Cloud Virtual Machine
Operations Guide
Product Documentation
Copyright Notice

©2013-2019 Tencent Cloud. All rights reserved.

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

Trademark Notice

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

Service Statement

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

Operations Guide
   Operation Guide Overview
   Use Limits Overview
Instances
   Creating Instances
   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
Rename Instances
Reset Instance Password
Management instance IP address
   Obtaining the Private IP Address of an Instance and Private Network DNS Settings
   Modify Instance Private IP
   Obtaining a Public IP Address of the Instance
   Change Instance Public IP
   Retrieve the public network IP address
Change Instance Subnet
Change Security Group
Search Instances
Export Instances
Querying the Repossession Status of a Spot Instance
Shutdown Instances
Restart Instances
Logging into Linux Instance
   Log into Linux Instance Using Standard Login Method
   Logging into Linux Instance via SSH Key
   Logging into Linux Instance via Remote Login Tools
   Logging into Linux Instance via VNC
Logging into Windows instance
Logging into Windows Instance via Remote Desktop
Log in to the Windows instance using the RDP file (recommended)

Logging into Windows Instance via VNC

Reinstall System
Terminate Instances
Instance Expires
Spot Instances
No Charges When Shut down for Pay-as-You-Go Instances
Change Disk Media Type

Images
Create Custom Images
Copy Images
Share Custom Images
Cancel Image Sharing
Delete Custom Images
Import Images
  Overview
  Linux System Check virtio Driver
  Install Cloudbase-Init on Windows
  Install Cloud-Init on Linux
  Forcibly Import Image
Linux Image Creation
Windows Image Creation

Service Migration
Online Migration
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

Online Migration
Offline Migration
Contact Us
Network
  ENI
  Configuring a Public Gateway
  Switch to VPC
  Elastic Public IP
  EIP Direct Connection
Cloud Disks
  Expand cloud disks
Security
  Security Groups
    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
  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
  Operation Guide
  Limits
  Protection of Sensitive Operations
  Manage Login Password
  Managing SSH keys
  Spread Placement Group
  Unblocking Port 25
Tags
  User guide on tags
Requirements
Edit Tags
Filter Resources Based on Tags
Monitoring and Alarms
Get 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
Use Instance as Web Server

Use Instance as FTP Server

Overview of Common Ports

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
Use Limits Overview

Last updated: 2020-02-02 16:56:25

Account Limits for Purchasing CVM Instances

- You need to sign up for a Tencent Cloud account. For more information, please see Sign up for Tencent Cloud for registration instructions.
- You need to go through identity verification. For more information on how to verify your identity, please see Identity Verification Guide.
- When you create a postpaid CVM, the system will freeze the CVM fee for one hour. Make sure that the account has sufficient balance to pay for the order.

Use Limits for CVM Instances

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

Purchase Limits for CVM Instances

- For each user in each availability zone, the total quota for postpaid CVM instances is 30.
- For more information, please see Purchase Limits for CVM Instances.

Image Limits

- Public image and service marketplace image: none.
- Custom image: Each region supports a maximum of 10 custom images.
- Shared image: Each custom image can be shared to a maximum of 50 Tencent Cloud users, and can only be shared to the accounts in the same region as the source account.
- For more information, please see Image Type Limits.
ENI Limits

- The number of ENIs bound to a CVM is quite different from that of private IPs bound to an ENI depending on the CPU and memory configurations. These allowed numbers are shown in the following table:

<table>
<thead>
<tr>
<th>CVM Configuration</th>
<th>Max. Number of ENIs</th>
<th>Max. Number of IPs Bound to Each 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-core</td>
<td>2</td>
<td>10</td>
</tr>
<tr>
<td>CPU: 4-core Memory: &lt; 16 GB</td>
<td>4</td>
<td>10</td>
</tr>
<tr>
<td>CPU: 4-core Memory: &gt; 16 GB</td>
<td>4</td>
<td>20</td>
</tr>
<tr>
<td>CPU: 8- to 12-core</td>
<td>6</td>
<td>20</td>
</tr>
<tr>
<td>CPU: &gt;12-core</td>
<td>8</td>
<td>30</td>
</tr>
</tbody>
</table>

Bandwidth Limits

- Upper Limit of the Outbound Bandwidth (Downstream Bandwidth):

<table>
<thead>
<tr>
<th>Network Billing Method</th>
<th>CVM Billing Method</th>
<th>CVM Configuration</th>
<th>Available range of the upper limit of bandwidth (Mbps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bill-by-Traffic</td>
<td>Postpaid CVM</td>
<td>ALL</td>
<td>0-100</td>
</tr>
<tr>
<td></td>
<td>Prepaid CVM</td>
<td>Cores ≤ 8</td>
<td>0-200</td>
</tr>
<tr>
<td></td>
<td></td>
<td>8 &lt; Cores &lt; 24</td>
<td>0-400</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cores ≥ 24</td>
<td>0-400 or no speed limit</td>
</tr>
<tr>
<td>Bill-by-Bandwidth</td>
<td>Postpaid CVM</td>
<td>ALL</td>
<td>0-100</td>
</tr>
<tr>
<td></td>
<td>Prepaid CVM</td>
<td>Guangzhou</td>
<td>0-200</td>
</tr>
</tbody>
</table>
Upper Limit of the Inbound Bandwidth (Upstream Bandwidth):
- If the fixed bandwidth purchased by users is larger than 10 Mbps, Tencent Cloud assigns the public network inbound bandwidth that is equal to the purchased bandwidth.
- If the fixed bandwidth purchased by users is less than 10 Mbps, Tencent Cloud assigns 10 Mbps public network inbound bandwidth.

Disk Limits

<table>
<thead>
<tr>
<th>Limits on</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Elastic cloud disk capability</td>
<td>Since May 2018, all the data disks bought with instances are all elastic cloud disks. You can unmount them from your CVM and get them remounted. This capability is available in all Availability Zones.</td>
</tr>
<tr>
<td>Cloud disk performance</td>
<td>The I/O performance described in the product documentation. For example, a 1 TB SSD cloud disk can deliver up to 24,000 random IOPS. This means the 24,000 IOPS is achievable for both read and write operations. The I/O performances of 4 KB/8 KB can both reach this number, while the IO of 16 KB cannot reach 24,000 IOPS because its throughput has already reached the limit of 260 MB/s.</td>
</tr>
<tr>
<td>Maximum number of cloud disks per instance</td>
<td>20 at most</td>
</tr>
</tbody>
</table>
### Security Group Limits

- Security groups are region and project-specific. CVMs can only be associated with the security groups in the same region and project.
- Security groups apply to any CVM instances in network environment.
- Each user can set a maximum of 50 security groups for each project in each region.
- A maximum of 100 inbound/outbound access policies can be set for a security group.
- A CVM can be associated with multiple security groups, and a security group can be associated with multiple CVMs. No number limit is imposed.
- Security groups bound with CVMs in **basic network cannot filter** data packets sent from (or to) relational database (CDB) and cloud cache service (Redis and Memcached) of Tencent Cloud. If necessary, you can use iptables to filter traffic of such instances.
- The quota limits are as follows:

<table>
<thead>
<tr>
<th>Limits on</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of snapshots in a single region</td>
<td>64 + count of disks in the region * 64</td>
</tr>
<tr>
<td>Mounting elastic cloud storage to CVM</td>
<td>The instance and the elastic cloud storage must be in the same availability zone.</td>
</tr>
<tr>
<td>Snapshot rollback</td>
<td>Snapshot data can only be rolled back to the cloud disk from which the snapshot was created.</td>
</tr>
<tr>
<td>Allowed disk type for creating elastic cloud disks using snapshots</td>
<td>You can only use data disk snapshots to create new elastic cloud disks.</td>
</tr>
<tr>
<td>Allowed disk size for creating elastic cloud disks using snapshots</td>
<td>The size of the created elastic cloud disk must be bigger or equal to the size of the cloud disk from which the snapshot was created.</td>
</tr>
</tbody>
</table>
### Feature Count

<table>
<thead>
<tr>
<th>Feature</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security group</td>
<td>50/Region</td>
</tr>
<tr>
<td>Access policy</td>
<td>100 (Inbound/Outbound)</td>
</tr>
<tr>
<td>Number of instances associated with a security group</td>
<td>100</td>
</tr>
<tr>
<td>Number of security groups associated with an instance</td>
<td>5</td>
</tr>
<tr>
<td>Number of rules of a security group</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 VPCs in a region</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</td>
<td>100</td>
</tr>
<tr>
<td>Number of routing tables per VPC</td>
<td>10</td>
</tr>
<tr>
<td>Number of routing policies per routing table</td>
<td>100</td>
</tr>
<tr>
<td>Number of associated routing tables per subnet</td>
<td>1</td>
</tr>
<tr>
<td>Number of HAVIP per VPC</td>
<td>10</td>
</tr>
</tbody>
</table>
Instances
Creating Instances

Last updated: 2020-02-05 15:24:05

Scenario

This topic guides you through how to create a Tencent Cloud Virtual Machine (CVM) instance. The custom configuration mode is used as an example.

Prerequisites

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

- Sign Up for Tencent Cloud, 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 in the VPC.
- If you don’t want to use the default project, please create a new project.
- If you don’t want to 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 service requirements.
- To bind an SSH key pair during creating a Linux instance, you need to Create an 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.

Steps

1. Log in to Tencent Cloud. Choose Products > Compute > Cloud Virtual Machine. Click Contact Sales to open the CVM purchase page.

   - Quick Configuration: This mode is applicable to general scenarios. It helps users quickly purchase a CVM instance that meets general requirements.
   - Custom Configuration: This mode is applicable to specific scenarios. 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>Configuration</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
</table>
| Billing mode       | Yes      | Select a value as required:  
  - **Pay as you go**: An elastic billing mode for the CVM. It is applicable to scenarios such as sudden high sales volumes on e-commerce platforms where the number of required CVMs fluctuates dramatically. The unit price in this mode is three or four times more expensive than that in the monthly subscription mode.  
  For more information about billing modes, see [Billing Modes](#). |
| Region/Availability zone | Yes      |  
  - **Region**: The region closest to your customer is recommended, which reduces the access latency and increases the access speed.  
  - **Availability zone**: Select a value as required.  
    If you want to purchase multiple CVMs, we recommend that you select different availability zones to implement disaster recovery.  
    For more information about options for regions and availability zones, see [Regions and Availability Zones](#). |
| Network            | Yes      | Logically isolated space that is built in Tencent Cloud. A 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 in 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           | Yes      | Tencent Cloud provides different types of instances for different underlying hardware. To achieve optimal performance, new-generation instances are recommended.  
    For more information about instances, see [Instance Specifications](#). |
| Image              | Yes      | Tencent Cloud provides public images, custom images, shared images, and marketplaces. For more information about images, see [Image Types](#). |
| System disk        | Yes      | Used to install the operating system. By default, its |

©2013-2019 Tencent Cloud. All rights reserved.  
Page 18 of 285
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data disk</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Used to scale up the storage capacity of the CVM to ensure high efficiency and reliability. Cloud data disks are not added by default. For more information about cloud disks, see Cloud Disk Types.</td>
</tr>
<tr>
<td>Public network bandwidth</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>A free independent public IP address is allocated by default. Tencent Cloud provides two network billing modes. Set a value greater than 0 Mbit/s as required.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Bill-by-bandwidth</strong>: Select a fixed bandwidth. Packet loss occurs when this bandwidth is exceeded. This mode is applicable to scenarios where network connection fluctuation is slight.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Bill-by-traffic</strong>: Billing is based on the traffic that is actually used. You can specify a peak bandwidth to prevent from being charged for unexpected traffic. Packet loss occurs when the instantaneous bandwidth exceeds this value. This mode is applicable to scenarios where network connection fluctuation is heavy.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: The allocated free independent public IP address cannot be unbound from the instance. To unbind this IP address, convert the public IP address to an elastic public IP address, and then unbind the elastic public IP address. For more information about the elastic public IP address, see Elastic Public IP Address.</td>
</tr>
<tr>
<td>Public gateway</td>
<td>Yes</td>
</tr>
<tr>
<td></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. For more information, see Public Gateway.</td>
</tr>
<tr>
<td>Quantity</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>The number of CVMs to be purchased.</td>
</tr>
<tr>
<td>Duration</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Applicable only to CVMs with monthly subscription. It indicates the usage duration of a CVM.</td>
</tr>
</tbody>
</table>

3. Click **Next: Security Group and CVM** to open the Security Group and CVM page.
4. Configure the following information as prompted by the page:

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project</td>
<td>Yes</td>
<td>The default project is selected by default. You can select an existing project as required to manage different CVMs.</td>
</tr>
</tbody>
</table>
| Security group      | Yes      | - If no security group is available, you can choose **Create Security Group**.  
- If there are available security groups, you can choose **Existing Security Group**.  
For more information about the security groups, see Security Groups. |
| Instance Name       | No       | Customized by users to indicate the name of the CVM to be created.  
- If no instance name is customized, the name of the created instance is **Unnamed**.  
- An instance name can up to 60 characters. You can also perform Batch Sequential Naming or String Pattern-Based Naming.  
**Note**: This name is displayed only in the console, but not the hostname of the CVM. |
| Login Method        | Yes      | The method of logging in to the CVM. Select a value as required.  
- **Set the password**: Customize the password for logging in to the instance.  
- **SSH Key Pair (Only for Linux instances)**: Associate the instance with an SSH key, which ensures secure login to the CVM.  
  If no key is available or existing keys are inappropriate, you can click **Create Now** to create a key. For more information about SSH keys, see SSH Key.  
- **Random Password**: An automatically generated password will be sent via Internal Messages. |
| Security Reinforcement | No    | By default, DDoS protection and host security are enabled for free to help users build a CVM security protection system against data leakage. |
| Cloud Monitoring    | No       | By default, monitoring is enabled for Tencent Cloud services for free. You can install a component to retrieve CVM monitoring metrics and display results in monitoring graphs.  
You can also specify custom alarm thresholds. In addition, you can configure three-dimensional CVM data monitoring, |
5. Click **Next: Confirm** to open the configuration information confirmation page.

6. Check the information of the CVM to be purchased and the costs details of each configuration item.
7. Select **Agree with the Refund Rule.** (This option is applicable only to CVMs with monthly subscription.)

8. Click **Purchase Now** and complete the payment. Then, you can check your CVM by logging in to the **CVM Console.**

   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 via **Internal Messages.** You can log in to and manage instances based on the information. To ensure the security of the CVM, change your CVM login password as soon as possible.
Batch Sequential Naming or Pattern String-Based Naming

Last updated: 2019-11-12 11:06:41

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`.
Scenario

The Tencent Cloud instances' hardware devices can be adjusted easily with great flexibility. This document describes how to upgrade, degrade, or adjust instance configuration.

Prerequisites

Instance status

You can adjust an instance’s configuration when the instance has been either started up or shut down, and the change takes effect after the instance is forced to shut down and restarted.

Note:

- When the instance has been shut down, you can make changes in the console directly.

- When the instance has been started up, you can make changes online, and confirm forced shutdown after changes are made. The changes to configuration take effect after the instance is restarted.

- You can adjust configuration in batch online for multiple instances. If there is a server that has been started up in the batch of instances, you need to confirm the forced shutdown individually, and the changes take effect after the servers are restarted.

Limit of configuration adjustment

- Upgrading configuration
  No limit is imposed on the number of times configuration upgrade can be performed. The upgrade takes effect immediately.

- Degrading configuration
  - Postpaid instances can be degraded at any time and for unlimited times.

Hardware
The instances whose system disk and data disk are both cloud disks support adjusting configuration.

**Change of private IP**
For few instances, their private IPs will change after the configuration adjustment and there will be a note on the adjustment page.

**Directions**
You can upgrade the configuration of CVMs to adapt to you growing business. For all CVM types, the upgraded configuration takes effect immediately. That is, after you upgrade the configuration and pay the additional fees, the CVM will run with the new configuration immediately.

**Adjusting via console**
1. Log in to the CVM console
2. For the instance to adjust, click More -> Resource Adjustment -> Adjust Configuration.
3. In the popup box, select the configuration you want to adjust, and then click Next.
4. Confirm the billing details. Click Next.
5. In Shutdown CVM, read the information and check Agree to a forced shutdown. Click Adjust Now.

**Adjusting via API**
You can upgrade instance configuration using the APIs ResizeInstance and ResizeInstanceHour. For more information, please see APIs for adjusting instance configuration.
Adjust Network Configuration

Last updated: 2020-02-05 15:09:37

Change Billing Method

Tencent Cloud provides a variety of billing methods. You can switch between Bill-by-bandwidth and Bill-by-traffic in the console, but for each CVM, switching between the two methods can only be performed twice at most.

Billing description: Overview of Billing Methods for Public Network

Adjustment for Public Network

Tencent Cloud provides two types of network configurations: exclusive public network and shared public network. The shared public network service is billed by bandwidth. You need to submit a ticket to apply for activating it. For more information about the billing methods, please see Billing of Shared Public Network. This document mainly describes the adjustment between exclusive public networks. For more information about the billing methods, please see Billing of Exclusive Public Network.

Bill-by-bandwidth for postpaid CVMs

This billing method supports adjusting (upgrading or degrading) bandwidth at any time. If the bandwidth is changed several times during an hour, the billing is based on the highest bandwidth tier.

Bill-by-traffic

This billing method supports adjusting (upgrading or degrading) the bandwidth cap at any time and the change takes effect in real time.

This billing method can be used for both prepaid and postpaid CVMs.

Bandwidth cap

The options vary with different payment methods and CVM configurations. For more information, please see Bandwidth Cap of Public Network.
Procedure

1. Log in to the CVM Console, select the instance for which you want to change the network configuration, and then click More -> Resource Adjustment -> Adjust Network.

2. In the Adjust Network popup page, you can change the billing method and bandwidth cap.

3. Click OK.
Adjust Project Configuration

Scenario

The project function is used to manage cloud resources by project, and cloud resources can be managed by project. When creating a Cloud Virtual Machine instance, you must add the instance to the project. Tencent Cloud supports users to re-transfer the instance to the new project after creating the Cloud Virtual Machine instance.

