Elastic Compute Service

User Guide

User Guide

Quick reference

This article provides a quick reference for you on the use of ECS on the ECS Management Console.

Must read: ECS usage instructions

- A must-read for using ECS

Log on to an instance

How to use a username and password to log on to a Linux instance?

How to use an SSH key pair to log on to a Linux instance?

How to log on to a Windows instance?

If you forget your instance logon password (not the Management Terminal password), you can reset the password.

Operate disks

- How to attach a data disk after you purchase a cloud disk?

Change the operating system

You can change the operating system, such as:

From Windows to Linux, or from Linux to Windows.

From one version to another, for example, from Windows Server 2008 to Windows Server

2012.

Change the image, for example, change to custom images, or shared images.

Use images and snapshots

How to copy images across different regions?

How to define automatic snapshot policies when you want an automatic update policy for configurations or applications?

Enable Intranet communication

- How to use security groups to enable intranet communication?

For the answers to the above questions, click the corresponding node in the left navigation bar.

ECS operation instruction

To ensure proper operation of your ECS instance, you must take the considerations outlined in this section into account before use.

Prohibitions

Alibaba Cloud prohibits you from:

- Using your instance for flow-through services. Any violation will result in punishment up to shutdown and lockout of instance, and termination of services.
- Upgrading the ECS kernel or OS without prior authorization.
- Activating SELinux.
- Uninstalling PVDriver.
- Arbitrarily modifying the network adapter’ s MAC address.

General operating system considerations

- For an ECS with more than 4 GB RAM, use of a 64-bit OS is recommended, because a 32-bit OS supports a maximum of 4 GB RAM. Currently available 64-bit systems include:

- Aliyun Linux
- CoreOS
- CentOS
- Debian
- FreeBSD
- OpenSUSE
- SUSE Linux
- Ubuntu
- Windows 2008/2012

- 32-bit Windows OS support CPUs with up to 4 cores.
- To ensure service continuity and avoid service downtime, enable auto-start of service applications upon OS boot.
- For I/O-optimized instances, do not stop the **aliyun-service** process.

Restrictions

ECS does not support:

- Sound card applications.
- The installation of external hardware devices such as hardware dongles, USB drives, external hard drives, and the USB security keys issued by banks.
- SNAT and other IP packet address translation services. Achieve this using an external VPN or proxy.
- Multicast protocol. If multicasting services are required, unicast point-to-point method is recommended.
- Virtual application installation or subsequent virtualization such as when using VMware.

Linux restrictions

To ensure stable system operation, **DO NOT**:

- Modify the content of the default /etc/issue file. Modifying this file will render management console buttons unusable.
- Modify directory permissions in partitions, particularly permissions for directories such as /etc, /sbin, /bin, /boot, /dev, /usr, and /lib. Improper modification of permissions may cause errors.
- Rename, delete, or disable the Linux **root** account.
- Compile or perform any other operations the Linux kernel.
- Enable the **NetWorkManager** service. This service conflicts with the internal network service of the system and will cause network errors.

Windows restrictions

- Do not close the built-in **shutdownmon.exe** process. This may delay the restart of your

Windows server.
- Do not rename, delete, or disable the **Administrator** account.
- The use of virtual memory is not recommended.

Pay-As-You-Go restrictions

The Pay-As-You-Go service is subject to the following restrictions:

- An ECS server can use only one payment method, meaning that you cannot switch between Subscription and Pay-As-You-Go services. You cannot modify the configuration of the Pay-As-You-Go service， including upgrades of bandwidth, CPU/memory, and data disks.
- If a fixed 0 Mbps bandwidth is selected, you will not be allocated an external IP address, neither can you upgrade the bandwidth.
- A record-filing service is not offered for Pay-As-You-Go services.
- The 5-day unconditional refund is not offered for Pay-As-You-Go services.
- The fee for Pay-As-You-Go services is calculated per hour as follows: Total fee = CPU fee ＋ memory fee ＋ data disk fee ＋ public bandwidth fee.

ECS API product and business restrictions

Restricted item	**Parameter**	**To apply for an exception or unlock configuration rights**
User creation of ECS resources	N/A	Users must undergo real-name authentication
Zones in which users may create instances	1 online zone	Request increase via ticket
Zones in which users may create disks	The zone combinations in which users may create instances and the zones where instances will remain after overlap removal	N/A
Default pay-as-you-go instance types	ecs.t1.small (single-core 1 GB)	Request change via ticket
	ecs.s1.small (single-core 2 GB)	
	ecs.s1.medium (single-core 4 GB)	
	ecs.s2.small (dual-core 2 GB)	
	ecs.s2.large (dual-core 4 GB)	
	ecs.s2.xlarge (dual-core 8 GB)	
	ecs.s3.medium (quad-core 4	

	GB)	
	ecs.s3.large (quad-core 8 GB)	
	ecs.m1.medium (quad-core 16 GB)	
Default pay-as-you-go instance quota	30	Request increase via ticket
Number of disks within a single instance	API 5 (including the system disk)	No higher configurations exist
Support for pay-as-you-go ephemeral disks	Supported	For APIs, open a ticket.Other types do not support this disk type.
Capacity of a single ephemeral disk	20 to 1,024 GB	No higher configurations exist
Total ephemeral disk size for a single instance	2,048 GB	No higher configurations exist
Number of snapshots	(Number of disks)*64*	No higher configurations exist
Capacity of a single basic cloud disk	5 to 2,000 GB	No higher configurations exist
List of available system images	List of images for sale on the official website (10 images at present)	Common users cannot change; for others, open a ticket to add other images
Number of images	30	Request change via ticket
Available incoming bandwidth for a public network	Up to 200 Mbps	No higher configurations exist
Available outgoing bandwidth for a public network	Up to 200 Mbps	No higher configurations exist
Available range of public network outgoing traffic	Up to 200 Mbps	No higher configurations exist
Number of instances allowed in a single security group	1000	No higher configurations exist
Number of authorization rules for a single security group	100	No higher configurations exist
Security group quota	100	Request increase via ticket
Maximum number of security groups that a single instance can belong to	5	No higher configurations exist
Restrictions on image and instance types	Instances with 4 GB or more of memory cannot use 32-bit images	N/A

Adding new disks for ephemeral disk instances	Not supported	N/A
Changing the configuration of an instance with ephemeral disks	Bandwidth is adjustable	No exceptions (cloud disks can be used for attachment)
Relationship between the system disk and data disk	If the system disk is a cloud disk, all data disks must be cloud disks	N/A
Total number of pay-as-you-go cloud disks that can be purchased	ECS Instance Quota 5	Open a ticket
Basic cloud disk capacity	5 to 2,000 GB	No higher configurations exist
User restrictions for the creation of pay-as-you-go cloud disks	Users must pass real-name authentication (for buy only)	N/A
Range of system disk attaching points	/dev/xvda	N/A
Range of data disk attaching points	/dev/xvd[b-z]	N/A
Number of EIPs for a single user	20	Request change via ticket
EIP available bandwidth range	0 to 200 Mbps	Request increase via ticket
Number of VPCs for a single user	1	Request change via ticket
VPC optional CIDR range	192.168.0.0/16, 172.16.0.0/12, and their subnets	Request change via ticket
Number of VSwitches for a single VPC	24	Request change via ticket
Number of route entries in a route table	48	Request change via ticket
Capacity of a single SSD cloud disk	20 to 2,048 GB	No higher configurations exist
Capacity of a single Ultra Cloud disk	20 to 2,048 GB	No higher configurations exist

Connect

Use Management Terminal (VNC) to connect to an ECS instance

You can use the Management Terminal, also called VNC, to connect to an ECS instance, especially when the remote access software program that you are using, such as PuTTy, Xshell, or SecureCRT, cannot work.

Usage scenarios

The Management Terminal is used to:

- Check the status of an ECS instance if boot speed is slow.
- Reconfigure the firewall if a remote connection fails due to a software error within the ECS instance.
- End abnormal processes consuming excessive CPU usage or bandwidth.

Note: The Management Terminal can be used to connect to an instance even if purchased bandwidth is insufficient.

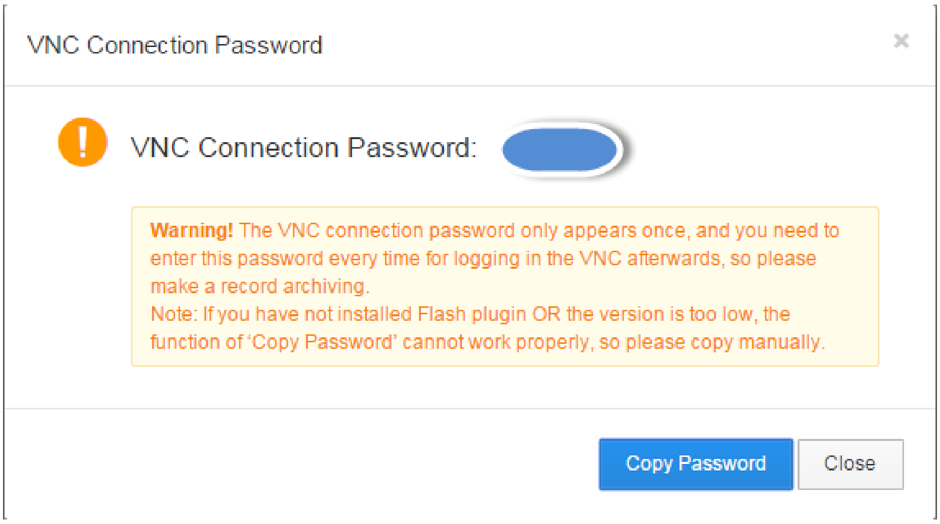
Procedure

Log on to the ECS Management Console.

Go to the ECS instance to connect to, and click **VNC** on the right.

Follow the tips below to connect to the **Management Terminal**:

- If you connect the **Management Terminal** for the first time, follow the steps below:
    a. On the **VNC Connection Password** dialog, copy the password. This dialog appears only once, but you need to enter the connection password each time you want to connect to the **Management Terminal**, so **write down the password**.



VNC Connection Password

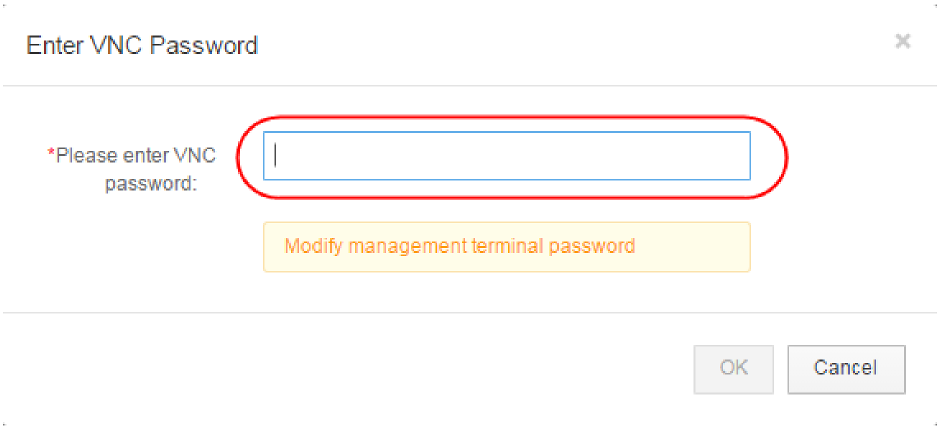
VNC Connection Password:

Warning! The VNC connection password only appears once, and you need to enter this password every time for logging in the VNC afterwards, so please make a record archiving.

Note: If you have not installed Flash plugin OR the version is too low, the function of 'Copy Password' cannot work properly, so please copy manually.

b. Click the **Close** button to close the **VNC Connection Password** dialog.

c. On the **Enter VNC Password** dialog, paste the connection password that you copied, and then click the **OK** button to connect to the **Management Terminal**.



Enter VNC Password

*Please enter VNC password:

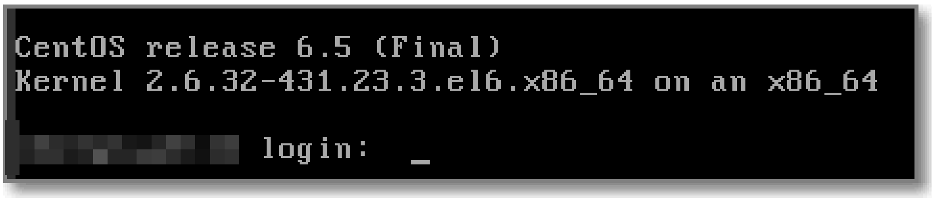
Modify management terminal password

- If this is not your initial connection to the **Management Terminal**, the **Enter VNC Password** dialog appears, and you need to enter the connection password and click the **OK** button to connect to the **Management Terminal**.
- If you forget the password, you can follow the steps below to connect to the **Management Terminal**:
  a. Change password.
  b. On the upper left corner of the **Management Terminal** interface, click **Send remote command** > **Connect to management terminal**.
  c. On the **Enter VNC Password** dialog, enter the new password to finish connection.

Follow the steps below to connect to an instance:

For a Linux instance, enter the user name（“root”）and the password to connect to it. Your screen may go black constantly, which occurs when the Linux instance is in sleep mode. Click the mouse or press any key to wake it up.

