No	Array of String	One or more instance IDs to be operated. You can obtain the instance ID through the InstanceId in the returned value from the API DescribeInstances. A maximum of 100 batch instances per request are allowed. Example: ["ins-r8hr2upy"]
DryRun	No	No	Bool	Trial run. False by default. Example: true

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidInstanceId.NotFound	No corresponding instance was found.
InvalidInstance.NotSupported	Unsupported instance.
InvalidParameterValue	Invalid parameter value. The format of the parameter value is incorrect or not supported, etc.
InternalServerError	Internal operation error.
InvalidInstanceId.Malformed	Invalid Instance ID. The format of the specified instance ID is incorrect, for example, an instance ID length error ins-1122 .
MissingParameter	Parameters are missing. The request did not include mandatory parameters.

ResetInstance

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

This API (ResetInstance) is used to reinstall the operating system on a specified instance.

- If you have specified the parameter `ImageId` , use the specified image for reinstallation. Otherwise, perform reinstallation based on the image currently used by the instance.
- The system disk will be formatted and reset. Ensure that there are no important files in the system disk.
- When switching between the Linux and Windows systems is performed, the system disk ID of the instance will change. If the system disk is associated with the snapshot, data cannot be rolled back and restored.
- If you do not specify a password, a random password will be sent via Message Center.
- Currently, only instances whose System Disk Type is `CLOUD_BASIC` , `CLOUD_PREMIUM` , or `CLOUD_SSD` are supported for implementing switching between the Linux and Windows operating systems through this API.
- Currently, instances in overseas regions are not supported for implementing switching between the Linux and Windows operating systems through this API.

Default interface request rate limit: 10 times per second.

Interface update time: 2022-10-28 03:44:11.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ResetInstance
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
InstanceId	Yes	No	String	Instance ID. Can be obtained through the `InstanceId` in the returned value from the API DescribeInstances. Example: ins-i8hr2upy
ImageId	No	No	String	Specify a valid Image ID, in the format of `img-xxx` . There are four types of images: • Public Image • Custom Image • Shared Image • Service Market Image You can obtain available image IDs in the following ways: • The image IDs for the `PublicBnbsp;Image` , `CustomBnbsp;Image` , and `SharedBnbsp;Image` can be queried by logging in to the Console. • Through the `ImageId` field in the returned information by calling the API DescribeImages. Example: img-pmqg1cw7
SystemDisk	No	No	SystemDisk	Instance system disk configuration information. Instances whose system disk is a CBS can specify the system disk size after reinstallation through this parameter to perform expansion on the system disk. If not specified, the default system disk size retains unchanged. Only expanding the system disk size is supported, but reducing the system disk size is not supported. Reinstallation only supports modifying the system disk size but the system disk type. Example:View
LoginSettings	No	No	LoginSettings	Instance login settings. You can set login method, password, or key of the instance or retain the original login settings of the image. By default, a password will be randomly generated and notified to the user through Message Center. Example:View
EnhancedService	No	No	EnhancedService	Enhanced services. You can specify whether to enable services such as Cloud Security and Cloud Monitor through this parameter. If this parameter is not specified, the Cloud Monitor and Cloud Security is enabled by default. Example:View
DryRun	No	No	Bool	Whether to skip the actual execution logic. Example: false

3. Output Parameters

Parameter name	Type	Description
TaskId	String	Task ID Example: 435323
flowId	Int64	Task Flow ID Example: 4
FlowId	Int64	Task Flow ID Example: 4
RequestId	String	Unique request id, Each request will return. The `RequestId` of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidInstanceId.NotFound	No corresponding instance was found.
InvalidInstance.NotSupported	Unsupported instance.
InvalidParameterValue	Invalid parameter value. The format of the parameter value is incorrect or not supported, etc.
InternalServerError	Internal operation error.
InvalidInstanceId.Malformed	Invalid Instance ID. The format of the specified instance ID is incorrect, for example, an instance ID length error `ins-1122` .
MissingParameter	Parameters are missing. The request did not include mandatory parameters.
InvalidImageId.NotFound	Image not found

ResetInstancesInternetMaxBandwidth

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

This API (ResetInstancesInternetMaxBandwidth) is used to adjust the public network bandwidth cap of an instance.

- The bandwidth cap range varies for different models.
- For bandwidth billed by using the `BANDWIDTH_PREPAID` method, parameters `StartTime` and `EndTime` need to be entered to specify the time period when the adjusted bandwidth takes effect. In this scenario, it is not supported to reduce the bandwidth, which may involve charges. Make sure your account balance is sufficient.
- For bandwidth billed by using the `TRAFFIC_POSTPAID_BY_HOUR` , `BANDWIDTH_POSTPAID_BY_HOUR` , and `BANDWIDTH_PACKAGE` methods, adjusting the bandwidth cap through this API takes effect in real time. You can increase or reduce the bandwidth within the allowed range. It is not supported to enter parameters `StartTime` and `EndTime` .
- The API does not support adjusting the bandwidth billed by using the `BANDWIDTH_POSTPAID_BY_MONTH` method.
- The API does not support adjusting the bandwidth billed by using the `BANDWIDTH_PREPAID` and `BANDWIDTH_POSTPAID_BY_HOUR` methods in batches.
- The API does not support adjusting bandwidth billed by using mixed methods in batches. For example, it does not support adjusting the bandwidth billed by using the `TRAFFIC_POSTPAID_BY_HOUR` and `BANDWIDTH_PACKAGE` methods.

Default interface request rate limit: 10 times per second.

Interface update time: 2022-10-28 03:43:18.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ResetInstancesInternetMaxBandwidth
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
InstanceIds	Yes	No	Array of String	One or more instance IDs to be operated. You can obtain the instance ID through the `InstanceId` in the returned value from the API DescribeInstances. A maximum of 100 batch instances per request are allowed. Example: ["ins-r8hr2upy"]
InternetAccessible	Yes	No	InternetAccessible	Public network outbound bandwidth configuration. Different models have different bandwidth cap ranges. For specific restrictions, see the bandwidth limit reconciliation statement. Currently, only the `InternetMaxBandwidthOut` parameter is supported. Example:View
StartTime	No	No	String	Data from which the bandwidth takes effect, in the format of `YYYY-MM-DD` , such as `2016-10-30` . The start data should not be earlier than the current time. If the start data is today, the new bandwidth takes effect immediately. This parameter is only valid for monthly subscription bandwidth, and is not supported for bandwidth billed by other modes. Otherwise, the API will return a corresponding error code. Example: 2017-03-15
EndTime	No	No	String	Date until which the bandwidth takes effect, in the format of `YYYY-MM-DD` , such as `2016-10-30` . The validity period of the new bandwidth covers the end date. The end date should not be later than the expiration date of a monthly subscription instance. You can obtain the expiration date of an instance through the `ExpiredTime` in the returned value from the API DescribeInstances. This parameter is only valid for monthly subscription bandwidth, and is not supported for bandwidth billed by other modes. Otherwise, the API will return a correspo Example: 2017-03-16

3. Output Parameters

Parameter name	Type	Description
TaskId	String	Task ID Example: 435123
FlowId	Int64	Task Flow ID Example: 4
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidInstanceId.NotFound	No corresponding instance was found.
InvalidInstance.NotSupported	Unsupported instance.
InvalidParameterValue	Invalid parameter value. The format of the parameter value is incorrect or not supported, etc.
InternalServerError	Internal operation error.
InvalidParameterValue.Range	Invalid parameter value. The range of the parameter value is not legal.
InvalidAccount.InsufficientBalance	Insufficient account balance
InvalidInstanceId.Malformed	Invalid Instance ID. The format of the specified instance ID is incorrect, for example, an instance ID length error `ins-1122` .
InvalidParameter	Invalid parameter. The parameter does not meet the requirements, is not supported, or the like.
MissingParameter	Parameters are missing. The request did not include mandatory parameters.
InvalidAccount.UnpaidOrder	The account has unpaid orders.
InvalidPermission	The account does not support this operation.

ResetInstancesPassword

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

This API (ResetInstancesPassword) is used to reset the password of an instance operating system to a user-specified password.

- Only the password of the administrator account is modified. The administrator account varies with different instance operating systems (Windows: Administrator , Ubuntu : ubuntu , other systems: root).
- To reset the password of an instance in the running state, you need to explicitly specify the forced stop parameter ForceStop . If you do not explicitly specify the forced stop parameter, only instances in the stop state are allowed to reset the password.
- Batch operations are supported. Set the passwords of multiple instance operating systems as the same password. A maximum of 100 batch instances per request are allowed.

Default interface request rate limit: 10 times per second.

Interface update time: 2022-10-28 03:42:15.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ResetInstancesPassword
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
InstanceIds	Yes	No	Array of String	One or more instance IDs to be operated. You can obtain the instance ID through the InstanceId in the returned value from the API DescribeInstances. A maximum of 100 batch instances per request are allowed. Example: ["ins-r8hr2upy","ins-5d8a23rs"]
Password	Yes	No	String	Instance login password. The password complexity requirements vary by different operating system types, as follows: • The password of a Linux instance should contain 8 to 16 characters, including at least two of [a-z, A-Z], [0-9] , and symbols `[( ) ~ ! @ # $ % ^ & * - + = _
UserName	No	No	String	Username of the instance operating system whose password is to be reset. It should not exceed 64 characters. Example: asdc21
ForceStop	No	No	Bool	Whether to perform forced shutdown on the running instance. It is recommended to perform manual shutdown on the running instance first, and then reset the user password. Value Range: • TRUE: Indicates forced shutdown performed after normal shutdown fails. • FALSE: Indicates no forced shutdown performed after normal shutdown fails. Default value: FALSE. The effect of forced stop is equivalent to turning off the switch of the physical computer. Forced stop may lead to data loss or damage of the file system. Use it only when the server cannot be normally stopped. Example: true

3. Output Parameters

Parameter name	Type	Description
TaskId	String	Task ID Example: 435323
flowId	Int64	Task Flow ID Example: 4
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidInstanceId.NotFound	No corresponding instance was found.
InvalidInstance.NotSupported	Unsupported instance.
InvalidParameterValue	Invalid parameter value. The format of the parameter value is incorrect or not supported, etc.
InternalServerError	Internal operation error.
InvalidParameterValue.LimitExceeded	The parameter value is out of range
InvalidParameterValue.TooLong	Invalid input: Excessive length of the parameter.
InvalidInstanceId.Malformed	Invalid Instance ID. The format of the specified instance ID is incorrect, for example, an instance ID length error ins-1122 .
MissingParameter	Parameters are missing. The request did not include mandatory parameters.
InvalidPassword	Invalid password. The specified password does not meet password complexity restrictions. For example, the password length does not meet restrictions.

ResetInstancesType

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

This API (ResetInstancesType) is used to adjust the model of an instance.

- Currently, only instances with System Disk Types of CLOUD_BASIC , CLOUD_PREMIUM , or CLOUD_SSD are supported for adjusting the model through this API.
- Currently, CDH instances are not supported for adjusting the model through this API. * Currently, adjusting the model across model systems is not supported. In other words, when you use this API, the specified InstanceType and the original model of the instance need to belong to the same series. * For monthly subscription instances, using this API will involve charges. Make sure your account balance is sufficient.

Default interface request rate limit: 10 times per second.

Interface update time: 2020-12-10 07:43:59.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ResetInstancesType
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
InstanceIds	Yes	No	Array of String	One or more instance IDs to be operated. You can obtain the instance ID through the InstanceId in the returned value from the API DescribeInstances. A maximum of 1 batch instance per request is allowed. Example: ["ins-r8hr2upy"]
InstanceType	Yes	No	String	Instance model. Different instance models specify different resource specifications. For specific values, see the attached instance resource specification comparison table. Alternatively, you can call the API for querying a list of instance resource specifications to obtain the latest specification table. Example: S5.16XLARGE256
ForceStop	No	No	Bool	Whether to perform forced shutdown on the running instance. It is recommended to perform manual shutdown on the running instance first, and then reset the user password. Value Range: • TRUE: Indicates forced shutdown performed after normal shutdown fails. • FALSE: Indicates no forced shutdown performed after normal shutdown fails. Default value: FALSE. The effect of forced stop is equivalent to turning off the switch of the physical computer. Forced stop may lead to data loss or damage of the file system. Use it only when the server cannot be normally stopped. Example: false
Online	No	No	Bool	Whether to upgrade the configuration online. Example: true
IsAllowedAcrossHost	No	No	Bool	Whether to allow cross-host adjustment. Example: False

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidPermission	The account does not support this operation.
InternalServerError	Internal operation error.
InvalidAccount.InsufficientBalance	Insufficient account balance
InvalidInstanceId.Malformed	Invalid Instance ID. The format of the specified instance ID is incorrect, for example, an instance ID length error ins-1122 .
InvalidInstance.NotSupported	Unsupported instance.
InvalidParameterValue	Invalid parameter value. The format of the parameter value is incorrect or not supported, etc.
InvalidParameter	Invalid parameter. The parameter does not meet the requirements, is not supported, or the like.
MissingParameter	Parameters are missing. The request did not include mandatory parameters.
InvalidInstanceId.NotFound	No corresponding instance was found.
InvalidAccount.UnpaidOrder	The account has unpaid orders.

ResizeInstanceDisks

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

This API (ResizeInstanceDisks) is used to expand the data disk of an instance.

- Currently, only data disks purchased with the instance and with Data Disk Types of `CLOUD_BASIC` , `CLOUD_PREMIUM` , or `CLOUD_SSD` are supported for expansion.

Default interface request rate limit: 10 times per second.

Interface update time: 2022-12-02 07:34:09.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ResizeInstanceDisks
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
InstanceId	Yes	No	String	Instance ID to be operated. Can be obtained through the `InstanceId` in the returned value from the API DescribeInstances. Example: ins-r8hr2upy
SystemDisk	No	No	SystemDisk	Data disk configuration information to be expanded. Currently, only data disks purchased with the instance and with Data Disk Types of `CLOUD_BASIC` , `CLOUD_PREMIUM` , or `CLOUD_SSD` are supported for expansion. Unit of the system disk capacity: GB. Minimum expansion step: 10 GB. For the selection of system disk types, see the disk product introduction. Available system disk types are limited by the instance type `InstanceType` . In addition, the maximum capacity allowed for expar Example:View
DataDisks	No	No	Array of DataDisk	Describe Information about Data Disk to be Expanded Example:View
ResizeOnline	No	No	Bool	Whether the scale-out method for CBS is online scale-out. Example: true
ForceStop	No	No	Bool	Whether to perform forced shutdown on the running instance, False by default. Example: true

3. Output Parameters

Parameter name	Type	Description
TaskId	String	Task ID Example: 435323
flowId	String	Task Flow ID Example: 3
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidInstanceId.NotFound	No corresponding instance was found.
InvalidInstance.NotSupported	Unsupported instance.
InvalidParameterValue	Invalid parameter value. The format of the parameter value is incorrect or not supported, etc.
InternalServerError	Internal operation error.
InvalidAccount.InsufficientBalance	Insufficient account balance
InvalidInstanceId.Malformed	Invalid Instance ID. The format of the specified instance ID is incorrect, for example, an instance ID length error `ins-1122` .
MissingParameter	Parameters are missing. The request did not include mandatory parameters.
InvalidAccount.UnpaidOrder	The account has unpaid orders.
UnsupportedOperation.InstanceStateRunning	The instance is running.

RunInstances

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

This API is used to create one or more instances with specified configurations.

- Once an instance is successfully created, it will automatically start upon boot. [Instance status],/data structure#instancestatus) will change to "Running".
- This API is asynchronous. When the creation request is successfully issued, it returns a list of instance IDs . At this point, the instance creation is not yet complete. During this period, the instance status will be "Preparing". You can call the DescribeInstancesStatus API to query the status of the instance to determine if the creation was ultimately successful. If the instance status changes from "Preparing" to "Running", it has been successfully created.

Default interface request rate limit: 10 times per second.

Interface update time: 2022-04-22 07:24:14.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: RunInstances
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
InstanceChargeType	No	No	String	Instance billing type. • POSTPAID_BY_HOUR: Postpaid by hour • CDHPAID: CDHPAID (created based on a CDH, where CDH resources are free of charge). In this billing mode, the placement.hostid parameter is mandatory. Default value: POSTPAID_BY_HOUR. Example: POSTPAID_BY_HOUR
InstanceChargePrepaid	No	No	InstanceChargePrepaid	Prepaid mode, that is, monthly subscription-related parameter settings. You can specify attributes of a monthly subscription instance, such as purchase duration and whether to set auto-renewal, through this parameter. If the billing mode of the specified instance is prepaid mode, this parameter is required. ExampleView
Placement	Yes	No	Placement	Location of the instance. You can specify attributes such as availability zone, project, and CDH (for creating a instance with a dedicated host billing mode) to which the instance belongs through this parameter. ExampleView
InstanceType	No	No	String	Instance model. Different instance models specify different resource specifications. • For creating a instance with billing mode as PREPAID or POSTPAID_BY_HOUR, you can obtain the specific values by calling the API DescribeInstanceTypeConfigs to obtain the latest specification table or seeing the description of the Instance Types. If this parameter is not specified, the default model is S1.SMALL1. • For creating a instance with billing mode as CDHPAID, this parameter starts with a prefix CDH_ and is generated based on the CPU and memory configurations. Its specific form is CDH_XCXG. For example, for creating a CDH instance with 1 core CPU and 1 GB memory, this parameter should be CDH_1C1G. Example: S5.LARGE4
ImageId	Yes	No	String	Specify a valid Image ID, in the format of img-xxx . There are three types of images: • Public Image • Custom Image • Shared Image • You can obtain available image IDs in the following ways: • The image IDs for the Public Image , Custom Image , and Shared Image can be queried by logging in to the Console; • Through the ImageId field in the returned information by calling the API DescribeImages. Example: img-irmxe45l
PurchaseSource	No	No	String	Purchase Source Example: MC
SystemDisk	No	No	SystemDisk	Instance system disk configuration information. If this parameter is not specified, it will be assigned based on the system default values. ExampleView
DataDisks	No	No	Array of DataDisk	Instance data disk configuration information. If this parameter is not specified, no data disks are purchased by default. Specifying multiple data disks when purchasing is supported. ExampleView
VirtualPrivateCloud	No	No	VirtualPrivateCloud	VPC-related information configuration. You can specify information such as VPC ID and subnet ID through this parameter. If this parameter is not specified, use the basic network by default. If a VPC IP is specified in this parameter, the InstanceCount parameter can be 1 or 2. ExampleView
InternetAccessible	No	No	InternetAccessible	Public bandwidth-related settings. If this parameter is not specified, the public bandwidth is 0 Mbps by default. ExampleView
InstanceCount	No	No	Int64	Number of instances to purchase. Value range: [1,100]. Default value: 1. The specified number of instances to purchase should not exceed the remaining quota of the user. Example: 1
InstanceName	No	No	String	Instance display name. If not specified, it will be displayed as unnamed by default. A maximum of 60 characters are supported. Names after a period will be filtered out. Example: server_{R:3}
LoginSettings	No	No	LoginSettings	Instance login settings. You can set login method, password, or key of the instance or retain the original login settings of the image. By default, a password will be randomly generated and notified to the user through Message Center. ExampleView
SecurityGroupIds	No	No	Array of String	Security groups to which an instance belongs. If this parameter is not specified, bind the security group by default. Example: ["sg-ajhm9q1q"]
EnhancedService	No	No	EnhancedService	Enhanced services. You can specify whether to enable services such as Cloud Security and Cloud Monitor through this parameter. If this parameter is not specified, the Cloud Monitor and Cloud Security is enabled by default. ExampleView
ClientToken	No	No	String	String used to ensure request idempotency. This string is generated by the customer and should be unique across different requests. The maximum length should be no more than 64 ASCII characters. If this parameter is not specified, the idempotency of the request cannot be ensured. Example: system-f2827db9-c58a-49cc-bf10-33fc1923a34e
SpotPrice	No	No	String	Used to specify price production, currently mainly used to spot instances. Example: 300.0
HostName	No	No	String	Hostname of CVM. • Period (.) and hyphen (-) should not be used as the first or last character of the HostName, and should not be used consecutively. • Windows instance: The name should contain [2, 15] characters, including letters (case insensitive), digits, and hyphens (-), does not support periods (.), and should not be all digits. • Instance of other types (such as Linux instances): The name should contain [2, 31] characters, including multiple periods, with each segment between periods considered as one section. Each section can contain letters (case insensitive), digits, and hyphens (-), but should not be all digits. Period and hyphen placed together (.-) is not supported. Example: MyHostName
UserData	No	No	String	User data provided for the instance, should be encoded in base64 format, supports a maximum data size of 16 KB. Example: TXNiZVRGF0YQo=
DisasterRecoverGroupIds	No	No	Array of String	Placement group ID, only one can be specified. Example: ["ps-3p88qhfo"]
TagSpecification	No	No	Array of TagSpecification	List of tag descriptions. You can bind tags to corresponding resource instances at the same time by specifying this parameter. Currently, only binding tags to the CVM is supported. ExampleView
ProjectSpecification	No	No	ProjectSpecification	Specified project ID, only one can be specified. ExampleView
HpcClusterId	No	No	String	High-performance computing cluster ID. If the created instance is a high-performance computing instance, the cluster where the instance is placed should be specified. Otherwise, it cannot be specified. Example: hpc-a5nb66lo
DisableApiTermination	No	No	Bool	Instance destruction protection flag, indicating whether deletion through APIs is allowed. Valid values: • TRUE: instance protection is enabled and deletion through APIs is not allowed • FALSE: instance protection is disabled and deletion through APIs is allowed Default value: FALSE. Example: false

3. Output Parameters

Parameter name	Type	Description
InstanceIdSet	Array of String	When creating an instance through this API, this parameter will be returned, indicating one or more instance IDs. Returning a list of instance IDs does not indicate that the instance is successfully created. You can determine whether the creation is completed by querying the status of the corresponding instance ID in the returned InstancesSet through the API. DescribeInstancesStatus. If the instance status changes from Preparing to Running, it indicates that the instance is successfully created. Example: ["ins-mi99mut1"]
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidPermission	The account does not support this operation.
InvalidParameterValue	Invalid parameter value. The format of the parameter value is incorrect or not supported, etc.
InvalidParameterValue.Range	Invalid parameter value. The range of the parameter value is not legal.
InvalidInstanceType.Malformed	The parameter format of the specified InstanceType is invalid.
InvalidPeriod	Invalid duration. Currently, only the following durations are supported: [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 24, 36], unit: months.
VpcIpIsUsed	The VPC IP has already been used.
VpcAddrNotInSubNet	The VPC IP is not within the subnet.
InvalidClientToken.TooLong	The string length of the specified ClientToken exceeds the limit. It should be less than or equal to 64 bytes.
InvalidHostId.NotFound	The specified HostId does not exist, or does not belong to the requesting account.
MissingParameter	Parameters are missing. The request did not include mandatory parameters.
InstancesQuotaLimitExceeded	It indicates that the number of instances being created exceeds the remaining quota allowed for purchase by the account.
InvalidParameterCombination	It indicates that the parameter combination is incorrect.
InvalidParameter.InvalidIpFormat	The specified VPC IP format is incorrect.
InvalidZone.MismatchRegion	The specified zone does not exist.
AccountQualificationRestrictions	The requesting account did not pass the qualification audit.
InvalidPassword	Invalid password. The specified password does not meet password complexity restrictions. For example, the password length does not meet restrictions.
InvalidInstanceName.TooLong	The string length of the specified InstanceName exceeds the limit. It should be less than or equal to 60 bytes.
InvalidCloudDisk.SoldOut	The cloud disk has been sold out.
TradeUnknownError	Billing request error
ResourceInsufficient.SpecifiedInstanceType	The inventory of the specified instance type is insufficient.

StartInstances

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

This API (StartInstances) is used to start one or more instances.

- Operation can be performed on only instances in a STOPPED state.
- When the API is successfully called, the instance will enter the STARTING state. When the instance is successfully started, it will enter the RUNNING state.
- Batch operations are supported. A maximum of 100 batch instances per request are allowed.

Default interface request rate limit: 10 times per second.

Interface update time: 2023-03-14 03:33:01.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: StartInstances
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
InstanceIds	Yes	No	Array of String	One or more instance IDs to be operated. You can obtain the instance ID through the InstanceId in the returned value from the API DescribeInstances. A maximum of 100 batch instances per request are allowed. Example: ["ins-r8hr2upy","ins-5d8a23rs"]

3. Output Parameters

Parameter name	Type	Description
TaskId	String	Task ID Example: 542324
flowId	Int64	Task Flow ID Example: 4
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidInstanceId.NotFound	No corresponding instance was found.
InvalidInstance.NotSupported	Unsupported instance.
InvalidParameterValue	Invalid parameter value. The format of the parameter value is incorrect or not supported, etc.
InternalServerError	Internal operation error.
InvalidParameterValue.LimitExceeded	The parameter value is out of range
InvalidInstanceId.Malformed	Invalid Instance ID. The format of the specified instance ID is incorrect, for example, an instance ID length error ins-1122 .
MissingParameter	Parameters are missing. The request did not include mandatory parameters.

StopInstances

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

This API (StopInstances) is used to stop one or more instances.

- Only instances in the RUNNING state can be stopped.
- When the API is successfully called, the instance will enter the STOPPING state. When the instance is successfully stopped, it will enter the STOPPED state.
- Forced stop is supported. The effect of forced stop is equivalent to turning off the switch of the physical computer. Forced stop may lead to data loss or damage of the file system. Use it only when the server cannot be normally stopped.
- Batch operations are supported. A maximum of 100 batch instances per request are allowed.

Default interface request rate limit: 10 times per second.

Interface update time: 2025-07-31 04:07:53.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: StopInstances
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
InstanceIds	Yes	No	Array of String	One or more instance IDs to be operated. You can obtain the instance ID through the InstanceId in the returned value from the API DescribeInstances. A maximum of 100 batch instances per request are allowed. Example: ["ins-r8hr2upy","ins-5d8a23rs"]
ForceStop	No	No	Bool	Whether to choose to perform forced shutdown on the instance after a normal shutdown fails. Value range: • TRUE: Indicates a forced shutdown after a normal shutdown fails • FALSE: Indicates no forced shutdown after a normal shutdown fails Default value: FALSE. Example: false
StoppedMode	No	No	String	Shutdown mode of an instance. Value range: • SOFT_FIRST: Indicates forced shutdown after normal shutdown fails • HARD: Directly perform forced shutdown • SOFT: Soft shutdown only Default value: SOFT. Example: KEEP_CHARGING
StopType	No	No	String	Shutdown mode of an instance. Value range: SOFT_FIRST: Indicates forced shutdown after normal shutdown fails; HARD: Directly perform forced shutdown; SOFT: Soft shutdown only; Default value: SOFT. Example: SOFT
DryRun	No	No	Bool	Internal parameter trial run. Example: false

3. Output Parameters

Parameter name	Type	Description
TaskId	String	Task ID Example: 542324
flowId	Int64	Task Flow ID Example: 5
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidInstanceId.NotFound	No corresponding instance was found.
InvalidInstance.NotSupported	Unsupported instance.
InternalServerError	Internal operation error.
InvalidParameterValue.LimitExceeded	The parameter value is out of range
InvalidParameterValue	Invalid parameter value. The format of the parameter value is incorrect or not supported, etc.
MissingParameter	Parameters are missing. The request did not include mandatory parameters.
InvalidInstanceId.Malformed	Invalid Instance ID. The format of the specified instance ID is incorrect, for example, an instance ID length error ins-1122 .
UnsupportedOperation.InstanceStateStopped	The request does not support instances that are shut down.

SwitchParameterRunInstances

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

This API has been discontinued for maintenance from April 14, 2022.
This API (SwitchParameterRunInstances) is used to create one or more instances with a specified configuration, supporting parameter conversion.

- After an instance is successfully created, it will automatically start up, and the Instance Status will change to Running.
- The purchase of prepaid instances will deduct the amount required for the instance purchase in advance. The purchase of pay-per-hour postpaid instances will freeze the amount required for the instance purchase within 1 hour in advance. Make sure your account balance is sufficient before calling this API.
- This API is an asynchronous API. After the creation request is successfully sent, a list of instance IDs will be returned. At this point, the creation of the instance is not immediately completed. During this period, the instance status will be Preparing. You can query the status of the corresponding instance by calling the API DescribeInstancesStatus to determine whether the production ultimately succeeded. If the instance status changes from Preparing to Running, it indicates that the instance is successfully created.

Default interface request rate limit: 10 times per second.

Interface update time: 2022-11-30 07:47:38.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: SwitchParameterRunInstances
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available

Parameter name	Required	Allow NULL	Type	Description
				through the DescribeRegions interface
HostName	No	No	String	1 Example: alice
ClientToken	No	No	String	1 Example: 98114f60-c600-4fe4-84a4-f9b303d11fe6
Placement	Yes	No	Placement	1 Example:View
InstanceChargePrepaid	No	No	InstanceChargePrepaid	1 Example:View
InstanceChargeType	No	No	String	1 Example: PREPAID
InstanceType	No	No	String	1 Example: S1.SMALL1
ImageId	Yes	No	String	1 Example: img-6mre94jv
SystemDisk	No	No	SystemDisk	1 Example:View
DataDisks	No	No	Array of DataDisk	1 Example:View
VirtualPrivateCloud	No	No	VirtualPrivateCloud	1 Example:View
InternetAccessible	No	No	InternetAccessible	1 Example:View
InstanceCount	No	No	Int64	1 Example: 1
InstanceName	No	No	String	1 Example: alice-1
LoginSettings	No	No	LoginSettings	1 Example:View
SecurityGroupIds	No	No	Array of String	1 Example: ["sec-61dyt49h"]

Parameter name	Required	Allow NULL	Type	Description
EnhancedService	No	No	EnhancedService	1 Example:View
DryRun	No	No	Bool	1 Example: true
UserData	No	No	String	1 Example: SKADAFKASPOASDASFOSAC==
AvailableZone	No	No	String	1 Example: region1
PurchaseSource	No	No	String	1 Example: MC
DisasterRecoverGroupIds	No	No	Array of String	1 Example: ["ps-l86ok62z"]
DesAction	No	No	String	1 Example: GetRecycleInfo
ActionTimer	No	No	ActionTimer	1 Example:View

3. Output Parameters

Parameter name	Type	Description
InstanceOrder	InstanceOrder	Detailed information of instance order. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	Invalid parameter value. The format of the parameter value is incorrect or

Error Code	Description
	not supported, etc.
AccountQualificationRestrictions	The requesting account did not pass the qualification audit.
InvalidParameterValue.Range	Invalid parameter value. The range of the parameter value is not legal.
InvalidInstanceName.TooLong	The string length of the specified InstanceName exceeds the limit. It should be less than or equal to 60 bytes.
InvalidParameterCombination	It indicates that the parameter combination is incorrect.
InvalidInstanceType.Malformed	The parameter format of the specified InstanceType is invalid.
InvalidHostId.NotFound	The specified HostId does not exist, or does not belong to the requesting account.
InvalidPeriod	Invalid duration. Currently, only the following durations are supported: [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 24, 36], unit: months.
InstancesQuotaLimitExceeded	It indicates that the number of instances being created exceeds the remaining quota allowed for purchase by the account.
InvalidZone.MismatchRegion	The specified zone does not exist.
InvalidClientToken.TooLong	The string length of the specified ClientToken exceeds the limit. It should be less than or equal to 64 bytes.
MissingParameter	Parameters are missing. The request did not include mandatory parameters.
InvalidPassword	Invalid password. The specified password does not meet password complexity restrictions. For example, the password length does not meet restrictions.
VpcIpIsUsed	The VPC IP has already been used.
VpcAddrNotInSubNet	The VPC IP is not within the subnet.
InvalidPermission	The account does not support this operation.

TerminateInstances

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

This API (TerminateInstances) is used to proactively return instances.

- Instances that are no longer required can be proactively returned through this API.
- Pay-as-you-go instances can be directly proactively returned through this API. Monthly subscription instances that comply with the return rules can also be proactively returned through this API.
- Batch operations are supported. A maximum of 100 batch instances per request are allowed.

Default interface request rate limit: 10 times per second.

Interface update time: 2022-10-28 03:46:28.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: TerminateInstances
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
InstanceIds	Yes	No	Array of String	One or more instance IDs to be operated. You can obtain the instance ID through the InstanceId in the returned value from the API DescribeInstances. A maximum of 100 batch instances per request are allowed. Example: ['ins-2pajzo4q']
ReleaseAddress	No	No	Bool	Internal parameters, release the elastic IP. Example: true
DryRun	No	No	Bool	Trial run. Example: false
RemainTime	No	No	Int64	Duration Example: 0

3. Output Parameters

Parameter name	Type	Description
TaskId	String	Task ID Example: 543225
flowId	Int64	Task Flow ID Example: 4
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidInstance.NotSupported	Unsupported instance.
InvalidParameterValue	Invalid parameter value. The format of the parameter value is incorrect or not supported, etc.
InternalServerError	Internal operation error.
InvalidParameterValue.LimitExceeded	The parameter value is out of range
InvalidInstanceId.Malformed	Invalid Instance ID. The format of the specified instance ID is incorrect, for example, an instance ID length error ins-1122 .
MissingParameter	Parameters are missing. The request did not include mandatory parameters.
InvalidInstanceNotSupportedPrepaidInstance	The instance does not comply with the return rules for monthly subscription instances.

