Copyright Notice

©2013-2019 Tencent Cloud. All rights reserved.

Copyright in this document is exclusively owned by Tencent Cloud. You must not reproduce, modify, copy or distribute in any way, in whole or in part, the contents of this document without Tencent Cloud's the prior written consent.

Trademark Notice

All trademarks associated with Tencent Cloud and its services are owned by Tencent Cloud Computing (Beijing) Company Limited and its affiliated companies. Trademarks of third parties referred to in this document are owned by their respective proprietors.

Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud’s products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.
Contents

Operation Guide
    Operation Guide Overview
    Use Limits Overview
Instances
    Creating Instances
        Purchasing with Same Configurations
        Guidelines for Creating Instances
        Creating Instances via CVM Purchase Page
        Creating Instances via Images
Batch Sequential Naming or Pattern String-Based Naming
Resource Adjustment
    Change Instance Configuration
    Adjust Network Configuration
    Adjust Project Configuration
Query Info
    Query Instance Info
    Query Instance Monitoring Info
    Instance Metadata
Renaming Instances
Resetting Instances
Management instance IP address
    Getting Private IP Addresses and Setting DNS
    Modifying Private IP Addresses
    Getting Public IP Addresses
    Changing Public IP Addresses
    Retrieve the public network IP address
Change Instance Subnet
Change Security Group
Search Instances
Export Instances
Querying the Repossession Status of a Spot Instance
Renew Instances
Shutdown Instances
Restarting Instances
Logging into Linux Instance
Log into Linux Instance Using Standard Login Method
Logging into Linux Instance via SSH Key
Logging into Linux Instances via Remote Login Tools
Logging into Linux Instances via VNC
Logging into Windows instance
  Logging into Windows Instance via Remote Desktop
Logging in to a Windows Instance Using the RDP File (Recommended)
Logging into Windows Instance via VNC
Reinstalling System
Terminating Instances
Instance Expires
Spot Instances
No Charges When Shut down for Pay-as-You-Go Instances
Images
  Creating Custom Images
  Copying Images
  Sharing Custom Images
  Cancelling Image Sharing
  Delete Custom Images
Import Images
  Overview
    Linux System Check virtio Driver
    Installing Cloudbase-Init on Windows
    Install Cloud-Init on Linux
    Forcibly Import Image
Linux Image Creation
Windows Image Creation
Service Migration
Online Migration
  Overview
  Online Migration Tool
Tencent Cloud Migration Tutorial
  Migrating Tencent Cloud CVM Data Across Availability Zones
  Migrating Tencent Cloud CVM Data Across Accounts
Migration Tutorial for Different Source Environments
  Migrating AWS EC2 Data to Tencent Cloud
  Migrating Alibaba Cloud ECS Data to Tencent Cloud
  Migrating Huawei Cloud ECS Data to Tencent Cloud
Migrating UCloud UHost Data to Tencent Cloud
Migrating Baidu Cloud BCC Data to Tencent Cloud
Migrating VMWare Virtual Machine Data to Tencent Cloud
Migrating China Telecom e-Cloud Cloud Server Data to Tencent Cloud

Offline Migration

Contact Us

Network

ENI
Configuring a Public Gateway
Switch to VPC
Elastic IP
EIP Direct Connection

Cloud Block Storage
Expand cloud disks
Change Disk Media Type

Security

Security Groups
Creating a Security Group
Adding Security Group Rules
Associating CVM Instances with Security Groups
Managing Security Groups
Viewing Security Groups
Deleting a Security Group
Remove from Security Groups
Cloning Security Groups
Adjusting Security Group Priority
Managing Security Group Rules
Viewing Security Group Rules
Modifying Security Group Rules
Importing Security Group Rules
Exporting Security Group Rules
Delete security group policies

Security Group Use Cases
Server Common Port
Security Group API Overview
Protection of Sensitive Operations
Managing Login Password
Managing SSH keys
Spread Placement Group
Unblocking Port 25
Tags
  User guide on tags
  Edit Tags
Monitoring and Alarms
  Getting Monitoring Statistics
  Create Alarm Policies
Console Example
When using the CVM, you may perform various operations, such as logging in, reinstalling operating system, adjusting configuration and resetting password, etc. This document provides an overview of CVM instance and describes how to work with CVM-related products for your reference.

Instance

CVM Instance is also known as Cloud Virtual Machine instance. Tencent Cloud CVM instance supports customizing all resources, including CPU, memory, disk, network, security, etc. It also allows easy adjustment of the resources in case of any change in visits, load and other demands. Common features supported by CVM instance are provided as follows:

**Common operations**

- Create Instance
- Log in to an instance
- Log in to Linux Instance
- Log into Windows Instances
- Search for Instance
- Restart Instance
- Shut Down Instance
- Terminate Instance
- Reclaim Instance

**Modifying instance attributes**
• Reset Password

• Adjust configurations

  • Adjust Instance Configuration

  • Adjust Network Configuration

  • Adjust Project Configuration

• Modify Instance Name

• Modify IP

• Modify Private IP

• Modify Public IP

• Change Subnet of Instance

• Change Security Group

• Reinstall Operating System

Image

An Image provides all information required to launch a CVM instance. In another word, an image is the installation disk of a CVM. Tencent Cloud provides four types of images: public image, service marketplace image, custom image and shared image. Common operations supported by image are described as follows.

Common operations

• Create Custom Image

• Delete Custom Image

• Import Image
Security Group

Security Group is an important means of network security isolation provided by Tencent Cloud. It is a stateful virtual firewall for filtering packets and is used to set the network access controls for a single or multiple CVMs. The following describes common operations supported by security group and how to set the security group in typical scenarios to meet your business needs. Overview of common ports is provided at the end of this section for your reference.

Common operations

- Creating a security group
- Deleting a security group
- Cloning a security group
- Adding rules to security group
- Configuring a security group to associate with CVM instances
- Importing/exporting security group rules

Configuration in typical scenarios

- Remotely Log in to Linux Instance via SSH
- Logging in to a Windows Instance via MSTSC
- Ping Public IP of Instance
EIP

Elastic IP Address (EIP) is also known as elastic IP. It is a static IP designed for dynamic cloud computing, and a fixed public IP in a certain region. With EIPs, you can quickly remap an address to another instance in your account (or NAT gateway instance) to block instance failures. Common operations supported by EIP are provided as follows.

Common operations

- Applying for EIPs
- Releasing EIPs
- Binding instances
- Unbinding instances
- Adjusting bandwidth
- Converting public IPs to EIPs

SSH Key

Common operations

- Creating SSH keys
- Deleting SSH keys
- Binding/unbinding instances
• Modifying name/description

• Logging in to a Linux instance using a key
Limits on Accounts for Purchasing CVM Instances

- You need to sign up for a Tencent Cloud account. For more information on registration instructions, see Signing Up for a Tencent Cloud Account.
- You need to verify your identity. For more information, see Identity Verification Guide.
- If you create a pay-as-you-go CVM, the system will freeze the cost of one-hour CVM usage. Therefore, ensure that your account has sufficient balance for the order.

CVM Instance Use Limits

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

CVM Instance Purchase Limits

- Each user can only purchase a maximum of 30 pay-as-you-go CVM instances in each availability zone.
- For more information, see CVM Instance Purchase Limits.

Image Limits

- Public images: no use limits are applied.
- Custom images: each region supports a maximum of 10 custom images.
- Shared images: each custom image can be shared with a maximum of 50 Tencent Cloud users, and only be shared with accounts in the same region as the source account.
- For more information, see Image Types.

EIP Limits
Quota limits

<table>
<thead>
<tr>
<th>Resource</th>
<th>Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of EIPS that can be configured for each Tencent Cloud account in each region</td>
<td>20</td>
</tr>
<tr>
<td>Number of daily purchase applications for each Tencent Cloud account in each region</td>
<td>Quota * 2</td>
</tr>
<tr>
<td>Number of times that public IP addresses can be reassigned to each account for free per day when an EIP is unbound</td>
<td>10</td>
</tr>
</tbody>
</table>

Limits on public IP addresses bound to a CVM

Starting on September 18, 2019, the maximum number of public IP addresses that can be bound to a single CVM changed based on CPU configurations. The following table lists the detailed quotas.

This limit does not apply to CVM instances purchased before 00:00, September 18, 2019. For these instances, the number of public IP addresses that can be bound to each instance is equal to the number of private IP addresses supported by your server.

<table>
<thead>
<tr>
<th>Number of CPUs on a CVM</th>
<th>Maximum Number of Public IP Addresses That Can Be Bound (Including Common and Elastic Public IP Addresses)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1–5</td>
<td>2</td>
</tr>
<tr>
<td>6–11</td>
<td>3</td>
</tr>
<tr>
<td>12–17</td>
<td>4</td>
</tr>
<tr>
<td>18–23</td>
<td>5</td>
</tr>
<tr>
<td>24–29</td>
<td>6</td>
</tr>
<tr>
<td>30–35</td>
<td>7</td>
</tr>
<tr>
<td>36–41</td>
<td>8</td>
</tr>
<tr>
<td>42–47</td>
<td>9</td>
</tr>
<tr>
<td>≥ 48</td>
<td>10</td>
</tr>
</tbody>
</table>

ENI Limits
Based on CPU and memory configurations, the number of ENIs that can be bound to a CVM and the number of private IP addresses that can be bound to an ENI differ greatly. The following table lists the limits.

The number of IP addresses bound to a single ENI indicates the maximum number of IP addresses that can be bound to an ENI. The EIP quota is provided not based on this upper limit but based on EIP use limits.

<table>
<thead>
<tr>
<th>CVM Configuration</th>
<th>Number of ENIs</th>
<th>Number of Private IP Addresses Bound to a Single ENI</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU: 1 core Memory: 1 GB</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>CPU: 1 core Memory: &gt; 1 GB</td>
<td>2</td>
<td>6</td>
</tr>
<tr>
<td>CPU: 2 cores</td>
<td>2</td>
<td>10</td>
</tr>
<tr>
<td>CPU: 4 cores Memory: &lt; 16 GB</td>
<td>4</td>
<td>10</td>
</tr>
<tr>
<td>CPU: 4 cores Memory: &gt; 16 GB</td>
<td>4</td>
<td>20</td>
</tr>
<tr>
<td>CPU: 8–12 cores</td>
<td>6</td>
<td>20</td>
</tr>
<tr>
<td>CPU: &gt; 12 cores</td>
<td>8</td>
<td>30</td>
</tr>
</tbody>
</table>

**Bandwidth Limits**

- Maximum outbound bandwidth (downstream bandwidth)

  - The following table describes rules for CVMs created before 00:00, February 24, 2020.

<table>
<thead>
<tr>
<th>Network Billing Method</th>
<th>Instance Billing Method</th>
<th>Instance Configuration</th>
<th>Maximum Bandwidth Range (Mbps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bill-by-traffic</td>
<td>Pay-as-you-go instances</td>
<td>All</td>
<td>0–100</td>
</tr>
</tbody>
</table>
The following table describes rules for CVMs created after 00:00, February 24, 2020.

<table>
<thead>
<tr>
<th>Network Billing Method</th>
<th>Instance Billing Method</th>
<th>Instance Configuration</th>
<th>Maximum Bandwidth Range (Mbps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bill-by-traffic</td>
<td>Pay-as-you-go instances</td>
<td>All</td>
<td>0–100</td>
</tr>
<tr>
<td>Bill-by-bandwidth</td>
<td>Pay-as-you-go instances</td>
<td>ALL</td>
<td>0–100</td>
</tr>
<tr>
<td>Bandwidth package</td>
<td>All</td>
<td></td>
<td>0–2000</td>
</tr>
</tbody>
</table>

- Maximum inbound bandwidth (upstream bandwidth)
  - If the fixed bandwidth that you purchased is greater than 10 Mbps, Tencent Cloud assigns a public network inbound bandwidth that is equal to the purchased bandwidth.
  - If the fixed bandwidth that you purchased is less than 10 Mbps, Tencent Cloud assigns 10-Mbps public network inbound bandwidth.

### Disk Limits

<table>
<thead>
<tr>
<th>Limit Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Elastic cloud disk capability</td>
<td>Starting from May 2018, all data disks purchased with CVMs are CBS cloud disks. They can be unmounted from and then remounted to CVMs. This feature is supported in all availability zones.</td>
</tr>
<tr>
<td>CBS cloud disk performance</td>
<td>I/O performance takes effect concurrently. For example, if a 1-TB SSD has a maximum random IOPS of 26,000, both the read and write IOPS values can reach the maximum value. Due to multiple performance limits, if the block size in this example is 4 KB or 8 KB, the maximum IOPS can be reached. If the block size is 16 KB, the maximum IOPS</td>
</tr>
</tbody>
</table>

©2013-2019 Tencent Cloud. All rights reserved.
**cannot be reached (because throughput has already reached the limit of 260 MB/s.)**

<table>
<thead>
<tr>
<th>Table Title</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of elastic cloud disks that can be mounted to a CVM</td>
<td>A maximum of 20</td>
</tr>
<tr>
<td>Number of snapshots in one region</td>
<td>64 + Number of CBS cloud disks in the region x 64</td>
</tr>
<tr>
<td>Mounting CBS cloud disks to a CVM</td>
<td>The CVM and CBS cloud disks must be in the same availability zone.</td>
</tr>
<tr>
<td>Snapshot rollback</td>
<td>Snapshot data can be rolled back only to the CBS cloud disk where the snapshot was created.</td>
</tr>
<tr>
<td>Type of cloud disks that can be created by using snapshots</td>
<td>Only snapshots of data disks can be used to create elastic cloud disks.</td>
</tr>
<tr>
<td>Size of cloud disks created by using snapshots</td>
<td>The size of CBS cloud disks created by using snapshots must be larger than or equal to that of source CBS cloud disks.</td>
</tr>
</tbody>
</table>

**Security Group Limits**

- Security groups are region-specific. A CVM can be bound only to security groups in the same region.
- Security groups apply to CVM instances in any network environment.
- Each user can create a maximum of 50 security groups for each project in a region.
- A maximum of 100 inbound or outbound rules can be set for a security group.
• One CVM can have multiple security groups, and one security group can be associated with multiple CVMs.

• Security groups associated with CVMs on the basic network cannot filter packets from or to TencentDB and the elastic cache (Redis or Memcached) on Tencent Cloud. Instead, you can use iptables to filter traffic for such instances.

• The following table describes related quota limits.

<table>
<thead>
<tr>
<th>Item</th>
<th>Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of security groups</td>
<td>50 per region</td>
</tr>
<tr>
<td>Number of rules in a security group</td>
<td>100 for inbound rules and 100 for outbound rules</td>
</tr>
<tr>
<td>Number of CVM instances associated with a security group</td>
<td>2,000</td>
</tr>
<tr>
<td>Number of security groups associated with a CVM instance</td>
<td>5</td>
</tr>
<tr>
<td>Number of rules in each security group that reference the security group ID</td>
<td>10</td>
</tr>
</tbody>
</table>

### VPC Limits

<table>
<thead>
<tr>
<th>Resource</th>
<th>Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of VPC instances per region for each account</td>
<td>5</td>
</tr>
<tr>
<td>Number of subnets per VPC</td>
<td>10</td>
</tr>
<tr>
<td>Number of basic network CVMs that can be associated with each VPC instance</td>
<td>100</td>
</tr>
<tr>
<td>Number of route tables per VPC</td>
<td>10</td>
</tr>
<tr>
<td>Number of route tables associated with each subnet</td>
<td>1</td>
</tr>
<tr>
<td>Number of routing policies per route table</td>
<td>100</td>
</tr>
<tr>
<td>Number of default HAVIPs per VPC</td>
<td>10</td>
</tr>
</tbody>
</table>
Overview

This document guides you through how to create a Tencent Cloud Virtual Machine (CVM) instance using the custom configuration mode as an example.

Prerequisites

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

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

Directions

1. Log in to **Tencent Cloud**. Choose **Products** -> **Compute** -> **Cloud Virtual Machine**. Click **Get Started** to access the CVM purchase page.
   
   - **Custom Configuration**: This mode is suitable for specific use cases. It allows users to purchase a CVM instance that meets their specific requirements.

2. Configure the following information as prompted by the page:

<table>
<thead>
<tr>
<th>Category</th>
<th>Required/Optional</th>
<th>Configuration Description</th>
</tr>
</thead>
</table>

---

©2013-2019 Tencent Cloud. All rights reserved.
<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
</table>
| Billing Mode                | Please select based on your actual needs:  
  - **Pay as you go**: an elastic billing mode for the CVM.  
  For more information on billing modes, see [Billing Modes](#). |
| Region/Availability Zone    |  
  - **Region**: we recommend you select the region closest to your customers to reduce access latency and increase access speed.  
  - **Availability zone**: please select based on your actual needs.  
  If you want to purchase multiple CVMs, we recommend you select different availability zones to implement disaster recovery.  
  For more information on regions and availability zones, see [Regions and Availability Zones](#). |
| Network                     | A logically isolated network space built in Tencent Cloud. A virtual private cloud (VPC) includes at least one subnet. The system provides a default VPC and subnet for each region.  
  If the existing VPC or subnet does not meet your requirements, you can create a VPC or subnet on the VPC Console.  
  **Note**:  
  - resources in the same VPC can be shared within the private network.  
  - When purchasing the CVM, ensure that the CVM and the subnet where the CVM is created have the same availability zones. |
| Instance                    | Tencent Cloud provides different instance types based on the underlying hardware. For optimal performance, we recommend you use instance types of the latest generation.  
  For more information on instances, see [Instance Types](#). |
| Image                       | Tencent Cloud provides public images, custom images, and shared images. For more information on images, see [Image Types Overview](#). |
| System Disk                 | Used to install the operating system. Its default capacity is 50 GB.  
  Available Cloud Block Storage (CBS) types vary with regions. Please select a value as instructed. |
<table>
<thead>
<tr>
<th>Data Disk</th>
<th>Optional</th>
<th>Used to scale up the storage capacity of the CVM to ensure high efficiency and reliability. CBS data disks are not added by default. For more information on CBS, see <a href="#">CBS Types</a>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public Network Bandwidth</td>
<td>Required</td>
<td>A free independent public IP address is allocated by default. Tencent Cloud provides two network billing modes. Configure a value greater than 0 Mbps as needed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>Bill-by-bandwidth</strong>: select a fixed bandwidth. Packet loss will occur when the bandwidth exceeds this value. This is applicable to scenarios where the network connection fluctuates slightly.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>Bill-by-traffic</strong>: billing is based on traffic that is actually used. You can specify a peak bandwidth to prevent charges incurred by unexpected traffic. Packet loss will occur when the instantaneous bandwidth exceeds this value. This is applicable to scenarios where the network connection fluctuates significantly.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong>: the allocated free independent public IP cannot be unbound from the instance. To unbind this IP address, first convert the public IP to an elastic IP. For more information on elastic IP, see <a href="#">Elastic Public IP (EIP)</a>.</td>
</tr>
<tr>
<td>Public Gateway</td>
<td>Optional</td>
<td>Applicable only to Linux images. As a network interface between the VPC and the public network, the public gateway can forward requests of CVMs that are within different subnets of the VPC and have no public IP addresses.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong>: Tencent Cloud discontinued configuring the public gateway on the CVM purchase page after December 6, 2019. To configure the public gateway, see <a href="#">Configuring a Public Gateway</a>.</td>
</tr>
<tr>
<td>Quantity</td>
<td>Required</td>
<td>Number of CVMs to be purchased.</td>
</tr>
</tbody>
</table>

3. Click **Next: Complete Configuration** to access the CVM configuration page.

4. Configure the following information as prompted by the page:

<table>
<thead>
<tr>
<th>Category</th>
<th>Required/Optional</th>
<th>Configuration Description</th>
</tr>
</thead>
</table>

©2013-2019 Tencent Cloud. All rights reserved.
<table>
<thead>
<tr>
<th></th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Project</strong></td>
<td>Required</td>
<td>The default project is selected. You can select an existing project as needed to manage different CVMs.</td>
</tr>
</tbody>
</table>
| **Security Group**   | Required | - If there is no available security group, you can choose **Create a Security Group**.  
  - If there are available security groups, you can choose **Existing Security Groups**.  
  For more information on security groups, see Security Groups. |
| **Instance Name**    | Optional | You can customize the name of the CVM to be created.  
  - If no instance name is specified, **unnamed** will be used by default.  
  - An instance name cannot be longer than 60 characters. Batch Sequential Naming or Pattern String-Based Naming is also supported.  
  **Note**: this name is displayed only on the Console. It is not the hostname of the CVM. |
| **Login Method**     | Required | Configure the method to log in to the CVM as needed.  
  - **Custom Password**: customize the password for logging in to the instance.  
  - **SSH Key Pair (only for Linux instances)**: associate the instance with an SSH key to ensure secure login to the CVM.  
    If no key is available or existing keys are inappropriate, click **Create Now** to create a key. For more information on SSH keys, see SSH Keys.  
  - **Random Password**: an automatically generated password will be sent through the Message Center. |
| **Security Service** | Optional | By default, DDoS protection and host security are enabled for free to help you build a CVM security system to prevent data leakage. |
| **Cloud Monitoring** | Optional | By default, cloud monitoring is enabled for free. You can install components to obtain CVM monitoring metrics and display them in visual charts. You can also specify custom alarm thresholds. In addition, you can configure three-dimensional CVM data monitoring, intelligent data analysis, real-time fault alarms, and custom data reports to precisely monitor |
the health conditions of Tencent Cloud services and CVM.

Configure additional settings for the instance as needed.
- **Hostname**: you can customize the name of the computer in the CVM operating system. After a CVM is created, you can log in to the CVM to view the hostname.
- **Placement Group**: you can add an instance to a placement group as needed to improve service availability. For more information, see Placement Group.
- **Tag**: you can specify a tag to manage CVM resources by category. For more information, see User Guide on Tags.
- **Custom Data**: you can configure an instance by specifying custom data, and the configured scripts will run when an instance is launched. If multiple CVMs are purchased together, the custom data will run on all CVMs. The Linux operating system supports the Shell format while the Windows operating system supports the PowerShell format. A maximum of 16 KB of raw data is supported. For details, see Configuring Custom Data (Linux CVM).

**Note**: custom data configuration only supports certain common images with the Cloud-init service. For more information, see Cloud-Init & Cloudbase-Init.

5. Click **Next: Confirm Configuration** to access the configuration information confirmation page.
6. Validate the information of the CVM to be purchased and the cost details of each configuration item.
7. Click **Purchase** and complete the payment. Then, you can log in to the CVM Console to see your CVM.

Information such as the instance name, public IP address, private IP address, login username, and initial login password of the CVM will be sent to your account through the Message Center. You can use this information to log in to and manage your instances. To ensure the security of your CVM, please change your CVM login password as soon as possible.
This document introduces several methods of creating CVM instances, from basic operations to advanced custom features.

- Creating CVM instances via the CVM purchase page is the most commonly used method. It allows you to flexibly select the configurations that meet your business requirements. For more information, see \textit{Creating Instances via CVM Purchase Page}.
- If you want to use a particular operating system, application, or other configuration that you are familiar with, you can first create a custom image and select it when creating an instance to increase efficiency. For more information, see \textit{Creating Instances via Images}.
- If you want to purchase an instance with the same configurations as those of the current instance, you can directly create an instance with the same configurations. For more information, see \textit{Purchasing with Same Configurations}.
Creating Instances via CVM Purchase Page

Overview

If you want to purchase again an instance with the same configurations, you can use the Purchase with same configurations feature on the CVM Console to save time and improve scale-out efficiency.

Directions

1. Log in to the CVM Console.

2. Select a region at the top of the Instances page.

3. Under the Operation column of the instance, click More -> Purchase with same configurations.

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

5. Click Purchase and complete the payment.
Creating Instances via Images

Overview

You can use a custom image to create CVM instances of the same operating system, applications, and data to improve efficiency. This document guides you through how to create an instance using a custom image.

Prerequisites

You must have a custom image under your account and in the region where you want to create an instance.

If there is no custom image, see the following solutions:

<table>
<thead>
<tr>
<th>Image Status</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Images on local computers or other platforms</td>
<td>Import the system disk image on local computers or other platforms to the custom image on CVM. For more information, see Overview.</td>
</tr>
<tr>
<td>There are template instances but no custom images</td>
<td>For more information, see Creating Custom Images.</td>
</tr>
<tr>
<td>Custom images in other regions</td>
<td>Copy the custom image to the target region where you want to create an instance. For more information, see Copying Images.</td>
</tr>
<tr>
<td>Custom images under another account</td>
<td>Share the custom image with the account under which you want to create an instance. For more information, see Sharing Custom Images.</td>
</tr>
</tbody>
</table>

Directions

1. Log in to the CVM Console.
2. Click Images on the left sidebar to access the Image page.
3. Select a region at the top of the Image page.
4. Select a tab based on the image source to view its image list.
- **Public Image**: go to the public image page.
- **Custom Image**: go to the custom image page.
- **Shared Image**: go to the shared image page.

5. Under the **Operation** column of the image you want to use, click **Create Instance**.

6. In the pop-up window, click **OK**.

7. Configure and create the instance as prompted by the page.
   
   The **Region** and **Image** fields are automatically filled. Complete the other configurations of the instance as needed. For more information, see **Creating Instances via CVM Purchase Page**.

If you use a custom image that contains one or more data disk snapshots, the operating system will automatically create the same quantity of Cloud Block Storage (CBS) as snapshots and the same capacity as each snapshot. You can expand, but cannot reduce, the CBS capacity.

**Related Documentation**

You can also create a custom image using the RunInstances API. For more information, see **RunInstances**
Batch Sequential Naming or Pattern String-Based Naming

Scenario

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

- When you need to purchase $n$ instances and generate instance names in specific forms, such as “CVM+Sequence number” (for example, CVM 1, CVM 2, and CVM 3), you can use the feature of Automatically Ascending Suffixed Numbers.
- When you need to create $n$ instances and name specific instances with ascending numbers starting from $x$, you can use the feature of Specifying a Single Pattern String.
- When you need to create $n$ instances with multiple prefixes in their names, each of which contains a specified serial number, you can use the feature of Specifying Multiple Pattern Strings.

Steps

Automatically Ascending Suffixed Numbers

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

Created instances are suffixed with numbers starting from 1 by default. The starting suffix number is fixed.

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

Operations on the Purchase Page

1. Purchase three instances by referring to Create an Instance. On the Security Group and CVM tab page, enter the instance name in the form of Prefix+Sequence number. In this case, enter
2. Follow the prompts on the page and complete payment.
3. Return to the CVM Console to view the newly purchased instances. You can see that these batch purchased instances are named with the same prefix and ascending suffixed numbers.

**API Operations**

In the RunInstances API, set the InstanceName field to `CVM`.

**Specifying Pattern Strings**

This feature allows you to name batch purchased instances in a complex form with specified serial numbers. You can use one or more pattern strings in instance names as required.
The instance name with a specified pattern string is in the form of \( \{R:x\} \), where \( x \) indicates the starting number in generated instance names.

**Specifying a Single Pattern String**

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

**Operations on the Purchase Page**

1. Purchase three instances by referring to Create an Instance. On the 2. Set the CVM tab page, enter the instance name in the form of Prefix+Specified pattern string \( \{R:x\} \). In this case, enter \( \text{CVM}\{R:3\} \) as the instance name.

2. Follow the prompts on the page and complete payment.
3. Return to the CVM Console to view the newly purchased instances. You can see that these batch purchased instances are named with the same prefix and ascending suffixed numbers starting
API Operations

In the RunInstances API, set the InstanceName field to `CVM(R:3)`.

Specifying Multiple Pattern Strings

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

Operations on the Purchase Page

1. Purchase three instances by referring to Create an Instance. On the 2. Set the CVM tab page, enter the instance name in the form of `Prefix+specified pattern string {R:x}-Prefix+specified pattern string {R:x}-Prefix`. In this case, enter `cvm{R:13}-Big{R:2}-test` as
2. Follow the prompts on the page and complete payment.
3. Return to the CVM Console to view the newly purchased instances. You can see that these batch purchased instances are named with prefixes followed by ascending numbers starting from the specified numbers.

API Operations

In the RunInstances API, set the InstanceName field to `cvm(R:13)-Big(R:2)-test`.
Resource Adjustment
Change Instance Configuration

Scenario

Hardware devices of Tencent Cloud CVM instances can be adjusted quickly and conveniently. This document describes the methods and precautions for configuration upgrade, downgrade, and cross-model adjustment.

Prerequisites

You can adjust an instance's configuration when the instance is either started or shut down.

- When the instance is **shut down**, you can directly adjust its configuration in the console.
- When the instance is **started**, you can adjust the configuration online and confirm the forced shutdown of the instance. The adjusted configuration takes effect after the instance is restarted.
- You can adjust configurations **in batches** online for multiple instances. If an instance in the batch of instances is **started**, you need to confirm forced shutdown for the instance. The adjusted configuration takes effects after the instance is restarted.

Limits and Impacts

**Configuration adjustment limits**

Only the configurations of instances *whose system and data disks are both CBS cloud disks* can be adjusted.

- Upgrading the configuration:
  The number of configuration upgrades is not limited. The upgraded configuration takes effect immediately.
- Downgrading the configuration:
  The configurations of pay-as-you-go instances can be downgraded at any time an unlimited
number of times.

- Adjustment across instance families: configurations can be adjusted between different instance families without the need of data migration.

During configuration adjustment, target instance types depend on the instance types provided in the current availability zone. Pay attention to the following limits:

- **Spot instances** do not support cross-model configuration adjustment.
- **Exclusive instances** do not support cross-model configuration adjustment. The configuration adjustment scope is limited to the remaining resources of the dedicated host where the instance is located.
- **Heterogeneous instances, such as GPU and FPGA instances**, cannot be used as the source or destination instance type for configuration adjustment across instance families.
- **Instances configured with a basic network** cannot be adjusted to instances that only support VPC instances.
- If the target instance type does not support the CBS type configured for the current instance type, the configuration cannot be adjusted.
- If the target instance type does not support the image type configured for the current instance type, the configuration cannot be adjusted.
- If the target instance type does not support the ENI or ENI quantity configured for the current instance type, the configuration cannot be adjusted. For more information, see [Use Limits](#).
- If the target instance type does not support the public network bandwidth upper limit configured for the current instance type, the configuration cannot be adjusted. For more information, see the [Public Network Bandwidth Cap](#).

**Impacts**

The private IP address of an instance may be changed after configuration adjustment. If the private IP address of an instance is changed after configuration adjustment, a prompt appears on the configuration adjustment page. If no prompt appears, the private IP address is not changed.

**Directions**

- If your business changes, you can adjust configurations.
- During configuration upgrade, upgrade the configuration and pay any fees involved.
- During configuration downgrade, confirm the refund details and forcibly shut down and restart your CVM instance for the new configuration to take effect. Then, the CVM instance runs based on the new configuration.
Configuration adjustment in the console

Adjusting the configuration of a single instance

1. Log in to the CVM console and click **Instances** to view the CVM instance list.
2. Locate the target instance and choose **More > Resource Adjustment > Adjust Configuration** in the **Action** column on the right, as shown in the following figure:

![Instance List](image)

3. In the "Select target configuration" step, confirm the instance status and operation, **select the required model and instance type, confirm the type and performance parameters**, and
click **Next**, as shown in the following figure:

4. Based on the instance billing method, confirm the fees and click **Next**.
   - Pay-as-you-go instances: confirm the amount to be frozen for the new instance type. After the configuration is adjusted, pay-as-you-go instances are charged starting from the tier-1 price.
   - Confirm the billing rules before configuration adjustment, as shown in the following figure:

5. In the "Shutdown CVM" step, carefully read the prompt for different instance running states.
   - If the current instance is running, carefully read the prompt and select "Agree to a forced shutdown", as shown in the following figure:
If the current instance is shut down, the following prompt appears:

6. Click **Adjust Now** to go to the order page and pay for the order.

**Configuration adjustment through APIs**

You can use the ResetInstancesType API to adjust the instance configuration. For more information, see the [ResetInstancesType API document](#).
Adjust Network Configuration

Last updated: 2020-05-08 14:53:29

Changing the Billing Method

Tencent Cloud provides multiple network billing methods. You can switch the billing method between Bill-by-bandwidth and Bill-by-traffic in the console. For each CVM instance, however, you can switch between both billing methods twice at most.

For more information on billing, see Public Network Billing Methods.