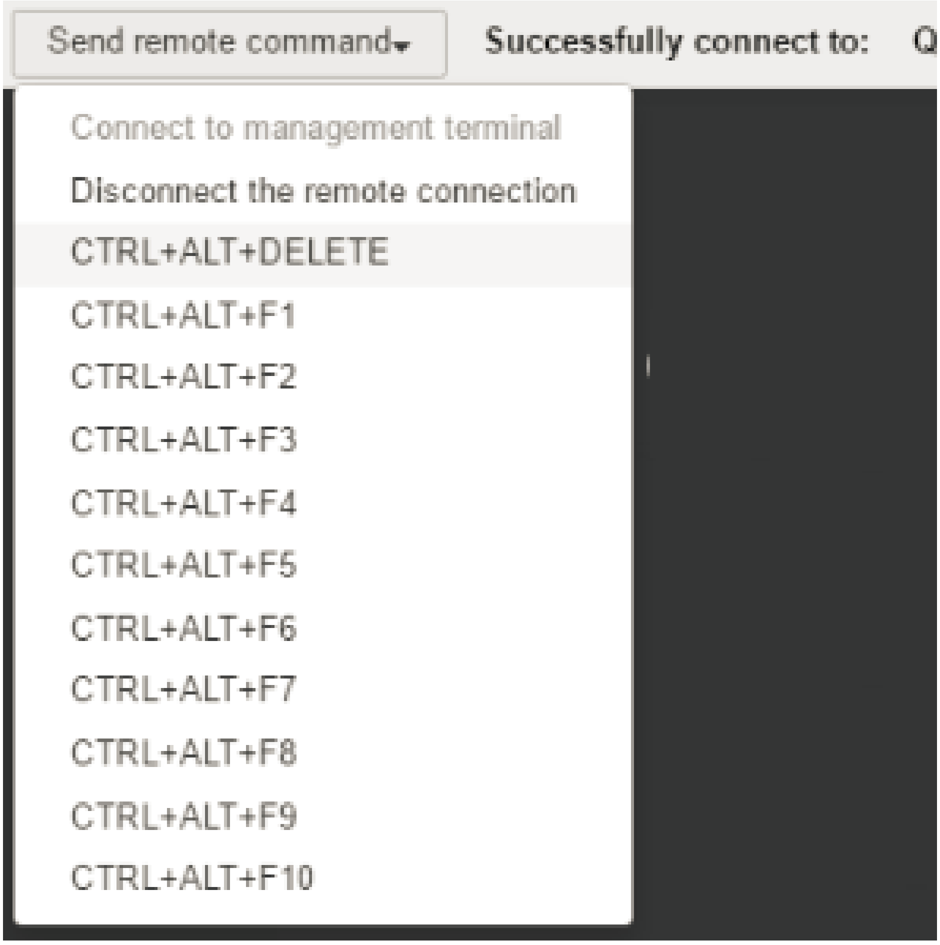
If you are operating several Linux instances, you can click **Send remote command** > **CTRL+ALT+Fx**, of which **Fx** can be any one from **F1** to **F10**, to switch management terminals.



```
CentOS release 6.5 (Final)
Kernel 2.6.32-431.23.3.el6.x86_64 on an x86_64

[redacted] login: _
```

For a Windows instance, on the upper left corner of the **Management Terminal** interface, click **Send remote command** > **CTRL+ALT+DELETE** to get to the logon screen. Enter the user name, Administrator, and password to log on.



Successfully connect to: Q

Change password

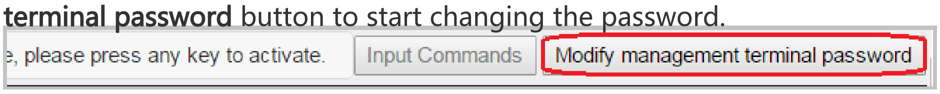
If you prefer a password that you are familiar with rather than the password displayed on the **VNC Connection Password** dialog, or if you forget your password, you can change the connection password.

Note: If the instance that you are connecting to is not I/O optimized, you need restart your instance to make the new VNC connection password take effect after you change it. The restart operation will stop the work of your instance and interrupt your business. So you must be cautious to change the password.

Log on to the ECS Management Console.

Go to the ECS instance to connect to, and click **VNC** on the right.

Close the **VNC Connection Password** dialog or **Enter VNC Password** dialog, and on the upper right corner of the **Management Terminal** interface, click the **Modify management terminal password** button to start changing the password.


e, please press any key to activate.
Input Commands
Modify management terminal password

Enter a new password, which must be of 6-character length, composed of uppercase letters, lowercase letters, digits, or a combination of them, but not special characters.

Make the new password take effect:

- If the instance that you are connecting to is I/O optimized, the new password takes effect immediately.
- If the instance that you are connecting to is not I/O optimized, restart the instance through the Management Console for the new password to take effect. Restarting within the instance does not work.

FAQ

Q: Can multiple users be simultaneously connected to the Management Terminal?
A: No. Only one user can be connected to the Management Terminal at any given time.

Q: Why can I not connect to an instancethrough the Management Terminal after changing the password?
A:Ensure you are entering the right **VNC connection password**. If the instance that you are connecting to is not I/O optimized, you must restart the instance through the Management Console for the new **VNC connection password** to take effect. Restarting directly within the instance will not make the password take effect.

Q: Why do I see a black screen after logging on to my instance?
A: A black screen indicates that the instance is in sleep mode.

- For a Linux instance, press any key to wake it up.
- For a Windows instance, click **Send remote command** > **Ctrl+ALT+DELETE** to bring back the logon interface.

Q: Why can I not access the Management Terminal?
A: To address login issues, open your browser and connect to the Management Terminal. Press the F12 key to open the developer tool. The Management Terminal information can then be analyzed to locate faults under the Console tab.

Q: I cannot use IE8.0 or Firefox to open the Management Terminal. How can I resolve this?
A: Only IE10 or higher is supported, and only certain versions of Firefox are supported.
To resolve this issue, update or change your browser to a compatible version.
Note: Google Chrome offers the best support for the Management Terminal function, and is recommended for use when you connect to the Management Terminal.

Log on to an instance using an SSH key pair

In this section, it is demonstrated how to use a key pair to log on to a Linux instance, using the popular SSH tools PuTTY and PuTTYgen as an example.

Prerequisites

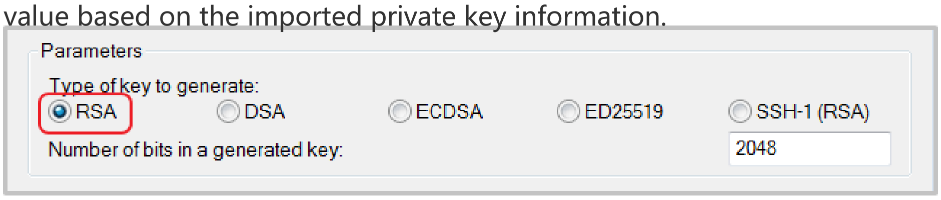
- PuTTY and PuTTYgen must have been installed. You can download them at:
  - For PuTTY: https://the.earth.li/~sgtatham/putty/latest/w64/putty.exe.
  - For PuTTYgen: https://the.earth.li/~sgtatham/putty/latest/w64/puttygen.exe.
- You must have a Linux instance that have been bound to an instance. You can allocate an SSH key pair when creating an instance or bind an SSH key pair to an instance.

Operating procedure

(**Optional**) If you are using a key pair generated by Alibaba, of which the private key is a .pem file, you must convert it to a .ppk file. If your private key is a .ppk file, you can skip this step.

i. Start PuTTYgen. In this example, we use PuTTYgen version 0.68.

Under the **Type of key to generate** option, select **RSA**. The value of **Number of bits in a generated key** can be left as is. The software will automatically update the value based on the imported private key information.



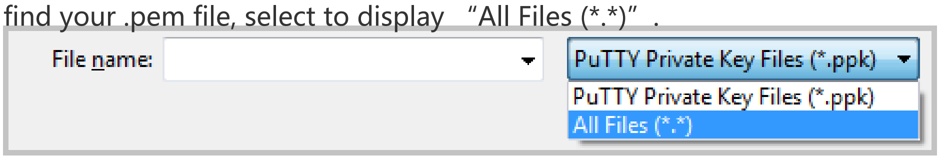
Parameters

Type of key to generate:

● RSA ○ DSA ○ ECDSA ○ ED25519 ○ SSH-1 (RSA)

Number of bits in a generated key: 2048

Click **Load**. By default, PuTTYgen only displays files with an extension of .ppk. To find your .pem file, select to display "All Files (*.*)".



File name:
PuTTY Private Key Files (*.ppk)
PuTTY Private Key Files (*.ppk)
All Files (*.*)

Select the downloaded private key file from Alibaba Cloud, or the ready private key file, and click **Open**.

Click **OK** to close the confirmation dialog box.

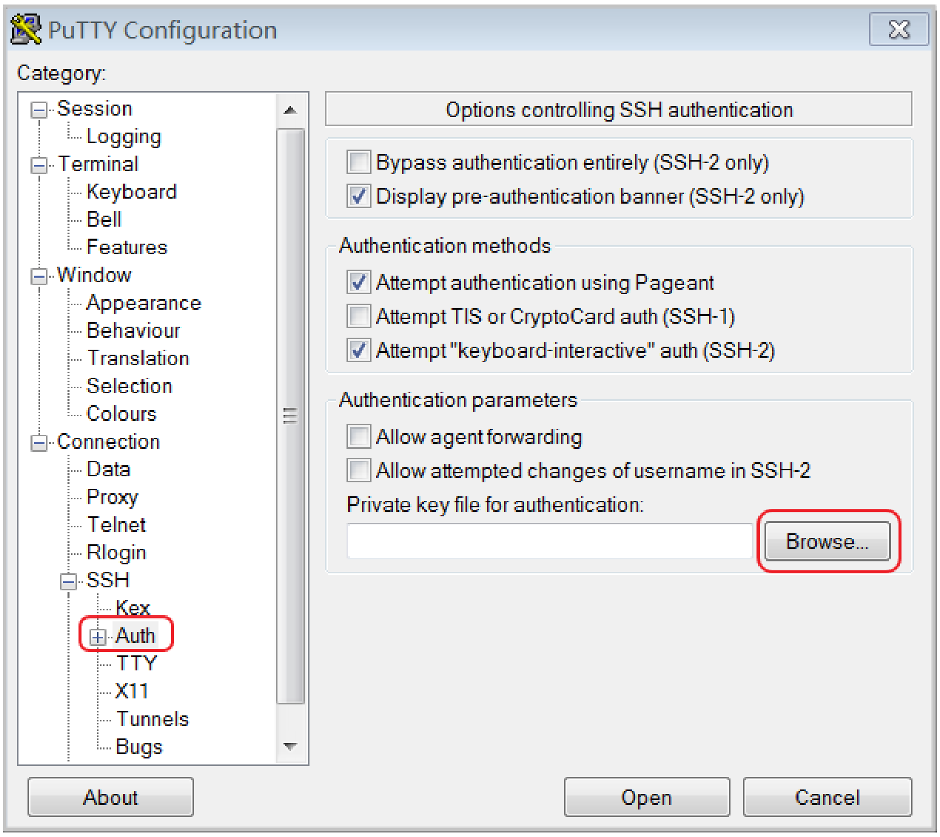
Click **Save private key**. PuTTYgen will display a warning about saving the key without a password. Click **Yes**.

Specify the same name for the private key with the key pair, and save the settings. PuTTY automatically adds the .ppk file.

Start PuTTY.

Click **Connection** > **SSH** > **Auth**.

Click **Browse...** and select the .ppk file generated in Step **1**.



Options controlling SSH authentication

□ Bypass authentication entirely (SSH-2 only)
☑ Display pre-authentication banner (SSH-2 only)

Authentication methods

☑ Attempt authentication using Pageant
□ Attempt TIS or CryptoCard auth (SSH-1)
☑ Attempt "keyboard-interactive" auth (SSH-2)

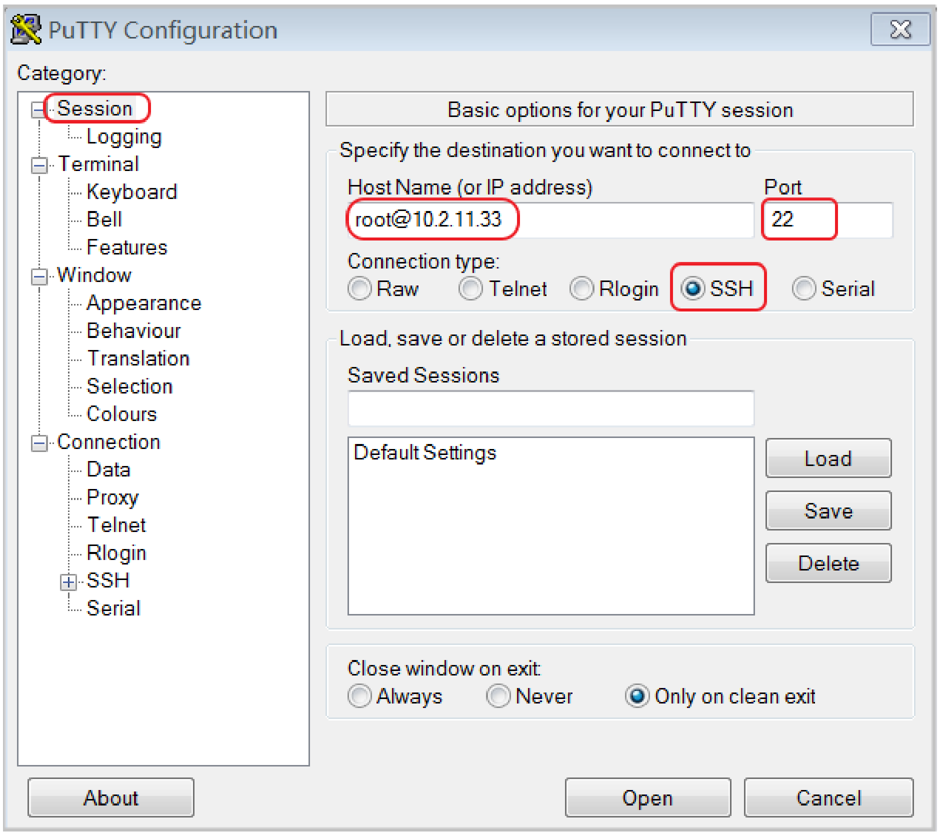
Authentication parameters

□ Allow agent forwarding
□ Allow attempted changes of username in SSH-2

Private key file for authentication:

Click **Session**.

- In **Host Name (or IP address)**, enter your account and the public IP address of the instance to be connected to. The format is “root@IP address”.
- In **Port**, enter the port number **22**.
- For **Connection type**, select **SSH**.



PuTTY Configuration

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): root@10.2.11.33

Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Load, save or delete a stored session

Saved Sessions: Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

Click **Open** to start accessing your Linux instance.

When the window shows *Connection established.*, it indicates you have successfully logged on to the instance using the key pair.

Connect to a Linux instance

The utilities used to remotely connect to Linux ECS instances vary based on the local OS as follows:

- For a Linux OS, use Secure Shell (SSH) Command Line.
- For a Windows OS, use either Management Terminal or use SSH Command Line through PuTTY or other SSH clients.
- For a Mac OS, use Management Terminal or SSH Command Line.
- For iPhone, use SSH Control Lite.
- For Android, use SSH Control Lite.