ViewModifyInstancesAttribute

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

This API is used to modify the attributes of instances. Currently, only the instance name can be modified.

- The instance name is used only for management by users. The cloud platform does not use this name for submitting tickets or performing instance management operations.
- Batch operations are supported. Each request can involve up to 100 instances.

Default interface request rate limit: 10 times per second.

Interface update time: 2025-07-31 03:24:07.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ViewModifyInstancesAttribute
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
InstanceIds	Yes	No	Array of String	One or more instance IDs to be operated. You can obtain the instance ID through the InstanceId in the returned value from the API DescribeInstances. A maximum of 100 batch instances per request are allowed. Example: ["ins-rf6ogz49"]
InstanceName	No	No	String	Instance display name. It can be named as required, but should not exceed 60 characters. Example: MyInsName
UserData	No	No	String	Internal parameters, user data. Example: TXIVc2VyRGF0YQo
SecurityGroups	No	No	Array of String	Internal parameters, list of security group IDs. Example: ["sg-rf6ogz49"]
ResetNewCreationIdentify	No	No	Bool	Internal parameters, unknown. Example: false
DisableApiTermination	No	No	Bool	Instance destruction protection flag, indicating whether deletion through APIs is allowed. Valid values: • TRUE: instance protection is enabled and deletion through APIs is not allowed • FALSE: instance protection is disabled and deletion through APIs is allowed Default value: FALSE. Example: false

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.LimitExceeded	The parameter value is out of range
InternalServerError	Internal operation error.
InvalidInstanceName.TooLong	The string length of the specified InstanceName exceeds the limit. It should be less than or equal to 60 bytes.
InvalidInstance.NotSupported	Unsupported instance.
InvalidInstanceId.NotFound	No corresponding instance was found.
MissingParameter	Parameters are missing. The request did not include mandatory parameters.
InvalidInstanceId.Malformed	Invalid Instance ID. The format of the specified instance ID is incorrect, for example, an instance ID length error ins-1122 .
InvalidParameterValue	Invalid parameter value. The format of the parameter value is incorrect or not supported, etc.

Instance Launch Template APIs
CreateLaunchTemplate

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

This API (CreateLaunchTemplate) is used to create an instance launch template.

An instance launch template is a type of configuration data and can be used to create instances. Its content includes configurations required to create instances, such as instance type, types and sizes of data disk and system disk, security groups, and other information.

Default interface request rate limit: 20 times per second.

Interface update time: 2023-03-18 07:13:24.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CreateLaunchTemplate
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
LaunchTemplateName	Yes	No	String	Name of an instance launch template. It contains 2 to 128 English characters. Example: MyLaunchTemplate
Placement	Yes	No	Placement	Location of the instance. You can specify attributes such as availability zone, project, and host (specified when creating a instance on the CDH) to which the instance belongs through this parameter. Example:View
ImageId	Yes	No	String	Specifies a valid Image ID in the formats such as img-xxx. There are four types of images: 1. Public Image 2. Custom Image 3. Shared Image 4. Service Market Image. The IDs of the Public Image, Custom Image, and Shared Image can be found by logging in to the Console. The ID of the Service Market Image can be found in the Cloud Marketplace. By calling the DescribeImages API and inputting InstanceType, you can get the list of images supported by th Example: img-dkwyg5lor
LaunchTemplateVersionDescription	No	No	String	Version description of an instance launch template. It contains 2 to 256 English characters. Example: MyLaunchTemplateVersionDesc
InstanceType	Yes	No	String	Instance model. Different instance models specify different resource specifications. Example: S5.16XLARGE256
SystemDisk	No	No	SystemDisk	Instance system disk configuration information. If this parameter is not specified, it will be assigned based on the system default values. Example:View
DataDisks	No	No	Array of DataDisk	Array of DataDisk Instance data disk configuration information. If this parameter is not specified, no data disks are purchased by default. A maximum of 21 data disks can be specified when purchasing, including up to one LOCAL_BASIC or LOCAL_SSD data disk and up to 20 CLOUD_BASIC , CLOUD_PREMIUM , or CLOUD_SSD data disks. Example:View
VirtualPrivateCloud	No	No	VirtualPrivateCloud	VPC-related information configuration. You can specify information such as VPC ID and subnet ID through this parameter. If this parameter is not specified, use the basic network by default. If a VPC IP is specified in this parameter, it indicates the primary network interface card IP of each instance. In addition, the number of the InstanceCount parameter should be consistent with the number of the VPC IP and should not exceed 20. Example:View
InternetAccessible	No	No	InternetAccessible	Public bandwidth-related settings. If this parameter is not specified, the public bandwidth is 0 Mbps by default. Example:View
InstanceCount	No	No	Int64	Number of instances to purchase. For monthly subscription instances, the value range is [1,300]. For pay-as-you-go instances, the value range is [1,100]. Default value: 1. The specified number of instances to purchase should not exceed the remaining quota of the user. For specific restrictions on quota, see the CVM instance purchase restrictions. Example: 1
InstanceName	No	No	String	Instance display name. Example: MyInstance
LoginSettings	No	No	LoginSettings	Instance login settings. You can set login method, password, or key of the instance or retain the original login settings of the image. By default, a password will be randomly generated and notified to the user through Message Center. Example:View
SecurityGroupIds	No	No	Array of String	Security groups to which an instance belongs. You can obtain this parameter through the sgId field in the returned value by calling DescribeSecurityGroups. If this parameter is not specified, bind the security group by default. Example: ["sg-efbcgy4R"]
EnhancedService	No	No	EnhancedService	Enhanced services. You can specify whether to enable services such as Cloud Security and Cloud Monitor through this parameter. If this parameter is not specified, the Cloud Monitor and Cloud Security is enabled by default. For custom images and image market images, the Cloud Monitor and Cloud Security is not enabled by default. Instead, they use services retained in the images. Example:View
ClientToken	No	No	String	String used to ensure request idempotency. This string is generated by the customer and should be unique across different requests. The maximum length should be no more than 64 ASCII characters. If this parameter is not specified, the idempotency of the request cannot be ensured. Example: 123asfa423fdasq5twerra
HostName	No	No	String	The HostName for Cloud Virtual Machine (CVM) cannot have a dot (.) or hyphen (-) at the beginning or end, and they can not be used consecutively. Windows instances: The name must have [2, 15] characters, which can include letters (case insensitive), numbers, and hyphens (-), but cannot include dots (.) or be comprised entirely of numbers. Other types of instances (such as Linux): The name must have [2, 60] characters, which can include multiple dots, Example: zhangsan
ActionTimer	No	No	Datetime	Scheduled task. You can specify a scheduled task for the instance through this parameter. Currently, only scheduled termination is supported. Example: 2014-08-03 12:00:00
DisasterRecoverGroupIds	No	No	Array of String	Placement group ID, only one can be specified. Example: ["prs-3p88qhfo"]
TagSpecification	No	No	Array of TagSpecification	List of tag descriptions. You can bind tags to corresponding resource instances at the same time by specifying this parameter. Currently, only binding tags to the CVM is supported. Example:View
UserData	No	No	String	User data provided for the instance, should be encoded in base64 format, supports a maximum data size of 16 KB. Example: YmFzZTY0Cg==
CamRoleName	No	No	String	CAM role name. Can be obtained through the roleName in the returned value from the API DescribeRoleList. Example: roleName001
HpcClusterId	No	No	String	High-performance computing cluster ID. If the created instance is a high-performance computing instance, the cluster where the instance is placed should be specified. Otherwise, it cannot be specified. Example: hpc-a5n66i8o
InstanceChargeType	No	No	String	Instance billing type. Example: PREPAID
InstanceChargePrepaid	No	No	InstanceChargePrepaid	Prepaid mode, that is, monthly subscription-related parameter settings. You can specify attributes of a monthly subscription instance, such as purchase duration and whether to set auto-renewal, through this parameter. If the billing mode of the specified instance is prepaid mode, this parameter is required. Example:View
DisableApiTermination	No	No	Bool	Instance termination protection flag, indicating whether the instance is allowed to be deleted through the API. Value range: • TRUE: Indicates that instance protection is enabled, and the instance is not allowed to be deleted through the API • FALSE: Indicates that instance protection is disabled, and the instance is allowed to be deleted through the API Default value: FALSE. Example: false
ProjectSpecification	No	No	Array of ProjectSpecification	Project specifications. Example:View

3. Output Parameters

Parameter name	Type	Description
LaunchTemplateId	String	When an instance launch template is created through this API, this parameter will be returned, indicating the successfully created instance launch template ID. Example: lt-a5s125lo
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
AccountQualificationRestrictions	The requesting account did not pass the qualification audit.
FailedOperation.DisasterRecoverGroupNotFound	The specified disaster recovery group was not found.
FailedOperation.InquiryPriceFailed	Failed to get the cost
FailedOperation.NoAvailableIpAddressCountInSubnet	The available IPs in the subnet are exhausted.
FailedOperation.SnapshotSizeLargerThanDataSize	The snapshot capacity exceeds the disk size. Choose a larger disk space.
InternalError	Internal error
InvalidParameterValueLimit	The parameter value is out of range
InvalidParameterCombination	It indicates that the parameter combination is incorrect.
InvalidParameter.ValueTooLarge	The parameter length exceeds the limit.
VpcAddrNotInSubNet	The VPC IP is not within the subnet.
InvalidInstanceType.Malformed	The parameter format of the specified InstanceType is invalid.
InvalidClientToken.TooLong	The string length of the specified ClientToken exceeds the limit. It should be less than or equal to 64 bytes.
InvalidImageOsType.Unsupported	Unsupported operating system type.
InvalidParameter.InvalidIpFormat	The specified VPC IP format is incorrect.
ImageQuotaLimitExceeded	The image quota has exceeded the limit.
InvalidCloudDisk.SoldOut	The cloud disk has been sold out.
SecGroupActionFailure	General error in security group service API calling.
FailedOperation.NoAvailableInstanceType	No available instance types.

DeleteLaunchTemplate

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

This API (DeleteLaunchTemplate) is used to delete an instance launch template.

Default interface request rate limit: 20 times per second.

Interface update time: 2025-08-20 00:35:49.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteLaunchTemplate
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
LaunchTemplateId	Yes	No	String	Launch template ID. Example: lt-rf6ogz49

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error
InvalidPermission	The account does not support this operation.
InvalidParameterCombination	It indicates that the parameter combination is incorrect.
InvalidParameterValue.LaunchTemplateIdNotExisted	The instance launch template ID does not exist.

DeleteLaunchTemplates

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

This API (DeleteLaunchTemplates) is used to delete one or more instance launch templates.

Default interface request rate limit: 20 times per second.

Interface update time: 2025-08-20 00:37:33.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteLaunchTemplates
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
LaunchTemplateIds	Yes	No	Array of String	Launch template ID. Example: ["lt-34vaef8fe"]

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request

Parameter name	Type	Description
		needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error
InvalidPermission	The account does not support this operation.
InvalidParameterCombination	It indicates that the parameter combination is incorrect.
InvalidParameterValue.LaunchTemplateIdMalformed	The format of the instance launch template ID is incorrect.
InvalidParameterValue.LaunchTemplateIdNotExisted	The instance launch template ID does not exist.
InvalidParameterValue.LaunchTemplateNotFound	The instance launch template was not found.

DescribeLaunchTemplatesInfo

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

This API (DescribeLaunchTemplatesInfo) is used to query detailed information of one or more instance launch templates.

Default interface request rate limit: 20 times per second.

Interface update time: 2025-08-20 00:39:19.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeLaunchTemplatesInfo
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
LaunchTemplateIds	No	No	Array of String	Launch template ID, one or more launch template IDs. If it is not specified, all templates of the user will be displayed by default. Example: ["lt-k8wrok8e"]
Filters	No	No	Array of Filter	Filter by [LaunchTemplateName]. Example:View
Offset	No	No	Int64	Offset, 0 by default. Example: 0
Limit	No	No	Int64	Number of returns, 20 by default, and the maximum value is 100. Example: 20

3. Output Parameters

Parameter name	Type	Description
TotalCount	Int64	Number of eligible instance templates. Note: This field may return null, indicating that no valid values can be obtained. Example: 50
LaunchTemplateSet	Array of LaunchTemplatesInfo	List of detailed information of instances. Note: This field may return null, indicating that no valid values can be obtained. Example:View
LaunchTemplateInfoSet	Array of LaunchTemplatesInfo	List of detailed information of instances. Note: This field may return null, indicating that no valid values can be obtained. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidFilter	Invalid filter.
InvalidParameterValue.LaunchTemplateIdMalformed	The format of the instance launch template ID is incorrect.
InvalidParameterValue.LaunchTemplateIdNotExisted	The instance launch template ID does not exist.
InvalidParameterValue.LaunchTemplateIdVerNotExisted	The combination of the instance launch template and version ID does not exist.
InvalidParameterValue.LaunchTemplateNotFound	The instance launch template was not found.
InvalidParameterValue.LaunchTemplateVersion	Version number of invalid instance launch template.
InvalidParameterValue.InvalidLaunchTemplateName	The format of the instance launch template name is incorrect.
InvalidParameter	Invalid parameter. The parameter does not meet the requirements, is not supported, or the like.

ModifyLaunchTemplate

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

This API (ModifyLaunchTemplate) is used to modify the instance launch template.

An instance launch template is a type of configuration data and can be used to create instances. Its content includes configurations required to create instances, such as instance type, types and sizes of data disk and system disk, security groups, and other information.

Default interface request rate limit: 20 times per second.

Interface update time: 2025-08-20 00:51:33.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyLaunchTemplate
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
LaunchTemplateName	No	No	String	Name of an instance launch template. It contains 2 to 128 English characters. Example: jack_use
Placement	Yes	No	Placement	Location of the instance. You can specify attributes such as availability zone, project, and host (specified when creating a instance on the CDH) to which the instance belongs through this parameter. Example:View
ImageId	Yes	No	String	Specifies a valid Image ID in the formats such as img-xxx. There are four types of images: 1. Public Image 2. Custom Image 3. Shared Image 4. Service Market Image. The IDs of the Public Image, Custom Image, and Shared Image can be found by logging in to the Console. The ID of the Service Market Image can be found in the Cloud Marketplace. By calling the DescribeImages API and inputting InstanceType, you can get the list of images supported by th Example: img-c1otswj
LaunchTemplateVersionDescription	No	No	String	Version description of an instance launch template. It contains 2 to 256 English characters. Example: jack use
InstanceType	Yes	No	String	Instance model. Different instance models specify different resource specifications. Example: S2.SMALL1
SystemDisk	No	No	SystemDisk	Instance system disk configuration information. If this parameter is not specified, it will be assigned based on the system default values. Example:View
DataDisks	No	No	Array of DataDisk	Array of DataDisk Instance data disk configuration information. If this parameter is not specified, no data disks are purchased by default. A maximum of 21 data disks can be specified when purchasing, including up to one LOCAL_BASIC or LOCAL_SSD data disk and up to 20 CLOUD_BASIC , CLOUD_PREMIUM , or CLOUD_SSD data disks. Example:View
VirtualPrivateCloud	No	No	VirtualPrivateCloud	VPC-related information configuration. You can specify information such as VPC ID and subnet ID through this parameter. If this parameter is not specified, use the basic network by default. If a VPC IP is specified in this parameter, it indicates the primary network interface card IP of each instance. In addition, the number of the InstanceCount parameter should be consistent with the number of the VPC IP and should not exceed 20. Example:View
InternetAccessible	No	No	InternetAccessible	Public bandwidth-related settings. If this parameter is not specified, the public bandwidth is 0 Mbps by default. Example:View
InstanceCount	Yes	No	Int64	Number of instances to purchase. For monthly subscription instances, the value range is [1,300]. For pay-as-you-go instances, the value range is [1,100]. Default value: 1. The specified number of instances to purchase should not exceed the remaining quota of the user. For specific restrictions on quota, see the CVM instance purchase restrictions. Example: 30
InstanceName	No	No	String	Instance display name. Example: jack-use
LoginSettings	No	No	LoginSettings	Instance login settings. You can set login method, password, or key of the instance or retain the original login settings of the image. By default, a password will be randomly generated and notified to the user through Message Center. Example:View
SecurityGroupIds	No	No	Array of String	Security groups to which an instance belongs. You can obtain this parameter through the sgId field in the returned value by calling DescribeSecurityGroups. If this parameter is not specified, bind the security group by default. Example: ["sec-3ad6dgq5"]
EnhancedService	No	No	EnhancedService	Enhanced services. You can specify whether to enable services such as Cloud Security and Cloud Monitor through this parameter. If this parameter is not specified, the Cloud Monitor and Cloud Security is enabled by default. For custom images and image market images, the Cloud Monitor and Cloud Security is not enabled by default. Instead, they use services retained in the images. Example:View
ClientToken	No	No	String	String used to ensure request idempotency. This string is generated by the customer and should be unique across different requests. The maximum length should be no more than 64 ASCII characters. If this parameter is not specified, the idempotency of the request cannot be ensured. Example: 5b310d86-0bf4-48e1-8cdb-d2e0ca5d04fa
HostName	No	No	String	The HostName for Cloud Virtual Machine (CVM) cannot have a dot (.) or hyphen (-) at the beginning or end, and they can not be used consecutively. Windows instances: The name must have [2, 15] characters, which can include letters (case insensitive), numbers, and hyphens (-), but cannot include dots (.) or be comprised entirely of numbers. Other types of instances (such as Linux): The name must have [2, 60] characters, which can include multiple dots, . Example: jenny
ActionTimer	No	No	Datetime	Scheduled task. You can specify a scheduled task for the instance through this parameter. Currently, only scheduled termination is supported. Example: 2014-08-03 12:00:00
DisasterRecoverGroupIds	No	No	Array of String	Placement group ID, only one can be specified. Example: ["sn-86ok62x"].
TagSpecification	No	No	Array of TagSpecification	List of tag descriptions. You can bind tags to corresponding resource instances at the same time by specifying this parameter. Currently, only binding tags to the CVM is supported. Example:View
UserData	No	No	String	User data provided for the instance, should be encoded in base64 format, supports a maximum data size of 16 KB. Example: ZiAiPS9KIiSAKKI===
CamRoleName	No	No	String	CAM role name. Can be obtained through the roleName in the returned value from the API DescribeRoleList. Example: roleName001
HpcClusterId	No	No	String	High-performance computing cluster ID. If the created instance is a high-performance computing instance, the cluster where the instance is placed should be specified. Otherwise, it cannot be specified. Example: hpc-g5obwc5o
InstanceChargeType	No	No	String	Instance billing type. Example: POSTPAID_BY_HOUR
InstanceChargePrepaid	No	No	InstanceChargePrepaid	Prepaid mode, that is, monthly subscription-related parameter settings. You can specify attributes of a monthly subscription instance, such as purchase duration and whether to set auto-renewal, through this parameter. If the billing mode of the specified instance is prepaid mode, this parameter is required. Example:View
DisableApiTermination	No	No	Bool	Instance termination protection flag, indicating whether the instance is allowed to be deleted through the API. Value range: • TRUE: Indicates that instance protection is enabled, and the instance is not allowed to be deleted through the API. • FALSE: Indicates that instance protection is disabled, and the instance is allowed to be deleted through the API. Default value: FALSE. Example: TRUE
LaunchTemplateId	Yes	No	String	Instance Template ID Example: lt-k8vnxtdle

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
AccountQualificationRestrictions	The requesting account did not pass the qualification audit.
FailedOperation.DisasterRecoverGroupNotFound	The specified disaster recovery group was not found.
FailedOperation.InquiryPriceFailed	Failed to get the cost
FailedOperation.NoAvailableIpAddressCountInSubnet	The available IPs in the subnet are exhausted.
FailedOperation.SnapshotSizeLargerThanDataSize	The snapshot capacity exceeds the disk size. Choose a larger disk space.
InternalError	Internal error
InvalidParameterValueLimit	The parameter value is out of range
InvalidParameterCombination	It indicates that the parameter combination is incorrect.
InvalidParameterValueTooLarge	The parameter length exceeds the limit.
VpcAddrNotInSubNet	The VPC IP is not within the subnet.
InvalidInstanceType.Malformed	The parameter format of the specified InstanceType is invalid.
InvalidClientToken.TooLong	The string length of the specified ClientToken exceeds the limit. It should be less than or equal to 64 bytes.
InvalidImageOsType.Unsupported	Unsupported operating system type.
InvalidParameterInvalidIpFormat	The specified VPC IP format is incorrect.
ImageQuotaLimitExceeded	The image quota has exceeded the limit.
InvalidCloudDisk.SoldOut	The cloud disk has been sold out.
SecGroupActionFailure	General error in security group service API calling.
FailedOperation.NoAvailableInstanceType	No available instance types.

ModifyLaunchTemplateName

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

This API (ModifyLaunchTemplateName) is used to modify the name of an instance launch template.

Default interface request rate limit: 20 times per second.

Interface update time: 2025-08-20 00:52:23.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyLaunchTemplateName
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
LaunchTemplateId	Yes	No	String	Launch template ID. Example: lt-k8wrok8e
LaunchTemplateName	Yes	No	String	Launch template name. Example: jack-use

3. Output Parameters

Parameter name	Type	Description

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error
InvalidPermission	The account does not support this operation.
InvalidParameterCombination	It indicates that the parameter combination is incorrect.
InvalidParameterValue.LaunchTemplateIdMalformed	The format of the instance launch template ID is incorrect.
InvalidParameterValue.LaunchTemplateIdNotExisted	The instance launch template ID does not exist.
InvalidParameterValue.LaunchTemplateNotFound	The instance launch template was not found.

Key APIs
AssociateInstancesKeyPairs

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

This API (AssociateInstancesKeyPairs) is used to associate the key with an instance.

- By writing the public key of the key into the SSH configuration of the instance, users can log in to the instance by using the private key of the key.
- If the instance was previously associated with a key, the original key will become invalid.
- If the instance was previously logged in with a password, after associating the key, you cannot use the password to log in.
- Batch operations are supported. A maximum of 100 batch instances per request are allowed. If there are instances in the batch that are not allowed to be operated, operations will be returned with a specific error code.

Default interface request rate limit: 10 times per second.

Interface update time: 2022-10-28 03:51:28.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: AssociateInstancesKeyPairs
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
InstanceIds	Yes	No	Array of String	One or more instance IDs to be operated. A maximum of 100 batch instances per request are allowed. You can obtain an available instance ID in the following ways: • By querying the instance ID by logging in to the Console. • By calling the InstanceId in the returned information from the API DescribeInstances. Example: ["ins-1e4r6y8i","ins-3e56fg78"]
KeyIds	Yes	No	Array of String	One or more key pair IDs to be operated. A maximum of 100 batch instances per request are allowed. The key pair ID is in the format of skey-11112222 . You can obtain an available key pair ID in the following ways: • By querying the key pair ID by logging in to the Console. • By calling the KeyId in the returned information from the API DescribeKeyPairs. Example: ["skey-4e5ty7i8"]
ForceStop	No	No	Bool	Whether to perform forced shutdown on the running instance. It is recommended to perform manual shutdown on the running instance first, and then reset the user password. Value Range: • TRUE: Indicates forced shutdown performed after normal shutdown fails. • FALSE: Indicates no forced shutdown performed after normal shutdown fails. Default value: FALSE. Example: true

3. Output Parameters

Parameter name	Type	Description
TaskId	String	Task ID Example: 345342
FlowId	Int64	Task Flow ID Example: 2
flowId	Int64	Task Flow ID Example: 2
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidInstanceId.NotFound	No corresponding instance was found.
InvalidInstance.NotSupported	Unsupported instance.
InvalidParameterValue	Invalid parameter value. The format of the parameter value is incorrect or not supported, etc.
InvalidKeyPairId.Malformed	Invalid key pair ID. The format of the specified key pair ID is incorrect, for example, an ID length error skey-1122 .
InternalServerError	Internal operation error.
InvalidParameterValue.LimitExceeded	The parameter value is out of range
InvalidInstanceId.Malformed	Invalid Instance ID. The format of the specified instance ID is incorrect, for example, an instance ID length error ins-1122 .
InvalidKeyPairId.NotFound	Invalid key pair ID. The specified key pair ID does not exist.
MissingParameter	Parameters are missing. The request did not include mandatory parameters.

CreateKeyPair

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

This API is used to create an OpenSSH RSA key pair, which can be used to log in to a Linux instance.

- Developers only need to specify the key pair name. The system will automatically create the key pair and return the ID, public key, and private key of the generated key pair.
- The key pair name cannot be the same as that of existing key pairs.
- The private key can be saved to a file for SSH authentication.
- The cloud platform will not save the private key. Please keep it properly.

Default interface request rate limit: 10 times per second.

Interface update time: 2022-04-20 03:42:29.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CreateKeyPair
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
KeyName	Yes	No	String	Key pair name, which can include numbers, letters, and underscores, with a length not exceeding 25 characters. Key pair names should be different from existing ones. Example: alice_use
ProjectId	Yes	No	Int64	Can only be set to 0. Example: 0

3. Output Parameters

Parameter name	Type	Description
KeyPair	CreateKeyPair	Key pair information. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidProjectId.NotFound	Invalid project ID. The specified project ID does not exist.
InternalServerError	Internal operation error.
InvalidKeyPairNameEmpty	The key name is empty.
InvalidParameterValue	Invalid parameter value. The format of the parameter value is incorrect or not supported, etc.
MissingParameter	Parameters are missing. The request did not include mandatory parameters.
InvalidKeyPairName.Duplicate	The key pair names are duplicate.
InvalidKeyPair.LimitExceeded	The number of key pairs exceeds the limit.
InvalidKeyPairNameTooLong	The key name exceeds 25 characters.
InvalidKeyPairNameIncludeIllegalChar	The key name includes illegal characters. The key name only supports letters, digits, and underscores.

DeleteKeyPairs

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

This API is used to delete key pairs managed on the cloud platform.

- Multiple key pairs can be deleted at the same time.
- Key pairs referenced by instances or images cannot be deleted. Therefore, it is necessary to independently determine whether each key pair is successfully deleted.

Default interface request rate limit: 10 times per second.

Interface update time: 2018-04-04 09:23:06.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteKeyPairs
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
KeyIds	Yes	No	Array of String	One or more key pair IDs to be operated. A maximum of 100 batch instances per request are allowed. You can obtain an available key pair ID in the following ways: • By querying the key pair ID by logging in to the Console. • By calling the KeyId in the returned information from the API DescribeKeyPairs. Example: ["skey-mv9yzyjj"]

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	Invalid parameter value. The format of the parameter value is incorrect or not supported, etc.
InvalidKeyPairId.Malformed	Invalid key pair ID. The format of the specified key pair ID is incorrect, for example, an ID length error skey-1122 .

Error Code	Description
InvalidKeyPair.LimitExceeded	The number of key pairs exceeds the limit.
InternalServerError	Internal operation error.
InvalidParameterValue.LimitExceeded	The parameter value is out of range
MissingParameter	Parameters are missing. The request did not include mandatory parameters.
InvalidParameterValue.KeyPairNotSupported	The key is not supported.

DescribeKeyPairs

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

This API (DescribeKeyPairs) is used to query key pair information.

- A key pair is a pair of keys generated through an algorithm, including two keys: one is made public, known as the public key, the other is retained by the user, known as the private key. For a key pair, content of the public key can be queried through this API, but content of the private key is not retained by the system.

Default interface request rate limit: 10 times per second.

Interface update time: 2018-04-04 09:23:06.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeKeyPairs
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
KeyIds	No	No	Array of String	Key pair ID. The key pair ID is in the format of skey-11112222 (This API supports filtering by passing multiple IDs at the same time. For the specific format of this parameter, see the section id.N in the API Introduction). This parameter does not support specifying KeyIds and Filters at the same time. You can query the key pair ID by logging in to the Console. Example: skey-11112222
Filters	No	No	Array of Filter	Filter conditions support: key-name, tag-key, and tag-value. Parameters KeyIds and Filters cannot be specified at the same time. Example:View
Offset	No	No	Int64	Offset, 0 by default. For further introduction to the Offset , see relevant sections in the API Introduction. Example: 0
Limit	No	No	Int64	Number of returns, 20 by default, and the maximum value is 100. For further introduction to the Limit , see relevant sections in the API Introduction. Example: 20

3. Output Parameters

Parameter name	Type	Description
TotalCount	Int64	Number of eligible key pairs. Example: 1
KeyPairSet	Array of KeyPair	List of detailed information of key pairs. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidFilter	Invalid filter.
InvalidParameterValue	Invalid parameter value. The format of the parameter value is incorrect or not supported, etc.
InvalidParameterValueLimit	The parameter value is out of range
InvalidParameterValueOffset	Invalid parameter value. The specified offset is invalid.
InvalidFilterValue.LimitExceeded	The number of Filter> Filter parameter values exceeds the limit.
InvalidKeyPairId.Malformed	Invalid key pair ID. The format of the specified key pair ID is incorrect, for example, an ID length error skey-1122 .
InvalidKeyPair.LimitExceeded	The number of key pairs exceeds the limit.
InternalServerError	Internal operation error.
InvalidParameter	Invalid parameter. The parameter does not meet the requirements, is not supported, or the like.

DisassociateInstancesKeyPairs

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

This API (DisassociateInstancesKeyPairs) is used to disassociate a key from an instance.

- Only instances in the STOPPED state in the Linux operating system are supported.
- After dissociating the key, you can log in to the instance with the previously set password.
- If no password was previously set, you cannot log in via an SSH key after dissociation. You can call the API ResetInstancesPassword to set a login password.
- Batch operations are supported. A maximum of 100 batch instances per request are allowed. If there are instances in the batch that are not allowed to be operated, operations will be returned with a specific error code.

Default interface request rate limit: 10 times per second.

Interface update time: 2022-10-28 03:52:02.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DisassociateInstancesKeyPairs
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
InstanceIds	Yes	No	Array of String	One or more instance IDs to be operated. A maximum of 100 batch instances per request are allowed. You can obtain an available instance ID in the following ways: • By querying the instance ID by logging in to the Console. • Obtain the key pair ID by calling the InstanceId in the returned information from the API DescribeInstances. Example: ["ins-w34e5rl9"]
KeyIds	Yes	No	Array of String	List of key pair IDs. A maximum of 100 batch key pairs per request are allowed. The key pair ID is in the format of skey-11112222 . You can obtain the available key pair ID in the following ways: • By querying the key ID by logging in to the Console. • By calling the KeyId in the returned information from the API DescribeKeyPairs. Example: ["skey-e3r6y7ji"]
ForceStop	No	No	Bool	Whether to perform forced shutdown on the running instance. It is recommended to perform manual shutdown on the running instance first, and then reset the user password. Value Range: • TRUE: Indicates forced shutdown performed after normal shutdown fails. • FALSE: Indicates no forced shutdown performed after normal shutdown fails. Default value: FALSE. Example: true

3. Output Parameters

Parameter name	Type	Description
TaskId	String	Task ID Example: 432322
flowId	Int64	Task Flow ID Example: 2
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidInstanceId.NotFound	No corresponding instance was found.
InvalidInstance.NotSupported	Unsupported instance.
InvalidParameterValue	Invalid parameter value. The format of the parameter value is incorrect or not supported, etc.
InvalidKeyPairId.Malformed	Invalid key pair ID. The format of the specified key pair ID is incorrect, for example, an ID length error skey-1122 .
InternalServerError	Internal operation error.
InvalidParameterValue.LimitExceeded	The parameter value is out of range
InvalidInstanceId.Malformed	Invalid Instance ID. The format of the specified instance ID is incorrect, for example, an instance ID length error ins-1122 .
InvalidKeyPairId.NotFound	Invalid key pair ID. The specified key pair ID does not exist.
MissingParameter	Parameters are missing. The request did not include mandatory parameters.

ImportKeyPair

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

This API (ImportKeyPair) is used to import key pairs.

- The feature of this API is to import key pairs into the user account without automatically associating them with instances. To associate, you can use the API AssociateInstancesKeyPairs.
- You need to specify the key pair name and the public key text of the key pair.
- If users have only a private key, they can convert the private key into a public key by using the SSL tool and then import it.

Default interface request rate limit: 10 times per second.