Directions

1. Log in to the CVM Console.
2. In the instance list, select Cloud Virtual Machine who needs to be re-Assign to the new project, and click more-> instance Settings-> Assign to Project on the right. as shown below:

   If there are multiple servers that need to reconnect Assign to Cloud Virtual Machine of the new project, check Cloud Virtual Machine, and click more Operations-> instance Settings-> Assign to Project at the top.

3. In the pop-up "Assign to Project" window, select a new project name and click "submit" to complete the operation of Assign to the project.
Query Info

Query Instance Info

Last updated : 2020-02-02 15:43:57

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 in the Overview page in Console.
- View the information of all CVM instances in a region on the Instances page in Console.
- View the details of a CVM instance on the instance details page.

Prerequisite

Log in to CVM Console.

Directions

Viewing Instance Overview

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

Viewing Information ofInstances

The information available in the Instances page includes CVM IDs and names, monitoring information/status, availability zones, CVM type, configuration, primary IP address, CVM billing method, network billing method and the projects to which the CVMs belong.
Click the gear button in the upper right corner to select the list details you want to display.

Viewing Instance Details

Go to the instance details page to view the details of an instance by following the steps below:

1. Log in to the CVM Console.
2. Select a region.
3. Locate the instance for which you want to view the details, and click the instance ID to go to the instance details page.
4. In the instance details page, the following instance information is displayed, including CVM information, CVM configuration, system image, SSH key, ENI, public IP, monitoring, health check,
security group, etc.
Query Instance Monitoring Info

Last updated: 2020-02-02 15:33:48

Tencent Cloud provides the following two options for you to view the monitoring information of a CVM instance.

- View the monitoring information of a CVM instance in the Cloud Monitor Console.
- View the monitoring information of a CVM instance on the instance details page in the CVM Console.

Viewing Instance Monitoring Information in Cloud Monitor Console

1. Log in to the Cloud Monitor Console of CVM.
2. Select a region.
3. Click an instance ID to enter the monitoring information page of the instance.

4. In the monitoring information page, you can view the CVM instance's monitoring information such as CPU, memory, bandwidth of private network/public network, and disk usage.
5. You can view the monitoring information of public network traffic in the Traffic Monitoring page.

Viewing Instance Monitoring Information in CVM Console

1. Log in to the CVM Console.
2. Select a region.
3. Click an instance ID to enter the instance details page, and then click Monitoring.
4. In the monitoring information page, you can view the CVM instance's monitoring information such as CPU, memory, bandwidth of private network/public network, and disk usage.
5. You can view the monitoring information of public network traffic in the Traffic Monitoring page.
Instance Metadata

Last updated: 2020-02-25 10:33:38

Instance metadata represents the relevant data of the instance and can be used to configure or manage running instances.

Note: Although instance metadata can only be accessed internally from the instance, the data has not been protected through encryption. Anyone who accesses the instance can view its metadata. Therefore, you should take proper precautions to protect sensitive data. For example, using permanent encryption key.

Overview of Instance Metadata

Tencent Cloud provides the following meta-data:

<table>
<thead>
<tr>
<th>Data</th>
<th>DESCRIPTION</th>
<th>Version Where It Was Introduced</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</td>
<td>1.0</td>
</tr>
<tr>
<td>Public-ipv4</td>
<td>Instance public IP</td>
<td>1.0</td>
</tr>
<tr>
<td>Mac</td>
<td>MAC address of instance's eth0 device</td>
<td>1.0</td>
</tr>
<tr>
<td>Placement/region</td>
<td>Information of the region in which the instance resides</td>
<td>1.1</td>
</tr>
<tr>
<td>Placement/zone</td>
<td>Information of the availability zone in which the instance resides</td>
<td>1.1</td>
</tr>
<tr>
<td>Network/interfaces/macs/ $ / mac</td>
<td>Device address of instance network interface</td>
<td>1.0</td>
</tr>
<tr>
<td>Data</td>
<td>DESCRIPTION</td>
<td>Version Where It Was Introduced</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>Network/network/macs/ <strong>Mac</strong> / primary-local-ipv4</td>
<td>The primary private IP for the network interface of the instance</td>
<td>1.2</td>
</tr>
<tr>
<td>Network/network/macs/ <strong>Mac</strong> / public-ipv4s</td>
<td>The public IP for the network interface of the instance</td>
<td>1.2</td>
</tr>
<tr>
<td>Network/interfaces/macs/ $ / vpc-id</td>
<td>Example network interface VPC network ID</td>
<td>Update of 2017 MULT09MULTHUE 19</td>
</tr>
<tr>
<td>Network/interfaces/macs/ $ / subnet-id</td>
<td>Instance Network Interface Subnet ID</td>
<td>Update of 2017 MULT09MULTHUE 19</td>
</tr>
<tr>
<td>Network/network/macs/ <strong>Mac</strong> / local-ipv4s/ <strong>Local-ipv4</strong> / gateway</td>
<td>The gateway address for the network interface of the instance</td>
<td>1.2</td>
</tr>
<tr>
<td>Network/network/macs/ <strong>Mac</strong> / local-ipv4s/ <strong>Local-ipv4</strong> / local-ipv4</td>
<td>The private IP for the network interface of the instance</td>
<td>1.2</td>
</tr>
<tr>
<td>Network/network/macs/ <strong>Mac</strong> / local-ipv4s/ <strong>Local-ipv4</strong> / public-ipv4</td>
<td>The public IP for the network interface of the instance</td>
<td>1.2</td>
</tr>
<tr>
<td>Network/network/macs/ <strong>Mac</strong> / local-ipv4s/ <strong>Local-ipv4</strong> / public-ipv4-mode</td>
<td>The public network mode for the network interface of the instance</td>
<td>1.2</td>
</tr>
<tr>
<td>Network/network/macs/ <strong>Mac</strong> / local-ipv4s/ <strong>Local-ipv4</strong> / subnet-mask</td>
<td>The subnet mask for the network interface of the instance</td>
<td>1.2</td>
</tr>
<tr>
<td>Payment/charge-type</td>
<td>Instance billing mode</td>
<td>Update of 2017 MULT09MULTHUE 19</td>
</tr>
<tr>
<td>Payment/create-time</td>
<td>Instance creation time</td>
<td>Update of 2017 MULT09MULTHUE 19</td>
</tr>
<tr>
<td>Payment/termination-time</td>
<td>Example Terminate time</td>
<td>Update of 2017 MULT09MULTHUE 19</td>
</tr>
<tr>
<td>App-id</td>
<td>AppId of the user to which the instance belongs</td>
<td>Update of 2017 MULT09MULTHUE 19</td>
</tr>
<tr>
<td>Data</td>
<td>DESCRIPTION</td>
<td>Version Where It Was Introduced</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>As-group-id</td>
<td>Elastic Scaling group ID where the instance resides</td>
<td>Update of 2017 MULT09MULTHUE 19</td>
</tr>
<tr>
<td>Spot/termination-time</td>
<td>Spot instance Terminate time</td>
<td>Update of 2017 MULT09MULTHUE 19</td>
</tr>
<tr>
<td>/ meta-data/instance/instance-type</td>
<td>Instance specifications</td>
<td>Update of 2017 MULT09MULTHUE 19</td>
</tr>
<tr>
<td>/ instance/image-id</td>
<td>Example Image ID</td>
<td>Update of 2017 MULT09MULTHUE 19</td>
</tr>
<tr>
<td>/ instance/security-group</td>
<td>Instance binds security group information</td>
<td>Update of 2017 MULT09MULTHUE 19</td>
</tr>
</tbody>
</table>

Fields mac and local-ipv4 in red in the above table indicate the device address and private IP of the network interface specified for the instance, 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.

In the current version, the returned data of placement has been changed. 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 about the returned data of placement, please see Region and Availability Zone.

### Querying Instance Metadata

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

To view all the instance metadata from within a running instance, use the following URI:
To obtain information about the repossesion status of a spot instance, you can access the metadata by using the cURL tool or an HTTP GET request.

Example of querying metadata

The following example shows how to obtain the metadata version information.

Note: When the Tencent Cloud modifies the metadata access path or returned data, a new metadata version is released. If your application or script depends on the structure or returned data of previous version, you can access metadata using the specified previous version.

The following example shows how to view the metadata root Directory. In which / The ending word means Directory, not with / The word at the end represents Access's data. For the specific meaning of Access's data, please refer to the previous article. Instance metadata classification.

The following example shows how to get the physical location information of an instance. For the relationship between the returned data and the physical location, please refer to Regions and AZs.
The following example shows how to get the instance Private IP. If there are multiple ENI in the
instance, return the network address of eth0 Device.

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

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

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

```
[qcloud-user]# curl http://metadata.tencentyun.com/latest/meta-data/public-ipv4
139.199,11.29
```

The following example shows how to get the instance ID. The instance ID is the unique identity of the
instance.

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

The following example shows how to get the instance uuid. Instance uuid can be used as the unique
identity of an instance. It is recommended to use instance ID to distinguish between instances.

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

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

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

The following example shows how to get the information of instance ENI. Multiple pieces of ENI will
return multiple rows of data, each of which is a piece of ENI's data Directory.

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

The following example shows how to obtain the information of specified ENI.
The following example shows how to get VPC information to which a specified ENI belongs.

```bash
vpc-ja82n9op

subnet-ja82n9op
```

The following example shows how to get the address list of the specified ENI binding Private IP. If ENI binds multiple Private IP, it returns multiple rows of data.

```bash
```

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

```bash
```

The following example shows how to get a Private IP gateway. Only VPC Model can query this data. VPC Model, please refer to [Virtual Private Cloud](#).

```bash
10.15.1.1
```
The following example shows how to obtain the public network mode of Private IP and Access. Only VPC Model can query this data. Basic network Model through Public gateway Access public network.

```bash
NAT
```

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

```bash
139.199.11.29
```

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

```bash
255.255.192.0
```

The following example shows how to get the instance billing type.

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

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

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

The following example shows how to get the time of instance Terminate. (Prepaid mode only)

```bash
curl metadata.tencentyun.com/latest/meta-data/spot/termination-time
2018-10-18 11:27:33
```

The following example shows how spot instance obtains the Terminate time of the instance.

```bash
curl metadata.tencentyun.com/latest/meta-data/spot/termination-time
2018-08-18 12:05:33
```

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

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

You can specify the instance user data when you create the instance. After setting the cloud-init, CVM can access the data by Access.

**Retrieve user data**

Users can Access user data in the following ways within CVM.

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

Last updated: 2020-02-05 15:24:49

Scenario

To help users manage instances on the CVM console by identifying them by names, Tencent Cloud supports renaming instances. You can modify the name of an instance at any time, and the new name takes effect instantly.

Modifying the Name of an Instance

- Enter the CVM console, and select the CVM that needs to be renamed.
- Click More -> Instance Settings -> Rename on the page.
- On the renaming page, enter a new CVM name, and then click OK.

Modifying Names of Multiple Instances

- Enter the CVM console, and select multiple CVMs that need to be renamed.
- Click More actions -> Instance Settings -> Rename on the page.
- On the rename page, enter a new CVM name, and then click OK.

Note: The names of multiple CVMs that are renamed by this way are the same.
If you forget your password, you can reset the login password of the instance on the console. This document introduces how to change the login password of the instance on the CVM console.

**Note:**

1. Password resetting is only allowed for instances that have been shut down.

2. For a running instance whose password has been modified on the console, the CVM is shut down in the process of password reset. Schedule the time in advance to avoid data loss. You are recommended to perform the operation at the lows of business to minimize the impact.

**Reseting Password of Single Instance**

- Log in to the [CVM console](https://console.cloud.tencent.com), and select a CVM whose password needs to be reset.
• Click **More -> Password/Key -> Reset Password** on the page.

• Go to the Reset Password page. If the instance has been shut down, directly select the account whose password needs to be reset, then enter and confirm the new password, and click **Reset**.
Go to the Reset Password page. If the instance is running, select the account whose password needs to be reset, then enter and confirm the new password, and click Next. Select Agree to
force shutdown, and click Change Now.

Resetting Password of Multiple Instances

- Log in to the CVM console, and select multiple CVMs whose password needs to be reset.
- Click Reset password on the page.
- Go to the Reset password page. If all of the instances have been shut down, directly select the account whose password needs to be reset, then enter and confirm the new password, and click Reset.
- Go to the Reset password page. If some instances are still running, select the account whose password needs to be reset, then enter and confirm the new password, and click Next. Select Agree to forced shutdown, and click Change Now.
Management instance IP address
Obtaining the Private IP Address of an Instance and Private Network DNS Settings

Last updated: 2019-08-07 12:11:11

Obtaining the private IP address of an instance

**Obtaining the Address on the Console**

1. Log in to the CVM Console.

2. The CVM list displays the instances under your account. Move the mouse cursor over the private IP of the CVM, and the "Copy" button will appear; click the button to copy the private IP.

Obtaining the Address Using API

For more information, please see `DescribeInstances API`.

Obtaining the 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`.

2. Enter the command:

```
curl http://metadata.tencentyun.com/meta-data/local-ipv4
```
If the returned value is in the following structure, you can see the private IP address:

```
[croot@UM_58.22_centos ~]# curl http://metadata.tencentyun.com/meta-data/local-ipv4
18.00.00.27
```

For more information, please see Instance Metadata.

**Private Network DNS Settings**

When a network resolution error occurs, users can set the private network DNS manually. The private network DNS can be set as follows:

- **For Linux users.** CVM DNS can be modified by editing the `/etc/resolv.conf` file on the CVM. Run the command `vi /etc/resolv.conf`, and edit the DNS IP according to the above table.

```
root@vm-90-86-ubuntu:~# vi /etc/resolv.conf
nameserver 10.243.28.52
nameserver 10.225.30.178
options timeout:1 rotate
~
```

- **For Windows users.** On the CVM, open Control Panel -> Network and Sharing Center -> Change Adapter Settings, right-click the Property of the ENI, and double-click IPv4 to modify
the DNS server IP.
Modify Instance Private IP

Last updated: 2019-12-31 18:01:19

You can modify the private IP of a CVM instance in the VPC directly on the console or by changing the subnet of the CVM instance. For more information on how to change the subnet, please see Change Subnet.

Limits

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

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 -> Modify Primary IP.**

Enter a new IP in the pop-up window and then click **OK.** It takes effect after the instance is restarted.
Note: You can only enter the private IP of the current subnet CIDR.
Obtaining a Public IP Address of the Instance

Scenario

You can get public IP through console, API, or Instance Metadata.

Directions

**Obtaining the Address on the Console**

1. Log in to the **CVM Console**.
2. For each instance, there is an copy icon for an IP address. Click the button to copy this IP address.

**Note:**
The public IP address is mapped to the private IP address through NAT. Therefore, if you view the attributes of a network interface within the instance (for example, by using the commands such as `ifconfig` (Linux) or `ipconfig` (Windows)), the public IP address is not displayed. To obtain the public IP address of an instance from within the instance, please see **Obtain the Public IP Address of an Instance Using Instance Metadata**.

**Obtaining the Address Using API**

For more information, please see **DescribeInstances API**.

**Obtaining the 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**.
2. Enter the command:

```
curl http://metadata.tencentyun.com/meta-data/public-ipv4
```
If the returned value is in the following structure, you can see the public IP address:

For more information, please see Instance Metadata.
Scenario
This document guides you on how to change the public network IP address. There are two ways to change the public network IP:

- Directly replace the public network IP
- First change to elastic public network IP, and then Unbind elastic public network IP

Considerations
If you choose Directly replace the public network IP Please note the following:

- No more than 3 times per day for a single account in a single region.
- Single instance Only one replacement is allowed Public network IP.
- The original public network IP will be released after replacement.

If you choose First change to elastic public network IP, and then Unbind elastic public network IP Please note the following:

- When an EIP is bound to a CVM instance, the current public IP address of the instance will be released.
- The number of flexible public network IP for single account and single region quota is 20.

3. EIPs that are not bound to CVMs will incur an idle fee, which is billed on hourly basis.

Prerequisites

- Log into CVM Console .

Directions

Method 1: directly change the public network IP
1. On the management page of the instance, select the Tencent Cloud services device line to be converted into IP, and click more-> IP/ ENI-> change Public Network IP
2. In the pop-up "replace IP" prompt box, click "OK" to complete the replacement.
Method 2: first change to elastic public network IP, and then Unbind elastic public network IP

Replace the elastic public network IP

1. On the management page of the instance, select the Tencent Cloud services device line to be converted into IP, and click [icon].
2. In the pop-up "convert to elastic public network IP" window, click "OK conversion".

Unbinding EIPs

1. After the conversion is completed, click more-> IP/ ENI-> Unbind elastic IP in the Tencent Cloud services device line.
2. In the pop-up window of "Unbind elastic public network IP", check "Free Assign public network IP after Unbind (Note: the public network IP is random Assign, and cannot be associated with the instance Unbind)", and click "OK".
3. In the pop-up dialog box, click OK To complete the cordonning.

Release elastic public network IP (optional)

Since Unbind's elastic public network IP is still under this account when Unbind's elastic public network IP is used, to avoid charging cost for idle IP that is not in use, it is recommended to do the following to release the elastic public network IP that is not bound to an instance.

1. In the left sidebar, click EIP To open the EIP management page.
2. On the elastic public network IP management page, select Unbind's elastic public network IP, and click more-> release.
3. In the pop-up "make sure to release the selected elastic public network IP?" In the window, check OK to release the above IP, and click release.
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:

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

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.
Change Security Group

Scenario

Security group is a stateful virtual firewall for filtering packets and is used to set the network access controls for a single or multiple CVMs. It is a logical grouping and an important means of network security isolation. When a CVM instance is created, you must configure the security group for it. Tencent Cloud supports configuring a new security group for the CVM instance after it is created.

Note:
To configure a new security group for the instance, create a security group first.

Steps

- Log in to CVM Console, and select the instance to be assigned to the new security group.
- Click More on the right, and then click Configure Security Group.
- Enter the security group configuration page, and select the name of the new security group (multiple names can be selected), and click Confirm.
- Another way is to select the instance and click More actions on the top > Add to security group to get into the configuration page.

Note:
You can only bind a security group in the same project and region as CVM.