Connect to a Linux instance using Windows OS

On a Windows system, you can connect to a Linux instance using either of the following methods:

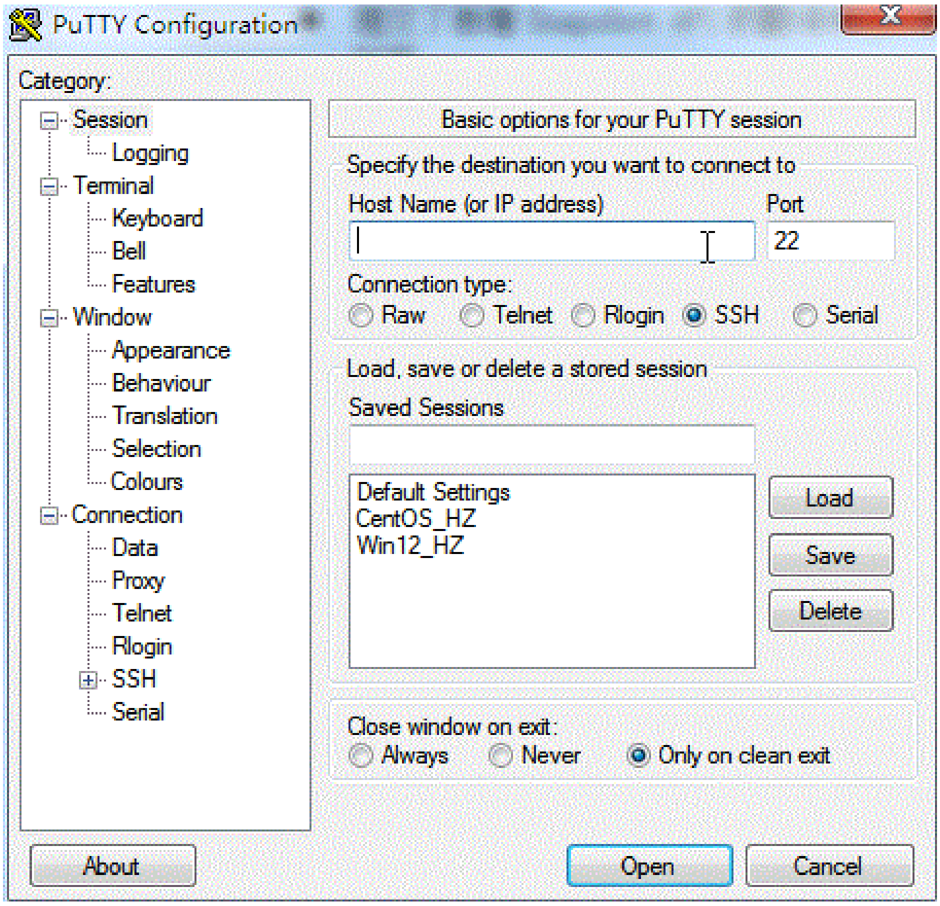
Remote access softwareThis method is available only if you purchased bandwidth when creating your instance. Prior to using this method, ensure the instance can be accessed through the Internet.

Management Terminal (VNC)Connection through the Management Terminal (VNC) can be completed disregarding whether bandwidth has been purchased.

Use a remote connection Application

This section uses PuTTY as an example. PuTTY can be downloaded at http://www.chiark.greenend.org.uk/~sgtatham/putty/.You can connect to a Linux instance via PuTTY as follows:

1. Start Putty.exe.
2. Enter the public IP address of the instance in **Host Name (or IP address)**.
3. Use the default port **22**.
4. Select **SSH** as **Connection Type**.
5. Type a session name in **Saved Sessions**, and then click **Save**. In later logins, you may directly load the session without re-entering the IP address.
6. Click **Open** to connect.



Host Name (or IP address):

Port: 22

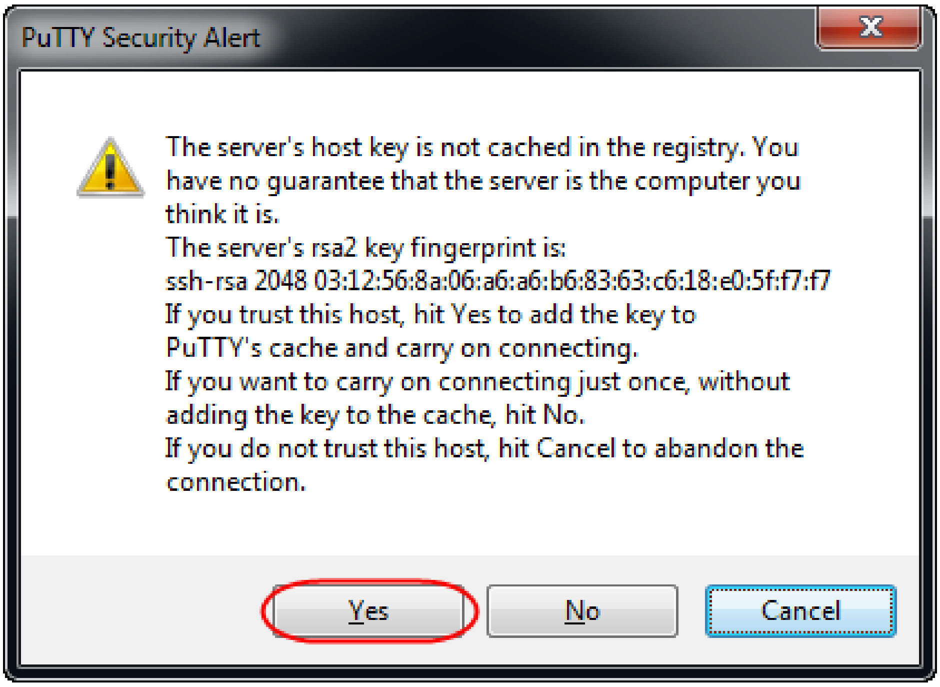
Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Saved Sessions:

Default Settings
CentOS_HZ
Win12_HZ

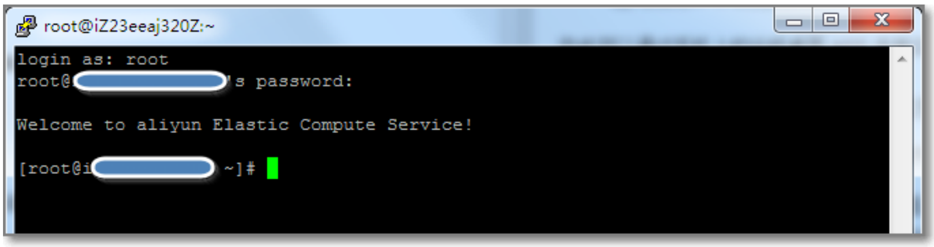
Close window on exit: ○ Always ○ Never ● Only on clean exit

7. Upon first connection, the following dialog box will be displayed. Click **Yes**.



The server's host key is not cached in the registry. You have no guarantee that the server is the computer you think it is.
The server's rsa2 key fingerprint is:
ssh-rsa 2048 03:12:56:8a:06:a6:a6:b6:83:63:c6:18:e0:5f:f7:f7
If you trust this host, hit Yes to add the key to PuTTY's cache and carry on connecting.
If you want to carry on connecting just once, without adding the key to the cache, hit No.
If you do not trust this host, hit Cancel to abandon the connection.

8. As prompted, enter the username and password for the Linux ECS instance. The password will not be displayed on-screen. Press the **Enter** key to complete connection to the instance.



```
login as: root
root@[redacted]'s password:

Welcome to aliyun Elastic Compute Service!

[root@i[redacted] ~]#
```

When you connect your computer to the Linux instance successfully, you can operate the instance from your computer.

Use Management Terminal to connect to an ECS instance

Refer to Use Management Terminal (VNC) to connect to an ECS instance.

Connect to a Linux instance using Linux OS or Mac OS X

1. Connect to the instance using SSH commands (for example: ssh root@Instance’ s public IP address.
2. Enter the root user password.

Connect to a Linux instance using an mobile app

You can connect to an instance via a remote desktop application installed on your smart phone. For example, iPhone users can download **SSH Control Light** from the App Store and use it to connect to Linux instances.

What if I forget my logon password?

If you forget your instance logon password (not the Management Terminal password), reset the logon password. For details, refer to Reset the password.

Connect to a Windows instance

The utilities used to remotely connect to Linux ECS instances vary based on local OS as follows:

- For a Linux OS, use rdesktop.
- For a Windows OS, use Management Terminal or Microsoft Terminal Services Client (MSTSC).
- For a Mac OS, use Management Terminal or MSTSC.
- For iPhone, use the Microsoft Remote Desktop app.
- For Android, use the Microsoft Remote Desktop app.

Connect to a Windows instance using Windows OS

Using a local Windows OS, connect to a Windows instance using one of the following:

Microsoft Terminal Services Client (MSTSC)
This method is available only if you purchased bandwidth when creating your instance. Prior to using this method, ensure the instance can be accessed through the Internet.

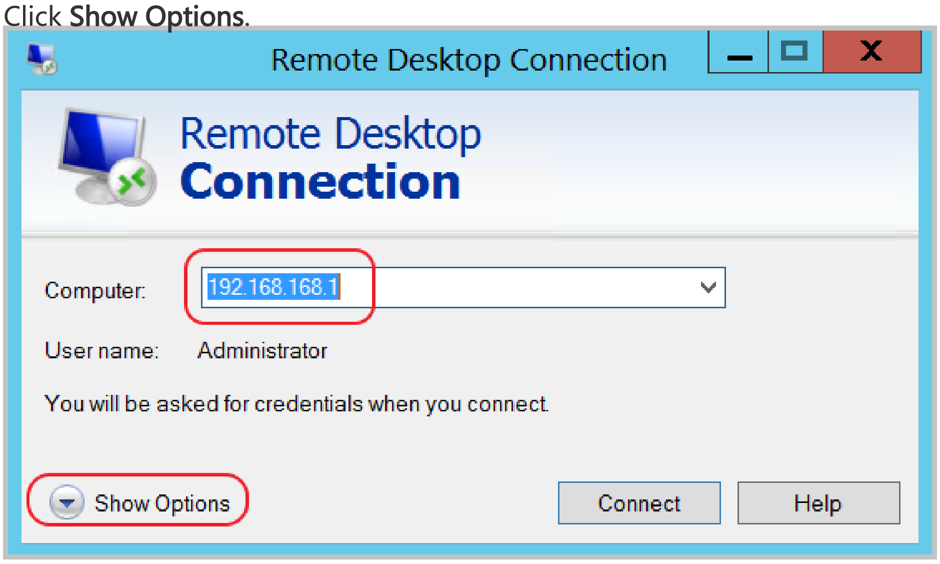
Management Terminal (VNC)
Connection through the Management Terminal can be completed disregarding whether bandwidth has been purchased.

Use MSTSC

Perform one of the following to start Remote Desktop Connection:

- Click **Start** > **Remote Desktop Connection**.
- Click the **Start** icon and enter **mstsc** in the search box.
- Press the shortcut key **Windows Logo** + **R** to open the **Run** window, enter **mstsc**, and then press the **Enter** key.

In the **Remote Desktop Connection** dialog box, enter the public IP address of the instance. Click **Show Options**.



Remote Desktop Connection

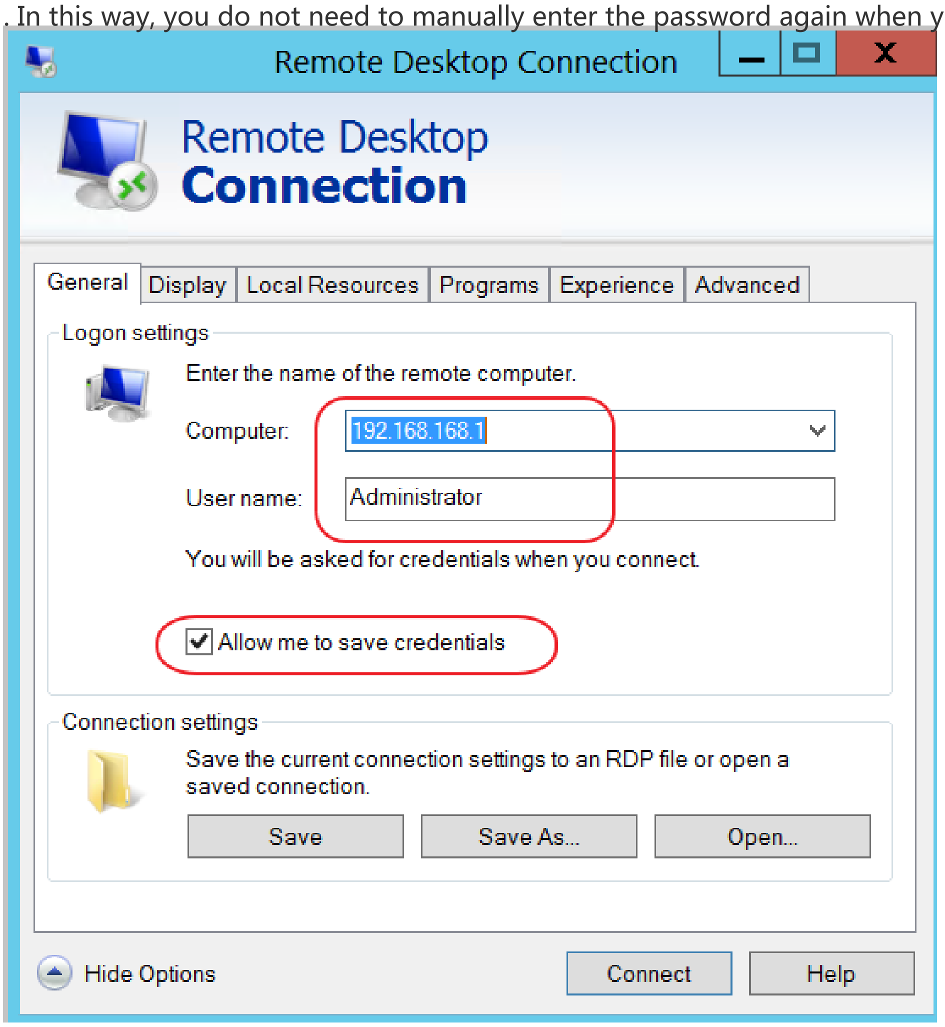
Remote Desktop Connection

Computer: 192.168.168.1

User name: Administrator

You will be asked for credentials when you connect.

Enter the user name. The default value is **Administrator**. Check **Allow me to save credentials** . In this way, you do not need to manually enter the password again when you log on later.



Remote Desktop Connection

Remote Desktop Connection

Logon settings

Enter the name of the remote computer.

Computer: 192.168.168.1

User name: Administrator

You will be asked for credentials when you connect.