Interface update time: 2020-05-19 04:15:05.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ImportKeyPair
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
KeyName	Yes	No	String	Key pair name, can contain digits, letters, and underscores, with no more than 25 characters. Example: operation_key
ProjectId	Yes	No	Int64	Project ID to which key pair belongs after creation. You can obtain a project ID in the following ways: • By querying the project ID through the List of Projects. • By calling the projectId in the returned information from the API DescribeProjects. Example: 0
PublicKey	Yes	No	String	Public key content of key pair, in the format of OpenSSH RSA . Example: ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC0ran+u+y09bSSoAbHBhJm2ivci0uwTif+/MqoGj5odBuGcDHGIBE7Th74ITXtbuqEXxdOSROi7DOVaTZa1MYe6qKGPAi5/8jJV8c9CKCezXr99A2Dps/eVPVn4yO2NhSXbr0U/voRxTqNprP0YLo25y1IVnN0vg0CfWL8DDYh6DkMMVufGikA7WVPdsHomTLlSPdlSLvCRZPHC7eBhkrznO0rnfM+cJY2fqqSrdI1kqtDRJNpNvPLaRnJsc3uoot2nGqrGD6yiwx2tvdLAqgQT5tASfvtTc3CTMMJRGlqm+CdGZS1y0VlMDmm9XHeVBmZuX5YDJPNGIOcBI2Cgrj5 skey-mk5eqeu6

3. Output Parameters

Parameter name	Type	Description
KeyId	String	Key pair ID. Example: skey-4e5ty7i8
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalServerError	Internal operation error.
InvalidKeyPairNameTooLong	The key name exceeds 25 characters.
InvalidKeyPairNameEmpty	The key name is empty.
InvalidKeyPairName.Duplicate	The key pair names are duplicate.
InvalidKeyPair.LimitExceeded	The number of key pairs exceeds the limit.
MissingParameter	Parameters are missing. The request did not include mandatory parameters.
InvalidKeyPairNameIncludeIllegalChar	The key name includes illegal characters. The key name only supports letters, digits, and underscores.
InvalidParameterValue	Invalid parameter value. The format of the parameter value is incorrect or not supported, etc.
InvalidPublicKey.Duplicate	Invalid public key. The specified public key already exists.
InvalidPublicKey.Malformed	Invalid public key. The format of the specified public key format is incorrect and does not meet the OpenSSH RSA format requirements.

ModifyKeyPairAttribute

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

This API (ModifyKeyPairAttribute) is used to modify attributes of a key pair.

- Modify the name and description information of the key pair specified by the key pair ID.
- The key pair name should not be the same as the name of an existing key pair.
- The key pair ID is the unique flag of the key pair and should not be modified.

Default interface request rate limit: 10 times per second.

Interface update time: 2018-04-04 09:23:06.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyKeyPairAttribute
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
KeyId	Yes	No	String	Key pair ID. The key pair ID is in the format of skey-11112222 . You can obtain the key ID in the following ways: • By querying the key ID by logging in to the Console. • By calling the KeyId in the returned information from the API DescribeKeyPairs. Example: skey-mv9yzyjj
KeyName	No	No	String	Modified key pair name, can contain digits, letters, and underscores, with no more than 25 characters. Example: alice_use
Description	No	No	String	Description information of modified key pair. It can be named as required, but should not exceed 60 characters. Example: KeyPair

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	Invalid parameter value. The format of the parameter value is incorrect or not supported, etc.
InvalidKeyPairId.Malformed	Invalid key pair ID. The format of the specified key pair ID is incorrect, for example, an ID length error skey-1122 .
InternalServerError	Internal operation error.
InvalidParameter	Invalid parameter. The parameter does not meet the requirements, is not supported, or the like.

Error Code	Description
InvalidKeyPairId.NotFound	Invalid key pair ID. The specified key pair ID does not exist.
MissingParameter	Parameters are missing. The request did not include mandatory parameters.
InvalidKeyPairName.Duplicate	The key pair names are duplicate.

Other APIs
CreateHpcCluster

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

Create High-Performance Computing Cluster

Default interface request rate limit: 20 times per second.

Interface update time: 2023-12-12 03:31:20.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CreateHpcCluster
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
Zone	Yes	No	String	Availability zone. Example: ap-region1-2
Name	Yes	No	String	Name of high-performance computing cluster. Example: MyHpcCluster
Remark	No	No	String	Remarks on high-performance computing cluster. Example: Remarks

3. Output Parameters

Parameter name	Type	Description
HpcClusterSet	Array of HpcClusterInfo	High-performance computing cluster information. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	Invalid parameter value. The format of the parameter value is incorrect or not supported, etc.
InvalidZone.MismatchRegion	The specified zone does not exist.
UnsupportedOperation.InvalidZone	The zone is invalid.

DeleteHpcClusters

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

Delete High-Performance Computing Cluster

Default interface request rate limit: 20 times per second.

Interface update time: 2023-12-12 03:35:27.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteHpcClusters
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
HpcClusterIds	Yes	No	Array of String	List of high-performance computing cluster IDs. Example: ["hpc-p64fdfa9\r\n"]

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request

Parameter name	Type	Description
		needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
ResourceNotFound.HpcCluster	The high-performance computing cluster does not exist.
ResourceInUse.HpcCluster	The high-performance computing cluster is in use.

DescribeHpcClusters

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

Query High-Performance Cluster Information

Default interface request rate limit: 20 times per second.

Interface update time: 2023-12-12 03:54:51.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeHpcClusters
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
HpcClusterIds	No	No	Array of String	High-performance computing cluster ID array. Example: ["hpc-p64fdfa9"]
Name	No	No	String	Name of high-performance computing cluster. Example: MyCluster
Zone	No	No	String	Availability zone. Example: ap-region1-2
Offset	No	No	Uint64	Offset, 0 by default. Example: 0

Parameter name	Required	Allow NULL	Type	Description
Limit	No	No	Uint64	Current request volume, 20 by default. Example: 20

3. Output Parameters

Parameter name	Type	Description
HpcClusterSet	Array of HpcClusterInfo	High-performance computing cluster information. Example:View
TotalCount	Uint64	Total number of high-performance computing clusters. Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidZone.MismatchRegion	The specified zone does not exist.
InternalError	Internal error

ModifyHpcClusterAttribute

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

Modify the HPC cluster attributes

Default interface request rate limit: 20 times per second.

Interface update time: 2023-12-13 07:37:41.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyHpcClusterAttribute
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
HpcClusterId	Yes	No	String	High-performance computing cluster ID. Example: hpc-jtynq57p
Name	No	No	String	New name of high-performance computing cluster. Example: MyHpcCluster
Remark	No	No	String	New remarks on high-performance computing cluster. Example: alice use

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	Invalid parameter value. The format of the parameter value is incorrect or not supported, etc.
ResourceNotFound.HpcCluster	The high-performance computing cluster does not exist.

Region APIs
DescribeRegions

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

This API (DescribeRegions) is used to query region information.

Default interface request rate limit: 20 times per second.

Interface update time: 2018-01-13 02:31:36.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeRegions
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.

3. Output Parameters

Parameter name	Type	Description
TotalCount	Uint64	Number of Regions Example: 9

Parameter name	Type	Description
RegionSet	Array of RegionInfo	List Information of Region Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

There is no error code related to business logic for this interface, For other error codes, see public ErrorCode.

DescribeZones

1. Interface Description

Interface request domain name: cvm.api3.convergecloud.com.

This API (DescribeZones) is used to query the availability zone information.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-11-16 06:42:28.

The interface only verifies the signature but does not authenticate.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeZones
Version	Yes	No	String	Public parameter, The value of this interface: 2017-03-12
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface

3. Output Parameters

Parameter name	Type	Description
TotalCount	Uint64	Number of Availability Zones Example: 5
ZoneSet	Array of ZoneInfo	List Information of Availability Zone Example:View

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

There is no error code related to business logic for this interface, For other error codes, see public ErrorCode.

Data structure

UserZoneStatusItem

Billing type status of an instance in the availability zone.

Referenced by the following interfaces: DescribeUserZoneStatus

name	required	NULL allowed	type	description
Zone	yes	no	String	Availability Zone Example: region1
InstanceChargeType	yes	no	String	Billing Method Example: PREPAID
Status	yes	no	String	Sales Status Example: AVALIBLE
IsPrimaryZone	no	no	Bool	Whether it is a primary AZ. Example: True

InstanceStatisticsSet

Instance Data Array

Referenced by the following interfaces: DescribeInstanceStatistics

name	required	NULL allowed	type	description
Region	yes	no	String	Region Example: region1
TotalCount	yes	no	Uint64	Total Number of Machines Example: 20
NewInstanceCount	yes	no	Uint64	Total Number of Red Point Hosts (Newly Created Machines) Example: 20
ExpiredInstanceCount	yes	no	Uint64	Total Number of Expired Hosts Example: 20

CreateKeyPair

Describe Key Pair Creation Information

Referenced by the following interfaces: CreateKeyPair

name	required	NULL allowed	type	description
KeyId	yes	yes	String	ID of a key pair, is the unique flag of the key pair. Example: skey-11112222
KeyName	yes	yes	String	Key pair name. Example: alice-key
ProjectId	yes	yes	Uint64	Project ID to which the key pair belongs. Example: 2
PublicKey	yes	yes	String	Plaintext public key of the key pair. Example: ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAAAgQDP0Yw2T4ItUKxyz
PrivateKey	yes	yes	String	Plaintext private key of the key pair. Example: ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAAAgQDP0Yw2T4ItUKxyz
AssociatedInstanceCount	no	yes	Uint64	Number of instances associated with the key. Example: 10
AssociatedImageCount	no	yes	Uint64	Number of images associated with the key. Example: 5

HostTypeConfigSetPrice

Price Information

Referenced by the following interfaces: DescribeZoneHostConfigInfos

name	required	NULL allowed	type	description
UnitPrice	yes	yes	Float	Original price of subsequent total costs, used for the postpaid billing mode, unit: USD. If other time interval items such as UnitPriceSecondStep are returned, this item represents the time interval of (0, 96) hours; if no other time interval items are returned, it represents the full period, that is, (0, ∞) hours. Note: This field may return null, indicating that no valid values can be obtained. Example: 0.64
ChargeUnit	yes	yes	String	Subsequent billing unit, used for postpaid modes. Possible value range: HOUR: Indicates that the billing unit is calculated on a hourly basis. Current scenarios involving this billing unit include: instance pay-per-hour postpaid (POSTPAID_BY_HOUR), bandwidth pay-per-hour postpaid (BANDWIDTH_POSTPAID_BY_HOUR); GB: Indicates that the billing unit is calculated per GB. Current scenarios involving this billing unit include: traffic pay-per-hour postpaid (TRAFFIC_POSTPAID_BY_HOUR). Note: This field may return null, indicating that no valid value was found. Example: 0.64
OriginalPrice	yes	yes	Float	Original price of total prepaid costs, used for the prepaid billing mode, unit: USD. Note: This field may return null, indicating that no valid values can be obtained. Example: 0.64
DiscountPrice	yes	yes	Float	Discount price of total prepaid costs, unit: USD. Note: This field may return null, indicating that no valid values can be obtained. Example: 0.64
OriginalPriceOneYear	no	yes	Float	Original price of total costs of one-year advance payment, used in the prepaid mode, unit: USD. Note: This field may return null, indicating that no valid value was found. Example: 0.64
DiscountPriceOneYear	no	yes	Float	Discount price of total prepaid costs for 1 year, used for the postpaid billing mode, unit: USD. Note: This field may return null, indicating that no valid values can be obtained. Note: This field may return null, indicating that no valid values can be obtained. Example: 0.64

InternetAccessibleModifyChargeType

It describes the network billing.

Referenced by the following interfaces: InquiryPriceModifyInstanceInternetChargeType, ModifyInstanceInternetChargeType, SwitchParameterModifyInstanceInternetChargeType

name	required	NULL allowed	type	description
InternetChargeType	yes	no	String	Online Payment Mode Example: TRAFFIC_POSTPAID_BY_HOUR
InternetMaxBandwidthOut	yes	no	Int64	Public Outbound Bandwidth Value Example: 20

AvailableZoneSet

Availability Zone Details

Referenced by the following interfaces: DescribeUserAvailableZones

name	required	NULL allowed	type	description
ZoneId	yes	yes	String	Availability Zone ID Example: 100001
Status	yes	yes	String	Status Example: SUCCESS
InstanceType	yes	yes	Array of Int64	Instance Type Example: 2

HostResource

Resource Information of CDH Instance

Referenced by the following interfaces: DescribeHosts

name	required	NULL allowed	type	description
CpuTotal	no	no	Uint64	Total Number of CPU Cores of CDH Instance Example: 32
CpuAvailable	no	no	Uint64	Number of Available CPU Cores of CDH Instance Example: 32
MemTotal	no	no	Float	Total Memory Size of CDH Instance (in GiB) Example: 96
MemAvailable	no	no	Float	Available Memory Size of CDH Instance (in GiB) Example: 96
DiskTotal	no	no	Uint64	Total Disk Size of CDH Instance (in GiB) Example: 1000
DiskAvailable	no	no	Uint64	Available Disk Size of CDH Instance (in GiB) Example: 1000
DiskType	no	no	String	CDH Instance Disk Type Example: "LOCAL_SSD"

VirtualPrivateCloud

It describes VPC-related information, including subnet, IP information, etc.

Referenced by the following interfaces: CloneInstance, CreateLaunchTemplate, DescribeInstances, DescribeLaunchTemplatesInfo, InquiryPriceRunInstances, ModifyInstancesVpcAttribute, ModifyLaunchTemplate, RunInstances, SwitchParameterRunInstances

name	required	NULL allowed	type	description
VpcId	yes	no	String	VPC ID, in the format of vpc-xxx . A valid VpcId can be queried by logging in to the Console. Example: vpc-2ij
SubnetId	yes	no	String	VPC subnet ID, in the format of subnet-xxx . You can obtain a valid VPC subnet ID by logging in to the Console. You can also call the API Console and obtain the valid VPC subnet ID through the unSubnetId field returned by the API. Example: subnet-2ks
SubnetName	no	yes	String	VPC subnet name. This parameter is only used as an output parameter. Example: cloud
AsVpcGateway	no	no	Bool	Whether it is used as a public gateway. The public gateway can be used normally only when the instance has a public IP and is located in the VPC. Value range: • TRUE: Indicates that it is used as a public gateway • FALSE: Indicates that it is not used as a public gateway Default value: FALSE. Example: false
PrivateIpAddresses	no	no	Array of String	VPC subnet IP array. You can use this parameter when creating an instance or modifying VPC attributes of an instance. Currently, passing multiple IPs of the same subnet is supported only when creating multiple instances in batches. Example: ["10.0.0.1"]
VpcName	no	yes	String	VPC name. This parameter is only used as an output parameter. Example: 6933:vpc-cfs-474d7bfd7
Ipv6AddressCount	no	no	Int64	Specify the number of randomly generated IPv6 addresses for ENI. Example: 1

RunMonitorServiceEnabled

It describes the information related to the Cloud Monitor service.

Referenced by the following interfaces: CloneInstance, CreateLaunchTemplate, DescribeLaunchTemplatesInfo, InquiryPriceResetInstance, InquiryPriceRunInstances, ModifyLaunchTemplate, ResetInstance, RunInstances, SwitchParameterRunInstances

name	required	NULL allowed	type	description
Enabled	no	no	Bool	Whether to enable the Cloud Monitor service. Value range:

name	required	NULL allowed	type	description
				• TRUE: Indicates that the Cloud Monitor service is enabled • FALSE: Indicates that the Cloud Monitor service is not enabled Default value: TRUE. Example: true

LocalDiskType

Local Disk Specifications

Referenced by the following interfaces: DescribeZoneInstanceConfigInfos

name	required	NULL allowed	type	description
Type	yes	no	String	Local disk type. Example: LOCAL_BASIC
PartitionType	yes	no	String	Local disk attributes. Example: ROOT
MinSize	yes	no	Int64	Minimum value of the local disk. Example: 20
MaxSize	yes	no	Int64	Maximum value of local disk. Example: 100
Required	yes	no	String	Whether the local disk is mandatory during purchasing. Value range: • REQUIRED: indicates mandatory • OPTIONAL: indicates optional. Example: REQUIRED

InstanceTypeConfig

Describes model configuration information of the instance

Referenced by the following interfaces: DescribeInstanceTypeConfigs, DescribeInstancesModification

name	required	NULL allowed	type	description
Zone	no	no	String	Availability zone. Example: ap-region1-2
InstanceType	no	no	String	Instance model. Example: S2.SMALL1
InstanceFamily	no	no	String	Instance model series. Example: S2
GPU	no	no	Int64	Number of GPU cores, unit: cores. Example: 2
GpuCount	no	no	Float	Number of physical GPU cards corresponding to the instance model. The number should be less than 1 for vGPU cards and greater than or equal to 1 for GPU cards in passthrough mode. vGPU is a GPU virtualization technology that splits physical GPU cards for use by different instances. GPU in passthrough mode are directly mounted to instances for use. Example: 1.0
CPU	no	no	Int64	Number of CPU cores, unit: cores. Example: 2
Memory	no	no	Int64	Memory capacity, in GB. Example: 2048
FPGA	yes	no	Uint64	Number of FPGA cores, unit: cores. Example: 2

ProductInfoItem

Product Description Information Items

Referenced by the following interfaces: SwitchParameterAllocateHosts

name	required	NULL allowed	type	description
name	yes	no	String	Information Item Name Example: item-name
value	yes	no	String	Value Corresponding to Information Item Example: item-value

Filter

Describes the key-value pair filter which is used for conditional filtering. For example, ID, name, and status.

- If there are multiple filters, the filters are of AND logic.
- If a filter involves multiple values, the values of this filter are of OR logic.

Take the filter of the [DescribeInstances](instance APIs/DescribeInstances) API as an example. To query instances whose availability zone (zone) is region 1 *and* the billing mode is monthly subscription *or* pay-as-you-go, the filters can be as follows:

```
Filters.1.Name=zone
&Filters.1.Values.1=ap-region1-1
&Filters.2.Name=instance-charge-type
&Filters.2.Values.1=PREPAID
&Filters.3.Values.2=POSTPAID_BY_HOUR
```

Referenced by the following interfaces: DescribeDiagnosticReports, DescribeHosts, DescribeImages, DescribeInstanceConfigInfos, DescribeInstanceStatistics, DescribeInstanceTypeConfigs, DescribeInstanceTypeDisasterGroupBlackList, DescribeInstanceTypeQuota, DescribeInstances, DescribeInstancesModification, DescribeKeyPairs, DescribeLaunchTemplatesInfo, DescribeUserAvailableZones, DescribeUserInstanceQuota, DescribeUserMigrateTasks, DescribeUserZoneStatus, DescribeZoneHostConfigInfos, DescribeZoneHostForSellStatus, DescribeZoneInstanceConfigInfos

name	required	NULL allowed	type	description
Name	yes	no	String	Fields need to be filtered. Example: ip
Values	yes	no	Array of String	Filter value of the field. Example: 12.34.32.11

InstanceOrder

Detailed information of instance order.

Referenced by the following interfaces: SwitchParameterModifyInstanceInternetChargeType, SwitchParameterResetInstancesInternetMaxBandwidth, SwitchParameterResizeInstanceDisks, SwitchParameterRunInstances

name	required	NULL allowed	type	description

InstanceCreateImageAttributeSet

List of Images Created by Instance

Referenced by the following interfaces: DescribeInstancesCreateImageAttributes

name	required	NULL allowed	type	description
InstanceId	yes	no	String	Cloud Host ID Example: ins-61dyt49h
SupportInstanceImage	yes	yes	Bool	Whether to support the instance image. Example: true
SupportOnlineCreateImage	yes	yes	Bool	Whether to support creating an image online. Example: true
SupportCloudinit	yes	yes	Bool	Whether to support cloud initialization. Example: true
NeedPowerOff	yes	yes	Bool	Whether to shut down. Example: true
UnavailableReason	no	yes	String	Reason for unavailability. Example: Need_Enable_Snapshot
SupportPreheat	no	no	Bool	Specifies whether the instance supports the preheating feature. Example: false
SupportPreheatZones	no	no	Array of String	List of AZs supporting preheating. Example: ["ap-city2-1"]
PreheatUnavailableReason	no	yes	String	Code for the reason why preheating is not supported. Example: PREHEAT_NOT_SUPPORTED
UnsupportedPreheatZones	no	yes	UnsupportedPreheatZones	AZs that do not support preheating and the reason codes. Example:View

ImportImageOsListSupported

List of OS Supported by Imported Images

Referenced by the following interfaces: DescribeImportImageOs

name	required	NULL allowed	type	description
linux	yes	no	Array of String	List of Linux Systems Example: ["CentOS"]
windows	yes	no	Array of String	List of Windows Systems Example: ["Windows Server 2016"]

InstancesRecentFailedOperationSet

Latest Failed Operation on Instance

Referenced by the following interfaces: DescribeInstancesRecentFailedOperation

name	required	NULL allowed	type	description
InstanceId	yes	no	String	Instance ID Example: ins-61dyt49h
EventType	yes	no	String	Operation Event Type Example: Modify
CreateTime	yes	no	Datetime	Operation Event Occurrence Time Example: 2014-08-03 12:00:00

RequiredEnhancedService

Require Enhanced Services

Referenced by the following interfaces: DescribeInstanceConfigInfos, DescribeInstancesActionTimer, DescribeLaunchTemplatesInfo, DescribeZoneInstanceConfigInfos, ImportInstancesActionTimer, ModifyInstancesActionTimer, QueryInstancesActionTimer, SwitchParameterRunInstances, UpdateInstancesActionTimer

name	required	NULL allowed	type	description
MonitorService	no	yes	MonitorServiceItem	Monitoring service Example:View

InstanceDeniedActions

List of Instance Operation Restrictions

Referenced by the following interfaces: DescribeInstancesDeniedActions

name	required	NULL allowed	type	description
InstanceId	no	no	String	Instance ID Example: ins-61dyt49h
DeniedActions	no	no	Array of DeniedActions	List of Operation Restrictions Example:View

ImageSet

Image collection.

Referenced by the following interfaces: SyncImages

name	required	NULL allowed	type	description
Region	no	yes	String	Region Info Example: ap-region
ImageId	no	yes	String	Image ID Example: img1111111111

ZoneInfo

AZ Info

Referenced by the following interfaces: DescribeZones

name	required	NULL allowed	type	description
Zone	yes	no	String	Availability zone name. For example, ap-region1-3. Example: ap-region1-3
ZoneName	yes	no	String	Availability zone description. For example, zone 3 in region 1. Example: Zone 3 in region 1
ZoneId	yes	no	String	Availability Zone ID Example: 100003
ZoneState	yes	no	String	Availability zone status Example: AVAILABLE

StorageBlock

HDD Local Storage Information
Referenced by the following APIs: CreateLaunchTemplate, CreateLaunchTemplateVersion, DescribeZoneInstanceConfigInfos, and RunInstances.

Referenced by the following interfaces: DescribeInstanceConfigInfos, DescribeInstancesActionTimer, DescribeLaunchTemplatesInfo, DescribeZoneInstanceConfigInfos, ImportInstancesActionTimer, ModifyInstancesActionTimer, QueryInstancesActionTimer, SwitchParameterRunInstances, UpdateInstancesActionTimer

name	required	NULL allowed	type	description
Type	no	no	String	HDD local storage type, whose value is LOCAL_PRO. Note: This field may return null, indicating that no valid values can be obtained. Example: LOCAL_PRO
MinSize	no	no	Int64	Minimum HDD Local Storage Capacity Note: This field may return null, indicating that no valid value was found. Example: 10
MaxSize	no	no	Int64	Maximum Capacity of HDD Local Storage Note: This field may return null, indicating that no valid values can be obtained. Example: 500

Image

A structure about detailed information of an image, mainly includes the main status and attributes of the image.

Referenced by the following interfaces: DescribeImages

name	required	NULL allowed	type	description
ImageId	no	no	String	Image ID Example: img-19mu3fy3
OsName	no	no	String	Image OS Example: CentOS 8.0 64-bit
ImageType	no	no	String	Image type Example: PRIVATE_IMAGE
CreatedTime	yes	yes	Datetime_iso	Image created Example: 2022-03-21T08:41:45Z
ImageName	yes	no	String	Image name Example: centos
ImageDescription	yes	no	String	Description Example: alice use
ImageSize	yes	no	Int64	Image size Example: 50
Architecture	yes	no	String	Image Architecture Example: x86_64
ImageState	yes	no	String	Instance status Example: NORMAL
Platform	no	no	String	Image Source Platform Example: CentOS
ImageCreator	no	yes	String	Image Creator Example: 1255000041
ImageSource	no	no	String	Image source Example: CREATE_IMAGE
SyncPercent	yes	yes	Int64	Synchronization Percentage Example: null
IsSupportCloudinit	no	yes	Bool	Whether the Image Supports cloud-init Example: true
SnapshotSet	no	yes	Array of Snapshot	Snapshot Information Associated with Image Example:View
IsSupportAutoInstallGPUDriver	yes	yes	Bool	Whether the image supports automatically install the GPU driver. Example: true
OsKey	yes	no	String	Image name Example: centos7.9
ProductCode	no	yes	String	Product Code Example: image-zero
GPUDriverList	yes	no	Array of String	List of GPU Drivers Example: [{ "version": "460.32.03", "name": "NVIDIA-Linux-x86_64-460.32.03", "CUDA": [{ "version": "460.32.03", "name": "CUDA 11.0" }] }]
ImageFormat	yes	no	String	Image format Example: qcow2
OperationMask	yes	no	Int64	Image Operation Mask Example: 64
Flags	yes	no	Array of String	Image Marking Example: centos
DeviceImageId	yes	yes	Int64	Custom Image ID Example: img-c1otssej
IsSupportTat	no	no	Bool	Image Situation Supported by TAT Example: true
OsVersion	no	no	String	Operating system version Example: 0.0.0
OsType	no	no	String	OS type Example: linux
Encrypt	no	no	Bool	Encryption Example: false
BootMode	no	no	String	Boot mode Example: Legacy BIOS
IsCommercial	no	no	Bool	Whether it is for commercial use. Example: false
IsSupportChargeGridLicense	no	no	Bool	Whether the charging grid license is supported. Example: false
ImageIsShared	no	no	Bool	The image has been shared. Example: false
ImagePreheat	no	no	Bool	Image warm-up. Example: false
ImagePreheatZones	no	yes	String	Image warm-up area. Example: null
ImageDeprecated	no	no	Bool	Deprecated image. Example: false
ImageFamily	no	no	String	Image Family Example: business-daily-update
Tags	yes	yes	Array of Tag	List of tags associated with the image. Example:View
Locations	no	no	Array of ImageLocation	Image location information. Example:View
_ImageStatusInner	no	no	Uint64	Internal status of the image, which is used to identify the current image status (for example, creating, normal, and deleting). Example: 1
ImagePreheatPlacement	no	yes	String	Location identifier for image preheating, which is usually the name of an AZ or a location. Example: ap-city1-cdz-haerbin-1

HostItem

Detailed Information of CDH Instance

Referenced by the following interfaces: DescribeHosts

name	required	NULL allowed	type	description
Placement	no	no	Placement	CDH instance location. You can specify attributes such as the availability zone and project to which the instance belongs through this parameter. Example:View
HostId	no	no	String	CDH Instance ID Example: host-61dyt49h
HostType	no	no	String	CDH Instance Type Example: M10
HostName	no	no	String	CDH Instance Name Example: alice-host

name	required	NULL allowed	type	description
HostChargeType	no	no	String	CDH Instance Billing Mode Example: PREPAID
RenewFlag	no	no	String	CDH Instance Auto-Renewal Flag Example: DISABLE_NOTIFY_AND_MANUAL_RENEW
CreatedTime	no	no	Datetime_iso	CDH Instance Creation Time Example: 2014-08-03 12:00:00
ExpiredTime	no	yes	Datetime_iso	CDH Instance Expiration Time Example: 2014-08-03 12:00:00
InstanceIds	no	no	Array of String	List of Instance IDs for Newly Created Cloud Virtual Machines on CDH Instance Example: ["ins-61dyt49hx"]
HostState	no	no	String	CDH Instance Status Example: RUNNING
HostIp	no	no	String	CDH Instance IP Example: 10.21.0.11
HostResource	no	no	HostResource	CDH Instance Resource Information Example:View
CageId	no	no	String	cage id Example: ap-region1-2
OperationMask	no	no	Int64	Operation Mask Example: 62
Tags	no	no	Array of String	Tag Example: ["alice-1"]

KeyQuota

It describes the quotas under the user availability zone.

Referenced by the following interfaces: DescribeUserInstanceQuota

name	required	NULL allowed	type	description
Zone	no	no	String	Availability zone ID to which the instance belongs. Filter by the availability zone. Example: region1
InstanceChargeType	no	no	String	Instance billing mode. Supported types: PREPAID, POSTPAID_BY_HOUR, SPOTPAID. The maximum limit is 10, and the maximum limit of value is 5. Example: POSTPAID_BY_HOUR
QuotaCurrent	yes	no	Uint64	Current quantity Example: 2
QuotaLimit	yes	no	Uint64	Quota Example: 1

RegionInfo

Region Info

Referenced by the following interfaces: DescribeRegions

name	required	NULL allowed	type	description
Region	yes	no	String	Region name. For example, ap-region1. Example: ap-region1
RegionName	yes	no	String	Region description. For example, region 1. Example: Region 1
RegionState	yes	no	String	Whether the region is in an available state. Example: available

ReportDetailSet

ReportDetailSet

Referenced by the following interfaces: DescribeDiagnosticReports

name	required	NULL allowed	type	description
Category	no	no	String	Detection Type Example: Expense
CategoryName	no	no	String	Detection Type Name Example: Account fees detection
Code	no	no	String	Detection Code Example: Instance.Deadline
CodeName	no	no	String	Code Name Example: utf-8
IsAuthorized	no	no	Bool	Authorized Example: false
Message	no	no	String	Information Example: success
Severity	no	no	String	Detection status Example: Normal
Status	no	no	String	Status Example: Finished

HostTypeConfigSet

Obtain CDH model configuration information and a list of information about the sell-out state.

Referenced by the following interfaces: DescribeZoneHostConfigInfos

name	required	NULL allowed	type	description
Zone	yes	yes	String	Availability Zone Example: ap-region1-2
HostType	yes	yes	String	Model. Note: This field may return null, indicating that no valid values can be obtained. Example: M10
HostChargeType	yes	yes	String	CDH Instance Billing Mode Example: PREPAID
HostFamily	yes	yes	String	CDH Type Example: Balance
CPU	yes	yes	Uint64	Number of CPU cores of an instance, unit: cores. Example: 2
Memory	yes	yes	Uint64	Instance memory capacity, in GB. Example: 2048
DiskSize	yes	yes	Uint64	The size of the CBS for creating this snapshot, in GB. Example: 500
DiskType	yes	yes	String	System Disk Type Example: Local Hard Disk
HostQuota	no	yes	Uint64	CDH Quota Example: 5
Price	yes	yes	HostTypeConfigSetPrice	Pricing information Example:View
CpuModeLName	no	yes	String	CPU model name. Example: Intel Xeon Skylake 6133
Status	yes	yes	String	Whether the instance is for sale. Value range: SELL: Indicates that the instance is available for purchase; SOLD_OUT: Indicates that the instance has been sold out. Example: PENDING
SupportCustomizedInstanceType	no	no	Bool	Specifies whether custom models are supported. Example: true
SupportStandardInstanceType	no	no	Bool	Specifies whether standard models are supported. Example: false
SupportStandardInstanceTypeSet	no	no	Array of String	List of supported standard models. Example: ["S1.SMALL1", "S2.MEDIUM2"]

InternetBandwidthConfig

It describes the related information of billing by bandwidth.

Referenced by the following interfaces: DescribeInstanceInternetBandwidthConfigs

name	required	NULL allowed	type	description
StartTime	no	no	Datetime_iso	Start Time. It is expressed according to the ISO8601 standard by using the UTC time. The format is YYYY-MM-DDThh:mm:ssZ . Example: 2014-08-03T12:00:00+08:00
EndTime	no	no	Datetime_iso	End time. It is expressed according to the ISO8601 standard by using the UTC time. The format is YYYY-MM-DDThh:mm:ssZ . Example: 2014-08-03T12:00:00+08:00
InternetAccessible	no	no	InternetAccessible	Instance bandwidth information. Example:View

ResourceForInstanceType

Resources of Instance Type

Referenced by the following interfaces: InquiryResourceResetInstancesType

name	required	NULL allowed	type	description
Memory	yes	no	Uint64	Memory size, in GB. Example: 2048
CPU	yes	no	Uint64	CPU cores Example: 2
InstanceType	yes	no	String	Instance model specification, such as S1.SMALL1 and S1.SMALL2. Example: S1.SMALL2
Status	yes	no	String	Instance Specification Status Example: SELL

InstanceTypeConfigStatusSet

List of Model Instances and Their Statuses Returned by Adjusting Configuration (Across Models)

Referenced by the following interfaces: DescribeInstancesModification

name	required	NULL allowed	type	description
Status	no	no	String	Status Example: SELL

name	required	NULL allowed	type	description
Message	no	yes	String	Description Example: success
InstanceTypeConfig	no	no	InstanceTypeConfig	List of Models Example:View

InstanceReturnable

Refundable information of an instance.

Referenced by the following interfaces: DescribeInstancesReturnable

name	required	NULL allowed	type	description
InstanceId	yes	no	String	Instance ID. Example: ins-61dyt49h
IsReturnable	yes	no	Bool	Whether the Instance is Refundable. Example: true
ReturnFailCode	yes	no	Int64	Error code of instance return failure. Example: 0
ReturnFailMessage	yes	no	String	Error information of instance return failure. Example: success

ChargePrepaid

It describes the prepaid mode, that is, the monthly subscription-related parameters, including purchase duration, auto-renewal logic, etc.