Changing the Public Network Type

Tencent Cloud provides two types of network configurations: dedicated public network and shared public network. The shared public network service is billed by bandwidth. To activate this service, you need to submit a ticket. For more information on billing methods, see Billing of Shared Public Network. This document describes the billing methods of a single CVM instance. For more information, see Public Network Billing Methods.

Bill-by-bandwidth for pay-as-you-go CVM instances

This billing method supports adjustment (increase or decrease) of the network bandwidth at any time. If you have changed the network bandwidth more than once within an hour, you are billed based on the maximum bandwidth.

Bill-by-traffic

This billing method supports the adjustment (increase or decrease) of the bandwidth cap at any time, and the change takes effect immediately.

The Bill-by-traffic billing method is also applicable to pay-as-you-go CVM instances.

Bandwidth cap

The bandwidth cap varies with the billing methods and CVM configurations. For more information, see Public Network Bandwidth Cap.
Directions

1. Log in to the CVM Console.
2. In the instance list, select the target instance, and choose More > Resource Adjustment > Adjust Network.
3. In the Adjust Network window that appears, set the target bandwidth cap or change the billing method, and then click OK.
Adjust Project Configuration

Last updated: 2020-05-08 12:55:34

Introduction

Project is a Tencent Cloud feature used to manage cloud resources. When you create a CVM instance, you must assign it to a project. You can change the instance project afterwards if you want to.

You need to create at least one project before you can assign an instance to a project. For more information on how to create a project, refer to New Project.

Directions

1. Log in to the CVM Console.

2. In the instance list, select the desired CVM instance and click More -> Instance Settings -> Assign to Project, as shown below:

   If you need to reassign multiple CVM instances to a new project, select them and click More -> Instance Settings -> Assign to Project on the top of the interface.

3. In the displayed “Assign to Project” window, select the name of the new project, and click Submit to complete the process.
Query Info

Query Instance Info

Last updated : 2020-05-09 17:04:17

Operation Scenario

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

- View the total number of CVM instances under your account and their status, as well as the quantity and quota of resources in each region on the Overview page of the CVM Console.
- View the information of all CVM instances in a region on the Instances page on the CVM Console.
- View the details of a CVM instance on the instance details page.

Prerequisites

Log in to the CVM Console.

Directions

Viewing the CVM instance list

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

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

You can click 🌟 in the upper right corner to configure in the pop-up “Display Settings” window the
details you want to display, as shown below:

![Display Settings](image)

**Viewing instance details**

1. Go to the **Instances** page to select the region, as shown below:
2. Find the instance for which you want to view its details, and click the instance ID or name to enter the details page, as shown below:

On the instance details page, you can view information such as CVM information, architecture, network information, specifications, image information, billing information, ENI, monitoring, security groups, operation logs, and more.
Query Instance Monitoring Info


Scenario

Tencent Cloud provides two options for viewing the monitoring information of a CVM instance:

- Cloud Monitor console
- **Instance Details** page in the CVM console

To view monitoring information for public network traffic, go to **Traffic Monitor**.

Directions

**Viewing instance monitoring information in the Cloud Monitor console**

1. Log in to the Cloud Monitor console of the **CVM**.
2. Select the region where the instance whose monitoring information is to be viewed is located, as shown in the following figure.

3. Click the instance ID to go to the **Monitoring** page. On this page, you can view the CPU, memory, private network bandwidth, public network bandwidth, and disk utilization metrics of the CVM, as
shown in the following figure.

![Monitoring Page](image)

Viewing instance monitoring information in the CVM console

1. Log in to the CVM console.
2. Select the region where the instance whose monitoring information is to be viewed is located.
3. Click the instance ID to go to the Instance Details page.
4. Click the Monitoring tab to open the Monitoring page. On this page, you can view the CPU, memory, private network bandwidth, public network bandwidth, and disk utilization metrics of the
CVM, as shown in the following figure.
Instance Metadata

Last updated: 2020-05-08 11:28:33

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

Although instance metadata can only be accessed internally from the instance, their values have not been encrypted. Anyone who has access to the instance can view its metadata. Therefore, you should take proper precautions to protect sensitive data (for example, using a permanent encryption key).

Overview

Tencent Cloud provides the following metadata:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>instance-id</td>
<td>Instance ID</td>
<td>1.0</td>
</tr>
<tr>
<td>instance-name</td>
<td>Instance name</td>
<td>1.0</td>
</tr>
<tr>
<td>uuid</td>
<td>Instance ID</td>
<td>1.0</td>
</tr>
<tr>
<td>local-ipv4</td>
<td>Instance private IP address</td>
<td>1.0</td>
</tr>
<tr>
<td>public-ipv4</td>
<td>Instance public IP address</td>
<td>1.0</td>
</tr>
<tr>
<td>mac</td>
<td>MAC address of the instance's eth0 device</td>
<td>1.0</td>
</tr>
<tr>
<td>placement/region</td>
<td>Instance region information</td>
<td>Updated on 09/19/2017</td>
</tr>
<tr>
<td>placement/zone</td>
<td>Instance availability zone information</td>
<td>Updated on 09/19/2017</td>
</tr>
<tr>
<td>network/interfaces/macs/${mac}/mac</td>
<td>Instance network interface mac address</td>
<td>1.0</td>
</tr>
<tr>
<td>network/interfaces/macs/${mac}/primary-local-ipv4</td>
<td>Instance network interface primary private IP</td>
<td>1.0</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Version</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
<td>---------</td>
</tr>
<tr>
<td><code>network/interfaces/mac/$mac/public-ipv4s</code></td>
<td>Instance network interface public IP address</td>
<td>1.0</td>
</tr>
<tr>
<td><code>network/interfaces/mac/$mac/vpc-id</code></td>
<td>Instance network interface VPC ID</td>
<td>Updated on 09/19/2017</td>
</tr>
<tr>
<td><code>network/interfaces/mac/$mac/subnet-id</code></td>
<td>Instance network interface subnet ID</td>
<td>Updated on 09/19/2017</td>
</tr>
<tr>
<td><code>network/interfaces/mac/$mac/local-ipv4s/$local-ipv4/gateway</code></td>
<td>Instance network interface gateway address</td>
<td>1.0</td>
</tr>
<tr>
<td><code>network/interfaces/mac/$mac/local-ipv4s/$local-ipv4/local-ipv4</code></td>
<td>Instance network interface private IP address</td>
<td>1.0</td>
</tr>
<tr>
<td><code>network/interfaces/mac/$mac/local-ipv4s/$local-ipv4/public-ipv4</code></td>
<td>Instance network interface public IP address</td>
<td>1.0</td>
</tr>
<tr>
<td><code>network/interfaces/mac/$mac/local-ipv4s/$local-ipv4/public-ipv4-mode</code></td>
<td>Instance network interface public network mode</td>
<td>1.0</td>
</tr>
<tr>
<td><code>network/interfaces/mac/$mac/local-ipv4s/$local-ipv4/subnet-mask</code></td>
<td>Instance network interface subnet mask</td>
<td>1.0</td>
</tr>
<tr>
<td><code>payment/charge-type</code></td>
<td>Instance billing plan</td>
<td>Updated on 09/19/2017</td>
</tr>
<tr>
<td><code>payment/create-time</code></td>
<td>Instance creation time</td>
<td>Updated on 09/19/2017</td>
</tr>
<tr>
<td><code>payment/termination-time</code></td>
<td>Instance termination time</td>
<td>Updated on 09/19/2017</td>
</tr>
<tr>
<td><code>app-id</code></td>
<td>AppId of the user to which the instance belong</td>
<td>Updated on 09/19/2017</td>
</tr>
<tr>
<td><code>as-group-id</code></td>
<td>Auto scaling group ID of the instance</td>
<td>Updated on 09/19/2017</td>
</tr>
<tr>
<td><code>spot/termination-time</code></td>
<td>Spot instance termination time</td>
<td>Updated on 09/19/2017</td>
</tr>
<tr>
<td><code>/meta-data/instance/instance-type</code></td>
<td>Instance model</td>
<td>Updated on 09/19/2017</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Version</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>/instance/image-id</td>
<td>Instance image ID</td>
<td>Updated on 09/19/2017</td>
</tr>
<tr>
<td>/instance/security-group</td>
<td>Information of the security groups bound to the instance</td>
<td>Updated on 09/19/2017</td>
</tr>
</tbody>
</table>

${mac}$ and ${local-ipv4}$ in the above table indicate the mac address and private IP address of the specified network interface, respectively.

The destination URL address of the request is case-sensitive. You must construct the destination URL address of a new request according to the returned result of the request.

The returned data of placement is changed in the new version. To use the data in the previous version, specify the previous version path or leave the version path empty to access the data of version 1.0. For more information on the returned data of placement, see Region and Availability Zone.

### Querying Instance Metadata

You can access the instance metadata such as instance's local IP address and public IP address within an instance to manage connections with external applications.

To view all the instance metadata within a running instance, use the following URI:

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

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

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

- For resources that do not exist, the HTTP error code "404 - Not Found" is returned.
- Operations on the instance metadata can only be performed **internally within the instance**.
  You first need to log in to the instance. For more information, see Log in to Windows Instance and Log in to Linux Instance.

### Sample metadata query

The following shows how to query the metadata version.
When Tencent Cloud modifies the metadata access path or returned data, a new metadata version is released. If your application or script relies on the structure or returned data of a previous version, you can specify that version. If no version is specified, version 1.0 is used by default.

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

The following shows how to view the metadata root directory. The lines ending with `/` represent directories and the ones that do not represent the accessed data. For the description of accessed data, refer to **Overview**.

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

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

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

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

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

```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/local-ipv4
10.104.13.59
```
The following shows how to obtain the public IP address of an instance.

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

The following shows how to obtain an instance ID. The instance ID is used to uniquely identify an instance.

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

The following shows how to query the instance UUID. The instance UUID can also be used as the unique identifier of an instance, but it is recommended that you use instance IDs to identify instances.

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

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

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

The following example shows how to obtain the ENI information of an instance. In case of multiple ENIs, multiple lines of data are returned, with each line indicating the data directory of an ENI.

```
52:54:00:BF:B3:51/
```

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

```
4:00:BF:B3:51/
local-ipv4s/
mac
vpc-id
subnet-id
owner-id
primary-local-ipv4
public-ipv4s
local-ipv4s/
```

The following shows how to obtain the VPC information of the specified ENI.
The following shows how to obtain a list of private IP addresses bound to the specified ENI. If the ENI is bound with multiple private IP addresses, multiple lines of data are returned.

```
vpc-ja82n9op

subnet-ja82n9op
```

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

```
```

The following example shows how to obtain the gateway of a private IP address. This data is only available for VPC models. For more information, refer to Virtual Private Cloud (VPC).

```
10.15.1.1
```

The following shows how to obtain the access mode used by a private IP address to access the public network. This data is only available for VPC models. A basic network CVM instance accesses the public network through the public gateway.

```
NAT
```

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

```
```
139.199.11.29

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

```
255.255.192.0
```

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

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

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

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

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

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

The following shows how to obtain the account AppId of the CVM.

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

### Querying Instance User Data

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

**Searching user data**

Users can access user data within the CVM by using the following:

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

Last updated: 2020-04-01 11:11:53

Scenario

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

Directions

Modifying the name of an instance

1. Log in to the CVM Console.
2. In the instance list, select the CVM whose name needs to be modified and click More>Instance Settings> Rename on the right.
3. In the “Rename” window that pops up, enter a new instance name, and then click OK.

Modifying the names of multiple instances

1. Log in to the CVM Console.
2. In the instance list, select multiples CVM instances whose names need to be modified and click More actions>Instance Settings> Rename on the top.
3. In the “Rename” window that pops up, enter a new instance name, and then click OK.

CVMs modified using this method will have the same instance name.
Resetting Instance Password

Last updated : 2020-06-15 17:04:42

Use Cases

If you forget your CVM instance login password, you can use the console to reset it. This article describes how to reset your instance login password through the console.

- You can only reset your instance login password when the instance status is shutdown.
- Running instances are shutdown when you reset their login passwords through the console, which may cause service interruption and data loss. Plan ahead and perform password resets during off hours to minimize the impact.

Directions

Resetting the password of a single instance

1. Log in to the CVM Console.
2. In the instance management page select the desired CVM instance and click More -> Password/key -> Reset Password, as shown in the following figure:

3. Instances in different statuses have different steps for resetting passwords. Pick one of the following:
   - If you need to reset the password of a Running instance:
     a. Select a user name type and enter the desired user name. Enter the New password and Confirm password. Click Next, as shown in the following figure:
b. Select **Agree to a forced shutdown** and click **Reset Password**, as shown in the following figure:
If the instance is Stopped, select user name type and enter the desired user name. Enter New password and Confirm password. Click Reset Password to complete the process, as shown in the following figure:

Resetting passwords in batches

1. Log in to the CVM Console.
2. In the instance management page, select desired CVM instances and click Reset Password at the top of the instance list. The Reset Password page appears.
3. In the “Reset Password” pop-up window, the password reset operation is different for instances with different statuses. Select one of the following:
   - If the selected instances include a **Running** instance:
     - a. Select a **user name type** and enter the desired user name. Enter **New password** and **Confirm password** and click **Next**, as shown in the following figure:
b. Select **Agree to a forced shutdown** and click **Reset Password**, as shown in the following figure:
If all selected instances are **Stopped**, select a **user name type** and enter the desired user name. Enter **New password** and **Confirm password** and click **Reset Password**, as shown in the following figure:
This document describes how to obtain the private IP address of the instance and configure the private DNS.

**Obtaining the private IP address of an instance**

**Obtaining the private IP address on the console**

1. Log in to the CVM Console.
2. On the instance management page, select the instance and move the mouse to the **Primary IP** column to view its private IP, and click to copy the private IP, as shown below:

![Private IP on Console](image)

**Obtaining the private IP address using API**

Please see [DescribeInstances API](#).

**Obtaining the private IP address using instance metadata**

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

   The following operations use the cURL tool as an example.

```bash
curl http://metadata.tencentyun.com/meta-data/local-ipv4
```
The returned information is the private IP address, as shown below:

For more information about instance metadata, see Instance Metadata.

Configuring private network DNS

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

**For Linux operating system**

1. Log into the Linux CVM.
2. Execute the following command to open the `/etc/grub.conf` file.
   ```
   vi /etc/resolv.conf
   ```
3. Press `i` to switch to the edit mode, and modify the DNS IP according to the corresponding region in the Private Network DNS list.
   
   For example, change the private network DNS IP to an private network DNS server in the Beijing region.
   ```
   nameserver 10.53.216.182
   nameserver 10.53.216.198
   options timeout:1 rotate
   ```
4. Press `Esc`, enter `:wq`, save the file and return.

**For Windows operating system**

1. Log in to the Windows CVM.
2. On the operating system interface, open Control Panel > Network and Sharing Center > Change adapter settings.
3. Right-click the Ethernet and select Properties to open the “Ethernet Properties” window.
4. In the “Ethernet Properties” window, double-click **IP version 4 (TCP/IPv4)**, as shown below:

5. Select [Use the following DNS server address] and modify the DNS IP according to the corresponding region in the Private Network DNS list.

6. Click **OK**.
Modifying Private IP Addresses

Last updated: 2020-04-01 11:11:54

Scenario

You can modify the private IP of a CVM instance in VPC directly on the console or by changing the subnet of the CVM instance. This document describes how to modify the private IP of a CVM instance in the VPC console.

For details on changing the subnet, see Change Instance Subnet.

Limits

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

Directions

1. Log in to the CVM Console.
2. Select the region of the instance whose private IP you want to modify, and click the instance ID/name to enter its details page.
3. On the instance details page, select the [ENI] tab and click Modify Primary IP.
4. In the primary ENI operation list, click Modify Primary IP.
5. In the “Modify Primary IP” window that pops up, enter the new IP and then click OK. It takes effect after the instance is restarted.

You can only enter private IP in the current subnet CIDR.
Getting Public IP Addresses

Scenario

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

Directions

Obtaining the public IP address on the console

1. Log in to the CVM Console.
2. On the instance management page, move the mouse to the primary IP column, and appears, as shown below:

3. Click to copy the IP address.

Obtaining the public IP address using API

Please see DescribeInstances.

Obtaining the public IP address using instance metadata

1. Log in to the CVM instance.
   
   For more information, please see Log in to Linux Instance and Log in to Windows Instance.

The public IP address is mapped to the private IP address through NAT. If you view the network interface attributes from within the instance (such as by using commands such as `ifconfig` (Linux) or `ipconfig` (Windows)), the public IP address is not displayed. To obtain the public IP from within the instance, please see Obtaining a Public IP Address of the Instance Using Instance Metadata.
2. To obtain the public IP address, you can access the metadata by using the cURL tool or an HTTP GET request.

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

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

```
115.8.8.2
```

For more information, see Instance Metadata.
Changing Public IP Addresses
Last updated : 2020-06-03 14:36:20

Overview

This document describes how to change a public IP address.

Notes

- Each account can change public IP addresses within the same region a maximum of 3 times per day.
- Each instance can only change its public IP once.
- The old public IP will be released after the change.

Prerequisites

You have logged in to CVM Console.

Directions

1. On the **Instances** management page, locate the CVM that you want to change the public IP for, click **More -> IP/ENI -> Change Public IP**, as shown below:

![Change Public IP](image)

2. In the “Change IP” dialog box, click **Confirm** to change the IP.
Retrieve the public network IP address

Last updated: 2020-02-11 14:45:42

Scenario

This document describes how to retrieve a public IP address that has been used before but not yet assigned to other users.

Notes

- The retrieved IP address is an EIP, and the total number of EIPs must not exceed the total quota.
- Each account can apply for a specific IP address up to three times per month in each region.

Directions

1. Log in to CVM Console.
2. In the left sidebar, click EIP to access the EIP management page.
3. Click Retrieve IP, as shown in the following figure:

![Retrieve IP](image)

4. In the Retrieve IP pop-up window, enter the public IP address and click Check to query whether the IP address can be retrieved, as shown in the following figure.
If yes, click **Apply Now**.

If no, the IP address that you applied for cannot be retrieved for reasons such as it has already been assigned. In this case, try to apply for another IP address or click **Cancel** to exit.
Change Instance Subnet

Last updated: 2019-10-18 11:18:09

The subnet of the CVM instance in VPC can be directly replaced in the console.

Limits

- The associated CVM restarts automatically after its subnet is replaced.
- The subnet cannot be replaced for the secondary ENI.

Procedure

- Log in to the CVM Console.
- Select a region.
- Click the ID of the instance to go to its details page.
On the instance details page, click **ENI**, and then click the ID of primary ENI.
• Go to the primary ENI details page, and click **Replace Subnet**.

• Select the new subnet in the pop-up subnet replacement page, enter the new primary IP, and click **OK**. Then, the instance restarts to complete the replacement.
Note:

i. If you have not created a subnet in this availability zone, create a new subnet first.
ii. You can only enter the private IP of the current subnet CIDR.
Cloud Virtual Machine

Change Security Group

Last updated : 2020-05-09 17:04:17

Operation Scenario

Security group is a virtual firewall for filtering packets and is used to set the network access controls for one or multiple CVMs. It is an important network security isolation method provided by Tencent Cloud. When creating a CVM instance, you must configure a security group for it. Tencent Cloud allows you to configure a new security group for the CVM instance after it is created.

To configure a new security group for the instance, create a security group first. For more information, please see Creating a Security Group.

Prerequisites

Log in to the CVM Console.

Directions

Change the configured security group

To improve your experience on the CVM Console, security group can be configured on the instance management page or on the instance details page.

Configuring a security group on the instance management page

1. Select a CVM to be reassigned to a new security group on the instance management page and click More > Security Groups > Configure Security Groups, as shown below:
2. On the “Configure Security Group” pop-up window, check the name of the new security group (multiple names can be selected) and click **Confirm** to change the security group.

**Configuring a security group on the instance details page**

1. On the instance management page, click the CVM instance ID/name for which you want to change the security group and enter the instance details page.
2. Click **More Actions > Security Groups > Configure Security Groups** on the upper right corner of the instance details page, as shown below:

3. On the “Configure Security Group” pop-up window, check the name of the new security group (multiple names can be selected) and click **Confirm**.

**Change the bound security group**

1. On the instance management page, click the CVM instance ID/name for which you want to bind the security group and enter the instance details page.
2. On the instance details page, select the **Security Groups** tab and click **Bind** on the “Bound to security group” column, as shown below:
3. On the “Security Groups” pop-up window, check the name of the security group (multiple names can be selected) to be bound based on your actual needs and click **OK** to bind the security group.
Security Groups

Projects: All projects

Select a security group

Enter the security group name or ID

Selected (4)

<table>
<thead>
<tr>
<th>ID/Name</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

OK Cancel
Search Instances

Last updated : 2020-04-27 14:46:34

Scenario

By default, the CVM console displays the instances for all projects in the current region. To help you quickly search instances in the current region, Tencent Cloud provides a CVM search feature. You can filter out instances by resource attributes such as project, instance billing method, instance type, availability zone, IP, instance ID, and instance name.

Directions

1. Log in to the CVM Console.
2. Enter the content you wish to search based on your needs, and click to search.
- Enter the keyword in the search text box, and click , as shown below:

![](image)

- Choose a specific dimension to search (such as project, project, instance billing method, instance type, etc..) and click , as shown below:

![](image)
3. To learn more about search syntaxe, click 💡 to view the relevant syntax of search instances. For more search instance syntax, please see the following figure.
<table>
<thead>
<tr>
<th>Enter Format</th>
<th>Example</th>
<th>Display in Search Box</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single keyword</td>
<td>[Keyword]</td>
<td>10.0.0.1</td>
<td>List all instances including the keyword “10.0.0.1”</td>
</tr>
<tr>
<td>Multiple keywords</td>
<td>[Keyword] [Enter key++] [Keyword]</td>
<td>10.0.0.1 <a href="http://www.123.com">www.123.com</a> 192.168.23.54</td>
<td>List all instances that include all the three keywords “10.0.0.1,” “www.123.com,” and “192.168.23.54”</td>
</tr>
<tr>
<td>Single resource type</td>
<td>[Resource type]: [Keyword]</td>
<td>IP: 10.0.0.1</td>
<td>List all instances whose IP is “10.0.0.1”</td>
</tr>
<tr>
<td>Multiple resource types</td>
<td>[Resource type]: [Keyword] [Enter key++] [Resource type]: [Keyword]</td>
<td>Availability Zone: Hong Kong Zone 2 Project: Default</td>
<td>List all instances whose “Availability Zone” is “Hong Kong Zone 2” and “Project” is “Default”</td>
</tr>
<tr>
<td>Single resource type and multiple keywords</td>
<td>[Resource type]: [Keyword]</td>
<td>CVM Status: Creating</td>
<td>List all instances whose “CVM Status” is “Creating” or “Shutdown”</td>
</tr>
<tr>
<td>Pasted contents</td>
<td>[pasted contents]</td>
<td>112.11.22.33 112.11.22.34 112.11.22.53</td>
<td>List all instances include the keywords “112.11.22.33,” “112.11.22.34,” or “112.11.22.53”</td>
</tr>
</tbody>
</table>
Export Instances

Last updated : 2020-04-27 14:46:34

Scenario

You can export the CVM instance list of a region in the console, and customize the fields to be exported. You can select a maximum of 27 fields, including ID, instance name, status, region, availability zone, instance type, operating system, image ID, CPU, MEM, bandwidth, public IP, private IP, system disk type, system disk size, data disk type, data disk size, network type, subnet ID, VPC name, creation time, expiry time, instance billing mode, network billing mode, project, dedicated host ID, and tag.

Directions

1. Log in to the CVM Console.
2. Select a region.
3. Click in the upper right of the instance list, as shown below:

4. In the pop-up “Export instances” window, select the fields you want to export and click “OK”, as shown below:

   You can select a maximum of 27 fields to export.
Export Instances

- Select All
- ID
- Instance Name
- Status
- Region
- Availability Zone
- Instance Type
- CPU (core)
- MEM (GB)
- Operating System
- Image ID
- VPC name
- Subnet ID
- Subnet name
- Creation Time
- Expiry Time
- Instance Billing Mode
- Network billing mode
- Project
- Dedicated Host ID
- Tag

Export range
- All Instance
- Only export search result
- Selected Instance

OK  Close
Spot instances may be repossessed by Tencent Cloud due to price or inventory reasons. To enable users to perform custom operations before instance repossession, we provide an API for obtaining information about repossession status via an internal metadata mechanism.

### Metadata

Instance metadata refers to data relevant to an instance. It can be used for configuring or managing an operating instance. You can access and obtain instance metadata via an instance. For more information, see [Instance Metadata](#).

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

To obtain information about the repossession status of a spot instance, you can access the metadata by using the cURL tool or an HTTP GET request.

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

- If the following information is returned, it indicates the repossession time of the spot instance.

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

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

For more information, see [Instance Metadata](#).
Renew Instances

This document introduces how to renew Postpaid instance.

- Postpaid instance: Postpaid instances can be automatically activated with sufficient balance in your account. For more information, please see Online Top-up.
Shutdown Instances

Scenario

The instance can be shut down when you need to stop the service, or modify configurations that can be done only in the shutdown state. Shutting down an instance is like shutting down a local computer.

Notes

- You can shut down an instance using system commands (such as the shutdown command under Windows system and Linux system) or through the Tencent Cloud console. We recommend you view the shutdown process on the console to check whether any problem occurs.
- The instance will no longer provide services after the shutdown. Before the shutdown, make sure the CVM has stopped receiving service requests.
- During the shutdown, the status of the instance will change from "shutting down" to "shutdown". If the shutdown process takes too long, there may be an exception. For more information, please see Close an CVM to avoid forced shutdown.
- After an instance is shut down, all storage is still connected to the instance, and all disk data are retained. Data in the memory will be lost.
- Shutting down an instance does not change its physical attributes. The public and private IPs of the instance remain unchanged. Elastic Public IP is still bound to the instance. Due to service interruption, however, you will receive an error response when accessing these IPs. Classiclink relationship remains unchanged.
- If the instance belongs to the real server cluster of the CLB instance, it can no longer provide services after the shutdown. If the health check policy has been configured, the instance that has been shut down will be automatically blocked and requests will no longer be forwarded to it. Otherwise, the client may receive a 502 error code. For more information, please see Health Check.
- If the instance that has been shut down is in an auto scaling group, the auto scaling service will mark the instance as having poor performance, and may replace and move it out of the auto scaling group. For more information, please see Auto Scaling.
Directions

Shutdown an instance via the console

1. Log in to the CVM Console.
2. Select different methods based on actual needs.
   - Shut down an instance: select the instance to be shut down, and click 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 to shut down instances in batches.
   Reasons are given for instances that cannot be shut down.

Shutdown an instance via API

For more information, see the StopInstances API.

Subsequent Operations

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

- **Instance configuration (CPU, memory):** To change the instance type, see Change Instance Configuration.
- **Change password:** see Login Password.
- **Load SSH key:** see SSH Key.
Operation Scenario

Restarting the CVM instance is a common method to maintain it. It is equivalent to restarting the operating system of the local computer. This document describes how to restart instances.

Notes

- **Preparing to restart instances**: The instance cannot provide services during restart. Make sure before restarting the CVM that it has stopped receiving service requests.
- **How to restart instances**: We recommended you restart an instance using the restart operations provided by Tencent Cloud instead of running the restart command in the instance (such as the relaunch command under Windows and the reboot command under Linux).
- **Restart time**: Generally, it takes only a few minutes to restart an instance.
- **Physical features of instances**: Restarting an instance does not change its physical features. Its public and private IP addresses as well as stored data will not be changed.
- **Billing**: Restarting an instance will not start a new instance billing period.

Directions

You can restart instances via the following methods:

- Use the console to restart instances
- Use API to restart instances

**Use the console to restart instances**

1. Log in to the CVM Console.
2. On the instance management page, select the instance restart method based on the actual number of instances to be restarted.
   - Restarting a single instance: On the row of the instance you want to restart, click **More** > **Instance Status** > **Restart**, as shown below:
Restarting multiple instances: Check all instances you want to restart and click **Restart** at the top of the list to batch restart the instances. If they cannot be restarted, the reason will be displayed, as shown below:

A single instance can also be restarted using this method.

**Use API to restart instances**

Please see **RebootInstances API**.
Logging into Linux Instance
Log into Linux Instance Using Standard Login Method

Last updated: 2020-01-21 10:19:51

**Scenario**

WebShell is the login method recommended by Tencent Cloud. No matter your local OS is Windows, Linux or Mac OS, as long as you have purchased public IPs for your instances, you can log in via Web Shell. This document describes how to log into a Linux instance via Web Shell.

Benefits of Web Shell:

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

**Applicable Local OS**

Windows, Linux, or Mac OS.

**Authentication Method**

*Password* or *Key*

**Prerequisites**

- You must already have the admin account and password (or key) for the instance to be logged into.
  - If you choose **Random Password** when creating the instance, please go to **Internal Message** to check the password.
  - If you forgot your password, then **reset the instance password**.
- Make sure the CVM instance has a public IP, and port 22 is open (if the CVM is purchased with “Quick Configuration”, this port is open by default.)
Directions

1. Log in to the CVM Console.

2. On the instance’s management page, select the Linux CVM that you want to log in to and click Log In, as shown below:

3. In the Log into Linux Instance pop-up window, select Standard login method and click Log In Now, as shown below.
4. In the **Log into Instance** window, select **Password Login** or **Key Login**, as shown below:
If the login is successful, “Socket connection established” will display as shown below:

![Socket connection established](image)

**Subsequent Operations**

After logging into the CVM, you can build a personal website or forum on the Tencent Cloud CVM or perform other operations. For more information, see the following documents:

- Build a personal WordPress site
Logging into Linux Instance via SSH Key

Scenario

This document describes how to use SSH key to log into a Linux instance in a local computer using Linux or MacOS.

Applicable local OS

Linux or Mac OS

Authentication Method

Password or SSH Key

Prerequisites

- You must already have the admin account and password (or key) for logging into the instance.
  - If you use a system default password to log in to the instance, obtain it by visiting Internal Message.
  - If you log in to the instance with a key, you must have created a key and bound it to this CVM. For more information, see SSH Keys.
  - If you forget your password, reset the instance password.
- A public IP has been purchased for your CVM instance, and port 22 is open (this is open by default for CVMs purchased with quick configuration).

Steps

Logging in with a password

1. Execute the following command to connect to the Linux CVM.
If your local computer uses Mac OS, you must open the terminal provided by the system and then execute the following command. If your local computer uses Linux, you can directly execute the following command.

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

- **username** is the default account name obtained as a prerequisite.
- **hostname or IP address** is the public IP address or custom domain name of your Linux instance.

2. Enter the password you have already obtained, and press **Enter** to log in.

### Logging in with a key

1. Execute the following command to set the private key file readable only to you.

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

2. Execute the following command for remote login.

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

- **username** is the default account name obtained as a prerequisite.
- **hostname or IP address** is the public IP address or custom domain name of your Linux instance.

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

### Subsequent Operations
After logging into the CVM, you can build a personal website or forum on Tencent Cloud CVM or perform other operations. For more information, see the following:

- [Manually Build WordPress Website](#)
Logging into Linux Instances via Remote Login Tools

Last updated: 2020-04-01 11:11:54

Scenario

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

Applicable OS

Windows

Authentication Method

Password or Key

Prerequisites

- You must already have the admin account and password (or key) of the instance to be logged in to.
  - If you use a system default password to log in to the instance, first go to Internal Message to get it.
  - If you forget your password, please reset the instance password.
- A public IP has been purchased and obtained for your CVM instance, and port 22 is open (this is open by default for CVM purchased with quick configuration).

Directions

Logging in with a password

1. Download the Windows remote login software, PuTTY.
   - To download PuTTY: Click here
2. Double-click `putty.exe` to open the PuTTY client.

3. In the **PuTTY Configuration** window, enter the following content. This is shown in the following figure:

![PuTTY Configuration Window](image)

Parameters are as follows:
- **Host Name (or IP address):** The public IP of the CVM (log in to the CVM Console to obtain the public IP in the instance list and details pages).
- **Port:** The port of the CVM. This must be set to 22.
- **Connect type:** Select **SSH**.
- **Saved Sessions:** Enter the session name, such as `test`.

After configuring **Host Name**, configure **Saved Sessions** and save it. You can double-click the session name saved under **Saved Sessions** to log in to the CVM subsequently.