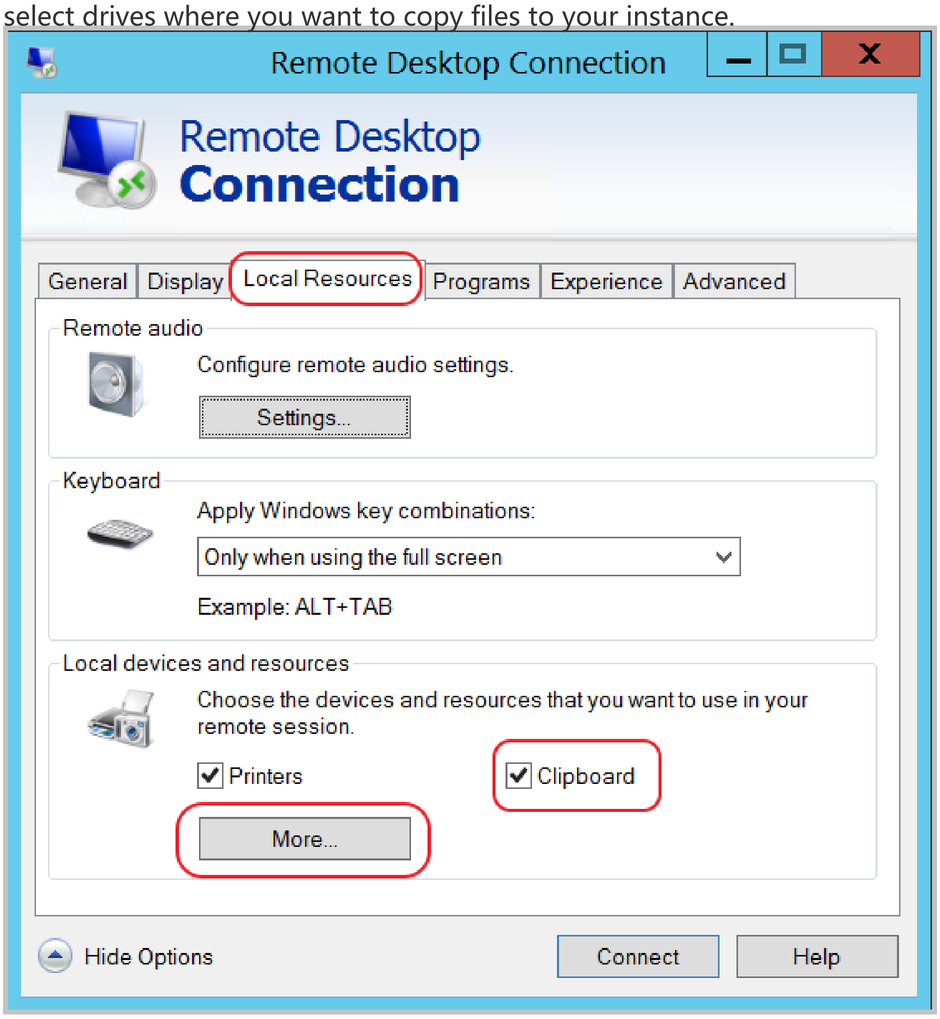
☑ Allow me to save credentials

Connection settings

Save the current connection settings to an RDP file or open a saved connection.

(Optional) If you want to copy text or files from your computer to the instance, click the **Local Resources** tab to see options for sharing local computer resources.

- If you need to copy text only, check **Clipboard**.
- If you need to copy files from your computer as well, click **More** > **Drives**, and select drives where you want to copy files to your instance.



Remote audio

Configure remote audio settings.

Keyboard

Apply Windows key combinations:

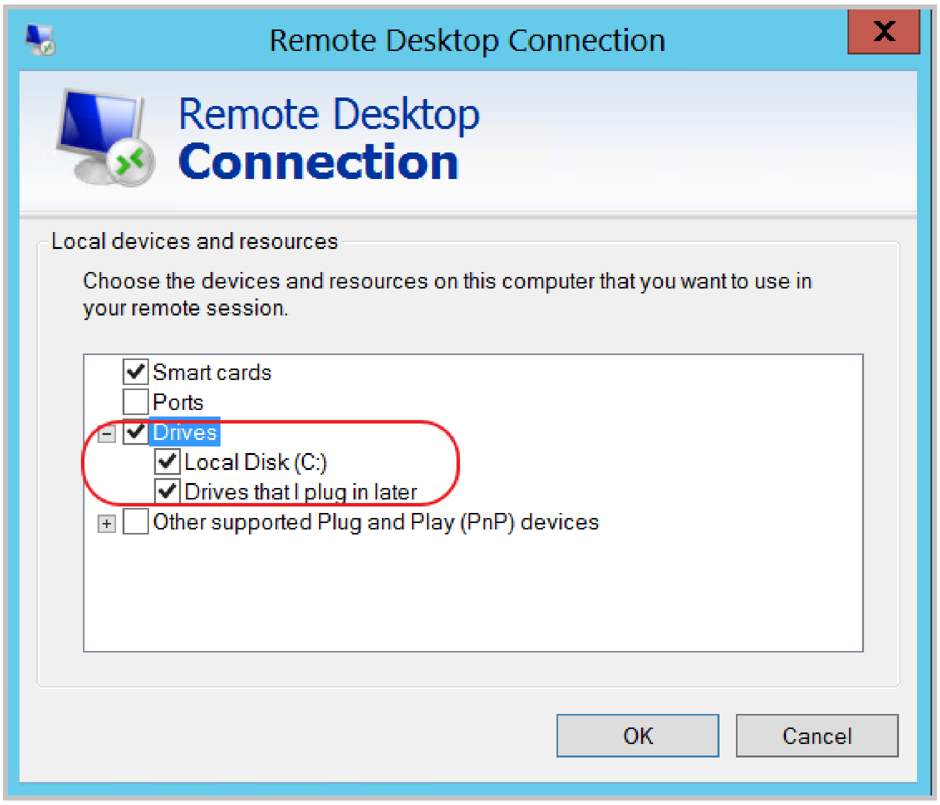
Only when using the full screen

Example: ALT+TAB

Local devices and resources

Choose the devices and resources that you want to use in your remote session.

☑ Printers ☑ Clipboard



Remote Desktop Connection

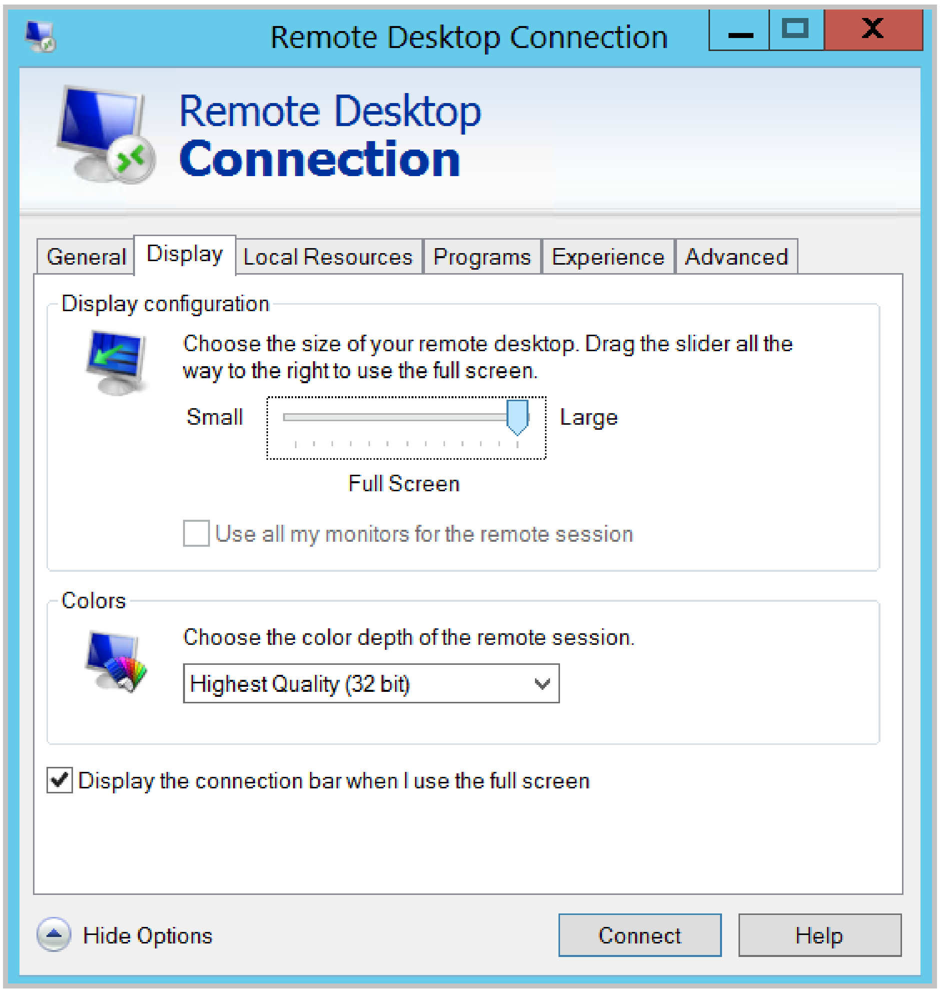
Remote Desktop Connection

Local devices and resources

Choose the devices and resources on this computer that you want to use in your remote session.

- ☑ Smart cards
- □ Ports
- ☑ Drives
  - ☑ Local Disk (C:)
  - ☑ Drives that I plug in later
- □ Other supported Plug and Play (PnP) devices

(Optional) Open the **Display** tab to resize the remote desktop window. **Full Screen** is recommended.



Remote Desktop Connection

Remote Desktop Connection

Display configuration

Choose the size of your remote desktop. Drag the slider all the way to the right to use the full screen.

Small Large

Full Screen

□ Use all my monitors for the remote session

Colors

Choose the color depth of the remote session.

Highest Quality (32 bit)

☑ Display the connection bar when I use the full screen

Click the **Connect** button to complete connection to the instance.

When you connect your computer to the Windows instance successfully, you can operate the instance from your computer.

Use Management Terminal (VNC) to connect to an ECS instance

Refer to Use Management Terminal (VNC) to connect to an ECS instance.

Connect to a Windows instance on a Linux OS

If you are connecting to a Windows Instance on a Linux OS, you can use either remote access software or the Management Terminal.

If no bandwidth has been purchased, you must log on to the Alibaba Cloud Console and use the Management Terminal to connect to the instance.

Use a remote connection application

This section uses the rdesktop application as an example. rdesktop can be downloaded at http://www.rdesktop.org/. To connect to a Windows instance using rdesktop, perform the following:

1. Start rdesktop.
2. Enter the following command (using your parameters):

```
rdesktop -u administrator -p password -f -g 1024*720 192.168.1.1 -r clipboard:PRIMARYCLIPBOARD -r
disk:sunray=/home/yz16184
```

The following table defines the parameters used in the rdesktop command.

Parameter	Description
-u	Indicates username. For a Windows instance, the default username is Administrator.
-p	Indicates the Windows instance login password.
-f	Indicates full screen is the default view. Use the key combination Ctrl+Alt+Enter to exit full screen mode.
-g	Indicates the resolution. If the connector "*" is omitted, the default resolution will be the native resolution in full screen.
IPADDRESS	Enter the IP address of your Windows instance
-d	Indicates the domain name. For example, INC domains will use –d INC.
-r	Indicates a multimedia redirection. For example: To enable sound, use -r sound. To use the local sound card, use -r sound : local. To enable a Udisk, use -r disk:usb=/mnt/usbdevice
-r clipboard:PRIMARYCLIPBOARD	This parameter can be used to directly copy and paste text between the local Linux system and the remote Windows instance. Chinese characters are also supported.
-r disk:sunray=/home/yz16184	This indicates that a directory on the local Linux system is mapped onto the Windows hard disk. This allows you to transfer files without relying on Samba or FTP.

Use the Management Terminal (VNC) to connect to an ECS instance

The operation procedure is the same as that from a local Windows OS.

Connect to a Windows instance using Mac OS X

Download and install the remote desktop client for Mac OS X at https://itunes.apple.com/us/app/microsoft-remote-desktop/id715768417.

Follow the in-app directions to complete login.

Connect to a Windows instance using a mobile app

Download and install **Microsoft Remote Desktop** from the iTunes App Store. Follow the in-app directions to complete login.

What if I forget my logon password?

If you forget your instance logon password (not the VNC connection password), see Reset the password.

Instances

Create an instance

Create an instance

You can create instances running Linux, Windows, or a custom system image. Detailed information for each is provided as follows:

- To create a Windows instance, see Quick Start for Windows.
- To create a Linux instance, see Quick Start for Linux.
- If you wish to clone the operating system, installed applications, and data of an existing instance, see Create an instance using a custom image.

Create an instance using a custom image

When creating instances using images, it is recommended that images with 32-bit or 64-bit versions of Linux or Windows be used. When purchasing an instance, you can select a custom, public, or shared image. Details of image types are as follows:

- Custom images are manually created images. They can be queried and managed through the custom image page found in the management console. See Create a custom image.
- Public images are official images provided by Alibaba Cloud.
- Shared images are custom images provided by another user account.

Note:
Only images of the current region can be used. Cross-regional use of images is not supported, but images can be copied to another region. For details, see Copy an image.

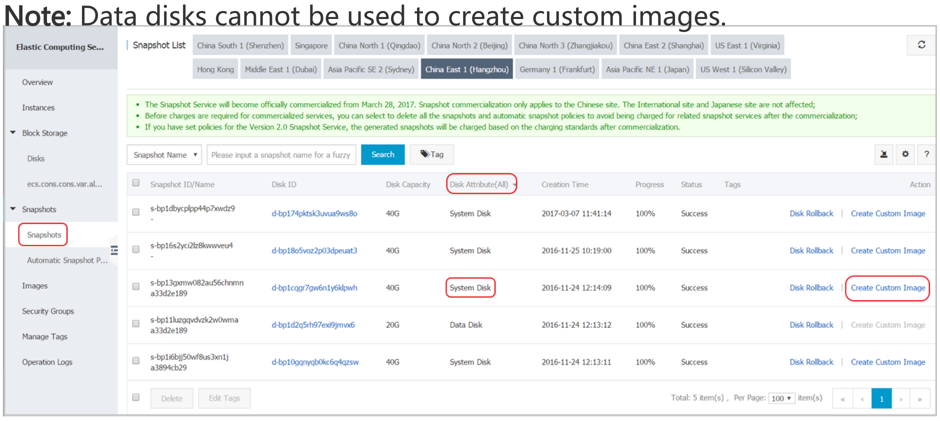
Operating procedure

Log on to the ECS Management Console.

Click **Snapshots** > **Snapshots**.

Select your preferred region.

Select a snapshot with the disk attribute as the **System Disk**. Click **Create Custom Image**.
Note: Data disks cannot be used to create custom images.



- The Snapshot Service will become officially commercialized from March 28, 2017. Snapshot commercialization only applies to the Chinese site. The International site and Japanese site are not affected;
- Before charges are required for commercialized services, you can select to delete all the snapshots and automatic snapshot policies to avoid being charged for related snapshot services after the commercialization;
- If you have set policies for the Version 2.0 Snapshot Service, the generated snapshots will be charged based on the charging standards after commercialization.