Referenced by the following interfaces: AllocateHosts, InquiryPriceAllocateHosts, RenewHosts, SwitchParameterAllocateHosts

name	required	NULL allowed	type	description
Period	yes	no	Uint64	Duration for purchasing an instance, unit: months. Value range: 1, 2, 3, 4, 5, 6, 7, 8, 9, 12, 24, and 36. Example: 1
RenewFlag	no	no	String	Auto-renewal flag. Value range: • NOTIFY_AND_AUTO_RENEW: Notifies of expiration and performs auto-renewal • NOTIFY_AND_MANUAL_RENEW: Notifies of expiration but does not perform auto-renewal • DISABLE_NOTIFY_AND_MANUAL_RENEW: Does not notify of expiration nor perform auto-renewal Default value: NOTIFY_AND_AUTO_RENEW. If this parameter is specified to NOTIFY_AND_AUTO_RENEW, the instance will be automatically renewed on a monthly basis after it expires if there is sufficient account balance. Example: NOTIFY_AND_MANUAL_RENEW

UnsupportedPreheatZones

AZs that do not support preheating and the reason codes.

Referenced by the following interfaces: DescribeInstancesCreateImageAttributes

name	required	NULL allowed	type	description
zone	no	no	String	AZ name Example: ap-city2-1

InstanceDisasterMap

Placement Group Pair Corresponding to Instance ID

Referenced by the following interfaces: RemoveInstancesDisasterRecoverGroup

name	required	NULL allowed	type	description
InstanceId	no	no	String	Instance ID Example: ins-61dyt49h
DisasterIds	no	no	Array of String	Placement Group ID Example: ["ps-l86okb2z"]

ImageLocation

Image location information.

Referenced by the following interfaces: DescribeImages

name	required	NULL allowed	type	description
Type	no	no	String	Position Example: cdz
Position	no	no	String	Location value. Example: ap-city1-cdz-haerbin-1

Placement

It describes the abstract location of the instance, including its availability zone, associated project, host, etc (available only for CDH products).

Referenced by the following interfaces: AllocateHosts, CloneInstance, CreateLaunchTemplate, DescribeHosts, DescribeInstances, DescribeLaunchTemplatesInfo, InquiryPriceAllocateHosts, InquiryPriceRunInstances, ModifyLaunchTemplate, RunInstances, SwitchParameterAllocateHosts, SwitchParameterRunInstances

name	required	NULL allowed	type	description
Zone	yes	no	String	Availability Zone ID to which the instance belongs. You can also obtain this parameter through the Zone field in the returned value by calling DescribeZones. Example: region1
ProjectId	no	no	Int64	Project ID to which the instance belongs. You can obtain this parameter through the projectId field in the returned value by calling Availability Zone. If it is not specified, the default project is used. Example: 0
HostId	no	yes	String	List of IDs of CDH instances where CVM instances reside. If you have purchased CDH instances and specified this parameter, CVM instances you purchase are deployed on these CDH instances randomly. This parameter is only used as an output parameter and is not supported currently. Example: host-o5l742go
HostIds	no	yes	Array of String	ID list of CDHs from which the instance can be created. If you have purchased CDHs and specify this parameter, the instances you purchase will be randomly deployed on the CDHs. Example: ["host-o5l742go"]
ProjectName	no	no	String	Project name of the instance. Example: default project

LoginSettings

It describes related configuration and information of instance login.

Referenced by the following interfaces: CloneInstance, CreateLaunchTemplate, DescribeInstances, DescribeLaunchTemplatesInfo, InquiryPriceResetInstance, InquiryPriceRunInstances, ModifyLaunchTemplate, ResetInstance, RunInstances, SwitchParameterRunInstances

name	required	NULL allowed	type	description
Password	no	yes	String	Instance login password. The password complexity requirements vary by different operating system types, as follows: • The password of a Linux instance should contain 10 to 30 characters, including at least three of [a-z], [A-Z], [0-9], and special symbols [()`~!@#$%^&*-+=_
KeyIds	no	yes	Array of String	List of key IDs. After associating a key, the instance can be accessed by using the corresponding private key. You can obtain the keyId through the API DescribeKeyPairs. Key and password should not be specified at the same time, and the Windows operating system does not support specifying a key. Currently, only one key can be specified at the time of purchase. Example: ["skey-3qlfot13"]
KeepImageLogin	no	yes	String	Retain the original settings of an image. This parameter should not be specified at the same time as Password or KeyIds.N. You can specify this parameter as TRUE only when using custom images, shared images, or externally imported images to create the instance. Value range: • TRUE: Indicates retaining the login settings of the image • FALSE: Indicates not retaining the login settings of the image Default value: FALSE. Example: TRUE

InstanceChargePrepaid

It describes the billing mode of an instance.

Referenced by the following interfaces: CloneInstance, CreateLaunchTemplate, InquiryPriceModifyInstancesChargeType, InquiryPriceRenewInstances, InquiryPriceRunInstances, ModifyInstancesChargeType, ModifyLaunchTemplate, RunInstances, SwitchParameterRunInstances

name	required	NULL allowed	type	description
Period	yes	no	Int64	Duration for purchasing an instance, unit: months. Value range: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 24, and 36. Example: 1
RenewFlag	no	no	String	Auto-renewal flag. Value range: • NOTIFY_AND_AUTO_RENEW: Notifies of expiration and performs auto-renewal • NOTIFY_AND_MANUAL_RENEW: Notifies of expiration but does not perform auto-renewal • DISABLE_NOTIFY_AND_MANUAL_RENEW: Does not notify of expiration nor perform auto-renewal Default value: NOTIFY_AND_AUTO_RENEW. If this parameter is specified to NOTIFY_AND_AUTO_RENEW, the instance will be automatically renewed on a monthly basis after it expires if there is sufficient account balance. Example: NOTIFY_AND_MANUAL_RENEW

OfflineMigrateUserTaskData

Offline migration task data types, including instance migration and data migration.

Referenced by the following interfaces: DescribeUserMigrateTasks

name	required	NULL allowed	type	description
JobId	yes	yes	String	Task ID Example: migrate-qwer1343
JobName	yes	yes	String	Task Name Example: onejob
AppId	yes	yes	Uint64	Cloud platform application ID, usually has a one-to-one correspondence with UIN. Example: 1255000041
Uin	yes	yes	String	User UIN Example: 32432442
Uuid	no	yes	String	Instance UUID Example: 5b33b986-084c-48e1-8cdb-d2e5ca5d045a
InstanceId	no	yes	String	Instance ID Example: ins-61dyt49h
ImageUrl	no	yes	String	System Disk Image COS URL Example: https://kaijian-gz-1251783334.cos.ap-region1.convergecloud.com/image_m-wz95mjeh07vy3d48fcj9_system.raw
DataSize	no	yes	Uint64	Auxiliary Data Disk Size Example: 50
Region	yes	yes	String	Region . Example: region1
Status	yes	yes	String	Task Status Example: SUCCESS
Progress	yes	yes	Uint64	Migration Task Progress Example: 2
CreateTime	yes	yes	String	Creation Time Example: 2019-12-04T16:44:55+08:00
EndTime	yes	yes	String	End time Example: 2019-12-04T16:44:55+08:00
SnapshotUrl	no	yes	String	Data Disk Image URL Example: https://kaijian-gz-1251783334.cos.ap-region1.convergecloud.com/image_m-wz95mjeh07vy3d48fcj9_system.raw

name	required	NULL allowed	type	description
DiskId	no	yes	String	Data Disk ID Example: disk-adggyzhh
DiskSize	no	yes	Uint64	Data Disk Size Example: 50
Action	no	yes	String	Migration action name. Example: ColdMigrateInstance

ItemPrice

It describes the price information of a single item.

Referenced by the following interfaces: DescribeZoneInstanceConfigInfos, InquiryPriceAllocateHosts, InquiryPriceModifyInstancesChargeType, InquiryPriceRenewInstances, InquiryPriceResetInstance, InquiryPriceResetInstancesInternetMaxBandwidth, InquiryPriceResetInstancesType, InquiryPriceResizeInstanceDisks, InquiryPriceRunInstances

name	required	NULL allowed	type	description
UnitPrice	no	yes	Float	Subsequent unit price, unit: USD. Example: 35.5
ChargeUnit	no	yes	String	Subsequent billing unit, possible value range: • HOUR: Indicates that the billing unit is calculated on a hourly basis. Current scenarios involving this billing unit include: instance pay-per-hour postpaid (POSTPAID_BY_HOUR), bandwidth pay-per-hour postpaid (BANDWIDTH_POSTPAID_BY_HOUR); • GB: Indicates that the billing unit is calculated per GB. Current scenarios involving this billing unit include: traffic pay-per-hour postpaid (TRAFFIC_POSTPAID_BY_HOUR). Example: 35.5
OriginalPrice	no	yes	Float	Original price of prepaid costs, unit: USD. Example: 35.5
DiscountPrice	no	yes	Float	Discount price of prepaid costs, unit: USD. Example: 35.5
Discount	no	yes	Float	Discount, for example, 20.0 represents 80% off. Example: 20.0
UnitPriceDiscount	no	yes	Float	Discount price of subsequent total costs, used for the postpaid billing mode, unit: USD. • If other time interval items such as UnitPriceDiscountSecondStep are returned, this item represents the time interval of (0, 96) hours; if no other time interval items are returned, this item represents the entire period, that is, (0, ∞) hours. Example: 35.5
UnitPriceSecondStep	no	yes	Float	Original price for subsequent total costs of usage time range between (96, 360) hours, used in the postpaid mode, unit: USD. Example: 35.5
UnitPriceDiscountSecondStep	no	yes	Float	Discount price for subsequent total costs of usage time range between (96, 360) hours, used in the postpaid mode, unit: USD. Example: 35.5
UnitPriceThirdStep	no	yes	Float	Original price for subsequent total costs of usage time range between (360, ∞) hours, used in the postpaid mode, unit: USD. Example: 35.5
UnitPriceDiscountThirdStep	no	yes	Float	Discount price for subsequent total costs of usage time range between (360, ∞) hours, used in the postpaid mode, unit: USD. Example: 35.5
DetailPrices	no	yes	DetailPrices	Detailed Price Example:View
DiscountThirdStep	no	yes	Float	Discount, for example, 20.0 represents 80% off. Example: 20.0
DiscountSecondStep	no	yes	Float	Discount, for example, 20.0 represents 80% off. Example: 20.0
DiskType	no	yes	String	Disk type Example: CLOUD_SSD

ActionTimers

Returned Value of ActionTimers

Referenced by the following interfaces: QueryInstancesActionTimer

name	required	NULL allowed	type	description
ActionTimerId	yes	no	String	ActionTimerId Example: 4904ffac-02e4-4161-9636-cca0a687e841
AppId	yes	no	Uint64	AppId Example: 125550001
InstanceId	yes	no	String	InstanceId Example: ins-61dyt49h
TimerAction	yes	no	String	TimerAction Example: TerminateInstances
ActionTime	yes	no	String	ActionTime Example: 2018-08-01 20:00:00
Status	yes	no	String	Status Example: SUCCESS
Externals	yes	no	Externals	Externals Example:View

KeyPairAttributeSet

Key pair

Referenced by the following interfaces: DescribeKeyPairsAttribute

name	required	NULL allowed	type	description
KeyId	yes	no	String	Key ID Example: skey-mv9yzyjj
InnerKeyId	yes	no	String	Internal Key ID Example: 83723

DataDisks

Description of the data disk image, including the image COS URL, data disk size, and data disk device name (DiskId);

Referenced by the following interfaces: ImportFullCvmImage

name	required	NULL allowed	type	description
ImageUrl	yes	no	String	Data Disk Image COS URL Example: http://kiki-1255000041.cos.region1.csp.yfm4.fsphere.cn/xxx
Size	yes	no	Uint64	Data Disk Size Example: 22
Device	yes	no	String	Device name corresponding to the data disk, currently is DiskId. Example: disk-61dyt49h

DiagnosticReportSet

DiagnosticReportSet

Referenced by the following interfaces: CreateDiagnosticReports

name	required	NULL allowed	type	description
InstanceId	no	no	String	Instance ID Example: ins-61dyt49h
DiagnosticReportId	no	no	String	Detection Report ID Example: dr-61dyt49h

InstanceTypeQuotaItemArchitecture

Model quota information of an instance with CPU architecture.

Referenced by the following interfaces: DescribeZoneInstanceConfigInfos

name	required	NULL allowed	type	description
Zone	yes	no	String	Availability zone. Example: ap-region1-2
InstanceType	yes	no	String	Instance model. Example: S1.SMALL2
InstanceChargeType	yes	no	String	Instance billing mode. Value range: • PREPAID: Indicates prepaid, that is, monthly subscription • POSTPAID_BY_HOUR: Indicates postpaid, that is, pay-as-you-go • CDHPAID: Indicates CDH payment, that is, billed only on the CDH but not on instances on the CDH. • SPOTPAID : Indicates spot instance payment. Example: PREPAID
NetworkCard	yes	no	Int64	Network interface card type, for example, 25 represents a 25 GB network interface card. Example: 0
Externals	yes	yes	Externals	Extended attributes. Example:View
Cpu	yes	no	Int64	Number of CPU cores of an instance, unit: cores. Example: 2
Memory	yes	no	Int64	Instance memory capacity, in GB. Example: 2048
InstanceFamily	yes	no	String	Instance model series. Example: S2
TypeName	yes	no	String	Model name. Example: Standard
LocalDiskTypeList	yes	no	Array of LocalDiskType	Local disk specification list. When this parameter returns a null value, it indicates that the local disk cannot be created under the current conditions. Example:View
Status	yes	no	String	Whether the instance is for sale. Value range: • SELL: Indicates that the instance is available for purchase. • SOLD_OUT: Indicates the instance has been sold out. Example: PENDING
Price	yes	no	ItemPrice	Instance selling price. Example:View
SoldOutReason	yes	yes	String	Reasons for sell out. Example: Insufficient resources in this AZ
InstanceBandwidth	yes	no	Float	Internal network bandwidth, in Gbps. Example: 10.0
InstancePps	yes	no	Int64	network packet send and receive processing capability, unit: ten thousand PPS. Example: 2
StorageBlockAmount	yes	no	Int64	Number of local storage blocks. Example: 3
CpuType	yes	no	String	Processor model. Example: AMD Ryzen 7 5600G
Gpu	yes	no	Int64	Number of GPUs on the Instance. Example: 1
Fpga	yes	no	Int64	Number of FPGAs on the Instance. Example: 0

name	required	NULL allowed	type	description
Remark	yes	no	String	Instance remark information. Example: alice use
Architecture	yes	yes	String	CPU architecture Example: x86_64
ConfigId	no	no	String	Configuration ID Example: qw4324352
DeviceClass	no	yes	String	Device Type Example: VSELF_2
Disable	no	yes	String	Disable Example: DISABLE
StorageBlock	no	yes	Int64	Local Storage Block Example: 0
Frequency	no	no	String	Frequency Example: 2.5 GHz
StatusCategory	no	no	String	Status category. Example: WithoutStock
GpuCount	no	no	Float	Number of GPUs. Calculation method: gpu x GpuAttrRatio. Example: 1
ExtraProperty	no	no	ExtraProperty	Additional attribute information. Example:View

UserMigrateTaskData

User Migration Task Details

Referenced by the following interfaces: DescribeUserMigrateTasks

name	required	NULL allowed	type	description
JobId	yes	yes	String	Task ID Example: migrate-qwer1353
JobName	yes	yes	String	Task Name Example: onejob
AppId	yes	yes	Uint64	Cloud platform application ID, usually has a one-to-one correspondence with UIN. Example: 125000111
Uin	yes	yes	String	User UIN Example: 32431223
Uuid	yes	yes	String	Instance UUID Example: 5b33b986-084c-48e1-8cdb-d2e5ca5d045a
InstanceId	yes	yes	String	Instance ID Example: ins-61dyt49h
ImageUrl	yes	yes	String	Data Disk Image COS URL Example: http://111-1251433127.cosd.convergecloud.com/Windows%20Server%202008%20R2%20x64a.vmdk.
DataSize	yes	yes	Uint64	Data Size Example: 500
Region	yes	yes	String	Region. Example: region1
Status	yes	yes	String	Task Status Example: RUNNING
Progress	yes	yes	Uint64	Migration Task Progress Example: 3
CreateTime	yes	yes	String	Creation Time Example: 2019-04-20 22:00:00
EndTime	yes	yes	String	End time Example: 2019-04-20 22:00:00

ResourceInfo

Detailed Information of User Instance Resource

Referenced by the following interfaces: SearchUserInstance

name	required	NULL allowed	type	description
ResourceId	yes	no	String	User resource instance ID. Example: ins-61dyt49h
SearchWord	yes	no	String	User resource keywords. Example: alice
RelationInstanceId	no	no	String	CVM instance ID associated with the user resource instance. Example: ins-61dyt49h
Region	no	no	String	Region. Example: region1
KeyType	no	no	String	Type used for this data search, values are instance ID (instance), instance name (alias), instance private IP (lan), and instance public IP (wan). Example: instance

TagSpecification

Explanation of Tag Pair to Be Bound when Creating CVM Instance

Referenced by the following interfaces: CloneInstance, CreateLaunchTemplate, DescribeLaunchTemplatesInfo, ModifyLaunchTemplate, RunInstances

name	required	NULL allowed	type	description
ResourceType	yes	no	String	Resource Type Associated with Tag Example: instance
Tags	yes	no	Array of Tag	List of Tag Pairs Example:View

DetailPrices

Detailed Price Information

Referenced by the following interfaces: DescribeZoneInstanceConfigInfos, InquiryPriceAllocateHosts, InquiryPriceModifyInstancesChargeType, InquiryPriceRenewInstances, InquiryPriceResetInstance, InquiryPriceResetInstancesInternetMaxBandwidth, InquiryPriceResetInstancesType, InquiryPriceResizeInstanceDisks, InquiryPriceRunInstances

name	required	NULL allowed	type	description
ImagePrice	no	yes	ItemPrice	Image Price Example:View
DataDisksPrice	no	yes	Array of ItemPrice	Data Disk Price Example:View
CpuMemPrice	no	yes	ItemPrice	CPU Memory Price Example:View
SystemDiskPrice	no	yes	ItemPrice	System Disk Price Example:View
SystemDiskBackupPrice	no	yes	ItemPrice	Details of system disk fees. Example:View
DataDisksBackupPrice	no	yes	Array of ItemPrice	Details of data disk fees. Example:View

LaunchTemplateVersionData

Version information of the instance launch template.
Referenced by the following API. DescribeLaunchTemplateVersions.

Referenced by the following interfaces: DescribeLaunchTemplatesInfo

name	required	NULL allowed	type	description
Placement	no	yes	Placement	Position of the instance. Note: This field may return null, indicating that no valid value was found. Example:View
InstanceType	no	yes	String	Instance model. Note: This field may return null, indicating that no valid value was found. Example: S1.SMALL2
InstanceName	no	yes	String	Instance name. Note: This field may return null, indicating that no valid values can be obtained. Example: MyInstance
InstanceChargeType	no	yes	String	Instance billing type. Value range: • PREPAID: Indicates prepaid, that is, monthly subscription • POSTPAID_BY_HOUR: Indicates postpaid, that is, pay-as-you-go • CDHPAID: CDH payment, that is, billed only on the CDH but not on instances on the CDH. • SPOTPAID: Indicates spot instance payment. Note: This field may return null, indicating that no valid values can be obtained. Example: PREPAID
SystemDisk	no	yes	SystemDisk	System disk information of an instance. Note: This field may return null, indicating that no valid values can be obtained. Example:View
DataDisks	no	yes	Array of DataDisk	Instance data disk information. Only includes data disks purchased with the instance. Note: This field may return null, indicating that no valid values can be obtained. Example:View
InternetAccessible	no	yes	InternetAccessible	Instance bandwidth information. Note: This field may return null, indicating that no valid values can be obtained. Example:View
VirtualPrivateCloud	no	yes	VirtualPrivateCloud	Information about virtual VPC to which the instance belongs. Note: This field may return null, indicating that no valid values can be obtained. Example:View
ImageId	no	yes	String	Image ID used by instance production. Note: This field may return null, indicating no valid value was found. Example: img-pl0aa46f
SecurityGroupIds	no	yes	Array of String	Security groups to which an instance belongs. You can obtain this parameter through the sgId field in the returned value by calling DescribeSecurityGroups. Note: This field may return null, indicating that no valid values can be obtained. Example: ["sg-rf6ogz49"]
LoginSettings	no	yes	LoginSettings	Instance login setttings. Currently, only the key associated with the instance is returned. Note: This field may return null, indicating that no valid value was found. Example:View
CamRoleName	no	yes	String	CAM role name. Note: This field may return null, indicating that no valid values can be obtained. Example: roleName001
HpcClusterId	no	yes	String	High-performance computing cluster ID. Note: This field may return null, indicating that no valid values can be obtained. Example: hpc-a5n666lo
InstanceCount	no	yes	Int64	Number of Instances to Purchase. Note: This field may return null, indicating that no valid value was found. Example: 1
EnhancedService	no	yes	EnhancedService	Enhanced service. Note: This field may return null, indicating no valid value was found. Example:View

name	required	NULL allowed	type	description
UserData	no	yes	String	User data provided for the instance, should be encoded in base64 format, supports a maximum data size of 16 KB. Note: This field may return null, indicating that no valid values can be obtained. Example: TXIVC2VyRGF0YQo=
DisasterRecoverGroupIds	no	yes	Array of String	Placement Group ID, only one can be specified. Note: This field may return null, indicating that no valid values can be obtained. Example: ['ps-3p88qhfx']
ActionTimer	no	yes	ActionTimer	Scheduled task. You can specify a scheduled task for the instance through this parameter. Currently, only scheduled termination is supported. Note: This field may return null, indicating that no valid values can be obtained. Example:View
HostName	no	yes	String	Hostname of the cloud server. Note: This field may return null, indicating no valid value was found. Example: MyHostName
ClientToken	no	yes	String	String used to ensure request idempotency. Note: This field may return null, indicating that no valid values can be obtained. Example: system-f3827db9-c58a-49cc-bf10-33fc1923a34a
TagSpecification	no	yes	Array of TagSpecification	Tag description list. By specifying this parameter, you can associate a tag with the corresponding cloud server and cloud disk instance at the same time. Note: This field may return null, indicating that no valid value was found. Example:View
CPU	no	no	Int64	CPU Example: 2
Memory	no	no	Int64	Memory. Example: 1024
OperatorUin	no	no	String	Operator UIN. Example: 110000004676
DisableApiTermination	no	no	Bool	Whether to allow instance deletion through the API. Example: false

InstanceFamilyConfig

Description of the model family configuration information of the instance.
Example: {'InstanceFamilyName': 'Standard Type S1', 'InstanceFamily': 'S1'}, {'InstanceFamilyName': 'Network Optimized N1', 'InstanceFamily': 'N1'}, {'InstanceFamilyName': 'High IO Type I1', 'InstanceFamily': 'I1'}, etc.

Referenced by the following interfaces: DescribeInstanceFamilyConfigs

name	required	NULL allowed	type	description
InstanceFamilyName	yes	no	String	Full name of model family. Example: Standard S1
InstanceFamily	yes	no	String	English abbreviation of the model family name. Example: S1

InternetAccessible

It describes the public network accessibility of the instance, and claims public network usage billing mode, maximum bandwidth, etc of the instance.

Referenced by the following interfaces: CloneInstance, CreateLaunchTemplate, DescribeInstanceInternetBandwidthConfigs, DescribeInstances, DescribeLaunchTemplatesInfo, InquiryPriceRenewInstances, InquiryPriceResetInstancesInternetMaxBandwidth, InquiryPriceRunInstances, ModifyLaunchTemplate, ResetInstancesInternetMaxBandwidth, RunInstances, SwitchParameterResetInstancesInternetMaxBandwidth, SwitchParameterRunInstances

name	required	NULL allowed	type	description
InternetChargeType	no	yes	String	Network billing type. Value range: • BANDWIDTH_PREPAID: Prepaid by bandwidth • TRAFFIC_POSTPAID_BY_HOUR: Traffic pay-per-hour postpaid • BANDWIDTH_POSTPAID_BY_HOUR: Bandwidth pay-per-hour postpaid • BANDWIDTH_PACKAGE: Bandwidth package users Default value: TRAFFIC_POSTPAID_BY_HOUR. Example: TRAFFIC_POSTPAID_BY_HOUR
InternetMaxBandwidthOut	no	no	Int64	Public network outbound bandwidth cap, in Mbps. Default value: 0 Mbps. Different models have different bandwidth cap ranges. Example: 20
PublicIpAssigned	no	no	Bool	Whether to allocate a public IP. Value range: • TRUE: Indicates assigning a public IP • FALSE: Indicates not assigning a public IP When the public network bandwidth is greater than 0, it should be set to True by default. When the public network bandwidth is 0, it is not allowed to assign a public IP. Example: false
InternetServiceProvider	no	yes	String	Network modes: Mobile: CMCC, Unicom: CTCC, Telecom: CUCC, Public network: CAP: BGP. Under the three network modes (Mobile, Unicom, Telecom), it should be bandwidth package billing mode. In other words, the parameter InternetChargeType must be provided and its value must be BANDWIDTH_PACKAGE. There are no such restrictions under the BGP mode. This API does not support multi-operator mode. In other words, the parameter InternetServiceProvider should not be Multi-operator. Example: CTCC

InstanceConnectivity

Instance port connectivity status, used to indicate the connectivity of the default remote login port and ICMP port of the instance.

Referenced by the following interfaces: CheckInstancesConnectivity

name	required	NULL allowed	type	description
InstanceId	yes	no	String	Instance ID Example: ins-61dyt49h
DefaultLoginPortConnectivity	yes	no	Bool	Default Remote Login Port Connectivity Status Example: true
ICMPConnectivity	yes	no	Bool	Whether the ping packet is reachable. Example: true

DeniedActions

List of Restricted Operations

Referenced by the following interfaces: DescribeInstancesDeniedActions

name	required	NULL allowed	type	description
Action	yes	no	String	Action Name Example: AllocateHosts
Code	yes	no	String	Returned values Example: AddressQuotaLimitExceeded_DailyAllocate
Message	yes	no	String	Returned Information Example: Insufficient purchase attempts. Each account in a region has a daily purchase attempt limit of quota * 2.

HostGoodsDetailItem

Detailed Information of CDH Shipment Instance

Referenced by the following interfaces: SwitchParameterAllocateHosts

name	required	NULL allowed	type	description
transactionId	no	no	String	Request Transaction ID Example: f5a23f7d-2262-4933-b544-b0fa1dccc2e4
action	no	no	String	Operation Name Example: ModifyInstanceInternetChargeType
autoRenewFlag	no	no	UInt64	Auto-Renewal Flag Example: 1
pid	no	no	UInt64	pid Example: 2
timeSpan	no	no	UInt64	Purchase or Renewal Duration Example: 60
timeUnit	no	no	String	Time unit Example: m
resourceId	no	no	String	Resource ID Example: ins-3botj2dn
curDeadline	no	no	Datetime	Current expiry time Example: 2018-04-27 14:35:57
signature	no	no	String	Digital signature Example: 13af5ff01c878914ec60fca51b097cbc
productInfo	no	no	Array of ProductInfoItem	Product Information Item List Example:View

HostForSellZoneStatus

CDH sales status in the availability zone.

Referenced by the following interfaces: DescribeZoneHostForSellStatus

name	required	NULL allowed	type	description
Zone	yes	no	String	Availability Zone Example: ap-region1-2
Status	yes	no	String	Sales status, (SELL: Normally in sale, SOLD_OUT: Sold out). Example: PENDING

SwapDisks

System disk information.

Referenced by the following interfaces: DescribeInstances

name	required	NULL allowed	type	description
DiskType	no	no	String	System Disk Type Example: CLOUD_SSD
DiskSize	no	no	UInt64	System Disk Size (GB) Example: 50
DiskId	no	yes	String	Unique identifier of the system disk. Example: disk-r92o1auc
Encrypt	no	yes	Bool	Encryption Example: true
KmsKeyId	no	yes	String	Encryption key ID. Example: kms-33456736
ThroughputPerformance	no	yes	UInt64	Throughput performance (MB/s). Example: 100
CdcId	no	yes	String	Dedicated Cluster ID Example: cluster-0dwcu6ns

GpuAttr

GPU Parameters

Referenced by the following interfaces: DescribeInstanceConfigInfos, DescribeInstancesActionTimer, DescribeLaunchTemplatesInfo, DescribeZoneInstanceConfigInfos, ImportInstancesActionTimer, ModifyInstancesActionTimer, QueryInstancesActionTimer, SwitchParameterRunInstances, UpdateInstancesActionTimer

name	required	NULL allowed	type	description
Type	no	yes	String	Type Note: This field may return null, indicating that no valid values can be obtained. Example: {"Type": "wx"}

InternetChargeTypeConfig

It describes the network billing.

Referenced by the following interfaces: DescribeInternetChargeTypeConfigs

name	required	NULL allowed	type	description
InternetChargeType	no	no	String	Network billing mode. Example: TRAFFIC_POSTPAID_BY_HOUR
Description	no	no	String	Description information of network billing mode. Example: alice use

InstanceFamilyItemArchitecture

Instance family information with CPU architecture.

Referenced by the following interfaces: DescribeInstanceConfigInfos

name	required	NULL allowed	type	description
instanceFamily	yes	no	String	Instance family. Example: S2
order	yes	no	Int64	Priority. Example: 1
instanceTypes	yes	no	Array of InstanceTypeItem	List of instance type information. Example:View
TypeName	yes	no	String	Instance Type Name Example: Standard S2
Architecture	yes	no	String	CPU Architecture Information Example: x86_64

HibernationOptions

Instance hibernation option configurations.

Referenced by the following interfaces: DescribeInstances

name	required	NULL allowed	type	description
Configured	no	yes	Bool	Whether hibernation options are configured. Example: true

DisasterRecoverGroup

Disaster Recovery Group Information

Referenced by the following interfaces: DescribeDisasterRecoverGroups

name	required	NULL allowed	type	description
DisasterRecoverGroupId	yes	no	String	Placement Group ID. Example: ps-n4becvb9
Name	yes	no	String	Placement group name, with a length of 1-60 characters. Example: myGroup
Type	yes	no	String	Placement group type. Valid values: • HOST: Physical machine • SW: Switch • RACK: Rack Example: "HOST"
CvmQuotaTotal	yes	no	Int64	Maximum number of cloud servers accommodated in the placement group. Example: 50
CurrentNum	yes	no	Int64	Current quantity of CVMs in the placement group. Example: 2
InstanceIds	yes	yes	Array of String	ID list of CVMs in the placement group. Example: ["ins-19029pru"]
CreateTime	yes	yes	Datetime_iso	Placement group creation time. Example: "2021-04-27T08:49:34Z"
Affinity	no	yes	Int64	Placement group affinity Example: 1
Strategy	yes	no	String	Placement group policies Example: PARTITION
Tags	no	yes	Array of Tag	Placement group tag. Example:View

ProjectSpecification

Platform Project ID

Referenced by the following interfaces: CloneInstance, CreateLaunchTemplate, RunInstances

name	required	NULL allowed	type	description
ResourceType	yes	no	String	Resource type, instance by default. Example: instance
PlatformProjectId	yes	no	String	Project ID Example: pr-46fbb87b

HostPrice

CDH-Related Price Information

Referenced by the following interfaces: InquiryPriceAllocateHosts

name	required	NULL allowed	type	description
HostPrice	no	no	ItemPrice	It describes CDH instance-related price information. Example:View

SystemDisk

It describes the information about the block device, namely, the system disk, where the operating system is located.

Referenced by the following interfaces: CloneInstance, CreateLaunchTemplate, DescribeInstances, DescribeLaunchTemplatesInfo, InquiryPriceResetInstance, InquiryPriceResizeInstanceDisks, InquiryPriceRunInstances, ModifyLaunchTemplate, ResetInstance, ResizeInstanceDisks, RunInstances, SwitchParameterRunInstances

name	required	NULL allowed	type	description
DiskType	no	no	String	System disk type. Value range: • LOCAL_BASIC: Local HDD • LOCAL_SSD: Local SSD • CLOUD_BASIC: Standard CBS • CLOUD_SSD: SSD CBS • CLOUD_PREMIUM: High-Performance CBS Default value: LOCAL_BASIC. Example: Local Hard Disk
DiskId	no	yes	String	System disk ID. The LOCAL_BASIC and LOCAL_SSD types do not have an ID. Currently, this parameter is not supported. Example: disk-61dy449h
DiskSize	no	no	Int64	System disk size, in GB. The default value is 50. Example: 500
DiskStoragePoolGroup	no	yes	String	Storage pool specified by the system disk. Example: alice-1255000080
AutoSnapshotPolicyId	no	yes	String	Auto Backup Policy ID of CBS Example: asp-c0jt9yym
Encrypt	no	no	Bool	Encryption Example: true
KmsKeyId	no	yes	String	Encryption key ID. Example: kms-33453241
ThroughputPerformance	no	no	Uint64	Throughput performance (MB/s). Example: 100
CdcId	no	yes	String	Dedicated Cluster ID Example: cluster-0dwcu6ns

AutomationServiceEnabled

It describes information related to tat-agent.