4. Click **Open** to enter the **PuTTY** interface, and **login as:** is prompted.

5. Enter the username after **login as:** and press **Enter**.

6. Enter the password after **Password** and press **Enter**.

The entered password is not displayed by default, as shown below:
After logging in, information about the CVM that you currently log in to appears to the left of the command prompt.

**Logging in with a key**

1. Download the Windows remote login software, PuTTY. Download putty.exe and puttygen.exe. To download PuTTY, [click here](#).
2. Double-click `puttygen.exe` to open the PuTTY Key client.
3. Click **Load**, select and open the path where the downloaded private key is saved. This is shown in the following figure:

For example, select and open the private key file named `david`.
4. In the **PuTTY Key Generator** window, enter the key name and the encrypted private key password. Click **Save private key**. This is shown in the following figure:

![PuTTY Key Generator](image)

5. In the pop-up window, select the path where the key will be saved. In the file name field, enter **Key Name.ppk** and click **Save**. For example, save the private key file **david** as **david.ppk**. This
6. Double-click **putty.exe** to open the PuTTY client.

7. In the left sidebar, select **Connection > SSH > Auth**, to enter the Auth configuration interface.

8. Click **Browse**, and select and open the path where the key is saved. This is shown in the following figure:
9. Switch to Session configuration interface. Configure the CVM IP, port, and connection type. This is shown in the following figure:
- Host Name (IP address): The public IP of the CVM. Log in to the CVM Console to obtain the public IP in the instance list and details pages.
- Port: Port of the CVM, which must be 22.
- Connect type: Select SSH.
- Saved Sessions: Enter the session name, such as test. After configuring Host Name, configure Saved Sessions and save it. You can double-click the session name saved under Saved Sessions to log in to the CVM subsequently.

0. Click Open to initiate the login request.

Subsequent Operations

After logging in to the CVM, you can build a personal website or forum on Tencent Cloud CVM or perform other operations. For more information, see the following documents:

- Build a personal WordPress site
- Build a Discuz! forum
Logging into Linux Instances via VNC

Last updated: 2020-04-01 11:11:55

Scenario

VNC login provided by Tencent Cloud allows users to remotely log in to CVM via a web browser. If a client does not have remote login installed or it cannot be used, user can log in to the CVM using VNC login to check the CVM status and perform basic management operations using the CVM account.

Applicable OS

Windows, Linux, or macOS.

Use Limits

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

Prerequisites

You must already have the admin account and password (or key) of the Linux instance to be logged in to.

- If you use a system default password to log in to the instance, first go to Internal Message to get it.
- If you forget your password, please reset the instance password.

Directions

1. Log in to the CVM Console.
2. On the Instance management page, select the Linux CVM you want to log in to and click **Log In**, as shown below:

![Instance management page](image)

3. In the **Log into Linux instance** window that pops up, select **Alternative login methods (VNC)** and click **Log In Now**, as shown below.

![Log into Linux instance](image)

4. In the pop-up dialog box, enter the username after **login** and press **Enter**.
5. Enter the password after **Password** and press **Enter**.
   
   The entered password is not displayed by default, as shown below:
After logging in, information about the CVM that you currently log in to appears to the left of the command prompt.

**Subsequent Operations**

After logging in to the CVM, you can build a personal website or forum or perform other operations. For more information, see the following documents:

- [Build a personal WordPress site](#)
- [Build a Discuz! forum](#)
Logging into Windows instance
Logging into Windows Instance via Remote Desktop

Scenario

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

Applicable OS

Windows

Prerequisites

- You must already have the admin account/password for logging into Windows instance remotely.
  - If you use a system default password to log in to the instance, obtain it by visiting Internal Message.
    If you forgot the password, then reset instance password.
- A public IP has been purchased for your CVM instance, and port 3389 is open (if the CVM is purchased with “Quick Configuration”, this port is open by default.)

Steps

The following steps take the Windows 7 operating system as an example.

1. On the local Windows computer, click , and enter mstsc in Search programs and files and press Enter to open the remote desktop connection dialog box, as shown below:
2. Enter the Windows server’s public IP after Computer and click Connect.
3. Enter the instance’s admin account/password in the Windows Security pop-up window, as shown below:

If the Do you trust this remote connection? dialog box pops up, you can check Don’t ask me again for connections to this computer and click Connect.

4. Click OK to log in to the Windows CVM instance.
Logging in to a Windows Instance Using the RDP File (Recommended)

Overview

Remote Desktop Protocol (RDP) is a multiple-channel protocol developed by Microsoft that allows a local computer to connect to a remote computer. We recommend you use RDP to log in to your Windows CVMs. This document describes how to log in to Windows instances using RDP files.

Supported Systems

You can log in to your CVMs from Windows, Linux, and MacOS using RDP.

Prerequisites

- You must have the admin account and password for logging in to a Windows instance remotely.
  - If you use a system default password to log in to the instance, you can obtain the password at the Message Center.
  - If you forgot your password, please reset the instance password.
- You have purchased public IPs for your CVM instance and port 3389 is open.

Directions

Logging in to your CVM on Windows using RDP

1. Log in to the CVM Console.
2. On the Instances page, locate the Windows CVM you want to log in to and click Log In as shown below.
3. In the **Log into Windows instance** pop-up window, select **Log in with RDP file** and click **Download RDP file** to download the RDP file to your local computer.

4. Double-click the downloaded RDP file, enter the password, and click **OK** to remotely connect to your Windows CVM.
   - If you use a system default password to log in to the instance, you can obtain the password at the **Message Center**.
If you forgot your password, please reset the instance password.

Logging in to your CVM on Linux using RDP

We recommend you use rdesktop as the remote desktop client. For more information, see the official introduction to rdesktop.

1. Run the following command to check whether rdesktop has been installed.

   rdesktop

   - If yes, perform step 4.
   - If no, you will be prompted with "command not found". In this case, perform step 2.

2. Open a terminal window and run the following command to download rdesktop. This step uses rdesktop v1.8.3 as an example.

   wget https://github.com/rdesktop/rdesktop/releases/download/v1.8.3/rdesktop-1.8.3.tar.gz

   If you want to install the latest version, visit the rdesktop page on GitHub to find it. Then replace the path in the command with that of the latest version.

3. In the directory where rdesktop will be installed, run the following commands to decompress and install rdesktop.

   tar xvzf rdesktop-<x.x.x>.tar.gz  ## Replace <x.x.x> with the version number of the downloaded rdesktop.
   cd rdesktop-1.8.3
   ./configure
   make
   make install

4. Run the following command to connect to the remote Windows instance.

   rdesktop -u Administrator -p <your-password> <hostname or IP address>

   - Administrator refers to the admin account mentioned in the prerequisites section.
   - <your-password> refers to the login password that you set.

   If you use a system default password to log in to the instance, you can obtain the password at
the Message Center. If you forgot your password, please reset the instance password.

- `<hostname or IP address>` refers to the public IP address or custom domain name of your Windows instance.

**Logging in to your CVM on MacOS using RDP**

- The following operations use Microsoft Remote Desktop for Mac as an example. Microsoft stopped providing a link to download the Remote Desktop client in 2017. Currently, its subsidiary HockeyApp is responsible for releasing the beta client.
- The following operations use a CVM on Windows Server 2012 R2 as an example.

1. Download and install Microsoft Remote Desktop for Mac on your local computer.
2. Start MRD and click **Add Desktop**, as shown below:

![Microsoft Remote Desktop](image)

3. In the **Add Desktop** pop-up window, follow the steps illustrated in the following image to establish a connection to your Windows CVM.
i. In the **PC name** text field, enter the public IP address of your CVM.

ii. Click **Add**.

iii. Retain the default settings for the other options and establish the connection.

Your entry has now been saved, as shown below:
4. Double-click the new entry. Input your username and password for CVM and click **Continue**.
   - If you use a system default password to log in to the instance, you can obtain the password at the **Message Center**.
   - If you forgot your password, please reset the instance password.
5. In the pop-up window, click **Continue** to establish the connection, as shown below:
If the connection is successful, the following page will appear:
Logging into Windows Instance via VNC

Last updated: 2020-02-11 10:03:24

Scenario

VNC login offered by Tencent allows users to remotely connect to a CVM via a web browser. If a client does not have remote login installed, it cannot be used or logged into via any other means, users can connect to a CVM using VNC login to observe the CVM’s status and do basic CVM management operations using the CVM account.

Use Limits

- Features such as copy/paste, Chinese input, and file upload/download are currently not supported on CVMs using VNC login.
- Mainstream browsers must be used when using VNC login on a CVM, such as Chrome, Firefox, and IE 10 or above.
- A VNC login is a dedicated terminal, meaning only one user can use a VNC login at a time.

Applicable OS

Windows, Linux, or macOS.

Prerequisites

You must already have admin account/password for logging into Windows instance remotely.

- If you use a system default password to log in to the instance, obtain it by visiting Internal Message.
  If you forgot the password, then reset instance password.

Steps

1. Log in to the CVM Console.
2. On the instance’s management page, select the Windows CVM that you want to log in to and click **Log In**, as shown below:

![Image of instance management page](image)

3. In the **Log into Windows instance** pop-up window, select **Alternative login methods (VNC)** and click **Log In Now**, as shown below.
4. In the login window, select “Send Remote Command” in the top left corner, and press **Ctrl-Alt-Delete** to enter the system login interface as shown below:
Connection succeeded. To paste the command, please click here other login methods.

Ctrl-Alt-Delete to sign in.

Monday, November 4
Reinstalling System

Last updated : 2020-05-28 17:11:02

Operation Scenario

Reinstalling the operation system is an important method to restore instances to their initial status in the event of a system failure. This document describes how to reinstall the operating system.

Cloud Virtual Machine (CVM) supports two reinstallation types:

- **Single-system reinstallation**: is applicable to CVMs in any region. For example, reinstall from Linux to Linux or from Windows to Windows.
- **Cross-system reinstallation**: is available to Mainland China only, excluding Hong Kong, SAR. For example, reinstall from Linux to Windows or from Linux to Windows.

Currently, all new CBS instances and local disks support cross-system reinstallation. However, some existing 20-GB local disks currently do not support cross-system reinstallation through the console. If you are using these local disks, you can submit a ticket to apply for the cross-system installation feature, when needed.

Spot instances do not support system reinstallation.

Notes

- **Preparations**: back up important data in your system disk before reinstallation, because data in the system disk will be lost after reinstallation. To keep your system data, we recommend that you create a custom image and use this image to reinstall the system.
- **Recommended images**: we recommend that you use the image provided by Tencent Cloud or your custom image instead of those from unknown or other sources. Do not perform any other operations when the system disk is being reinstalled.
- **Physical features of the instance**: the public IP address of the instance does not change.
- **Billing**: when adjusting the size of the system disk (for CBS only), you will be charged according to the pricing standards of CBS. For more information, see CBS Pricing.
- **Subsequent operations**: after the system disk is reinstalled, data in data disks is not affected, but will be available for use only after the data disks are remounted.
Directions

You can reinstall the operating system in two ways:

- Reinstalling the system in the console
- Reinstalling the system through the API

**Reinstalling the system in the console**

1. Log in to the CVM console.
2. In the row of the instance for which you want to reinstall the system, choose More > Reinstall System, as shown in the following figure:

![CVM console](image)

3. In the system reinstallation window that appears, select the image used by the current instance or another image, set the disk size, enter the password, and click Reinstall Now.

Here, the password is the one that you set when configuring the CVM instance or that was generated automatically by the system. If you forget the login password of your CVM instance and want to reset it, see Resetting the Instance Password.
Reinstalling the system through the API

- For more information, see the ResetInstance API.
Terminating Instances

This article describes how to terminate and release a Cloud Virtual Machine (CVM) instance. For more information on expiration, see Expiration Notifications.

Overview

If you no longer need an instance, you can terminate it. The terminated instance is moved to the Recycle Bin. You can renew, restore, or release the instances in the Recycle Bin.

If your account is overdue, you need to add funds before restoring pay-as-you-go instances.

You can use the following methods to terminate and release pay-as-you-go instances:

- **Manual termination**: if your account is in good standing, you can manually terminate a pay-as-you-go instance. A pay-as-you-go instance is released after it remains in the recycle bin for over 2 hours.

- **Scheduled termination**: you can schedule a time (to the second) to automatically terminate a pay-as-you-go instance. You can select a future time to terminate resources. A instance terminated using scheduled termination bypasses the recycle bin and is released immediately. You can cancel a scheduled termination at any time before the scheduled time.

- **Automatic termination upon expiration or when account is overdue**: A pay-as-you-go instance with its balance below 0 will be automatically released after 2 hours and 15 days. For the first 2 hours, billing continues and you can still use the instance. For the next 15 days, however, the instance will be shut down, and billing will stop. Pay-as-you-go instances in arrears cannot be moved to the recycle bin. Instead, you need to check the instance in the CVM instance list. You can continue to use the instance if you renew it within the specified time.
<table>
<thead>
<tr>
<th>Pay-as-you-go instances</th>
<th>Manual termination (not overdue)</th>
<th>Scheduled termination (not overdue)</th>
<th>Automatic termination upon expiration or when account is overdue</th>
</tr>
</thead>
<tbody>
<tr>
<td>After termination, pay-as-you-go instances will be released after being retained in the recycle bin for a maximum of 2 hours.</td>
<td>Instances for which timed termination is set will be released immediately as scheduled, instead of going into the recycle bin.</td>
<td>When your account is in arrears, for the first 2 hours, billing continues and you can still use the instance. For the next 15 days, however, the instance will be shut down, and billing will stop. Pay-as-you-go instances in arrears are not moved to the recycle bin. If the instance is not renewed within this period, the instance will be released.</td>
<td></td>
</tr>
</tbody>
</table>

**Impact**

What happen to the data, EIPs and charges of an instance once it is terminated:

- **Billing**: once an instance is terminated or released, no more charge will incurred.
- **Instance data**: local disks and non-elastic cloud disks mounted to the instance are all released, and the data on these disks are lost. Back up the data in advance. Elastic cloud disks follow their own lifecycle.
- **EIP**: EIPs (including IP addresses on secondary ENIs) of a terminated instance are retained, and idle IP addresses may incur charges. If you don’t need them anymore, release them as soon as possible.

**Terminating and Releasing Pay-As-You-Go Instances**

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

**Terminating instances using the Console**

1. Log in to the CVM Console.
2. Choose one of the following:
   - **Terminate a single instance**: find the desired instance in the list and click More -> **Instance Status** -> **Terminate/Return** on the right side.
   - **Terminate instances in batches**: select all desired instances and click More -> **Terminate/Return** on the top of the interface. For instances that cannot be terminated, the reasons will be displayed.
3. In the pop-up window, choose **Immediate Termination** or **Scheduled Termination**.
   - **Immediate Termination**: you can choose to release resources immediately or in 2 hours. If you choose to release resources immediately, the instance data is cleared and cannot be restored.
   - **Scheduled Termination**: if you choose scheduled termination, you need to specify the termination time. The instance is terminated and released at that time and the data cannot be restored.
4. Click **Next** to confirm the resources to be terminated or retained.
5. Click **Start Termination**.

### Canceling a scheduled termination

1. Log in to the **CVM Console**.
2. In the instance list, find the desired instance and the corresponding **Scheduled Termination** in the **Instance Billing Plan** column. Move your cursor over the **Scheduled Termination** dialog box, as shown below:

   3. Click **Cancel**. A dialog box is displayed prompting you to confirm the cancellation.
4. In the dialog box, confirm the information of the instance for which you want to cancel timed termination and click **OK**. The cancellation takes effect immediately, as shown below:

Terminating Instances Using Tencent Cloud APIs

Refer to **TerminateInstances API** for more information.
This document describes how to repossess and restore a Cloud Virtual Machine (CVM) instance. For more information, see Arrears Reminder.

Reclaiming Instances

Tencent Cloud Recycle Bin provides a CVM instance repossession mechanism. Pay-as-you-go instances that are manually terminated or terminated at a scheduled time will be moved to the recycle bin. If the account is and remains in arrears for 2 hours and 15 days, pay-as-you-go instances are directly released, instead of going to the recycle bin.

Moving pay-as-you-go instances to the recycle bin

- **Retention period**: if the account is not in arrears, instances manually terminated by users are retained in the recycle bin for 2 hours.
- **Processing upon expiration**: if the instances are not renewed in time before the retention period expires, the system releases these instance resources and starts to automatically terminate instances. The terminated instances cannot be reclaimed. In addition, EIPs bound to these instances are also released.
- **Binding relationship**: after an instance is moved into the recycle bin, the binding relationships with Cloud Load Balancer, Cloud Block Storage, and Classiclink are not automatically terminated.
- **Operation restriction**: instances in the recycle bin can only be restored after renewal or terminated.

- A pay-as-you-go instance in the recycle bin cannot be restored if the account is in arrears. To restore this instance, you must first pay the renewal fee.
- A pay-as-you-go instance can be retained for up to 2 hours in the recycle bin. Therefore, you need to renew and restore the instance in time so that you can continue to use it.
- If your account is already in arrears, pay-as-you-go instances cannot be moved to the recycle bin. Instead, you need to check the instance in the CVM instance list. If the instance is not renewed within 2 hours and 15 days after the account is in arrears, the instance will be released.
Restoring Instances

1. Log in to the CVM Console.
2. In the left sidebar, choose Recycle Bin > CVM Recycle Bin to go to the CVM repossession list.
3. To restore a single instance, find the target instance in the list, click Restore, and pay the renewal fee.
4. To restore instances in batch, select all target instances, click Batch Restore at the top, and pay the renewal fee.
Spot Instances

Last updated : 2020-04-01 11:30:14

Scenario

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

- **CVM console**: Spot Instances has been added as an option to Billing Mode on the CVM purchase page.
- **BatchCompute console**: Spot instances can be selected when users submit jobs and create computing environments in the BatchCompute console.
- **TencentCloud API**: Parameters related to spot instances have been added to the RunInstances API.

Directions

**CVM console**

1. Log in to the CVM purchase page.
2. On the Select a model tab page, set Billing Mode to Spot Instances.
3. Specify Region, Availability Zone, Network, Instance, and other configurations as required and prompted.
4. Check the information of the spot instance to be purchased and the cost details of each configuration item.
5. Click Purchase and complete payment.
   After completing payment, you can log in to the CVM console to check your spot instance.

**BatchCompute console**

- **Async API**: When you submit a job, create a computing environment, or modify the expected number of instances in a computing environment, the BatchCompute instance processes your requests asynchronously. When it cannot fulfill the current request due to inventory or price reasons, the BatchCompute instance continuously applies for spot instance resources until the current request is fulfilled.

If you need to release an instance, you need to adjust the expected number of instances in the computing environment via the BatchCompute console. If you release instances via the CVM
console, the BatchCompute console will automatically create instances until the expected number of instances is met.

- **Cluster Mode**: The computing environment of a BatchCompute instance can maintain a batch of spot instances as a cluster. You only need to submit the expected quantity, configurations, and maximum price of the spot instances. The computing environment will continuously apply for spot instances until the expected quantity is met. Even if spot instances go offline, the computing environment will automatically apply for spot instances again to meet the expected quantity.

- **Fixed Price**: Currently, spot instances are provided at fixed discounts. You must set a value that is greater than or equal to the current market price. For the market prices, see [Spot Instances - Supported regions and instance types](#).

**Directions**

1. Log in to the BatchCompute console.
2. On the **Computing environment** page, randomly select a region, such as Guangzhou, and then click **New**.
   The **New computing environment** page appears.
3. On the **New computing environment** page, set **Billing Type** to **Spot Instance** and then specify configurations such as **Model Type**, **Image**, **Name**, and **Expected quantity** as required, as shown in the following figure:

   ![New computing environment](#)

4. Click **OK** to finish creation.

   Then you can check the new computing environment in the BatchCompute console. To view the creation progress of CVM instances that are being created in the computing environment, click **Activity Logs** and **Instance List** for the computing environment.
**TencentCloud API**

In the RunInstances API, you can specify the `InstanceMarketOptionsRequest` parameter to enable or disable the spot instance mode and configure the information about spot instances.

- **Sync API**: Currently, RunInstances provides a one-time synchronization request API. This means that if the application fails because the inventory is insufficient or the requested price is lower than the market price, the RunInstances API immediately returns a failure code and does not apply for the spot instance again.

- **Fixed Price**: Currently, spot instances are provided at fixed discounts. You must set a value that is greater than or equal to the current market price. For the market prices, see Spot Instances - Supported regions and instance types.

**Example**

You have an instance in Guangzhou Zone 3, and the billing mode of the instance is pay-as-you-go on an hourly basis and in spot mode. The specific configurations of the billing mode are as follows:

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

**Request parameters**

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

**Response parameters**

```
{
  "Response": {
    "InstanceIdSet": [
      "ins-1vogaxgk"
    ],
```
"RequestID": "3c140219-cfe9-470e-b241-907877d6fb03"
}
}
No Charges When Shut down for Pay-as-You-Go Instances

Scenario

"CVM No Charge When Shut Down" means pay-as-you-go instances (CPUs and memory) that have been shut down will not be billed. Cloud disks (system disk and data disk), public network bandwidth, images, and other key components of the CVM are still billed. For more information, please see No Charges When Shut down for Pay-as-You-Go Instances Details.

Directions

**Shut down an instance via console**

1. Log in to the CVM Console.
2. Choose different operation methods based on actual needs.
   - Shutting down a single instance:
     a. Select the instance you want to shut down, and click **More > Instance Status > Shutdown** on the right operation column.
     b. Tick **CVM No Charge when Shut down** and click **OK**.
        If the instance does not support this feature, "No Charge when Shut Down" is not supported will be displayed in the instance list.
   - Shutting down multiple instances:
     a. Select all the instances you want to shut down and click **Shutdown** at the top of the list to shut down instances in batches.
        Reasons are given for instances that cannot be shut down.
     b. Tick **CVM No Charge when Shut down** and click **OK**.
        If the instance does not support this feature, "No Charge when Shut Down" is not supported will be displayed in the instance list.

**Shut down an instance via API**

You can use StopInstances API to shut down an instance. For details, please see StopInstances. To enable this feature via API, please add the following parameter:
<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Required</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>StoppedMode</td>
<td>No</td>
<td>String</td>
<td>The &quot;No Charge when Shut down&quot; feature is only available for pay-as-you-go instances</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>Range:</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>KEEP_CHARGING: Keep charging after the instance is shut down</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>STOP_CHARGING: No charge when shut down</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>*Default value: *</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>KEEP_CHARGING</td>
</tr>
</tbody>
</table>
Images
Creating Custom Images
Last updated: 2020-05-29 16:06:33

Scenario

When creating an image, you can start an instance with a public image, connect it to the instance, and deploy your software environment. If the instance runs normally, you can create a new custom image based on this as needed, so you can use this image to start more new instances that have the same custom configurations as the original one.

- When you create a custom image, the system creates a related snapshot by default. You need to delete the associated images before deleting this snapshot. Because snapshot has been commercialized, retaining a custom image will incur a certain snapshot fee. For more information on snapshot billing, please see Commercialization FAQs.
- For CVMs created based on public images after July, 2018, creating images online is supported (i.e., you can create images without shutting down the instance).
- For other CVMs, shut down the instance before creating a custom image to ensure that the image has the same deployment environment as the current instance.

Notes

- Each region supports a maximum of 10 custom images.
- The following directories and files will be removed.
  - /var/log/
  - /root/.bash_history, /home/ubuntu/.bash_history (Ubuntu system)
- When Linux instance creates a custom image, make sure /etc/fstab does not include data disk configuration. Otherwise, instances created with this image cannot be started normally. If the Linux instance that creates the custom image has a data disk mounted, note or delete the relevant data disk configurations in /etc/fstab.
- The creation process takes ten minutes or more, which depends on the data size of the instance. Please prepare in advance to avoid business impacts.
Directions

Create a custom image from an instance through the console

1. Log in to the CVM Console.
2. On the instance management page, select the instance for which images will be created, and click More > Instance Status > Shutdown.
3. After the instance is shut down, click More > Create Image.
4. In the pop-up "Create custom image" window, enter "Image Name" and "Description", and click Create Image.

You can click at the top right of the console to view the image creation progress.

5. After the image is created, click Images on the left sidebar to enter the image management page.
6. To purchase a server with the same image as the previous one, select the image you created in the image list, and click Create Instance.

Create a custom image through API

You can use the CreateImage API to create a custom image. For more information, see CreateImage API.

Best Practices

Migrate data on a data disk

If you need to keep the data on the data disk of the original instance when starting a new instance, you can first take a snapshot of the data disk, and then use this data disk snapshot to create a new CBS data disk.

For more information, see Creating Cloud Disks Using Snapshots.
Copying Images

Last updated : 2020-05-28 17:09:15

Overview

Common Steps

Cross-region replication can help users deploy the same CVM across regions quickly. You can use this feature to copy images across regions, and then create a CVM by copying the images under the new region.

Notes

- The copied image must be a custom image. You must create a custom image first. For details, see [Create Custom Images](https://intl.cloud.tencent.com/document/product/213/4942).
- Cross-region replication allows you to copy images in or outside China. If you need to copy images from China to other countries or vice versa, please contact after-sale service.
- Cross-region replication of images is currently free of charge.
- Cross-region replication currently does not support custom images larger than 50 GB.
- Cross-region replication takes 10 to 30 minutes.

Methods

Copy images via 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, as shown below:
4. Find the instance whose image needs to be copied, click **More > Cross-region replication**.

For batch operations, select all the images you want to copy and click **Cross-region replication**.

5. In the pop-up "Cross-region copying" 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 a destination region. Select the successfully copied image in the image list under the region, and click **Create Instance** to create the same CVM instance.

**Copy images via API**

You can also use SyncCvmImage API to copy images. For details, see [SyncCvmImage API](#).
Scenario

**Shared image** means that you share with **other users** a **custom image** you have created. Users can easily get shared images from each other to obtain necessary components and add custom contents.

Tencent Cloud cannot guarantee the integrity or security of shared images. Please only use shared images from reliable sources.

Notes

- Each image can be shared with up to 50 users.
- The name and description of shared images cannot be changed. They are used to create CVM instances only.
- Images shared to other users do not occupy your own image quota.
- Images shared to other users can be deleted, but you must cancel image sharing first. For more information, see [Cancel Image Sharing](#). The obtained shared images can not be deleted.
- Images can be shared to the same region with other accounts. To share the image to a different region, you need to copy it to the other region before sharing.
- The obtained shared images cannot be shared with other users.

Directions

**Obtain the ID of the account with which you want to share the image**

Tencent Cloud shared image is identified by the unique ID of the account with which you want to share the image. You can inform the other account to obtain his/her ID as follows:

1. Log in to the CVM Console.
2. Click the account name in the upper right corner and select **Account Information**.
3. View and record the account ID in the “Account Information” management page.
4. Send his/her account ID to you.
Share images via console

1. Log in to the CVM Console.
2. In the left sidebar, click Images.
3. Click the Custom Image tab to enter the custom image management page.
4. Select the custom image you want to share in the custom image list and click Share on the right.
5. In the pop-up “Shared Image” window, enter the ID of the account you want to share the image with, and click Share.
6. Inform the other account to log in to the CVM Console, and select Images>Shared Image to view the image you have shared.
7. To share the image with multiple users, repeat the steps above.

Share images via API

You can use the ShareImage API to share images. For details, see Shared Images API.
Cancelling Image Sharing

Scenario

This document describes how to cancel custom image sharing. You can cancel your image sharing status with other users at any time. This does not affect instances created by other users using this shared image, but they can no longer see the image nor create new instances using this image.

Directions

**Cancel image sharing through the console**

1. Log in to the CVM Console.
2. On the left sidebar, click Images.
3. Select **Custom Image** tab to enter the custom image management page.
4. In the custom image list, select the custom images you want to cancel sharing and click **More > Cancel Sharing**.
5. On the new page, select the unique ID of the account from which you want to cancel the image sharing and click **Cancel Sharing**.
6. In the pop-up window, click **OK** to cancel image sharing.

**Cancel image sharing through API**

You can use the ModifyImageSharePermission API to cancel image sharing. For more information, see [ModifyImageSharePermission](#).
Delete Custom Images

Last updated: 2020-04-20 18:33:17

Scenario

This document describes how to delete custom images.

Notes

Before deleting custom images, please note the following items:

- After a custom image is deleted, it can no longer be used to start a new CVM instance, but will not affect instances that have already been started. If you want to delete all instances started from this image, see Reclaiming Instances or Terminate Instances.
- A custom image that has been shared with others cannot be deleted. To delete it, you need to cancel image sharing first. For more information, see Cancel Image Sharing.
- You can only delete the custom image, not common image or shared image.

Directions

Delete images through the console

1. Log in to the CVM Console.
2. On the left sidebar, click Images and select the Custom Image tab to enter the custom image management page.
3. Select the method to delete custom images based on actual needs.
   - Deleting a single image: locate the custom image to be deleted in the image list and click More > Delete.
   - Deleting multiple images: select all custom images to be deleted in the image list and click Delete on the top.
4. In the pop-up window, click OK.
   - If the deletion fails, possible reasons will be prompted.

Delete images through API

You can use the DeleteImages API to delete images. For details, see Delete Images.
In addition to creating custom images, Tencent Cloud also allows you to import images. You can import an image file in the system disk of the local server or a server on another platform into CVM custom images. After an image is imported, you can use it to create a CVM or reinstall the operating system (OS) for an existing CVM.

**Import Preparations**

Prepare an image file that meets import requirements in advance.

- **Requirements for Linux images:**

<table>
<thead>
<tr>
<th>Image Attribute</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS</td>
<td>CentOS, Ubuntu, Debian, CoreOS, OpenSUSE, and SUSE</td>
</tr>
<tr>
<td></td>
<td>Both 32-bit and 64-bit OSs are supported.</td>
</tr>
<tr>
<td>Image format</td>
<td>RAW, VHD, QCOW2, and VMDK</td>
</tr>
<tr>
<td></td>
<td>Run `qemu-img info imageName</td>
</tr>
<tr>
<td>File system</td>
<td>GPT partition is not supported</td>
</tr>
<tr>
<td>Image size</td>
<td>The actual image size cannot exceed 50 GB. Run `qemu-img info imageName</td>
</tr>
<tr>
<td></td>
<td>The image vsize cannot exceed 500 GB. Run `qemu-img info imageName</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> when an image is imported, the size of the image in QCOW2 format prevails.</td>
</tr>
<tr>
<td>Network</td>
<td>Tencent Cloud provides the <code>eth0</code> network interface for the instance by default.</td>
</tr>
<tr>
<td></td>
<td>You can use the metadata service in the instance to check the network configuration of the instance. For more information, see Instance Metadata.</td>
</tr>
<tr>
<td>Driver</td>
<td>The Virtio driver of the visualization platform KVM must be installed for the image. For more information, see Checking the Virtio Driver on Linux.</td>
</tr>
<tr>
<td></td>
<td>We recommend that you install cloud-init for the image. For more information, see Installing cloud-init on Linux.</td>
</tr>
</tbody>
</table>
If cloud-init cannot be installed for the image due to other reasons, configure the instance by referring to [Forcibly Importing an Image](#).

### Kernel

The native kernel is preferred for an image. Any modifications on the kernel may cause a failure in importing the image into the CVM.

### Requirements for Windows images:

<table>
<thead>
<tr>
<th>Image Attribute</th>
<th>Requirements</th>
</tr>
</thead>
</table>
Both 32-bit and 64-bit OSs are supported. |
| Image format    | RAW, VHD, QCOW2, and VMDK  
Run `qemu-img info imageName | grep 'file format'` to check the image format. |
| File system type| Only NTFS with MBR partitions is supported.  
GPT partitions are not supported.  
Logical Volume Manager (LVM) is not supported. |
| Image size      | The actual image size cannot exceed 50 GB. Run `qemu-img info imageName | grep 'disk size'` to check the actual image size.  
The image vsize cannot exceed 500 GB. Run `qemu-img info imageName | grep 'virtual size'` to check the image vsize.  
**Note:** when an image is imported, the size of the image in qcow2 format prevails. |
| Network         | Tencent Cloud provides the Local Area Connection network interface for the instance by default.  
You can use the metadata service in the instance to check the network configuration of the instance. For more information, see Instance Metadata. |
| Driver          | The Virtio driver of the visualization platform KVM must be installed for the image.  
The Virtio driver is not installed in the Windows OS by default. You can install the Virtio driver for Windows and then export the local image. |
| Others          | Imported Windows images do not provide the Windows license activation service. |

### Directions

1. Log in to the CVM console.
2. In the left sidebar, click Images.
3. Select **Custom Image** and click **Import Image**.
4. Enable **Cloud Object Storage**, and then create a bucket. Upload the image file to the bucket and obtain the image file URL.
5. Click **Next**.
6. Complete the form based on the actual situation and click **Import**.