□	Snapshot ID/Name	Disk ID	Disk Capacity	Disk Attribute(All)	Creation Time	Progress	Status	Tags	Action
□	s-bp1dbycplpp44p7xwdz9 -	d-bp174pktsk3uvua9ws8o	40G	System Disk	2017-03-07 11:41:14	100%	Success		Disk Rollback | Create Custom Image
□	s-bp16s2yci2lz8kwwveu4 -	d-bp18o5voz2p03dpeuat3	40G	System Disk	2016-11-25 10:19:00	100%	Success		Disk Rollback | Create Custom Image
□	s-bp13gxmw082au56chnmn a33d2e189	d-bp1cqgr7gw6n1y6klpwh	40G	System Disk	2016-11-24 12:14:09	100%	Success		Disk Rollback | Create Custom Image
□	s-bp11luzgqvdvzk2w0wma a33d2e189	d-bp1d2q5rh97exi9jmvx6	20G	Data Disk	2016-11-24 12:13:12	100%	Success		Disk Rollback | Create Custom Image
□	s-bp1i6bjj50wf8us3xn1j a3894cb29	d-bp10gqnyqb0kc6q4qzsw	40G	System Disk	2016-11-24 12:13:11	100%	Success		Disk Rollback | Create Custom Image

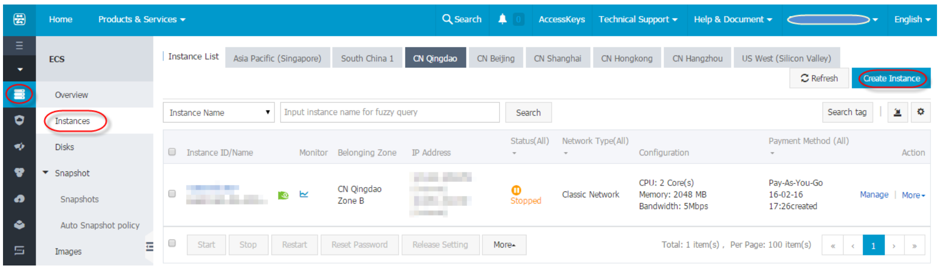
The snapshot ID will now be shown in displayed dialog box. Enter a name and description for the custom image.

(Optional) Data snapshot can be added to the image at this time.

Click **Create**.

Click **Instances** in the left-side menu.

In the top-right corner of the page, click **Create Instance**.



Instance ID/Name	Monitor	Belonging Zone	IP Address	Status(All)	Network Type(All)	Configuration	Payment Method (All)	Action
[redacted]		CN Qingdao Zone B	[redacted]	Stopped	Classic Network	CPU: 2 Core(s) Memory: 2048 MB Bandwidth: 5Mbps	Pay-As-You-Go 16-02-16 17:26created	Manage | More

Select desired payment method, region, network type, instance, network bandwidth, and other parameters. For details, see the instance creation process in the Quick Start for Linux and Quick Start for Windows.

Select an image.
Note: If the selected custom image contains more than one data disk snapshot, a corresponding number of data disks will be automatically created. By default, the size of each disk will be identical to that of the source snapshot. The size of each disk can be increased but not decreased.

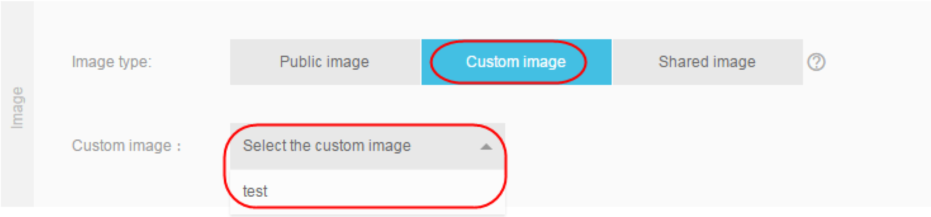


Image type: Custom image

Custom image : Select the custom image
test

Configure additional parameters based on requirements.

Click **Buy Now** to complete this process.

Change the operating system

Use the management console to convert the instance OS to your preferred OS. For details, see

Change system disk to your custom image or Change the system disk to a public image.

Note: Hong Kong, Singapore, US, Dubai, Sydney, Germany, and Japan do not currently support transition between Linux and Windows OSs. If your instance is hosted in one of these regions, you are not allowed to change the operating system between Windows and Linux. You can only change the version of Windows OS, or replace one Linux OS with another Linux OS.

Reset the instance password

- For Linux instances, the default username is **root**.
- For Windows instances, the default username is **Administrator**.

To reset the instance password, perform the following:

Log on to the ECS Management Console.

Click **Instances** in the left navigation bar.

Select your preferred region.

Select your desired instance. You may select multiple instances with identical operating statuses.

Click **More** > **Reset Password**.

Enter a new password in the displayed dialog box. Click **Submit**.

Click **OK**.

Select the instance on which the password was changed and click **Restart**.
Note: The new password will only take effect after the instance is restarted through the console. Restarting directly within the instance will not apply the new password.

Click **OK** in the displayed dialog box to restart the instance.

Start, view, or stop an instance

This section describes how to start, view, and stop an instance.

Start an instance

Note: Only instances in **Stopped** status can be started.

To start an instance, perform the following:

1. Log on to the ECS Management Console.
2. Click **Instances** in the left navigation bar.
3. Select your preferred region.
4. Select the desired instance. You can select multiple instances, as long as they are all in **Stopped** status.
5. Click **Start** at the bottom of the page.

View an instance

Use the console to view the following instance information:

- Quantity and operating statuses of instances in each region.
- Basic configuration, payment, and monitoring information.
- Disks.
- Snapshots.
- Related security groups.

To view instances, perform the following:

1. Log on to the ECS Management Console.
2. On the overview page, you can view the operating statuses of ECS instances in all regions.
3. Click **Instances** in the left navigation bar.
4. Select your preferred region, and click the name of the instance you want to view. **(Optional)** You can also search for the name of the instance you want to view.

You can then view instance details, including its:

- Region.
- Zone.
- Configuration specification.
- Payment status.
- CPU.
- Network usage.

Note: You can also view and manage the instance’ s disks, snapshots, and security group information.

Stop an instance

On the console, you can stop an instance in a similar manner to an actual server.

Note:

- Stopping an instance may disrupt your business traffic. Proceed with caution.
- Only instances in **Running** status can be stopped.

To stop an instance, perform the following:

1. Log on to the ECS Management Console.
2. Click **Instances** in the left navigation bar.
3. Select your preferred region.
4. Select the desired instance. You can select multiple instances, as long as they are all in **Running** status.
5. Click **Stop**.
6. Select **Stop** in the displayed dialog box. Click **OK**.

Restart an instance

Instances can be restarted from within or through the management console.

Note: Restarting an instance may disrupt your business traffic. Proceed with caution.

Only instances in **Running** status can be restarted.

To restart an instance, perform the following:

Log on to the ECS Management Console.

Click **Instances** in the left side navigation bar.

Select your desired region.

Select the desired instance. You can select multiple instances, as long as they are all in **Running** status.

Click **Restart**.

In the displayed dialog box, click **Restart**, and then click **OK**.

Release an instance and disable auto release

(for Pay-As-You-Go instances)

Release an instance

If you no longer require a Pay-As-You-Go instance, it is recommended that you release it immediately. Charges will continue when the instance is stopped but not released.

Release instances by performing either of the following:

- **Release Now:** Immediately releases the Pay-As-You-Go instance.
- **Timed Release:** Arranges a release plan for your Pay-As-You-Go instances by defining future release times. These times are definable to the hour. Applying new time settings will overwrite previous ones.

Note: Instances can be released every half hour or every hour, however, the system will stop billing according to your specified release time.

To perform either release type, perform the following:

Log on to the ECS Management Console.

Click **Instances** in the left navigation bar.

Select your desired region.

Select the instance to be released, and then click **Release Setting**.

In the displayed dialog box, select your preferred release action.
Note: If you select **Timed Release**, first specify whether it is to be auto released, and then specify the release date and time.

Click **Next** > **OK**.

Disable auto release

If wish to cancel the automatic release of Pay-As-You-Go instances, you can disable the set auto release function as follows:

Log on to the ECS Management Console.

Click **Instances** in the left navigation bar.

Select your desired region.

Select the required instance. .

Select **More** > **Release Setting**.

In the displayed dialog box, select **Timed Release**.

Disable the **Auto-release Setting** option.

Click **Next** > **OK**.

Add an instance to a security group

You can add an instance to a security group using the ECS Management Console. One ECS instance can be added to up to five security groups. After adding the instance to a security group, the security group rules will automatically be applied to the instance.

To add an instance to a security group, perform the following:

Log on to the ECS Management Console.

Click **Instances** in the left navigation bar.

Select your desired region.

Select the desired instance. Click the instance name or corresponding **Manage** button.

Click **Security Groups** in the left navigation bar.

Click **Add Security Group**. In the displayed dialog box, select the appropriate security group.

Click **OK**.

Remove an instance from a security group

You can remove instances from security groups. Note that an instance must be in at least two security group for this action to be performed, and you have done enough test before this operation to avoid any intranet communication error between instances.

To remove an instance from a security group, perform the following:

Log on to the ECS Management Console.

Click **Instances** in the left navigation bar.

Select your desired region.

Select the desired instance. Click the instance name or corresponding **Manage** button.

Click **Security Groups** in the left navigation bar.

Select the security group to remove from and click **Remove**.

Click **OK**.

User Data and Instance Meta Data

Disks

Create a cloud disk

Cloud disks, also known as data disks, can be purchased from the ECS Management Console. Each user account can own up to 250 cloud disks simultaneously. Up to four data disks can be attached to any single ECS instance, with a maximum capacity of 32768 GB per data disk.

To purchase a cloud disk, perform the following:

Log on to the ECS Management Console.

Click **Disks** in the left navigation bar.

Select your desired region, then click **Create Cloud Disk** in the top-right corner of the page.

Select a region and zone.
Note: A cloud disk can be attached to only a server in the same zone of the same region. Cloud disks do not support cross-regional functionality.

Select the cloud disk type, size, and quantity. Click **Buy Now** on the right side of the page.

Next step for Linux

For Linux instances, cloud disks must be attached, partitioned, and formatted before they can be displayed and used in the system.

- For details on attaching a data disk, see Attach a data disk.
- For details on formatting partitions and mounting new partitions to an attached data disk, see Format and mount a data disk.

Next step for Windows

For Windows instances, you must attach and format a cloud disk before using it.

- For details on attaching a data disk, see Attach a data disk.
- For details on formatting an attached data disk, see Format a data disk.

Create a cloud disk from a snapshot

If you need to access data from a snapshot, but do not want to roll back your disk to the snapshot, you can create a cloud disk from the snapshot and access the data from the disk.

For example, if you cannot start your instance because of a system disk failure, you can take a snapshot of the system disk, and use it to create a cloud disk. Then, you can copy and analyze its data.

To create a cloud disk from a snapshot, perform the following:

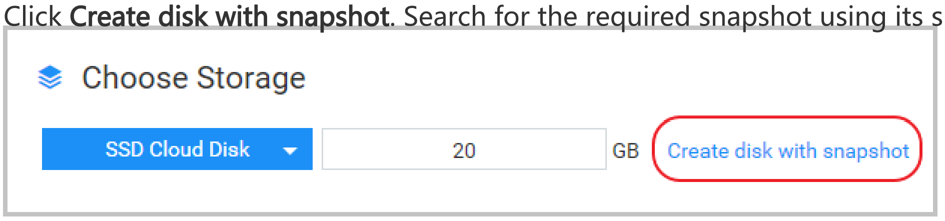
Log on to the ECS Management Console.

Click **Disks** in the left navigation bar.

Click **Create Cloud Disk** in the top-right corner of the page.

Select a region and zone.
Note: A cloud disk can be attached to only a server in the same zone of the same region. Cloud disks do not support cross-regional functionality.

Click **Create disk with snapshot**. Search for the required snapshot using its snapshot ID.



Confirm the order. The created disk will be displayed in the disk list.

Click **Attach Disk**. Enter the instance ID to which the disk is to be attached. Select the device name. You can now log on to the instance to view the disk data.
Note:

- For Windows instances, the disk will be displayed after login.
- For Linux instances, the disk must be mounted to be displayed.

Attach a data disk

The following disk types can be attached:

- Basic Cloud Disks
- Ultra Cloud Disks
- SSD Cloud Disks that serve as data disks.

Before attaching a cloud disk, an instance must meet the following requirements:

- The instance is in **Stopped** status.
- The security control marker is not Locked.
- The instance is not in payment arrears.

To attach a cloud disk, the following conditions must be adhered to:

- The cloud disk must be in available status.
- A single instance can have one system and up to four data disks attached. This includes disks of all types.
- A cloud disk can be attached to an instance of the same zone only.
- A cloud disk can be attached to only one instance at a time. Attachment to multiple instances is not supported.
- A cloud disk can be attached to any instance of the same region and zone. Both Subscription and Pay-As-You-Go instances are supported.
- When a cloud disk is acting as the system disk of an instance, it cannot be separately attached.

You can attach a disk through either of the following:

Instances Menu
Recommended if you require multiple disks to a single instance.

Disks Menu
Recommended if you require disks be attached to different instances.

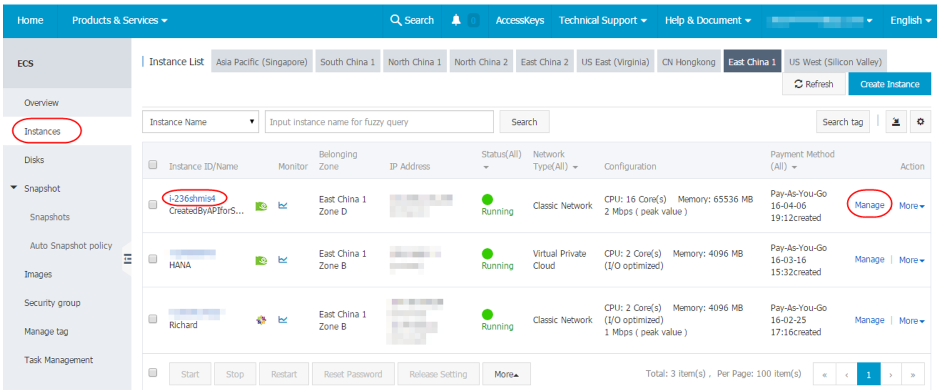
From the Instances menu

Log on to the ECS Management Console.

Click **Instances** in the left navigation bar.

Select your desired region.