- You can also enter the instance details page, click Security Groups tab > Bind to bind the security group.
- Enter the security group configuration page, and select the name of the new security group (multiple names can be selected), and click OK to replace the security group.
Search Instances

Last updated: 2020-02-05 15:25:04

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 CVM search feature. You can filter out instances by such resource attributes as project, instance billing method, instance type, availability zone, IP, instance ID, and instance name.

Directions

1. Log in to the CVM Console, enter the keyword in the search text box, and then click the search icon to query the CVMs that match the search conditions. Or you can choose a specific dimension
for searching after clicking the search icon.
2. You can click **Help** to view the syntax of search examples.
3. For more syntaxes, 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><strong>Single keyword</strong></td>
<td>[Keyword]</td>
<td>10.0.0.1</td>
<td>Use ↑ to split more than one keyword</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>10.0.0.1</strong></td>
<td>List all instances including the keyword “10.0.0.1”</td>
</tr>
<tr>
<td><strong>Multiple keywords</strong></td>
<td>[Keyword] [Enter key +] [Keyword]</td>
<td>10.0.0.1</td>
<td><strong><a href="http://www.123.com">www.123.com</a></strong> 192.169.23.54</td>
</tr>
<tr>
<td><strong>Single resource type</strong></td>
<td>[Resource type]: [Keyword]</td>
<td>IP: 10.0.0.1</td>
<td><strong>IP: 10.0.0.1</strong></td>
</tr>
<tr>
<td><strong>Multiple resource types</strong></td>
<td>[Resource type]: [Keyword]: [Enter key +] [Resource type]: [Keyword]</td>
<td>Availability Zone: Hong Kong Zone 2 Project: Default</td>
<td><strong>Availability Zone: Hong Kong Zone 2 Project: Default</strong></td>
</tr>
<tr>
<td><strong>Single resource type and multiple keywords</strong></td>
<td>[Resource type]: [Keyword]: [Keyword]</td>
<td>CVM Status: Creating</td>
<td><strong>CVM Status: Creating</strong></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><strong>112.11.22.33 112.11.22.34</strong></td>
</tr>
</tbody>
</table>
You can export the CVM instance list of a region in the console, and customize the fields of the list to be exported. You can select a maximum of 28 fields. The fields supported for export include: ID, instance name, status, region, availability zone, instance type, operating system, image ID, CPU, MEM, bandwidth, Primary private IPv4, Primary public IPv4, Primary IPv6, system disk type, system disk capacity, data disk type, data disk capacity, network, subnet, associated VPC, creation time, expiry time, CVM billing method, network billing method, dedicated host ID, tag and project.

Procedure

- Log in to the CVM console.
- Select a region.
- Click the Download All icon.

On the page of customizing fields to be exported, you can select the fields to export. Then, click OK to export.
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.

```
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.

  
  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](#).
Shutdown Instances

Last updated : 2020-02-02 17:40:06

The instance can be shut down when you need to stop the instance service or modify the configurations only for the instance that have been shut down. Shutting down an instance is like shutting down a local computer.

Overview

- **Preparation for shutdown**: The instance will no longer function to provide services after shutdown. Make sure the CVM has stopped receiving service requests before shutdown.

- **How to shut down a instance**: You can shut down instances by using system commands (such as the shutdown command under Windows system and Linux system) or on the Tencent Cloud console. It is recommended to view the shutdown process on the console to check whether any problem occurs.

- **Shutdown process**: The instance will be shut down. The status of the instance will first change to "shutting down" and then "off" after it has been shut down. Overlong shutdown may cause problems. For more information, please see shutdown-related information to avoid forced shutdown.

- **Data storage**: All the storage of the instance will remain connected to the instance, and all disk data are saved. Data in memory will be lost.

- **Physical attributes of instances**: Shutting down an instance does not change any of its physical attributes. The instance public IP and private IP remain unchanged, and Elastic Public IP maintains a binding relationship, but accessing these IP will get you an error response (for stopped services); if the instance is part of the Classiclink, this interconnection will remain unchanged.

- **Load balancer**: If the shutdown instance belongs to Real Server Cluster of Load Balancer Instances, it will no longer function to provide services after shutdown. If the load balancer instance is configured with the health check policy, such shutdown instance will be automatically blocked from the request; but if not, the client may receive a 502 error code. For more information, please see Health Check.

- **Auto scaling**: If the shutdown instance is in an auto scaling group, the Auto Scaling service will mark shutdown instance as poor performance, move the same out of the auto scaling group and launch a replacement instance. For more information, please see Auto Scaling Product Documentation.
Shutdown Instance via the Console

1. Log in to the CVM Console.
2. Shut down an instance: Select the instance to be shut down, and click **Shutdown** at the top of the list or click **More** -> **Instance Status** -> **Shutdown** in the Operation column on the right side.
3. Restart an instance: Select all the instance to be shut down, and click **Shutdown** at the top of the list. Instances can be shut down in batches. Reasons are given for instances that cannot be shut down.

Shutdown instance via API

For more information, please see the API StopInstances.

Modify a Instance that Has Been Shut Down

You cannot modify the following instance attributes until the instance has been shut down.

- **Size of a mounted cloud disk:** To adjust the size of a cloud disk, please see Expanding Capacity of Cloud Disks.
- **Change password:** Please see Login Password.
- **Load key:** Please see SSH Key.
Restart Instances

Last updated: 2020-02-05 15:50:51

Scenario

Reboot is a necessary method to maintain CVM. Rebooting CVM instances is equivalent to restarting operating systems of local computers.

- It is recommended that users reboot instances using the reboot operation provided by Tencent Cloud rather than running reboot command in instances (such as restart command in Windows and Reboot command in Linux). Generally speaking, it takes only a few minutes to reboot your instances after the reboot operation is performed, but instances are unable to provide services during rebooting. Therefore, please make sure the CVM has stopped receiving service requests before rebooting.
- Since the physical characteristics of instances are not changed after the reboot, the Public IP address and Private IP address of, and any data stored in the instances will not be altered.
- Rebooting instances will not start a new billing period. The length of time for use of postpaid instance will be kept, which will not affect its price range.

Directions

Use console to reboot instances

1) Open CVM console.

2) To reboot a CVM instance running solely, click More > Instance Status > Restart on the action bar to the right side.

3) To reboot CVM instances running in batch, check all the instances to be rebooted, and click Restart on the top of the list. Reasons will be given for CVMs that cannot be restarted.

Use API to reboot instances

Please refer to RestartInstances 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 in to.
  - 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:

![Log into Instance Window](image)

- **Instance IP**: [IP address]
- **Port**: 22
- **User Name**: root
- **Login password**: [Password]

**Note:**
Please make sure that remote login ports from Webshell proxy IP (such as port 22 for SSH, port 36000 for tlnux) are open. Details.
In case of failures while logging in, please check the CPU and MEM Subscribe to Cloud Monitor Notify you when exception occurs. Details.
Tencent Cloud does not store your instance password or key. Please store them securely.

**OK**  **Cancel**
If the login is successful, “Socket connection established” will display as shown below:

```
* Socket connection established *
Last login: [time]
[root]$ [command]
```

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

Last updated: 2020-02-12 09:40:19

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.

```bash
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.