   Ensure that the entered COS file URL is correct.

You will be notified whether the import is successful through **internal messages**.

### Failed Import

Images may fail to be imported in the console. If the import fails, troubleshoot as follows:

**Notes**

Before troubleshooting, ensure that you have subscribed to product service notifications on the message subscription page. This ensures that you can receive internal messages, SMS messages, and emails about the causes of the failure.

If you do not subscribe to product service notifications, you will not receive messages about the import result.

**Troubleshooting**

For more information on error messages and descriptions, see [Error Codes](# errorcode).

**InvalidUrl: invalid COS URL**

The InvalidUrl error indicates that an incorrect COS URL is entered on the import page. The possible causes include:

- The image URL that you entered is not a Tencent Cloud Object Storage image URL.
- The access permission of the COS file is private read, and the signature has expired.

A COS file URL with the signature can be accessed only once.
A COS URL of another region has been entered. 

The image import service accesses the COS server in the local region through a VPC instance.

The user's image file has been deleted. 

After you receive the error message stating that the COS URL is invalid, troubleshoot based on the preceding causes.

InvalidFormatSize: invalid format or size

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

- Supported image file formats are `qcow2`, `vhd`, `vmdk`, and `raw`.
- The actual image file size cannot exceed 50 GB (based on the converted image file in qcow2 format).
- The size of the system disk to which the image is imported cannot exceed 500 GB.

After you receive an error message stating that the format or size is invalid:

- Convert the image file into an appropriate format according to Linux Image Creation, reduce the image size to meet the size requirements, and then reimport it.
- You can also use the offline instance migration feature to migrate the instance. This feature supports the migration of an image file with a size up to 500 GB.

VirtioNotInstall: the Virtio driver is not installed

The VirtioNotInstall error indicates that the image to be imported does not have the Virtio driver installed. Tencent Cloud uses the KVM virtualization technology and requires users to install the Virtio driver on the image to be imported. Except for a few customized Linux OSs, most Linux OSs have the Virtio driver installed. In Windows OSs, users need to manually install the Virtio driver:

- For Linux image import, see Checking the Virtio Driver on Linux.
- For Windows image import, see Windows Image Creation to install the Virtio driver.

CloudInitNotInstalled: the cloud-init program is not installed

The CloudInitNotInstalled error indicates that the image to be imported does not have the cloud-init program installed. Tencent Cloud uses the open-source cloud-init program to initialize the CVM. If the cloud-init program is not installed, the CVM will fail to be initialized.
For Linux image import, see Installing cloud-init on Linux.
For Windows image import, see Installing cloudbase-init on Windows.
After you install cloud-init or cloudbase-init, replace the configuration file according to the related document so that the CVM can pull data from the correct data source upon startup.

**PartitionNotPresent: partition information is lost**
The PartitionNotPresent error indicates that the imported image is incomplete. In this case, check whether the boot partition was included when the image was created.

**RootPartitionNotFound: the root partition is lost**
The RootPartitionNotFound error indicates that the root partition cannot be detected in the image to be imported. In this case, check the image file. The possible causes include:

- The installation package is uploaded.
- The data disk image is uploaded.
- The boot partition image is uploaded.
- An incorrect file is uploaded.

**InternalError: unknown error**
The InternalError error indicates that the image import service does not record the cause of the error. In this case, contact our customer service. Our technical personnel will help you resolve the issue as soon as possible.

### Error Codes

<table>
<thead>
<tr>
<th>Error Code</th>
<th>Reason</th>
<th>Recommended Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>InvalidUrl</td>
<td>The COS link is invalid.</td>
<td>Check whether the COS URL is the same as the imported image URL.</td>
</tr>
<tr>
<td>InvalidFormatSize</td>
<td>The format or size does not meet requirements.</td>
<td>Images need to meet the image format and image size requirements described in Import Preparations.</td>
</tr>
<tr>
<td>VirtioNotInstall</td>
<td>The Virtio driver is not installed.</td>
<td>Install the Virtio driver in the image by referring to the Driver section in Import Preparations.</td>
</tr>
<tr>
<td>PartitionNotPresent</td>
<td>Partition information is not found.</td>
<td>The image is corrupted possibly due to an incorrect image creation method.</td>
</tr>
<tr>
<td>Error Code</td>
<td>Reason</td>
<td>Recommended Solution</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------------------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>CloudInitNotInstalled</td>
<td>The cloud-init program is not installed.</td>
<td>Install cloud-init in the Linux image by referring to the Driver section in Import Preparations.</td>
</tr>
<tr>
<td>RootPartitionNotFound</td>
<td>The root partition is not found.</td>
<td>The image is corrupted possibly due to an incorrect image creation method.</td>
</tr>
<tr>
<td>InternalError</td>
<td>An internal error other than the preceding ones occurs.</td>
<td>Contact our customer service.</td>
</tr>
</tbody>
</table>
Introduction

To run in Tencent Cloud, a CVM must have a kernel supporting virtio drivers, including the block device driver `virtio_blk` and the NIC driver `virtio_net`. To ensure that a CVM created with a custom image can start up properly, please check whether your image support virtio drivers in the source server before importing the image. This document uses CentOS as an example to describe how to check if an image supports virtio drivers.

Directions

**Step 1: Checking whether the kernel supports virtio drivers**

Execute the following command to check whether the current kernel supports virtio drivers:

```
grep -i virtio /boot/config-$\(\text{uname -r}\)
```

A response similar to the following will be returned:

```
[root@VM_0_120_centos ~]\# grep -i virtio /boot/config-$\(\text{uname -r}\)
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_RANDCM_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 value of `CONFIG_VIRTIO_BLK` and `CONFIG_VIRTIO_NET` is `m` in the response, please go to **Step 2**.
If the value of `CONFIG_VIRTIO_BLK` and `CONFIG_VIRTIO_NET` is `y` in the response, which means the OS contains the virtio drivers, you can import the custom image to Tencent Cloud. For details, see Import Images > Overview.

If you cannot find `CONFIG_VIRTIO_BLK` and `CONFIG_VIRTIO_NET` in the response, it means that images with the OS cannot be imported to Tencent Cloud. Please download and compile kernel.

**Step 2: Checking whether virtio drivers are in the temporary file system**

If the value of the parameters is `m` in Step 1, you need to check whether `initramfs` or `initrd` contains the `virtio` drivers. Please execute the corresponding command according to the operating system:

- For CentOS 6/CentOS 7/RedHat 6/RedHat 7:
  ```bash
  lsinitrd /boot/initramfs-$(uname -r).img | grep virtio
  ```
- For RedHat 5/CentOS 5:
  ```bash
  mkdir -p /tmp/initrd && cd /tmp/initrd
  zcat /boot/initrd-$(uname -r).img | cpio -idmv
  find . -name "virtio*"
  ```
- For Debian/Ubuntu:
  ```bash
  lsinitramfs /boot/initrd.img-$(uname -r) | grep virtio
  ```

If a result similar to the following is returned:

![Example Result](image)

It means that `initramfs` contains the `virtio_blk` driver and `virtio.ko`, `virtio_pci.ko`, and `virtio_ring.ko` on which the driver depends. In this case, you can import the custom image to Tencent Cloud. For details, see Import Images > Overview.

If `initramfs` or `initrd` does not contain the `virtio` drivers, please go to **Step 3**.

**Step 3: Reconfigure the temporary file system**

If you find that `initramfs` or `initrd` does not contain the `virtio` drivers in [Step 2)](#CheckVirtioForInitramfs), you will need to reconfigure the temporary file system to make sure that...
initramfs or initrd contains the virtio drivers. Please execute the corresponding command according to the operating system:

- For CentOS 6/CentOS 7/RedHat 6/RedHat 7:
  
  ```bash
  cp /boot/initramfs-$(uname -r).img /boot/initramfs-$(uname -r).img.bak
  mkinitrd -f --with=virtio_blk --with=virtio_pci /boot/initramfs-$(uname -r).img $(uname -r)
  ```

- For RedHat 5/CentOS 5:
  
  ```bash
  cp /boot/initrd-$(uname -r).img /boot/initrd-$(uname -r).img.bak
  mkinitrd -f --with=virtio_blk --with=virtio_pci /boot/initrd-$(uname -r).img $(uname -r)
  ```

- For Debian/Ubuntu:
  
  ```bash
  echo -e "virtio_pci\nvirtio_blk" >> /etc/initramfs-tools/modules
  update-initramfs -u
  ```

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 view the current version of the kernel.

   ```
   uname -r
   ```

   A response similar to the following will be returned, indicating the current kernel version 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 Linux Kernel Download Page to download the source code of the corresponding kernel version.

   For example, for the 2.6.32-642.6.2.el6.x86_64 version, you should download linux-2.6.32.tar.gz at https://mirrors.edge.kernel.org/pub/linux/kernel/v2.6/linux-2.6.32.tar.gz.

4. Execute the following command to switch 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 make connection.

```
l -s linux-2.6.32 linux
```

8. Execute the following command to switch directory.

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

Compling the kernel

1. Execute the following commands to compile the kernel.

```
make mrproper
symvers_path=$(find /usr/src -name "Module.symvers")
test -f $symvers_path && cp $symvers_path .
cp /boot/config-$(uname -r) ./.config
make menuconfig
Enter the “Linux Kernel vX.X.XX Configuration” interface as shown below:  

If you are not taken to the “Linux Kernel vX.X.XX Configuration” interface, please go to [Step 18](# OptionalStep).

“Linux Kernel vX.X.XX Configuration” interface:

- Press “Tab” or “↑” “↓” 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” to enter the Virtualization details interface.
4. In the Virtualization details interface, check whether the Kernel-based Virtual Machine (KVM) support option is selected as shown below:
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 enter the Processor type and features details interface.

7. Press the "↓" key to move the cursor to "Paravirtualized guest support" and press "Enter" to enter the detailed interface of Paravirtualized guest support.

8. In the Paravirtualized guest support details interface, check whether "KVM paravirtualized clock" and "KVM Guest support" are selected as shown below:

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.
0. Press the "↓" key to move the cursor to "Device Drivers" and press "Enter" to enter the Device Drivers details interface.

1. Press the "↓" key to move the cursor to "Block devices" and press "Enter" to enter the Block devices details interface.

2. In the Block devices details interface, check whether "Virtio block driver (EXPERIMENTAL)" is selected as shown below:

   ![Block devices configuration]

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

3. Press "Esc" to return to the Device Drivers details interface.

4. Press the "↓" key to move the cursor to "Network device support" and press "Enter" to enter the Network device support details interface.

5. In the Network device support details interface, check whether "Virtio network driver (EXPERIMENTAL)" is selected as shown below:
If it is not selected, press the space bar to select the "Virtio network driver (EXPERIMENTAL)" option.

6. Press "Esc" to exit the kernel configuration interface, and select "YES" to save the `.config` file.

7. Take **Step 1: Checking whether the kernel supports the virtio drivers** to verify whether the virtio drivers have been configured correctly.

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

   This step is recommended if any of the following two is true:
   
   - The kernel still contains no configuration information related to the virtio drivers after you finish checking.
   - When compiling the kernel, you can not enter the kernel configuration interface or save the `.config` file.

   ```
   make oldconfig
   make prepare
   make scripts
   make
   make install
   ```

9. Execute the following commands to check 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 any of the commands returns a list of files such as `virtio_blk`, `virtio_pci.virtio_console`, it indicates that you have installed the virtio drivers correctly.
Installing Cloudbase-Init on Windows

Last updated: 2020-06-03 14:36:20

Overview

This document describes how to install Cloudbase-Init on the Windows Server 2012 R2 64-bit operating system.

Required Software

The following table describes the software required for installing Cloudbase-Init.

<table>
<thead>
<tr>
<th>Software</th>
<th>Download Link</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CloudbaseInitSetup_X_X_XX_xXX.msi</td>
<td>Download the Cloudbase-Init installation package based on the operating system used.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Stable version (recommended)</td>
<td>Used to install Cloudbase-Init</td>
</tr>
<tr>
<td></td>
<td>◦ Windows 64-bit operating system: Click here to download the installation package.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>◦ Windows 32-bit operating system: Click here to download the installation package.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Beta version</td>
<td></td>
</tr>
<tr>
<td></td>
<td>For details, see the Cloudbase-Init official website.</td>
<td></td>
</tr>
<tr>
<td>TencentCloudRun.ps1</td>
<td>Click here to download the installation package.</td>
<td></td>
</tr>
<tr>
<td>localscripts.py</td>
<td>Click here to download the installation package.</td>
<td>Used to ensure that Cloudbase-Init starts properly</td>
</tr>
</tbody>
</table>

Directions
Installing Cloudbase-Init

1. On the desktop, double-click the Cloudbase-Init installation package.
2. In the dialog box, click **Run** to enter the Cloudbase-Init setup wizard, as shown below:

3. Click **Next**.
4. Check **I accept the terms in the License Agreement** and click **Next** for the following two operations.
5. On the **Configuration options** page, set **Serial port for logging** to **COM1** and click **Next**, as shown below:
6. Click **Install**.

7. When the installation is completed, click **Finish** to close the Cloudbase-Init setup wizard, as shown below:

When closing the Cloudbase-Init setup wizard, do not check any checkbox or run Sysprep.
Modifying the Cloudbase-Init configuration file

1. Open the `cloudbase-init.conf` configuration file.
   - The `cloudbase-init.conf` configuration file is saved in `C:\Program Files\Cloudbase Solutions\Cloudbase-Init\conf` by default.

2. Replace content in the `cloudbase-init.conf` configuration file with the following:

   ```
   [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\mtools.exe
   metadata_services=cloudbaseinit.metadata.services.configdrive.ConfigDriveService
   plugins=cloudbaseinit.plugins.windows,extendvolumes,cloudbaseinit.plugins.common.networkconfig
   plugins.common.xen,cloudbaseinit.plugins.common.sethostname,cloudbaseinit.plugins.common.setuserpassword
   plugins.commonuserdata.UserDataPlugin
   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=false
activate_windows=true
kms_host="kms.tencentyun.com"
local_scripts_path=C:\Program Files\Cloudbase Solutions\Cloudbase-Init\LocalScripts\n
3. Copy the TencentCloudRun.ps1 script to C:\Program Files\Cloudbase Solutions\Cloudbase-Init\LocalScripts .
4. Replace localscripts.py in C:\Program Files\Cloudbase Solutions\Cloudbase-Init\Python\Lib\site-packages\cloudbaseinit\plugins\common with the localscripts.py file in Required Software.
Install Cloud-Init on Linux


Scenario

Cloud-init allows you to customize configurations during the first initialization of an instance. If the imported image does not have the cloud-init service installed, instances booted through the image cannot be initialized properly. As a result, the image fails to be imported. This document describes how to install the cloud-init service.

You can install cloud-init in two ways:

- Manually downloading the cloud-init source package
- Using the cloud-init package from the software source

Notes

Before importing a Linux image, ensure that you have properly installed the cloud-init service in the image.

Prerequisites

A server with the cloud-init service installed can correctly access external networks.

Directions

**Manually downloading the cloud-init source package**

**Downloading the cloud-init source package**

- cloud-init-17.1 is the version best compatible with Tencent Cloud. It ensures that all configuration items of CVMs created through the image can be initialized properly. We recommend that you install **cloud-init-17.1.tar.gz**. You can also [click here](#) to download other versions. This document uses cloud-init-17.1 as an example.
- If the installation fails, manually download the green cloud-init package to install the service.
Run the following command to download the cloud-init source package:

```bash
wget https://launchpad.net/cloud-init/trunk/17.1/+download/cloud-init-17.1.tar.gz
```

### Installing cloud-init

1. Run the following command to decompress the cloud-init installation package:

   ```bash
   tar -zxvf cloud-init-17.1.tar.gz
   ```

2. Run the following command to enter the decompressed cloud-init installation package directory, that is, the cloud-init-17.1 directory:

   ```bash
   cd cloud-init-17.1
   ```

3. Install Python-pip according to the operating system version.
   - For CentOS 6 or 7, run the following command:
     ```bash
     yum install python-pip -y
     ```
   - For Ubuntu, run the following command:
     ```bash
     apt-get install python-pip -y
     ```

4. Run the following command to install dependencies:

   ```bash
   pip install -r requirements.txt
   ```

5. Install the cloud-utils component according to the operating system version.
   - For CentOS 6, run the following command:
yum install cloud-utils-growpart
dracut-modules-growroot -y
dracut -f

- For CentOS 7, run the following command:
  
  yum install cloud-utils-growpart -y

- For Ubuntu, run the following command:
  
  apt-get install cloud-guest-utils -y

6. Run the following commands to install cloud-init:

```
python setup.py build
python setup.py install --init-system systemd
```

---

- Optional parameters of init-system include systemd, sysvinit, sysvinit_deb, sysvinit_freebsd, sysvinit_openrc, sysvinit_suse, and upstart [default: None]. Configure parameters based on the auto-start service management method of the operating system. If incorrect parameters are configured, the cloud-init service cannot automatically start upon system startup. This document uses the systemd self-start service management method as an example.

**Modifying the cloud-init configuration file**

1. Download cloud.cfg for your operating system.
   - Click here to download cloud.cfg for Ubuntu.
   - Click here to download cloud.cfg for CentOS.

2. Replace the content of `/etc/cloud/cloud.cfg` with that of the downloaded cloud.cfg file.

**Adding a syslog user**

Run the following command to add a syslog user:

```
useradd syslog
```

**Setting the cloud-init service to automatically start upon system startup**

- If your operating system uses systemd to manage self-start services, run the following commands.
  - Run the following command in Ubuntu or Debian:
ii. Run the following commands in all operating systems:

```bash
ln -s /usr/local/bin/cloud-init /usr/bin/cloud-init

systemctl enable cloud-init-local.service
systemctl start cloud-init-local.service
systemctl enable cloud-init.service
systemctl start cloud-init.service
systemctl enable cloud-config.service
systemctl start cloud-config.service
systemctl enable cloud-final.service
systemctl start cloud-final.service
systemctl status cloud-init-local.service
systemctl status cloud-init.service
systemctl status cloud-config.service
systemctl status cloud-final.service
```

iii. Run the following command in CentOS or Redhat.

Replace the content of `/lib/systemd/system/cloud-init-local.service` with the following:

```ini
[Unit]
Description=Initial cloud-init job (pre-networking)
Wants=network-pre.target
After=systemd-remount-fs.service
Before=NetworkManager.service
Before=network-pre.target
Before=shutdown.target
Conflicts=shutdown.target
RequiresMountsFor=/var/lib/cloud

[Service]
Type=oneshot
ExecStart=/usr/bin/cloud-init init --local
ExecStart=/bin/touch /run/cloud-init/network-config-ready
RemainAfterExit=yes
TimeoutSec=0
# Output needs to appear in instance console output
StandardOutput=journal+console

[Install]
WantedBy=cloud-init.target
```

Replace the content of `/lib/systemd/system/cloud-init.service` with the following:

```ini
[Unit]
Description=Initial cloud-init job (metadata service crawler)
Wants=cloud-init-local.service
Wants=sshd-keygen.service
Wants=sshd.service
```

©2013-2019 Tencent Cloud. All rights reserved.
### Cloud Virtual Machine

**After**=cloud-init-local.service
**After**=systemd-networkd-wait-online.service
**After**=networking.service
**After**=systemd-hostnamed.service
**Before**=network-online.target
**Before**=sshd-keygen.service
**Before**=sshd.service
**Before**=systemd-user-sessions.service
**Conflicts**=shutdown.target

[Service]
**Type**=oneshot
**ExecStart**=/usr/bin/cloud-init init
**RemainAfterExit**=yes
**TimeoutSec**=0

# Output needs to appear in instance console output
**StandardOutput**=journal+console

[Install]
**WantedBy**=cloud-init.target

- If your operating system uses sysvinit to manage self-start services, run the following commands:

    ```
    chkconfig --add cloud-init-local
    chkconfig --add cloud-init
    chkconfig --add cloud-config
    chkconfig --add cloud-final
    chkconfig cloud-init-local on
    chkconfig cloud-init on
    chkconfig cloud-config on
    chkconfig cloud-final on
    ```

### Using the cloud-init package from the software source

#### Installing cloud-init

Run the following command to install cloud-init:

```
apt-get/yum install cloud-init
```
initialized as expected. Therefore, we recommend that you install the service by manually downloading the cloud-init source package.

Modifying the cloud-init configuration file

1. Download cloud.cfg for your operating system.
   - Click here to download cloud.cfg for Ubuntu.
   - Click here to download cloud.cfg for CentOS.
2. Replace the content of /etc/cloud/cloud.cfg with that of the downloaded cloud.cfg file.

Relevant Operations

Do not restart the server after performing the following operations. Otherwise, you need to perform them again.

1. Run the following commands to check whether the cloud-init configuration is successful:
   
   ```
   cloud-init init --local
   rm -rf /var/lib/cloud
   ```

2. Run the following command in Ubuntu or Debian:

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

3. For Ubuntu or Debian, replace the content of /etc/network/interfaces with the following:

   ```
   # 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/*
   ```

Appendix

Manually downloading the green cloud-init package

If the cloud-init service fails to be installed by manually downloading the cloud-init source package, complete the following steps to install cloud-init:

1. Click here to obtain the green cloud-init package.
2. Run the following command to decompress the green cloud-init package:
3. Run the following command to enter the decompressed green cloud-init package directory, that is, the greeninit directory:

   ```bash
cd greeninit
   ```

4. Run the following command to install cloud-init:

   ```bash
sh install.sh
   ```
Forcibly Import Image

Last updated: 2020-04-27 14:46:37

Scenario

If you cannot install cloudinit in your Linux image, use Forced Image Import to import the image. If you use this image for import, which does not have cloudinit installed, Tencent Cloud cannot initialize your CVM. In this case, you need to set up the script on your own to configure the CVM based on the configuration file provided by Tencent Cloud. This document describes how to configure the CVM if the image is forcibly imported.

Tencent Cloud provides the user with CDROM device containing the configuration information. The user needs to mount CDROM and read the information of `mount_point/qcloud_action/os.conf` for configuration. If other configuration data or UserData needs to be used, the user can directly read files under `mount_point/`.

os.conf Configuration File

The content of os.conf is as follows.

```plaintext
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"
```

The parameter names above are for reference, and the values are used as examples only.

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

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hostname</td>
<td>CVM name</td>
</tr>
<tr>
<td>password</td>
<td>Encrypted password</td>
</tr>
</tbody>
</table>
### Parameter Name | Description
---|---
eth0_ip_addr | LAN IP of eth0
eth0_mac_addr | MAC address of eth0
eth0_netmask | Subnet mask of eth0
eth0_gateway | Gateway of eth0
dns_nameserver | DNS resolution server

### Limits
- The image must meet the limits on Linux images as outlined in Import Images, except for cloudinit.
- The system partition for importing the image is not full.
- The imported image contains no vulnerability that can be exploited remotely.
- We recommend you change the password immediately after the instance is created successfully with the forcibly imported image.

### Notes
Note the following when configuring script parsing:
- The script is executed automatically at startup. Please implement this requirement based on your operating system.
- Mount `/dev/cdrom` and read `os_action/os.conf` file under the mount point to obtain the configuration information.
- The password placed in CDROM by Tencent Cloud is encrypted. You can set new password with `chpasswd -e`.
- *Note that the encrypted password may contain special characters. We recommend you place it in a file and then set the password with `chpasswd -e < passwd_file`.*
- When you use the forcibly imported image to create an instance and then create an image, you need to ensure that the script will still be executed to ensure that the instance is configured correctly. You can also install cloudinit in this instance.

### Directions
Tencent Cloud provides a script sample based on CentOS. You can refer to it to create script for your images. During the creation, note that:

- **The script must be properly placed in the system before image import.**
- The script is not applicable to all operating systems. You need to modify it according to your own operating systems.

1. Create an `os_config` script based on the following script sample.

   You can modify the script as needed.

```bash
#!/bin/bash
### BEGIN INIT INFO
# Provides: os-config
# Required-Start: $local_fs $network $named $remote_fs
# Required-Stop:
# Should-Stop:
# Default-Start: 2 3 4 5
# Default-Stop: 0 1 6
# Short-Description: config of os-init job
# Description: run the config phase without cloud-init
### END INIT INFO

###################user settings#####################
cdrom_path=`blkid -L config-2`
load_os_config() {
  mount_path=$(mktemp -d /mnt/tmp.XXXX)
  mount /dev/cdrom $mount_path
  if [[ -f $mount_path/qcloud_action/os.conf ]]; then
    $mount_path/qcloud_action/os.conf
    if [[ -n $password ]]; then
      passwd_file=$(mktemp /mnt/pass.XXXX)
      passwd_line=$(grep password $mount_path/qcloud_action/os.conf)
      echo root:${passwd_line#*=} > $passwd_file
      fi
      return 0
    else
      return 1
    fi
  }
  cleanup() {
    umount /dev/cdrom
    if [[ -f $passwd_file ]]; then
      echo $passwd_file
      rm -f $passwd_file
      fi
```
if [[ -d $mount_path ]]; then
echo $mount_path
rm -rf $mount_path
fi
}
config_password() {
if [[ -f $passwd_file ]]; then
chpasswd -e < $passwd_file
fi
}
config_hostname() {
if [[ -n $hostname ]]; then
sed -i "/^HOSTNAME=.*/d" /etc/sysconfig/network
echo "HOSTNAME=$hostname" >> /etc/sysconfig/network
fi
}
config_dns() {
if [[ -n $dns_nameserver ]]; then
dns_conf=/etc/resolv.conf
sed -i '/^nameserver.*/d' $dns_conf
for i in $dns_nameserver; do
echo "nameserver $i" >> $dns_conf
done
fi
}
config_network() {
/etc/init.d/network stop
cat << EOF > /etc/sysconfig/network-scripts/ifcfg-eth0
DEVICE=eth0
IPADDR=$eth0_ip_addr
NETMASK=$eth0_netmask
HWADDR=$eth0_mac_addr
ONBOOT=yes
GATEWAY=$eth0_gateway
BOOTPROTO=static
EOF
if [[ -n $hostname ]]; then
sed -i "/$eth0_ip_addr.*/d" /etc/hosts
echo "$eth0_ip_addr $hostname" >> /etc/hosts
fi
/etc/init.d/network start
}
config_gateway() {
sed -i "s/GATEWAY=.*/GATEWAY=$eth0_gateway" /etc/sysconfig/network
}

###########################init###########################
start() {
if load_os_config ; then
config_password
config_hostname
config_dns
config_network
cleanup
exit 0
else
echo "mount ${cdrom_path} failed"
exit 1
fi

RETVAL=0
case "$1" in
  start)
    start
    RETVAL=$?
  ;;
  *)
    echo "Usage: $0 {start}"
    RETVAL=3
  ;;
esac
exit $RETVAL

2. Place the `os_config` script in the `/etc/init.d/` directory and 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 service.

    chkconfig --list

You must ensure that the script is correctly executed. If you fail to connect to the instance via SSH or network exception occurs after the image import, try to connect to the instance via the console to execute the script again. If such problems remain, contact the customer service.
Linux Image Creation

Last updated: 2020-05-08 12:35:18

Scenario

This document describes how to create a Linux image.

Directions

Preparations

Before creating and exporting a system disk image, complete the following checks.

If you need to prepare and export a data disk image, skip this operation.

Checking the partitioning mode and launch mode of the operating system

1. Run the following command to check whether the operating system partition is a GPT partition.

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

   - If the returned result is msdos, the partition is an MBR partition. In this case, go to the next step.
   - If the returned result is gpt, the partition is a GPT partition. Currently, service migration does not support GPT partitions. In this case, submit a ticket.

2. Run the following command to check whether the operating system launch mode is EFI.

   ```bash
   sudo ls /sys/firmware/efi
   ```

   - If the EFI file exists, the current launch mode is EFI. In this case, submit a ticket.
   - If the EFI file does not exist, proceed to the next step.

Checking system-critical files

System-critical files to be checked include but are not limited to:

Follow the standards of relevant distributions to ensure that the locations and permissions of the system-critical files are correct and that the files can be read and written normally.
• /etc/grub/grub.cfg: in the kernel parameter, uuid is recommended for mounting root. Other methods (such as root=/dev/sda) may cause failure in launching the system.
• /etc/fstab: do not mount other disks. After migration, the system may fail to start due to disk missing.
• /etc/shadow: it has appropriate permissions and can be read and written.

Unmounting software programs

Unmount the drivers and software that incur conflicts (including VMWare tools, Xen tools, Virtualbox GuestAdditions, and other software that comes with underlying drivers).

Checking the virtio driver

For more information, see Checking the Virtio Driver in the Linux System.

Installing cloud-init

For more information, see Installing cloud-init in the Linux System.

Checking other hardware-related configurations

After the migration to the cloud, changes to the hardware include but are not limited to:

• Replaces the graphics card with Cirrus VGA.
• Replaces the disk with Virtio Disk. The device name is vda or vdb.
• Replaces the ENI with Virtio Nic. By default, only eth0 is available.

Querying partitions and their sizes

Run the following command to query the current partition format of the operating system and determine the partitions to be copied and their sizes.

```
mount
```

The returned result is similar to the following:

```
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)
```
From the result, you can see the root partition resides in /dev/sda1, no independent partitions reside in /boot or /home, sda1 contains the boot partition, and mbr is missing. Therefore, we only need to copy the entire sda.

The exported image should contain at least the root partition and mbr. If the exported image lacks mbr, it cannot be launched.

In the current operating system, if /boot and /home are independent partitions, the exported image also needs to include both independent partitions.

Exporting an image

You can select different methods to export an image based on your actual requirements.

- Export by using tools
- Export by running commands
Exporting an image by using a platform tool

For more information on how to use image export tools of VMWare vCenter Convert, Citrix XenConvert, and other virtualization platforms, see the document for the respective platform. Image formats supported by Tencent Cloud Service Migration are qcow2, vhd, raw, and vmdk.

Exporting an image by running commands

Manual export with commands poses a high risk. (For example, the file system's metadata may be corrupted when I/O is busy.) We recommend that you check the image to make sure that the image is intact and correct after it is exported.

You can use the following commands to export an image:

- **Use the `qemu-img` command**
  For example, run the following command to export /dev/sda to /mnt/sdb/test.qcow2.
  
  ```bash
  sudo qemu-img convert -f raw -O qcow2 /dev/sda /mnt/sdb/test.qcow2
  ```

  In this command, /mnt/sdb indicates the mounted new disk or another network storage. To convert it to other formats, change the value of `-O`. Supported values are described as follows:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>qcow2</td>
<td></td>
<td>qcow2 format</td>
</tr>
<tr>
<td>vpc</td>
<td></td>
<td>vhd format</td>
</tr>
<tr>
<td>vmdk</td>
<td></td>
<td>vmdk format</td>
</tr>
<tr>
<td>raw</td>
<td></td>
<td>No format</td>
</tr>
</tbody>
</table>

- **Use the `dd` command**
  For example, run the following command to export the image in raw format.
  
  ```bash
  sudo dd if=/dev/sda of=/mnt/sdb/test.imag bs=1K count=$count
  ```
The `count` parameter specifies the number of partitions to be copied, which can be queried by running the `fdisk` command. To copy all partitions, ignore the `count` parameter.

For example, run the following command to view the number of partitions of `/dev/sda`.

```
fdisk -lu /dev/sda
```

A result similar to 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
```

From the returned result of the `fdisk` command, you can see that sda1 ends at 41945087 * 512 bytes, so set `count` to 20481M.

The image exported by using `dd` is in raw format. We recommend that you convert the format to qcow2, vhd, or other image formats.

**Converting the image format**

At present, Tencent Cloud service migration supports image formats of qcow2, vhd, vmdk, and raw. We recommend that you use a compressed image format to accelerate the transmission and migration.

Convert the image format by using the `qemu-img` command:

For example, run the following command to convert the image from the raw format to the qcow2 format.
sudo qemu-img convert -f raw -O qcow2 test.img test.qcow2

- `-f` indicates the source image format.
- `-O` indicates the target image format. For the supported formats, see `-O` parameter values.

Checking the image

The image file system that you create may be corrupted if you create the image without stopping the service or due to other reasons. Therefore, we recommend that you check the image after creating it.