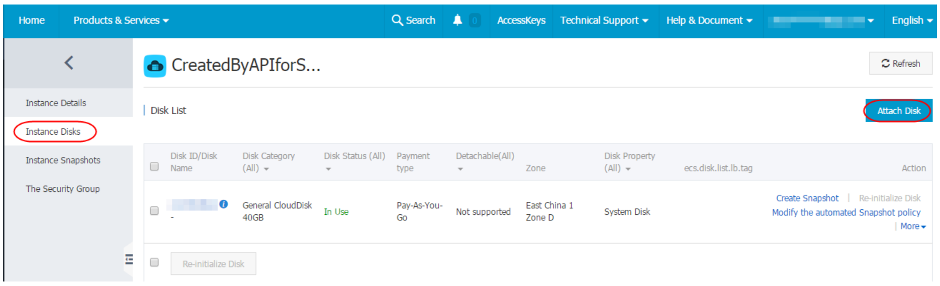
Click the name of the instance for attachment or click **Manage**.



Instance ID/Name	Monitor	Belonging Zone	IP Address	Status(All)	Network Type(All)	Configuration	Payment Method (All)	Action
i-236shmis4 CreatedByAPIforS...		East China 1 Zone D	[redacted]	Running	Classic Network	CPU: 16 Core(s) Memory: 65536 MB 2 Mbps (peak value)	Pay-As-You-Go 16-04-06 19:12created	Manage More
[redacted] HANA		East China 1 Zone B	[redacted]	Running	Virtual Private Cloud	CPU: 2 Core(s) Memory: 4096 MB (I/O optimized)	Pay-As-You-Go 16-03-16 15:32created	Manage | More
[redacted] Richard		East China 1 Zone B	[redacted]	Running	Classic Network	CPU: 2 Core(s) Memory: 4096 MB (I/O optimized) 1 Mbps (peak value)	Pay-As-You-Go 16-02-25 17:16created	Manage | More

Total: 3 item(s) , Per Page: 100 item(s) « ‹ 1 › »

Click **Instance Disks** in the left navigation bar. The disks already attached to the instance is displayed.



CreatedByAPIforS...

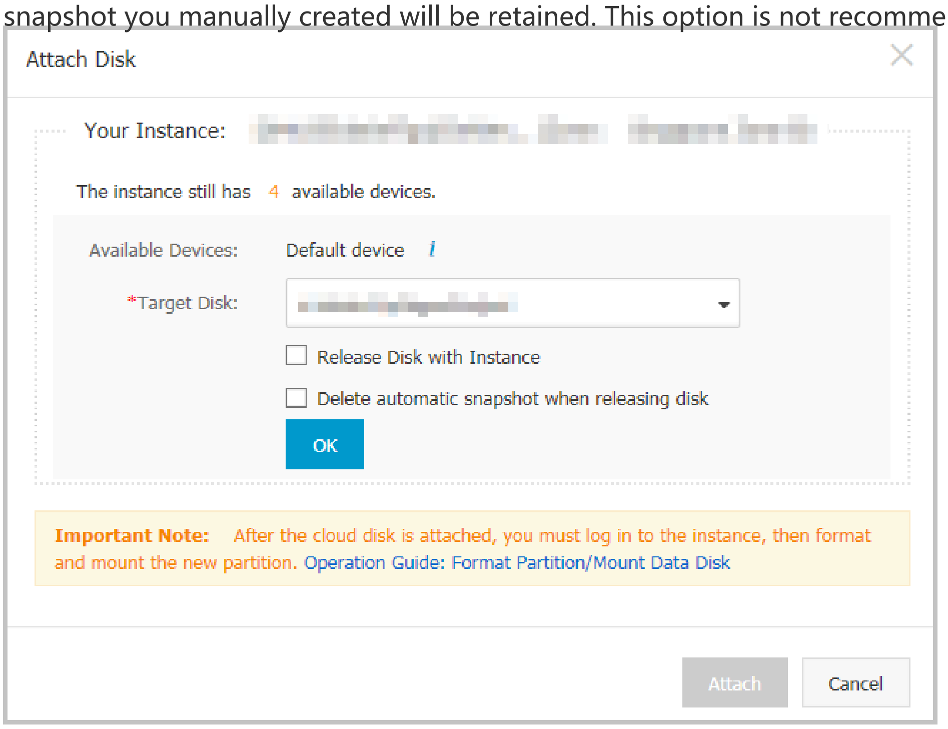
Disk List

Disk ID/Disk Name	Disk Category (All)	Disk Status (All)	Payment type	Detachable(All)	Zone	Disk Property (All)	ecs.disk.list.lb.tag	Action
[redacted] -	General CloudDisk 40GB	In Use	Pay-As-You-Go	Not supported	East China 1 Zone D	System Disk		Create Snapshot | Re-initialize Disk Modify the automated Snapshot policy | More

Click **Attach Disk** on the right side of the page. Select **Available Devices** and **Target Disk** to attach the disk.

(Optional) Set whether disks are to be released with instances and whether snapshots are to be deleted with disks.

- **Release disk with instance**
  When you release the instance, the disk will be released together.
- **Delete automatic snapshots when releasing disk**
  When you release the disk, all auto snapshots will be deleted. However, the snapshot you manually created will be retained. This option is not recommended.



Your Instance: [redacted]

The instance still has 4 available devices.

Available Devices: Default device

*Target Disk: [redacted]

□ Release Disk with Instance

□ Delete automatic snapshot when releasing disk

Important Note: After the cloud disk is attached, you must log in to the instance, then format and mount the new partition. Operation Guide: Format Partition/Mount Data Disk

After attaching a disk, you need to log on to the instance to format disk partitions and attach new partitions. For details, refer to **Next step** at the bottom of this section.

From the Disks menu

Log on to the ECS Management Console.

Click **Disks** in the left navigation bar.

Select your desired region.

Find the disk to attach. The disk status must be **Available**.

Click **More** > **Attach**. Select the target instance and release action:

- **Release disk with instance**
  When you release the instance, the disk will be released together.
- **Delete automatic snapshots when releasing disk**
  When you release the disk, all auto snapshots will be deleted. However, the snapshot you manually created will be retained. This option is not recommended.

After attaching a disk, you need to log on to the instance to format disk partitions and attach new partitions. For details, refer to **Next step** at the bottom of this section.

Next step for Linux

After attaching a disk, you must log on to the instance to format disk partitions and mount new partitions. For detailed instructions, see Format and mount a data disk.

Next step for Windows

After attaching a disk, you must log on to the instance to format disk partitions. For detailed instructions, see Format a data disk.

Detach a data disk

ECS supports the detachment of Basic Cloud Disks, Ultra Cloud Disks, and SSD Cloud Disks serving as data disks. System disks cannot be detached. Detach disks through the **Instances** or **Disks** menus.

Ensure the following based on OS:

- For Linux OSs, log on to the instance and run the umount command for the disk to be unmounted. After the command runs, navigate to the management console and detach the disk.
- For Windows OSs, stop read and write operations on all file systems of the disk to ensure data integrity. Otherwise, data being read and written will be lost.

Using the Instances menu

Log on to the ECS Management Console.

Click **Instances** in the left navigation bar.

Select your desired region.

Click the name of the instance to be detached or click **Manage**.

Click **Instance Disks** in the left navigation bar. The disks already attached to the instance is displayed.

Select the disk to be detached.

Click **Detach** in the top-right corner of the page.

In the displayed dialog box, click **Confirm Detaching**.

Using the Disks menu

Log on to the ECS Management Console.

Click **Disks** in the left navigation bar.

Select your desired region.

Click the name of the disk to be detached. The disk status must be **In Use**.

Click **Detach** in the top-right corner of the page.

In the displayed dialog box, click **Confirm Detaching**.

Change the system disk - change your instance OS to a custom image

By changing the system disk, you can change the operating system to your custom image. For instructions about how to change the OS to a public image, refer to Change the system disk (public image).

Changing the system disk will not change your instance IP address.

Note: Regions that are not in mainland China do not support replacement between Linux and Windows. A Linux or Windows can be only replaced by a different version of the same operating system type.

Warning:

- Stopping an instance may disrupt traffic.
- Redeploying the runtime environment on the new system disk is required once it is stopped and this may disrupt traffic.
- Automatic snapshots and data from your original system disk will be lost once the system disk is replaced. Ensure that all necessary data has been backed up in advance. If you want to retain auto snapshots, see disable releasing auto snapshots with disk.
- Manually created snapshots from the original system disk are retained but cannot be used to roll back the new system disk because the disk ID is changed. You can use the retained snapshots to create custom images.
- The original system disk will be deleted once the system disk is replaced.
- Ensure that the system disk has at least 1 GB of free space. Otherwise, the instance may fail to start after you change the system disk.

Procedure of changing the system disk

A complete procedure of changing the system disk includes the following steps:

- Step 1. Back up the current system disk by creating a snapshot.
- Step 2. Create an image from the snapshot.
- Step 3. Change the system disk and selecting a new OS.
- Step 4. Set auto snapshot policies for the new system disk.

To retain enough snapshot quota for the auto snapshot policy of the new disk, please delete unwanted snapshots before proceeding. If you wish to change the OS and do not need to retain the data from the current system disk, you can proceed directly to Step 3 of this section.

Step 1: Back up the current system disk by creating a snapshot

Note:

- Skip this step if you do not want to retain the data in the system disk.
- Do not create the snapshot during busy hours.
- It takes about 40 minutes to create a snapshot of 40 GB. Ensure you reserve sufficient time for it.
- Make sure the system disk has at least 1 GB free space. Otherwise, the instance may fail to start after you change the system disk.

Log on to ECS Management Console.

Click **Instances** in the left navigation bar.

Select your desired region.

Select the instance containing the system disk with the OS to be changed.

Click **Instance Disks** on the left navigation bar.

Select the system disk with the OS to be changed, and then click **Create Snapshot**.

Enter a name for the snapshot.

Click **Instance Snapshots** on the left navigation bar to check the progress and status of the snapshot.

Step 2: Create an image from the snapshot

Note:

- Skip this step if you do not want to retain the data in the system disk.
- If you do want to retain the data in the current system disk, you need to create an image to replicate the data in the system disk.
- Make sure the system disk has at least 1 GB free space. Otherwise, the instance may fail to start after you change the system disk.

Select the snapshot created in Step 1 and click **Create Custom Image**.

Enter a name and description for the image.

Return to the navigation bar, and then click **Images**.

You can now check the process and status of the new image.

Step 3: Change the system disk

To change a system disk:

Log on to the ECS Management Console.

Click **Instances** in the left navigation bar.

Select your desired region.

Stop the instance before changing the system disk. To do this, select the instance for which you wish to replace the system disk in the instance list and click **Stop**.

Once the instance is stopped, click **More** > **Change System Disk**.

Click **Custom Image** and select the image created in Step 2.

Click **Confirm Change**. Any expenditure that may have occurred will need to be paid at this time.

Step 4: Set auto snapshot policies for the new system disk

After changing the system disk, any auto snapshot policies you have set will no longer work for the new system disk, because the disk ID has changed. In this scenario, you must configure auto snapshot policies for the new system disk. For more information, see Set auto snapshot policies for disks.

Step 5: Attach data disks (for Linux instances only)

For Linux instances, you must re-attach the data disks after changing the system disk, but you do not need to partition them. For more information, see Attach a data disk.

Change the system disk to a public image

By changing the system disk, you can change the operating system to a public image, for example, from Windows Server 2003 to Windows 2012.

Note: The Hong Kong, Singapore, US, Dubai, Japan, and Germany regions do not support replacement between Linux and Windows. A Linux or Windows can be only replaced by a different version of the same operating system type.

Considerations for changing the system disk

Risks

- This operation requires you to stop your instance, which means interruption of your business. Therefore, perform this operation with caution.
- After replacement, you must redeploy the runtime environment on the new system disk. There is a possibility of a long interruption of your business. Therefore, perform this operation with caution.
- Replacing the system disk will result in the loss of the automatic snapshots and data on your original system disk. Make necessary backup in advance.

Note:

- To retain enough snapshot quota for the auto snapshot policy of the new disk, you can delete unwanted snapshots.
- Changing the system disk will not change your instance IP address.
- Manually created snapshots are retained after the replacement. However, since the disk ID is changed, you can no longer use the manually created snapshots on the original system disk to roll back the new system disk. The retained snapshots can be used to create custom images.
- After the system disk is replaced, the original system disk will be deleted.

Retain automatic snapshots

By default, the automatic snapshots will be released along with the disk. If you want to keep the automatic snapshots, see Configure releasing auto snapshots together with disk.

Procedure of changing the system disk

A complete procedure of changing the system disk includes the following steps:

1. Create a snapshot for the current system disk.
2. Change the system disk.
3. Set automatic snapshot policies for the new system disk.
4. Attach data disks (for Linux instances only).

Step 1: Create a snapshot based on the current system disk

Skip this step if you do not want to retain the data on the system disk.

Do not create the snapshot during busy hours. It takes about 40 minutes to create a snapshot of 40GB. Ensure you reserve sufficient time for it.

Note: Make sure the system disk has at least 1GB free space; otherwise, the instance may fail to start after you change the system disk.

Log on to ECS Management Console.

Click **Instances** on the left navigation bar. Then click the region.

Click the instance for which you want to change the system disk.

Click **Instance Disks** on the left navigation bar.

Find the system disk you want to change, and then click **Create Snapshot**.

Enter a name for the snapshot.

Click **Snapshots** on the left navigation bar, you can check the progress and status of the snapshot.

Step 2: Change the system disk

To change a system disk:

Log on to the ECS Management Console.

Click **Instances** on the left navigation bar. Then, select a region at the top of the page.

Stop the instance before changing the system disk. In the instance list, select the instance for system disk replacement and click **Stop** at the bottom.

After the instance is stopped, on the right end of the instance table, click **More** > **Change System Disk**.

A dialog box showing the considerations is displayed. Read the considerations carefully, and then confirm the operation.

Select a public image.

Set the password for Administrator or root.

Click **Pay Now**. Pay for the expenditure that incurred, if any.

An important message is prompted. Read it carefully. After confirming everything is correct, click **OK**.

Step 3: Configure the automatic snapshot policies

After changing the system disk, the automatic snapshot policies you have set will no longer work for the new system disk, because the disk ID has changed. In this case, you need to configure automatic snapshot policies for the new system disk. For more information, see Set automatic snapshot policies for disks.

Step 4: Attach data disks (for Linux instances only)

For Linux instances, after you have changed the system disk, you need to attach the data disks again, but you don’ t need to partition them. For more information, see Attach a data disk.

Re-initialize a disk

Disk re-initialization restores a disk to its initial state and settings.

Warning: Re-initializing a disk will erase all data on that disk. Ensure that you have backed up all necessary data before proceeding.