Referenced by the following interfaces: CloneInstance, CreateLaunchTemplate, DescribeLaunchTemplatesInfo, InquiryPriceResetInstance, InquiryPriceRunInstances, ModifyLaunchTemplate, ResetInstance, RunInstances, SwitchParameterRunInstances

name	required	NULL allowed	type	description
Enabled	no	no	Bool	Whether to install [tat-agent]. Value range: • TRUE: Indicates installation • FALSE: Indicates no installation Default value: TRUE. Example: true

InstanceConfigInfoItemArchitecture

Static configuration information of an instance with CPU architecture.

Referenced by the following interfaces: DescribeInstanceConfigInfos

name	required	NULL allowed	type	description
type	yes	no	String	Instance specifications. Example: S2.SMALL1
typeName	yes	no	String	Instance specification name. Example: Standard S2
order	yes	no	Int64	Priority. Example: 1
instanceFamilies	yes	no	Array of InstanceFamilyItemArchitecture	List of instance family information. Example:View

KeyPair

It describes the key pair information.

Referenced by the following interfaces: DescribeKeyPairs

name	required	NULL allowed	type	description
KeyId	no	no	String	ID of a key pair, is the unique flag of the key pair. Example: skey-q29u65hu
KeyName	no	no	String	Key pair name. Example: alice-key
Description	no	no	String	Key Pair Description Example: alice use
PublicKey	no	no	String	Plaintext public key of the key pair. Example: ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC0ran+u+y09bSSoAbHBhJm2ivcI0uwTiF+/MqoGj5odBuGcDHGIBE7Th74ETXtbuqEXxdOSRO/7DOVaTZa1MYe6qKGPAi5/8jlV8c9CKCezXr99A2Dps/eVPVn4yO2NhSXbr0U/voRxTqNpr90YLo25y1VnN0vg0CfWL8DDYh6DkMMVuflGlkA7WVPdsHomTLISRdSLvCRZPHC7e8hkrznO0mfM+c/JY9qqSrd1lkqtDRJNpNvPLaRnJsc3uoot2nGqrGD6yiwx2tvdLAggQT5tAS5vt1c3CTMMJRGlqm+CdG2S1y0VIMDmm9XHeVBmZuX5YDJPNGlOcBI2Cgrj5 skey-mk5eqeu6
AssociatedImageCount	no	no	Int64	Number of images associated with the key. Example: 0
AssociatedInstanceCount	no	no	Int64	Number of instances associated with the key. Example: 0
AssociatedInstanceIds	no	no	Array of String	List of instance IDs associated with the key. Example: ["ins-syht65r4"]
ProjectId	no	no	Int64	Project ID to which the key pair belongs. When the value of ProjectId is 0, it indicates the default project. Example: 0
Tags	no	yes	Array of Tag	List of tags associated with keys. Example:View
CreatedTime	yes	no	Datetime_iso	Key Pair Creation Date Example: 2022-03-21T08:41:45Z

UsbInfo

USB information.

Referenced by the following interfaces: DescribeInstanceUsbInfo

name	required	NULL allowed	type	description
BusNumber	no	no	String	Bus number. Example: 001
DeviceNumber	no	no	String	Device number. Example: 004
VendorId	no	no	String	Vendor number. Example: 0x17ef
ProductId	no	no	String	Product number. Example: 0x38ac
Name	no	no	String	Name Example: Lenovo
Version	no	no	String	Version Example: 2.00
DevType	no	no	String	Dev type. Example: Mass Storage
CreateTime	no	no	String	Creation Time Example: 2023-03-09 11:17:08
UpdateTime	no	no	String	Update time Example: 2023-03-14 16:09:20

ImageAttributeSet

Array of Mappings from unImgId to deviceImageId

Referenced by the following interfaces: DescribeImagesAttribute

name	required	NULL allowed	type	description
ImageId	yes	no	String	Image ID Example: img-c1otssej
InnerImageId	yes	no	Uint64	Internal Image ID Example: 53242

ActionTimer

Schedule task

Referenced by the following interfaces: DescribeInstancesActionTimer, DescribeLaunchTemplateInfo, ImportInstancesActionTimer, ModifyInstancesActionTimer, SwitchParameterRunInstances, UpdateInstancesActionTimer

name	required	NULL allowed	type	description
TimerAction	no	no	String	Timer Example: TerminateInstances
ActionTime	no	no	String	Execution time Example: 2024-05-29T11:26:40Z
Externals	yes	no	Externals	Extended data. This parameter is only used as an output parameter. Example:View

DataDisk

It describes the information about the data disk.

Referenced by the following interfaces: CloneInstance, CreateLaunchTemplate, DescribeInstances, DescribeLaunchTemplatesInfo, InquiryPriceRunInstances, ModifyLaunchTemplate, ResizeInstanceDisks, RunInstances, SwitchParameterResizeInstanceDisks, SwitchParameterRunInstances

name	required	NULL allowed	type	description
DiskType	no	no	String	Data disk type. Value range: • LOCAL_BASIC: Local HDD • LOCAL_SSD: Local SSD • CLOUD_BASIC: Basic Cloud Disk • CLOUD_PREMIUM: Premium Cloud Disk • CLOUD_SSD: SSD Cloud Disk Default value: LOCAL_BASIC. This parameter is invalid for the API ResizeInstanceDisk . Example: CLOUD_BASIC
DiskId	no	no	String	System disk ID. The LOCAL_BASIC and LOCAL_SSD types do not have an ID. Currently, this parameter is not supported. Example: disk-61dyt49h
DiskSize	yes	no	Int64	Data disk size, in GB. The minimum adjustment step size is 10 GB. The value range varies with different data disk types. The default value is 0, indicating that no data disk is purchased. For more restrictions, see Product Documentation. Example: 324
DeleteWithInstance	no	yes	Bool	Whether the data disk is terminated with the instance. Value range: • TRUE: When the instance is terminated, the data disk is also terminated. Only pay-per-hour postpaid cloud disks are supported. • FALSE: When the instance is terminated, the data disk is retained. Default value: TRUE Currently, this parameter is only used for the API RunInstances . Example: false
DiskStoragePoolGroup	no	yes	String	Storage pool specified by the data disk. Example: alica-1255000080
AutoSnapshotPolicyId	no	yes	String	Automatic Backup Policy of CBS Example: asp-mrsrn243
SnapshotId	no	yes	String	Snapshot ID of CBS Example: snap-7et7t234

Instance

Description of Instance Information

Referenced by the following interfaces: DescribeInstances

name	required	NULL allowed	type	description
Placement	no	no	Placement	Instance Location. Example:View
InstanceId	no	no	String	Instance ID. Example: ins-9bxeibeo
InstanceType	no	no	String	Instance model. Example: S1.SMALL1
CPU	no	no	Int64	Number of CPU cores of an instance, unit: cores. Example: 1
Memory	no	no	Int64	Instance memory capacity, in GB. Example: 1
RestrictState	no	yes	String	Instance service status. Value range: • NORMAL: Indicates an instance in the normal state • EXPIRED: Indicates an expired instance • PROTECTIVELY_ISOLATED: Indicates an instance that is protectively isolated. Example: NORMAL
InstanceName	no	no	String	Instance name. Example: Test instance
InstanceChargeType	no	no	String	Instance billing mode. Value range: • PREPAID : Indicates prepaid, that is, monthly subscription • POSTPAID_BY_HOUR : Indicates postpaid, that is, pay-as-you-go • CDHPAID : Indicates CDH payment, that is, billed only on the CDH but not on instances on the CDH . Example: PREPAID
SystemDisk	no	no	SystemDisk	System disk information of an instance. Example:View
DataDisks	no	yes	Array of DataDisk	Instance data disk information. Only includes data disks purchased with the instance. Example:View
PrivateIpAddresses	no	yes	Array of String	List of private IP s of primary network interface card of instance. Example: ["172.16.32.78"]
PublicIpAddresses	no	yes	Array of String	List of public IP s of primary network interface card of instance. Example: ["122.207.11.190"]
InternetAccessible	no	no	InternetAccessible	Instance bandwidth information. Example:View
VirtualPrivateCloud	no	no	VirtualPrivateCloud	Information about virtual VPC to which the instance belongs. Example:View
ImageId	no	yes	String	Image ID used for instance production. Example: img-9qabwvbn

name	required	NULL allowed	type	description
RenewFlag	no	yes	String	Auto-renewal flag. Value range: • NOTIFY_AND_MANUAL_RENEW : Indicates that notification that it is about to expire is made, but auto-renewal is not performed • NOTIFY_AND_AUTO_RENEW : Indicates that notification that it is about to expire is made, and auto-renewal is performed • DISABLE_NOTIFY_AND_MANUAL_RENEW : Indicates that notification that it is about to expire is not made, and auto-renewal is neither performed. Example: NOTIFY_AND_MANUAL_RENEW
CreatedTime	no	no	Datetime_iso	Creation time. It is expressed according to the ISO8601 standard by using the UTC time. The format is YYYY-MM-DDThh:mm:ssZ . Example: 2020-03-10T02:43:51Z
ExpiredTime	no	yes	Datetime_iso	Expiration time. It is expressed according to the ISO8601 standard by using the UTC time. The format is YYYY-MM-DDThh:mm:ssZ . Example: 2020-04-10T02:47:36Z
InstanceState	yes	yes	String	Instance status. Value range: • PENDING: Indicates creating in progress • LAUNCH_FAILED: Indicates creation failed • RUNNING: Indicates running • STOPPED: Indicates shutdown • STARTING: Indicates starting • STOPPING: Indicates shutdown in progress • REBOOTING: Indicates rebooting • SHUTDOWN: Indicates shutdown and pending termination • TERMINATING: Indicates terminating in progress. Example: RUNNING
LatestOperation	yes	yes	String	Latest operation on the instance, such as StopInstances, ResetInstance. Example: RenewInstances
LatestOperationState	yes	yes	String	Latest operation status of the instance. Value range: • SUCCESS: Indicates that the operation succeeded • OPERATING: Indicates that the operation is in progress • FAILED: Indicates that the operation failed. Example: SUCCESS
LatestOperationRequestId	yes	yes	String	Unique request ID for the latest operation on an instance. Example: 3554eb5b-1cfa-471a-aa76-dc436c9d43e8
SecurityGroupIds	yes	yes	Array of String	Security Group of the Instance. You can obtain this parameter by calling the sgId field in the returned value from DescribeSecurityGroups. Example: ["sg-p1ezv4wz"]
LoginSettings	yes	yes	LoginSettings	Instance login settings. Currently, only keys associated with the instance are returned. Example:View
DisasterRecoverGroupId	yes	yes	String	Spread placement group ID. Example: null
Tags	yes	yes	Array of Tag	List of tags associated with the instance. Example:View
Uuid	yes	no	String	Instance UUID Example: 68b510db-b4c1-4630-a62b-73d0c7c970f9
OsName	yes	yes	String	Instance OS Name Example: CentOS 7.6 64bit
IPv6Addresses	yes	yes	Array of String	IPv6 Address of Instance Example: null
StopChargingMode	yes	yes	String	Shutdown Billing Mode of Instance Value range: • KEEP_CHARGING: Continue charging after shutdown • STOP_CHARGING: Stop charging after shutdown • NOT_APPLICABLE: the instance is in a non-shutdown state or conditions not applicable for stopping charges upon shutdown . Example: NOT_APPLICABLE
CamRoleName	yes	yes	String	CAM role name. Example: null
IsolatedSource	yes	yes	String	IsolatedSource Example: NOTISOLATED
PlatformProjectId	yes	yes	String	Project ID to which Resource Belongs Example: 0
RemainTime	yes	yes	String	Duration Example: 10
HpcClusterId	no	yes	String	High-performance computing cluster ID. Example: null
DefaultLoginUser	no	yes	String	Default Login User Example: root
DefaultLoginPort	no	yes	Uint64	Default Login Port Example: 22
DedicatedClusterId	no	yes	String	Dedicated cluster ID where the instance is located. Example: cluster-du3jkxn
OperatorUin	yes	yes	String	Operator UIN Example: 34232423
RdmaIpAddresses	no	yes	Array of String	List of High-Performance Computing Cluster IP s Example: 10.34.23.4
DeviceId	no	yes	Uint64	Instance ID Example: 12
InstanceClass	no	yes	String	Instance Type Example: S
IsolatedTime	no	yes	Datetime_iso	Isolated at Example: 2014-08-03T12:00:00+08:00
ErrorKey	no	yes	String	Incorrect Key Example: 12
GPU	no	yes	Int64	GPU Example: 2
NewCreationIdentify	no	yes	Bool	Newly Created Identification Example: false
OperationMask	no	yes	Uint64	Operation Mask Example: 64
ImageType	no	yes	String	Image type Example: PUBLIC_IMAGE
KeyPairIds	no	yes	Array of String	Secret key ID, data source is MC, BATCH, AS, tke, VPC_CGW, or when there is neither Token nor CamContext in the request, the keypairids field will be returned. Other data sources will not return the keypairids field. Example: ["skey-a7qf43n"]
RunFlag	no	no	Int64	Runtime Flag Example: 1
InnerVpcId	no	yes	Uint64	Internal VPC ID Example: 2
InstanceFamily	no	yes	String	Family of Instance Example: S1
Architecture	no	yes	String	Architecture Example: x86_64
ErrorCode	no	yes	Int64	Error code Example: SUCCESS
SafeIsolatedInfo	no	yes	String	Security Isolation Information Example: null
IsSafeIsolated	no	yes	Bool	Whether it is protectively isolated. Example: true
Hypervisor	no	yes	Int64	Virtualization Example: 1
LatestOperationErrorMsg	no	yes	String	Error message of the latest operation on the instance. Example: None
UnderwriteExpiredTime	no	yes	Datetime_iso	Instance expiration time in committed use mode. It should be a UTC time in the format defined in the ISO 8601 standard. Format: YYYY-MM-DDThh:mm:ssZ. Note: This field is null for the postpaid mode. Example: 2020-04-10T02:47:36Z
DisableApiTermination	no	no	Bool	Instance termination protection flag. It indicates whether instance deletion through an API is allowed. true: instance protection enabled (deletion through an API not allowed); false: instance protection disabled (deletion through an API allowed). Default value: false. Example: false
HibernationOptions	no	yes	HibernationOptions	Whether hibernation is configured for the instance. Example:View
VmEniTrunking	no	yes	String	ENI trunking status. Example: on
BootMode	no	yes	String	Boot mode of the instance. Example: UEFI
ChcInstanceType	no	yes	String	CHC instance type. Example: CHC.S3
SwapDisks	no	yes	SwapDisks	List of swap disk information on the instance. Example:View
LatestOperationCode	no	yes	String	Error code of the latest operation. It indicates the operation failure cause. Example: InternalError
DisasterRecoverGroupIds	no	no	Array of String	Placement Group List Example: ["ps-g0qd8r"]
LicenseType	no	no	String	Operating system license type of the instance. Example: Cloud
EnableGridLicence	no	yes	String	Whether to enable the GRID license. Example: ENABLED

InstanceTypeQuota

Description of Instance Model Quota Information

Referenced by the following interfaces: DescribeInstanceTypeQuota

name	required	NULL allowed	type	description
Zone	yes	no	String	Availability zone. Example: ap-region1-1
InstanceType	yes	no	String	Instance model. Example: I1.MEDIUM4
InstanceQuota	yes	no	Int64	Instance model quota. Example: 20
InstanceChargeType	yes	no	String	Instance billing mode. Value range: *PREPAID : Indicates prepaid, that is, monthly subscription* POSTPAID_BY_HOUR : Indicates postpaid, that is, pay-as-you-go * CDHPAID : CDH payment, that is, billed only on the CDH but not on instances on the CDH. Example: PREPAID
DeviceClass	no	no	String	Instance type. Example: S
CPU	no	no	Int64	Number of CPU cores of an instance, unit: cores. Example: 2
Memory	no	no	Int64	Instance memory capacity, in GB. Example: 1024
GPU	no	no	Int64	Number of GPU cores of the instance, unit: cores. Example: 3

AccountAttribute

Account Attribute Object

Referenced by the following interfaces: DescribeAccountAttributes

name	required	NULL allowed	type	description
AttributeName	yes	no	String	Payment type: Postpaid (PostPaidInstanceCountLimit), prepaid (PrePaidInstanceCountLimit). Example: jack
AttributeValue	yes	no	String	Maximum Purchase Quantity at a Time Example: 20
AttributeValues	no	no	String	Maximum Purchase Quantity at a Time Example: 20

DisasterRecoverGroups

Placement Group Information

Referenced by the following interfaces: QueryDisasterRecoverGroup

name	required	NULL allowed	type	description
currentNum	yes	yes	Uint64	Number of placement groups the current user has created. Example: 12
uDisasterRecoverGroupId	yes	yes	String	Placement Group ID. Example: ps-l86ok62z
cvmQuotaTotal	yes	yes	Uint64	Maximum number of cloud servers accommodated in the placement group. Example: 100
uuids	yes	yes	Array of String	uuid Example: ["5b33b986-084c-48e1-8cdb-d2e5ca5d045a"]
owner	yes	yes	String	Owner UIN of Account Example: 125550001
disasterRecoverTag	yes	yes	String	Tag Example: TAG_HARD_SW_ps-bpsqiuy1
type	yes	yes	String	Type Example: HOST
createTime	yes	yes	String	Creation Time Example: 2018-05-16 10:40:58
name	yes	yes	String	Placement Group Name Example: alice-1
partitionCount	yes	yes	Uint64	Partition quantity Example: 4
strategy	yes	yes	String	Policies Example: SPREAD
affinity	yes	yes	Int64	Affinity, Matching Degree Example: 1

RunSecurityServiceEnabled

It describes the information related to the Cloud Security service.

Referenced by the following interfaces: CloneInstance, CreateLaunchTemplate, DescribeLaunchTemplatesInfo, InquiryPriceResetInstance, InquiryPriceRunInstances, ModifyLaunchTemplate, ResetInstance, RunInstances, SwitchParameterRunInstances

name	required	NULL allowed	type	description
Enabled	no	no	Bool	Whether to enable Cloud Security service. Value Range: • TRUE: Indicates that the Cloud Security service is enabled • FALSE: Indicates that the Cloud Security service is not enabled Default Value: TRUE Example: false

CbsMigrateTask

Offline Data Migration Task Details

Referenced by the following interfaces: DescribeUserMigrateTasks

name	required	NULL allowed	type	description
JobId	yes	no	String	Task ID Example: migrate-2d43254d
JobName	yes	no	String	Task Name Example: onejob
AppId	yes	no	Uint64	Cloud platform application ID, usually has a one-to-one correspondence with UIN. Example: 125550001
Uin	yes	no	String	User UIN Example: 1243244232
SnapshotUrl	yes	no	String	Snapshot URL Example: http://kiki-1255000041.cos.region1.csp.yfm4.fsphere.cn/Windows%20Server%202008%20R2%20x64a.vmdk
DiskId	yes	no	Uint64	Disk ID Example: 2
Region	yes	no	String	Region Example: region1
DiskSize	yes	no	Uint64	Data Size Example: 512
Status	yes	no	String	Task Status Example: SUCCESS
Progress	yes	no	Uint64	Migration Task Progress Example: 5
CreateTime	yes	no	String	Creation Time Example: 2019-12-04T16:44:55+08:00
EndTime	yes	no	String	End time Example: 2019-12-04T16:44:55+08:00

InstanceChargeTypeConfig

Billing Type Configuration Information

Referenced by the following interfaces: DescribeInstanceChargeTypeConfigs

name	required	NULL allowed	type	description
InstanceChargeType	yes	no	String	Instance Billing Type Example: PREPAID
Description	yes	no	String	Instance Billing Type Description Example: jack use

DiagnosticReportDataSet

DiagnosticReportDataSet

Referenced by the following interfaces: DescribeDiagnosticReports

name	required	NULL allowed	type	description
CreateTime	no	no	Datetime	Start Time Example: 2014-08-03 12:00:00
DiagnosticReportId	no	no	String	Report ID Example: dr-61dyt49h
FinishTime	no	no	Datetime	End time Example: 2014-08-03 12:00:00
InstanceId	no	no	String	Instance ID Example: ins-61dyt49h
InstanceName	no	no	String	Instance name Example: jack-use
ReportDetailSet	no	no	Array of ReportDetailSet	ReportDetailSet Example:View
Severity	no	yes	String	Detection status Example: Normal
Status	no	no	String	Status Example: Finished
Uuid	no	no	String	uuid Example: 4904ffac-02e4-4161-9636-cca0a687e841

Externals

Extended Data

Referenced by the following interfaces: DescribeInstanceConfigInfos, DescribeInstancesActionTimer, DescribeLaunchTemplatesInfo, DescribeZoneInstanceConfigInfos, ImportInstancesActionTimer, ModifyInstancesActionTimer, QueryInstancesActionTimer, SwitchParameterRunInstances, UpdateInstancesActionTimer

name	required	NULL allowed	type	description
ReleaseAddress	no	yes	Bool	Release Address Note: This field may return null, indicating that no valid value was found. Example: true
UnsupportNetworks	no	yes	Array of String	Unsupported network types, possible value range: • BASIC: Basic network • VPC1.0: VPC VPC1.0 Note: This field may return null, indicating that no valid value was found. Example: ["BASIC"]
StorageBlockAttr	no	yes	StorageBlock	HDD Local Storage Attributes Note: This field may return null, indicating that no valid values can be obtained. Example:View
InquiryWithEntireServer	no	yes	String	Query Entire Server Example: true
RequireNetworkFeatures	no	yes	Array of String	Required Network Feature Note: This field may return null, indicating that no valid values can be obtained. Example: null
RequiredEnhancedService	no	yes	RequiredEnhancedService	Service required to be enhanced. Note: This field may return null, indicating no valid value was found. Example:View
GpuAttr	no	yes	GpuAttr	GPU Parameters Note: This field may return null, indicating that no valid values can be obtained. Example:View

name	required	NULL allowed	type	description
UnsupportNetworkFeature	no	no	Array of String	Not support the network feature. Example: VPC_GATEWAY
CoresOfOneThreadPerCore	no	no	Array of Int64	Specifies the number of cores (for example, '1'), with each core bound to a single thread. Example: 1
CoresOfTwoThreadPerCore	no	no	Array of Int64	Specifies the number of cores (for example, '2'), with each core bound to two threads. Example: 2
Hypervisor	no	yes	String	Instance category. Example: kvm
HypervisorSpec	no	yes	Array of String	Instance property Example: ["rdma"]

BasicService

Describes the relevant information about the basic service.

Referenced by the following interfaces: CloneInstance, CreateLaunchTemplate, DescribeLaunchTemplatesInfo, InquiryPriceResetInstance, InquiryPriceRunInstances, ModifyLaunchTemplate, ResetInstance, RunInstances, SwitchParameterRunInstances

name	required	NULL allowed	type	description
Enabled	no	no	Bool	Whether the basic service is enabled. Valid values: • TRUE: enabled; • FALSE: not enabled. Default value: TRUE. Example: false

SharePermission

Image Sharing Information Structure

Referenced by the following interfaces: DescribeImageSharePermission

name	required	NULL allowed	type	description
CreatedTime	yes	no	Datetime_iso	Image Sharing Duration Example: 2014-08-03T12:00:00+08:00
AccountId	yes	no	String	Account ID for Image Sharing Example: 32344323

EnhancedService

It describes the enhanced services enabling situation and settings of the instance, such as Cloud Security, Cloud Monitor, and other instance agents.

Referenced by the following interfaces: CloneInstance, CreateLaunchTemplate, DescribeLaunchTemplatesInfo, InquiryPriceResetInstance, InquiryPriceRunInstances, ModifyLaunchTemplate, ResetInstance, RunInstances, SwitchParameterRunInstances

name	required	NULL allowed	type	description
SecurityService	no	no	RunSecurityServiceEnabled	Enable the Cloud Security service. If this parameter is not specified, the Cloud Security service is enabled by default. Example:View
MonitorService	no	no	RunMonitorServiceEnabled	Enable the Cloud Security service. If this parameter is not specified, the Cloud Monitor service is enabled by default. Example:View
AutomationService	no	no	AutomationServiceEnabled	Install tat-agent. If this parameter is not specified, it will be installed by default. Example:View
BasicService	no	no	BasicService	Enables basic service. Example:View

InstanceTypeNameConfig

Instance Type Name Configuration

Referenced by the following interfaces: DescribeInstanceTypeNameConfigs

name	required	NULL allowed	type	description
ShowInMenu	yes	no	Bool	Whether to display it in the list of instance types. Example: false
InstanceFamilyName	yes	no	String	Name of Instance Type Example: Standard S1
InstanceFamily	yes	no	String	Instance Type Example: S1

Price

Price

Referenced by the following interfaces: InquiryPriceModifyInstancesChargeType, InquiryPriceRenewInstances, InquiryPriceResetInstance, InquiryPriceResetInstancesInternetMaxBandwidth, InquiryPriceResetInstancesType, InquiryPriceResizeInstanceDisks, InquiryPriceRunInstances

name	required	NULL allowed	type	description
InstancePrice	no	no	ItemPrice	It describes the instance price. Example:View
BandwidthPrice	no	yes	ItemPrice	It describes the network price. Example:View

HpcClusterInfo

HPC cluster

Referenced by the following interfaces: CreateHpcCluster, DescribeHpcClusters

name	required	NULL allowed	type	description
HpcClusterId	yes	no	String	HPC cluster ID Example: hpc-g9zbwc5o
Name	yes	yes	String	Hyper computing cluster name. Example: jack
Remark	yes	yes	String	Hyper Computing Cluster remarks. Example: H20
CvmQuotaTotal	yes	no	Uint64	Device capacity under the cluster. Example: 20
Zone	yes	no	String	Cluster AZ Example: region1
CurrentNum	yes	no	Uint64	Current number of devices in the cluster. Example: 2
CreateTime	yes	yes	Datetime_iso	Cluster Creation Time Example: 2014-08-03T12:00:00+08:00
InstanceIds	yes	yes	Array of String	List of instance IDs in the cluster. Example: ["ins-61dyt49h"]
HpcClusterType	no	yes	String	HPC cluster type. Example: CDC
HpcClusterBusinessId	no	yes	String	Workload ID of the HPC cluster. Example: cluster-1f6v312
HpcInstanceFamily	no	yes	String	HPC instance family type. Example: H1

ClientSysInfo

Used to pass client system information during live migration.

Referenced by the following interfaces: LiveMigrateInstance

name	required	NULL allowed	type	description
OsType	yes	no	String	Operating System Example: CentOS
OsVersion	yes	no	String	Operating system version Example: 6
DiskSize	yes	no	Array of Uint64	Data Disk Information of to-be-Imported System Disk Example: 100
ExtraInfo	no	no	String	Additional Information Example: extral

InstanceStatus

Description of the instance status. For details on status types, see Instance Status Table.

Referenced by the following interfaces: DescribeInstancesStatus

name	required	NULL allowed	type	description
InstanceId	no	no	String	Instance ID. Example: ins-61dyt49h
InstanceState	no	no	String	Instance Status. Example: RUNNING
OperationMask	no	no	Int64	Operation Mask Example: 14088
RunFlag	no	no	Int64	Instance Status Example: 0
Hypervisor	no	no	Int64	Virtualization Type Example: 0
IsReturnable	no	no	Bool	Whether the instance can be proactively returned. Example: true
ReturnFailCode	no	no	Int64	Reason why proactive return is not supported. Example: 0
ReturnFailMessage	no	no	String	Error message when proactive return is not supported. Example: Refundable
TotalDuration	no	no	Int64	TotalDuration Example: 0
UsedDuration	no	no	Int64	UsedDuration Example: 0
InnerVpcId	no	no	Int64	VPC ID Example: 5350233

Snapshot

Description of Snapshot Information Associated with Image

Referenced by the following interfaces: DescribeImages

name	required	NULL allowed	type	description
SnapshotId	yes	no	String	Snapshot ID. Example: snap-7et7t234
DiskUsage	yes	no	String	Cloud disk type that creates the snapshot. Value range: SYSTEM_DISK: System disk DATA_DISK: Data disk. Example: SYSTEM_DISK
DiskSize	yes	no	Uint64	The size of the CBS for creating this snapshot, in GB. Example: 50

ExtraProperty

Describes additional attribute information.

Referenced by the following interfaces: DescribeZoneInstanceConfigInfos

name	required	NULL allowed	type	description
edgeZonePid	no	no	Uint64	Edge zone process. Example: 0

KeyBill

Description of Instance Order ID

Referenced by the following interfaces: DescribeInstancesAttribute

name	required	NULL allowed	type	description
InstanceId	yes	no	String	Instance ID, in the format of ins-11112222. Example: ins-61dyt49h
BillId	yes	yes	String	Order ID Example: 2018122583483923 4

InstanceTypeItem

Instance type information.

Referenced by the following interfaces: DescribeInstanceConfigInfos

name	required	NULL allowed	type	description
InstanceType	yes	no	String	Instance type. Example: S1.SMALL2
Cpu	yes	no	Uint64	Number of CPU cores. Example: 2
Memory	yes	no	Uint64	Memory size. Example: 2048
Gpu	yes	no	Uint64	Number of GPU cores. Example: 2
Fpga	yes	no	Uint64	Number of FPGA cores. Example: 2
StorageBlock	yes	no	Uint64	Number of storage blocks. Example: 2
NetworkCard	yes	no	Uint64	Number of network interface cards. Example: 2
MaxBandwidth	yes	no	Float	Maximum bandwidth. Example: 100.0
Frequency	yes	no	String	Frequency. Example: 2.5 GHz
CpuModelName	yes	no	String	CPU model name. Example: Intel Xeon Skylake 6133
Pps	yes	no	Uint64	Packet forwarding rate. Example: 10
Externals	yes	no	Externals	External information. Example:View
Remark	yes	no	String	Remark information. Example: alice use

HostOrder

Order Information Related to CDH Instance

Referenced by the following interfaces: SwitchParameterAllocateHosts

name	required	NULL allowed	type	description
appId	no	no	Uint64	Application ID of Order Account Example: 125550011
uin	no	no	String	Account UIN that Created Order Example: 324532343
ownerUin	no	no	String	Owner UIN of Order Account Example: 324532343
goods	no	no	Array of HostGoodsItem	List of Resource Information for Order Shipment Example:View

MonitorServiceItem

Monitoring Service

Referenced by the following interfaces: DescribeInstanceConfigInfos, DescribeInstancesActionTimer, DescribeLaunchTemplatesInfo, DescribeZoneInstanceConfigInfos, ImportInstancesActionTimer, ModifyInstancesActionTimer, QueryInstancesActionTimer, SwitchParameterRunInstances, UpdateInstancesActionTimer

name	required	NULL allowed	type	description
Enabled	no	yes	String	Enable/Disable Example: FALSE

LaunchTemplatesInfo

Information about an instance launch template.
Referenced by the following API: DescribeLaunchTemplateInfo.

Referenced by the following interfaces: DescribeLaunchTemplatesInfo

name	required	NULL allowed	type	description
LaunchTemplateId	no	yes	String	Instance launch template ID. Note: This field may return null, indicating that no valid value was found. Example: lt-k8wrok8e
LaunchTemplateName	no	yes	String	Name of an instance launch template. Note: This field may return null, indicating that no valid values can be obtained. Example: jack lt
LaunchTemplateVersionData	no	yes	LaunchTemplateVersionData	Version information of an instance launch template. Note: This field may return null, indicating that no valid values can be obtained. Example:View
LaunchTemplateVersionDescription	no	yes	String	Description of an instance launch template. Note: This field may return null, indicating that no valid values can be obtained. Example: alice use
CreatedBy	no	yes	String	Create the user UIN of this template. Note: This field may return null, indicating that no valid values can be obtained. Example: 32341324
CreationTime	no	yes	String	Creation time of this template. Note: This field may return null, indicating that no valid values can be obtained. Example: 2014-08-03 12:00:00

KvType

Key Value Type

Referenced by the following interfaces: DescribeUserGlobalConfigs

name	required	NULL allowed	type	description
Name	yes	no	String	Key Name Example: key
Value	yes	no	String	Value Corresponding to Key Example: val

Tag

Tag Key-Value Pair

Referenced by the following interfaces: CloneInstance, CreateLaunchTemplate, DescribeDisasterRecoverGroups, DescribeImages, DescribeInstances, DescribeKeyPairs, DescribeLaunchTemplatesInfo, ModifyLaunchTemplate, RunInstances

name	required	NULL allowed	type	description
Key	yes	no	String	Tag Key Example: alice-key
Value	yes	no	String	Tag Value Example: alice-value
tagKey	no	yes	String	Tag Key Example: alice-key
tagValue	no	yes	String	Tag Value Example: alice-value

AccountAttributeSet

Account Attribute Settings

Referenced by the following interfaces: DescribeAccountAttributes

name	required	NULL allowed	type	description
AttributeClass	yes	yes	String	Attribute Type Example: PostPaidInstanceCountLimit
AttributeValueSet	yes	yes	Array of AccountAttribute	Attribute Value Example:View

HostGoodsItem

Detailed Information of CDH Shipment Instance

Referenced by the following interfaces: SwitchParameterAllocateHosts

name	required	NULL allowed	type	description
goodsCategoryId	no	no	Uint64	goodsCategoryId Example: 100021
payMode	no	no	Uint64	Instance Billing Mode Example: 2
goodsNum	no	no	Uint64	Number of Shipped Instances Example: 5
regionId	no	no	Uint64	Region ID Example: 1
uin	no	no	String	UIN of User Initiating Shipment Example: 12443154
ownerUin	no	no	String	Owner UIN of Account Initiating Shipment Example: 12443154
appId	no	no	Uint64	AppId Corresponding to Account Initiating Shipment Example: 122443154
projectId	no	no	Uint64	Project ID Example: 1
zoneId	no	no	Uint64	Availability Zone ID Example: 100002
goodsDetail	no	no	HostGoodsDetailItem	Detailed Information of CDH Instance ExampleView

ErrorCode

Feature Description

If there is an Error field in the response, it means that the API call failed. For example:

```
{
    "Response": {
        "Error": {
            "Code": "AuthFailure.SignatureFailure",
            "Message": "The provided credentials could not be validated. Please check your signature is cor
rect."
        },
        "RequestId": "ed93f3cb-f35e-473f-b9f3-0d451b8b79c6"
    }
}
```

Code in Error indicates the error code, and Message indicates the specific information of the error.