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

2. Execute the following command for remote login.

```bash
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](#)
Scenario

This document takes PuTTY software as an example to describe how to log in to a Linux instance by using remote login software on a local computer with a Windows system.

Applicable local OS

Windows

Authentication Method

Password or 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 forget your password, 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 CVMs purchased with quick configuration).

Steps

Logging in with a password

1. Download the Windows remote login software, PuTTY. How to get 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 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 the **Host Name**, configure **Saved Sessions** and save it. You can double click the session name saved under **Saved Sessions** to directly log into the CVM from now on.

4. Click **Open** to enter PuTTY interface. **login as:** appears.
5. Enter the user name after **login as:** and press **Enter**.
6. Enter the password after **Password** and press **Enter**.

Information about the CVM that you are currently logged in to will appear on the left of the
command prompt. This is shown in the following figure:

![Command Prompt](image)

**Logging in with a key**

1. Download the Windows remote login software, PuTTY.
   
   Download putty.exe and puttygen.exe software. To obtain PuTTY, [click here](#).

2. Double click **puttygen.exe** to open the PuTTY Key client.

3. Click **Load**, select and open the saved path of the downloaded private key. This is shown in the following figure:

   For example, select and open the private key file that has the file name **david**.

![PuTTY Key Generator](image)
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:

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 **david** private key file as **david.ppk** key
file. This is shown in the following figure:

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**, select and open the saved path of the key. This is shown in the following figure:
9. Switch to the Session configuration interface. Configure the CVM’s 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 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 the **Host Name**, configure **Saved Sessions** and save it. You can double click the session name saved under **Saved Sessions** to directly log into the CVM from now on.

0. Click **Open** to initiate the login request.

### 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 Instance via VNC

Last updated : 2020-02-11 10:02:05

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.

Applicable OS

Windows, Linux, or macOS.

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.

Prerequisites

You must already have the admin account/password (or key) for logging into Linux instance.

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

![Instance Management Page](image)

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

![Log into Linux instance Pop-up](image)

4. Enter the username/password in the pop-up dialog box to complete the login process, as shown below:
Connection succeeded: press any key to wake up your screen to paste the command, please click here.

CentOS Linux 7 (Core)
Kernel 3.10.0-357.21.3.el7.x86_64 on an x86_64

ul1_157_0_centos login:
Logging into Windows instance

Logging into Windows Instance via Remote Desktop

Last updated : 2020-02-11 10:11:34

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.
Log in to the Windows instance using the RDP file (recommended)

Operation scene

RDP, which stands for Remote Desktop Protocol, is a multi-channel Protocol developed by Microsoft to help your local computer connect to a remote computer. RDP is recommended by Tencent Cloud to log in to your Windows Cloud Virtual Machine. This article describes how to log in to a Windows instance using a RDP file.

Suitable for local operating system

Both Windows, Linux and Mac OS can log in to Cloud Virtual Machine using RDP.

prerequisite

- You need to use the administrator account number and the corresponding password of the instance to log in to the Windows instance remotely.
- If you log in to the instance using the system default password, go to Internal message Get.
- If you Forgot password, please Resetting Instance Password.
- Your Cloud Virtual Machine instance has purchased a public network IP, and the instance has port 3389 of Enable Cloud Virtual Machine instance (Enable is the default for Cloud Virtual Machine instances purchased through quick configuration).

Operation step

The Windows system logs in using RDP

1. Login Cloud Virtual Machine console.
2. On the instance management page, select the Windows Cloud Virtual Machine that needs to be logged in, and click *Log in*.
3. In the pop-up "Log in to Windows instance" window, select "Log in with RDP File", and click "download RDP File" to download the RDP file locally.
4. Double-click the downloaded RDP file to remotely connect to Windows Cloud Virtual Machine.

- If you log in to the instance using the system default password, go to Internal message Get.
- If you Forgot password, please Resetting Instance Password.

**The Linux system logs in using RDP**

You need to install the appropriate remote desktop connection program, it is recommended to use rdesktop to connect. For more details, please refer to Rdesktop official statement.

1. Execute the following command to check if rdesktop is installed on the system.

   ```
   rdesktop
   ```

   - If you have installed rdesktop, please execute Step 4.
   - If you prompt command not found, it means that rdesktop, is not installed. Please execute Step 2.

2. Execute the following command on the terminal to download the rdesktop installation package, using rdesktop version 1.8.3 as an example.

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

   If you need the latest installation package, you can go to GitHub rdesktop page Find the latest installation package and replace it with the latest installation path on the command line.

3. Under Directory to install rdesktop, execute the following command to extract and install rdesktop.

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

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

   ```
   Please change the parameters in the example to your own.
   ```
rdesktop -u Administrator -p <your-password> <hostname or IP address>

- **Administrator** That is, the administrator account obtained in the prerequisite.
- **<your-password>** That is, the login password set for you.

If you log in to the instance using the system default password, go to Internal message Get. If you Forgot password, please Resetting Instance Password.

- **<hostname or IP address>** That is, the public network IP or custom domain name of your Windows instance.

**The MacOS system logs in using RDP**

- The following action takes Microsoft Remote Desktop for Mac as an example. Microsoft officially stopped providing download links for Remote Desktop clients in 2017 and transferred to its subsidiary HockeyApp to carry out the Beta version of publish.
- The following action takes Cloud Virtual Machine, who is connected to the Windows Server 2012 R2 operating system, as an example.

1. Download Microsoft Remote Desktop for Mac And install it locally.
2. Launch MRD, and click [Add Desktop]. as shown below:
3. A pop-up "Add Desktop" window, follow these steps to create a connection. as shown below:

i. Enter Cloud Virtual Machine public network IP at "PC name".

ii. Click [Add] to confirm creation.

iii. The rest of the options remain at the default settings, and the connection is created.

You can view the connections that have been successfully created in the window. as shown
Double-click to open the newly created connection, and in the pop-up window, enter Cloud Virtual Machine's account number and password as prompted, and click [Continue].

- If you log in to the instance using the system default password, go to Internal message Get.
- If you Forgot password, please Resetting Instance Password.

5. Click [Continue] in the pop-up window to confirm the connection. as shown below:

After a successful connection, the Windows Cloud Virtual Machine interface will be opened.
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:

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:
Reinstall System

System reinstallation enables instances to recover to a newly started status. It is a recovery method when CVM instances are suffering software failures. CVM instances support reinstallation of different types of systems. Whether you choose to change to a Linux series system or a Windows series system, Tencent Cloud will offer various-sized system disks to you.

It should be noted that reinstalling the system will result in loss of all contents of system disks. Data in data disks will not be affected, but need to be re-recognized. Therefore, in case that system operation data need to be retained, it is strongly recommended that you [Create Custom Image](/doc/product/213/4942) before reinstalling the system and decide whether to use the image for reinstallation.

Sizes of system disks of different operating systems

- If the newly purchased Linux CVM comes with a cloud block storage, it can support a system disk of 20GB - 50GB.
- If the newly purchased Linux CVM comes with a local disk, it can support a system disk of 20GB.
- A newly purchased Windows CVM with any type of hard disk supports a system disk of 50GB.

Charges for system disks

- For Linux instance system disks, the first 20GB of Tencent Cloud is free of charge. If the system disk supports capacity adjustment (i.e. if it is a Cloud Block Storage), the part beyond 20GB will be charged as per the charging standard of Cloud Block S.
- For Windows instance system disks, the first 50GB of Tencent Cloud is free of charge. Since Windows instances do not support system disk capacity adjustment, no fees will be charged for system disks of Windows instances.

Use console to reinstall system

1) Open CVM Console.

2) For CVM instances that requires system reinstallation, click "More" - "Reinstall System" on the action bar to the right side.
3) In the pop-up box of system reinstallation, select the image used by the current machine or other images.

4) If other operating systems are needed, choose from the images provided by Tencent Cloud. Click "Reinstall System".

Note:

- Do not perform other operations during system disk reinstallation.
- The data in current system disks cannot be recovered after system disk reinstallation.
- The data in data disks will be retained and will not be affected after system disk reinstallation, which however need to be mounted manually before use.

Questions about the switching between Windows system instances and Linux system instances

**Can the system disk of an old user's Linux CVM that comes with a local disk be scaled out to 20GB?**

For a Linux CVM that comes with a local disk of 8GB, the system disk can be scaled out to 20GB by reinstalling the system.

**A user has purchased a Linux CVM that comes with an over-20GB Cloud Block Storage. How the charges are calculated if the user reinstalls the operating system and changes it to Windows?**

If a user purchases a Linux CVM that comes with an over-20GB Cloud Block Storage, and then changes the operating system to Windows, the charges will be calculated based on the billing mode:

- If the CVM is based on an annual or monthly plan, a refund will be made (exclusive of the amount of voucher used in payment) or the price will be lowered according to the payment conditions.
- If the CVM is based on charge-by-quantity, the calculation of configuration charge for the part exceeding 20GB of the system disk will be stopped (i.e. the system disk will be free of charge afterwards) after the operating system is changed to Windows;

**A user has purchased a Windows CVM that comes with a Cloud Block Storage. How the charges are calculated if the user reinstalls the operating system and changes it to Linux?**
Since the current system disk does not support capacity reduction, when a 50GB Windows Cloud Block Storage is changed to Linux, the capacity shall be kept and corresponding fees for the Cloud Block Storage shall be paid. (The first 20GB is free of charge, and fees for another 30GB shall be paid).
Terminate Instances

This document introduces the Terminate of the instance and the overview and operation method of releasing the instance. For more expiration information, please refer to Expiration reminder.

Overview

When you do not need an instance, you can use Terminate for the instance, and the instance that was given by Terminate will be put into Recycle bin. For the instance in Recycle bin, you can renew, Resume or release the instance according to different scenarios and requirements.

If your account in arrears, for your Pay as you go instance, you need to renew it before Resume.

For Pay as you go's instance type, Terminate and his release instance include the following ways.

- **Manual Terminate method** For an example of Pay as you go without in arrears, you can choose manual Terminate. An instance of the type of Pay as you go will be completely released after Recycle bin has retained it for 2 hours at most.

- **Timing Terminate mode:** Set timing Terminate for the instance of on demand's payment type. You can choose a future time timing Terminate resources, Terminate time accurate to seconds. The instance resources of Terminate will be released immediately and will no longer enter Recycle bin. Before setting the time for Terminate, you can do it at any time, Cancel Scheduled Termination.

- **Due / in arrears automatic Terminate mode:** Instances of Pay as you go type will be automatically released after the balance is less than 0 for 26 hours (the fee will continue to be deducted in the first 2 hours, and the phone will be shut down and stopped in the next 24 hours. In arrears's Pay as you go instance is not included in Recycle bin. You can view it in the instance list. Complete within the specified time to renew Can continue to use.

<p>| Active Terminate (not in arrears) | Timed Terminate (not in arrears) | Due / in arrears automatic Terminate |</p>
<table>
<thead>
<tr>
<th>Pay as you go type example</th>
<th>Active Terminate (not in arrears)</th>
<th>Timed Terminate (not in arrears)</th>
<th>Due / in arrears automatic Terminate</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>After Terminate, the instance will be retained in Recycle bin for up to 2 hours, and if Resume is not released after the expiration date, the instance will be released.</td>
<td>The instance of setting timing Terminate will be released directly after the set time and will not enter Recycle bin.</td>
<td>After the instance in arrears, the fee will continue to be deducted in the first 2 hours, and the instance can be used normally. The phone will be turned off and the deduction will be stopped in the next 24 hours, and the Pay as you go instance of in arrears will not enter Recycle bin. If the renewal is not completed during this period, the instance will be released.</td>
</tr>
</tbody>
</table>

**Related influence**

When an instance enters the status of Terminate, the related effects of instance data, elastic IP and billing are as follows:

- **Billing**: When an instance is being terminated or has been terminated, no expenses related to this instance are incurred.
- **Instance data**: Both the mounted local site and the inelastic HDD cloud disk will be released at the same time. The data cannot be recovered. Please back up in advance. Elastic HDD cloud disk will follow its own life cycle.
- **EIP**: EIPs (including IPs on the secondary ENI) of a terminated instance are retained, and idle IPs may incur expenses.

**An example of Terminate and the release of Pay as you go**

For the example of Pay as you go, you can choose Terminate immediately or Terminate on time.

**Terminating Instances on the Console**

1. Log in to the CVM Console.
2. According to the actual demand, choose different Terminate examples to operate.
3. Terminate a single instance: Find the instance to be terminated in the list, and click More -> CVM Status -> Terminate On the right side.

- **Batch Terminate instances** Check all the instances that require Terminate, and click more Operations-> Terminate / return at the top. The example of Terminate will show the reason.

3. In the pop-up window, you can select **Terminate Now** or **Scheduled Termination** Instances.
   - **Terminate Now** If you choose Terminate immediately, you can choose whether to release resources immediately or 2 hours later. If you choose to release immediately, the data related to the instance will be cleared and cannot be Resume.
   - **Scheduled Termination** If you select timed Terminate, you need to set a timed time for Terminate. After expiration, the instance will be timed and released by Terminate, and the data cannot be Resume.

4. After selecting Terminate method, click "next" to confirm Terminate and retain the actual and related resources.

5. Click "start Terminate" after confirming Terminate's resources.

**Cancel Scheduled Termination**

1. Log in to the CVM Console.

2. In the list of instances, find the instance that needs to undo timing Terminate, and in "Instance billing mode" found in column" Scheduled Termination Move the mouse to The prompt box
3. Click "undo", and the confirmation revocation timing Terminate prompt box pops up.
4. In the pop-up prompt box, confirm the instance information of Terminate with timing for cancellation, and click **OK**. The cancellation by Terminate will take effect immediately. as shown
Terminating Instances using API

For more information, please see the API TerminateInstances.
Instance Expire

This document describes the reclaiming mechanism of an instance and the operation method for recovering an instance. For more information on expiration, please see Expiry Reminder.

Reclaiming Instance

Tencent Cloud Recycle Bin is a cloud service reclaiming mechanism. The prepaid instance will be shut down on the expiry date or on the day when it is actively terminated before expiry, and then is automatically put into the recycle bin. The instance configured with auto renewal is automatically renewed if account balance is sufficient. No reclaiming mechanism is provided for postpaid instances. The instance will be released after 26 hours.

Postpaid Instance in Recycle Bin

- **Retention time:** The instance deleted by the user is retained for 2 hours in the recycle bin.
- **Expiry processing:** If the instance is not renewed within 7 days, the system will release resources and start to automatically Terminate Instance.
- **Mounting relationship:** After the instance is put into the recycle bin, the mounting relationship with CLB, elastic public IP, elastic cloud disk, secondary ENI, and Classiclink will not be stopped automatically.
- **Operation limits:** You can only renew or terminate the instances in the recycle bin.

Recovering Instance

1. Log in to the CVM Console.
2. On the left navigation bar, click Recycle Bin -> CVM to enter the CVM reclaiming list.
3. Recover single instance: Find the instance to be recovered in the list, click Recover button, and complete the renewal payment.
4. Recover instances in batch: Select all instances to be recovered, click Recover Selected on the top, and complete the renewal payment.
Spot Instances

There are two ways to use spot instances.

**TencentCloud API**

You can find parameters related to spot instances in CVM RunInstance API.

- **Batch Compute Console**
  
  Now you can select spot instances when submitting jobs and creating a computing environment in the Batch Compute console.

**TencentCloud API**

`InstanceMarketOptionsRequest`, a parameter in RunInstance API can specify the use of the spot instance mode and make related configuration.

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MarketType</td>
<td>String</td>
<td>No</td>
<td>Market type. Only &quot;spot&quot; is supported.</td>
</tr>
<tr>
<td>SpotOptions</td>
<td><code>SpotMarketOptions</code></td>
<td>No</td>
<td>Spot-related options</td>
</tr>
</tbody>
</table>

**SpotMarketOptions**

Spot-related options

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MaxPrice</td>
<td>String</td>
<td>Yes</td>
<td>Bid rate</td>
</tr>
<tr>
<td>SpotInstanceType</td>
<td>String</td>
<td>No</td>
<td>Spot request type. Only &quot;one-time&quot; is supported.</td>
</tr>
</tbody>
</table>
• **Sync API**: Currently RunInstance provides a one-time sync request API, which means that if the application fails due to insufficient supply or request price lower than market price, it will immediately return failure, and will not apply again.

• **Fixed price (beta testing)**: Fixed discount mode is used during the beta testing period, so you must set the parameter to greater than or equal to the current market price. For detailed market prices, see [Spot Instance - Supported Regions and Types](https://intl.cloud.tencent.com/doc/product/213/17817).

### TencentCloud API Example

#### Use Case
Region of the instance: Guangzhou Zone 3; billing mode: hourly pay as you go; highest bid price: $0.6/hour; bid request mode: one-time request; image ID: img-pmqg1cw7; selected model: S2.MEDIUM4 (Standard S2, 2-core, 4 GB); quantity: 1.

#### Request Parameters

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

#### Response Parameters

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

- **Async API**: When you submit a job, create a computing environment, or modify the expected number of computing environments, Batch Compute will process your request asynchronously. That means if the current request cannot be fulfilled due to factors such as inventory and price, Batch Compute will continue to apply for spot instance resources until the request is fulfilled. Therefore, before you release instances, you need to first change the number of computing environment instances via the Batch Compute console; otherwise, after you release instances in the CVM console, Batch Compute will automatically create new instances until the expected number is met.

- **Cluster mode**: The computing environment of Batch Compute supports maintaining a batch of spot instances as a cluster. You only need to submit the desired quantity, configuration and highest bid. The computing environment will automatically and continuously initiate requests until the desired quantity is met. Even if there is an interruption, Batch Compute will automatically make applications again.

- **Fixed price (beta testing)**: Like the price used in TencentCloud API, the price must be higher than or equal to the current market price.

**Directions**

I. Go to the Batch Compute Console

Go to the **Batch Compute Console**.

II. Go to Computing Environment

Click **New** to enter the computing environment creation page.
Verify that you are on the whitelist for using spot instances: select an availability zone that supports spot instances, such as Guangzhou zone 3. If you can see the **Spot Instance** option in the drop-down menu shown in the figure above, it means that you are on the whitelist; otherwise, please submit an application for using spot instances first.

**III. Create Computing Environment with Spot Instance**
Select **Spot Instance** type, and select the model, image, name, number of expected instances, etc. you need, click **OK**.

### IV. View the New Computing Environment

[![CVMs in new computing environment](image)](image)

After you finish the creation, go back to the [Batch Compute Console](https://console.cloud.tencent.com/batch/env), you will see the new computing environment and CVMs being created in it. You can go to **Activity Log** and **Instance List** to check the creating progress.
No Charges When Shut down for Pay-as-You-Go Instances

Scenario

When users enable the "No Charges When Shut down" feature, they will not need to pay for Pay-as-You-Go instances (CPUs, memory) that are in `shutdown` mode. However, other resources bound with these instances, like cloud disks (system disk, data disk), public network bandwidth, and images, are still charged. For more information, please see No Charges When Shut down for Pay-as-You-Go Instances Details.

Directions

1. Log into CVM Console.
2. Shut down one instance: Select an instance and click Shutdown on the top of the list. Alternatively, go to the operation pane on the right, select More > Instance Status > Shut down. Check No Charges when Shut down in the pop-up page. Does not support No Charges when Shut down will be displayed if the instance is not eligible for this feature.
3. Shut down several instances: Select desired instances and click Shut down on the top of the list. Check No Charges when Shut down. Does not support No Charges when Shut down will be displayed if the instance is not eligible for this feature.

Enabling via Cloud API

To enable this feature via API, please add the following parameter while shutting down instance using StopInstances API. For details, please see Stop Instances.

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Required</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Parameter Name</td>
<td>Required</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>----------</td>
<td>--------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| StoppedMode    | No       | String | The "No Charges when Shut down" feature is only available for Pay-as-You-Go instances  
**Range :**  
KEEP_CHARGING : Keep charging when shut down  
STOP_CHARGING : No charges when shut down  
**Default value :**  
KEEP_CHARGING |
Change Disk Media Type

Last updated : 2019-10-09 19:48:12

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 local disks to cloud disks, the data on the local disks will be copied to the cloud disks. How long it takes depends on the amount of data and the data transmission speed. The process may take a while.
- 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 the list of CVM 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.
Images
Create Custom Images
Last updated : 2020-02-01 20:29:13

Scenario

You can launch an instance with a public image or a service marketplace image, and then connect to the instance and deploy your software environment. If the instance runs normally, you can create a new custom image based on this instance as needed, so that you can use this image to launch more new instances that have the same custom configurations with the original one.

- Shut down the instance before you can create a custom image to ensure that the image has exactly the same deployment environment as that of the current instance.
- To keep the data in the original instance data disk when you lunch a new instance, you can first take a Snapshot of the data disk, and then create a new CBS data disk with this snapshot when launching the new instance.

Notes

- Each region supports a maximum of 10 custom images.
- The following directory and files will be removed.

  - /var/log/
  - /root/.bash_history, /home/ubuntu/.bash_history (Ubuntu system)

- When create image for Linux instance, make sure that /etc/fstab does not include data disk configuration. Otherwise, launching the instance created by the image might fail.

Directions

Create an image from an instance via the console
1. Log in to the CVM Console.
2. Shut down the instance. Select the instance to be shut down, and then click More > Instance Status > Shutdown.
3. Click More on the right side of the instance used to create an image, and click Create Image.
4. Enter Image Name and Image Description in the pop-up box, and click Create Image to submit the creation application.
5. To purchase a server with the same image as the previous one, click Create Instance on the right side of the image in the image list.

**Create an image using API**

You can use the API CreatedImage to create a custom image.
Copy Images

Overview

Cross-region Copying allows you to quickly deploy the same CVM instances in different regions. Deploying the same CVM instance in different regions using image synchronization is a reliable way to improve application robustness.

Synchronizing images to different regions on Console

1) Log in to CVM Console.  
2) Click Image in the navigation pane.  
3) Check the image you want to copy, click More > Cross-region copying.  
4) Select the destination region, and click OK.  
5) After successful synchronization, the image list status in the destination region is updated to 100%.

Synchronize images to different regions via API

You can use the SyncCvmImage API to synchronize images. For details, refer to SyncCvmImage API.
Share Custom Images

Last updated: 2020-02-02 14:53:03

Shared image means that you share a custom image that you have created with others users. You can easily get shared images from other users, to get necessary components and then add custom contents.

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

Sharing Images

Obtaining Account of the Counterpart

To share an image with another user, you need to obtain his/her unique account ID. You can inform him of obtaining your ID in this way:

1) Log in to Tencent Cloud console, and click the account name in the upper right corner > Account Information.
2) View the Account ID in Basic Information.

Sharing Images on Console

1) Log in to Tencent Cloud Console.
2) Click Images in the navigation pane.
3) Click the Custom Image tab, and select the custom image you want to share.
4) Click the Share button, enter the unique Tencent Cloud account ID of the counterpart, and click OK.
5) Inform him of logging in to Tencent Cloud Console and select “CVM” - “Image” - ”Shared Image”, to view the image that you has shared with him.
6) To share this image with multiple users, repeat the above steps until you have added all users.

Sharing Images via API

You can use the ShareImage API to share images.

Using Shared Images
Shared images can only be used to launch CVM instances. For details, refer to Purchase and Start Instances.
Cancel Image Sharing

You can at any time cancel the status of sharing images with others. This operation does not affect instances that other users have created using this shared image, but other users can no longer see the image or create more new instances using this image.

Cancel image sharing on Console

1) Open Tencent Cloud Console.

2) Click CVM - Images in the navigation pane.

3) Click the Custom Image tab. Find out the custom image you want to cancel sharing and click More - Cancel Sharing. Select the account you want to unshare, click the "Unshare" button and confirm the operation to unshare the image.

Cancel image sharing via API

You can use the CancelShareImage API to cancel image sharing.
Delete Custom Images

Last updated : 2020-02-02 15:20:16

After using the custom image, you can delete it. When you delete a custom image, you will not be able to use this image to start a new CVM instance, but any instances that are already started will not be affected. If you want to remove all instances that were purchased and started from this image, you can refer to Expiration of Prepaid Instances or Terminate Postpaid Instances.

- If you have already shared a custom image to others (see here), you cannot delete it. You need to cancel all of its sharing before deleting a custom image.
- You can only delete the custom image, but neither the common image nor the shared image.

Deleting custom images on Console

1) Open Tencent Cloud Console.
2) Click CVM - Images in the navigation pane.
3) Click the "Custom Image" tab, and select the custom image you want to share in the list.
4) Click the "Delete" button and confirm the operation, to delete all selected custom images. In case of failed deletion, the reasons will be prompted above the image.

Deleting custom images via API

You can use the DeletelImages API to delete images. For details, refer to
In addition to the Create Custom Image feature, Tencent Cloud also supports image import feature. You can import an image file of a server system disk on the local machine or another platform into the CVM custom images. After the image is imported, you can use it to create a CVM or reinstall the system for an existing CVM.

Preparations for Import

Applying for Permission

Before using this feature, make sure that you have activated the image import permission. If you need to activate the permission, contact the Business Manager and submit relevant information to the ticket system.

Prepare the image file

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

- **Limits on Linux images:**

<table>
<thead>
<tr>
<th>Image Attribute</th>
<th>Condition</th>
</tr>
</thead>
</table>
| Operating system | - The image that is based on CentOS, Ubuntu, Debian, CoreOS, OpenSUSE, and SUSE distributions.  
                     - Both 32-bit and 64-bit systems are supported. |
| Image format | - The image formats such as RAW, VHD, QCOW2 and VMDK are supported.  
                             - Use `qemu-img info imageName | grep 'file format'` to check the image format. |
| Image size | - Use `qemu-img info imageName | grep 'disk size'` to check the actual size of the image if it does not exceed 50 GB.  
                        - Use `qemu-img info imageName | grep 'virtual size'` to check the vsize of the image if it does not exceed 500 GB.  
                        - Note: Check the image size when you import an image, which is subject to the information of the image that is converted to the QCOW2 format. |
<table>
<thead>
<tr>
<th>Image Attribute</th>
<th>Condition</th>
</tr>
</thead>
</table>
| **Network**     | - Tencent Cloud provides the `eth0` network interface for the instance by default.  
- You can query the network configuration of an instance through the metadata service in the instance. For more information, please see [Instance Metadata](#). |
| **Driver**      | - The virtio driver of the visualization platform KVM must be installed in the image. For more information, please see [Import Image to Linux to Check virtio Driver](#).  
- It is recommended to install cloudinit for the image.  
- If cloudinit cannot be installed in the image for some reason, you can configure the instance manually by referring to [Forced Import](#). |
| **Limit on Kernel** | - Native kernel is preferable for an image. Any modifications may cause failure in importing the image into the CVM. |

**Limits on Windows images:**

<table>
<thead>
<tr>
<th>Image Attribute</th>
<th>Condition</th>
</tr>
</thead>
</table>
- Both 32-bit and 64-bit systems are supported. |
| **Image format** | - The image formats such as RAW, VHD, QCOW2 and VMDK are supported.  
- Use `qemu-img info imageName | grep 'file format'` to check the image format. |
| **File system type** | - Only NTFS file system using the MBR-style partition is supported.  
- GPT-style partition is not supported.  
- Logical Volume Management (LVM) is not supported. |
| **Image size** | - Use `qemu-img info imageName | grep 'disk size'` to check the actual size of the image if it does not exceed 50 GB.  
- Use `qemu-img info imageName | grep 'virtual size'` to check the vsize of the image if it does not exceed 500 GB.  
- Note: Check the image size when you import an image, which is subject to the information of the image that is converted to the QCOW2 format. |
| **Network** | - Tencent Cloud provides the Local Area Connection network interface for the instance by default.  
- You can query the network configuration of an instance through the metadata service in the instance. For more information, please see [Instance Metadata](#). |
<table>
<thead>
<tr>
<th>Image Attribute</th>
<th>Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Driver</td>
<td>- The virtio driver of the visualization platform KVM must be installed in the image. If it is not installed in the Windows system by default, you can install the Windows virtio driver, and then export the local image.</td>
</tr>
<tr>
<td>Other</td>
<td>- The imported Windows image <strong>does not provide</strong> the Windows Activation service.</td>
</tr>
</tbody>
</table>

**Importing Steps**

1. Log in to the [CVM Console](#).
2. Click **Image** in the left navigation bar.
3. Click **Custom Image**, and then click the **Import Image** button.
4. As instructed in the steps, you need to **Enable Cloud Object Storage**, **Create bucket**, then **Upload the image file to the bucket and get Image file URL**, and then click **Next**.
5. Fill in the form according to the actual situation. Be sure to enter the correct COS file URL, and then click **Import**.
6. You will be notified whether the import is successful or failed via internal message.

**Error Codes**

<table>
<thead>
<tr>
<th>Error Code</th>
<th>Reason</th>
<th>Recommended Processing Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>InvalidUrl</td>
<td>COS link is invalid</td>
<td>Check if the COS file URL is the same as the imported image URL.</td>
</tr>
<tr>
<td>InvalidFormatSize</td>
<td>The format or size is unqualified.</td>
<td>The image must meet the limits on Image format and Image size in Preparations for Import.</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 Preparations for Import.</td>
</tr>
<tr>
<td>PartitionNotPresent</td>
<td>The partition information is not found</td>
<td>The image is corrupted probably because it is created incorrectly.</td>
</tr>
<tr>
<td>CloudInitNotInstalled</td>
<td>cloud-init is not installed</td>
<td>Install cloud-init in the Linux image by referring to the <code>Driver</code> section in Preparations for Import.</td>
</tr>
<tr>
<td>Error Code</td>
<td>Reason</td>
<td>Recommended Processing Method</td>
</tr>
<tr>
<td>---------------------</td>
<td>----------------------------------</td>
<td>---------------------------------------------------------------------</td>
</tr>
<tr>
<td>RootPartitionNotFound</td>
<td>The root partition is not found</td>
<td>The image is corrupted probably because it is created incorrectly.</td>
</tr>
<tr>
<td>InternalError</td>
<td>Other errors</td>
<td>Contact 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-$($uname -r)
```

A response similar to the following will be returned:

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

- If the 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:
  ```
  lsinitrd /boot/initramfs-$\left(\text{uname -r}\right).img | grep virtio
  ```

- For RedHat 5/CentOS 5:
  ```
  mkdir -p /tmp/initrd && cd /tmp/initrd
  zcat /boot/initrd-$\left(\text{uname -r}\right).img | cpio -idmv
  find . -name “virtio*”
  ```

- For Debian/Ubuntu:
  ```
  lsinitramfs /boot/initrd.img-$\left(\text{uname -r}\right) | grep virtio
  ```

If a result similar to the following is returned:

```
[...]
  .../cache/virtio_blk.ko
  .../kernel/drivers/block/virtio_blk.ko
  .../cache/virtio_pci.ko
  .../cache/virtio_pci.ko
  .../cache/virtio_ring.ko
  .../cache/virtio_ring.ko
[...]
```

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:
  ```
  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:
  ```
  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:
  ```
  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.

   ![Kernel Version Example]

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

4. Execute the following command to switch directory.
5. Execute the following command to download the installation package.
   
   ```
   cd /usr/src/
   ```
   
   ```
   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.
   