If the image format is supported by the current platform, you can directly open the image to check the file system. For example, the Windows platform supports VHD images, the Linux platform allows you to use qemu-nbd to open QCOW2 images, and the Xen platform allows you to directly open VHD files.

Take the Linux platform as an example:

```
modprobe nbd
qemu-nbd -c /dev/nbd0 xxxx.qcow2
mount /dev/nbd0p1 /mnt
```

If the file system is corrupted when the first partition of the qcow2 image is exported, an error occurs when you use the mount command.

In addition, you can launch the CVM to check whether the image file works before uploading the image.
Windows Image Creation

Last updated : 2020-06-12 16:02:33

Scenario

This document describes how to prepare a Windows image by using the Windows Server 2012 operating system as an example.

Directions

Preparations

Before preparing and exporting a system disk image, complete the following checks.

If you need to prepare and export a data disk image, skip this operation.

Check the partitioning mode and launch mode of the operating system

1. In the operating system, click to open the “Windows PowerShell” window.
2. In the “Windows PowerShell” window, enter `gpedit.msc` and press Enter to go to “Disk Management”.
3. Right-click the disk to check, choose Properties, click the Volume tab, and check the disk partitioning mode.
4. Check whether the disk partitioning mode is GPT.
   ○ If yes, submit a ticket because service migration currently does not support the GPT partition.
   ○ If no, proceed with the next step.
5. Start CMD as admin, and run the following command to check whether the operating system launches in EFI mode:

   ```
   bcedit /enum {current}
   ```

   The return result is similar to the following:

   ```
   Windows boot loader
   ID {current}
   device partition=C:
   path %WINDIR%/system32/winload.exe
   description Windows 10
   ```

©2013-2019 Tencent Cloud. All rights reserved.
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 contains "efi", the operating system starts in EFI mode. In this case, submit a ticket.
- If path does not contain "efi", proceed with the next step.

Unmounting software
Unmount the drivers and software programs (including VMware tools, Xen tools, Virtualbox GuestAdditions, and other software that comes with underlying drivers) that produce conflicts.

Installing cloud-base
Install cloud-base by referring to Installing cloud-base.

Checking or installing the virtIO driver
1. Choose Control Panel > Programs and Features, and enter "Virtio" in the search box.
If the result shown in the following figure is returned, the virtIO driver has been installed.

If the virtIO driver is not installed, manually install the virtIO driver.
- For other operating system versions, download [virtIO for Community](#).

### Checking other hardware-related configurations

After the migration to the cloud, hardware changes include but are not limited to:
- The graphic card is changed to Cirrus VGA.
- The disk is changed to Virtio Disk.
- The ENI is changed to Virtio Nic, and Local Area Connection is used by default.

### Exporting an image

You can select different tools to export an image based on your actual requirements.
- Use a platform tool to export an image
- Use disk2vhd to export an image
Using a platform tool to export an image

For more information on how to use the image export tools of virtualization platforms, such as VMWare vCenter Convert and Citrix XenConvert, see the document for the respective platform.

Tencent Cloud supports the following image formats for service migration: QCOW2, VHD, RAW, and VMDK.

Using Disk2vhd to export an image

To export the system on a physical machine or if you do not want to use a platform tool to export an image, use Disk2vhd instead.

1. Install and start the Disk2vhd tool.
   [Click here to download Disk2vhd.]

2. Select the storage path of the image to export, select the volumes to copy, and click Create, as shown in the following figure.

   - Disk2vhd can be started only after the Volume Shadow Copy Service (VSS) is installed in the Windows system.
   - Do not select "Use Vhdx" because the system currently does not support images in VHDX format.
   - We recommend that you select "Use volume Shadow Copy" to better ensure data integrity.
Checking the image

The image file system that you prepare may be corrupted because you prepared the image without stopping the service or due to other reasons. Therefore, we recommend that you check the image after preparing it.

If the image format is supported by the current platform, you can directly open the image to check the file system. For example, the Windows platform supports the VHD image, the Linux platform allows you to run qemu-nbd to open QCOW2 images, and the Xen platform allows you to directly open VHD files.

Take the Linux platform as an example:

```
modprobe nbd
qemu-nbd -c /dev/nbd0 xxxx.qcow2
mount /dev/nbd0p1 /mnt
```

If the file system is corrupted when the first partition of the QCOW2 image is exported, an error occurs when you run the `mount` command.

You can also launch the CVM to check whether the image file works before uploading the image.
Online migration is a service migration method that can migrate systems and applications on source servers from your own IDC or cloud platform to Tencent Cloud. It meets service requirements for enterprise cloudification, migration across cloud platforms, migration across accounts or regions, and hybrid cloud deployment.

Here, the source server can be a physical server, a virtual machine, or even a cloud server on another cloud platform, such as AWS, Microsoft Azure, Google Cloud Platform, Alibaba Cloud, or Huawei Cloud.

Scenarios

Online migration is applicable to the following scenarios:

- IT architecture cloudification
- Hybrid cloud architecture deployment
- Cross-cloud migration
- Cross-account or cross-region migration

Differences from Offline Migration

In offline migration, system disks or data disks on the source server are made into an image, and then the image is migrated to your designated Cloud Virtual Machine (CVM) or Cloud Block Storage (CBS). In contrast, the preparation of images is not required for online migration. Instead, you only need to run the migration tool on the source server to migrate the source server to your designated CVM.

Features
Currently, online migration supports the server migration feature.

Preparations

- Register a Tencent Cloud account and prepare the destination CVM.
- Stop applications on the source server to avoid potential impact from migration on existing applications.
  
  Click here to download the compressed migration tool package.

FAQs

For more information, see About Service Migration.
Online Migration Tool

Last updated : 2020-05-13 16:54:06

Overview

Online migration refers to migrating or synchronizing the system and applications on the server or virtual machine from your own IDC, cloud platform, or other source environments to Tencent Cloud without interrupting the system.

Tencent Cloud provides the migration tool go2tencentcloud. After you run the migration tool on the source server, the entire source server can be migrated to the destination Cloud Virtual Machine (CVM) on Tencent Cloud. With this migration tool, you do not need to prepare, upload, or import images. Instead, the source server is directly migrated onto the cloud, which meets service requirements for enterprise cloudification, migration across cloud platforms, migration across accounts or regions, and hybrid cloud deployment.

Migration Tool

Supported migration modes

Default mode

If both your source server and destination CVM can access the public network, you can adopt the default migration mode.

In the current default mode, the source server calls Tencent Cloud APIs through the Internet to
initiate a migration request, and transfers data to the destination CVM to complete the migration.

**Private network migration mode**

If your source server or destination CVM is located in a private network or Virtual Private Cloud (VPC) instance, the source server cannot directly establish a connection with the destination CVM through the Internet. In this case, you can adopt the private network migration mode of the tool. If this migration mode is used, you need to establish a connection between the source server and destination CVM by using **VPC Peering Connection**, **VPN Connection**, **Cloud Connect Network**, or **Direct Connect**.

- Scenario 1: if your source server or destination CVM cannot access the public network, use a server (such as the gateway) that can access the public network to call Tencent Cloud APIs through the Internet to initiate a migration request. Then, transfer data to the destination CVM through the connection to complete the migration. In this scenario, both the source server and
destination CVM do not need to be able to access the public network.

- Scenario 2: if your source server can access the public network, use the source server to call Tencent Cloud APIs through the Internet to initiate a migration request. Then, transfer data to the destination CVM through the connection to complete the migration. In this scenario, the source server must be able to access the public network, but the destination CVM does not need to have this capability.

- Scenario 3: if your source server can access the public network through a proxy, use the source server to call Tencent Cloud APIs through the network proxy to initiate a migration request. Then, transfer data to the destination CVM through the connection to complete the migration. In this scenario, both the source server and destination CVM do not need to be able to access the public network.
Supported operating systems

Operating systems supported by the online migration tool include but are not limited to the following (32-bit or 64-bit):

<table>
<thead>
<tr>
<th>Linux</th>
<th>Windows</th>
</tr>
</thead>
<tbody>
<tr>
<td>CentOS 5/6/7</td>
<td></td>
</tr>
<tr>
<td>Ubuntu 10/12/14/16/18</td>
<td></td>
</tr>
<tr>
<td>Debian 7/8/9</td>
<td></td>
</tr>
<tr>
<td>SUSE 11/12/15</td>
<td></td>
</tr>
<tr>
<td>openSUSE 42</td>
<td>-</td>
</tr>
<tr>
<td>Amazon Linux AMI</td>
<td></td>
</tr>
<tr>
<td>Red Hat 7/8</td>
<td></td>
</tr>
</tbody>
</table>

Files in the compressed package

<table>
<thead>
<tr>
<th>File Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>go2tencentcloud_x64</td>
<td>Executable program of the migration tool for the 64-bit Linux operating system</td>
</tr>
<tr>
<td>go2tencentcloud_x32</td>
<td>Executable program of the migration tool for the 32-bit Linux operating system</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>user.json</td>
<td>Configuration file of the source server and destination CVM during the migration. You need to modify the settings in the file based on the description of parameters in the user.json file.</td>
</tr>
<tr>
<td>client.json</td>
<td>Configuration file of the migration tool. You need to modify the settings in the file based on the description of parameters in the client.json file.</td>
</tr>
<tr>
<td>rsync_excludes_linux.txt</td>
<td>rsync configuration file, which excludes the files and directories that do not need to be migrated in the Linux system</td>
</tr>
</tbody>
</table>

The configuration files cannot be deleted. You must store these files under the same folder as the go2tencentcloud executable program.

- Description of parameters in the user.json file:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SecretId</td>
<td>String</td>
<td>Yes</td>
<td>Secret ID used by your account to access APIs. For more information, see Access Keys.</td>
</tr>
<tr>
<td>SecretKey</td>
<td>String</td>
<td>Yes</td>
<td>Secret key used by your account to access APIs. For more information, see Access Keys.</td>
</tr>
<tr>
<td>Region</td>
<td>String</td>
<td>Yes</td>
<td>Region of the destination CVM. You only need to specify the region, but not the availability zone. For more information on values, see the region list.</td>
</tr>
<tr>
<td>InstanceId</td>
<td>String</td>
<td>Yes</td>
<td>Instance ID of the destination CVM. The ID format is <code>ins-xxxxxxxxxx</code>.</td>
</tr>
<tr>
<td>DataDisks</td>
<td>Array</td>
<td>No</td>
<td>List of data disks to be migrated from the source server. Each entry represents one data disk, and up to 20 data disks are supported.</td>
</tr>
<tr>
<td>DataDisks.Index</td>
<td>Integer</td>
<td>Yes</td>
<td>Serial number of the data disk on the source server. Value range: [1,20]. The value 1 indicates that this data disk will be migrated to the first data disk on the destination CVM.</td>
</tr>
<tr>
<td>Field</td>
<td>Type</td>
<td>Required</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------</td>
<td>----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>DataDisks.Size</td>
<td>Integer</td>
<td>Yes</td>
<td>Size of the data disk on the source server, Unit: GB. Value range: [10,16000].</td>
</tr>
<tr>
<td>DataDisks.MountPoint</td>
<td>String</td>
<td>Yes</td>
<td>Mount target of the data disk on the source server, for example, &quot;/mnt/disk1&quot;.</td>
</tr>
</tbody>
</table>

Example 1: to migrate a source Linux server to a CVM located in Guangzhou, configure the user.json file as follows:

```json
{
  "SecretId": "your secretId",
  "SecretKey": "your secretKey",
  "Region": "ap-guangzhou",
  "InstanceId": "your instance id"
}
```

You need to replace the parameter values with the actual values.

Example 2: a source Linux server has one data disk, the mount target is `/mnt/disk1`, and the size of the data disk is 10 GB. To migrate this server to a CVM located in Guangzhou, configure the user.json file as follows:

```json
{
  "SecretId": "your secretId",
  "SecretKey": "your secretKey",
  "Region": "ap-guangzhou",
  "InstanceId": "your instance id",
  "DataDisks": [
    {
      "Index": 1,
      "Size": 10,
      "MountPoint": "/mnt/disk1"
    }
  ]
}
```

You need to replace the parameter values with the actual values.
• Description of parameters in the client.json file:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client.Net.Mode</td>
<td>Integer</td>
<td>Yes</td>
<td>Default value: 0. Valid values: 0 (default mode), 1 (private network migration mode: scenario 1), 2 (private network migration mode: scenario 2), 3 (private network migration mode: scenario 3). Choose a value based on your actual migration mode or scenario.</td>
</tr>
<tr>
<td>Client.Net.Proxy.Ip</td>
<td>String</td>
<td>No</td>
<td>IP address of the network proxy. If you select private network migration mode: scenario 3, this parameter must be specified.</td>
</tr>
<tr>
<td>Client.Net.Proxy.Port</td>
<td>Integer</td>
<td>No</td>
<td>Port of the network proxy. If you select private network migration mode: scenario 3, this parameter must be specified.</td>
</tr>
<tr>
<td>Client.Net.Proxy.User</td>
<td>String</td>
<td>No</td>
<td>Username of the network proxy. If you select private network migration mode: scenario 3, and the network proxy needs to be authenticated, this parameter must be specified.</td>
</tr>
<tr>
<td>Client.Net.Proxy.Password</td>
<td>String</td>
<td>No</td>
<td>Password of the network proxy. If you select private network migration mode: scenario 3, and the network proxy needs to be authenticated, this parameter must be specified.</td>
</tr>
<tr>
<td>Client.Extra.IgnoreCheck</td>
<td>Bool</td>
<td>No</td>
<td>Default value: false. When started, the migration tool automatically checks the environment of the source server. To skip this check, set this parameter to true.</td>
</tr>
</tbody>
</table>

• Description of the rsync_excludes_linux.txt file:

This file is used to exclude files or configuration files under specified directories on the source Linux server, which do not need to be migrated. By default, the rsync_excludes_linux.txt file already excludes the following directories and files. **Do not delete or modify these settings.**
To exclude other directories or files, append them to the `rsync_excludes_linux.txt` file. For example, to exclude all the content of the data disk mounted on `/mnt/disk1`, configure the `rsync_excludes_linux.txt` file as follows:

```
/dev/*
/sys/*
/proc/*
/var/cache/yum/*
/lost+found/*
/var/lib/lxcfs/*
/var/lib/docker-storage.btrfs/root/.local/share/gvfs-metadata/*
/mnt/disk1/*
```

---

### Parameters of the migration tool

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>--help</code></td>
<td>Prints help information.</td>
</tr>
<tr>
<td><code>--check</code></td>
<td>Checks the source server without performing migration.</td>
</tr>
<tr>
<td><code>--log-file</code></td>
<td>Sets the log file name, which is <code>log</code> by default.</td>
</tr>
<tr>
<td><code>--log-level</code></td>
<td>Sets the log output level. Valid values: 1 (ERROR level), 2 (INFO level), and 3 (DEBUG level). Default value: 2.</td>
</tr>
<tr>
<td><code>--clean</code></td>
<td>Enables the destination CVM to forcibly exit the migration mode and cleanse the site. For example, if <code>Please execute '--clean' option manually.</code> appears in the console, you need to specify this parameter and run the tool so that the destination CVM exits the migration mode.</td>
</tr>
<tr>
<td><code>--version</code></td>
<td>Prints the version number.</td>
</tr>
</tbody>
</table>
## Pre-Migration Checks

Before migration, check the following items of the source server and destination CVM:

<table>
<thead>
<tr>
<th>Destination CVM</th>
<th>1. Storage: the cloud disks of the destination CVM, including system disks and data disks. Verify that they have sufficient storage to store the data from the source server.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2. Security group: ports 443 and 80 must be open in a security group.</td>
</tr>
<tr>
<td></td>
<td>3. Bandwidth: it is recommended that you increase the bandwidth for faster migration. The traffic consumed during migration will be approximately equal to the data volume. Change your networking billing method in advance if needed.</td>
</tr>
<tr>
<td></td>
<td>4. Operating system: it is recommended that the destination CVM and the source server use the same operating system. Different operating systems will result in inconsistency between the image that will be created later and the actual operating system. For example, when migrating a source server with the CentOS 7 system installed, choose a CVM with the CentOS 7 system installed as the migration destination.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Linux source server</th>
<th>1. Check for and install virtIO. For more information, see <a href="#">Checking VirtIO Drivers in Linux</a>.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2. Check whether rsync and grub2-install (or grub-install) are installed.</td>
</tr>
<tr>
<td></td>
<td>3. Check whether SELinux is enabled. Disable SELinux if it is enabled.</td>
</tr>
<tr>
<td></td>
<td>4. When a migration request is sent to the Tencent Cloud API, the API checks the generated token based on the current UNIX time. In this case, ensure that the current system time is correct.</td>
</tr>
</tbody>
</table>

You can use tool commands to automate the checks of the source server, for example,

```
sudo ./go2tencentcloud_x64 --check
```

By default, the go2tencentcloud migration tool automatically performs checking when it is started. To skip the checks and directly perform migration, set the `Client.Extra.IgnoreCheck` field to `true` in the client.json file.

## Migration Directions

If you use go2tencentcloud provided by Tencent Cloud for migration, the entire migration process is done in three stages. You can learn the migration progress from the tool when the tool is running.

- **Stage 1**: initialize the remote instance.
- **Stage 2**: transfer data.
Stage 3: release the remote instance.

In each stage, some subtasks are generated to execute related operations. Some time-consuming subtasks also have the maximum timeout by default. The time required for data transfer depends on the size of the data on the source server and the network bandwidth. The migration tool supports resumable data transfer.

After the migration starts, the destination CVM enters the migration mode. Therefore, do not perform the following operations on the destination CVM until the migration is completed and the destination CVM exits the migration mode: system reinstallation, shutdown, termination, and password resetting.

Migration directions in default mode

1. In the user.json file, configure the source server and destination CVM for the migration. Configure the required parameters based on the description of parameters in the user.json file.
2. In the client.json file, configure the migration mode and other parameters. Set Client.Net.Mode in the client.json file to 0, that is, select the default mode. If necessary, configure other parameters based on the description of parameters in the client.json file.
3. (Optional) Exclude files and directories on the source server that do not need to be migrated. When migrating the source Linux server, if you need to exclude some files and directories that do not need to be migrated, append them to the rsync_excludes_linux.txt file.
4. Run the tool.
   For example, on a 64-bit Linux source server, run the following command as the root user to run the tool.
   
   ```
   sudo ./go2tencentcloud_x64
   ```

   To set the log file name and log output level when running the tool, run the following command:

   ```
   sudo ./go2tencentcloud --log-file=my.log --log-level=3
   ```

   Wait for the migration process to complete.
   If the migration succeeds in default mode, the console output is as follows:
Migration directions in private network migration mode

Scenario 1

1. Establish a connection between the source server and the destination CVM.
   Establish a connection between the source server and the destination CVM by using VPC Peering Connection, VPN connection, or CCN.

2. In the user.json file, configure the source server and destination CVM for the migration.
   Configure the required parameters based on the description of parameters in the user.json file.

3. In the client.json file, configure the migration mode and other parameters.
   Set `Client.Net.Mode` in the client.json file to 1, that is, select private network migration mode: scenario 1. If necessary, configure other parameters based on the description of parameters in the client.json file.

4. (Optional) Exclude files and directories on the source server that do not need to be migrated.
   When migrating the source Linux server, if you need to exclude some files and directories that do not need to be migrated, append them to the `rsync_excludes_linux.txt` file.

5. Run the tool on a server (such as the gateway) that can access the public network.
   For example, on a server that can access the public network, run the following command to run the tool for migration stage 1.

   ```bash
   sudo ./go2tencentcloud_x64
   ```
If the Stage 1 is finished and please run next stage at source machine prompt appears, stage 1 is completed.

6. Run the tool on the source server.

After step 5 (stage 1) is completed, copy the entire tool directory in stage 1 to the source server, and then run the tool for migration stage 2.

Run the following command to run the tool for migration stage 2.

```
sudo ./go2tencentcloud_x64
```

If the Stage 2 is finished and please run next stage at gateway machine prompt appears, stage 2 is completed.

7. Run the tool on a server (such as the gateway) that can access the public network.

After step 6 (stage 2) is completed, copy the entire tool directory in stage 2 to the source server in stage 1, and then run the tool for migration stage 3.

Run the following command to run the tool for migration stage 3.

```
sudo ./go2tencentcloud_x64
```
If the **Migrate successfully** prompt appears, the entire migration task is completed.

```
[root@M_0_12_centos go2tencentcloud]# sudo ./go2tencentcloud_x64
[2019-09-23 11:30:08] Start go2tencentcloud 1.3.0
[2019-09-23 11:30:08] Load user.json successfully.
```

**Scenario 2**

1. Establish a connection between the source server and the destination CVM.
   Establish a connection between the source server and the destination CVM by using **VPC Peering Connection, VPN connection, or CCN**.

2. In the `user.json` file, configure the source server and destination CVM for the migration.
   Configure the required parameters based on the **description of parameters in the user.json file**.

3. In the `client.json` file, configure the migration mode and other parameters.
   Set `Client.Net.Mode` in the `client.json` file to **2**, that is, select **private network migration mode: scenario 2**. If necessary, configure other parameters based on the **description of parameters in the client.json file**.

4. (Optional) Exclude files and directories on the source server that do not need to be migrated.
   When migrating the source Linux server, if you need to exclude some files and directories that do not need to be migrated, append them to the **rsync_excludes_linux.txt file**.

5. Run the tool.
   For example, on a 64-bit Linux source server, run the following command as the root user to run the tool.
   ```
   sudo ./go2tencentcloud_x64
   ```

   Wait for the migration process to complete.

   If the migration is successful, the following console output appears:
Scenario 3

1. Establish a connection between the source server and the destination CVM.
   
   Establish a connection between the source server and the destination CVM by using VPC Peering Connection, VPN connection, or CCN.
   
2. In the user.json file, configure the source server and destination CVM for the migration.
   
   Configure the required parameters based on the description of parameters in the user.json file.
   
3. In the client.json file, configure the migration mode and other parameters.
   
   i. Set Client.Net.Mode in the client.json file to 3, that is, select private network migration mode: scenario 3.
   
       
       If your network proxy needs to be authenticated, enter the username and password of the network proxy for Client.Net.Proxy.User and Client.Net.Proxy.Password, respectively. If authentication is not needed, you can ignore both parameters. If necessary, you can configure other parameters based on the description of parameters in the client.json file.
   
4. (Optional) Exclude files and directories on the source server that do not need to be migrated.

   When migrating the source Linux server, if you need to exclude some files and directories that do not need to be migrated, append them to the rsync_excludes_linux.txt file.
5. Run the tool.

For example, on a 64-bit Linux source server, run the following command as the root user to run the tool.

```bash
sudo ./go2tencentcloud_x64
```

Wait for the migration process to complete.

If the migration is successful, the following console output appears:

```
[root@VM_0_7_centos go2tencentcloud]# sudo ./go2tencentcloud_x64
[2019-09-25 21:06:08] Start go2tencentcloud 1.3.0
[2019-09-25 21:06:09] [1/3] Initialize instance
[2019-09-25 21:06:10] Restart remote instance...
Used: 00:01:16 | Max Timeout: 00:10:00
[2019-09-25 21:07:27] Start preparing remote server...
[2019-09-25 21:07:27] Start initializing remote server...
Used: 00:00:11 | Max Timeout: 00:03:00
[2019-09-25 21:07:39] Transmitting files...
[2019-09-25 21:10:19] Reconfigure remote instance...
Used: 00:00:09 | Max Timeout: 00:05:00
```

### Post-Migration Checks

1. If the migration fails, check error information in the log files (under the migration tool directory by default), guides, or [About Service Migration](#), and rectify the fault.

2. If the migration succeeds, check whether the destination CVM can be started normally, whether the data on the destination CVM is consistent with that on the source server, whether the network is normal, and whether other system services are running normally.

3. If you have any questions or encounter migration errors, check [About Service Migration](#) or submit a ticket.
Cross-region data migration moves the data on a CVM in an availability zone in one region to a destination CVM in an availability zone of another region. It can also mean the migration of data between CVMs in different availability zones within the same region.

Obtaining the migration tool

Click here to obtain the compressed migration tool package.

Choosing a migration mode based on the network environment

Choose the appropriate migration mode according to the network environments of your source servers and destination CVMs. Currently, the migration tool supports the default mode and the private network mode. The private network mode applies to three scenarios. Each migration mode or scenario has different network requirements for source servers and destination CVMs. If both source servers and destination CVMs can access the public network, you can use the default mode for migration. If source servers or destination CVMs cannot directly access the public network, you need to establish connections through VPC Peering Connection, VPN Connection, Cloud Connect Network, or Direct Connect before using the private network mode for migration.

Data Backup

You can back up your data by creating snapshots.

Checking before migrating
Before migrating, check the following items for source servers and destination CVMs respectively:

| Destination CVM | 1. Storage: The cloud disks of the destination CVM, including system disks and data disks. Verify that they have sufficient storage to store the data from the source server.  
2. Security group: Ports 443 and 80 must be open in a security group.  
3. Bandwidth setting: We recommend that you increase bandwidth for faster migration. The traffic consumed during migration will be approximately equal to the data volume. Change your networking billing method in advance if needed.  
4. Operating system: We recommend that the destination CVM and the source server use the same operating system. Different operating systems will result in inconsistency between the image that will be created later and the actual operating system. For example, when migrating a source server with the CentOS 7 system installed, choose a CVM with the CentOS 7 system installed as the migration destination. |
| Linux source server | 1. Check for and install Virtio. For more information, see Checking Virtio Drivers in Linux.  
2. Check whether rsync and grub2-install (or grub-install) are installed.  
3. Check whether SELinux is enabled. Disable it if enabled.  
4. When a migration request is sent to Tencent Cloud API, the API uses the current UNIX time to check against the generated token. In this case, ensure that the current system time is correct. |

- You can use tool commands to automate the checking of source servers, for example, 
  ```bash
  sudo ./go2tencentcloud_x64 --check
  ```
- By default, the go2tencentcloud migration tool automatically performs checking when it starts to run. If you want to skip the check and force migration, configure the value of the `Client.Extra.IgnoreCheck` field in the client.json file to `true`.

### Starting Migration

1. (Optional) Establish a connection between the source server and the destination CVM.
   - If you are using the private network mode, establish a connection between the source sever and the destination CVM through VPC Peering Connection, VPN Connection, Cloud Connect Network, or Direct Connect.
   - Skip this step if you are using the default mode.
2. Configure the user.json file.
   The user.json file is for configuring the source server and the destination CVM. It contains the following configuration items:
   - The access key pair of your account API, that is, SecretId and SecretKey. For more information, see Access Keys.
   - The region and instance ID of the target CVM.
   - (Optional) The data disk configuration of the source server.

3. Configure the client.json file.
   The client.json file is for configuring the migration mode and other migration configuration items. You need to configure the Client.Net.Mode parameter in the client.json file despite migration modes or scenarios.

4. (Optional) Remove files and directories on the server that do not need to be migrated.
   Edit the rsync_excludes_linux.txt file on the Linux source server to remove files and directories that do not need to be migrated.

5. Run the tool.
   For example, on a 64-bit Linux source server, run the following command with root permissions to run the tool.

   ```
sudo ./go2tencentcloud_x64
   ```
Migrating Tencent Cloud CVM Data Across Accounts

The online migration tool supports migrating Tencent Cloud CVM data across accounts. Cross-account data migration moves data between CVMs under two different accounts.

Obtaining the migration tool

Click here to obtain the compressed migration tool package.

Choosing a migration mode based on the network environment

Choose the appropriate migration mode according to the network environments of your source servers and destination CVMs.

Currently, the migration tool supports the default mode and the private network mode. The private network mode applies to three scenarios. Each migration mode or scenario has different network requirements for source servers and destination CVMs. If both source servers and destination CVMs can access the public network, you can use the default mode for migration. If source servers or destination CVMs cannot directly access the public network, you need to establish connections through VPC Peering Connection, VPN Connection, Cloud Connect Network, or Direct Connect before using the private network mode for migration.

Data Backup

You can back up your data by creating snapshots.

Checking before migrating

Before migrating, check the following items for source servers and destination CVMs respectively:

<table>
<thead>
<tr>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Storage: The cloud disks of the destination CVM, including system disks and</td>
</tr>
</tbody>
</table>
### Cloud Virtual Machine

1. Check for and install Virtio. For more information, see [Checking Virtio Drivers in Linux](#).
2. Check whether rsync and grub2-install (or grub-install) are installed.
3. Check whether SELinux is enabled. Disable it if enabled.
4. When a migration request is sent to Tencent Cloud API, the API uses the current UNIX time to check against the generated token. In this case, ensure that the current system time is correct.

#### Starting Migration

1. (Optional) Establish a connection between the source server and the destination CVM.
   - If you are using the private network mode, establish a connection between the source server and the destination CVM through [VPC Peering Connection](#), [VPN Connection](#), [Cloud Connect Network](#), or [Direct Connect](#).
   - Skip this step if you are using the default mode.
2. Configure the user.json file.
   - The user.json file is for configuring the source server and the destination CVM. It contains the following configuration items:
- The access key pair of your account API, that is, SecretId and SecretKey. For more information, see Access Keys.
- The region where the destination CVM resides.
- The instance ID of the destination CVM.
- (Optional) The data disk configuration of the source server.

3. Configure the client.json file.
   The client.json file is for configuring the migration mode and other migration configuration items. You need to configure the `Client.Net.Mode` parameter in the client.json file despite migration modes or scenarios.

4. (Optional) Remove files and directories on the server that do not need to be migrated.
   Edit the rsync_excludes_linux.txt file on the Linux source server to remove files and directories that do not need to be migrated.

5. Run the tool.
   Take cross-account migration in private network mode: Scenario 1 as an example:
   i. On a CVM that has access to the public network, execute the following command to run the tool for migration stage 1.

   ```
   sudo ./go2tencentcloud_x64
   ```

   If the **Stage 1 is finished and please run next stage at source machine** prompt appears, stage 1 is completed.

   ![Stage 1 successful output]

   ii. After the previous step (stage 1) is completed, copy the entire tool directory in stage 1 to the source server to be migrated, and then run the tool for migration stage 2. Execute the following command to run the tool for migration stage 2.

   ```
   sudo ./go2tencentcloud_x64
   ```

   If the **Stage 2 is finished and please run next stage at gateway machine** prompt appears, stage 2 is completed.
iii. After the previous step (stage 2) is completed, copy the entire tool directory in stage 2 to the source server in stage 1, and then run the tool for migration stage 3.

Execute the following command to run the tool for migration stage 3.

```bash
sudo ./go2tencentcloud_x64
```

If the Migrate successfully prompt appears, the entire migration task has been completed successfully.
Migration Tutorial for Different Source Environments
Migrating AWS EC2 Data to Tencent Cloud

Last updated : 2020-02-11 14:12:46

Obtaining the migration tool

Click here to obtain the compressed migration tool package.

Choosing a migration mode based on the network environment

Choose the appropriate migration mode according to the network environments of your source servers and destination CVMs. Currently, the migration tool supports the default mode and the private network mode. The private network mode applies to three scenarios. Each migration mode or scenario has different network requirements for source servers and destination CVMs. If both source servers and destination CVMs can access the public network, you can use the default mode for migration. If source servers or destination CVMs cannot directly access the public network, you need to establish connections through VPC peering connection, VPN Connection, Cloud Connect Network, or Direct Connect before using the private network mode for migration.

Data Backup

You can back up your data by creating snapshots.

Checking before migrating

Before migrating, check the following items for source servers and destination CVMs respectively:
1. Storage: The cloud disks of the destination CVM, including system disks and data disks. Verify that they have sufficient storage to store the data from the source server.
2. Security group: Ports 443 and 80 must be open in a security group.
3. Bandwidth setting: We recommend that you increase bandwidth for faster migration. The traffic consumed during migration will be approximately equal to the data volume. Change your networking billing method in advance if needed.
4. Operating system: We recommend that the destination CVM and the source server use the same operating system. Different operating systems will result in inconsistency between the image that will be created later and the actual operating system. For example, when migrating a source server with the CentOS 7 system installed, choose a CVM with the CentOS 7 system installed as the migration destination.

### Linux source server

1. Check for and install Virtio. For more information, see [Checking Virtio Drivers in Linux](#).
2. Check whether rsync and grub2-install (or grub-install) are installed.
3. Check whether SELinux is enabled. Disable it if enabled.
4. When a migration request is sent to Tencent Cloud API, the API uses the current UNIX time to check against the generated token. Please ensure that the current system time is correct.
5. Check the login method of the source server. If your AWS source server uses SSH key pair authentication, switch it to password login. For more information, see [Enabling password login for AWS EC2 instances](#).