Note:

- The operating system and version of the instance is retained, and will be restored to its initial state and settings.
- The IP address of the instance will not change. The data on the original system disk will be cleared, but the automatic backup of snapshots on the instance will be retained, and can be used to roll back the applications on the instance.
- If you are re-initializing a data disk, you do not need to attach it after re-initialization.

Perform the following steps to re-initialize a data disk:

Log on to the ECS Management Console.

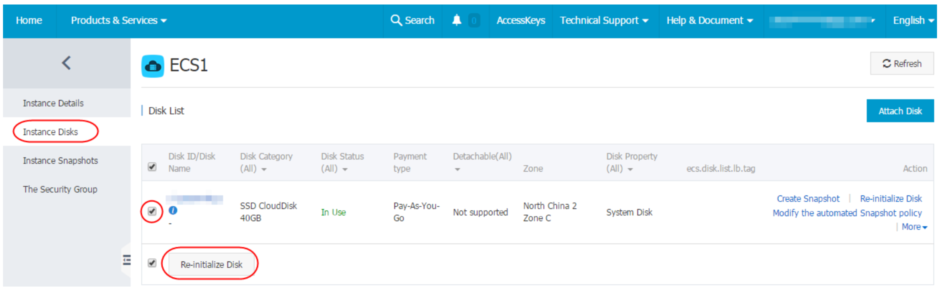
Click **Instances** in the left navigation bar.

Select your desired region.

Select the instance for disk re-initialization, and click **Stop**.

Select the instance name and then click **Instance Disks** in the left navigation bar.

Select one or more disks to re-initialize and click **Re-initialize Disk**.



☑	Disk ID/Disk Name	Disk Category (All)	Disk Status (All)	Payment type	Detachable(All)	Zone	Disk Property (All)	ecs.disk.list.lb.tag	Action
☑	[redacted] -	SSD CloudDisk 40GB	In Use	Pay-As-You-Go	Not supported	North China 2 Zone C	System Disk		Create Snapshot | Re-initialize Disk Modify the automated Snapshot policy | More

Enter a new login password once the re-initialization is finished, and then click **Confirm Re-initializing Disk**.

Roll back a disk

Disk rollback restores a disk to a state and setting from previous point in time.

Note:

- Snapshot rollback is a permanent action and cannot be reversed. Once rollback is completed, the original data cannot be restored. You are recommended to proceed with caution.
- Disk rollback can only be performed when the instance is completely stopped.

To rollback a disk, perform the following:

Log on to the ECS Management Console.

Click **Instances** in the left navigation bar.

Select your desired region.

Select the instance for disk rollback, and click **Stop**.

Click the instance name. Then, click **Snapshots** > **Snapshots** in the left navigation bar.

Select the snapshot for rollback. You can select only one snapshot at a time.

Click **Disk Rollback**.

In the displayed dialog box, click **OK**.

View monitoring information of a disk

To view the monitoring information of a disk, such as IOPS and BPS, perform the following:

Log on to the ECS Management Console.

Select a disk to view monitoring information by using one of the following methods:

- Click the instance that the disk is attached to from the instance list page and click **Instance Disks**.
- Locate the disk from the **Disks** list.

Click **Disk Monitoring** to view the monitoring information of the selected disk.

Note: You can select pre-set time segments to initiate regular monitoring periods, such as 1 hour, 6 hours, 1 day, and 7 days. You can also set custom monitoring start and end times.

Delete a data disk

Warning: Deleting a data disk is a permanent action and cannot be reversed. Once deleted, the original data on the data disk cannot be restored. You are recommended to proceed with caution.

If you no longer need a data disk, you can delete it by performing the following:

Log on to the ECS Management Console.

Click **Disks** in the left navigation bar.

Select your desired region.

Select the disk that you want to delete.
Note: If you want to keep all automatic snapshots of the disk, click **More** > **Modify Attributes**, unselect **Delete automatic snapshots when releasing disk**, and then click **OK**.

Click **More** > **Delete**.

Click **Confirm Deletion**.

Snapshots

Create a snapshot

You can create instance snapshots to save the system state from a certain point in time for data backup or to create images.

Note:

- Creation of the first snapshot will take relatively longer than subsequent snapshots due to the first snapshot being a full snapshot. However, depending on the amount of changed data since previous snapshots, the length of time for each snapshot creation may vary.
- Creating snapshots of a disk may reduce disk performance.
- It is recommended that you not create snapshots during peak traffic hours.
- Manually created snapshots, unlike automatic snapshots, will be retained until they are manually deleted.

To create a snapshot, perform the following:

Log on to the ECS Management Console.

Click **Disks** in the left navigation bar.

Select a system or data disk for which you want to create a snapshot. You can only select one disk at a time.

Click **Create Snapshot**.

Enter a name for the snapshot and click **OK**.

To view all snapshots, go to the left navigation bar and click **Snapshots** > **Snapshots**.

To view snapshots of a particular instance, navigate to **Instances**, select the particular instance, and then click **Instance Snapshots** in the left navigation bar.

Create and delete an automatic snapshot policy

An automatic snapshot policy is a set of defined parameters for automatically creating snapshots.

You can create a maximum of three automatic snapshot policies in each region.

Create an automatic snapshot policy

To create an automatic snapshot policy, perform the following:

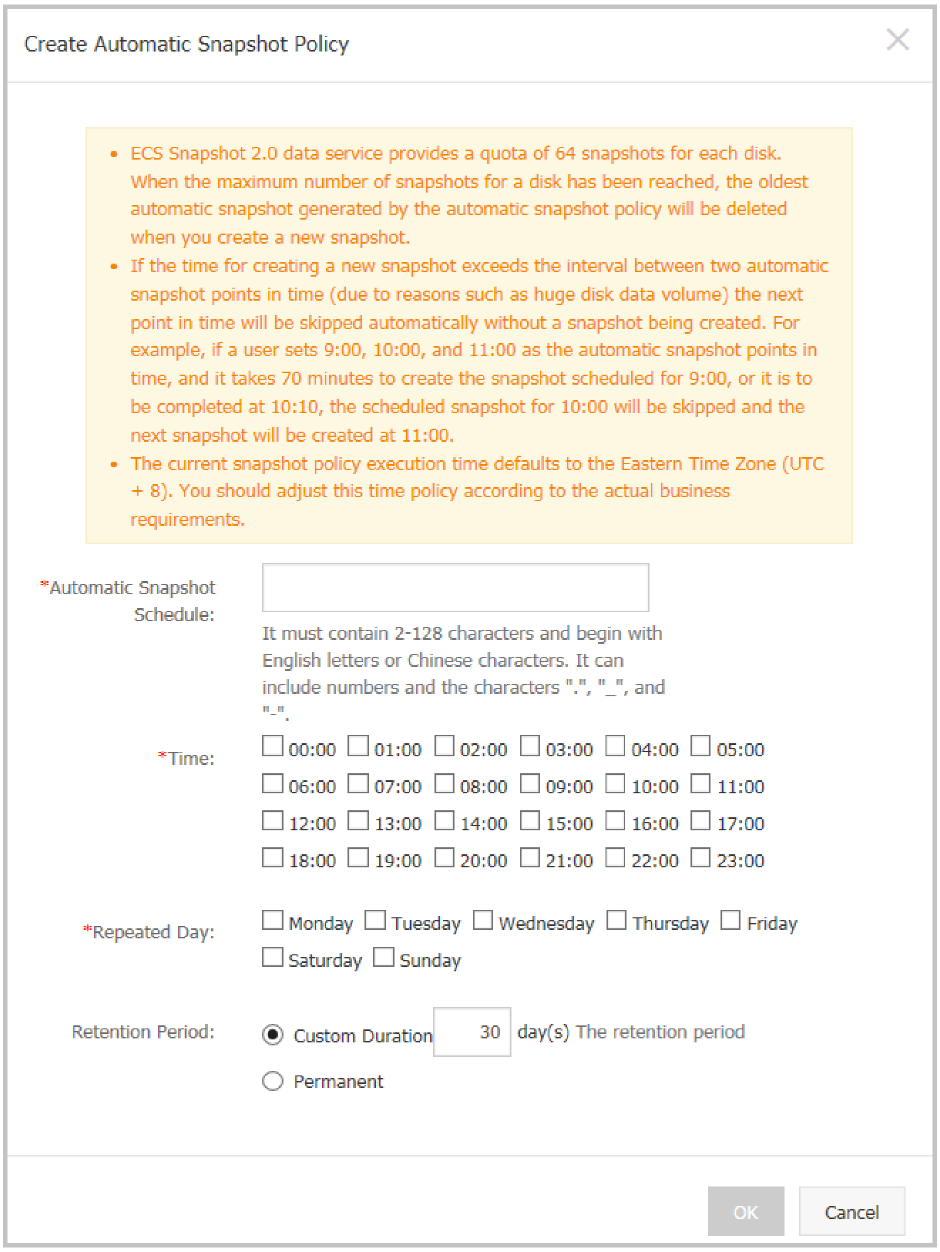
Log on to the ECS Management Console.

Click **Snapshots** > **Automatic Snapshot Policy** in the left navigation bar.

Click **Create Automatic Snapshot Policy**.

Define automatic snapshot policy parameters:

- **Automatic Snapshot Policy**
  This parameter is the name of the automatic snapshot policy. It must contain 2 ~ 128 characters and begin with English letters or Chinese characters. It can include numbers and the characters “.”, “_”, and “-”.
- **Time**
  Defines the time of day for automatically creating snapshots. There are 24 snapshot creation points available between 00:00 and 23:00.
- **Repeated day**
  There are seven available repetition day configurations.
- **Retention period**
  Defines the number of days a snapshot can be retained. This parameter can be set between 1 ~ 65536 days, or permanently. By default, it is set to 30 days.



Create Automatic Snapshot Policy

- ECS Snapshot 2.0 data service provides a quota of 64 snapshots for each disk. When the maximum number of snapshots for a disk has been reached, the oldest automatic snapshot generated by the automatic snapshot policy will be deleted when you create a new snapshot.
- If the time for creating a new snapshot exceeds the interval between two automatic snapshot points in time (due to reasons such as huge disk data volume) the next point in time will be skipped automatically without a snapshot being created. For example, if a user sets 9:00, 10:00, and 11:00 as the automatic snapshot points in time, and it takes 70 minutes to create the snapshot scheduled for 9:00, or it is to be completed at 10:10, the scheduled snapshot for 10:00 will be skipped and the next snapshot will be created at 11:00.
- The current snapshot policy execution time defaults to the Eastern Time Zone (UTC + 8). You should adjust this time policy according to the actual business requirements.

*Automatic Snapshot Schedule:

It must contain 2-128 characters and begin with English letters or Chinese characters. It can include numbers and the characters ".", "_", and "-".

*Time:
□ 00:00 □ 01:00 □ 02:00 □ 03:00 □ 04:00 □ 05:00
□ 06:00 □ 07:00 □ 08:00 □ 09:00 □ 10:00 □ 11:00
□ 12:00 □ 13:00 □ 14:00 □ 15:00 □ 16:00 □ 17:00
□ 18:00 □ 19:00 □ 20:00 □ 21:00 □ 22:00 □ 23:00

*Repeated Day:
□ Monday □ Tuesday □ Wednesday □ Thursday □ Friday
□ Saturday □ Sunday

Retention Period:
● Custom Duration 30 day(s) The retention period
○ Permanent

Click **OK**.

Delete an automatic snapshot policy

If you no longer need an automatic snapshot policy, navigate to the policy you want to delete and then click **Delete Automatic Snapshot Policy**.

Apply automatic snapshot policies to disks

You can apply an auto snapshot policy to disks according to your business needs. All the automatic snapshots are named in the format of auto_yyyyMMdd_1, for example, auto_20140418_1.

Note:

- Creating snapshots may disturb read and write operations on your disk. It is recommended that you perform auto snapshots during periods when service load is low to reduce effects on your service.
- Auto snapshot policies cannot be applied to basic cloud disks when they are not in use.
- Snapshots that are manually created do not conflict with auto snapshots. However, if you are performing an auto snapshot on a disk, you must wait for it to finish before manually creating a snapshot.

You can apply an auto snapshot policy to a disk through either of the following:

Disks menu
For applying an auto snapshot policy to a specific disk.

Snapshots menu
For applying a unified auto snapshot policy to several or all disks.

From the Disks menu

To apply an auto snapshot policy through the **Disks** menu, perform the following:

Log on to the ECS Management Console.

Click **Disks** in the left navigation bar.

Select your desired region.

Select the disk for which you want to execute the policy and click **Automatic Snapshot Policy**.

Enable the auto snapshot function and select the desired snapshot policy.

Click **OK**.

From the Disks menu

To apply or disable an auto snapshot policy through Snapshot, perform the following:

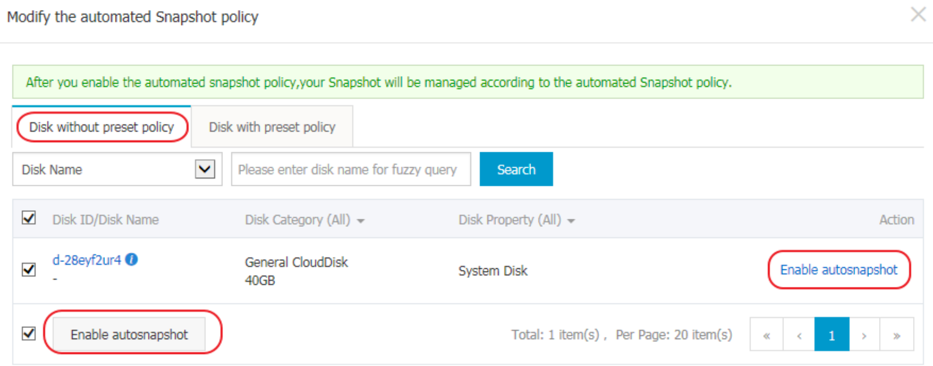
Log on to the ECS Management Console.

In the left navigation bar, click **Snapshots** > **Automatic Snapshot Policy**.

Select your desired region.

Select the auto snapshot policy you wish to apply and click **Set Disk**.

- To enable the auto snapshot policy, select the **Disk without Preset Policy** tab to view the disks. Select the disks in which you want to enable the policy, and then click **Enable the Automatic Snapshot**.



Modify the automated Snapshot policy

After you enable the automated snapshot policy,your Snapshot will be managed according to the automated Snapshot policy.