   ```
   ln -s linux-2.6.32 linux
   ```

8. Execute the following command to switch directory.
   
   ```
   cd /usr/src/linux
   ```

Combining 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 ./.config
   make menuconfig
   ```
Enter the “Linux Kernel vX.X.XXX Configuration” interface as shown below:

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

“Linux Kernel vX.X.XXX 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:
If it is not selected, press the space bar to select the “Kernel-based Virtual Machine (KVM) support” option.

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

6. Press the "↓" key to move the cursor to "Processor type and features" and press "Enter" to 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:

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.
Install Cloudbase-Init on Windows

Last updated: 2019-10-09 18:41:40

Downloading the Cloudbase-Init installer

Download the Cloudbase-Init installer corresponding to your operating system architecture. For details, visit Cloudbase-Init Official Site.

Cloudbase-init has the following versions:

- **Stable version (recommended)**
  Download via the following links:
  - 64-bit Windows: https://www.cloudbase.it/downloads/CloudbaseInitSetup_Stable_x64.msi
  - 32-bit Windows: https://www.cloudbase.it/downloads/CloudbaseInitSetup_Stable_x86.msi
- **Beta version**

Installing Cloudbase-Init

When installing Cloudbase-Init, please note:

- **In the “Configuration options” window, set “Serial port for logging” to “COM1” as shown below.**
- *At the final step of the installation, do not check any box as shown below:*
Modifying the Cloudbase-Init configuration file

1. Open the Cloudbase-Init configuration file at `\PATH\TO\Cloudbase Solutions\Cloubase-Init\conf\cloudbase-init.conf`.
2. Replace the content in the file with the following:

```plaintext
[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\
metadata_services=cloudbaseinit.metadata.services.configdrive.ConfigDriveService
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\C:\powershell
C:*powershell
PS C:*Set-ExecutionPolicy Unrestricted
```

3. Copy the `TencentCloudRun.ps1` script to the `C:\Program Files\Cloudbase Solutions\Cloudbase-Init\LocalScripts\` directory.
Install Cloud-Init on Linux

Last updated: 2020-03-06 16:22:41

Introduction

Cloud-init enables you to customize configuration during the first initialization of an instance. If the imported image is not installed with the cloud-init service, instances booted with the image will not be initialized properly, which will result in image import failures. This document describes how to install the cloud-init service.

You can install cloud-init in two ways:

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

Notes

Before importing a Linux image, please make sure you have properly installed the cloud-init service in your image.

Prerequisites

Servers installed with the cloud-init service can visit external IPs.

Directions

Manually downloading cloud-init source package

Downloading the cloud-init source package

The cloud-init-17.1 version is the most compatible with Tencent Cloud, which can ensure that all configuration items of the CVMs created with the image can be initialized properly. It is recommended to 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.
Execute 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. Execute the following command to decompress the cloud-init installation package.

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

2. Execute the following command to enter the directory of the decompressed package, i.e., the `cloud-init-17.1` directory.

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

3. Install Python-pip according to your OS version.
   - For CentOS 6/7, execute the following command:
     ```bash
     yum install python-pip -y
     ```
   - For Ubuntu, execute the following command:
     ```bash
     apt-get install python-pip -y
     ```

4. Execute the following command to install dependencies.

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

   Python 2.6 is not supported when cloud-init uses requests 2.20.0. If the Python interpreter installed in the image environment is Python 2.6 or below, please execute `pip install 'requests<2.20.0'` to install requests version below 2.20.0 before installing the cloud-init dependencies.

5. Install the cloud-utils components according to your OS version.
   - For CentOS 6, execute the following command:
yum install cloud-utils-growpart dracut-modules-growroot \ -y
dracut -f

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

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

6. Execute the following command to install cloud-init.

   python setup.py build

   python setup.py install \ --init-system systemd

   Optional parameters for \ --init-system \ include: (systemd, sysvinit, sysvinit_deb, sysvinit_freebsd, sysvinit_openrc, sysvinit_suse, upstart) [default: None]. Make a selection based on the current method of managing auto-start services of your OS. If you select a wrong one, the cloud-init service will not auto-start on boot. This document uses the systemd auto-start service manager 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 in /etc/cloud/cloud.cfg with the content of the downloaded cloud.cfg file.

**Adding syslog user**

Execute the following command to add a syslog user.

   useradd syslog

**Configuring the auto-start of the cloud-init service on boot**

- If your operating system uses systemd to manage auto-start services, execute the following commands to make the configuration.
  
  i. Execute the following command in Ubuntu or Debian.

    ln -s /usr/local/bin/cloud-init /usr/bin/cloud-init
ii. Execute the following commands in all operating systems.

```
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. Execute the following command in CentOS or Redhat.

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

```
[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 in `/lib/systemd/system/cloud-init.service` with the following:

```
[Unit]
Description=Initial cloud-init job (metadata service crawler)
Wants=cloud-init-local.service
Wants=sshd-keygen.service
Wants=sshd.service
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 auto-start services, execute the following commands to make the configuration.

    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

Execute the following command to install cloud-init.

    apt-get/yum install cloud-init

By default, the cloud-init version installed via `apt-get` or `yum` is the default cloud-init version in the software source configured for the current operating system. In the instances created with images whose cloud-init is installed this way, some configuration items may not be initialized as expected. It is recommended to install the service by manually downloading 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 in `/etc/cloud/cloud.cfg` with the content of the downloaded cloud.cfg file.

Related Operations

Please do not restart the server after you finish the following operations. Otherwise, you will need to perform the following operations again.

1. Execute the following command to see if cloud-init has been configured successfully.
   
   ```
   cloud-init init --local
   rm -rf /var/lib/cloud
   ```

2. Execute the following command in Ubuntu or Debian.
   
   ```
   rm -rf /etc/network/interfaces.d/50-cloud-init.cfg
   ```

3. For Ubuntu or Debian, you need to modify the content of `/etc/network/interfaces` to 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/*
   ```
Forcibly Import Image

Last updated: 2019-07-25 17:33:49

If you cannot install cloudinit in your Linux image for some reason, use Forced Image Import to import the image. At this point, Tencent Cloud cannot initialize your virtual machine. You need to define scripts to configure the virtual machine according to the configuration file provided by Tencent Cloud.

Limits and Configuration

Applying for Permission

Before using this feature, make sure that you have activated the image import permission. If you need to activate the permission, contact the Business Manager and submit relevant information to the ticket system.

Image Limits

- The image must meet the limits on importing Linux image in Import Image.
- The system partition for importing the image is not full.
- The imported image contains no vulnerability that can be exploited remotely.
- It is recommended that the user change the password immediately after the instance is created with forced image import.

Configuration of Image Import

Images forcibly imported by users do not use cloudinit, so automatic configuration is not available. Tencent Cloud provides the CDROM device containing configuration information for users to manually configure the images. Users need to mount the CDROM and read the configuration information from mount_point/qcloud_action/os.conf. Users can directly read the files in mount_point/ if other configuration data or UserData is required.

Content of 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
```
The parameter names above are for reference, and the values are only for example purpose.

The description of the parameters 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>
<tr>
<td>eth0_ip_addr</td>
<td>LAN IP of eth0</td>
</tr>
<tr>
<td>eth0_mac_addr</td>
<td>MAC address of eth0</td>
</tr>
<tr>
<td>eth0_netmask</td>
<td>Subnet mask of eth0</td>
</tr>
<tr>
<td>eth0_gateway</td>
<td>Gateway of eth0</td>
</tr>
<tr>
<td>dns_nameserver</td>
<td>DNS resolution server</td>
</tr>
</tbody>
</table>

Configuration Script Resolution

Notes
- The script must be executed on startup.
- Mount /dev/cdrom and read os_action/os.conf file under the mount point to obtain configuration information.
- The password placed in the CDROM by Tencent Cloud is encrypted. Users can set new password with chpasswd -e. Note that the encrypted password may contain special characters. It is recommended to place the password in a file and set it with chpasswd -e < passwd_file.
- When creating images from an instance created by forced image import, be sure to execute the script for proper configuration, or install cloudinit in the instance.

Example

Tencent Cloud provides an example script based on CentOS for users to define scripts for their images. Note that:

- **The script must be properly placed in the system before image import.**
- The script does not apply to all operating systems. Users need to modify it according to their own operating systems.
- The script must be set to execute on startup for normal use. Make the configuration according to the type of operating system. (For example, place the script `os_config` under `/etc/init.d/` directory and execute the following command.)

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

Run `chkconfig --list` to check if `os_config` is added to the startup service.

- Users must ensure that the script is properly executed. If problems such as failed to connect to the instance via SSH and failed to connect network occur after importing the image, try to connect to the instance in the console to execute the script again. If the problem remains, contact Customer Service.

The following is the example script `os_config`. Users 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
    fi
    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
EOF

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}\n"
RETVAL=3
;;
esac
exit $RETVAL
Linux Image Creation

Last updated: 2020-02-25 10:31:02

Scenario
This document guides you through the production of Linux Image.

Directions

Preparations
When making the system disk Image and Export, the following checks need to be carried out:

If you are through the data disk Image Export, you can skip this operation.

Check OS partition and Launch method

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

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

   - If the returned result is msdos, it is represented as a MBR partition, please perform the next step.
   - If the returned result is gpt, it is represented as GPT partition. GPT partition is not supported for service migration. Please Submit a ticket Feedback.

2. Execute the following command to check if the operating system is Launch in EFI mode.

   sudo ls /sys/firmware/efi

   - If you need to use the custom image feature, Submit a ticket .
   - If no, proceed to the next step.

Check the key files of the system
System key files to be checked include, but are not limited to, the following files:

Follow the standards of relevant distributions to ensure that the locations and permissions of the system-critical files are correct and the files can be read and written normally.
In the kernel parameter, `uuid` is recommended for mounting root. Other methods (such as `root=/dev/sda`) may cause the failure in starting 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 normal permissions and can be read and written.

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

### Check the virtio driver
Check the virtio driver: Please see [Check virtio Driver in Linux System](#).

### Installing cloud-init
- For Linux, see [Linux Image Production](#).

### Check other hardware-related configurations
Changes to the hardware on the cloud include but not limited to:

- Replacing the graphics card with cirrus vga.
- Replacing the disk with virtio disk. Device name is vda, vdb, and so on.
- Replacing the ENI with virtio nic. By default, only eth0 is available.

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

```
# mount
```

Take the returned result as an example:

```
proc on /proc  type  proc (rw, nosuid, nodev, noexec, relatime)
sys on /sys   type  sysfs (rw, nosuid, nodev, noexec, relatime)
dev on /dev   type  devtmpfs (rw, nosuid, relatime, size=4080220k, nr_inodes=1020055, mode=755)
run on /run   type  tmpfs (rw, nosuid, nodev, relatime, mode=755)
/dev/sda1 on /  type  ext4 (rw, relatime, data=ordered)
securityfs on /sys/kernel/security  type  securityfs (rw, nosuid, nodev, noexec, relatime)
tmpfs on /dev/shm  type  tmpfs (rw, nosuid, nodev)
devpts on /dev/pts  type  devpts (rw, nosuid, noexec, relatime, gid=5, mode=620, ptmxmode=000)
tmpfs on /sys/fs/cgroup  type  tmpfs (ro, nosuid, nodev, noexec, mode=755)
```
As you can see, the root partition is in `/dev/sda1` Medium, `/boot` and `/home`. There are no separate partitions, sda1 contains boot partitions, missing mbr, we just need to copy the entire sda.

At least the root partition and mbr should be included in Export's Image. If Export's Image lacks mbr, he will not be able to Launch.

In the current operating system, if `/boot` and `/home` For independent partitions, Export's Image also needs to include these two independent partitions.

**Export Image**

According to the actual needs, choose different ways Export Image.

- Use the tool Export
- Use orders Export Image
Use the platform tool Export Image

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

Use orders Export Image

Due to the use of commands, the risk of manual Export Image is relatively large (for example, it may cause metadata confusion of the file system when IO is busy, etc.). It is suggested that after Export and Image, Check Image Intact.

You can execute the following order Export Image:

Use qemu-img command

For example, execute the following command to set the /dev/sda Export to /mnt/sdb/test.qcow2.

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

among, /mnt/sdb For mounted new disks or other network storage.
If you need to convert to another format, please modify -O Gets or sets the parameter value of the
The parameter values that can be modified are as follows:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>Qcow2</td>
<td>Qcow2 format</td>
</tr>
<tr>
<td>VPC</td>
<td>Vhd format</td>
</tr>
<tr>
<td>Vmdk</td>
<td>Vmdk format</td>
</tr>
<tr>
<td>Raw</td>
<td>No format</td>
</tr>
</tbody>
</table>

# Use dd command for example, execute the following command, Image in Export raw format.
Parameter `count` is the number of partitions to be copied, which can be found by `fdisk` command. If you need to copy it completely, the parameter `count` can be ignored. For example, execute the following command to check the number of partitions for `/ dev/ sda`. `Disk-<new> / dev/ sda` A message similar to the one below is returned: `disk / dev/sda: 1495.0 GB, 1494996746240 bytes255 heads, 63 sectors/track, 181756 cylinders, total 2919915520 sectorsUnits = sectors of 1 * 512 = 512`
As you can see from the return result of `fdisk` command, the end position of sda1 is 41945087 * 512 bytes, and `count` can be set to 20481m.

The image exported through the `dd` command is in raw format. It is recommended to [convert it to qcow2, vhd or other image format](#ImageFormatConversion).

### Image format conversion

- At present, service migration supports image formats of qcow2, vpc, vmdk, and raw. A compressed image format is recommended to shorten the transmission and migration.

  Convert the image format using the qemu-img command:

  ```
  Sudo qemu-img convert-f raw-O qcow2 test.img test.qcow2
  ```

  `-f` is the source image file format.

  `-O` For the destination mirror file format, please refer to the supported format[`-Parameter value of O`](#-OParameterValue).

### Check the mirror image

When you create an image directly without stopping the service or for other reasons, the image file system may be incorrect. Therefore, it is recommended that you check whether the image is correct after creating the image.

When the image format is consistent with the format supported by the current platform, you can directly turn on the image to check the file system. For example, Windows platform can directly attach vhd format image, Linux platform can use qemu-nbd to open qcow2 format image, and Xen platform can directly enable vhd file.

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 will occur when using the mount command. In addition, you can start the CVM to check whether the image file works before uploading the image.
1. Preparations

The following checks are required to export a system disk image, and can be ignored when you export a data disk image.

- Check the OS partition. Service Migration does not support GPT-style partition.

  How to check the partition:

  Open the Control Panel -> Disk Management, right-click the disk to select Property, and you can find the Partition style in the figure below.

  If it reads GPT, the GPT-style partition is used.
Check the startup mode. Service Migration does not support starting the system with EFI. If EFI exists in the path, then the current operating system starts in the EFI mode. Open the command prompt (CMD) as admin and execute the following command:

```
bcdedit /enum {current}
```

Example of execution result:

```
C:\WINDOWS\system32>bcdedit /enum {current}
Windows bootstrapper
-------------------
identifier {current}
device partition=C:
  path ¥WINDOWS\system32\winload.exe
description Windows 10
locale zh-CN
inherit {bootloadersettings}
recoverysequence {f9dbeba1-1935-11e8-88dd-ff37cca2625c}
displaymessageoverride Recovery
recoveryenabled Yes
flightsigning Yes
allowedinmemorysettings 0x15000075
osdevice partition=C:
systemroot ¥WINDOWS
resumeobject {1bcd0c6f-1935-11e8-8d3e-3464a915af28}
xn OptIn
bootsmenupolicy Standard
```

Check the network configuration. Service Migration does not support IPv6 nor multi-ENI. Services that rely on both IPv6 and multi-ENI cannot work normally.

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

Check or install the virtio driver
The virtio driver has been installed if it is found in the **Control Panel -> Programs and Features**: 
Otherwise, you need to manually install the virtio driver:

- For the following system versions, download Tencent Cloud's customized virtio
  Microsoft Windows Server 2012 R2 (Standard Edition)
- For other system versions, download the virtio community version.

- Check the configurations of other hardware. Changes to the hardware on the cloud include but not
  limited to:
  - Replacing the graphics card with cirrus vga.
  - Replacing the disk with virtio disk.
  - Replacing the ENI with virtio nic. Local Area Connection is used by default.