- You can use tool commands to automate the checking of source servers, for example, `sudo ./go2tencentcloud_x64 --check`.
- By default, the go2tencentcloud migration tool automatically performs checking when it starts to run. If you want to skip the check and enforce migration, configure the value of the `Client.Extra.IgnoreCheck` field in the client.json file to `true`.

## Starting Migration

1. (Optional) Establish a connection between the source server and the destination CVM.
   - If you are using the private network mode, establish a connection between the source server and the destination CVM through VPC Peering Connection, VPN Connection, Cloud Connect Network, or Direct Connect.
   - Skip this step if you are using the default mode.
2. Configure the user.json file.
   The user.json file is for configuring the source server and the destination CVM. It contains the following configuration items:
   - The access key pair of your account API, that is, SecretId and SecretKey. For more information, see Access Keys.
   - The region where the destination CVM resides.
   - The instance ID of the destination CVM.
   - (Optional) The data disk configuration of the source server.

3. Configure the client.json file.
   The client.json file is for configuring the migration mode and other migration configuration items. You need to configure the \texttt{Client.Net.Mode} parameter in the client.json file despite migration modes or scenarios.

4. (Optional) Remove files and directories on the server that do not need to be migrated.
   Edit the \texttt{rsync_excludes_linux.txt} file on the Linux source server to remove files and directories that do not need to be migrated.

5. Run the tool.
   For example, on a 64-bit Linux source server, run the following command with root permissions to run the tool.
   
   ```
   sudo ./go2tencentcloud_x64
   ```

   Wait for the migration process to complete.
   If the migration is successful, the following console output appears:
[2019-10-02 13:29:43] Start go2tencentcloud 1.3.0
[2019-10-02 13:29:47] Check environment...
[2019-10-02 13:29:49] Restart remote instance...
Used: 00:04:52 | Max Timeout: 00:10:00
[2019-10-02 13:34:43] Start preparing remote server...
[2019-10-02 13:34:43] Start initializing remote server...
Used: 00:00:20 | Max Timeout: 00:03:00
[2019-10-02 13:35:04] [2/3] Synchronize files
[2019-10-02 13:35:04] Transmitting files...
[2019-10-02 13:37:06] Reconfigure remote instance...
Used: 00:00:07 | Max Timeout: 00:05:00
Migrating Alibaba Cloud ECS Data to Tencent Cloud

Obtaining the migration tool

Click here to obtain the compressed migration tool package.

Choosing a migration mode based on the network environment

Choose the appropriate migration mode according to the network environments of your source servers and destination CVMs.

Currently, the migration tool supports the default mode and the private network mode. The private network mode applies to three scenarios. Each migration mode or scenario has different network requirements for source servers and destination CVMs. If both source servers and destination CVMs can access the public network, you can use the default mode for migration. If source servers or destination CVMs cannot directly access the public network, you need to establish connections through VPC Peering Connection, VPN Connection, Cloud Connect Network, or Direct Connect before using the private network mode for migration.

Data Backup

You can back up your data by creating snapshots.

Checking before migrating

Before migrating, check the following items for source servers and destination CVMs respectively:

<table>
<thead>
<tr>
<th>Destination CVM</th>
<th>1. Storage: The cloud disks of the destination CVM, including system disks and data disks. Verify that they have sufficient storage to store the data from the source server.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2. Security group: Ports 443 and 80 must be open in a security group.</td>
</tr>
</tbody>
</table>

©2013-2019 Tencent Cloud. All rights reserved.
3. Bandwidth setting: We recommend that you increase bandwidth for faster migration. The traffic consumed during migration will be approximately equal to the data volume. Change your networking billing method in advance if needed.

4. Operating system: We recommend that the destination CVM and the source server use the same operating system. Different operating systems will result in inconsistency between the image that will be created later and the actual operating system. For example, when migrating a source server with the CentOS 7 system installed, choose a CVM with the CentOS 7 system installed as the migration destination.

### Linux source server

| 1. Check for and install Virtio. For more information, see [Checking Virtio Drivers in Linux](#). |
| 2. Check whether rsync and grub2-install (or grub-install) are installed. |
| 3. Check whether SELinux is enabled. Disable it if enabled. |
| 4. When a migration request is sent to Tencent Cloud API, the API uses the current UNIX time to check against the generated token. In this case, ensure that the current system time is correct. |

You can use tool commands to automate the checking of source servers, for example, `sudo ./go2tencentcloud_x64 --check`. By default, the go2tencentcloud migration tool automatically performs checking when it starts to run. If you want to skip the check and force migration, configure the value of the `Client.Extra.IgnoreCheck` field in the client.json file to `true`.

### Starting Migration

1. (Optional) Establish a connection between the source server and the destination CVM.
   - If you are using the private network mode, establish a connection between the source sever and the destination CVM through [VPC Peering Connection](#), [VPN Connection](#), [Cloud Connect Network](#), or [Direct Connect](#).
   - Skip this step if you are using the default mode.

2. Configure the user.json file.
   
   The user.json file is for configuring the source server and the destination CVM. It contains the following configuration items:
   - The access key pair of your account API, that is, SecretId and SecretKey. For more information, see [Access Keys](#).
   - The region where the destination CVM resides.
The instance ID of the destination CVM.

(Optional) The data disk configuration of the source server.

3. Configure the client.json file.

The client.json file is for configuring the migration mode and other migration configuration items. You need to configure the `Client.Net.Mode` parameter in the client.json file despite migration modes or scenarios.

4. (Optional) Remove files and directories on the server that do not need to be migrated.

Edit the `rsync_excludes_linux.txt` file on the Linux source server to remove files and directories that do not need to be migrated.

5. Run the tool.

For example, on a 64-bit Linux source server, run the following command with root permissions to run the tool.

```
sudo ./go2tencentcloud_x64
```

If the migration is successful, the following console output appears:

```
[2019-10-02 10:41:58] Start go2tencentcloud 1.3.0
[2019-10-02 10:42:17] Check environment...
[2019-10-02 10:42:21] [1/3] Initialize instance
[2019-10-02 10:42:21] Restart remote instance...
Used: 00:01:20 | Max Timeout: 00:10:00
[2019-10-02 10:43:42] Start preparing remote server...
[2019-10-02 10:43:42] Start initializing remote server...
Used: 00:00:11 | Max Timeout: 00:03:00
[2019-10-02 10:43:54] [2/3] Synchronize files
[2019-10-02 10:43:54] Transmitting files...
[2019-10-02 10:47:13] Reconfigure remote instance...
Used: 00:00:07 | Max Timeout: 00:05:00
```
Migrating Huawei Cloud ECS Data to Tencent Cloud

Last updated: 2020-02-11 14:15:02

Obtaining the migration tool

Click here to obtain the compressed migration tool package.

Choosing a migration mode based on the network environment

Choose the appropriate migration mode according to the network environments of your source servers and destination CVMs.

Currently, the migration tool supports the default mode and the private network mode. The private network mode applies to three scenarios. Each migration mode or scenario has different network requirements for source servers and destination CVMs. If both source servers and destination CVMs can access the public network, you can use the default mode for migration. If source servers or destination CVMs cannot directly access the public network, you need to establish connections through VPC Peering Connection, VPN Connection, Cloud Connect Network, or Direct Connect before using the private network mode for migration.

Data Backup

You can back up your data by creating snapshots.

Checking before migrating

Before migrating, check the following items for source servers and destination CVMs respectively:

<table>
<thead>
<tr>
<th>Destination CVM</th>
<th>1. Storage: The cloud disks of the destination CVM, including system disks and data disks. Verify that they have sufficient storage to store the data from the source server.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2. Security group: Ports 443 and 80 must be open in a security group.</td>
</tr>
</tbody>
</table>
3. Bandwidth setting: We recommend that you increase bandwidth for faster migration. The traffic consumed during migration will be approximately equal to the data volume. Change your networking billing method in advance if needed.

4. Operating system: We recommend that the destination CVM and the source server use the same operating system. Different operating systems will result in inconsistency between the image that will be created later and the actual operating system. For example, when migrating a source server with the CentOS 7 system installed, choose a CVM with the CentOS 7 system installed as the migration destination.

Linux source server

1. Check for and install Virtio. For more information, see Checking Virtio Drivers in Linux.
2. Check whether rsync and grub2-install (or grub-install) are installed.
3. Check whether SELinux is enabled. Disable SELinux if it is enabled.
4. When a migration request is sent to Tencent Cloud API, the API uses the current UNIX time to check against the generated token. In this case, ensure that the current system time is correct.
5. Run the `cloud-init --version` command to check the version information of cloud-init installed on the source server.
   - We recommend that you uninstall or remove the cloud-init whose version is earlier than 17.1.
   - Skip this step if the source server does not have cloud-init installed.

You can use tool commands to automate the checking of source servers, for example, `sudo ./go2tencentcloud_x64 --check`.

By default, the go2tencentcloud migration tool automatically performs checking when it starts to run. If you want to skip the check and enforce migration, configure the value of the `Client.Extra.IgnoreCheck` field in the client.json file to `true`.

### Starting Migration

1. (Optional) Establish a connection between the source server and the destination CVM.
   - If you are using the private network mode, establish a connection between the source server and the destination CVM through VPC Peering Connection, VPN Connection, Cloud Connect Network, or Direct Connect.
   - Skip this step if you are using the default mode.
2. Configure the user.json file.
   - The user.json file is for configuring the source server and the destination CVM. It contains the
following configuration items:
- The access key pair of your account API, that is, SecretId and SecretKey. For more information, see Access Keys.
- The region where the destination CVM resides.
- The instance ID of the destination CVM.
- (Optional) The data disk configuration of the source server.

3. Configure the client.json file.
   The client.json file is for configuring the migration mode and other migration configuration items. You need to configure the `Client.Net.Mode` parameter in the client.json file despite migration modes or scenarios.

4. (Optional) Remove files and directories on the server that do not need to be migrated.
   Edit the rsync_excludes_linux.txt file on the Linux source server to remove files and directories that do not need to be migrated.

5. Run the tool.
   For example, on a 64-bit Linux source server, run the following command with root permissions to run the tool.

```
sudo ./go2tencentcloud_x64
```

Wait for the migration process to complete.
If the migration is successful, the following console output appears:
[root@kaijianyao-10-02 go2tencentcloud]# sudo ./go2tencentcloud_x64
[2019-10-02 22:13:34] Check environment...
[2019-10-02 22:13:38] [1/3] Initialize instance
[2019-10-02 22:13:38] Restart remote instance...

Used: 00:01:24 | Max Timeout: 00:10:00
[2019-10-02 22:15:03] Start preparing remote server...
[2019-10-02 22:15:03] Start initializing remote server...

Used: 00:00:11 | Max Timeout: 00:03:00
[2019-10-02 22:15:15] Transmitting files...
[##########################################] 100% | 00:03:04
[2019-10-02 22:18:19] Reconfigure remote instance...

Used: 00:00:07 | Max Timeout: 00:05:00
Migrating UCloud UHost Data to Tencent Cloud

Obtaining the migration Tool

Click here to obtain the compressed migration tool package.

Choosing a migration mode based on the network environment

Choose the appropriate migration mode according to the network environments of your source servers and destination CVMs. Currently, the migration tool supports the default mode and the private network mode. The private network mode applies to three scenarios. Each migration mode or scenario has different network requirements for source servers and destination CVMs. If both source servers and destination CVMs can access the public network, you can use the default mode for migration. If source servers or destination CVMs cannot directly access the public network, you need to establish connections through VPC Peering Connection, VPN Connection, Cloud Connect Network, or Direct Connect before using the private network mode for migration.

Data Backup

You can back up your data by creating snapshots.

Checking before migrating

Before migrating, check the following items for source servers and destination CVMs respectively:

| Destination CVM | 1. Storage: The cloud disks of the destination CVM, including system disks and data disks. Verify that they have sufficient storage to store the data from the source server.  
2. Security group: Ports 443 and 80 must be open in a security group. |
3. Bandwidth setting: We recommend that you increase bandwidth for faster migration. The traffic consumed during migration will be approximately equal to the data volume. Change your networking billing method in advance if needed.

4. Operating system: We recommend that the destination CVM and the source server use the same operating system. Different operating systems will result in inconsistency between the image that will be created later and the actual operating system. For example, when migrating a source server with the CentOS 7 system installed, choose a CVM with the CentOS 7 system installed as the migration destination.

### Linux source server

1. Check for and install Virtio. For more information, see [Checking Virtio Drivers in Linux](#).

2. Check whether rsync and grub2-install (or grub-install) are installed.

3. Check whether SELinux is enabled. Disable it if enabled.

4. When a migration request is sent to Tencent Cloud API, the API uses the current UNIX time to check against the generated token. In this case, ensure that the current system time is correct.

---

You can use tool commands to automate the checking of source servers, for example, **sudo ./go2tencentcloud_x64 --check**.

By default, the go2tencentcloud migration tool automatically performs checking when it starts to run. If you want to skip the check and enforce migration, configure the value of the `Client.Extra.IgnoreCheck` field in the client.json file to **true**.

---

### Starting Migration

1. (Optional) Establish a connection between the source server and the destination CVM.
   - If you are using the private network mode, establish a connection between the source server and the destination CVM through [VPC Peering Connection](#), [VPN Connection](#), [Cloud Connect Network](#), or [Direct Connect](#).
   - Skip this step if you are using the default mode.

2. Configure the user.json file.

   The user.json file is for configuring the source server and the destination CVM. It contains the following configuration items:
   - The access key pair of your account API, that is, SecretId and SecretKey. For more information, see [Access Keys](#).
   - The region where the destination CVM resides.
3. Configure the client.json file.

The client.json file is for configuring the migration mode and other migration configuration items. You need to configure the `Client.Net.Mode` parameter in the client.json file despite migration modes or scenarios.

4. (Optional) Remove files and directories on the server that do not need to be migrated.

Edit the `rsync_excludes_linux.txt` file on the Linux source server to remove files and directories that do not need to be migrated.

5. Run the tool.

For example, on a 64-bit Linux source server, run the following command with root permissions to run the tool.

```bash
sudo ./go2tencentcloud_x64
```

Wait for the migration process to complete.

If the migration is successful, the following console output appears:

```
[root@10-29-133-82 go2tencentcloud]# sudo ./go2tencentcloud_x64
[2019-10-03 05:30:21] Start go2tencentcloud 1.3.0
[2019-10-03 05:30:21] Load user.json successfully.
[2019-10-03 05:30:22] Check environment...
[2019-10-03 05:30:28] Check environment successfully.
[2019-10-03 05:30:28] [1/3] Initialize instance
[2019-10-03 05:30:30] Restart remote instance...
Used: 00:01:23 | Max Timeout: 00:10:00
[2019-10-03 05:31:54] Restart remote instance successfully.
[2019-10-03 05:31:54] Start preparing remote server...
[2019-10-03 05:31:54] Start initializing remote server...
Used: 00:00:23 | Max Timeout: 00:03:00
[2019-10-03 05:32:18] [2/3] Synchronize files
[2019-10-03 05:32:18] Transmitting files...

[-------------------------------------------------] 100% | 00:02:13
[2019-10-03 05:34:31] Reconfigure remote instance...
Used: 00:00:42 | Max Timeout: 00:05:00
```
Migrating Baidu Cloud BCC Data to Tencent Cloud

Last updated: 2020-02-11 14:33:14

Obtaining the migration tool

Click here to obtain the compressed migration tool package.

Choosing a migration mode based on the network environment

Choose the appropriate migration mode according to the network environments of your source servers and destination CVMs.
Currently, the migration tool supports the default mode and the private network mode. The private network mode applies to three scenarios. Each migration mode or scenario has different network requirements for source servers and destination CVMs. If both source servers and destination CVMs can access the public network, you can use the default mode for migration. If source servers or destination CVMs cannot directly access the public network, you need to establish connections through VPC Peering Connection, VPN Connection, Cloud Connect Network, or Direct Connect before using the private network mode for migration.

Data Backup

You can back up your data by creating snapshots.

Checking before migrating

Before migrating, check the following items for source servers and destination CVMs respectively:

| Destination CVM | 1. Storage: The cloud disks of the destination CVM, including system disks and data disks. Verify that they have sufficient storage to store the data from the source server.  
2. Security group: Ports 443 and 80 must be open in a security group. |
3. Bandwidth setting: We recommend that you increase bandwidth for faster migration. The traffic consumed during migration will be approximately equal to the data volume. Change your networking billing method in advance if needed.

4. Operating system: We recommend that the destination CVM and the source server use the same operating system. Different operating systems will result in inconsistency between the image that will be created later and the actual operating system. For example, when migrating a source server with the CentOS 7 system installed, choose a CVM with the CentOS 7 system installed as the migration destination.

### Linux source server

1. Check for and install Virtio. For more information, see [Checking Virtio Drivers in Linux](#).

2. Check whether rsync and grub2-install (or grub-install) are installed.

3. Check whether SELinux is enabled. Disable it if enabled.

4. When a migration request is sent to Tencent Cloud API, the API uses the current UNIX time to check against the generated token. In this case, ensure that the current system time is correct.

#### You can use tool commands to automate the checking of source servers, for example, `sudo ./go2tencentcloud_x64 --check`.

#### By default, the go2tencentcloud migration tool automatically performs checking when it starts to run. If you want to skip the check and force migration, configure the value of the `Client.Extra.IgnoreCheck` field in the client.json file to `true`.

### Starting Migration

1. **(Optional) Establish a connection between the source server and the destination CVM.**
   - If you are using the private network mode, establish a connection between the source server and the destination CVM through [VPC Peering Connection](#), [VPN Connection](#), [Cloud Connect Network](#), or [Direct Connect](#).
   - Skip this step if you are using the default mode.

2. **Configure the user.json file.**
   - The user.json file is for configuring the source server and the destination CVM. It contains the following configuration items:
     - The access key pair of your account API, that is, SecretId and SecretKey. For more information, see [Access Keys](#).
     - The region where the destination CVM resides.
- The instance ID of the destination CVM.
- (Optional) The data disk configuration of the source server.

3. Configure the client.json file.
   The client.json file is for configuring the migration mode and other migration configuration items. You need to configure the `Client.Net.Mode` parameter in the client.json file despite migration modes or scenarios.

4. (Optional) Remove files and directories on the server that do not need to be migrated.
   Edit the `rsync_excludes_linux.txt` file on the Linux source server to remove files and directories that do not need to be migrated.

5. Run the tool.
   For example, on a 64-bit Linux source server, run the following command with root permissions to run the tool.

   ```bash
   sudo ./go2tencentcloud_x64
   ```

   Wait for the migration process to complete.
   If the migration is successful, the following console output appears:

   ![Console output of the migration process]
Migrating VMWare Virtual Machine Data to Tencent Cloud

Obtaining the migration Tool

Click here to obtain the compressed migration tool package.

Choosing a migration mode based on the network environment

Choose the appropriate migration mode according to the network environments of your source servers and destination CVMs. Currently, the migration tool supports the default mode and the private network mode. The private network mode applies to three scenarios. Each migration mode or scenario has different network requirements for source servers and destination CVMs. If both source servers and destination CVMs can access the public network, you can use the default mode for migration. If source servers or destination CVMs cannot directly access the public network, you need to establish connections through VPC Peering Connection, VPN Connection, Cloud Connect Network or Direct Connect before using the private network mode for migration.

Data Backup

You can back up your data by creating snapshots.

Checking before migrating

Before migrating, check the following items for source servers and destination CVMs respectively:

<table>
<thead>
<tr>
<th>Destination CVM</th>
<th>1. Storage: The cloud disks of the destination CVM, including system disks and data disks. Verify that they have sufficient storage to store the data from the source server.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2. Security group: Ports 443 and 80 must be open in a security group.</td>
</tr>
</tbody>
</table>
3. Bandwidth setting: We recommend that you increase bandwidth for faster migration. The traffic consumed during migration will be approximately equal to the data volume. Change your networking billing method in advance if needed.

4. Operating system: We recommend that the destination CVM and the source server use the same operating system. Different operating systems will result in inconsistency between the image that will be created later and the actual operating system. For example, when migrating a source server with the CentOS 7 system installed, choose a CVM with the CentOS 7 system installed as the migration destination.

| Linux source server | 1. Check for and install Virtio. For more information, see Checking Virtio Drivers in Linux.  
2. Check whether rsync and grub2-install (or grub-install) are installed.  
3. Check whether SELinux is enabled. Disable it if enabled.  
4. When a migration request is sent to Tencent Cloud API, the API uses the current UNIX time to check against the generated token. In this case, ensure that the current system time is correct. |

- You can use tool commands to automate the checking of source servers, for example, `sudo ./go2tencentcloud_x64 --check`.
- By default, the go2tencentcloud migration tool automatically performs checking when it starts to run. If you want to skip the check and enforce migration, configure the value of the `Client.Extra.IgnoreCheck` field in the client.json file to `true`.

**Starting Migration**

1. (Optional) Establish a connection between the source server and the destination CVM.
   - If you are using the private network mode, establish a connection between the source server and the destination CVM through VPC Peering Connection, VPN Connection, Cloud Connect Network, or Direct Connect.
   - Skip this step if you are using the default mode.

2. Configure the user.json file.
   - The user.json file is for configuring the source server and the destination CVM. It contains the following configuration items:
     - The access key pair of your account API, that is, SecretId and SecretKey. For more information, see Access Keys.
     - The region where the destination CVM resides.
- The instance ID of the destination CVM.
- (Optional) The data disk configuration of the source server.

3. Configure the client.json file.
The client.json file is for configuring the migration mode and other migration configuration items. You need to configure the `Client.Net.Mode` parameter in the client.json file despite migration modes or scenarios.

4. (Optional) Remove files and directories on the server that do not need to be migrated.
   Edit the `rsync_excludes_linux.txt` file on the Linux source server to remove files and directories that do not need to be migrated.

5. Run the tool.
   For example, on a 64-bit Linux source server, run the following command with root permissions to run the tool.

   ```bash
   sudo ./go2tencentcloud_x64
   ```

   Wait for the migration process to complete.

   If the migration is successful, the following console output appears:
Migrating China Telecom e-Cloud Cloud Server Data to Tencent Cloud

Obtaining the migration tool

Click here to obtain the compressed migration tool package.

Choosing a migration mode based on the network environment

Choose the appropriate migration mode according to the network environments of your source servers and destination CVMs.

Currently, the migration tool supports the default mode and the private network mode. The private network mode applies to three scenarios. Each migration mode or scenario has different network requirements for source servers and destination CVMs. If both source servers and destination CVMs can access the public network, you can use the default mode for migration. If source servers or destination CVMs cannot directly access the public network, you need to establish connections through VPC Peering Connection, VPN Connection, Cloud Connect Network, or Direct Connect before using the private network mode for migration.

Data Backup

You can back up your data by creating snapshots.

Checking before migrating

Before migrating, check the following items for source servers and destination CVMs respectively:

<table>
<thead>
<tr>
<th>Destination CVM</th>
<th>1. Storage: The cloud disks of the destination CVM, including system disks and data disks. Verify that they have sufficient storage to store the data from the source server.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2. Security group: Ports 443 and 80 must be open in a security group.</td>
</tr>
</tbody>
</table>
Cloud Virtual Machine

3. Bandwidth setting: We recommend that you increase bandwidth for faster migration. The traffic consumed during migration will be approximately equal to the data volume. Change your networking billing method in advance if needed.

4. Operating system: We recommend that the destination CVM and the source server use the same operating system. Different operating systems will result in inconsistency between the image that will be created later and the actual operating system. For example, when migrating a source server with the CentOS 7 system installed, choose a CVM with the CentOS 7 system installed as the migration destination.

Linux source server

1. Check for and install Virtio. For more information, see Checking Virtio Drivers in Linux.
2. Check whether rsync and grub2-install (or grub-install) are installed.
3. Check whether SELinux is enabled. Disable it if enabled.
4. When a migration request is sent to Tencent Cloud API, the API uses the current UNIX time to check against the generated token. In this case, ensure that the current system time is correct.

- You can use tool commands to automate the checking of source servers, for example, `sudo ./go2tencentcloud_x64 --check`.
- By default, the go2tencentcloud migration tool automatically performs checking when it starts to run. If you want to skip the check and enforce migration, configure the value of the `Client.Extra.IgnoreCheck` field in the client.json file to `true`.

Starting Migration

1. (Optional) Establish a connection between the source server and the destination CVM.
   - If you are using the private network mode, establish a connection between the source server and the destination CVM through VPC Peering Connection, VPN Connection, Cloud Connect Network, or Direct Connect.
   - Skip this step if you are using the default mode.

2. Configure the user.json file.

   The user.json file is for configuring the source server and the destination CVM. It contains the following configuration items:
   - The access key pair of your account API, that is, SecretId and SecretKey. For more information, see Access Keys.
   - The region where the destination CVM resides.
3. Configure the client.json file.

The client.json file is for configuring the migration mode and other migration configuration items. You need to configure the `Client.Net.Mode` parameter in the client.json file despite migration modes or scenarios.

4. (Optional) Remove files and directories on the server that do not need to be migrated.

   Edit the `rsync_excludes_linux.txt` file on the Linux source server to remove files and directories that do not need to be migrated.

5. Run the tool.

   For example, on a 64-bit Linux source server, run the following command with root permissions to run the tool.

   ```
   sudo ./go2tencentcloud_x64
   ```

   Wait for the migration process to complete.

   If the migration is successful, the following console output appears:

   ```
   [root@ecs-83ab go2tencentcloud]# sudo ./go2tencentcloud_x64
   [2019-10-03 13:35:41] Start go2tencentcloud 1.3.0
   [2019-10-03 13:35:47] Check environment...
   [2019-10-03 13:35:54] [1/3] Initialize instance
   [2019-10-03 13:35:59] Restart remote instance...
   Used: 00:01:17 | Max Timeout: 00:10:00
   [2019-10-03 13:37:17] Start preparing remote server...
   [2019-10-03 13:37:17] Start initializing remote server...
   Used: 00:00:11 | Max Timeout: 00:03:00
   [2019-10-03 13:37:29] Transmitting files...
   [2019-10-03 13:40:26] Reconfigure remote instance...
   Used: 00:00:06 | Max Timeout: 00:05:00
   ```
Offline Migration

Last updated: 2020-05-14 17:50:45

Scenario

Service Migration is a platform developed by Tencent Cloud. It helps enterprises migrate operating systems, applications, and application data from a source server to a Cloud Virtual Machine (CVM) or Cloud Block Storage (CBS) to meet enterprises' business needs for cloud deployment, cross-cloud platform migration, cross-account or cross-region migration, and hybrid cloud deployment.

Service migration is divided into offline migration and online migration. Offline migration includes offline instance migration and offline data migration.

- **Offline instance migration** allows you to migrate system disk images to a specific CVM.
- **Offline data migration** allows you to migrate data disk images to a specific CBS.

Prerequisites

Offline migration requires support from Cloud Object Storage (COS). Therefore, ensure that your region is supported by COS.

For more information on regions supported by COS, see [Regions and Access Domain Names](#).

Preparations

- Currently, Tencent Cloud service migration supports qcow2, vpc, vmdk, and raw image formats. We recommend that you use the compressed image format to reduce transmission and migration time.
- The COS region to which images are uploaded must be the same as that where the destination CVM is located.
- During offline migration, the size of the uploaded image file cannot be greater than the capacity of the destination disk. If the size of the image file is 50 GB, the destination system disk must have at least 50 GB capacity.
- Offline migration does not support snapshots, whose names are similar to *-00000*.vmdk.
Create an image for the server that needs to be migrated as instructed in the image creation document.
- For Windows, see Windows Image Creation.
- For Linux, see Linux Image Creation.

Upload the created image file to COS.
- As image files are generally large in size, image upload through the browser is prone to interruption. We recommend that you use the COSCMD tool to upload images. For more information, see COSCMD.
- If images that you export from other cloud platforms are compressed packages (such as .tar.gz files), you can directly upload them to COS without decompressing.

Obtain the address of COS to which images are uploaded.
In the COS console, locate the image file that you uploaded and view its information to obtain the file link.

Prepare the destination CVM or CBS.
Click here to purchase a CVM >>
Click here to view the purchase instructions for CBS >>.

Directions

Offline instance migration
1. Log in to the CVM console and click Service Migration in the left sidebar.
2. Click Create an instance migration task.
3. Prepare for and confirm instance migration. Then, click Next.
4. Select the region, complete migration configuration information such as the task name, COS link, and destination CVM instance. Then, click Complete to create a migration task.
Return to the offline data migration management page to check the migration task progress.

- Set public read and private write permissions for the COS file.
- The system disk capacity of the destination 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 and click Service Migration in the left sidebar.
2. Click Create and select Data migration.
3. Prepare for and confirm data migration. Then, click Next.
4. Select the region, complete migration configuration information such as the task name, COS link, and destination cloud disk. Then, click **Complete** to create a migration task.

The destination CBS capacity cannot be less than the size of the uploaded image file. Otherwise, the task will fail.

**FAQs**

For more information, see About Service Migration.
Contact Us

Last updated : 2020-03-06 10:50:14

If you encounter any issue during service migration, or have any feedback or suggestions, do not hesitate to contact us.

Submitting a Ticket

If you encounter any Ops or technical problems when using our product, you can log in to the Tencent Cloud Console and follow the on-screen prompts to submit a ticket. We will get back to you as soon as possible.

Ticket links:

- Submitting a ticket: Submit a ticket
- Querying ticket status: Ticket list
To configure ENIs for your CVM, following these instructions:

1. Create an ENI.  
   View the ENI you just created.

2. Bind the ENI to your CVM and configure it.

3. Configure the CVM and VPC route table.

4. Assign a private IP.
   i. Log in to Virtual Private Cloud Console.
   ii. Click ENI under IP and ENI in the left sidebar. The ENI page appears.
   iii. Click the ID/Name of an ENI to see its details.
   iv. Click IP Management to go to the details page.
   v. Click Assign private IP to assign a private IP to the ENI. If you do this manual, pick a usable private IP. Click OK.

5. Manage the ENI.
   - Releasing private IPs
   - Unbinding CVMs
   - Deleting ENIs
   - Binding EIPs
   - Unbinding EIPs
   - Modifying primary private IP
   - Changing the subnet of an ENI
Configuring a Public Gateway

Last updated: 2020-03-06 10:50:15

As of December 6, 2019, Tencent Cloud no longer supports Public Network Gateway configuration when purchasing a CVM. If you need to configure a gateway, following these instructions.

Scenario

If some of your CVMs in Tencent Cloud VPC do not have common public IP addresses but need to access the Internet, you can use a CVM with a public IP (common or elastic public IP) as the public gateway to enable them to access the Internet. The public gateway CVM translates the source IP of outbound traffic. When any other CVMs access the Internet through the public gateway CVM, the public gateway CVM translates their IPs to the public IP of the public gateway CVM, as shown in the figure below.

Prerequisites

- Log in to the CVM Console.
- The public gateway CVM and the CVMs that need to access the Internet through the public gateway CVM are located in different subnets because the public gateway CVM can only forward routing requests from other subnets.
- The public gateway CVM must be a Linux CVM. A Windows CVM cannot serve as a public gateway.
Directions

Step 1: Bind an elastic public IP (optional)

If the CVM that serves as the public gateway already has a public IP address, skip this step.

1. In the navigation panel to the left, click **EIP** to go to the EIP management page.
2. Find the target elastic public IP and select **More > Bind** in the **Operation** column to bring up the **Bind resources** window.
3. Select a CVM instance to serve as the public gateway and bind it to the elastic public IP.

Step 2: Configure a routing table for the subnet of the gateway
The gateway subnet and other subnets cannot use the same route table. A separate route table must be created for the gateway subnet.

1. Create a custom route table
2. Associate the route table with the subnet where the public gateway CVM is located as prompted.

Step 3: Configure a route table for the other subnets

This route table directs all traffic from the CVMs without a public IP to the gateway so they can access public networks as well.