Error Code List

Common Error Codes

Error codes	Description
AuthFailure.InvalidSecretId	Invalid key (not a Cloud API key type).
AuthFailure.MFAFailure	MFA failed.
AuthFailure.SecretIdNotFound	Key does not exist. Check if the key has been deleted or disabled in the console, and if not, check if the key is correctly entered. Note that whitespaces should not exist before or after the key.
AuthFailure.SignatureExpire	Signature expired. Timestamp and server time cannot differ by more than five minutes. Please ensure your current local time matches the standard time.
AuthFailure.SignatureFailure	Invalid signature. Signature calculation error. Please ensure you've followed the signature calculation process described in the Signature API documentation.
AuthFailure.TokenFailure	Token error.

Error codes	Description
AuthFailure.UnauthorizedOperation	The request does not have CAM authorization.
DryRunOperation	DryRun Operation. It means that the request would have succeeded, but the DryRun parameter was used.
FailedOperation	Operation failed.
InternalError	Internal error.
InvalidAction	The API does not exist.
InvalidParameter	Incorrect parameter.
InvalidParameterValue	Invalid parameter value.
LimitExceeded	Quota limit exceeded.
MissingParameter	A parameter is missing.
NoSuchVersion	The API version does not exist.
RequestLimitExceeded	The number of requests exceeds the frequency limit.
ResourceInUse	Resource is in use.
ResourceInsufficient	Insufficient resource.
ResourceNotFound	The resource does not exist.
ResourceUnavailable	Resource is unavailable.
UnauthorizedOperation	Unauthorized operation.
UnknownParameter	Unknown parameter.
UnsupportedOperation	Unsupported operation.
UnsupportedProtocol	HTTPS request method error. Only GET and POST requests are supported.
UnsupportedRegion	API does not support the requested region.

Service Error Codes

Error codes	Description
InvalidImageId.IncorrectState	The image status is illegal.

Error codes	Description
InvalidParameter.ContainsIllegalCharacter	The parameter contains illegal characters.
FailedOperation.NoAvailableIpAddressCountInSubnet	The available IPs in the subnet are exhausted.
InvalidParameterValue.LimitExceeded	The parameter value is out of range
InvalidParameterValue.InvalidHost	Invalid host
InvalidClientToken.TooLong	The string length of the specified ClientToken exceeds the limit. It should be less than or equal to 64 bytes.
SecGroupActionFailure	General error in security group service API calling.
InvalidAccount.InsufficientBalance	Insufficient account balance
InvalidKeyPairId.Malformed	Invalid key pair ID. The format of the specified key pair ID is incorrect, for example, an ID length error skey-1122 .
InternalError.TradeUnknownError	An internal billing error occurred.
InvalidAddressState	The current status of the specified EIP does not support this operation.
ResourceInsufficient.ZoneSoldOutForSpecifiedInstance	Instances in the specified zone have been sold out.
InvalidKeyPairNameEmpty	The key name is empty.
InvalidParameterValue.InstanceIdMalformed	The instance ID does not meet the requirements. Provide a standard instance ID, such as ins-xxxxxxxx, where the letter x represents a lowercase character or number.
InvalidParameterValue.Range	Invalid parameter value. The range of the parameter value is not legal.
InvalidAccountIs.YourSelf	You cannot share an image with yourself.
MissingParameter	Parameters are missing. The request did not include mandatory parameters.
InvalidAddressIps.NotFound	Invalid IP Address

Error codes	Description
UnauthorizedOperation.ProjectNotFound	This operation is not allowed. Please ensure this account is in the selected project.
InvalidParameter.CbsInUse	The provided CBS is in use.
ResourceNotFound.HpcCluster	The high-performance computing cluster does not exist.
UnsupportedOperation.InvalidZone	The zone is invalid.
InvalidKeyPairNameTooLong	The key name exceeds 25 characters.
InvalidProjectId.NotFound	Invalid project ID. The specified project ID does not exist.
InvalidImageId.NotFound	Image not found
InvalidPeriod	Invalid duration. Currently, only the following durations are supported: [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 24, 36], unit: months.
InvalidParameterValue.KeyPairNotSupported	The key is not supported.
InvalidParameter.InvalidParameterUrlError	Incorrect URL address.
InvalidKeyPairId.NotFound	Invalid key pair ID. The specified key pair ID does not exist.
InvalidImageId.TooLarge	The image size exceeds the limit.
InvalidInstance.NotSupported	Unsupported instance.
InvalidKeyPairNameIncludeIllegalChar	The key name includes illegal characters. The key name only supports letters, digits, and underscores.
InvalidPassword	Invalid password. The specified password does not meet password complexity restrictions. For example, the password length does not meet restrictions.
InstancesQuotaLimitExceeded	It indicates that the number of instances being created exceeds the remaining quota allowed for purchase by the account.

Error codes	Description
InvalidParameterValue.InvalidParameterValueLimit	Parameter value error.
InvalidInstanceType.Malformed	The parameter format of the specified InstanceType is invalid.
FailedOperation.PlacementSetNotEmpty	The placement group is not empty.
InvalidAccount.UnpaidOrder	The account has unpaid orders.
FailedOperation.InquiryPriceFailed	Failed to get the cost
InvalidParameterValue.LaunchTemplateNotFound	The instance launch template was not found.
InvalidRegion.Unavailable	Currently, this zone does not support synchronizing an image.
InvalidImageName.Duplicate	The image name is the same as the existing image.
InternalError	Internal error
ResourceInsufficient.SpecifiedInstanceType	The inventory of the specified instance type is insufficient.
ResourceInUse.HpcCluster	The high-performance computing cluster is in use.
FailedOperation.NoAvailablePublicImage	No available public images.
InvalidInstanceId.NotFound	No corresponding instance was found.
InvalidInstanceState	The specified instance's current status does not allow this operation.
InvalidParameter.JobIdNotExist	Invalid task ID. The specified task ID does not exist.
InvalidParameterValue.OutOfRange	The parameter value is out of range.
InvalidParameterValue.InvalidLaunchTemplateName	The format of the instance launch template name is incorrect.
ImageQuotaLimitExceeded	The image quota has exceeded the limit.
InvalidSearchWord.Valid	Invalid search keyword
VpcAddrNotInSubNet	The VPC IP is not within the subnet.

Error codes	Description
FailedOperation.NoAvailableInstanceFamily	No available instance families.
AuthFailure.CamRoleNameAuthenticateFailed	Role name authentication failed.
FailedOperation.InstanceMustHaveOneSecurityGroup	An instance should have at least one security group.
InvalidAddressId.NotFound	The specified EIP does not exist.
InvalidInstanceName.TooLong	The string length of the specified InstanceName exceeds the limit. It should be less than or equal to 60 bytes.
InvalidFilterValue.LimitExceeded	The number of Filter> Filter parameter values exceeds the limit.
ResourceNotFound.InvalidPlacementSet	The specified placement group does not exist.
InvalidKeyPairName.Duplicate	The key pair names are duplicate.
InvalidZone.MismatchRegion	The specified zone does not exist.
InvalidPublicKey.Duplicate	Invalid public key. The specified public key already exists.
InvalidParameter.ValueTooLarge	The parameter length exceeds the limit.
UnsupportedOperation.InstanceStateRunning	The instance is running.
InvalidHostId.Malformed	Invalid CDH ID. The format of the specified CDH ID is incorrect, for example, an ID length error host-1122 .
FailedOperation.SnapshotSizeLargerThanDataSize	The snapshot capacity exceeds the disk size. Choose a larger disk space.
InvalidParameterValueOffset	Invalid parameter value. The specified offset is invalid.
ResourceNotFound.SoldPoolNameNotFound	The sales pool name does not exist.
FailedOperation.NoAvailableVpc	There are no available VPC resources.
FailedOperation.NoAvailableCbs	No available CBS resources.
FailedOperation.NoQuotaForUserInstance	Insufficient quota to create an instance.

Error codes	Description
RegionAbilityLimit.UnsupportedToImportImage	This region does not support importing images.
InvalidParameterValue.LaunchTemplateVersion	Version number of invalid instance launch template.
InvalidHostId.NotFound	The specified HostId does not exist, or does not belong to the requesting account.
InvalidAccountId.NotFound	Invalid account ID
InvalidParameterCombination	It indicates that the parameter combination is incorrect.
ResourceNotFound.InvalidHostIpNotFound	Invalid host IP. The resource does not exist.
InvalidRegion.NotFound	The specified zone was not found.
VpcIpIsUsed	The VPC IP has already been used.
InvalidInstanceNotSupportedPrepaidInstance	The instance does not comply with the return rules for monthly subscription instances.
InvalidParameterValue.LaunchTemplateIdVerNotExisted	The combination of the instance launch template and version ID does not exist.
InvalidParameterValue	Invalid parameter value. The format of the parameter value is incorrect or not supported, etc.
InvalidParameter.InvalidParameterCoexistImageIdsFilters	You should not specify both ImageIds and Filters at the same time.
AccountQualificationRestrictions	The requesting account did not pass the qualification audit.
InvalidParameterValue.InvalidTaskIdFormat	The taskid is invalid.
FailedOperation.DisasterRecoverGroupNotFound	The specified disaster recovery group was not found.
InvalidParameter.InvalidIpFormat	The specified VPC IP format is incorrect.
InternalServerError	Internal operation error.

Error codes	Description
InvalidInstanceId.Malformed	Invalid Instance ID. The format of the specified instance ID is incorrect, for example, an instance ID length error ins-1122 .
InvalidSgId.Malformed	The format of the specified security group ID is incorrect, for example, an instance ID length error sg-ide32 .
InvalidFilter	Invalid filter.
InvalidParameterValue.LaunchTemplateIdNotExisted	The instance launch template ID does not exist.
InvalidCloudDisk.SoldOut	The cloud disk has been sold out.
InvalidParameterValueLimit	The parameter value is out of range
InvalidPermission	The account does not support this operation.
InvalidParameter	Invalid parameter. The parameter does not meet the requirements, is not supported, or the like.
InvalidImageId.Malformed	Invalid image ID
InvalidSecurityGroupId.NotFound	The specified security group ID does not exist.
InvalidImageId.InShared	The image is being shared.
FailedOperation.NoAvailableSubnet	There are no available subnet resources.
InvalidImageOsType.Unsupported	Unsupported operating system type.
FailedOperation.NoAvailableInstanceType	No available instance types.
InvalidParameterValue.LaunchTemplateIdMalformed	The format of the instance launch template ID is incorrect.
FailedOperation.NoAvailableSecurityGroup	No available security groups.
TradeUnknownError	Billing request error
InvalidPublicKey.Malformed	Invalid public key. The format of the specified public key format is incorrect and does not meet the OpenSSH RSA format

Error codes	Description
	requirements.
InvalidImageOsVersion.Unsupported	Unsupported operating system version.
MutexOperation.TaskRunning	The same task is already running.
InvalidHost.NotSupported	The specified operation is not supported by this host instance.
InvalidParameterValue.TooLong	Invalid input: Excessive length of the parameter.
FailedOperation.NoAvailableIpAddressCount	The subnet has no available IP addresses.
OverQuota	The maximum number of shared images allowed is reached
FailedOperation.NoCVMPermission	No instance operation permissions.
InvalidParameter.UrlError	The provided COS link cannot be accessed.
InvalidParameterValue.InvalidImageId	The image ID is invalid.
UnsupportedOperation.InstanceStateStopped	The request does not support instances that are shut down.
InvalidKeyPair.LimitExceeded	The number of key pairs exceeds the limit.
InvalidParameter.InvalidFilter	Invalid filter
InvalidParameter.InvalidTaskIdFormat	TaskId format error.

Service Migration(csm) version(2021-09-15) API overview

API version

V3

Instance APIs

Interface name	Interface function
CreateImageForTransitInstance	CreateImageForTransitInstance
CreateTransitInstance	CreateTransitInstance
DescribeTransitInstance	DescribeTransitInstance
ExitLiveMigrateLhInstance	ExitLiveMigrateLhInstance
LiveMigrateLhInstance	LiveMigrateLhInstance
TerminateTransitInstance	TerminateTransitInstance

Migration Source APIs

Interface name	Interface function
CreateSourceServer	CreateSourceServer
DeleteSourceServer	DeleteSourceServer
DescribeSourceServerDeniedActions	DescribeSourceServerDeniedActions
DescribeSourceServers	DescribeSourceServers
ModifySourceServer	ModifySourceServer

Task APIs

Interface name	Interface function
CreateMigrationJob	CreateMigrationJob
DeleteMigrationJob	DeleteMigrationJob
DescribeMigrationJobDeniedActions	DescribeMigrationJobDeniedActions
DescribeMigrationJobs	DescribeMigrationJobs
ModifyMigrationJob	ModifyMigrationJob
StartMigrationJob	StartMigrationJob
StopMigrationJob	StopMigrationJob

CallingMethod signaturev1

Converge Cloud authenticates each access request, i.e. each request needs to include authentication information (Signature) in the common parameters to verify the identity of the requester.
The Signature is generated by the security credentials which include SecretId and SecretKey. If you don't have the security credentials yet, go to the API Key page to apply for them; otherwise, you cannot invoke the API.

1. Applying for Security Credentials

Before using the API for the first time, go to the API Key page to apply for security credentials.
Security credentials consist of SecretId and SecretKey:

- SecretId is used to identify the API requester.
- SecretKey is used to encrypt the signature string and verify it on the server.
- You must keep your security credentials private and avoid disclosure.

You can apply for the security credentials through the following steps:

1. Log in to the Converge Cloud Console.
2. Go to the Cloud API Key page.
3. On the API Key Management page, click Create Key to create a SecretId/SecretKey pair.

Note: Each account can have up to two pairs of SecretId/SecretKey.

2. Generating a Signature

With the SecretId and SecretKey, a signature can be generated. The following describes how to generate a signature:

Assume that the SecretId and SecretKey are:

- SecretId: AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE
- SecretKey: Gu5t9xGARNpq86cd98joQYCN3EXAMPLE

Note: This is just an example. For actual operations, please use your own SecretId and SecretKey.

Take the Cloud Virtual Machine's request to view the instance list (DescribeInstances) as an example. When

you invoke this API, the request parameters may be as follows:

Parameter name	Description	Parameter value
Action	Method name	DescribeInstances
SecretId	Key ID	AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE
Timestamp	Current timestamp	1465185768
Nonce	Random positive integer	11886
Region	Region where the instance is located	luzon
InstanceIds.0	ID of the instance to query	ins-09dx96dg
Offset	Offset	0
Limit	Allowed maximum output	20
Version	API version number	2017-03-12

2.1. Sorting Parameters

First, sort all the request parameters in an ascending lexicographical order (ASCII code) by their names. Notes: (1) Parameters are sorted by their names instead of their values; (2) The parameters are sorted based on ASCII code, not in an alphabetical order or by values. For example, InstanceIds.2 should be arranged after InstanceIds.12. You can complete the sorting process using a sorting function in a programming language, such as the ksort function in PHP. The parameters in the example are sorted as follows:

```
{
    'Action' : 'DescribeInstances',
    'InstanceIds.0' : 'ins-09dx96dg',
    'Limit' : 20,
    'Nonce' : 11886,
    'Offset' : 0,
    'Region' : 'luzon',
    'SecretId' : 'AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE',
    'Timestamp' : 1465185768,
    'Version': '2017-03-12',
}
```

When developing in another programming language, you can sort these sample parameters and it will work as long as you obtain the same results.

2.2. Concatenating a Request String

This step generates a request string.
Format the request parameters sorted in the previous step into the form of "parameter name"="parameter value". For example, for the Action parameter, its parameter name is "Action" and its parameter value is "DescribeInstances", so it will become Action=DescribeInstances after formatted.
Note: The "parameter value" is the original value but not the value after URL encoding.

Then, concatenate the formatted parameters with "&". The resulting request string is as follows:

```
Action=DescribeInstances&InstanceIds.0=ins-09dx96dg&Limit=20&Nonce=11886&Offset=0&Region=luzon&SecretId=AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE&Timestamp=1465185768&Version=2017-03-12
```

2.3. Concatenating the Signature Original String

This step generates a signature original string.
The signature original string consists of the following parameters:

1. HTTP method: POST and GET modes are supported, and GET is used here for the request. Please note that the method name should be in all capital letters.
2. Request host: the domain name of the request to view the list of instances (DescribeInstances) is cvm.convergecloud.com. The actual request domain name varies by the module to which the API belongs. For more information, see the instructions of the specific API.
3. Request path: The request path in the current version of Cloud API is fixed to / .
4. Request string: the request string generated in the previous step.

The concatenation rule of the signature original string is: Request method + request host + request path + ? + request string

The concatenation result of the example is:

```
GETcvm.convergecloud.com/?Action=DescribeInstances&InstanceIds.0=ins-09dx96dg&Limit=20&Nonce=11886&Offset=0&Region=luzon&SecretId=AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE&Timestamp=1465185768&Version=2017-03-12
```

2.4. Generating a Signature String

This step generates a signature string.
First, use the HMAC-SHA1 algorithm to sign thesignature original stringobtained in the previous step, and then encode the generated signature using Base64 to obtain the final signature.

The specific code is as follows with the PHP language being used as an example:

```
$secretKey = 'Gu5t9xGARNpq86cd98joQYCN3EXAMPLE';
$srcStr = 'GETcvm.convergecloud.com/?Action=DescribeInstances&InstanceIds.0=ins-09dx96dg&Limit
=20&Nonce=11886&Offset=0&Region=luzon&SecretId=AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPL
E&Timestamp=1465185768&Version=2017-03-12';
$signStr = base64_encode(hash_hmac('sha1', $srcStr, $secretKey, true));
echo $signStr;
```

The final signature is:

```
EliP9YW3pW28FpsEdkXt/+WcGeI=
```

When developing in another programming language, you can sign and verify the original in the example above and it works as long as you get the same results.

3. Encoding a Signature String

The generated signature string cannot be directly used as a request parameter and must be URL encoded.

For example, if the signature string generated in the previous step is EliP9YW3pW28FpsEdkXt/+WcGeI= , the final signature string request parameter (Signature) is EliP9YW3pW28FpsEdkXt%2f%2bWcGeI%3d, which will be used to generate the final request URL.

**Note: If your request method is GET, or the request method is POST and the Content-Type is application/x-www-form-urlencoded, then all the request parameter values need to be URL encoded (except the parameter key and the symbol of =) when sending the request. Non-ASCII characters need to be encoded with UTF-8 before URL encoding. **

Note: The network libraries of some programming languages automatically URL encode all parameters, in which case there is no need to URL encode the signature string; otherwise, two rounds of URL encoding will cause the signature to fail.

Note: Other parameter values also need to be encoded using RFC 3986. Use %XY in percent-encoding for special characters such as Chinese characters, where "X" and "Y" are hexadecimal characters (0-9 and uppercase A-F), and using lowercase will cause an error.

4. Signature Failure

The following situational error codes for signature failure may occur. Please resolve the errors accordingly.

Error code	Error description
AuthFailure.SignatureExpire	The signature is expired

Error code	Error description
AuthFailure.SecretIdNotFound	The key does not exist
AuthFailure.SignatureFailure	Signature error
AuthFailure.TokenFailure	Token error
AuthFailure.InvalidSecretId	Invalid key (not a Cloud API key type)

5. Signature Demo

When calling API 3.0, you are recommended to use the corresponding Converge Cloud SDK 3.0, Swhich encapsulates the signature process, enabling you to focus on only the specific APIs provided by the product when developing. See SDK Center for more information. Currently, the following programming languages are supported:

- Python
- Java
- PHP
- Go
- Node

To further explain the signing process, we will use a programming language to implement the process described above. The request domain name, API and parameter values in the sample are used here. This goal of this example is only to provide additional clarification for the signature process, please see the SDK for actual usage.

The final output URL might be: https://cvm.convergecloud.com/?Action=DescribeInstances&InstanceIds.0=ins-09dx96dg&Limit=20&Nonce=11886&Offset=0&Region=luzon&SecretId=AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE&Signature=EliP9YW3pW28FpsEdkXt%2F%2BWcGeI%3D&Timestamp=1465185768&Version=2017-03-12

Note: The key in the example is fictitious, and the timestamp is not the current time of the system, so if this URL is opened in the browser or called using commands such as curl, an authentication error will be returned: Signature expired. In order to get a URL that can work properly, you need to replace the SecretId and SecretKey in the example with your real credentials and use the current time of the system as the Timestamp.

Note: In the example below, even if you use the same programming language, the order of the parameters in the URL may be different for each execution. However, the order does not matter, as long as all the parameters are included in the URL and the signature is calculated correctly.

Note: The following code is only applicable to API 3.0. It cannot be directly used in other signature processes. Even with an older API, signature calculation errors may occur due to the differences in details. Please refer to the corresponding documentation.

Java

```
import java.io.UnsupportedEncodingException;
import java.net.URLEncoder;
import java.util.Random;
import java.util.TreeMap;
import javax.crypto.Mac;
import javax.crypto.spec.SecretKeySpec;
import javax.xml.bind.DatatypeConverter;

public class CloudAPIDemo {
    private final static String CHARSET = "UTF-8";

    public static String sign(String s, String key, String method) throws Exception {
        Mac mac = Mac.getInstance(method);
        SecretKeySpec secretKeySpec = new SecretKeySpec(key.getBytes(CHARSET), mac.getAlgorithm());
        mac.init(secretKeySpec);
        byte[] hash = mac.doFinal(s.getBytes(CHARSET));
        return DatatypeConverter.printBase64Binary(hash);
    }

    public static String getStringToSign(TreeMap<String, Object> params) {
        StringBuilder s2s = new StringBuilder("GETcvm.convergecloud.com/?");
        // When signing, the parameters need to be sorted in lexicographical order. TreeMap is used here
to guarantee the correct order.
        for (String k : params.keySet()) {
            s2s.append(k).append("=").append(params.get(k).toString()).append("&");
        }
        return s2s.toString().substring(0, s2s.length() - 1);
    }

    public static String getUrl(TreeMap<String, Object> params) throws UnsupportedEncodingException
{
        StringBuilder url = new StringBuilder("https://cvm.convergecloud.com/?");
        // There is no requirement for the order of the parameters in the actual request URL.
        for (String k : params.keySet()) {
            // The request string needs to be URL encoded. As the Key is all in English letters, only the valu
e is URL encoded here.
            url.append(k).append("=").append(URLEncoder.encode(params.get(k).toString(), CHARSET)).app
end("&");
        }
        return url.toString().substring(0, url.length() - 1);
```

```
    }

    public static void main(String[] args) throws Exception {
        TreeMap<String, Object> params = new TreeMap<String, Object>(); // TreeMap enables automati
c sorting
        // A random number should be used when actually calling, for example: params.put("Nonce", new
Random().nextInt(java.lang.Integer.MAX_VALUE));
        params.put("Nonce", 11886); // Common parameter
        // The current time of the system should be used when actually calling, for example:   params.put
("Timestamp", System.currentTimeMillis() / 1000);
        params.put("Timestamp", 1465185768); // Common parameter
        params.put("SecretId", "AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE"); // Common parameter
        params.put("Action", "DescribeInstances"); // Common parameter
        params.put("Version", "2017-03-12"); // Common parameter
        params.put("Region", "luzon"); // Common parameter
        params.put("Limit", 20); // Business parameter
        params.put("Offset", 0); // Business parameter
        params.put("InstanceIds.0", "ins-09dx96dg"); // Business parameter
        params.put("Signature", sign(getStringToSign(params), "Gu5t9xGARNpq86cd98joQYCN3EXAMPLE
", "HmacSHA1")); // Common parameter
        System.out.println(getUrl(params));
    }
}
```

Python

Note: If running in a Python 2 environment, the following requests dependency package must be installed first: pip install requests .

```
# -*- coding: utf8 -*-
import base64
import hashlib
import hmac
import time

import requests

secret_id = "AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE"
secret_key = "Gu5t9xGARNpq86cd98joQYCN3EXAMPLE"

def get_string_to_sign(method, endpoint, params):
    s = method + endpoint + "/?"
    query_str = "&".join("%s=%s" % (k, params[k]) for k in sorted(params))
    return s + query_str

def sign_str(key, s, method):
```

```
    hmac_str = hmac.new(key.encode("utf8"), s.encode("utf8"), method).digest()
    return base64.b64encode(hmac_str)

if __name__ == '__main__':
    endpoint = "cvm.convergecloud.com"
    data = {
        'Action' : 'DescribeInstances',
        'InstanceIds.0' : 'ins-09dx96dg',
        'Limit' : 20,
        'Nonce' : 11886,
        'Offset' : 0,
        'Region' : 'luzon',
        'SecretId' : secret_id,
        'Timestamp' : 1465185768, # int(time.time())
        'Version': '2017-03-12'
    }
    s = get_string_to_sign("GET", endpoint, data)
    data["Signature"] = sign_str(secret_key, s, hashlib.sha1)
    print(data["Signature"])
    # n actual invocation would occur here, which may incur fees after success
    # resp = requests.get("https://" + endpoint, params=data)
    # print(resp.url)
```

signaturev3

Converge Cloud The API will authenticate each access request, meaning that each request must include signature information (Signature) in the public request parameters to verify the requester's identity.
The signature information is generated by the security credentials, which include SecretId and SecretKey . If the user does not have security credentials, please apply for them on the Cloud API Key page, otherwise they cannot call the Cloud API interfaces.

1. Apply for security credentials.

Before using the Cloud API for the first time, please go to the Cloud API Key page to apply for a security credential.
Security credentials include SecretId and SecretKey:

- SecretId The security credentials are used to identify the identity of the API caller.
- SecretKey The secret key is used to encrypt and sign the string for server-side verification of the signature.
- Users must strictly protect their security credentials and avoid disclosure them.

The specific steps to apply for security credentials are as follows:

1. Log in to Converge Cloud Administration Center Console
2. Go to the console page for cloud API keys
3. On the Cloud API Key page, click New to create a pair of SecretId/SecretKey

Note: Developer accounts can have up to two pairs SecretId / SecretKey.

2. TC3-HMAC-SHA256 signature method

Note: For GET method, only Content-Type: application/x-www-form-urlencoded protocol format is supported. For POST method, Content-Type: application/json and Content-Type: multipart/form-data are currently supported. By default, all business interfaces are supported in json format. Only specific business interfaces are supported in multipart format. In this case, the interface cannot be called in json format. Refer to the specific business interface document description.

The following takes Cloud Virtual Machine querying Region-1 instance list as an example to introduce the signature calculation process step by step. We only use two parameters for the query instance list: Limit and Offset, called using the GET method.

Assume that the SecretId and SecretKey of the user are AKIDz 8krbsJ 5yKBZQpn 74WFkmLPx 3EXAMPLE and Gu 5t9xGARNpq 86cd 98joQYCN3EXAMPLE, respectively.

2.1. splice specification request string

Concatenate CanonicalRequest strings in the following format:

```
CanonicalRequest =
  HTTPRequestMethod + '\n' +
  CanonicalURI + '\n' +
  CanonicalQueryString + '\n' +
  CanonicalHeaders + '\n' +
  SignedHeaders + '\n' +
  HashedRequestPayload
```

- HTTPRequestMethod: HTTP request methods (GET, POST), GET in this example;
- CanonicalURI: URI parameter, API 3.0 fixed to forward slash (/);
- CanonicalQueryString: Query string in the URL that initiates the HTTP request. For POST requests, it is fixed as an empty string. For GET requests, it is the question mark (?) in the URL. The following string content, this example value is: Limit=10&Offset=0. Note: CanonicalQueryString needs to be URL encoded.
- CanonicalHeaders: The header information of participating signature, at least including host and content-type, can also be added with customized header to improve the uniqueness and security of its own request. Splicing rules: 1) head key and value are uniformly converted to lowercase, and the first and last spaces are removed, and spliced according to the format of key:value\n;2) multiple heads are spliced according to the dictionary sorting of head key (lowercase). In this example: content-type: application/x-www-form-urlencoded\nhost: cvm.convergecloud.com\n
- SignedHeaders: The header information involved in the signature indicates which headers participate in the signature of this request, and the header content contained in CanonicalHeaders is one-to-one corresponding. content-type and host are required headers. constructed as: 1) The head key is uniformly converted to lowercase; 2) Multiple header keys (lowercase) are concatenated according to dictionary sorting and separated by semicolons (;). In this case: content-type;host
- HashedRequestPayload: The hash value of the request body, calculated as Lowercase(HexEncode(Hash.SHA256(RequestPayload))), SHA256 hash the entire payload of the HTTP request body, then hexadecimal encoding, and finally converting the encoding string to lowercase letters. Note: For GET requests, RequestPayload is fixed as an empty string. For POST requests, RequestPayload is the payload of the HTTP request body.

According to the above rules, the resulting canonical request string in the example is as follows (for clarity, \nnewlines are replaced by a new line printed separately):

```
GET
```

```
/
Limit=10&Offset=0
content-type:application/x-www-form-urlencoded
host:cvm.convergecloud.com

content-type;host
e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
```

2.2. Concatenate the string to be signed

Concatenate the string to be signed in the following format:

```
StringToSign =
  Algorithm + \n +
  RequestTimestamp + \n +
  CredentialScope + \n +
  HashedCanonicalRequest
```

- Algorithm: Signature algorithm, currently fixed as TC3-HMAC-SHA256;
- RequestTimestamp: Request timestamp, i.e. the X-TC-Timestamp value of the request header. The request in the example above is 1539084154;
- CredentialScope: Credential range in the format Date/service/tc3_request, containing date, requested service and termination string (tc3_request). **Date is the date of UTC standard time, the value needs to be consistent with UTC standard time converted by common parameter X-TC-Timestamp **;service is the product name, which must be consistent with the product domain name called, such as cvm. The above example request, the value is 2018-10-09/cvm/tc3_request;
- HashedCanonicalRequest: The hash value of the canonical request string obtained by concatenating the above steps is calculated by Lowercase(HexEncode(Hash.SHA256(CanonicalRequest))).

note:

> 1. Date must be calculated from timestamp X-TC-Timestamp and time zone UTC+0. Adding local time zone information to the system, such as East Zone 8, will cause calls to succeed during the day and night, but calls to fail in the early hours of the morning. Assuming the timestamp is 1551113065, the time in the East Eight District is 2019-02-26 00:44:25, but the calculated Date with UTC+0 should be 2019-02-25 instead of 2019-02-26.
> 2. Timestamp must be the current system time and ensure that the system time and standard time are synchronized. If the difference exceeds five minutes, it will fail. If it is not synchronized with the standard time for a long time, it may cause the request to fail after running for a period of time (return signature expiration error).