2. Export the Image Using a Platform Tool

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

3. Export the Image Using Disk2vhd

The Disk2vhd tool can be used to export the system if it is deployed on a physical machine or if you do not want to export it using a platform tool.

**Download Disk2vhd**

The interface after installation is shown as below:

![Disk2vhd Interface](image)

When using the tool, select the volume to be copied and the name of the file to be exported, and click **Create** to export vhd.

**Note:**

- The vss feature must be preset in Windows before Disk2vhd can run.
- Do not select "Use Vhdx". The system does not support vhdx images.
- "Use volume Shadow Copy" should be selected to ensure the data integrity.
4. Check the Image

As mentioned above, an error may be occurred with the image file system if it is created when the server is not shut down or due to other reasons. Therefore, you are recommended to check whether the created image is error-free.

When the image format is consistent with the format supported by the current platform, you can directly open the image to check the file system. For example, vhd images can be directly added to Windows platform, qcow2 images can be opened using qemu-nbd on Linux platform, and vhd images can be enabled directly on Xen platform. 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 will occur when using the mount command.

In addition, you can start the CVM to check whether the image file works before uploading the image.
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:

<table>
<thead>
<tr>
<th>Destination CVM</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Security group: Ports 443 and 80 must be open in a security group.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Linux source server</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Check for and install Virtio. For more information, see Checking Virtio Drivers in Linux.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Check whether rsync and grub2-install (or grub-install) are installed.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Check whether SELinux is enabled. Disable it if enabled.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- 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.
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:

| Destination | 1. Storage: The cloud disks of the destination CVM, including system disks and |
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.

```
[root@M_0_32_centos go2tencentcloud]# sudo ./go2tencentcloud_x64
[2019-10-03 20:29:46] Start go2tencentcloud 1.3.0
[2019-10-03 20:29:48] [1/3] Initialize instance
[2019-10-03 20:29:50] Restart remote instance...
Used: 00:01:13 | Max Timeout: 00:10:00
[2019-10-03 20:31:04] Start preparing remote server...
[2019-10-03 20:31:05] Start initializing remote server...
Used: 00:00:11 | Max Timeout: 00:03:00
[2019-10-03 20:31:17] Stage 1 is finished and please run next stage at source machine.
```

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.

```
[root@VM_0_7_centos go2tencentcloud]# sudo ./go2tencentcloud_x64
[2019-10-03 20:33:54] Start go2tencentcloud 1.3.0
[2019-10-03 20:33:54] Load user.json successfully.
[2019-10-03 20:34:01] Check environment...
[2019-10-03 20:34:07] [2/3] Synchronize files
[2019-10-03 20:34:07] Transmitting files...
[2019-10-03 20:37:39] Reconfigure remote instance...
Used: 00:00:18 | Max Timeout: 00:05:00
[2019-10-03 20:37:58] Stage 2 is finished and please run next stage at gateway machine.
```

```
[root@VM_0_12_centos go2tencentcloud]# sudo ./go2tencentcloud_x64
[2019-10-03 20:49:34] Start go2tencentcloud 1.3.0
[2019-10-03 20:49:34] Load user.json successfully.
```
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. 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 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.

   ```bash
   sudo ./go2tencentcloud_x64
   ```

   Wait for the migration process to complete.
   If the migration is successful, the following console output appears:
ubunto@ip-172-31-46-19:/go2tencentcloud$ sudo ./go2tencentcloud_x64
[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

Last updated: 2020-02-11 14:32:45

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. |

©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:

   ```
   [root@lZWz94ahxe8jo0vmifzcZ go2tencentcloud]# sudo ./go2tencentcloud_x64
   [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 10:44:42] 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:

<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>
### 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:

   ```bash
   [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: 00:00:23 | 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...
   [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:

<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 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:

   ```bash
   [root@instance-mpev8blob go2tencentcloud]# sudo ./go2tencentcloud_x64
   [2019-10-02 22:34:59] Start go2tencentcloud 1.3.0
   [2019-10-02 22:35:03] Check environment...
   [2019-10-02 22:35:08] [1/3] Initialize instance
   [2019-10-02 22:35:08] Restart remote instance...
   Used: 00:01:24 | Max Timeout: 00:10:00
   [2019-10-02 22:36:33] Start preparing remote server...
   [2019-10-02 22:36:33] Start initializing remote server...
   Used: 00:00:11 | Max Timeout: 00:03:00
   [2019-10-02 22:36:45] [2/3] Synchronize files
   [2019-10-02 22:36:45] Transmitting files...
   [2019-10-02 22:38:59] Reconfigure remote instance...
   Used: 00:00:07 | Max Timeout: 00:05:00
   ```
Migrating VMWare Virtual Machine Data to Tencent Cloud

Last updated: 2020-02-11 14:14:22

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. |
|-----------------|-------------------------------------------------------------------------------------------------|
### 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:

   ```bash
   [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...
   [2019-10-03 05:34:31] Reconfigure remote instance...
   Used: 00:00:42 | Max Timeout: 00:05:00
   ```
Migrating China Telecom e-Cloud Cloud Server Data to Tencent Cloud

Last updated : 2020-02-11 14:15:40

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.

   ```
sudo ./go2tencentcloud_x64
   ```

   Wait for the migration process to complete.

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

Last updated: 2019-08-01 11:43:23

Scenario

Online migration is a service migration method that supports migrating physical machines, virtual machines, and third-party cloud servers to Tencent Cloud CVM, making it easy for you to deploy a unified platform for computing resources or build a hybrid cloud across different platforms. This document guides you through how to use online migration.

The source server mentioned in this page can be a physical server, virtual machine, or cloud server on another cloud platform such as AWS, Microsoft Azure, Google Cloud Platform, Alibaba Cloud, and Huawei Cloud.

Application Scenarios

Online migration is suitable for the following scenarios:

- Migrate physical servers, virtual machines, and third-party cloud servers to CVM.
- Complete service migration without interrupting your business.

Differences from Offline Migration

Data of the current running environment on the source server can be migrated to the destination server without service interruption. Throughout the entire process, you can completely store the running state of the source server and restore it to the original or even another hardware platform. After restoration, the virtual machine can still run smoothly with no perceptible differences in the usage of the service.

Supported OS

Operating systems supported for online migration include without limitation the following (32-bit or 64-bit):

<p>| Linux | Windows |</p>
<table>
<thead>
<tr>
<th>Linux</th>
<th>Windows</th>
</tr>
</thead>
<tbody>
<tr>
<td>CentOS 5/6/7</td>
<td>Windows Server 2016</td>
</tr>
<tr>
<td>Ubuntu 10/12/14/16/17</td>
<td>Windows Server 2012</td>
</tr>
<tr>
<td>Debian 7/8/9</td>
<td>Windows Server 2008</td>
</tr>
<tr>
<td>SUSE 11.4/12.1/12.2</td>
<td>Windows Server 2003</td>
</tr>
<tr>
<td>openSUSE 13.1</td>
<td></td>
</tr>
</tbody>
</table>

### Prerequisites

- Register a Tencent Cloud account and prepare the destination CVM instance.
- Contact your Tencent Cloud sales rep or submit a ticket to request the permission and migration tool installation package and install it on the source server (i.e., the server to be migrated).

### Directions

1. Use the migration tool to check the information such as configuration and network connection of the source server and the destination server to determine whether migration is possible.
2. Send the request through an API, and the console puts the destination server (i.e., CVM instance) in "waiting for migration" status.
3. Perform an incremental system disk migration until the tool determines that the migration is completed.

For more information, see the Online Service Migration Guide in the migration toolkit.
Offline Migration

Scenario

Service migration is a tool for easy online and offline migration from local DC to the cloud. With this tool, you can migrate OS, applications, and application data on local computer disks to Tencent Cloud Cloud Virtual Machine (CVM) or Cloud Block Storage (CBS).

Offline migration includes offline instance migration and offline data migration.

Prerequisites

Offline migration requires Cloud Object Storage (COS) support. For the currently COS-supported regions, see COS Regions. Please ensure that you are located in one of the supported regions.

Preparations

- At present, service migration supports image formats of qcow2, vpc, vmdk, and raw. A compressed image format is recommended to shorten the transmission and migration.
- The COS region to which the image is uploaded should be the same as that where the destination CVM instance is located.
- For offline migration, the uploaded image file cannot be larger than the capacity of the destination disk. For example, if the image file is 50 GB, the destination system disk should be at least 50 GB.
- Create an image of the server that needs to be migrated as instructed in the image creation document.
  - For Windows, see Windows Image Production.
  - For Linux, see Linux Image Production.
- Upload the created image file to COS.
  As image files are generally large in size, browser uploads are often interrupted. We recommended using the COSCMD tool to upload the image. For more information, see COSCMD.
Get the COS address of the uploaded image. In the COS Console, find the image file you just uploaded and view its information to get the file link.

Prepare the destination CVM instance. Click here to purchase > >.

Directions

**Offline Instance Migration**

1. Log in to the CVM Console.
2. In the left sidebar, click Service Migration
3. Click Create > Instance Migration.
4. Prepare for instance migration, confirm that everything is good, and click Next.
5. Enter the migration configuration information such as task name, COS link, and destination CVM instance and click Finish to create the migration task. View the progress of the migration task.

- The COS file needs to be set to public read and private write access.
- The system disk capacity of the destination instance cannot be smaller than the uploaded image file size; otherwise, the task will fail.

**Offline Data Migration**

1. Log in to the CVM Console and click Service Migration on the left.
2. Click Create > Data Migration.
3. Prepare for data migration, confirm that everything is good, and click Next.
4. Enter the migration configuration information such as task name, COS link, and destination CVM instance and click Finish to create the migration task.

- The destination data disk capacity cannot be smaller than the uploaded image file size; otherwise, the task will fail.

**FAQs**

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
Network

ENI

Last updated: 2020-03-06 10:50:15

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
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.

**Note:** each subnet can only be bound with one route table. Once you click “Confirm”, the existing route table will be replaced with: lab-rt... 

**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.
• Next hop: private IP of the CVM instance to which the elastic public IP is bound in Step 1.

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:

```
#!/bin/bash

echo "----------------------------------------------------"
echo "(1)ip_forward config......"
file=/etc/sysctl.conf
grep -i "^net.ipv4.ip_forward.*" $file &>/dev/null && sed -i "$file" 's/net_ipv4_ip_forward.*/net_ipv4_ip_forward = 1/' $file ||
    echo "net.ipv4.ip_forward = 1" >> $file
    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 TCOPTSTRIP --strip-options timestamp &&
  echo "-->mangle:Success" || echo "-->mangle:Fail"

echo "(3)nf_conntrack config......"
```

©2013-2019 Tencent Cloud. All rights reserved.
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/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" $mask_head_num $mask_tail)
fi
else
    mask_num=$((2 ** cpu_nums - 1))
    mask=$(printf "%x" $mask_num)
fi

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
    done

    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
if ethtool -l $eth goes wrong.
[[ ! "$max_combined" =~ ^[0-9]+$ ]] && max_combined=1
if [ $(max_combined) -ge $(cpu_nums) ]; then
  echo "$eth has equally nic queue as cpu, don't set rps for it..."
  continue
fi
else
  echo "$eth is smartnic, set rps for it..."
fi

echo "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))

eth "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:

    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

Scenario

Tencent Cloud offers basic network and VPC, both of which provide quality services for users. On top of that, we provide more services, enabling you to manage the network more flexibly.

- Switching between networks
  - Switching from basic network to VPC: you can switch the network from basic network to VPC for a single CVM or multiple CVMs all at once.
  - Switching from VPC A to VPC B: you can switch the network from VPC A to VPC B for a single CVM or multiple CVMs all at once.
- Setting up a custom IP
- Choosing whether to keep HostName

Notes

- When you switch the network for multiple CVMs all at once, the selected CVMs must be in the same availability zone.
- Before the migration, please unbind the CVM(s) from the internal and external network LB and ENI, and release the secondary IP of the primary ENI. You can rebind them after the migration.
- During the migration, the host instance needs to be restarted. Do not perform other operations.
- After the migration, please check whether the instance(s) is/are running normally and whether you are able to access the CVM(s) via the private network and log in to the CVM(s) remotely as usual.
- You can only switch from basic network to VPC, not the other way around. After you switch the network from basic network to VPC for your CVMs, they will not be able to communicate with cloud services in basic networks.

_directions

Preparing for the migration

1. Log in to the CVM Console.
2. On the Instance page, select the instance for which you want to switch the network, click More in the Operation column on the right, and select Resource Adjustment > Switch to VPC.

For switch the network for multiple CVMs, you can check the instances, click More actions at the top of the instance list, and select Switch to VPC.

3. Read the notes in the “Switch to VPC” window and click Next as shown below:

Selecting Network
Select a VPC and a subnet and click **Next** as shown below:

### Setting IP and HostName

Set a pre-allocated IP address in the selected subnet and set the HostName options according to actual needs as shown below:

- If you do not set a pre-allocated IP address, the system will automatically allocate one.
- When configuring the HostName options, you can choose to reset the instance HostName while switching to the VPC or keep the original HostName.
Starting migration

Click **Start Migration**, and on the instance list page you will see the status of instance is "Modify instance’s VPC attribute" as shown below:
Elastic Public IP

Last updated: 2019-12-20 19:32:47

Elastic IP, is referred to as EIP for short. It is a static IP designed for dynamic cloud computing, and a fixed public IP in a certain region. In case of an instance failure, the EIP can be remapped to another instance in your account (or NAT gateway instance) quickly to block the failure.

Common Operations

The following describes how to use EIPs.

Applying for EIPs

1. Log in to the CVM Console.

2. In the left navigation pane, click EIP.

3. Click the Apply button, enter a region and the number of EIPs you want to apply for, and then click OK.

4. After this, you can see in the list the new EIP(s) you just applied for, which have an unbound status.

Binding EIPs to cloud products

1. Log in to the CVM Console.

2. In the left navigation pane, click EIP.

3. In the EIP list, click the Bind button next to the EIP to be bound to a cloud product. (If the EIP is already bound to an instance, this button is unavailable. Please unbind it first.)

4. In the popup box, select the cloud product type that you want to bind, and then select the cloud product instance ID. Click the Bind button to complete the binding.

Unbinding EIPs from cloud products
1. Log in to the CVM Console.

2. In the left navigation pane, click EIP.

3. In the EIP list, click the Unbind button next to the EIP that is already bound to a cloud product.

4. Click OK.

**Note:**
After unbinding, the cloud product instance may be assigned a new public IP, which may be different from the one before binding.

### Releasing EIPs

1. Log in to the CVM Console.

2. In the left navigation pane, click EIP.

3. In the EIP list, click More -> Release button next to the EIP to be released.

4. Click OK.

### Adjusting bandwidth

1. Log in to the CVM Console.

2. In the left navigation pane, click EIP.

3. In the EIP list, click the Change Bandwidth button next to the EIP for which you want to adjust bandwidth.

4. Adjust the target bandwidth value in the Adjust Bandwidth page.

5. Click OK.

### Converting public IP to EIP
The public IP purchased along with the CVM instance is an ordinary public IP. It does not have elasticity and cannot be mounted and unmounted. Tencent Cloud allows you to convert an ordinary public IP to an EIP by following the steps below:

1. Log in to the CVM Console.

2. Click the Convert icon.

3. Click Confirm Conversion.
Troubleshooting

Network inaccessibility may occur with an EIP. This is generally caused by the following reasons:

- The EIP is not bound to any cloud product. For more information about how to bind an EIP to cloud products, please see Binding EIP 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, for example: access to 8080 port is denied, the port 8080 of the EIP is also inaccessible.
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 following command as follows:
   1. Run the following command to add the execution permission:
      ```bash
      chmod +x eip_direct.sh
      ```
   2. Run the following command to run the script:
      ```bash
      ./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.

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 Disks

Expand cloud disks

Last updated: 2019-10-14 10:50:14

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.

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.
Security Groups

Security Group Overview

Security group is a stateful virtual firewall for filtering packets and is used to set the network access controls for a single or multiple CVMs. It is a logical grouping and an important means of network security isolation.

- You can add the basic network-based CVM or ENI instances with the same network security isolation requirements in the same region to the same security group.
- You can use the security group policies to filter the inbound and outbound traffic of an instance, which can be a basic network-based CVM or an ENI instance.
- You can modify security group rules at any time, and the new rules take effect immediately.

Security Group Template

You can create a custom security group, or create a security group from template. Three templates are available in the system:

- Open Port 22 on Linux: Only TCP port 22 for SSH login is open to Internet, and all private network ports are open.
- Open Port 3389 on Windows: Only TCP port 3389 for MSTSC login is open to Internet, and all private network ports are open.
- Open all ports: All ports are open to Internet and private networks. This poses certain security risks.

Security Group Rules

Security group rules are used to control the inbound and outbound traffic of instances associated with the security group (filtered based on the rules from top to bottom). By default, a new security
group rejects all traffic (All Drop). Therefore, a CVM associated with a security group with no rules will reject all traffic.

Each security group rule involves the following items:

- **Type:** You can select a system rule template, or create custom rules.
- **Source or destination:** Traffic source (inbound rules) or destination (outbound rules). Choose one of the following options:
  - Specify a single IP in CIDR notation.
  - Specify an IP address range in CIDR notation, such as 203.0.113.0/24.
  - Reference a security group ID. You can reference one of the following security group IDs:
    - Current security group. (This indicates whether CVMs associated with the security group can be mutually accessed or not)
    - Another security group. Another security group ID of the same project in the same region.
- **Policy:** Allow or Reject.

**Note:**

- Referencing security group ID is optional. The rules of the referenced security group will not be added to the current security group.
- If you enter the security group ID in Source/Destination when configuring security group rules, the private IPs of the CVM's primary ENI and the ENI that are associated with this security group ID are used as Source/Destination, excluding public IP.

**Security Group Priority**

- Multiple security groups associated with an instance are **prioritized from the smaller number to the bigger number**.
- The rules in a security group are **prioritized from top to bottom**.

An instance associated with a security group with no rules will reject all traffic by default.