In the route table for the common subnet, add the following routing policy:

- Destination: public IP to be accessed.
- Next-hop type: CVM.
Step 4: Configure the public gateway

1. Log in to the public gateway CVM, enable network forwarding and NAT proxy, and optimize related parameters.

i. Run the following command to create a file named `vpcGateway.sh` in `/usr/local/sbin`.

```
vim /usr/local/sbin/vpcGateway.sh
```

ii. Press i to enter edit mode and add the following code in the script:

```bash
#!/bin/bash

echo "----------------------------------------------------"
echo "(1)ip_forward config......"
file="/etc/sysctl.conf"
grep -i "net.ipv4.ip_forward.*" $file &>/dev/null && sed -i 's/net\.*ipv4\.*ip_forward\.*/net\.*ipv4\.*ip_forward = 1/' $file ||
echo "net.ipv4.ip_forward = 1" >> $file
1 > /proc/sys/net/ipv4/ip_forward
[ `cat /proc/sys/net/ipv4/ip_forward` -eq 1 ] && echo "-->ip_forward:Success" || echo "-->ip_forward:Fail"

echo "(2)Iptables set......"
iptables -t nat -A POSTROUTING -j MASQUERADE && echo "-->nat:Success" || echo "-->nat:Fail"
iptables -t mangle -A POSTROUTING -p tcp -j TCPOPTSTRIP --strip-options timestamp &&
echo "-->mangle:Success" || echo "-->mangle:Fail"

echo "(3)nf_conntrack config......"
```
echo 262144 > /sys/module/nf_conntrack/parameters/hashsize
[ `cat /sys/module/nf_conntrack/parameters/hashsize` -eq 262144 ] &&
echo "-->hashsize:Success" || echo "-->hashsize:Fail"

echo 1048576 > /proc/sys/net/netfilter/nf_conntrack_max
[ `cat /proc/sys/net/netfilter/nf_conntrack_max` -eq 1048576 ] &&
echo "-->nf_conntrack_max:Success" || echo "-->nf_conntrack_max:Fail"

echo 10800 >/proc/sys/net/netfilter/nf_conntrack_tcp_timeout_established
[ `cat /proc/sys/net/netfilter/nf_conntrack_tcp_timeout_established` -eq 10800 ] &&
echo "-->nf_conntrack_tcp_timeout_established:Success" ||
echo "-->nf_conntrack_tcp_timeout_established:Fail"

iii. Press Esc to exit edit mode and enter :wq to save the file and go back. Then, run the following commands:

chmod +x /usr/local/sbin/vpcGateway.sh
echo "/usr/local/sbin/vpcGateway.sh >/tmp/vpcGateway.log 2>&1" >> /etc/rc.local

2. Set the RPS of the public gateway.

i. Run the following command to create a file named setrps.sh in /usr/local/sbin.

vim /usr/local/sbin/set_rps.sh

ii. Press i to enter edit mode and add the following code in the script:

```bash
#!/bin/bash
echo "--------------------------------------------"
* date
mask=0
i=0
total_nic_queues=0

get_all_mask() {
    local cpu_nums=$1
    if [ $cpu_nums -gt 32 ]; then
        mask_tail=""
        mask_low32="ffffffff"
        idx=$((cpu_nums / 32))
        cpu_reset=$((cpu_nums - idx * 32))
```
if [ $cpu_reset -eq 0 ]; then
    mask=$mask_low32
    for ((i = 2; i <= idx; i++)); do
        mask="$mask,$mask_low32"
    done
else
    for ((i = 1; i <= idx; i++)); do
        mask_tail="$mask_tail,$mask_low32"
    done
    mask_head_num=$(($2 ** cpu_reset - 1))
    mask=$(printf "\%x%s\%x"
          $mask_head_num $mask_tail)
fi
else
    mask_num=$(($2 ** cpu_nums - 1))
    mask=$(printf "\%x"
          $mask_num)
fi

echo $mask
}
set_rps() {
    if ! command -v ethtool &>/dev/null; then
        source /etc/profile
    fi

ethtool=$(which ethtool)

cpu_nums=$(cat /proc/cpuinfo | grep processor | wc -l)
if [ $cpu_nums -eq 0 ]; then
    exit 0
fi

mask=$(get_all_mask $cpu_nums)
echo "cpu number:$cpu_nums mask:0x$mask"

ethSet=$(ls -d /sys/class/net/eth*)

for entry in $ethSet; do
    eth=$(basename $entry)
    nic_queues=$(ls -l /sys/class/net/$eth/queues/ | grep rx- | wc -l)
    if (($nic_queues == 0)); then
        continue
    fi

    cat /proc/interrupts | grep "LiquidIO.*rxtx" &>/dev/null
    if [ $? -ne 0 ]; then # not smartnic
        # multi queue don't set rps
        max_combined=$( ethtool -l $eth 2>/dev/null | grep -i "combined" | head -n 1 | awk '{print $2}' )
    fi

```bash
# if ethtool -l $eth goes wrong.
if [ $(ethtool -l $eth) != '' ]; then
    echo "$eth has equally nic queue as cpu, don't set rps for it..."
    continue
else
    echo "$eth is smartnic, set rps for it...
fi

eth:
$eth queues:$nic_queues

total_nic_queues=$(($total_nic_queues + $nic_queues))
i=0
while ((i < $nic_queues)); do
    echo $mask>/sys/class/net/$eth/queues/rx-$i/rps_cpus
    echo 4096 >/sys/class/net/$eth/queues/rx-$i/rps_flow_cnt
    i=$(($i + 1))
done
done

flow_entries=$(($total_nic_queues * 4096))
echo "total_nic_queues:$total_nic_queues flow_entries:$flow_entries"
echo $flow_entries >/proc/sys/net/core/rps_sock_flow_entries
}
set_rps
```

iii. Press **Esc** to exit edit mode and enter **:wq** to save the file and go back. Then, run the following commands:

```bash
chmod +x /usr/local/sbin/set_rps.sh
echo "'/usr/local/sbin/set_rps.sh >/tmp/setRps.log 2>&1' >> /etc/rc.local"
```

3. Reboot the gateway CVM to apply the configurations. Then, test if a CVM that has no public IP can access the Internet through the public gateway CVM.
Switch to VPC

Last updated: 2020-04-01 11:30:15

Scenario

Tencent Cloud provides basic networks and VPCs for different scenarios. Various features are offered to help you flexibly manage your networks.

- Switch between networks:
  - Switch from a basic network to a VPC: Tencent Cloud allows you to switch a CVM instance from a basic network to a VPC and batch switch CVM instances from basic networks to a VPC.
  - Switch between VPCs: Tencent Cloud allows you to switch one or more CVM instances from VPC A to VPC B at a time.
- Specify a custom IP address.
- Choose to retain the HostName.

Notes

- When you batch switch multiple CVM instances between networks, the selected CVM instances must be located in the same availability zone.
- Before migration, unbind the CVM instance or instances from the CLB and ENI in the private and public networks and release the secondary IP address of the primary ENI. Rebind them after the migration.
- During the migration, the CVM instance or instances need to be restarted. Therefore, do not perform other operations.
- After the migration, please check whether the CVM instance or instances are running normally and can be accessed via a private network and logged in to remotely.
- Switching from a basic network to a VPC is irreversible. A CVM instance cannot communicate with CVM instances in basic networks after being switched from a basic network to a VPC.

Procedure

1. Log in to the CVM console.
2. On the Instances page, find the CVM instance to be switched between networks. In the Actions column, click More and then choose Resource Adjustment > Switch VPC.
To switch the VPCs of multiple CVM instances in a batch, select the CVM instances to be switched, click More actions at the top of the page and then choose Resource Adjustment > Switch VPC.

3. In the Switch VPC window that appears, read the notes and then click Next.
4. Select the destination VPC and the corresponding subnet and then click Next.
5. In the selected subnet section, specify the pre-assigned IP address and the HostName options as required and then click Next.

- If no pre-assigned IP address is specified, the system will automatically assign an IP address.
- When specifying the HostName options, you can select Reset HostName or Retain original HostName of the instance.

6. Perform operations according to the instructions on the Shutdown CVM page and then click Start Migration. After the migration is complete, you can log in to the CVM console, and on the Instances page, you will see Modifies instance VPC attributes is displayed in the Status column of the instances to be switched.
Elastic IP

Last updated: 2020-06-11 17:04:08

Scenario

Elastic IP, or EIP, is a static IP designed for dynamic cloud computing and a fixed public IP in a certain region. With EIP, you can quickly remap an address to another instance in your account or NAT gateway instance to avoid instance failure. This document describes how to use EIPs.

Prerequisites

You have logged in to the CVM Console.

Directions

**Apply for EIPs**

1. In the left sidebar, click **EIP** to enter the EIP management page.
2. Click **Apply** in the EIP management page.
3. In the pop-up “Apply for EIP” window, select the region, IP address type, billing method and bandwidth limit, and enter the number of EIPs you want to apply for.
4. Click **OK** to complete the EIP application.

   After the application is completed, you can see in the list the EIP you have applied for, which is in an unbound status.

**Bind EIPs to cloud products**

1. In the left sidebar, click **EIP** to enter the EIP management page.
2. In the EIP management page, select the EIP which you want to bind to a cloud product and click **More > Bind**.
   
   If the EIP has been bound to a instance, please unbind it first.

3. In the pop-up “Bind resources” window, select the resource to be bound to the EIP and click **OK**.
4. In the pop-up window, click **OK** to complete binding the EIP to the cloud product.
Unbind EIPs from cloud products

1. In the left sidebar, click **EIP** to enter the EIP management page.
2. In the EIP management page, select the EIP which you want to unbind from the cloud product and click **More > Unbind**.
3. In the pop-up “Unbind EIP” window, confirm the unbinding information and click **OK**.
4. In the pop-up window, click **OK** to complete unbinding the EIP from the cloud product.

After unbinding, the cloud product instance may be assigned a new public IP, which may be different from the one before binding.

Release EIPs

1. In the left sidebar, click **EIP** to enter the EIP management page.
2. In the EIP management page, select the EIP which you want to release from the cloud product and click **More > Release**.
3. In the pop-up “Are you sure you want to release the selected EIPs?” window, select **Release the above EIPs** and click **Release**.

Adjust Bandwidth

1. In the left sidebar, click **EIP** to enter the EIP management page.
2. Select the EIP whose bandwidth needs to be adjusted and click **Adjust Bandwidth**
3. In the pop-up “Adjust Bandwidth” window, configure the bandwidth value and click **OK** to complete the adjustment.

Convert a public IP to an EIP

The public IP purchased along with the CVM instance is not elastic and cannot be mounted or unmounted. Tencent Cloud allows you to convert the public IP to an EIP by the following steps:

1. In the left sidebar, click **Instances** to enter the instance management page.
2. Select the instance whose public IP needs to be converted to an EIP and then click **Invite**, as shown below:
3. In the pop-up “Convert to EIP” window, click **OK**.

Troubleshoot Exceptions

Network inaccessibility may occur with an EIP due to the following reasons:

- The EIP is not bound to any cloud product. For more information about how to bind an EIP to the cloud product, please see **Bind EIPs to cloud products**.
- Security policy is invalid. Check if there is a valid security policy (security group or network ACL). If the bound cloud product has a security group policy, such as access to 8080 port is denied, the
port 8080 of the EIP is also inaccessible.
EIP Direct Connection

Last updated: 2020-04-13 19:05:01

Use Cases

When you want to access internet via an EIP, you can choose NAT mode or direct connection mode. The default mode is NAT mode.

- In NAT mode, EIP is invisible on the local machine.
- In direct connection mode, the EIP is visible on the local machine. You do not need to manually add an EIP address for each configuration, which can minimize development cost.
- NAT mode can meet most of the requirements. However, if you want to check the public IP on the CVM, you need to use EIP direct connection mode.

Use Limits

- At present, EIP direct connection is under beta test and is only available to whitelisted users. It only supports devices in a VPC. You can submit a ticket to apply for this feature.
- An NAT gateway can be bound with EIPs that are enabled with direct connection, but direct connection cannot be implemented.
- On CVM, EIP direct connection cannot take effect at the same time as an NAT gateway. If the routing table associated with the subnet where your CVM resides is configured with a routing policy of accessing the public network through the NAT gateway, direct connection cannot be implemented through the EIP on the CVM. You can allow the CVM to access the public network through its EIP by adjusting the priorities of NAT gateways and EIPs. In this case, EIP direct connection can be implemented.

Directions

To use EIP direct connection, you need to enable it in the console and add the IP to the ENI in the operating system. You also need to configure the routing in the operating system based on your application. Therefore, we provide a script for configuring the IP so that private network traffic goes through the private IP and public network traffic goes through the public IP.

For other applications, configure the routing accordingly.
Configuring EIP direct connection on Linux CVM

- The script for Linux supports CentOS 6 and later, and Ubuntu.
- The script for Linux supports only primary ENI (eth0) and does not support secondary ENI.
- If the public IP that is bound to the primary ENI is not an EIP, you need to convert the public IP to an EIP. For more information, see Converting public IP to EIP.

Scenario
The script for Linux is applicable to the following scenario: both the private IP and public IP are bound to the primary ENI (eth0), where the public network address is accessed through the public IP, and the private network address is accessed through the private IP.

Step 1: download the script for EIP direct connection
EIP direct connection may cause network interruption. Therefore, you need to download the script for EIP direct connection and upload it to CVM in advance. You can obtain the script by using one of the following methods:

- **Method 1: upload the script for EIP direct connection**
  1. Download the configuration script for EIP direct connection from Download Script for Linux
  2. After the script for Linux is downloaded onto the local machine, upload it to the CVM that requires EIP direct connection.
- **Method 2: directly use a command**
  Log in to the CVM, and run the following command on the CVM to download the script:

```bash
wget https://eip-direct-1254277469.cos.ap-guangzhou.myqcloud.com/eip_direct.sh
```

Step 2: run the script for EIP direct connection
1. Log in to the CVM that requires EIP direct connection.
2. Run the script for EIP direct connection as follows:
   1. Run the following command to add the execution permission:
```
   chmod +x eip_direct.sh
```
   2. Run the following command to run the script:
```
   ./eip_direct.sh install XX.XX.XX.XX
```
Here, XX.XX.XX.XX indicates the EIP address (optional). You may leave it blank and run 
./eip_direct.sh install directly.

**Step 3: enable EIP direct connection**

1. Log in to the EIP Console.
2. Find the target EIP, and choose More -> Direct connection in the Operation column on the right.

### Configuring EIP direct connection on Windows CVM

- To use EIP direct connection in Windows, you need one ENI for private IP and one ENI for public IP, and bind the public IP to the primary ENI and bind the private IP to the secondary ENI.
- During configuration of EIP direct connection in Windows, your internet connection may be interrupted. Therefore, we recommend that you log in to a Windows instance via VNC.

- If the public IP that is bound to the primary ENI is not an EIP, you need to convert the public IP to an EIP. For more information, see Converting public IP to EIP.

### Scenarios

The script for Windows is applicable to the following scenario: Public network traffic goes through the primary ENI, and private network traffic goes through the secondary ENI.

**Step 1: download the script for EIP direct connection**

During configuration of EIP direct connection, the internet connection will be interrupted. Therefore, you need to download the script for EIP direct connection and upload it to CVM in advance. Open the following link in the browser of the CVM to download the script for EIP direct connection:

https://windows-1254277469.cos.ap-guangzhou.myqcloud.com/eip_windows_direct.bat

**Step 2: configure the secondary ENI**

1. Log in to the CVM Console.
2. On the Instances page, click the configured CVM ID to go to the Basic Information page.
3. Select the ENI tab and click Bind ENI to create an ENI that is in the same subnet as the primary ENI.
4. In the pop-up window, select **Create and Bind an ENI**, enter the information, select **Automatic Assignment** in Assign IP section and click **OK**.

**Step 3: configure EIP direct connection for the primary ENI**
1. Log in to the EIP Console.
2. Find the EIP that is bound to the primary ENI and choose More -> Direct Connection in the Operation column on the right.

**Step 4: configure IP in CVM**

1. Log in to the CVM. This operation may cause public network interruption. Therefore, you need to Log in to a Windows instance via VNC.
2. On the operating system page, select 📱 in the lower-left corner and click ⏯️ to open the Windows PowerShell window. Enter `firewall.cpl` and press Enter to open the Windows Firewall page.
3. Click Turn Windows Firewall on or off to go to the Customize Settings page.

![Image of Windows Firewall settings](image)

4. Select Turn off Windows Firewall both in the Private network settings pane and the Public network settings pane.
5. Double-click to run the script downloaded in Step 1. Enter the public IP address and press Enter twice.

6. Enter `ipconfig` in the **Windows PowerShell** window and press Enter. You can see that the IPv4 address on the primary ENI changes to the public network address.

When the direct connection is enabled, you cannot assign a private IP to the primary ENI. Otherwise, the CVM cannot access the public network.
Cloud Block Storage
Expand cloud disks

Scenario

A cloud disk is an expandable storage device on the cloud. After a cloud disk is created, you can expand its capacity at any time to increase its storage capacity without losing any data. After a cloud disk is expanded, you need to allocate the added capacity to existing partitions or new partitions. Please refer to Expanding Windows File System or Expanding Linux File System.

MBR disks support a maximum disk capacity of 2TB. If your disk is a MBR disk and needs to be expanded to more than 2TB, we recommend that you create and mount a new data disk, initialize it to GPT, and copy the data on the MBR disk to the new disk.

Expanding data disks

Expanding via the Cloud Block Storage (CBS) Console
1. Log in to the CBS Console.
2. Select **More > Expand** to the right of the cloud disk you want to expand.
3. Select a new capacity. It must be greater than or equal to the current capacity.
4. Complete the payment.
5. Allocate the added capacity to existing partitions or new partitions. For details, see Expanding Windows File System or Expanding Linux File System depending on the operating system of the cloud services you want to use.

Expanding via the CVM Console
1. Log in to the CVM Console.
2. Select **More > Resource Adjustment > Adjust Disk** to the right of the CVM you want to make change to.
3. Select a new capacity. It must be greater than or equal to the current capacity.
4. Complete the payment.
5. Allocate the added capacity to existing partitions or new partitions. For details, see Expanding Windows File System or Expanding Linux File System depending on the operating system of the cloud services you want to use.

**Expanding via API**

You can create a snapshot with the ResizeCbsStorage API. For details, see ResizeDisk.

**Expanding system disks**

If a system disk is a cloud disk, you can expand it, but only by reinstall the system of the CVM.
Change Disk Media Type

Last updated: 2020-06-05 10:31:31

Scenario

Tencent Cloud CVM supports the adjustment of storage hardware media, which enables you to flexibly respond to different storage needs of different services. Tencent Cloud provides two types of block storage, i.e., Cloud Block Storage and Local Storage. We currently support the change of local disks to cloud disks. This document describes how to change disk media type.

The downside of CVMs with local disks:

- The configuration cannot be customized due to the limit of host resources.
- Features such as snapshots and creation acceleration are not supported.
- Low data reliability.
- Host failures will have a longer impact.

To avoid the downside of CVMs with local disks, you can change the existing CVMs with local disks in your account to CVMs with cloud disks.

Prerequisites

- **CVM Status**
  This operation can only be done when a CVM is in the **Shut down** state. Please shut down your CVM first.

- **CVM Type**
  - Spot CVMs do not support the change of local disks to cloud disks.
  - Dedicated CVMs do not support the change of local disks to cloud disks.
  - CVMs such as big data model D1 and D2 and high I/O model I3 and I4 do not support the change of local disks to cloud disks.
  - Bare metal instances do not support the change of local disks to cloud disks.

- **CVM Configuration**
  - You can change local disks to cloud disks only when there is at least one **regular local disk** or **SSD local disk** among the system disk and data disks of the CVM.
  - You can change local disks to cloud disks only when cloud disks are available in the availability zone of the CVM and the size of the local disks is within the range supported by cloud disks.
If both the system disk and the data disks of the CVM are local disks, when you change the disk media type, it will apply to all of the local disks of the CVM. You will also be able to configure the cloud disk type for each disk separately. That means when you change the disk media type for a CVM whose disks are all local disks, you cannot change only the system disk or only the data disks to cloud disks. If you make the change, it will apply to all the disks.

Changing the media type of a disk will not change its size. After you change the media type, you may expand cloud disks.

Changing local disks to cloud disks will not change the life cycle of a CVM, instance ID, internal/external network IP, disk name, and mount point.

Notes

- When you change a local disk to a cloud disk, all the data from the local disk needs to be copied to the cloud disk. Depending on the disk size and transmission speed, this could take some time.
- You can only change local disks to cloud disks, not the other way around.
- **It is recommended to start and log in to the CVM to check if there is any data loss after the change is completed.**

Directions

1. Log in to the CVM console and go to **Instances**.

   If the CVM has already been shut down, go to **Step 3**.

2. To the right of the CVM you want to make change to, click **More > Instance Status > Shutdown** to shut down the CVM.

3. To the right of the CVM you want to make change to, click **More > Resource Adjustment > Change Disk Media Type**.

4. In the pop-up window, select the cloud disk type you want to use for the system disk and the data disks, check the consent box, and click **Convert Now**.

5. Double-check the information, make a payment if applicable, and wait for the process to complete.
Security

Security Groups

Security Groups

A security group is a virtual firewall and features stateful data packet filtering. It is used to configure the network access control of CVM, Cloud Load Balancer, TencentDB, and other instances, while controlling their outbound and inbound traffic. It is an important means of network security isolation. You can configure security group rules to allow or reject inbound traffic and outbound traffic of instances within the security group.

Security group features

- A security group is a logical group. You can add CVM, ENI, TencentDB, and other instances in the same region with the same network security isolation requirements to the same security group.
- By default, instances associated with the same security group are not interconnect with each other, unless you add relevant rules.
- Security groups are stateful. Inbound traffic you have allowed can automatically go outward and vice versa.
- You can modify security group rules at any time, and the new rules take effect immediately.

Security group rules

Components

A security group rule consists of the following components:

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

Rule Priorities

- Security group rules have priorities, which are indicated by their positions in the list. The rule at the top of the list has the highest priority and is the first to be applied. The rule at the bottom has the lowest priority.
In case of rule conflict, the rule that is higher in the list prevails. When traffic enters or exits an instance that is bound to a security group, the security group rules will be matched in order from top to bottom. If a rule is matched successfully, the traffic is allowed to pass and the system no longer matches it with subsequent rules.

**Multiple security groups**

An instance can be bound with one or multiple security groups. When it is bound with multiple security groups, the security group rules will be matched in order from top to bottom. You can adjust security group priorities at any time.

**Security group templates**

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

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

If these templates cannot meet your actual needs, you can create custom security groups. For details, see [Creating a Security Group](https://intl.cloud.tencent.com/document/product/213/15379) and [Security group use cases](https://intl.cloud.tencent.com/document/product/213/15379).

- If you need to protect the application layer (HTTP/HTTPS), you can purchase Tencent Cloud Web Application Firewall (WAF). It defends web security at the application layer against web vulnerabilities, malicious crawlers, and CC attacks, helping protect your websites and web applications.

**Use Limits**

For use limits and quotas of security groups, see security group limits in [Use Limits Overview](https://intl.cloud.tencent.com/document/product/213/15379).
Directions

The process to use the security group is shown in the following figure:
Creating a Security Group

Scenario

Security Groups act as virtual firewalls for CVMs. Each CVM instance must associate with at least one security group. By default, each CVM instance has two templates (Open all ports and Open port 22, 80, 443, 3389 and ICMP protocol) for creating a default security group. For details, refer to Security Group Overview.

If the default security group does not meet your needs, you can create your own security group as instructed below.

Directions

1. Log in to the CVM Console.
2. In the left sidebar, select Security Group. The Security Group page then appears.
3. Select a region for the security group. Click +New.
4. In the Create a security group page, complete the following configurations:

   ◦ Template: select a template that suits your needs, as shown below:
<table>
<thead>
<tr>
<th>Template</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open all ports</td>
<td>All ports are open. May present security issues.</td>
<td>-</td>
</tr>
<tr>
<td>Open port 22, 80, 443, 3389 and ICMP protocol</td>
<td>Port 22, 80, 443 and 3389, and the ICMP protocol are open. All ports are open internally.</td>
<td>Suitable for instances with web services.</td>
</tr>
<tr>
<td>Custom</td>
<td>Creates a blank security group in which rules are added afterwards. For details on how to add rules, refer to this article.</td>
<td>-</td>
</tr>
</tbody>
</table>

- Name: name of the security group.
- Project: by default, Default project is selected. Select a project for better management.
- Notes: a short description for the security group.

5. Click OK to create the security group.

If you select Custom as the template for your security group, click Add rules now to add security group rules.
Adding Security Group Rules

Last updated: 2020-03-06 10:50:17

Scenario

Security groups are used to manage traffic to and from public and private networks. For the sake of security, most inbound traffic is denied by default. If you selected Open all ports or Open port 22, 80, 443, 3389 and ICMP protocol as the template when creating a security group, rules are automatically created and added to the security group to allow traffic on those ports. For details, refer to Security Groups.

This article describes how to add security group rules to allow or ban traffic to and from public or private networks.

Notes

- Security group rules support IPv4 and IPv6 rules.
- Open all ports allows both IPv4 and IPv6 traffic.

Prerequisites

- You should have an existing security group. If you do not, refer to Create a Security Group for details.
- You should have a clear understanding about which traffic is allowed or banned for your CVM instance. For more information on security group rules and their use cases, refer to Security group use cases.

Directions

1. Log in to the CVM Console.
2. In the left sidebar, select Security Group. The Security Group page then appears.
3. On the Security Group page, select a region, and find the security group for which you want to set rules.
4. Locate the desired security group and click the corresponding Modify Rules button to go to the Security Group Rule page.
5. Click **Inbound rules** and choose one of the following methods to add rules.

The following instructions use method two **Add a rule** as an example.

- Open all ports: this method is ideal if you do not need custom ICMP rules and all traffic goes through ports 20, 21, 22, 80, 443, and 3389 and the ICMP protocol.
- Add a rule: this method is ideal if you need to use multiple protocols and ports other than those mentioned above.

6. Click **Add a Rule** to bring up the **Add Inbound Rule** window.

Configure the following parameters:

- **Type**: by default, **Custom** is selected. You can select other types such as **Login Windows CVMs (3389)**, **Login Linux CVMs (22)**, **Ping**, **HTTP (80)**, **HTTPS (443)**, **MySQL (3306)**, and **SQL Server (1433)**.
- **Source or Destination**: traffic origin (inbound rules) or target (outbound rules). You can use one of the following to define Source or Destination:

<table>
<thead>
<tr>
<th>Source or Destination</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 addresses or ranges</td>
<td>in CIDR format 203.0.113.0, 203.0.113.0/24 or 0.0.0.0/0. 0.0.0.0/0 indicates all IPv4 addresses.</td>
</tr>
<tr>
<td>IPv6 addresses or ranges</td>
<td>in CIDR format, such as FF05::B5, FF05:B5::/60, ::/0 or 0::0/0. ::/0 or 0::0/0 indicates all IPv6 addresses.</td>
</tr>
<tr>
<td>ID of referenced security group.</td>
<td>- Current security group: CVMs associated with the current security group.</td>
</tr>
<tr>
<td></td>
<td>- Other security group: ID of another security group in the same region that belongs to the same project.</td>
</tr>
<tr>
<td>Reference IP address objects or IP group objects in a Parameter Template.</td>
<td>-</td>
</tr>
</tbody>
</table>

- **Protocol port**: `protocol:port`. You can also reference protocol/port or protocol/port groups in a Parameter Template.
- **Policy**: Allow or Refuse. By default, Allow is selected.
  - Allow: traffic to this port is allowed.
  - Refuse: data packets are dropped without any response.
- **Remarks**: a short description of the security group rule.
7. Click **Complete** to finish adding the rule.

8. To add an outbound rule, click **Outbound rule** and refer to **Step 5 to Step 7**.
Security Groups can be associated with CVMs, ENIs, cloud databases and CLBs. In this document, we use CVMs for example.

**Scenario**

A security groups can be associated with one or more CVMs for network access control. They are an important part of CVM network security measures. You can associate your CVM with one or more security groups if necessary. The following are detailed instructions.

**Prerequisites**

You should already have an CVM instance created before starting.

**Directions**

1. Log in to the CVM Console.
2. In the left sidebar, select **Security Group**. The Security Group page then appears.
3. Select the desired region and find the security group.
4. Under **Operations**, click **Manage Instances** that corresponds to the desired security group. The **Bind with Instance** page then appears.
5. Click **Add Instances**. The **Add Instances** page then appears.
6. Select desired instances and click **OK** to add.

**See Also**

- You can check all security groups in a specific region. See Viewing Security Groups.
If you want disassociate a CVM instance with one or more security groups, you can remove it from the security group.

See Removing From Security Groups.

If you no longer need a security group, you can delete it. Once a security group is deleted, all rules within it are also deleted.

See Deleting Security Groups.
Managing Security Groups
Viewing Security Groups

Scenario

This article describes how to view all security groups of a region.

Directions

**View security groups**

1. Log in to the CVM Console.
2. In the left sidebar, select Security Group. The Security Group page then appears.
3. Select a region to see a list of security groups under that region.

**Search for a security group**

You can also use the search bar on the Security Group page to quickly find a specific security group.

1. Log in to the CVM Console.
2. In the left sidebar, select Security Group. The Security Group page then appears.
4. Click the search bar and use one of the following fields to search for a security group.

- Security Group ID: input the desired ID and click to see the corresponding security group.
- Security Group Name: input the desired name and click to see the corresponding security group.
- Tag: input a tag and click to see a list of all security groups with that tag.

Other Operations
To learn more about how to search for a security group, click .
Deleting a Security Group

Scenario

If you no longer need a security group, you can delete it. Once a security group is deleted, all rules within it are also deleted.

Prerequisites

Before deleting a security group, you must remove all associated CVM instances. Otherwise, the operation will fail. For details, refer to Removing From Security Group.

Directions

1. Log in to the CVM Console.
2. In the left sidebar, select Security Group. The Security Group page then appears.
3. Select the desired region and find the security group to be deleted.
4. Locate the desired security group and click Delete.
5. In the pop-up window, click OK.
Remove from Security Groups

Last updated : 2020-03-06 11:37:16

Scenario

You can remove a CVM instance from a security group if necessary.

Prerequisites

The instance is associated with two or more security groups.

Directions

1. Log in to the CVM Console.
2. In the left sidebar, select Security Group. The Security Group page then appears.
3. Select the desired region and find the desired security group.
4. Click the corresponding Manage Instances button to go to the Bind with Instance page.
5. Select the instances to be removed and click Remove Selected.
6. In the pop-up window, click OK.
Cloning Security Groups

Scenario

You might need to clone a security group if you:

- Have created a security group sg-A in region A and you want to apply the same rules to an instance in region B. You can clone sg-A to region B, instead of creating a new security group from scratch.
- Need a new security group for your service but want to clone the old security group as a backup.

Notes

- By default, when you clone a security group, only the rules are cloned, not the association with instances.
- You can clone a security group across projects and regions.

Directions

1. Log in to the CVM Console.
2. In the left sidebar, select Security Group. The Security Group page then appears.
3. Select desired region. A list of security groups under the region then appears.
4. Locate the desired security group and click More. Then click Clone. The Clone security group page then appears.
5. Select a Target region and Target project and input a New name for the new security group. Click OK.
Adjusting Security Group Priority

Last updated: 2020-06-02 10:20:25

Scenario

You can bind one or more security groups to a CVM. If you have bound multiple security groups, these security groups are executed based on their priorities, such as 1, 2, and 3. You can adjust the priorities as follows.

Prerequisites

The instance is associated with two or more security groups.

Directions

1. Log in to the CVM console.
2. On the instance management page, click the ID of the CVM instance to go to the details page.
3. Click the Security Group tab to go to the security group management page.
4. In the "Bound Security Group" section on the right, click Order and select ☐ to the right of the group. Then, drag the security groups up or down to adjust their priorities. The security group at a higher position has a higher priority.
5. After finishing the adjustment, click Save.
Managing Security Group Rules
Viewing Security Group Rules

Scenario

After adding a security group rule, you can view its details in the console.

Prerequisites

You have created a security group and added at least one rule.
For information on how to create a security group and a security group rule, refer to Creating a Security Group and Adding Security Group Rules.

Directions

1. Log in to the CVM Console.
2. In the left sidebar, select Security Group. The Security Group page then appears.
3. On the Security Group page, select a region, and find the security group for which you want to view rules.
4. Click the name or ID or the desired security group to go to the details page.
5. Select Inbound rule or Outbound rule to view all inbound or outbound security group rules.
Modifying Security Group Rules

Last updated : 2020-03-06 11:43:58

Scenario

This article describes how to modify a security group rule. Rules are important because they protect your CVM instance from malicious attacks. For example, they can protect certain ports from being abused.