According to the above rules, the string to be signed in the example is as follows (for clarity,\nnewlines are

replaced by new lines printed):

```
TC3-HMAC-SHA256
1539084154
2018-10-09/cvm/tc3_request
91c9c192c14460df6c1ffc69e34e6c5e90708de2a6d282cccf957dbf1aa7f3a7
```

2.3. calculate the signature

1. Compute the derived signature key, pseudocode as follows

```
SecretKey = "Gu5t9xGARNpq86cd98joQYCN3EXAMPLE"
SecretDate = HMAC_SHA256("TC3" + SecretKey, Date)
SecretService = HMAC_SHA256(SecretDate, Service)
SecretSigning = HMAC_SHA256(SecretService, "tc3_request")
```

- SecretKey: Original SecretKey;
- Date: That is, the Date field information in Credential, as shown in the example above, is 2018-10-09.;
- Service: That is, the Service field information in Credential, as shown in the example above, is cvm;

2. Calculate the signature, pseudocode as follows

```
Signature = HexEncode(HMAC_SHA256(SecretSigning, StringToSign))
```

- SecretSigning: That is, the derivative signature key calculated above;
- StringToSign: That is, the character string to be signed calculated in step 2;

2.4. Splicing Authorization

Splice as follows Authorization:

```
Authorization =
    Algorithm + ' ' +
    'Credential=' + SecretId + '/' + CredentialScope + ', ' +
    'SignedHeaders=' + SignedHeaders + ', '
    'Signature=' + Signature
```

- Algorithm: Signature method, fixed as TC3-HMAC-SHA256;
- SecretId: SecretId in key pair;
- CredentialScope: See above, Scope of Voucher;
- SignedHeaders: See above, header information for participating signatures;
- Signature: signature value

According to the above rules, the values obtained in the example are:

```
TC3-HMAC-SHA256 Credential=AKIDEXAMPLE/Date/service/tc3_request, SignedHeaders=content-type;host, Signature=5da7a33f6993f0614b047e5df4582db9e9bf4672ba50567dba16c6ccf174c474
```

The final complete invocation information is as follows:

```
https://cvm.convergecloud.com/?Limit=10&Offset=0

Authorization: TC3-HMAC-SHA256 Credential=AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE/2018-10-09/cvm/tc3_request, SignedHeaders=content-type;host, Signature=5da7a33f6993f0614b047e5df4582db9e9bf4672ba50567dba16c6ccf174c474
Content-Type: application/x-www-form-urlencoded
Host: cvm.convergecloud.com
X-TC-Action: DescribeInstances
X-TC-Version: 2017-03-12
X-TC-Timestamp: 1539084154
X-TC-Region: luzon
```

3. signing failed

According to the actual situation, there are the following signature failure error codes, please handle according to the actual situation

error code	error description
AuthFailure.SignatureExpire	signature expiration
AuthFailure.SecretIdNotFound	key is not present
AuthFailure.SignatureFailure	signature error
AuthFailure.TokenFailure	token error
AuthFailure.InvalidSecretId	Illegal key (not cloud API key type)

4. Signature Demo

Java

```
import java.io.BufferedReader;
import java.io.InputStream;
```

```
import java.io.InputStreamReader;
import java.net.URL;
import java.text.SimpleDateFormat;
import java.util.Date;
import java.util.Map;
import java.util.TimeZone;
import java.util.TreeMap;
import javax.crypto.Mac;
import javax.crypto.spec.SecretKeySpec;
import javax.net.ssl.HttpsURLConnection;
import javax.xml.bind.DatatypeConverter;

import org.apache.commons.codec.digest.DigestUtils;

public class CloudAPITC3Demo {
    private final static String CHARSET = "UTF-8";
    private final static String ENDPOINT = "cvm.convergecloud.com";
    private final static String PATH = "/";
    private final static String SECRET_ID = "AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE";
    private final static String SECRET_KEY = "Gu5t9xGARNpq86cd98joQYCN3EXAMPLE";
    private final static String CT_X_WWW_FORM_URLENCODED = "application/x-www-form-urlencode
d";
    private final static String CT_JSON = "application/json";
    private final static String CT_FORM_DATA = "multipart/form-data";

    public static byte[] sign256(byte[] key, String msg) throws Exception {
        Mac mac = Mac.getInstance("HmacSHA256");
        SecretKeySpec secretKeySpec = new SecretKeySpec(key, mac.getAlgorithm());
        mac.init(secretKeySpec);
        return mac.doFinal(msg.getBytes(CHARSET));
    }

    public static void main(String[] args) throws Exception {
        String service = "cvm";
        String host = "cvm.convergecloud.com";
        String region = "luzon";
        String action = "DescribeInstances";
        String version = "2017-03-12";
        String algorithm = "TC3-HMAC-SHA256";
        String timestamp = "1539084154";
        //String timestamp = String.valueOf(System.currentTimeMillis() / 1000);
        SimpleDateFormat sdf = new SimpleDateFormat("yyyy-MM-dd");
        // Pay attention to the time zone, otherwise it is easy to make mistakes.
        sdf.setTimeZone(TimeZone.getTimeZone("UTC"));
        String date = sdf.format(new Date(Long.valueOf(timestamp + "000")));

        // ************* Step 1: Assemble the specification request string *************
```

```
        String httpRequestMethod = "GET";
        String canonicalUri = "/";
        String canonicalQueryString = "Limit=10&Offset=0";
        String canonicalHeaders = "content-type:application/x-www-form-urlencoded\n" + "host:" + host
+ "\n";
        String signedHeaders = "content-type;host";
        String hashedRequestPayload = DigestUtils.sha256Hex("");
        String canonicalRequest = httpRequestMethod + "\n" + canonicalUri + "\n" + canonicalQueryStri
ng + "\n"
                + canonicalHeaders + "\n" + signedHeaders + "\n" + hashedRequestPayload;
        System.out.println(canonicalRequest);

        // ************* Step 2: Stitching the string to be signed *************
        String credentialScope = date + "/" + service + "/" + "tc3_request";
        String hashedCanonicalRequest = DigestUtils.sha256Hex(canonicalRequest.getBytes(CHARSET));
        String stringToSign = algorithm + "\n" + timestamp + "\n" + credentialScope + "\n" + hashedCan
onicalRequest;
        System.out.println(stringToSign);

        // ************* Step 3: Calculate the signature *************
        byte[] secretDate = sign256(("TC3" + SECRET_KEY).getBytes(CHARSET), date);
        byte[] secretService = sign256(secretDate, service);
        byte[] secretSigning = sign256(secretService, "tc3_request");
        String signature = DatatypeConverter.printHexBinary(sign256(secretSigning, stringToSign)).toLow
erCase();
        System.out.println(signature);

        // ************* Step 4: Splicing Authorization *************
        String authorization = algorithm + " " + "Credential=" + SECRET_ID + "/" + credentialScope + ", "
                + "SignedHeaders=" + signedHeaders + ", " + "Signature=" + signature;
        System.out.println(authorization);

        TreeMap<String, String> headers = new TreeMap<String, String>();
        headers.put("Authorization", authorization);
        headers.put("Host", host);
        headers.put("Content-Type", CT_X_WWW_FORM_URLENCODED);
        headers.put("X-TC-Action", action);
        headers.put("X-TC-Timestamp", timestamp);
        headers.put("X-TC-Version", version);
        headers.put("X-TC-Region", region);
    }
}
```

Python

```
# -*- coding: utf-8 -*-
```

```
import hashlib, hmac, json, os, sys, time
from datetime import datetime

# key parameters
secret_id = "AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE"
secret_key = "Gu5t9xGARNpq86cd98joQYCN3EXAMPLE"

service = "cvm"
host = "cvm.convergecloud.com"
endpoint = "https://" + host
region = "luzon"
action = "DescribeInstances"
version = "2017-03-12"
algorithm = "TC3-HMAC-SHA256"
timestamp = 1539084154
date = datetime.utcfromtimestamp(timestamp).strftime("%Y-%m-%d")
params = {"Limit": 10, "Offset": 0}

# ************* Step 1: Assemble the specification request string *************
http_request_method = "GET"
canonical_uri = "/"
canonical_querystring = "Limit=10&Offset=0"
ct = "x-www-form-urlencoded"
payload = ""
if http_request_method == "POST":
    canonical_querystring = ""
    ct = "json"
    payload = json.dumps(params)
canonical_headers = "content-type:application/%s\nhost:%s\n" % (ct, host)
signed_headers = "content-type;host"
hashed_request_payload = hashlib.sha256(payload.encode("utf-8")).hexdigest()
canonical_request = (http_request_method + "\n" +
                     canonical_uri + "\n" +
                     canonical_querystring + "\n" +
                     canonical_headers + "\n" +
                     signed_headers + "\n" +
                     hashed_request_payload)
print(canonical_request)

# ************* Step 2: Stitching the string to be signed *************
credential_scope = date + "/" + service + "/" + "tc3_request"
hashed_canonical_request = hashlib.sha256(canonical_request.encode("utf-8")).hexdigest()
string_to_sign = (algorithm + "\n" +
                  str(timestamp) + "\n" +
                  credential_scope + "\n" +
                  hashed_canonical_request)
print(string_to_sign)
```

```
# ************* Step 3: Calculate the signature *************
# Compute signature digest function
def sign(key, msg):
    return hmac.new(key, msg.encode("utf-8"), hashlib.sha256).digest()
secret_date = sign(("TC3" + secret_key).encode("utf-8"), date)
secret_service = sign(secret_date, service)
secret_signing = sign(secret_service, "tc3_request")
signature = hmac.new(secret_signing, string_to_sign.encode("utf-8"), hashlib.sha256).hexdigest()
print(signature)

# ************* Step 4: Splicing Authorization *************
authorization = (algorithm + " " +
                 "Credential=" + secret_id + "/" + credential_scope + ", " +
                 "SignedHeaders=" + signed_headers + ", " +
                 "Signature=" + signature)
print(authorization)

# Common parameters added to request header
headers = {
    "Authorization": authorization,
    "Host": host,
    "Content-Type": "application/%s" % ct,
    "X-TC-Action": action,
    "X-TC-Timestamp": str(timestamp),
    "X-TC-Version": version,
    "X-TC-Region": region,
}
```

request

1. Service Address

Region refers to the geographical area of a physical data center. Converge Cloud ensures complete isolation between different regions, providing maximum stability and fault tolerance. To reduce access latency and improve download speed, it is recommended to choose the region closest to your customers.

You can view the complete region list by using the API interface "DescribeRegions".

2. Communications Protocol

All the Converge Cloud APIs communicate via HTTPS, providing highly secure communication tunnels.

3. Request Methods

Supported HTTP request methods:

- POST (recommended)
- GET

PThe Content-Type types supported by POST requests:

- application/json (recommended). The TC3-HMAC-SHA256 signature algorithm must be used.
- application/x-www-form-urlencoded. The HmacSHA1 or HmacSHA256 signature algorithm must be used.
- multipart/form-data (only supported by certain APIs). You must use TC3-HMAC-SHA256 to calculate the signature.

The size of a GET request packet is up to 32 KB. The size of a POST request is up to 1 MB when the HmacSHA1 or HmacSHA256 signature algorithm is used, and up to 10 MB when TC3-HMAC-SHA256 is used.

4. Character Encoding

Only UTF-8 encoding is used.

result

Response for Successful Requests

For example, when calling CAM API (version: 2017-03-12) to view the status of instances (DescribeInstancesStatus), if the request has succeeded, you may see the response as shown below:


```
{
    "Response": {
        "TotalCount": 0,
        "InstanceStatusSet": [],
        "RequestId": "b5b41468-520d-4192-b42f-595cc34b6c1c"
    }
}
```


- The API will return Response, which contains RequestId, as long as it processes the request. It does not matter if the request is successful or not.
- RequestId is the unique ID of an API request. Contact us with this ID when an exception occurs.
- Except for the fixed fields, all fields are action-specified. For the definitions of action-specified fields, see the corresponding API documentation. In this example, TotalCount and InstanceStatusSet are the fields specified by the API DescribeInstancesStatus. 0 TotalCount means that the requester owns 0 CVM instance so the InstanceStatusSet is empty.

Response for Failed Requests

If the request has failed, you may see the response as shown below:


```
{
    "Response": {
        "Error": {
            "Code": "AuthFailure.SignatureFailure",
            "Message": "The provided credentials could not be validated. Please check your signature is cor
rect."
        },
        "RequestId": "ed93f3cb-f35e-473f-b9f3-0d451b8b79c6"
    }
}
```


- The presence of the Error field indicates that the request has failed. A response for a failed request will include Error, Code and Message fields.

- Code is the code of the error that helps you identify the cause and solution. There are two types of error codes so you may find the code in either common error codes or API-specified error codes.
- Message explains the cause of the error. Note that the returned messages are subject to service updates. The information the messages provide may not be up-to-date and should not be the only source of reference.
- RequestId is the unique ID of an API request. Contact us with this ID when an exception occurs.

Common Error Codes

If there is an Error field in the response, it means that the API call failed. The Code field in Error indicates the error code. The following table lists the common error codes that all actions can return.

Error Code	Description
AuthFailure.InvalidSecretId	Invalid key (not a API key type).
AuthFailure.MFAFailure	MFA failed.
AuthFailure.SecretIdNotFound	The key does not exist.
AuthFailure.SignatureExpire	Signature expired.
AuthFailure.SignatureFailure	Signature error.
AuthFailure.TokenFailure	Token error.
AuthFailure.UnauthorizedOperation	The request does not have CAM authorization.
DryRunOperation	DryRun Operation. It means that the request would have succeeded, but the DryRun parameter was used.
FailedOperation	Operation failed.
InternalError	Internal error.
InvalidAction	The API does not exist.
InvalidParameter	Incorrect parameter.
InvalidParameterValue	Invalid parameter value.
LimitExceeded	Quota limit exceeded.
MissingParameter	A parameter is missing.
NoSuchVersion	The API version does not exist.

Error Code	Description
RequestLimitExceeded	The number of requests exceeds the frequency limit.
ResourceInUse	Resource is in use.
ResourceInsufficient	Insufficient resource.
ResourceNotFound	The resource does not exist.
ResourceUnavailable	Resource is unavailable.
UnauthorizedOperation	Unauthorized operation.
UnknownParameter	Unknown parameter.
UnsupportedOperation	Unsupported operation.
UnsupportedProtocol	hHTTPS request method error. Only GET and POST requests are supported.
UnsupportedRegion	API does not support the requested region.

PublicParameter

Common parameters are parameters used to identify users and interface authentication purposes. If not necessary, these parameters are not described in the separate interface document of each interface, but these parameters need to be carried in each request before the request can be normally initiated.

signature method v3

When using TC3-HMAC-SHA256 signature method, the common parameters need to be uniformly placed in the HTTP Header request header, as follows:

parameter name	type	required	described
X-TC-Action	String	Yes	The name of the operation interface. Refer to the description of the public parameter Action in the input parameters of the interface documentation for the value. For example, the value for the query instance list interface of the cloud server is DescribeInstances.
X-TC-Region	String	Yes	region parameters, Data used to identify which region you wish to operate on. The region value accepted by the interface refers to the description of the input parameter common parameter Region in the interface document. Note: Some interfaces do not need to pass this parameter, which is specifically stated in the interface documentation. In this case, even passing this parameter will not take effect.
X-TC-Timestamp	Integer	Yes	The current UNIX timestamp, which records the time when the API request was initiated. for example 1529223702. Note: If the time difference from the server exceeds 5 minutes, it will cause a signature expiration error.
X-TC-Version	String	Yes	Version of API for operation. Refer to the description of the public parameter Version in the interface document for the value. For example, the version of the cloud server. 2017-03-12.
Authorization	String	Yes	HTTP The standard authentication header field is "Authorization". For example: TC3-HMAC-SHA256 Credential=AKIDEXAMPLE/Date/service/tc3_request, SignedHeaders=content-type;host, Signature=fe5f80f77d5fa3beca038a248ff027d0445342fe2855ddc963176630326f1024 Here, - TC3-HMAC-SHA256: Signature method, currently fixed as this value, - Credential: Credential: Signature credential; AKIDEXAMPLE is the SecretId; Date is a date in UTC time, and this value must match the value of X-TC-Timestamp (a common parameter) in UTC time format; service is the name of the product/service, and is generally a domain name prefix. For example,cvm; - SignedHeaders: The headers that contains the authentication information; content-type and host are the required headers; - Signature: Signature digest.
X-TC-Token	String	No	The token used for temporary certificates needs to be used in conjunction with a temporary key. Temporary keys and tokens need to be obtained by calling the access management service interface. Long-term keys do not require tokens.

signature method v1

When using HmacSHA1 and HmacSHA256 signature methods, common parameters need to be placed uniformly in the request string, as follows

parameter name	type	required	described
Action	String	Yes	The name of the interface to be operated. The value refers to the explanation of the public parameter Action in the interface documentation. For example, for the cloud server's query instance list interface, the value is DescribeInstances .
Region	String	Yes	The region parameter is used to identify which region's data you want to operate on. The region value accepted by the interface is specified in the input parameter of the public parameter Region in the interface documentation. Note: Some interfaces do not require this parameter to be passed, which will be specifically mentioned in the interface documentation. Even if this parameter is passed, it will not take effect in this case.
Timestamp	Integer	Yes	The current UNIX timestamp, which can record the time when the API request is initiated. For example, 1529223702. If the difference between the current time is too large, it will cause a signature expiration error.
Nonce	Integer	Yes	A random positive integer combined with Timestamp is used to prevent replay attacks.
SecretId	String	Yes	The SecretId is an identifier applied for the cloud API key to identify the user's identity. A SecretId corresponds to a unique SecretKey , and the SecretKey is used to generate the request signature Signature .
Signature	String	Yes	Request signature is used to verify the legitimacy of this request. Users need to calculate it based on the actual input parameters. The specific calculation method can be found in the interface authentication documentation.
Version	String	Yes	The version of the API being operated on. The value refers to the description of the public parameter Version in the interface documentation. For example, the version of the cloud server. 2017-03-12.
SignatureMethod	String	No	Signature method, currently supports HmacSHA256 and HmacSHA1. HmacSHA256 algorithm is used to verify signatures only if this parameter is specified as HmacSHA 256, otherwise HmacSHA1 is used to verify signatures.
Token	String	No	Token used for temporary certificate needs to be used together with temporary key. The temporary key and Token need to be obtained from the Access Management service invocation interface. Long-term keys do not require tokens.

zone list

A region (Region) refers to the geographical area of a physical data center. Converge Cloud Translation: To deliver verification that completely isolates different regions, ensuring maximum stability and fault tolerance between regions. In order to reduce access latency and improve download speed, it is recommended that you choose the region closest to your customers.

You can view the complete region list by using the API interface Query Region List.

Instance APIs
CreateImageForTransitInstance

1. Interface Description

Interface request domain name: csm.api3.convergecloud.com.

This API is used to create images of the relay instances for migration.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-11-06 20:30:53.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CreateImageForTransitInstance
Version	Yes	No	String	Public parameter, The value of this interface: 2021-09-15
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
JobId	Yes	No	String	Migration job ID Example:

3. Output Parameters

Parameter name	Type	Description

Parameter name	Type	Description
ImageId	String	Image ID Example:
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
FailedOperation.JobIdNotExist	The jobId does not exist.

CreateTransitInstance

1. Interface Description

Interface request domain name: csm.api3.convergecloud.com.

This API is used to create relay instances for migration.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-11-06 20:16:20.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CreateTransitInstance
Version	Yes	No	String	Public parameter, The value of this interface: 2021-09-15
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
JobId	Yes	No	String	Migration job ID Example:
SystemDiskInfo	No	No	SystemDiskInfo	System disk information. Example:View
DataDisksInfo	No	No	Array of DataDiskInfo	Data disk information Example:View
DryRun	No	No	Bool	Whether to verify parameters only. Example:

3. Output Parameters

Parameter name	Type	Description
InstanceId	String	Relay instance ID. Example:
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
FailedOperation.JobIdNotExist	The jobId does not exist.

DescribeTransitInstance

1. Interface Description

Interface request domain name: csm.api3.convergecloud.com.

This API is used to query relay instances for migration.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-11-06 20:31:09.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeTransitInstance
Version	Yes	No	String	Public parameter, The value of this interface: 2021-09-15
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
JobId	Yes	No	String	Migration job ID Example:

3. Output Parameters

Parameter name	Type	Description
InstanceSet	Array of TransitInstance	Detailed information on the relay instance for migration. Example:View

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.InvalidJobId	The task ID is invalid, and the current operation cannot be performed.
FailedOperation.JobIdNotExist	The jobId does not exist.

ExitLiveMigrateLhInstance

1. Interface Description

Interface request domain name: csm.api3.convergecloud.com.

This API is used to exit a lightweight server from the online migration mode.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-11-06 20:30:38.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ExitLiveMigrateLhInstance
Version	Yes	No	String	Public parameter, The value of this interface: 2021-09-15
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
InstanceId	Yes	No	String	Lightweight instance ID, in the format of lhmins-xxx or lhins-xxx2. Example:
MigrateResult	Yes	No	String	Migration result. Value values: ["succ", "fail"]. Example:
SupportCloudInit	No	No	Bool	Whether cloud- init is supported. The default value is True. Example:
SourceSystemInfo	No	No	SourceSystemInfo	Source system information. Example:View

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
ResourceNotFound.InvalidInstanceIdNotFound	No corresponding instance was found.
InvalidParameterValue.InvalidInstanceIdMalformed	Invalid Instance ID. The format of the specified instance ID is incorrect, for example, an instance ID length error ins-1122 .

LiveMigrateLhInstance

1. Interface Description

Interface request domain name: csm.api3.convergecloud.com.

This API is used to initiate online migrations for lightweight servers.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-11-06 20:16:36.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: LiveMigrateLhInstance
Version	Yes	No	String	Public parameter, The value of this interface: 2021-09-15
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
InstanceId	Yes	No	String	Lightweight instance ID, including lhmins-xxxx and lhins-xxxx. Example:
ClientVersion	No	No	String	Tool version number. Example:
SysInfo	No	No	ClientSysInfo	Source system information. Example:View

3. Output Parameters

Parameter name	Type	Description

Parameter name	Type	Description
Ip	String	Public IP address of the target machine. If no value is returned, the default value is null. Example:
LanIp	String	Private IP address of the target machine. If no value is returned, the default value is null. Example:
Password	String	Password automatically generated for the migration. Example:
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
ResourceNotFound.InvalidInstanceIdNotFound	No corresponding instance was found.
InvalidParameterValue.InvalidInstanceIdMalformed	Invalid Instance ID. The format of the specified instance ID is incorrect, for example, an instance ID length error ins-1122 .

TerminateTransitInstance

1. Interface Description

Interface request domain name: csm.api3.convergecloud.com.

This API is used to terminate relay instances for migration.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-11-06 20:30:11.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: TerminateTransitInstance
Version	Yes	No	String	Public parameter, The value of this interface: 2021-09-15
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
JobId	Yes	No	String	Migration job ID Example:

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
FailedOperation.JobIdNotExist	The jobId does not exist.

Migration Source APIs
CreateSourceServer

1. Interface Description

Interface request domain name: csm.api3.convergecloud.com.

This API is used to create migration sources.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-11-06 20:31:34.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CreateSourceServer
Version	Yes	No	String	Public parameter, The value of this interface: 2021-09-15
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
ClientVersion	Yes	No	String	Version number of the migration tool, with a length of 1–64 characters, including English and digits. Single quotes ('), double quotes ("), semicolons (;), and backslashes () cannot be contained. Example:
SystemInfo	Yes	No	SystemInfo	Detailed information on the system of the migration source. Example:View
ServerInfo	Yes	No	ServerInfo	Detailed information on the migration source. Example:View
SystemDiskInfo	Yes	No	SystemDiskInfo	Detailed information on the system disk of the migration source. Example:View
Architecture	Yes	No	String	System architecture of the migration source. Valid values: x86_64 and x86_32. Example:
OsType	Yes	No	String	Operating system type of the migration source, with a length of 1– 64 characters, including English and digits. Single quotes ('), double quotes ("), semicolons (;), and backslashes () cannot be contained. Example:
Identifier	Yes	No	String	Unique identifier of the migration source, with a length of 64 characters, including English letters and digits. Other characters cannot be contained. Example:
Status	No	No	String	Migration source status. Example:
DataDisksInfo	No	No	Array of DataDiskInfo	Detailed information on the data disk of the migration source. Example:View
Name	No	No	String	Migration source name, with a length of 1–128 characters, including English, and digits. Single quotes ('), double quotes ("), semicolons (;), and backslashes () cannot be contained. Example:
Description	No	No	String	Migration source description, with a maximum length of 256 characters, including English, and digits. Single quotes ('), double quotes ("), semicolons (;), and backslashes () cannot be contained. Example:
SessionToken	No	No	String	Session token of the user's current migration. Example:
Platform	No	No	String	Source platform of the source machine. Example:
Product	No	No	String	Target product type. Example:

3. Output Parameters

Parameter name	Type	Description
SourceServerId	String	Migration source ID Example:
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.TooLong	Invalid input: Excessive length of the parameter.
InvalidParameterValue.InvalidTimeFormat	The time format is invalid.
InvalidParameterValue.ParameterValueContainsIllegalCharacter	The parameter value is invalid because it contains illegal characters.
InvalidParameterValue.TooShort	The parameter value is invalid because it is too short.
InvalidParameterValue.InvalidIdentifierFormat	The uniqueness parameter is invalid.
InvalidParameter.SourceServerExist	The source server has been registered.
InvalidParameterValue.SourceServerExist	The migration source already exists.
InvalidParameterValue.VersionFormatError	The version format is invalid.
InvalidParameterValue.VersionLowerThanRequired	The version number is invalid because it is earlier than the required version.
InvalidParameterValue.DataDiskSizeTooLarge	The data disk is too large.
InvalidParameterValue.SystemDiskSizeTooLarge	The system disk is too large.

DeleteSourceServer

1. Interface Description

Interface request domain name: csm.api3.convergecloud.com.

Remove migration source

Default interface request rate limit: 20 times per second.

Interface update time: 2024-11-06 20:28:57.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteSourceServer
Version	Yes	No	String	Public parameter, The value of this interface: 2021-09-15
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
SourceServerId	Yes	No	String	Migration source ID Example:

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
ResourceNotFound.InvalidLiveMigrateSourceServerId	The migration source ID does not exist.
FailedOperation.SourceServerRelatedUnFinishedJob	The specified migration source has been associated with unfinished migration tasks.
ResourceNotFound.InvalidLiveMigrateOnlineSourceServerId	The specified migration source is not in the online status.
FailedOperation.SourceServerStatusNotSupport	The migration source status does not support this operation.
InvalidParameterValue.InvalidSourceServerIdMalformed	The migration source ID is invalid because the specified migration source ID format is incorrect.

DescribeSourceServerDeniedActions

1. Interface Description

Interface request domain name: csm.api3.convergecloud.com.

This API is used to query prohibited operations for migration sources.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-11-06 20:31:46.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeSourceServerDeniedActions
Version	Yes	No	String	Public parameter, The value of this interface: 2021-09-15
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
SourceServerIds	Yes	No	Array of String	List of migration source IDs. Example:

3. Output Parameters

Parameter name	Type	Description
SourceServerDeniedActionSet	Array of SourceServerDeniedAction	List of prohibited operations for migration sources. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
ResourceNotFound.InvalidLiveMigrateSourceServerId	The migration source ID does not exist.

DescribeSourceServers

1. Interface Description

Interface request domain name: csm.api3.convergecloud.com.

This API is used to query the list of user migration sources.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-11-06 20:25:51.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeSourceServers
Version	Yes	No	String	Public parameter, The value of this interface: 2021-09-15
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
Limit	No	No	Uint64	Number of entries per page, which is used for pagination. Value range: [1, 50]. Example:
Filters	No	No	Array of Filter	Filtering condition. Valid values: source-server-id; name; job-id; status; os-type; architecture; product; session-token. Example:View
Offset	No	No	Uint64	Start number, used for pagination. Example:

3. Output Parameters

Parameter name	Type	Description
TotalCount	Uint64	Total number of results that meet conditions. Example:
SourceServers	Array of SourceServer	List of source machines on the current page. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.ParameterValueContainsIllegalCharacter	The parameter value is invalid because it contains illegal characters.
InvalidParameterValue.InvalidTaskIdFormat	The task ID format is incorrect.
InvalidParameterValue.ParameterValueNotSupportValue	The parameter value is not supported.
InvalidParameterValue.InvalidRegionNotFound	The region is invalid.
InvalidParameterValue.InvalidSourceServerIdMalformed	The migration source ID is invalid because the specified migration source ID format is incorrect.

ModifySourceServer

1. Interface Description

Interface request domain name: csm.api3.convergecloud.com.

This API is used to modify the migration source attributes.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-11-06 20:27:03.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifySourceServer
Version	Yes	No	String	Public parameter, The value of this interface: 2021-09-15
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
SourceServerId	Yes	No	String	Migration source ID Example:
Status	No	No	String	Migration Source Status Example:
UpdateTime	No	No	String	Update time of the migration source, in UTC+0 time zone. Its format is YYYY-MM-DDThh:mm:ssZ. Example:
Name	No	No	String	Migration source name, with a length of 1–128 characters, including English, and digits. Single quotes ('), double quotes ("), semicolons (;), and backslashes () cannot be contained. Example:
Description	No	No	String	Migration source description, with a maximum length of 256 characters, including English, and digits. Single quotes ('), double quotes ("), semicolons (;), and backslashes () cannot be contained. Example:

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.TooLong	Invalid input: Excessive length of the parameter.
InvalidParameterValue.InvalidTimeFormat	The time format is invalid.
InvalidParameterValue.TooShort	The parameter value is invalid because it is too short.
InvalidParameterValue.ParameterValueContainsIllegalCharacter	The parameter value is invalid because it contains illegal characters.
ResourceNotFound.InvalidLiveMigrateSourceServerId	The migration source ID does not exist.
InvalidParameterValue.InvalidSourceServerIdMalformed	The migration source ID is invalid because the specified migration source ID format is incorrect.

Task APIs
CreateMigrationJob

1. Interface Description

Interface request domain name: csm.api3.convergecloud.com.

This API is used to create online migration tasks.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-11-07 16:44:53.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CreateMigrationJob
Version	Yes	No	String	Public parameter, The value of this interface: 2021-09-15
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
SourceServerId	Yes	No	String	Source machine ID. Example:
SystemDiskInfo	Yes	No	SystemDiskInfo	Information on the system disk to be migrated. Example:View
Mode	Yes	No	Uint64	Migration task network mode. Value range: [0, 2]. 0 indicates the default mode; 2 indicates the private network migration mode scenario. Example:
TargetRegion	Yes	No	String	Target region of the migration task. Example:
Name	No	No	String	Migration task name, with a length of 1–128 characters, including English, and digits. Single quotes ('), double quotes ("), semicolons (;), and backslashes () cannot be contained. Example:
TargetType	No	No	String	Target result type of the migration task. Valid values: ["Image","Instance", "Lh-Image", "Lh-Instance"]. Example:
ImageName	No	No	String	Target image name of the migration task. The image name should comply with the custom image name specification and should be unique in the target region. If the entered image name is not unique, the migration backend will rename the image in the format of image_name_task_ID: testImageName_migrate-xxxxxxxx. Example:
DataDisksInfo	No	No	Array of DataDiskInfo	Information on the data disk to be migrated. Example:View
Description	No	No	String	Detailed description of the migration task, with a maximum length of 256 characters, including English, and digits. Single quotes ('), double quotes ("), semicolons (;), and backslashes () cannot be contained. Example:
InstanceId	No	No	String	Target instance ID of the migration task. Example:
MigrationConfigInfo	No	No	MigrationConfigInfo	Detailed configuration information on the migration task. Example:View
SecurityGroup	No	No	String	Security group ID of the relay instance for migration. Example:
VpcId	No	No	String	Virtual Private Cloud (VPC) ID of the relay instance for migration. Example:
StartTime	No	No	String	Start time of the migration task, in the UTC+0 time zone. Its format is YYYY-MM-DDThh:mm:ssZ, and the value should be later than or equal to the current time. If the value is null, it indicates that the task is created only and will be started by a trigger later. Example:
SubnetId	No	No	String	Subnet ID of the relay instance for migration. Example:
InstanceType	No	No	String	Model of the relay instance for migration. For the valid values of model specifications, see the CVM model documentation. Bare metal models are not supported currently. Example:
IncrementalMigration	No	No	Uint64	Whether to enable automatic incremental migration. Example:
IncrementalTime	No	No	String	End time of automatic incremental migration. Example:
OneClickJobId	No	No	String	One-click migration task ID. Example:
RunMode	No	No	String	Task running mode, which is used to set the timing for task startup. Valid values: ["Delayed", "Immediate", "Timed"]. The default value is "Delayed", which means the task will not be started after creation. If the parameter StartTime is set, the task running mode value is Timed. If the task needs to be run immediately after creation, set the value to Immediate. Example:
ExcludePathList	No	No	String	List of files or folders to be excluded. Example:
UserIntentList	No	No	String	User intent customized by the tool. Example:
Product	No	No	String	Migration product type. Example:

3. Output Parameters

Parameter name	Type	Description
JobId	String	Migration job ID Example:
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.IncrementalTimeGreaterThanSevenDays	The incremental migration time of the migration task is greater than seven days.
InvalidParameterValue.IncrementalTimeLessThanOneHour	The incremental migration time of the migration task is less than one hour.
UnsupportedOperation.MigrateJobCreateFullCvmImage	The migration task does not support creating a full-instance image.
InvalidParameterValue.InvalidSourceServerIdMalformed	The migration source ID is invalid because the specified migration source ID format is incorrect.
FailedOperation.NoAvailableIpAddressCountInSubnet	The available IPs in the subnet are exhausted.
InvalidParameterValue.SubnetNotExist	The specified subnet does not exist.
InvalidParameterValue.MigrateNotSupportInstanceType	The instance type is not supported for migration.
ResourceNotFound.InvalidInstanceIdNotFound	No corresponding instance was found.
InvalidParameterValue.InvalidRegionNotFound	The region is invalid.
InvalidParameterValue.SystemDiskSizeTooLarge	The system disk is too large.
InvalidParameterValue.DataDiskSizeTooLarge	The data disk is too large.
InvalidParameterValue.VpcIdSubnetIdNotMatch	The specified VpcId and SubnetId do not match.
InvalidParameterValue.MigrateJobNameExist	The specified migration task name already exists.
LimitExceeded.MigrateJobLimitExceeded	The number of migration tasks has reached the maximum value. Contact the administrator.
InvalidParameterValue.InvalidDataDiskIndex	The data disk index is invalid because it does not exist in the specified migration source.
InvalidParameterValue.VpcIdMalformed	The VPC ID xxx does not meet the requirements. Provide a standard VPC ID, such as vpc-xxxxxxxx, where the letter x represents a lowercase letter or digit.
InvalidParameterValue.SubnetIdMalformed	The subnet ID does not meet the requirements. Provide a standard subnet ID, such as subnet-xxxxxxxx, where the letter x represents a lowercase letter or digit.
InvalidParameterValue.TooLarge	The parameter value exceeds the maximum limit.
ResourceNotFound.InvalidLiveMigrateOnlineSourceServerId	The specified migration source is not in the online status.
FailedOperation.SourceServerRelatedUnFinishedJob	The specified migration source has been associated with unfinished migration tasks.
InvalidParameterValue.ParameterValueContainsIllegalCharacter	The parameter value is invalid because it contains illegal characters.
InvalidParameterValue.TooShort	The parameter value is invalid because it is too short.
InvalidParameterValue.InvalidTimeFormat	The time format is invalid.
InvalidParameterValue.TooLong	Invalid input: Excessive length of the parameter.