**Security Group Restrictions**

- Security groups are region and project-specific. CVMs can only be associated with the security groups in the same region and project.
- Security groups apply to any CVM instances in **network environment**.
Each user can set a maximum of 50 security groups for each project in each region. A maximum of 100 inbound/outbound access policies can be set for a security group. A CVM can be associated with multiple security groups, and a security group can be associated with multiple CVMs. No number limit is imposed.

Security groups associated with CVMs in **basic networks cannot filter** data packets sent from (or to) CDB and cloud cache service (Redis and Memcached) of Tencent Cloud. If necessary, you can use iptables to filter traffic of such instances.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security group</td>
<td>50/Region</td>
</tr>
<tr>
<td>Access policy</td>
<td>100 (Inbound/Outbound)</td>
</tr>
<tr>
<td>Number of security groups associated with an instance</td>
<td>No limit</td>
</tr>
<tr>
<td>Number of instances associated with a security group</td>
<td>No limit</td>
</tr>
</tbody>
</table>

**Note:**

If you have a large number of instances that need to access each other, you can assign them to multiple security groups, and achieve mutual authorization and access by configuring the rules for security group IDs.

**Comparison of Security Group and Network ACL**

<table>
<thead>
<tr>
<th>Security Group</th>
<th>Network ACL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operations at the CVM instance level (the primary defense layer)</td>
<td>Operations at the subnet level (the secondary defense layer)</td>
</tr>
<tr>
<td>Allow and Reject rules are supported</td>
<td>Allow and Reject rules are supported</td>
</tr>
<tr>
<td>Stateful: Returned traffic is automatically allowed without subjecting to any rules</td>
<td>Stateless: Returned traffic must be explicitly allowed by rules</td>
</tr>
</tbody>
</table>
Security Group-related Cloud APIs

Security group-related cloud APIs are Developer Tools of security groups. Cloud APIs can be used to work with security groups and manage the configurations of security groups and CVM instances.

<table>
<thead>
<tr>
<th>Security Group</th>
<th>Network ACL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operations are only applied to an instance if the security group is specified when the instance is launched or the security group is associated with the instance later.</td>
<td>Operations are automatically applied to all CVM instances in the associated subnet.</td>
</tr>
</tbody>
</table>
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:

```
Create a security group

Template: Open all ports
Name: Open all ports-2020030517310818894
Project: DEFAULT PROJECT
Notes: All ports open for both Internet and private network (HIGH-RISK)

OK Cancel
```

©2013-2019 Tencent Cloud. All rights reserved.
<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>
</tbody>
</table>
| ID of referenced security group | • Current security group: CVMs associated with the current security group.  
                                 | • Other security group: ID of another security group in the same region that belongs to the same project. |
| Reference IP address objects or IP group objects in a Parameter Template. | -                                                                           |

- **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.
Associating CVM Instances with Security Groups

Last updated: 2020-03-06 11:28:56

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 [link].
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

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

Last updated: 2020-03-06 11:38:51

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.
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

Last updated : 2020-03-06 11:47:18

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
Last updated : 2020-02-18 14:07:28

Operation scene
If you no longer need a security group rule, you can delete it.

prerequisite
- A security group has been created and security group rules have been added to the security group.
- It has been confirmed that Cloud Virtual Machine instance does not need to allow / prohibit which public network Access or private network Access.

Operation step
1. Login Cloud Virtual Machine console .
2. In Left sidebar, click [ Security Group ] to enter the security group management page
3. On the security group management page, select * * region * * to find the security group whose rules need to be deleted.
4. In the security group row where the rule needs to be deleted, click "modify Rule" in the action column to enter the security group rule page.
5. On the security group rules page, delete the direction to which the security group rules belong (inbound / outbound) as needed, and click the * * inbound / outbound rules * * tab.
6. Locate the security group rule that needs to be deleted, and click "Delete" in the action column.
7. In the pop-up prompt box, click OK.
Security group use cases

Last updated : 2020-02-25 10:08:18

Security groups are configured to manage access to Cloud Virtual Machines (CVMs). You can configure inbound and outbound rules for security groups to specify whether your CVMs can be accessed 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 open the inbound rule of the corresponding port to the Internet.
- 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 rejects 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 via SSH**

Case : You have created a Linux CVM and want to connect to the CVM via SSH remotely.
Solution When adding security group rules, select "Linux login" in "Type", Protocol port Enable 22, and Open to Internet Linux SSH login.

You can open all IP addresses or a specified IP address (or IP address range) to the Internet as required. This allows you to configure the source IP addresses of the CVMs that can be remotely connected to via 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&lt;br&gt;• Specified IP address: Enter your specified IP address or IP address range</td>
<td>TCP: 22</td>
<td>Allow</td>
</tr>
</tbody>
</table>
Scenario 2: Remotely connecting to a Windows CVM via RDP

Case: You have created a Windows CVM and want to remotely connect to the CVM via Remote Desktop (RDP).

Solution: When adding security group rules, select "Windows login" in "Type", Enable port 3389 Protocol, Open to Internet Windows remote login.

You can open all IP addresses or a specified IP address (or IP address range) to the Internet as required. This allows you to configure the source IP addresses of the CVMs that can be remotely connected to via 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</td>
<td>Login</td>
<td>TCP: 3389</td>
<td>Allow</td>
</tr>
<tr>
<td></td>
<td>Login</td>
<td>• All IP addresses: 0.0.0.0/0</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Specified IP address: Enter your specified IP address or IP address range</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Scenario 3: Pinging a CVM in a public network

Case: You have created a CVM and want to test whether its communication with other CVMs is normal.

Solution: Use the ping program for testing. That is, when adding security group rules, select the "type" as "Ping", Enable ICMP Protocol port, and allow other Cloud Virtual Machine to pass through ICMP Protocol Access this Cloud Virtual Machine.

You can open all IP addresses or a specified IP address (or IP address range) to the Internet as required. This allows you to configure the source IP addresses of the CVMs that can access this CVM via 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</td>
<td>ICMP</td>
<td>Allow</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Specified IP address: Enter your specified IP address or IP address range</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Scenario 4: Remotely logging in to a CVM via Telnet

Case: You want to remotely log in to a CVM via Telnet.

Solution: If you need to log in to Cloud Virtual Machine remotely through Telnet, you need to configure the following security group rules when adding security group rules:

<table>
<thead>
<tr>
<th>Direction</th>
<th>Type</th>
<th>Source</th>
<th>Protocol Port</th>
<th>Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Scenario 5: Opening access to a web service via HTTP or HTTPS

Case: You have built a website and want users to be able to access your website via HTTP or HTTPS.

Solution: If you need access to your website through HTTP or HTTPS, you need to configure the following security group rules according to your actual needs when adding security group rules:

- Allow all IP addresses in the public network 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</td>
<td>0.0.0.0/0</td>
<td>TCP: 443</td>
<td>Allow</td>
</tr>
</tbody>
</table>

- Allow some IP addresses in the public network to visit 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>The IP address or IP address range that is allowed to access your website</td>
<td>TCP: 80</td>
<td>Allow</td>
</tr>
<tr>
<td>Inbound</td>
<td>HTTPS</td>
<td>The IP address or IP address 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 1101) to be externally accessible.

Solution: When adding security group rules, select "Custom" in "Type", Enable 1101 Protocol port, which allows the service port specified by Access.

You can open all IP addresses or a specified IP address (or IP address 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>
<tbody>
<tr>
<td>Inbound</td>
<td>Custom</td>
<td>All IP addresses: 0.0.0.0/0</td>
<td>TCP: 1101</td>
<td>Allow</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Specified IP address: Enter your specified IP address or IP address range</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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 1102).

Solution: When adding security group rules, select "Custom" in "Type", configure Port 1102 of Protocol, set "Policy" to "reject", and reject the service port specified by 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>Inbound</td>
<td>Custom</td>
<td>• All IP addresses: 0.0.0.0/0</td>
<td>TCP: 1102</td>
<td>Reject</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Specified IP address: Enter your specified IP address or IP address range</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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 following these configurations:

- Allow the CVM instance to access a specified external IP address.
- Forbid the CVM instance from accessing any public IP addresses via 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>The specified public IP address that can be accessed by the CVM</td>
<td>The 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 following these 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>The 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 via FTP

Case: You want to upload a file to or download a file from a CVM by using the FTP software.

Solution: Add a security group rule by following these 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 to 21</td>
<td>Allow</td>
</tr>
</tbody>
</table>

Combination of multiple security rules

In a real 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 the security group at any time. For priority of security group rules, see Security Group Priority.
The following describes the common server ports. For more information on service application ports on Windows, please see Microsoft official document (*Windows Service Overview and Network Port Requirements*).

<table>
<thead>
<tr>
<th>Port</th>
<th>Service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>21</td>
<td>FTP</td>
<td>FTP server's open port for upload and download.</td>
</tr>
<tr>
<td>22</td>
<td>SSH</td>
<td>Port 22 is the SSH port, used to remotely connect to Linux system servers in command-line mode.</td>
</tr>
<tr>
<td>25</td>
<td>SMTP</td>
<td>SMTP server's open port for sending emails.</td>
</tr>
<tr>
<td>80</td>
<td>HTTP</td>
<td>Used for Web services, such as IIS, Apache, Nginx, to provide external access.</td>
</tr>
<tr>
<td>110</td>
<td>POP3</td>
<td>Port 110 is open for POP3 (email protocol 3) service.</td>
</tr>
<tr>
<td>137, 138, 139</td>
<td>NETBIOS protocol</td>
<td>Port 137 and 138 are UDP ports used to transfer files via My Network Places. Port 139: incoming connections over port 139 attempt to obtain NetBIOS/SMB service. This protocol is used for file and printer sharing on Windows as well as SAMBA service.</td>
</tr>
<tr>
<td>143</td>
<td>IMAP</td>
<td>Port 143 is mainly used for &quot;Internet Message Access Protocol&quot; (IMAP) v2, a protocol for receiving emails as the same as POP3.</td>
</tr>
<tr>
<td>443</td>
<td>HTTPS</td>
<td>Web browsing port. This is another type of HTTP that supports encryption and transfer over secure ports.</td>
</tr>
<tr>
<td>1433</td>
<td>SQL Server</td>
<td>Port 1433 is the default port for SQL Server. The SQL Server service uses two ports: TCP-1433 and UDP-1434. Port 1433 is used by SQL Server to provide external services, and port 1434 is used to send requester a response about which TCP/IP port is used by SQL Server.</td>
</tr>
<tr>
<td>3306</td>
<td>MySQL</td>
<td>Port 3306 is the default port for MySQL database and is used by MySQL to provide external services.</td>
</tr>
<tr>
<td>Port</td>
<td>Service</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>----------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>3389</td>
<td>Windows Server Remote Desktop Services</td>
<td>Port 3389 is the service port for remote desktop on Windows 2000 (2003) Server. You can connect to a remote server using the &quot;Remote Desktop&quot; connection tool via this port.</td>
</tr>
<tr>
<td>8080</td>
<td>Proxy Port</td>
<td>Just like port 80, port 8080 is used for WWW proxy service for web browsing. Port number &quot;:8080&quot; is often added when users visit a website or use a proxy server. In addition, after Apache Tomcat Web server is installed, the default service port is 8080.</td>
</tr>
</tbody>
</table>
# Security Group API Overview

Last updated: 2020-02-18 14:07:28

<table>
<thead>
<tr>
<th>API name</th>
<th>Interface function</th>
</tr>
</thead>
<tbody>
<tr>
<td>CreateSecurityGroup</td>
<td>Create a security group</td>
</tr>
<tr>
<td>CreateSecurityGroupPolicies</td>
<td>Add policies to a security group</td>
</tr>
<tr>
<td>DeleteSecurityGroup</td>
<td>Delete security group</td>
</tr>
<tr>
<td>DeleteSecurityGroupPolicies</td>
<td>Delete security group policies</td>
</tr>
<tr>
<td>DescribeSecurityGroupAssociationStatistics</td>
<td>Query statistics on the instances associated with a security group</td>
</tr>
<tr>
<td>DescribeSecurityGroupPolicies</td>
<td>Query security group policies</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 outbound and inbound policies of a security group</td>
</tr>
<tr>
<td>ReplaceSecurityGroupPolicy</td>
<td>Replace a single routing policy of a security group</td>
</tr>
</tbody>
</table>
You can create, view, update and delete security groups and security group rules or perform other operations on them in the CVM console.

Common Operations

Creating a security group
2. Click New button.
3. Enter the security group name (e.g. my-security-group) and the description.
4. Click OK to finish the creation.

Adding rules to security group
2. Select the security group to be updated, and then click Security Group ID. The Details pane will list the details of the security group as well as the tab for using inbound and outbound rules.
3. On the Inbound/Outbound Rules tab, click Edit. Select the options for the inbound/outbound rules from the tab, enter the required information, and then click Save.

Configuring a security group to associate with CVM instances
1. Open Console - CVM.
2. In the Operation column next to the instance for which you want to configure a security group, click More and then click Configure Security Group.
3. In the Configure Security Group dialog box, select one or more security groups from the list and click OK.

Or
2. Select the security group to be associated with CVMs, and then click Add Instances or Remove Instances button in the Operation column.
3. In the Add/Remove CVMs popup box, add or delete the CVMs to be associated with this security group, and click OK.
Importing/exporting security group rules

2. Select the security group to be updated, click Security Group ID. The Details pane will list the details of the security group as well as the tab for using inbound and outbound rules.
3. Select the options for inbound/outbound rules from the tab, and then click Import Rules button. If you already have the rules, it is recommended to export existing rules first. Importing the new rules will overwrite the existing rules. If the original rules are empty, you can export the template, edit the template file, and then import the file.

Cloning a security group

2. Click the Clone button for the security group to be cloned in the list.
3. In the Clone Security Group dialog box, select the destination region and project, and then click OK. If the new security group needs to be associated with a CVM, reconfigure the security group.

Deleting a security group

2. Click the Delete button for the security group to be deleted in the list.
3. In the Delete Security Group dialog box, click OK. If the current security group is associated with a CVM, disassociate the security group from the CVM before deleting it.

Typical Scenario Configuration

Remotely logging in to Linux instances via SSH

To log in to a Linux instance via SSH remotely, add the following inbound rule to the security group associated with the instance:

<table>
<thead>
<tr>
<th>Source</th>
<th>Protocol Port</th>
<th>Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0/0</td>
<td>TCP:22</td>
<td>Allow</td>
</tr>
</tbody>
</table>

Note: You can set IP address range or security group for the Source.
Logging in to Windows instances via MSTSC

To log in to a Windows instance via MSTSC, add the following inbound rule to the security group associated with the instance:

<table>
<thead>
<tr>
<th>Source</th>
<th>Protocol Port</th>
<th>Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0/0</td>
<td>TCP:3389</td>
<td>Allow</td>
</tr>
</tbody>
</table>

**Note:** You can set IP address range or security group for the Source.

Pinging a CVM instance in public network

To test the communication status of a CVM instance using Ping program, add the following inbound rule to the security group associated with the instance:

<table>
<thead>
<tr>
<th>Source</th>
<th>Protocol Port</th>
<th>Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0/0</td>
<td>ICMP</td>
<td>Allow</td>
</tr>
</tbody>
</table>

**Note:** You can set IP address range or security group for the Source.

Using CVM instance as Web servers

If you create an instance as a Web server, you need to install the Web server program on the instance, and add the following inbound rule to the security group associated with the instance:

<table>
<thead>
<tr>
<th>Source</th>
<th>Protocol Port</th>
<th>Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0/0</td>
<td>TCP:80</td>
<td>Allow</td>
</tr>
</tbody>
</table>

**Note:** You need to start the Web server program first, and check whether the port is set to 80.

Uploading or downloading files with FTP

To upload/download files to/from a CVM instance with FTP, add the following inbound rule to the security group associated with the instance:
**Note:** You need to install the FTP server program on the instance, and then check whether the port 20/21 works properly.

<table>
<thead>
<tr>
<th>Source</th>
<th>Protocol Port</th>
<th>Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0/0</td>
<td>TCP:20,21</td>
<td>Allow</td>
</tr>
</tbody>
</table>
Limits

Last updated: 2018-06-13 10:28:19

- Security groups are region and project-specific. CVMs can only be bound with the security groups in the same region and project.
- Security groups apply to any CVM instances in network environment.
- Each user can set a maximum of 50 security groups for each project in each region.
- A maximum of 100 inbound/outbound access policies can be set for a security group.
- A CVM can be associated with multiple security groups, and a security group can be associated with multiple CVMs. No number limit is imposed.
- Security groups bound with CVMs in basic network cannot filter data packets sent from (or to) relational database (CDB) and cloud cache service (Redis and Memcached) of Tencent Cloud. If necessary, you can use iptables to filter traffic of such instances.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security group</td>
<td>50/Region</td>
</tr>
<tr>
<td>Access policy</td>
<td>100 (Inbound/Outbound)</td>
</tr>
<tr>
<td>Number of security groups associated with an instance</td>
<td>No limit</td>
</tr>
<tr>
<td>Number of instances associated with a security group</td>
<td>No limit</td>
</tr>
</tbody>
</table>

**Note:**

If you have a large number of instances that need to access each other, you can assign them to multiple security groups, and achieve mutual authorization and access by configuring the rules for security group IDs.
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.
Manage Login Password

Last updated: 2020-02-25 10:15:35

Scenario

Cloud Virtual Machine's account number and password is credential who logs in to Cloud Virtual Machine. This document describes how to use and manage passwords when logging in to Cloud Virtual Machine.

Limits

When setting a password, the following restrictions must be met:

- Linux instance: password length should be 8mi 30. It is recommended to use a password of more than 12 characters, which cannot start with "/" and contains at least three (a-z, A-Z, 0-9 and `!@#$%^&*-+=_|{}[]':;'<>,.?/) The special symbol of).
- Windows instance: password length should be 12 / 30 characters, cannot start with "/", and contain at least three items (a-z, A-Z, 0-9 and `!@#$%^&*-+=_|{}[]':;'<>,.?), excluding the user name

Directions

Setting initial password

In the purchase of Cloud Virtual Machine, the choice of configuration is different, the initial password setting will be different.

- Approve Custom configuration Method to create an instance: during the creation process, the initial password is set in different ways depending on the login method.