Prerequisites

Make sure you have created a security group with rules.
Refer to Creating Security Groups and Adding Security Group Rules.

Directions

1. Log in to the CVM Console.
2. In the left sidebar, select Security Group. The Security Group page then appears.
3. Select the desired region and find the security group.
4. Locate desired security group and click Modify Rules. The Security Group Rule page then appears.
5. Use Inbound rule and Outbound rule to switch between inbound and outbound security group rules.
6. Locate the desired rule and click Edit to modify it.

You don’t need to reboot the CVM for the rule changes to take effect.
Importing Security Group Rules

Scenario

Security group rules can be imported from a file. You can use this feature to quickly restore or create security group rules.

Directions

1. Log in to the CVM Console.
2. In the left sidebar, select Security Group. The Security Group page then appears.
3. Select desired region to see a list of security groups.
4. Locate desired security group and click its name. Security Group Rule page appears.
5. Select inbound or outbound rules by clicking Inbound rule or Outbound rule.
7. Click Browse and select a rule template file. Click Import.

- If there are existing rules in the security group, export them before importing new rules. Existing rules are overwritten after importing.
- If there is no existing rules in the security group, download the template first. Use it as a start to modify rules to your liking. Import them once you are finished.
Exporting Security Group Rules

Scenario

You can export security group rules and save them locally for backup.

Directions

1. Log in to the CVM Console.
2. In the left sidebar, select Security Group. The Security Group page then appears.
3. Select a region to display a list of security groups.
4. Click the name or ID of the desired security group. The details page of the selected security group appears.
5. Select inbound or outbound rules by clicking Inbound rules or Outbound rules.
6. Click to export security group rules to a file and save it to your local device.
Delete security group policies

Scenario

If you no longer need a security group rule, you can delete it.

Prerequisites

- You have created a security group and added at least one rule to it. For information on how to create a security group and add security group rules to it, see Creating a Security Group and Adding Security Group Rules.
- You have confirmed that your CVM instance does not need to permit or forbid Internet access or private network access.

Directions

1. Log in to the CVM console.
2. In the left sidebar, click Security Group. The "Security Group" page then appears.
3. On the security group management page, select Region and locate the security group whose rules you want to delete.
4. In the action column, click Modify Rules to go to the security group rule page.
5. Select inbound or outbound rules by clicking Inbound rules or Outbound rules.
6. Locate the security group rule to delete and click Delete in the action column.
7. In the window that appears, click OK.
Security Group Use Cases

Last updated : 2020-06-02 09:49:37

By configuring security groups, you can manage access to a Cloud Virtual Machine (CVM). You can configure inbound and outbound rules for security groups to specify whether your server can be accessed by or can access other network resources.

The default inbound and outbound rules for security groups are as follows:

- **To ensure data security, the inbound rule for a security group is a rejection policy that forbids remote access from external networks.** To enable external network access to your CVM, you need to permit the inbound rule of the corresponding port.
- The outbound rule for a security group specifies whether your CVM can access external network resources. If you select "Open All Ports" or "Open Ports 22, 80, 443, and 3389 and ICMP", the outbound rule for the security group opens all ports to the Internet. If you select a custom security group rule, the outbound rule blocks all ports by default, and you need to configure the outbound rule to allow the corresponding port to access external network resources.

Common Use Cases

This document describes several common use cases of security groups. If the following cases meet your requirements, you can configure the security groups according to the recommended configurations for the corresponding use cases.

**Scenario 1: Remotely connecting to a Linux CVM through SSH**

**Case**: you have created a Linux CVM and want to remotely connect to it through SSH.

**Solution**: when adding a security group rule, set **Type** to **Linux login** and open TCP port 22 to the Internet to enable Linux login through SSH.

You can open all IP addresses or a specified IP address (or IP range) to the Internet as required. This allows you to configure the source IP addresses of the CVMs that can be remotely connected to through SSH.

<table>
<thead>
<tr>
<th>Direction</th>
<th>Type</th>
<th>Source</th>
<th>Protocol Port</th>
<th>Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound</td>
<td>Linux login</td>
<td>• All IP addresses: 0.0.0.0/0</td>
<td>TCP: 22</td>
<td>Allow</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Specified IP address: enter your specified IP address or IP range</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Scenario 2: Remotely connecting to a Windows CVM through RDP

**Case:** you have created a Windows CVM and want to remotely connect to it by using Remote Desktop (RDP).

**Solution:** when adding a security group rule, set **Type** to **Windows Login** and open TCP port 3389 to the Internet to enable remote login to Windows.

You can open all IP addresses or a specified IP address (or IP range) to the Internet as required. This enables you to configure the source IP addresses of the CVMs that can be remotely connected to through RDP.

<table>
<thead>
<tr>
<th>Direction</th>
<th>Type</th>
<th>Source</th>
<th>Protocol Port</th>
<th>Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound</td>
<td>Windows login</td>
<td>• All IP addresses: 0.0.0.0/0&lt;br&gt;• Specified IP address: enter your specified IP address or IP range</td>
<td>TCP: 3389</td>
<td>Allow</td>
</tr>
</tbody>
</table>

Scenario 3: Pinging a CVM on the Internet

**Case:** you have created a CVM and want to test whether its communication with other CVMs is normal.

**Solution:** test the connection by using the ping command. Specifically, when adding a security group rule, set **Type** to **Ping** and open Internet Control Message Protocol (ICMP) ports to the Internet to enable other CVMs to access this CVM through ICMP.

You can open all IP addresses or a specified IP address (or IP range) to the Internet as required. This allows you to configure the source IP addresses of the CVMs that can access this CVM through ICMP.

<table>
<thead>
<tr>
<th>Direction</th>
<th>Type</th>
<th>Source</th>
<th>Protocol Port</th>
<th>Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound</td>
<td>Ping</td>
<td>• All IP addresses: 0.0.0.0/0&lt;br&gt;• Specified IP address: enter your specified IP address or IP range</td>
<td>ICMP</td>
<td>Allow</td>
</tr>
</tbody>
</table>

Scenario 4: Remotely logging in to a CVM through Telnet

**Case:** you want to remotely log in to a CVM by using Telnet.

**Solution:** when adding a security group rule, configure the following security group rule:

<table>
<thead>
<tr>
<th>Direction</th>
<th>Type</th>
<th>Source</th>
<th>Protocol Port</th>
<th>Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound</td>
<td>Custom</td>
<td>• All IP addresses: 0.0.0.0/0</td>
<td>TCP: 23</td>
<td>Allow</td>
</tr>
</tbody>
</table>
Scenario 5: Allowing access to a web service through HTTP or HTTPS

**Case:** you have built a website and want to allow users to access your website through HTTP or HTTPS.

**Solution:** when adding a security group rule, configure the following security group rules as required:

- **Allow all public IP addresses to access this website**

<table>
<thead>
<tr>
<th>Direction</th>
<th>Type</th>
<th>Source</th>
<th>Protocol Port</th>
<th>Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound</td>
<td>HTTP (80)</td>
<td>0.0.0.0/0</td>
<td>TCP: 80</td>
<td>Allow</td>
</tr>
<tr>
<td>Inbound</td>
<td>HTTPS (443)</td>
<td>0.0.0.0/0</td>
<td>TCP: 443</td>
<td>Allow</td>
</tr>
</tbody>
</table>

- **Allow some public IP addresses to access this website**

<table>
<thead>
<tr>
<th>Direction</th>
<th>Type</th>
<th>Source</th>
<th>Protocol Port</th>
<th>Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound</td>
<td>HTTP (80)</td>
<td>IP address or IP range that is allowed to access your website</td>
<td>TCP: 80</td>
<td>Allow</td>
</tr>
<tr>
<td>Inbound</td>
<td>HTTPS (443)</td>
<td>IP address or IP range that is allowed to access your website</td>
<td>TCP: 443</td>
<td>Allow</td>
</tr>
</tbody>
</table>

Scenario 6: Allowing an external IP address to access a specified port

**Case:** you have deployed a service and want the specified service port (such as port 1101) to be externally accessible.

**Solution:** when adding a security group rule, set Type to Custom and open TCP port 1101 to the Internet to allow external access to the specified service port.

You can open all IP addresses or a specified IP address (or IP range) to the Internet as required. This allows the source IP address to access the specified service port.

<table>
<thead>
<tr>
<th>Direction</th>
<th>Type</th>
<th>Source</th>
<th>Protocol Port</th>
<th>Policy</th>
</tr>
</thead>
</table>
| Inbound   | Custom| • All IP addresses: 0.0.0.0/0
• Specified IP address: enter your specified IP address or IP range | TCP: 1101     | Allow  |
Scenario 7: Rejecting access to a specified port by external IP addresses

**Case**: you have deployed a service and want to prevent external access to a specified service port (such as port 1102).

**Solution**: when adding a security group rule, set **Type** to **Custom**, configure TCP port 1102, and set **Policy** to **Reject** to reject external access to the specified service port.

<table>
<thead>
<tr>
<th>Direction</th>
<th>Type</th>
<th>Source</th>
<th>Protocol Port</th>
<th>Policy</th>
</tr>
</thead>
</table>
| Inbound   | Custom | • All IP addresses: 0.0.0.0/0  
• Specified IP address: enter your specified IP address or IP range | TCP: 1102 | Reject |

Scenario 8: Allowing a CVM to access only a specified external IP address

**Case**: you want your CVM to access only a specified external IP address.

**Solution**: add two outbound security group rules by referring to the following configuration.

- Allow the CVM instance to access a specified external IP address
- Forbid the CVM instance from accessing any public IP addresses through any protocol

Rules that permit access take priority over those that forbid access.

<table>
<thead>
<tr>
<th>Direction</th>
<th>Type</th>
<th>Source</th>
<th>Protocol Port</th>
<th>Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outbound</td>
<td>Custom</td>
<td>Specified public IP address that can be accessed by the CVM</td>
<td>Required protocol and port</td>
<td>Allow</td>
</tr>
<tr>
<td>Outbound</td>
<td>Custom</td>
<td>0.0.0.0/0</td>
<td>All</td>
<td>Reject</td>
</tr>
</tbody>
</table>

Scenario 9: Prohibiting a CVM from accessing a specified external IP address

**Case**: you do not want your CVM to access a specified external IP address.

**Solution**: add a security group rule by referring to the following configuration.

<table>
<thead>
<tr>
<th>Direction</th>
<th>Type</th>
<th>Source</th>
<th>Protocol Port</th>
<th>Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outbound</td>
<td>Custom</td>
<td>Specified public IP address that you do not want your CVM instance to access</td>
<td>All</td>
<td>Reject</td>
</tr>
</tbody>
</table>
Scenario 10: Uploading or downloading a file from a CVM through FTP

Case: you want to upload a file to or download a file from a CVM by using FTP software.
Solution: add a security group rule by referring to the following configuration.

<table>
<thead>
<tr>
<th>Direction</th>
<th>Type</th>
<th>Source</th>
<th>Protocol Port</th>
<th>Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound</td>
<td>Custom</td>
<td>0.0.0.0/0</td>
<td>TCP: 20 or 21</td>
<td>Allow</td>
</tr>
</tbody>
</table>

Combination of Multiple Scenarios

In an actual scenario, you may need to configure multiple security group rules based on your business requirements, such as configuring inbound or outbound rules at the same time. One CVM may be bound to one or more security groups. When a CVM is bound to multiple security groups, security groups are matched and executed in descending order of priority. You can adjust the priority of a security group at any time. For information on the priorities of security group rules, see Security Group Priorities.
This document describes common server ports. For more information on service application ports for Windows, see [Service Overview and Network Port Requirements for Windows](#).

<table>
<thead>
<tr>
<th>Port</th>
<th>Service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>21</td>
<td>FTP</td>
<td>An open FTP server port for uploading and downloading.</td>
</tr>
<tr>
<td>22</td>
<td>SSH</td>
<td>An SSH port for remotely connecting to Linux servers in CLI mode.</td>
</tr>
<tr>
<td>25</td>
<td>SMTP</td>
<td>An open SMTP server port for sending emails.</td>
</tr>
<tr>
<td>80</td>
<td>HTTP</td>
<td>A port for web services, such as IIS, Apache, and Nginx, to provide external access.</td>
</tr>
<tr>
<td>110</td>
<td>POP3</td>
<td>A port for the POP3 (email protocol 3) service.</td>
</tr>
<tr>
<td>137, 138, 139</td>
<td>NetBIOS protocol</td>
<td>Ports 137 and 138 are UDP ports for transferring files through My Network Places. Port 139: connections established through port 139 attempt to access the NetBIOS/SMB service. This protocol is used for file and printer sharing on Windows and SAMBA.</td>
</tr>
<tr>
<td>143</td>
<td>IMAP</td>
<td>A port for Internet Message Access Protocol (IMAP) v2, which is a protocol for receiving emails like POP3.</td>
</tr>
<tr>
<td>443</td>
<td>HTTPS</td>
<td>A port for web browsing. HTTPS is a variant of HTTP that provides encryption and transmission over secure ports.</td>
</tr>
<tr>
<td>1433</td>
<td>SQL Server</td>
<td>Default port for SQL Server. The SQL Server service uses two ports: TCP-1433 and UDP-1434. Port 1433 is used to provide external services, and port 1434 is used to return a response to the requester to indicate the TCP/IP port used by SQL Server.</td>
</tr>
<tr>
<td>3306</td>
<td>MySQL</td>
<td>Default port for MySQL databases, which is used by MySQL to provide external services.</td>
</tr>
<tr>
<td>3389</td>
<td>Windows Server Remote Desktop Services</td>
<td>Service port for the Windows Server remote desktop, through which you can connect to a remote server by using the &quot;Remote Desktop&quot; connection tool.</td>
</tr>
<tr>
<td>Port</td>
<td>Service</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>----------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>8080</td>
<td>Proxy port</td>
<td>Similar to port 80, port 8080 is used in the WWW proxy service for web browsing. The port number &quot;:8080&quot; is often appended to the URL when you visit a website or use a proxy. In addition, after the Apache Tomcat web server is installed, its default service port is port 8080.</td>
</tr>
</tbody>
</table>
# Security Group API Overview

Last updated: 2020-04-22 12:24:49

<table>
<thead>
<tr>
<th>API Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CreateSecurityGroup</td>
<td>Create security groups</td>
</tr>
<tr>
<td>CreateSecurityGroupPolicies</td>
<td>Create security group rules</td>
</tr>
<tr>
<td>DeleteSecurityGroup</td>
<td>Delete security groups</td>
</tr>
<tr>
<td>DeleteSecurityGroupPolicies</td>
<td>Delete security group rules</td>
</tr>
<tr>
<td>DescribeSecurityGroupAssociationStatistics</td>
<td>Query the statistics of the instances associated with a security group</td>
</tr>
<tr>
<td>DescribeSecurityGroupPolicies</td>
<td>Query security group rules</td>
</tr>
<tr>
<td>DescribeSecurityGroups</td>
<td>Query security groups</td>
</tr>
<tr>
<td>ModifySecurityGroupAttribute</td>
<td>Modify security group attributes</td>
</tr>
<tr>
<td>ModifySecurityGroupPolicies</td>
<td>Modify the inbound and outbound rules of a security group</td>
</tr>
<tr>
<td>ReplaceSecurityGroupPolicy</td>
<td>Replace a single security group rule</td>
</tr>
</tbody>
</table>
Protection of Sensitive Operations

Overview

CVM supports sensitive operation protection. Before you perform sensitive operations, you need to enter a credential that can prove your identity. After the authentication is passed, you can perform related operations.

The sensitive operation protection of CVM can effectively protect the security of account resources, including the shutdown, restart, password reset, and termination of CVM.

Enable Operation Protection

Tencent Cloud provides two ways to protect operations:

1. Provide operation protection by enabling MFA authentication.
2. Provide operation protection by enabling mobile verification code.

You can enable the operation protection through Access Management Console.

Operation Protection Verification

When you have enabled the operation protection, the system will first perform operation protection verification when you perform sensitive operations:

- If you have enabled MFA verification for operation protection, you need to enter the 6-bit dynamic verification code on the MFA device.
- If you have enabled mobile verification code for operation protection, you need to enter the mobile verification code.

As shown in the following figure, when you try to shut down an instance, the following verification box pops up, and you need to verify the MFA device:
How do I view the MFA verification code?

1. Turn on the MFA device:
   Open the Tencent Cloud Assistant Mini Program and select "Tools" to see the bound authenticator.

2. View the dynamic verification code of the corresponding account. The dynamic verification code is updated every 30 seconds.
Managing Login Password

Introduction

CVM accounts and passwords can be used as credentials for CVM instances. This article describes how to use and manage passwords when logging in to a CVM instance.

Password Requirements

A password must meet these requirements:

- Linux instance password: the password must consist of 8 to 30 characters. We recommend that you use a password of at least 12 characters. The password cannot start with / and must contain at least three of the following: (a-z, A-Z, 0-9 and special symbols `~!@#$%^&*-+=_|{[]};':<>?,./).
- Windows instance password: the password must consist of 12 to 30 characters. The password cannot start with / and must contain at least three of the following: (a-z, A-Z, 0-9 and special symbols `~!@#$%^&*-+=_|{[]};':<>?,./), and it cannot contain your user name.

Directions

Setting an initial password

There are two ways to set the initial password depending on how you configured your CVM instance when purchasing it:

- If you used the **Quick Configuration** option, the initial password is sent to you through an email and a message to the console **Message Center**.
- If you used the **Custom Configuration** option, the initial password is set in the following ways depending on how you choose to log in:

<table>
<thead>
<tr>
<th>Login Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatic password generation</td>
<td>The initial password is sent to you through email and the console <strong>Message Center</strong>.</td>
</tr>
<tr>
<td>Associate</td>
<td><strong>Disabled by default</strong>. You log in using your user name and password, but</td>
</tr>
<tr>
<td>keys now</td>
<td>the initial password is sent to you through email and the console Message Center.</td>
</tr>
<tr>
<td>Set a password</td>
<td>You set the initial password.</td>
</tr>
</tbody>
</table>

**Viewing the password**

Your login password is sent to you through email and the console Message Center. The following describes how to check your messages in the message center.

1. Log in to the CVM Console.
2. Click 💬 in the upper right corner and select the corresponding product message, as shown in the following figure:
View your password on the message page.

**CVM Created Successfully**

Dear Tencent Cloud user,

Your (Account Name) CVM (1 in total) is created successfully.

Server operating system is TKE Ubuntu18 64 bits optimized, the default account is ubuntu, the initial password is : [Redacted]

**Resource** | **Resource Configuration** | **Status**
---|---|---
| Zone | ap-guangzhou-3 | SUCCESS |
| Configuration | D2/8Core/32GB/1Mbps | | System Disk | CLOUD_PREMIUM/50GB | |

**Resetting the password**

For instructions on how to reset your password, refer to Resetting the Password of an Instance.
Managing SSH keys

Scenario

The password is a unique login credential for each CVM instance. To ensure the security of an instance, Tencent Cloud provides the following two login methods:

- Password Login
- SSH key pair login

This document describes common operations related to using SSH key pair to log in to an instance.

Directions

Creating SSH keys

1. Log in to the CVM Console.
2. In the left sidebar, click SSH Key.
3. In the SSH key management page, click Create a key.
4. In the Create an SSH key window that pops up, select how you will create the key, enter the related information, and click OK.
   - If you select Create a new key pair, enter the key name.
   - If you select Use an existing public key, enter the key name and the original public key information.
5. In the prompt box that pops up, click Download to download the private key.

Tencent Cloud does not save your private key information. Download and obtain the private key within 10 minutes.

Binding/Unbinding a key to or from a CVM

1. Log in to the CVM Console.
2. In the left sidebar, click SSH Key.
3. In the SSH key management page, select the SSH key of the CVM to be bound or unbound, and click Bind/unbind Instance.
4. In the **Bind/unbind Instance** window that pops up, select the region and the CVM to be bound or unbound, and click **OK**.

**Modifying the SSH key name and description**

1. Log in to the **CVM Console**.
2. In the left sidebar, click **SSH Key**.
3. In the SSH key management page, select the key to be modified, and click **Modify**.
4. In the **Modify a key** window that pops up, enter the new key name and description, and click **OK**.

**Deleting SSH keys**

If the SSH key is associated with a CVM or a custom image, it cannot be deleted.

1. Log in to the **CVM Console**.
2. In the left sidebar, click **SSH Key**.
3. In the SSH key management page, select all SSH keys to be deleted, and click **Delete**.
4. In the **Delete key** window that pops up, click **OK**.

**Using an SSH key to log in to a Linux CVM**

1. **Create an SSH key**.
2. **Bind an SSH key to a CVM**.
3. **Log in to a Linux instance using SSH**.
Scenario

This document describes how to manage spread placement groups.

Directions

Creating a placement group

1. Log in to the CVM placement group console.
2. Click Create.
3. In the window that appears, enter a name for the placement group, and select the layer of the placement group.
4. Click OK to finish the creation.

Starting up 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 the CVM, click Advanced Configuration, select Add Instance to Spread Placement Group, and select an existing placement group.
     If no existing placement groups meet your requirement, create one in the console.
   - When confirming the configuration information, enter the total number of instances to be added to the placement group, which must be less than the quantity limit set for the placement group.

Modifying an instance's placement group

Currently, you can change only the name of a placement group. To do this, complete the following steps.

1. Log in to the CVM placement group console.
2. Hover the cursor over the ID or name of the target placement group and click 𝐈𝐝 𝐄dıtıng.
3. In the window that appears, enter the new name.
4. Click **OK** to finish the modification.

**Deleting a placement group**

You can delete a placement group that needs to be replaced or is no longer needed. You must terminate all instances running in the placement group before you can delete it. To do this, complete the following steps.

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.
3. Return to the placement group console, select the placement group to be deleted, and click **Delete**.
4. In the window that appears, click **OK** to finish the deletion.
   You can delete a single placement group or multiple placement groups in batches.
Unblocking Port 25

Last updated: 2020-03-06 10:50:18

Introduction

This article describes how to unblock port 25.

Notes

- You can only unblock port 25 for five instances for each Tencent Cloud account.
- Make sure that you only use port 25 to connect to a third-party SMTP server for sending email. If you use your CVMs to send email directly, we reserve the right to permanently ban you from opening port 25.

Directions

1. Log in to the Tencent Cloud console.
2. Click your account name in the upper-right corner. Select Security Control.
3. In the left sidebar, click Unblock port 25 to go to the Unblock port 25 page.
4. Click Apply to unlock port 25 to bring up the Apply to unblock port 25 window.
5. Select a region and the CVM instance that need to be unblocked. Select I have read and agree to the port 25 usage agreement., as shown below:

   Make sure you have not used up your unblocking quota. You can check the remaining quota in the lower left of the Apply to unblock port 25 window.
6. Click **OK** to finish the process.
Tags
User guide on tags

Last updated : 2020-04-01 11:30:16

Scenario

A tag is a key-value pair provided to identify resources on the Tencent Cloud. Tags allow you to flexibly classify and manage your CVM resources by service, purpose, owner, and other aspects. Note that tags are not used by Tencent Cloud. They only help you to manage CVM resources.

Use Limits

Note the following limits when using tags:

- Quantity limits: Each Tencent Cloud resource can be bound to a maximum of 50 tags.
- Tag key limits:
  - Do not create tag keys prefixed with `qcloud`, `tencent`, and `project`, because they are reserved for the system.
  - A tag key can only contain digits, letters, and `+.-@`. It cannot exceed 255 characters in length.
- Tag value limits: A tag value can only contain empty strings or digits, letters, and `+.-@`. It cannot exceed 127 characters in length.

Directions and Cases

Case description

Case: A company purchased six CVM instances. The following table lists the information about the deployment departments, business scope, and owners of the six CVM instances.

<table>
<thead>
<tr>
<th>Instance ID</th>
<th>Deployment Department</th>
<th>Business Scope</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>ins-abcdef1</td>
<td>E-commerce</td>
<td>Marketing campaigns</td>
<td>John Smith</td>
</tr>
<tr>
<td>ins-abcdef2</td>
<td>E-commerce</td>
<td>Marketing campaigns</td>
<td>Wangwu</td>
</tr>
<tr>
<td>ins-abcdef3</td>
<td>Games</td>
<td>Game A</td>
<td>Jane Smith</td>
</tr>
<tr>
<td>Instance ID</td>
<td>Deployment Department</td>
<td>Business Scope</td>
<td>Owner</td>
</tr>
<tr>
<td>--------------</td>
<td>------------------------</td>
<td>-----------------</td>
<td>-----------</td>
</tr>
<tr>
<td>ins-abcdef4</td>
<td>Games</td>
<td>Game B</td>
<td>Wangwu</td>
</tr>
<tr>
<td>ins-abcdef5</td>
<td>Entertainment</td>
<td>Post-production</td>
<td>Wangwu</td>
</tr>
<tr>
<td>ins-abcdef6</td>
<td>Entertainment</td>
<td>Post-production</td>
<td>John Smith</td>
</tr>
</tbody>
</table>

For example, we can add the following tag key-value pairs to the ins-abcdef1 instance:

<table>
<thead>
<tr>
<th>Tag Key</th>
<th>Tag Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>dept</td>
<td>ecommerce</td>
</tr>
<tr>
<td>business</td>
<td>mkt</td>
</tr>
<tr>
<td>owner</td>
<td>johnsmith</td>
</tr>
</tbody>
</table>

Similarly, you can add tag key-value pairs to other instances based on the different settings of deployment departments, business scopes, and owners.

**Specify one or more tags in the CVM console**

Take the preceding case as an example. After designing the tag key-value pairs, you can log in to the CVM console to specify the tags.

1. Log in to the CVM console.
2. On the Instances page, select the instance to be bound to the tags. In the Operation column, click More and then choose Instance Settings > Edit Tags.
3. In the You have selected 1 resource window that appears, specify the tags as required. For example, you can add three tag key-value pairs to the ins-abcdef1 instance.
4. Click OK. The system displays a message indicating that the modification was successful.

**Filters instances by tag**

If you need to query instances bound to a specified class of tags, you can perform filtering as follows:

1. In the search box, select Tag.
2. After Tag, enter the specified tag key-value pair and then click to search for the tags.
   For example, if you need to query CVM resources owned by John Smith, you can enter Tag:owner:johnsmith.
Edit Tags

Last updated: 2020-04-28 14:31:47

Operation Scenario

This document describes how to edit tags of resources.

Use Limits

There are several limitations on editing tags:

- **Quantity**: each resource can have at most 50 tags.
- **Tag key limitations**:
  - You cannot create tag keys that start with `qcloud`, `tencent`, and `project` as they are reserved for the system.
  - Tag keys can only contain `numbers`, `alphabet characters`, `+=.@-`, and must be less than 255 characters.
- **Tag value**: tag values can only contain `empty strings or numbers`, `alphabet characters`, `+=.@-`, and must be less than 127 characters.

Prerequisites

Log in to the CVM Console.

Directions

**Editing the tag of a single instance**

1. On the Instance management page, select the instance of which the tags need to be edited and click **More > Instance Settings > Edit Tags**, as shown below.
2. Add, modify, or delete tags in the “1 cloud resource(s) selected” pop-up window based on your needs.

**Editing the tags of multiple instances**

You can batch edit tags of up to 20 resources at one time.

1. On the Instance management page, select the instances of which the tags need to be edited and click **More Actions > Instance Settings > Edit Tags** on the top, as shown below:

2. Add, modify, and delete tags in the “n cloud resource(s) selected” pop-up window based on your needs.

**Operation Examples**

For information on how to use tags, please see **User Guide on Tags**.
Monitoring and Alarms
Getting Monitoring Statistics

Last updated : 2020-05-06 15:18:58

Scenario

Tencent Cloud provides cloud monitoring for all users by default. Before cloud monitoring can collect monitoring data, the user must have used Tencent Cloud products. This document describes how to get monitoring data.

Directions

Get monitoring data from the cloud product console

Tencent Cloud provides a separate page for retrieving monitoring data on CVM console. On this page, you can view monitoring data such as CPU, memory, network bandwidth, disks of the CVM instances and adjust the time range.

1. Log in to the CVM Console.
2. In the instance management page, click the ID of the CVM to enter its details page and view the monitoring data.
3. Click the Monitoring tab to get the instance monitoring data.

Get monitoring data from Cloud Monitoring Console

Cloud Monitoring Console is the unified entrance for all product monitoring data. There you can view monitoring data such as CPU, memory, network bandwidth, disks of the CVM instances and adjust the time range.

1. Log in to Cloud Monitoring Console.
2. In the left sidebar, select Cloud Product Monitoring > Cloud Virtual Machine to enter the “Cloud Virtual Machine” monitoring page.
3. Click the ID of the CVM Instance to enter its details page and view the monitoring data.

**Get monitoring data through the API**

You can use the GetMonitorData API to get monitoring data for all products. For details, see [GetMonitorData](#).
Create Alarm Polices

Last updated: 2020-04-20 18:33:18

Scenario

You can create an alarm to trigger and send alarm notifications when Tencent Cloud services change statues. The created alarm can determine whether to trigger alarm notifications based on comparison between a monitoring metric and a specified threshold at every interval. Each alarm policy is a set of trigger conditions with the logic relationship "or", that is, an alarm is triggered when any of the conditions is met. The alarm is sent to all users associated with the alarm policy. Upon receiving the alarm, you can view it and take appropriate actions in time. Creating an alarm can help you increase application reliability. For more information on alarms, see Create Alarm Policy.

Prerequisites

1. Log in to Cloud Monitor Console.

Directions

Create alarms

1. On the left sidebar, click Alarm Configuration > Alarm Policy to enter the alarm policy management page.
2. Click Add to create a new policy.
3. On the “Create Policy” page, enter the policy name, select the policy type and alarm object, and configure the trigger condition.
   The trigger condition is a semantic condition consisting of metric, comparison, threshold, statistical period, continuous periods and repeat notification policy.
4. Click Complete.

Associate Objects

1. On the left sidebar, click Alarm Configuration > Alarm Policy to enter the alarm policy management page.
2. Click the newly created alarm policy to enter the alarm policy management page.
3. Click **Add Object** on the alarm policy management page.
4. In the pop-up “Associate Alarm Object” window, select the CVM you want to associate with, and then click **Apply**.

**Configure alarm recipient objects**

1. On the left sidebar, click **Alarm Configuration > Alarm Policy** to enter the alarm policy management page.
2. Click the newly created alarm policy to enter the alarm policy management page.
3. Locate **Alarm Recipient Object** on the alarm policy management page, and click **Edit**.
4. In the pop-up “Alarm Recipient Object” window, select the user groups you want to notify and click **Save**.
Introduction

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

Examples

Read and write (CVM)

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

Refer to Authorization Management for instructions on how to grant the preset policy QcloudCVMFullAccess to a user.

Read-only (CVM)

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

Refer to Authorization Management for instructions on how to grant the preset policy QcloudCVMInnerReadOnlyAccess to a user.

Read-only (CVM and associated resources)

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

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

Console Example

Last updated: 2020-05-08 12:55:34
All operations in the Monitor.

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

**CBS policies**

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

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

The detailed steps are as follows:

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

   Use the following as a syntax reference:

   ```json
   {
   "version": "2.0",
   "statement": [
   {
   "effect": "allow",
   "action": [
   "name/cvm:CreateCbsStorages",
   "name/cvm:AttachCbsStorages",
   "name/cvm:DetachCbsStorages",
   "name/cvm:ModifyCbsStorageAttributes",
   "name/cvm:DescribeCbsStorages"
   ],
   "resource": [
   "qcs::cvm::uin/1410643447:*"
   ]
   }
   ```
2. Find the created policy, and in the “Action” column of the row, click **Associate User/Group**.
3. In the “Associate User/Group” window, select the user/group you want to associate, and click **OK**.

**Security group policies**

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

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

The detailed steps are as follows:

1. Refer to **Policies** for information and create a custom policy that grants the permissions to create, delete, and modify security groups on the CVM console.

   Use the following as a syntax reference:

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

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

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

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

The detailed steps are as follows:

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

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

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

**Policy for authorizing users to perform operations on specific CVMs**

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

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

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

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

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

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

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

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

You can do this by using one of the following two solutions:
• **Solution A**
  The account owner of CompanyExample associate the preset policy QcloudCVMFullAccess with Developer. For more information, refer to Authorization Management.

• **Solution B**
  i. Use the following as a syntax reference and create a custom policy.

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

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

**Granting a sub-account the permission to manage projects**

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

The detailed steps are as follows:

1. Create a custom policy for project management.
   For more information, refer to Policies.

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

**Custom policy**

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