DeleteMigrationJob

1. Interface Description

Interface request domain name: csm.api3.convergecloud.com.

Delete migration task

Default interface request rate limit: 20 times per second.

Interface update time: 2024-11-06 20:30:21.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteMigrationJob
Version	Yes	No	String	Public parameter, The value of this interface: 2021-09-15
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
JobId	Yes	No	String	Migration job ID Example:

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
ResourceNotFound.InvalidLiveMigrateSourceServerId	The migration source ID does not exist.
FailedOperation.JobIdNotExist	The jobId does not exist.
FailedOperation.MigrateJobStatusNotSupport	The migration task status does not support this operation.
FailedOperation.SourceServerStatusNotSupport	The migration source status does not support this operation.
InvalidParameterValue.InvalidMigrateJobIdMalformed	The migration task ID is invalid. The specified migration task ID format is incorrect.

DescribeMigrationJobDeniedActions

1. Interface Description

Interface request domain name: csm.api3.convergecloud.com.

This API is used to query the list of prohibited operations for migration tasks.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-11-06 20:24:03.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeMigrationJobDeniedActions
Version	Yes	No	String	Public parameter, The value of this interface: 2021-09-15
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
JobIds	Yes	No	Array of String	Migration Task ID List Example:

3. Output Parameters

Parameter name	Type	Description
JobDeniedActionSet	Array of JobDeniedAction	List of prohibited operations for migration tasks. Example:View

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
ResourceNotFound.InvalidLiveMigrateSourceServerId	The migration source ID does not exist.
FailedOperation.JobIdNotExist	The jobId does not exist.
InvalidParameterValue.InvalidMigrateJobIdMalformed	The migration task ID is invalid. The specified migration task ID format is incorrect.

DescribeMigrationJobs

1. Interface Description

Interface request domain name: csm.api3.convergecloud.com.

This API is used to query users' lists of online migration tasks.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-11-06 20:25:24.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeMigrationJobs
Version	Yes	No	String	Public parameter, The value of this interface: 2021-09-15
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
Limit	No	No	Uint64	Number of entries per page, which is used for pagination. Value range: [1, 50]. Example:
Filters	No	No	Array of Filter	Filtering condition. Valid values: source-server-id; job-name; job-id; status; product. Example:View
Offset	No	No	Uint64	Task start count, used for pagination. Example:

3. Output Parameters

Parameter name	Type	Description
MigrationJobs	Array of MigrationJob	Migration Task List Example:View
TotalCount	Uint64	Number of migration tasks that meet conditions. Example:
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.ParameterValueContainsIllegalCharacter	The parameter value is invalid because it contains illegal characters.
InvalidParameterValue.InvalidTaskIdFormat	The task ID format is incorrect.
InvalidParameterValue.ParameterValueNotSupportValue	The parameter value is not supported.
InvalidParameterValue.InvalidSourceServerIdMalformed	The migration source ID is invalid because the specified migration source ID format is incorrect.
InvalidParameterValue.InvalidMigrateJobIdMalformed	The migration task ID is invalid. The specified migration task ID format is incorrect.

ModifyMigrationJob

1. Interface Description

Interface request domain name: csm.api3.convergecloud.com.

This API is used to modify attributes of online migration tasks.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-11-07 16:45:11.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyMigrationJob
Version	Yes	No	String	Public parameter, The value of this interface: 2021-09-15
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
JobId	Yes	No	String	Migration job ID Example:
Status	No	No	String	Migration Task Status Example:
TargetType	No	No	String	Target result type of the migration task. Valid value: 'Image','Instance'. When the value of TargetType is modified from Instance to Image, the ImageName parameter should be added. Example:
Description	No	No	String	Detailed description of the migration task, with a maximum length of 256 characters, including English, and digits. Single quotes ('), double quotes ("), semicolons (;), and backslashes () cannot be contained. Example:
InstanceId	No	No	String	Target instance ID of the migration task. Example:
SecurityGroup	No	No	String	Security group ID of the relay instance for the migration task. Example:
ImageName	No	No	String	Target image name of the migration task. The image name should comply with the custom image name specification and should be unique in the target region. If the entered image name is not unique, the migration backend will rename the image in the format of image_name_task_ID: testImageName_migrate-xxxxxxxx. If the target type is instance, the modification is invalid. Example:
StartTime	No	No	String	Start time of the migration task, in the UTC+0 time zone. Its format is YYYY-MM-DDThh:mm:ssZ, and the value should be later than or equal to the current time. If the value is null, it indicates that the task is created only and will be started by a trigger later. Example:
Progress	No	No	String	Migration Task Progress Example:
MigrateResult	No	No	MigrateResult	Migration task result message. Example:View
ImageId	No	No	String	Image ID created by the migration task. Example:
InstanceType	No	No	String	Model of the relay instance for migration. For the valid values of model specifications, see the CVM model documentation. Bare metal models are not supported currently. Example:
Name	No	No	String	Migration task name, with a length of 1–128 characters, including English, and digits. Single quotes ('), double quotes ("), semicolons (;), and backslashes () cannot be contained. Example:
TransitInstanceId	No	No	String	Relay instance ID created when the migration target is an image. Example:
IncrementalTime	No	No	String	End time of automatic incremental migration. Example:
LastMessage	No	No	String	Latest messages to be reported. Example:
LastSpeed	No	No	String	Last migration speed, in KB/s. Example:
RemainingTimeEstimate	No	No	String	Remaining time of migration, in minutes. Example:

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue.InvalidTimeFormat	The time format is invalid.
InvalidParameterValue.ParameterValueContainsIllegalCharacter	The parameter value is invalid because it contains illegal characters.
InvalidParameterValue.InvalidTaskIdFormat	The task ID format is incorrect.
InvalidParameterValue.TooLarge	The parameter value exceeds the maximum limit.
InvalidParameterValue.MigrateJobNameExist	The specified migration task name already exists.
FailedOperation.JobIdNotExist	The jobId does not exist.
FailedOperation.MigrateJobStatusNotSupport	The migration task status does not support this operation.
InvalidParameterValue.InvalidProgressNumber	The progress value is invalid.
ResourceNotFound.InvalidInstanceIdNotFound	No corresponding instance was found.
InvalidParameterValue.MigrateNotSupportInstanceType	The instance type is not supported for migration.
InvalidParameterValue.InvalidMigrateJobIdMalformed	The migration task ID is invalid. The specified migration task ID format is incorrect.
InvalidParameterValue.IncrementalTimeLessThanOneHour	The incremental migration time of the migration task is less than one hour.
InvalidParameterValue.IncrementalTimeGreaterThanSevenDays	The incremental migration time of the migration task is greater than seven days.

StartMigrationJob

1. Interface Description

Interface request domain name: csm.api3.convergecloud.com.

Start Migration Task

Default interface request rate limit: 20 times per second.

Interface update time: 2024-11-06 20:29:11.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: StartMigrationJob
Version	Yes	No	String	Public parameter, The value of this interface: 2021-09-15
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
JobId	Yes	No	String	Migration job ID Example:

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
ResourceNotFound.InvalidLiveMigrateSourceServerId	The migration source ID does not exist.
FailedOperation.JobIdNotExist	The jobId does not exist.
FailedOperation.MigrateJobStatusNotSupport	The migration task status does not support this operation.
FailedOperation.SourceServerStatusNotSupport	The migration source status does not support this operation.
InvalidParameterValue.InvalidMigrateJobIdMalformed	The migration task ID is invalid. The specified migration task ID format is incorrect.

StopMigrationJob

1. Interface Description

Interface request domain name: csm.api3.convergecloud.com.

This API is used to stop the specified migration tasks.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-11-06 20:24:23.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: StopMigrationJob
Version	Yes	No	String	Public parameter, The value of this interface: 2021-09-15
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
JobId	Yes	No	String	Migration job ID Example:

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
ResourceNotFound.InvalidLiveMigrateSourceServerId	The migration source ID does not exist.
FailedOperation.JobIdNotExist	The jobId does not exist.
FailedOperation.MigrateJobStatusNotSupport	The migration task status does not support this operation.
FailedOperation.SourceServerStatusNotSupport	The migration source status does not support this operation.
InvalidParameterValue.InvalidMigrateJobIdMalformed	The migration task ID is invalid. The specified migration task ID format is incorrect.

Data structure

SourceServerDeniedAction

List of prohibited operations for migration sources.

Referenced by the following interfaces: DescribeSourceServerDeniedActions

name	required	NULL allowed	type	description
SourceServerId	no	no	String	Migration source ID Example:
DeniedActions	no	no	Array of DeniedAction	List of prohibited operations. Example:View

OneClickMigrationJob

One-click migration task parameters.

Referenced by the following interfaces: CreateOneClickMigrationJobs

name	required	NULL allowed	type	description
SourceInstanceId	no	no	String	Source machine instance ID, with a length of 1–128 characters. Special characters such as '*', *'', '.', '', and *
OsType	no	no	String	Operating system type of the source machine. Valid values: Linux and Windows. Example:
TargetRegion	no	no	String	Target Region Example:
PrivateIp	no	no	String	Private IP address of the source machine, with a length of 7–15 characters. Special characters such as '*', *'', '.', '', and *
Uuid	no	no	String	Unique ID or serial number of the source machine, such as SerialNumber. The length is 1–128 characters, and special characters such as '*', *'', '.', '', and *
SourceInstanceName	no	no	String	Source machine instance name, with a length of 1–256 characters. Special characters such as '*', *'', '.', '', and *
PublicIp	no	no	String	Public IP address of the source machine, with a length of 7–15 characters. Special characters such as '*', *'', '.', '', and *
OsName	no	no	String	English name of the source machine system, with a length of 1–128 characters. Special characters such as '*', *'', '.', '', and *
TargetInstanceId	no	no	String	Target machine instance ID. Example:
ImageName	no	no	String	Image Name Example:
Mode	no	no	Uint64	Network mode of migration. Valid values: 0, 2, 3. Specifically, 0 indicates public network migration; 2 and 3 indicate private network migration. The default value is 0. Example:
TargetType	no	no	String	Migration target type. Valid values: Instance and Image. Example:

DeniedAction

List of prohibited operations.

Referenced by the following interfaces: DescribeMigrationJobDeniedActions, DescribeSourceServerDeniedActions

name	required	NULL allowed	type	description
Action	no	no	String	Operation name, namely, API name. Example:
Code	no	no	String	Error Code Example:
Message	no	no	String	Detailed error message. Example:

MigrateResult

Result of the online migration task.

Referenced by the following interfaces: DescribeMigrationJobs, ModifyMigrationJob

name	required	NULL allowed	type	description
State	no	no	String	Error steps for migration failures, such as File Transmission Stopped, which indicates synchronization is paused, and Failed exitLiveMigrateInstance, which indicates exiting migration failed. Up to 128 characters are supported. Example:
Result	no	no	String	Migration result, such as 'succ', 'normalFailed', and 'malformedFailed'. Up to 128 characters are supported. Example:
Desc	no	no	String	Migration task success or failure description. Up to 1,024 characters are supported. Example:

SystemDiskInfo

Information on the system disk of the source machine.

Referenced by the following interfaces: CreateMigrationJob, CreateSourceServer, CreateTransitInstance, DescribeMigrationJobs, DescribeSourceServers

name	required	NULL allowed	type	description
Device	yes	no	String	System disk device name of the source machine. Example:
MountPoint	no	no	String	Mount point of the system disk device for the source machine. Example:
Size	yes	no	Uint64	System disk size of the source machine, in GB. Example:
Partitions	no	no	Array of Partition	List of the system disk partitions for the source machine. Example:View
PartitionStyle	no	no	String	Partitioning method of the system disk for the source machine, such as 'MBR' and 'GPT'. Example:
Block	no	no	BlockMigrate	Parameters supported by block migration. Example:View

OneClickMigrationJobInfo

Creation result of the one-click migration task.

Referenced by the following interfaces: CreateOneClickMigrationJobs

name	required	NULL allowed	type	description
OneClickJobId	no	no	String	One-click migration task ID. Example:
ApiPublicKey	no	no	String	Public key, which is used to encrypt the user's Cloud API SecretId and SecretKey. Example:
Script	no	no	String	One-click migration command script. Example:
TmpSecretId	no	no	String	Temporary key ID. Example:
TmpSecretKey	no	no	String	Temporary key. Example:
Token	no	no	String	Temporary token. Example:

ClientSysInfo

Used for transmitting client system information during migration.

Referenced by the following interfaces: LiveMigrateInstance, LiveMigrateLhInstance

name	required	NULL allowed	type	description
OsType	no	no	String	Operating system Example:
OsVersion	no	no	String	Operating system version Example:

name	required	NULL allowed	type	description
DiskSize	no	no	Array of Uint64	Data Disk Information of to-be-Imported System Disk Example:
ExtraInfo	no	no	String	Additional Information Example:

TransitInstance

Relay instance for migration.

Referenced by the following interfaces: DescribeTransitInstance

name	required	NULL allowed	type	description
InstanceId	no	no	String	Instance ID Example:
SystemDisk	no	no	DiskForMigrate	Information on the instance system disk. Example:View
CPU	no	no	Uint64	Number of CPU cores for the instance, in cores. Example:
Memory	no	no	Uint64	Instance memory capacity, in GB. Example:
Uuid	no	no	String	Globally unique ID of the instance. Example:
OsType	no	no	String	Operating system platform type, such as Linux and Windows. Example:
InstanceType	no	no	String	CVM instance model. Example:
PublicIpAddresses	no	no	Array of String	Public IP address for the primary NIC of the instance. Example:
InstanceState	no	no	String	Instance status. Example:
LatestOperation	no	no	String	Latest operation on the instance, such as StopInstances and ResetInstance. Note: This field may return null, indicating that no valid values can be obtained. Example:
LatestOperationState	no	no	String	Latest operation status of the instance. Valid values: SUCCESS indicates that the operation is successful; OPERATING indicates that the operation is in progress; FAILED indicates that the operation failed. Note: This field may return null, indicating that no valid values can be obtained. Example:
LatestOperationRequestId	no	no	String	Unique request ID for the latest operation of the instance. Note: This field may return null, indicating that no valid values can be obtained. Example:

SourceSystemInfo

System information of the migration source.

Referenced by the following interfaces: ExitLiveMigrateInstance, ExitLiveMigrateLhInstance

name	required	NULL allowed	type	description
OsName	no	no	String	Source Machine System Name Example:
KernelVersion	no	no	String	System Kernel Version of Source Machine Example:
Architecture	no	no	String	System Architecture of Source Machine Example:

BlockMigrate

Parameters related to block migration.

Referenced by the following interfaces: CreateMigrationJob, CreateSourceServer, CreateTransitInstance, DescribeMigrationJobs, DescribeSourceServers

name	required	NULL allowed	type	description
Supported	no	no	Bool	Whether block migration is supported. Example:
Enabled	no	no	Bool	Whether to enable block migration. Example:

DataDiskInfo

Information on the data disk of the source machine.

Referenced by the following interfaces: CreateMigrationJob, CreateSourceServer, CreateTransitInstance, DescribeMigrationJobs, DescribeSourceServers

name	required	NULL allowed	type	description
Index	yes	no	Uint64	Data disk sequence, counting from 1. Example:
PartitionStyle	no	no	String	Data disk partitioning method, such as 'MBR' and 'GPT'. Example:
Device	yes	no	String	Data disk device name. Example:
MountPoint	no	no	String	Data disk mount point. Example:
Partitions	no	no	Array of Partition	List of the data disk partitions. Example:View
Size	yes	no	Uint64	Data disk size, in GB. Example:
Block	no	no	BlockMigrate	Supports block migration. Example:View

MigrationJob

Online migration task details.

Referenced by the following interfaces: DescribeMigrationJobs

name	required	NULL allowed	type	description
TargetType	no	no	String	Target result type of the migration task. Valid values: 'Image'; 'Instance'. Example:
SourceServerId	no	no	String	Migration source ID Example:
SecurityGroup	no	no	String	Security group ID Example:
TargetRegion	no	no	String	Target region of the migration task. Example:
Progress	no	no	Float	Migration Task Progress Example:
EndTime	no	no	String	End time of the migration task. Example:
Status	no	no	String	Migration task status. Valid values: 'PENDING' (to be started); 'RUNNING' (migrating); 'SUCCESS' (successful); 'FAILED' (failed); 'STOPPING' (stopping); 'STOPPED' (stopped); 'DELETING' (deleting); 'DELETED' (deleted). Example:
UpdateTime	no	no	String	Update time of the migration task. Example:
VpcId	no	no	String	ID of the VPC to which the relay instances for migration belong. Example:
Description	no	no	String	Description of the migration task. Example:
InstanceId	no	no	String	Target instance ID for migration. Example:
MigrationConfigInfo	no	no	MigrationConfigInfo	Configuration message during the data synchronization process. Example:View
JobId	no	no	String	Migration job ID Example:

name	required	NULL allowed	type	description
ImageId	no	no	String	Image ID Example:
SubnetId	no	no	String	ID of the subnet to which the relay instance for migration belongs. Example:
InstanceType	no	no	String	Model of the relay instance for migration. Example:
DataDisksInfo	no	no	Array of DataDiskInfo	Information on the data disk to be migrated. Example:View
Name	no	no	String	Migration job name Example:
ImageName	no	no	String	Image Name Example:
Mode	no	no	Uint64	Network mode of the migration task. Example:
SystemDiskInfo	no	no	SystemDiskInfo	System disk information for migration. Example:View
StartTime	no	no	String	Migration Task Start Time Example:
MigrateResult	no	no	MigrateResult	Migration task result. Example:View
CreateTime	no	no	String	Creation time of the migration task. Example:
TransitInstanceId	no	no	String	ID of the relay machine created when the migration target is an image. Example:
IncrementalMigration	no	no	Uint64	Whether to enable automatic incremental migration. Example:
IncrementalTime	no	no	String	End time of automatic incremental migration. Example:
MigrateResults	no	no	MigrateResults	New migration task result. Example:View
LastReportMessage	no	no	LastReportMessage	Last reported message. Example:View
OneClickJobId	no	no	String	One-click migration task ID. Example:
RunMode	no	no	String	Running Pattern Example:
RemainingTimeEstimate	no	no	String	Estimated remaining time of migration, in minutes. Example:
LastSpeed	no	no	String	Migration speed, in KB/s. Example:
ExcludePathList	no	no	String	The directory/file list needs to be filtered during migration. Example:
UserIntentList	no	no	String	Parameters for the scaling of disk partitions set by customers. Example:
Product	no	no	String	Migration product type. Valid values: ["lh", "cvm"]. Example:

Partition

Information on the disk partition of the source machine.

Referenced by the following interfaces: CreateMigrationJob, CreateSourceServer, CreateTransitInstance, DescribeMigrationJobs, DescribeSourceServers

name	required	NULL allowed	type	description
Device	yes	no	String	Partition device name. Example:
MountPoint	no	no	String	Partition mount point. Example:
Size	yes	no	Uint64	Partition size, in GB. Example:
Bootable	no	no	Bool	Whether the partition is enabled. The default value is False. Example:
FileSystem	no	no	String	Partition file system type. Example:
Block	no	no	BlockMigrate	Block migration support. Example:View

SystemInfo

Detailed information on the system of the source machine.

Referenced by the following interfaces: CreateSourceServer, DescribeSourceServers

name	required	NULL allowed	type	description
KernelVersion	no	no	String	Kernel version of the operating system for the source machine, such as '3.10.107-1-tlinux2_kvm_guest-0050'. Example:
HostName	no	no	String	Host name of the source machine, such as 'VM_78_149_centos'. Example:
OsName	no	no	String	Operating system name of the source machine, such as 'CentOS Linux release 7.2 (Final)'. Example:

DiskForMigrate

Disk information, which is used to create relay instances.

Referenced by the following interfaces: DescribeTransitInstance

name	required	NULL allowed	type	description
DiskSize	no	no	Uint64	CBS disk size, in GB. Value range: [1, 450]. Example:
DiskId	no	no	String	CBS ID. When it is used as an input parameter, this parameter is not required to be specified. Example:

MigrateDesc

Migration result description.

Referenced by the following interfaces: DescribeMigrationJobs

name	required	NULL allowed	type	description
ErrorMessage	no	no	String	Error Message Example:
ErrorId	no	no	String	Error ID. Example:

MigrateResults

Describes the online migration task result.

Referenced by the following interfaces: DescribeMigrationJobs

name	required	NULL allowed	type	description
State	no	no	String	Error steps for migration failures, such as File Transmission Stopped, which indicates synchronization is paused, and Failed exitLiveMigrateInstance, which indicates exiting migration failed. Up to 128 characters are supported. Example:
Result	no	no	String	Migration result, such as 'succ', 'normalFailed', and 'malformedFailed'. Up to 128 characters are supported. Example:
Desc	no	no	MigrateDesc	Migration task success or failure description. Example:View

ServerInfo

Detailed information on the source machine, such as configuration and network.

Referenced by the following interfaces: CreateSourceServer, DescribeSourceServers

name	required	NULL allowed	type	description
ProcessorNum	no	no	Uint64	Number of CPU cores for the source machine. Example:
Ip	no	no	String	Private IP address of the source machine. Example:
Mac	no	no	String	MAC address of the source machine. Example:
Memory	no	no	Uint64	Memory size of the machine, in GB. Example:
BootMode	no	no	String	Startup mode of the source machine, such as 'BIOS' and 'UEFI'. Example:

LastReportMessage

Last reported message.

Referenced by the following interfaces: DescribeMigrationJobs

name	required	NULL allowed	type	description
Messages	no	no	Array of String	Message List Example:

JobDeniedAction

List of prohibited operations for migration tasks.

Referenced by the following interfaces: DescribeMigrationJobDeniedActions

name	required	NULL allowed	type	description
JobId	no	no	String	Migration job ID Example:
DeniedActions	no	no	Array of DeniedAction	List of prohibited operations. Example:View

MigrationConfigInfo

Detailed information on the migration task configuration.

Referenced by the following interfaces: CreateMigrationJob, DescribeMigrationJobs

name	required	NULL allowed	type	description
Checksum	no	no	Bool	Whether strong verification is enabled for the migration task. The default value is False (not enabled). True indicates enabled. Enabling strong verification will slow down the migration speed. Example:
BandwidthLimit	no	no	String	Speed limit of the migration task, in KB/S. The default value is null, namely, there is no speed limit. Example:

Filter

Describes the key-value pair filter, which is used for conditional filtering and queries, such as filtering by ID, name, or status. If there are multiple Filters, the relationship between these Filters is logical AND. If there are multiple Values for the same Filter, the relationship between these Values is logical OR. Take the Filter of the DescribeInstances API as an example. To query an instance whose availability zone (zone) is xxx and billing mode (instance-charge-type) is yearly/monthly subscription or pay-as-you-go, implement it as follows: Filters.0.Name=zone &Filters.0.Values.0=xxx &Filters.1.Name=instance-charge-type &Filters.1.Values.0=PREPAID &Filters.1.Values.1=POSTPAID_BY_HOUR.

Referenced by the following interfaces: DescribeMigrationJobs, DescribeSourceServers

name	required	NULL allowed	type	description
Values	yes	no	Array of String	Filter Value of Field Example:
Name	yes	no	String	Field Needing To Be Filtered Example:

SourceServer

Description of the source machine information.

Referenced by the following interfaces: DescribeSourceServers

name	required	NULL allowed	type	description
Status	no	no	String	Source machine status: 'OFFLINE' (offline); 'ONLINE' (online); 'MIGRATING' (migrating); 'DELETING' (deleting); 'DELETED' (deleted). Example:
UpdateTime	no	no	String	Update time of the source machine. Example:
DataDisksInfo	no	no	Array of DataDiskInfo	Detailed information on the data disk of the source machine. Example:View
Name	no	no	String	Source machine name. Example:
ClientVersion	no	no	String	Migration tool version number, such as '2.1.3'. Example:
SystemInfo	no	no	SystemInfo	Detailed information on the system of the source machine. Example:View
SourceServerId	no	no	String	Source machine ID. Example:
ServerInfo	no	no	ServerInfo	Information related to the source machine configuration. Example:View
SystemDiskInfo	no	no	SystemDiskInfo	Detailed information on the system disk of the source machine. Example:View
Architecture	no	no	String	System architecture of the source machine, such as 'x86_64'. Example:
EndTime	no	no	String	End time of the source machine. Example:
OsType	no	no	String	Operating system type of the source machine, such as 'CentOS'. Example:
Identifier	no	no	String	Unique identifier of the migration source, with a length of 64 characters, including English letters and digits. Other characters cannot be contained. Example:
CreateTime	no	no	String	Import time of the source machine. Example:
Description	no	no	String	Detailed description of the source machine. Example:
Product	no	no	String	Migration product type. Valid values: ["lh", "cvm"]. Example:
Platform	no	no	String	Platform where the source machine is located. Example:
SessionToken	no	no	String	Session token for user migration. Example:

ErrorCode

Feature Description

If there is an Error field in the response, it means that the API call failed. For example:

```
{
    "Response": {
        "Error": {
            "Code": "AuthFailure.SignatureFailure",
            "Message": "The provided credentials could not be validated. Please check your signature is cor
rect."
        },
        "RequestId": "ed93f3cb-f35e-473f-b9f3-0d451b8b79c6"
    }
}
```

Code in Error indicates the error code, and Message indicates the specific information of the error.

Error Code List

Common Error Codes

Error codes	Description
AuthFailure.InvalidSecretId	Invalid key (not a Cloud API key type).
AuthFailure.MFAFailure	MFA failed.
AuthFailure.SecretIdNotFound	Key does not exist. Check if the key has been deleted or disabled in the console, and if not, check if the key is correctly entered. Note that whitespaces should not exist before or after the key.
AuthFailure.SignatureExpire	Signature expired. Timestamp and server time cannot differ by more than five minutes. Please ensure your current local time matches the standard time.
AuthFailure.SignatureFailure	Invalid signature. Signature calculation error. Please ensure you've followed the signature calculation process described in the Signature API documentation.
AuthFailure.TokenFailure	Token error.

Error codes	Description
AuthFailure.UnauthorizedOperation	The request does not have CAM authorization.
DryRunOperation	DryRun Operation. It means that the request would have succeeded, but the DryRun parameter was used.
FailedOperation	Operation failed.
InternalError	Internal error.
InvalidAction	The API does not exist.
InvalidParameter	Incorrect parameter.
InvalidParameterValue	Invalid parameter value.
LimitExceeded	Quota limit exceeded.
MissingParameter	A parameter is missing.
NoSuchVersion	The API version does not exist.
RequestLimitExceeded	The number of requests exceeds the frequency limit.
ResourceInUse	Resource is in use.
ResourceInsufficient	Insufficient resource.
ResourceNotFound	The resource does not exist.
ResourceUnavailable	Resource is unavailable.
UnauthorizedOperation	Unauthorized operation.
UnknownParameter	Unknown parameter.
UnsupportedOperation	Unsupported operation.
UnsupportedProtocol	HTTPS request method error. Only GET and POST requests are supported.
UnsupportedRegion	API does not support the requested region.

Service Error Codes

Error codes	Description
InvalidParameterValue.SystemDiskSizeTooLarge	The system disk is too large.

Error codes	Description
InvalidParameterValue.VersionFormatError	The version format is invalid.
InvalidParameterValue.SubnetNotExist	The specified subnet does not exist.
InvalidParameterValue.IncrementalTimeLessThanOneHour	The incremental migration time of the migration task is less than one hour.
FailedOperation.TargetInstanceRelatedUnFinishedJob	The target machine has been associated with unfinished migration tasks.
FailedOperation.MigrateJobStatusNotSupport	The migration task status does not support this operation.
InvalidParameterValue.InvalidDataDiskIndex	The data disk index is invalid because it does not exist in the specified migration source.
FailedOperation.SourceServerRelatedUnFinishedJob	The specified migration source has been associated with unfinished migration tasks.
InvalidParameterValue.DataDiskSizeTooLarge	The data disk is too large.
InvalidParameterValue.VersionLowerThanRequired	The version number is invalid because it is earlier than the required version.
InvalidParameterValue.InvalidIdentifierFormat	The uniqueness parameter is invalid.
UnsupportedOperation.InstanceStateTerminating	The request does not support instances that are being terminated.
FailedOperation.OsTypeMismatch	The operating system type does not match.
UnsupportedOperation.InstanceStateEnterServiceLiveMigrate	The instance ins-xxxxxx with the status of ENTER_SERVICE_LIVE_MIGRATE is not supported.
UnsupportedOperation.MigrateJobCreateFullCvmImage	The migration task does not support creating a full-instance image.
InvalidParameterValue.InvalidSourceServerIdMalformed	The migration source ID is invalid because the specified migration

Error codes	Description
	source ID format is incorrect.
InvalidParameterValue.TooLarge	The parameter value exceeds the maximum limit.
ResourceNotFound.InvalidLiveMigrateOnlineSourceServerId	The specified migration source is not in the online status.
ResourceNotFound.InvalidLiveMigrateSourceServerId	The migration source ID does not exist.
FailedOperation.JobIdNotExist	The jobId does not exist.
ResourceNotFound.InvalidInstanceIdNotFound	No corresponding instance was found.
UnsupportedOperation.InstanceStateRebooting	The request does not support instances that are being restarted.
UnsupportedOperation.InstanceStateRunning	The request does not support instances that are in the startup status.
InvalidParameterValue.InvalidJobId	The task ID is invalid, and the current operation cannot be performed.
LimitExceeded.MigrateJobLimitExceeded	The number of migration tasks has reached the maximum value. Contact the administrator.
InvalidParameterValue.TooLong	Invalid input: Excessive length of the parameter.
UnsupportedOperation.InstanceStateStopped	The request does not support instances that are shut down.
InvalidParameterValue.InvalidTaskIdFormat	The task ID format is incorrect.
InvalidParameterValue.VpcIdMalformed	The VPC ID xxx does not meet the requirements. Provide a standard VPC ID, such as vpc-xxxxxxxx, where the letter x represents a lowercase letter or digit.
FailedOperation.PortUnreachable	The request requires the instance to enable the specified port.

Error codes	Description
InvalidParameterValue.ParameterValueNotSupportValue	The parameter value is not supported.
InvalidParameterValue.SubnetIdMalformed	The subnet ID does not meet the requirements. Provide a standard subnet ID, such as subnet-xxxxxxxx, where the letter x represents a lowercase letter or digit.
UnsupportedOperation.InstanceStateServiceLiveMigrate	The instances under service migration are not supported. Please try again later.
InvalidParameterValue.SourceServerExist	The migration source already exists.
InvalidParameterValue.MigrateNotSupportInstanceType	The instance type is not supported for migration.
InvalidParameterValue.TooShort	The parameter value is invalid because it is too short.
InvalidParameterValue.MigrateJobNameExist	The specified migration task name already exists.
InvalidParameterValue.InvalidTimeFormat	The time format is invalid.
FailedOperation.NoAvailableIpAddressCountInSubnet	The available IPs in the subnet are exhausted.
InvalidParameterValue.InvalidRegionNotFound	The region is invalid.
InvalidParameterValue.ParameterValueContainsIllegalCharacter	The parameter value is invalid because it contains illegal characters.
InvalidParameterValue.InvalidInstanceIdMalformed	Invalid Instance ID. The format of the specified instance ID is incorrect, for example, an instance ID length error ins-1122 .
FailedOperation.SourceServerStatusNotSupport	The migration source status does not support this operation.
InvalidParameter.SourceServerExist	The source server has been registered.

Error codes	Description
InvalidParameterValue.VpcIdSubnetIdNotMatch	The specified VpcId and SubnetId do not match.
InvalidParameterValue.IncrementalTimeGreaterThanSevenDays	The incremental migration time of the migration task is greater than seven days.
InvalidParameterValue.InvalidProgressNumber	The progress value is invalid.
InvalidParameterValue.InvalidMigrateJobIdMalformed	The migration task ID is invalid. The specified migration task ID format is incorrect.
UnsupportedOperation.InstanceStateStopping	The request does not support instances that are being shut down.