<table>
<thead>
<tr>
<th>Login mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatic password</td>
<td>The initial password will be via email and console Internal message I'll send it to you.</td>
</tr>
<tr>
<td>generation</td>
<td></td>
</tr>
<tr>
<td>Associate Key</td>
<td>Off by default Login with username and password, but the initial password will still be via email and console Internal message I’ll send it to you.</td>
</tr>
<tr>
<td>Now</td>
<td></td>
</tr>
</tbody>
</table>
The custom password is the initial password.

Viewing Password

The password to log in to Cloud Virtual Machine will be via email and console Internal message I'll send it to you. The following operations take internal message as an example.

1. Log in to the CVM Console.
2. Click in the upper right corner \( \text{✉️} \) Select the corresponding product message Go to the product message page to view the password.

Resetting Password

Reset Password
Managing SSH keys

Last updated: 2020-02-11 11:08:24

Scenario

The password is an exclusive login credential for every CVM. To ensure the reliability and security of an instance, Tencent Cloud provides the following two login methods:

- Password Login
- SSH key pair login

This document describes common operations in using SSH key pair to log in to an instance.

Steps

**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 pop-up Create SSH key window, select the method for creating a key, enter the 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 key 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 that need 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. **Logging into Linux Instance via SSH Key**.
Scenario
This document guides you in managing spread placement group.

Directions
Creates a placement group

1. Log in to the CVM Placement Group Console .
2. Click CREATE .
3. In the pop-up window, Enter places the name of the group and selects the placement group level.
4. Click OK To finish the creation process.

Starting up Instance in Placement Group

1. Go to the CVM Purchase Page .
2. Follow the prompts on the page to complete the purchase.
   During the purchase process, please pay attention to the following actions:
   
   - When setting up the host, click [ Advanced Settings ], check [ Add instance to spread placement group ], select an existing placement group.
   
   - If no existing placement group meets your requirement, you can Create a placement group In the console.

   - On the Confirm Configuration Page, enter the total number of instances to be added to the placement group, which must be less than the number limit set for the placement group.

Modifying Instance's Placement Group

You can only change the name of a placement group.

1. Log in to the CVM Placement Group Console .
2. Mouse over the ID/ name of the placement group, click 📝 .
3. In the pop-up window, enter the name you want to modify.
4. Click OK To finish the creation process.

Delete Placement Groups
If you need to replace or no longer need a placement group, you can delete it. Before deleting, you must first put all instances of Launch in the placement group by Terminate.

1. Log in to the **CVM Placement Group Console**.
2. In the placement group row to be deleted, click "number of instances" to go to the instance management page, and Terminate places all instances in the group.
3. Go back to the placement group console, select the placement group to be deleted, and click "Delete".
4. In the pop-up dialog box, click **OK** To complete the cordoning.
   Placement groups support batch deletions and individual deletions.
Unblocking Port 25

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: 2019-10-09 19:37:49

Overview

A tag is a key-value pair provided by Tencent Cloud which is used to identify resources on the cloud. You can use tags to classify CVM resources based on various factors such as service, usage, and person in charge. With tags, you can quickly sift through the resource pool and find the corresponding resources. The value of the tag keys does not mean anything to Tencent Cloud semantically and will be parsed and matched strictly according to the string.

Here we use a specific case to describe how to use tags.

Use Case Background

A company has 10 CVMs on Tencent Cloud, which are owned by three departments: e-commerce, games, and entertainment. The CVMs are used for services such as marketing campaigns, game A, game B, and post-production. The operation and maintenance managers of the three departments are Ada, Bob, and Chris.

Setting Tags

For more efficient management, the company uses tags to categorize the CVM resources, and defines the following key/value pairs.

<table>
<thead>
<tr>
<th>Tag Key</th>
<th>Tag Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Department</td>
<td>E-commerce, games, entertainment</td>
</tr>
<tr>
<td>Service</td>
<td>Marketing campaigns, game A, game B, post production</td>
</tr>
<tr>
<td>Operation and Maintenance Manager</td>
<td>Ada, Bob, Chris</td>
</tr>
</tbody>
</table>

After the key/value pairs are bound to the cloud services, the relationship between resources and key/value pairs will be as shown below:
<table>
<thead>
<tr>
<th>instance-id</th>
<th>Department</th>
<th>Service</th>
<th>Operation and maintenance manager</th>
</tr>
</thead>
<tbody>
<tr>
<td>ins-abcdef1</td>
<td>E-commerce</td>
<td>Marketing campaigns</td>
<td>Chris</td>
</tr>
<tr>
<td>ins-abcdef2</td>
<td>E-commerce</td>
<td>Marketing campaigns</td>
<td>Chris</td>
</tr>
<tr>
<td>ins-abcdef3</td>
<td>Games</td>
<td>Game A</td>
<td>Ada</td>
</tr>
<tr>
<td>ins-abcdef3</td>
<td>Games</td>
<td>Game B</td>
<td>Ada</td>
</tr>
<tr>
<td>ins-abcdef4</td>
<td>Games</td>
<td>Game B</td>
<td>Ada</td>
</tr>
<tr>
<td>ins-abcdef5</td>
<td>Games</td>
<td>Game B</td>
<td>Bob</td>
</tr>
<tr>
<td>ins-abcdef6</td>
<td>Games</td>
<td>Game B</td>
<td>Bob</td>
</tr>
<tr>
<td>ins-abcdef7</td>
<td>Games</td>
<td>Game B</td>
<td>Bob</td>
</tr>
<tr>
<td>ins-abcdef8</td>
<td>Entertainment</td>
<td>Post-production</td>
<td>Chris</td>
</tr>
<tr>
<td>ins-abcdef9</td>
<td>Entertainment</td>
<td>Post-production</td>
<td>Chris</td>
</tr>
<tr>
<td>ins-abcdef10</td>
<td>Entertainment</td>
<td>Post-production</td>
<td>Chris</td>
</tr>
</tbody>
</table>

**Using Tags**

**Looking for the CVM instances of which Chris is in charge**
You can find the corresponding CVM instances by looking for the tag **Operation and maintenance manager: Chris** according to the filter rules. For specific filtering methods, see Using Tags to Filter Resources.

**Looking for the CVM Instances which Bob is in charge of and which are used by the Games Department**
You can find the corresponding CVM instances by looking for the tags **Department: Games, Operation and maintenance manager: Bob** according to the filter rules. For specific filtering methods, see Using Tags to Filter Resources.
A tag is a key-value pair. You can set tags for your CVMs to categorize your resources. With tags, you can quickly sift through your resource pool and find the corresponding resources.

Now, you can edit tags for your CVMs in the Console. The following describes the requirements for tags.

**Maximum number of tags**
- Each cloud resource can have up to 50 tags.

**Requirements for tag keys**
- You cannot use “qcloud”, “tencent”, or “project” at the beginning of a tag key because they are reserved by the system.
- A tag key can only contain numbers, letters and special characters (+,=,@-).
- The maximum length of a tag key is 255 characters.

**Requirements for tag values**
- A tag value can only contain numbers, letters and special characters (+,=,@-) or be an empty string.
- The maximum length of a tag value is 127 characters.
Edit Tags

Last updated: 2020-02-01 18:05:54

Overview

You can edit the tags of resources according to the following steps.

Use Limits

There are some limits on editing tags:

- **Maximum**: each resource can have at most 50 tags.

- **Tag key**:
  - qcloud, tencent, project cannot create tags starting with system reserved tags.
  - Required to be number, alphabet character, +=@- less than 255 characters.

- **Value**: Required to be empty string or number, alphabet character, +=@- less than 127 characters.

Prerequisite

Log in to the CVM console, and open the CVM page.

**Edit the tags of a single instance**

1. Select the instance that you want to edit tags on the left.
   
   Click [More] > [Instance Setting] > [Edit Tags]

2. Add, modify, and delete tags in the Edit Tags box.

**Edit the tags of multiple instances**

You can edit tags of up to 20 instances at one time.

1. Select multiple instances, and at the top menu, click [More actions] > [Edit tags]

2. Add, modify, and delete tags in the Edit Tags box.
Filter Resources Based on Tags

You can use the following steps to filter resources based on tags.

1. Log in to the CVM console, and open the CVM page.
2. Select a region.
3. Select Tag in the search box at the top of the list.
4. Enter the tag key and tag value after the Tag:
   For example:
   - Filter out instances bound to a tag key (such as Name). Tag: name.
   - Filter out instance tags bound to a tag key-value pair (such as Name:tencent). Tag: name:tencent.
   - Filter out instance tags bound to multiple tag key-value pairs (such as Name: tencent and use:test). Tag: name:tencent, use:test.
5. Press Enter or click Search icon to search.
Monitoring and Alarms
Get Monitoring Statistics

Scenario

Tencent Cloud provides cloud monitoring for all users by default, no need for the user to manually turn on. But the user must use Tencent Cloud products before cloud monitoring can begin to collect monitoring data; to view these monitoring data, there are several ways:

Directions

Obtain monitoring data from the cloud product console

Some cloud products provide a separate monitoring data reading tab on their own console pages. CVM is used in this example

1. Open Tencent Cloud Console, select CVM.

2. Click the CVM Instance ID from the list of CVMs to view the monitoring data, and enter the CVM details page.

3. Click the Monitor tab; on this page, you can view the CPU, memory, network bandwidth, disk and monitoring data, etc. of the CVM instance. You can also freely adjust the time range.

Obtain monitoring data from Cloud Monitor Console

On Cloud Monitoring console, you can view monitoring data for most of the products used. In this case, CVM is used as an example.

1. Open Tencent Cloud Console, select Basic Cloud Monitor.

2. On the left navigation bar, select Cloud Product Monitoring - Cloud Virtual Machine.

3. Click the CVM Instance ID from the list of CVMs displayed to view the monitoring data, and enter the monitoring details page.
4. On this page, you can view the CPU, memory, network bandwidth, disk and all monitoring data of the CVM instance. You can also freely adjust the time range.

Obtain monitoring data through the API

Users can use the GetMonitorData API to obtain monitoring data for all products.
Create Alarm Polices

Last updated: 2020-02-01 19:15:11

Scenario

You can create an alarm to get notified for status change of Tencent Cloud services. The created alarm determines whether to trigger a notification according to the comparison results between a monitored metric and a specific threshold at regular interval.
You can take precautionary or remedial measures in a timely manner when an alarm is set off by status changes. Therefore, creating a valid alarm can help you improve your application's robustness and reliability.
Each alarm policy is a set of triggering 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, the user can view the alarm and take appropriate actions in time.

Prerequisite

Log in to Cloud Monitor Console

Directions

Create Alarm

1. On the left, choose Alarm Configuration > Alarm Policy
2. Click Add button.
3. On the new page, enter a policy name and select alarm triggering conditions. The triggering condition is a semantic condition consisting of metric, comparison relation, threshold, measurement period, number of continuous periods and repeated notification policy.
4. Click Complete

Associating an Object

1. On the left, choose Alarm Configuration > Alarm Policy
2. On the alarm policy list page, click the newly created alarm policy. On the details page, click Add Object button and select the cloud server you want to associate, and then click Apply to submit.
Set an Object to Receive Alarms

1. On the left, choose **Alarm Configuration > Alarm Policy**
2. Click the created alarm policy to enter its details page, in **Alarm Recipient Object** part, select the recipient groups that need to be edited.
Console Example

Last updated: 2020-02-25 10:18:28

Scenario

You can use Access to manage (Cloud Access Management, CAM) policy to let users have Permission who views and uses specific resources in the Cloud Virtual Machine (Cloud Virtual Machine, CVM) console. This document provides Permission examples of viewing and using specific resources to guide users on how to use policies for specific parts of the console.

Operation Examples

Full read-write policy for CVMs

If you want the user to have Permission who creates and manages the CVM instance, you can use a policy named: QcloudCVMFullAccess for that user. The strategy is achieved by allowing users to operate on all resources in CVM, VPC (Virtual Private Cloud), CLB (Cloud Load Balance) and MONITOR, respectively.

Detailed procedure is shown below:
Refer to Authorization Management To authorize the default policy QcloudCVMFullAccess to the user

Read-only policy for CVMs

If you want the user to have Permission to query the CVM instance, but not Permission to create, delete, and switch the machine, you can use the policy named QcloudCVMInnerReadOnlyAccess for the user. This strategy is achieved by allowing the user to have actions on all actions starting with the word "Describe" and all actions starting with the word "Inquiry" in the following action CVM, Permission. The specific steps are as follows:
Refer to Authorization Management To authorize the default policy QcloudCVMInnerReadOnlyAccess to the user

Read-only policy for CVM-related resources

To allow a user to only query CVM instances and relevant resources (VPC, Load Balance), without granting him/her the permissions to create, delete, start/shut down the instances, implement the policy named QcloudCVMReadOnlyAccess.

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 Load Balance.
All operations in the monitor.

Detailed procedure is shown below:
Refer to Authorization Management To authorize the default policy QcloudCVMReadOnlyAccess to the user

**Policy for elastic cloud disks**

If you want users to view HDD cloud disk information in the CVM console and have Permission who created HDD cloud disk and used HDD cloud disk, you can first add the following actions to your policy, and then apply the policy Associate to the user.

**CreateCbsStorages**: Create a cloud disk.

**AttachCbsStorages**: Mount the specified elastic cloud disk to the specified CVM.

**DetachCbsStorages**: Unmount the specified elastic 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 elastic cloud disks that have been mounted to a CVM and the maximum number of elastic cloud disks that are allowed to be mounted to the CVM.

**RenewCbsStorage**: Renew the specified elastic cloud disk.

**ResizeCbsStorage**: Expand the capacity of specified elastic cloud disk.

Detailed procedure is shown below:

1. According to Policy To create a custom policy that can view the information of HDD cloud disk in the CVM console, such as creating HDD cloud disk and using HDD cloud disk and other Permission. The policy content can be set by referring to the following policy syntax:

```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. Locate the created policy, and in the actions column of the policy row, click Associate user / Group.

3. In the pop-up Associate user / user Group window, select the user / group you need to authorize, and click OK.

**Policy for security groups**

If you want the user to be able to view and use the security group in the CVM console, you can add the following action to your policy, and then apply the policy Associate to that 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.

Detailed procedure is shown below:

1. According to Policy To create a custom policy that allows users to create, delete, modify security groups, and other Permission in the CVM console

   The policy content can be set by referring to the following policy syntax:

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

2. Locate the created policy, and in the actions column of the policy row, click Associate user / Group.
3. In the pop-up Associate user / user Group window, select the user / group you need to authorize, and click OK.

**Policy for EIPs**

If you want the user to view and use the elastic IP address in the CVM console, you can add the following action to your policy first, and then apply the policy Associate to the user.

- **AllocateAddresses**: Assign an EIP to VPC or CVM.
- **AssociateAddress**: Associate an EIP to an instance or a network interface.
- **DescribeAddresses**: View EIPs in 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.

Detailed procedure is shown below:

- **Policy management**
  
  This policy allows users to view the elastic IP address in the CVM console and give its Assign to the instance and compare it to Associate, but cannot modify the attributes of the elastic IP address, cancel Associate of the elastic IP address, or release Permission of the elastic IP address. The policy content can be set by referring to the following policy syntax:

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

2. Locate the created policy, and in the actions column of the policy row, click Associate user / Group.

3. In the pop-up Associate user / user Group window, select the user / group you need to authorize, and click OK.

**Policy for authorizing users to perform operations on specific CVMs**
If you want to authorize a user to have a specific CVM operation, Permission, you can apply the following policy Associate to that user. The specific steps are as follows:

- **Policy management**

  This policy allows users to operate on a CVM instance whose ID is ins-1, and whose region is Guangzhou. The policy content can be set by referring to the following policy syntax:

  ```json
  {
    "version": "2.0",
    "statement": {
      "action": "cvm:*",
      "resource": ["qcs::cdb:ap-guangzhou:uin/653339763:instanceId/*"]
    }
  }
  ```

  2. Locate the created policy, and in the actions column of the policy row, click Associate user / Group.

  3. In the pop-up Associate user / user Group window, select the user / group you need to authorize, and click OK.

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

If you want to authorize the user to have the operation of CVM in a specific region, Permission, you can apply the following policy Associate to that user. The specific steps are as follows:

- **Policy management**

  This policy allows users to operate on CVM machines in Guangzhou region, Permission. The policy content can be set by referring to the following policy syntax:

  ```json
  {
    "version": "2.0",
    "statement": {
      "action": "cvm:*",
      "resource": "qcs::cvm:ap-guangzhou::*"
    }
  }
  ```
2. Locate the created policy, and in the actions column of the policy row, click Associate user / Group.

3. In the pop-up Associate user / user Group window, select the user / group you need to authorize, and click OK.

Granting a sub-account full permissions for CVMs with the exception of billing

Suppose that there is a sub-account (Developer), under the enterprise account (CompanyExample, ownerUin is 12345678). The sub-account needs to have all the management Permission (such as creation, management, etc.) for the CVM service of the enterprise account, but does not include payment for Permission (orders can be placed but cannot be paid). We can achieve this through the following two scenarios:

- **Option A**
  The CompanyExample enterprise account directly authorizes the preset policy QcloudCVMFullAccess to the Developer sub-account. For more information about authorization, see Authorization Management.

- **Option B**

  1. Create a Custom Policy.

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

  2. Authorize the policy to the sub-account. For more information on authorization, see Authorization Management.

The sub-account is granted to have the operation of project management, Permission.

Suppose that under the enterprise account (CompanyExample, ownerUin is 12345678), there is a sub-account (Developer), that needs to manage resources on the console based on the project authorization sub-account. Detailed procedure is shown below:
1. Create a custom strategy for project management according to the business Permission.
2. Authorize the policy to the sub-account. For more information on authorization, see Authorization Management.
   
   If a sub-account is not prompted by Permission when doing project management, such as viewing snapshot, Image, VPC, elastic public network IP and other products without Permission, you can authorize the default policies of sub-account QcloudCVMAccessForNullProject, QcloudCVMOrderAccess and QcloudCVMLaunchToVPC. Please refer to the authorization method. Authorization Management.

Custom policy

If you feel that the preset policy does not meet your requirements, you can do so by creating a custom policy.

For detailed directions, see Creating a Cluster.

For more policy syntax related to CVM, please refer to Authorization policy syntax.