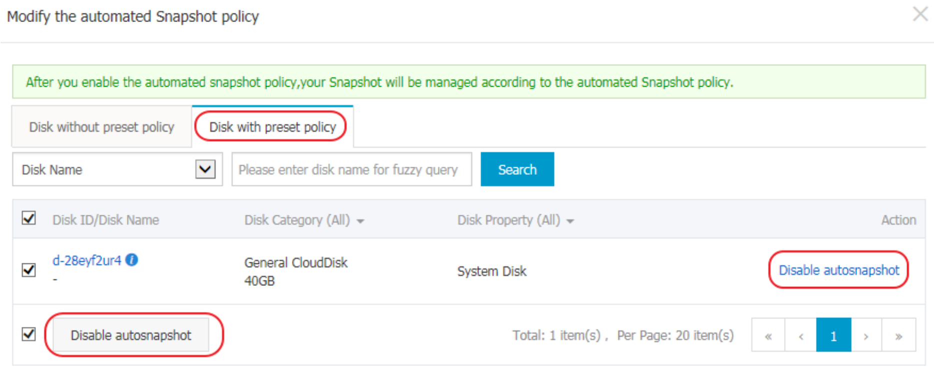
☑ Disk ID/Disk Name	Disk Category (All)	Disk Property (All)	Action
☑ d-28eyf2ur4 -	General CloudDisk 40GB	System Disk	Enable autosnapshot

☑ Enable autosnapshot

Total: 1 item(s)， Per Page: 20 item(s)

Disk without preset policy
Disk with preset policy
Disk Name
Please enter disk name for fuzzy query
Search
« ‹ 1 › »

- To disable the auto snapshot policy, select the **Disk with Preset Policy** tab to view the disks. Select the disks in which you want to disable the policy, and then click **Disable the Automatic Snapshot**.



Modify the automated Snapshot policy

After you enable the automated snapshot policy,your Snapshot will be managed according to the automated Snapshot policy.

☑ Disk ID/Disk Name	Disk Category (All)	Disk Property (All)	Action
☑ d-28eyf2ur4 -	General CloudDisk 40GB	System Disk	Disable autosnapshot

☑ Disable autosnapshot

Total: 1 item(s)， Per Page: 20 item(s)

Disk without preset policy
Disk with preset policy
Disk Name
Please enter disk name for fuzzy query
Search
« ‹ 1 › »

Retain automatic snapshots when releasing disk

To retain auto snapshots when releasing the disk, perform the following:

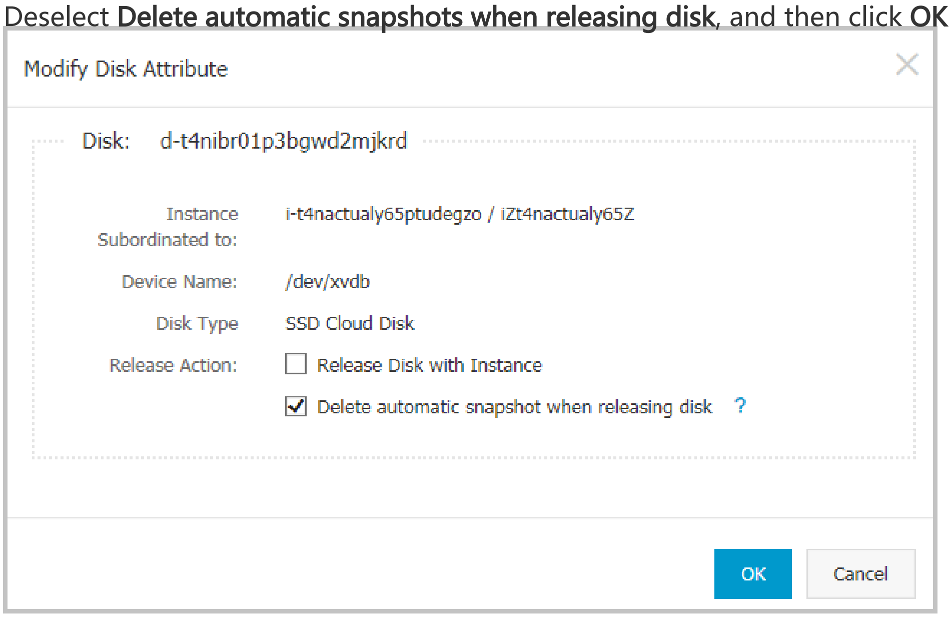
Log on to the ECS Management Console.

Click **Disks** in the left navigation bar.

Select your desired region.

Select the disk that you want to configure and click **More** > **Modify Attributes**.

Deselect **Delete automatic snapshots when releasing disk**, and then click **OK**.



Modify Disk Attribute

Disk: d-t4nibr01p3bgwd2mjkrd

Instance Subordinated to: i-t4nactualy65ptudegzo / iZt4nactualy65Z

Device Name: /dev/xvdb

Disk Type SSD Cloud Disk

Release Action: □ Release Disk with Instance

☑ Delete automatic snapshot when releasing disk ?

Delete a snapshot

When you no longer need a snapshot, or you have reached your snapshot quota, you can delete snapshots to free up space.

Note:

- Deleting a snapshot is a permanent action and cannot be reversed. Once deletion is completed, the original snapshot cannot be restored. You are recommended to proceed with caution.
- If a snapshot has been used to create a custom image, you must delete the associated image before you can delete the snapshot.

To delete a snapshot, perform the following:

Log on to the ECS Management Console.

Click **Snapshots** > **Snapshots** in the left navigation bar.

Select your desired region.

Select the snapshots you want to delete.

Click **Delete** at the bottom of the window.

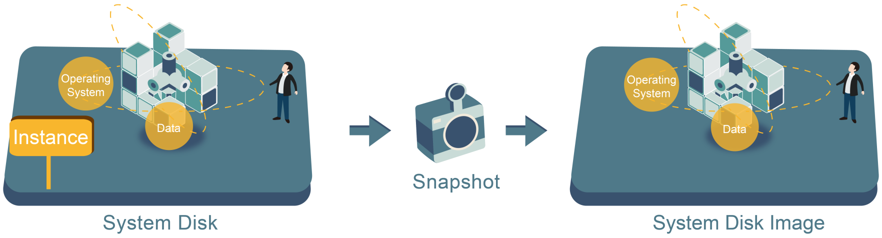
Click **OK**.

Images

Create a custom image using a snapshot

Custom images help you run ECS instances effectively by allowing you to create multiple ECS instances with identical OS and environment data to meet scaling requirements.

Custom images are based on ECS disk snapshots. You can set up identical or different configurations for ECS instances that are created from images.



Considerations

Custom images are subject to the following restrictions:

- One account can support up to 10 custom images with different data.
- If the ECS used for creating a custom image expires, or the data is erased (that is, the system disk used for the snapshot expires or is released), the custom image and the ECS instances created from the custom image will not be affected. However, auto snapshots will be cleared when an ECS instance is released.
- You can upgrade the CPU, memory, bandwidth, hard drive, and, other configurations of ECS instances activated using a custom image.

- Custom images cannot be used across regions.
- A custom image applies to any ECS payment method, either yearly/monthly subscription or Pay-As-You-Go. Custom images for ECS instances under yearly/monthly subscription plans can be used to create Pay-As-You-Go instances, and vice versa.

When creating custom images on a Linux instance, adhere to the following:

- Do not load data disk information in the /etc/fstab file. Otherwise, instances created using this image will not start.
- It is recommended that you unmount all data disks before taking a snapshot and creating an image. Otherwise, ECS instances that are created based on this custom image may not start.
- Modifying the default logon user name **root** is not allowed (Linux OS only).

Operating procedure

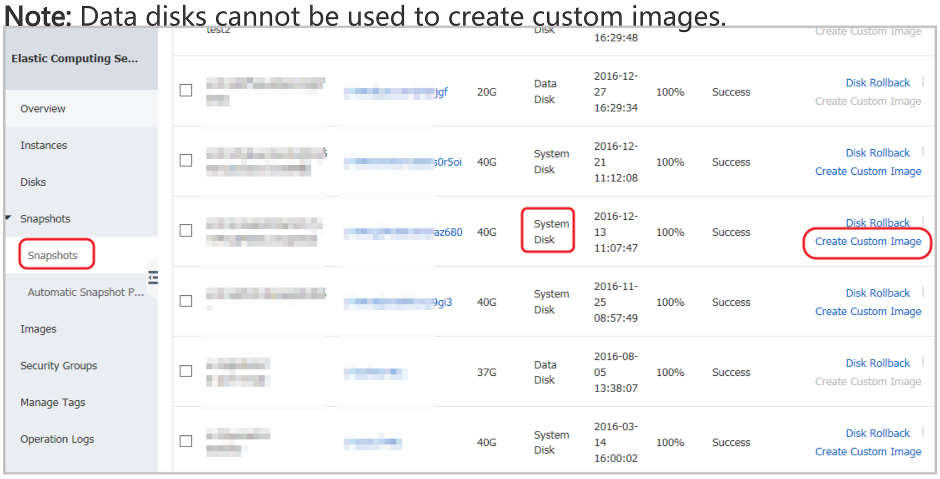
To create a custom image from a snapshot, perform the following:

Log on to the ECS Management Console.

Click **Snapshots** > **Snapshots** in the left navigation bar.

Select your desired region.

Select a snapshot with the disk attribute of **System Disk** and click **Create Custom Image**.
Note: Data disks cannot be used to create custom images.

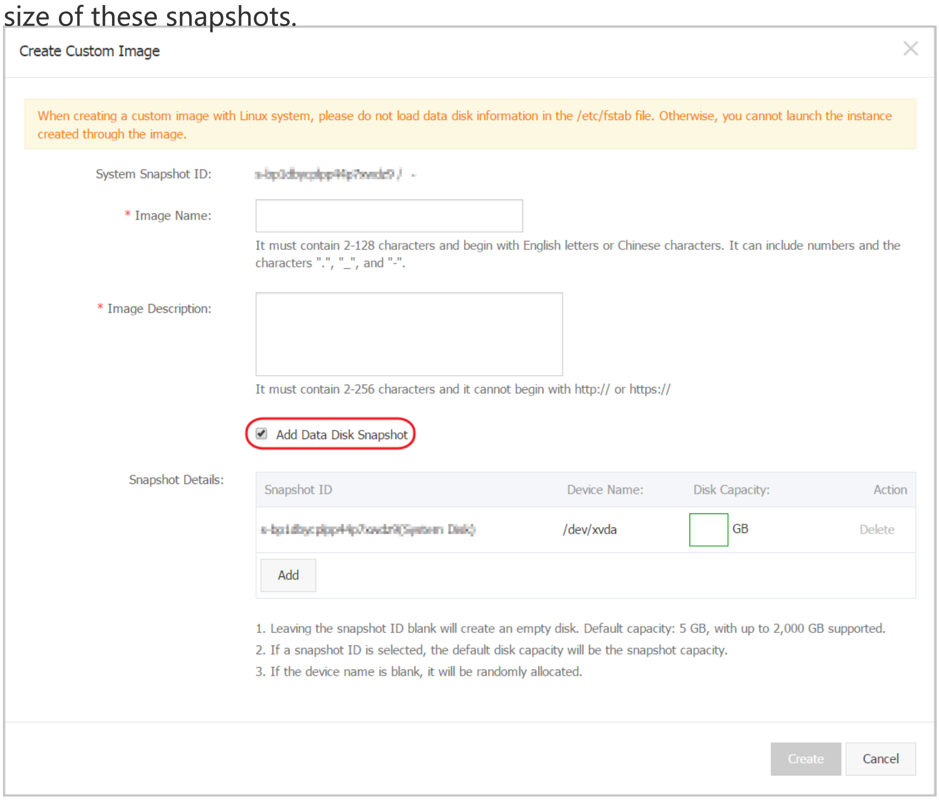


	test2			Disk	16:29:48			Create Custom Image
□	[redacted]	[redacted]jgf	20G	Data Disk	2016-12-27 16:29:34	100%	Success	Disk Rollback | Create Custom Image
□	[redacted]	[redacted]s0r5oi	40G	System Disk	2016-12-21 11:12:08	100%	Success	Disk Rollback | Create Custom Image
□	[redacted]	[redacted]az680	40G	System Disk	2016-12-13 11:07:47	100%	Success	Disk Rollback | Create Custom Image
□	[redacted]	[redacted]9gi3	40G	System Disk	2016-11-25 08:57:49	100%	Success	Disk Rollback | Create Custom Image
□	[redacted]	[redacted]	37G	Data Disk	2016-08-05 13:38:07	100%	Success	Disk Rollback | Create Custom Image
□	[redacted]	[redacted]	40G	System Disk	2016-03-14 16:00:02	100%	Success	Disk Rollback | Create Custom Image

In the displayed dialog box, you can view the snapshot ID. Enter a name and description for the custom image.

(Optional) Click **Add Data Disk Snapshot** to select multiple snapshots of data disks for the image.

Note: If the snapshot disk capacity is left blank, an empty disk will be created with the default capacity of 5 GB. If you select available snapshots, the disk size is the same as the size of these snapshots.



Create Custom Image

When creating a custom image with Linux system, please do not load data disk information in the /etc/fstab file. Otherwise, you cannot launch the instance created through the image.

System Snapshot ID: [redacted]

* Image Name:

It must contain 2-128 characters and begin with English letters or Chinese characters. It can include numbers and the characters ".", "_", and "-".

* Image Description:

It must contain 2-256 characters and it cannot begin with http:// or https://

☑ Add Data Disk Snapshot

Snapshot Details:

Snapshot ID	Device Name:	Disk Capacity:	Action
[redacted]	/dev/xvda	GB	Delete

Add

1. Leaving the snapshot ID blank will create an empty disk. Default capacity: 5 GB, with up to 2,000 GB supported.
2. If a snapshot ID is selected, the default disk capacity will be the snapshot capacity.
3. If the device name is blank, it will be randomly allocated.

Click **Create**. The custom image is successfully created.

(Optional) To view images you have created, select **Images** in the left navigation bar.

FAQ for images of Linux instances

How to unmount a disk and delete disk table data?

If **/dev/hda5** is attached to **/mnt/hda5**, run any of the following three commands to detach the file system:

```
    umount /dev/hda5
umount /mnt/hda5
umount /dev/hda5 /mnt/hda5
```

/etc/fstab is an important configuration file in Linux. It contains file system details and storage devices attached at startup.

If you do not want to mount a specified partition when starting the VM, delete the corresponding lines from **/etc/fstab**. For example, you can delete the following statement to disconnect xvdb1 at startup: /dev/xvdb1 /leejd ext4 defaults 0 0.

How to determine whether a data disk is detached and a custom image can be created?

You must ensure that the auto attach data disk statement line has been deleted from the **fstab** file.

Use the mount command to view information on all mounted devices. Ensure that the execution results do not contain the information of the data disk partition.

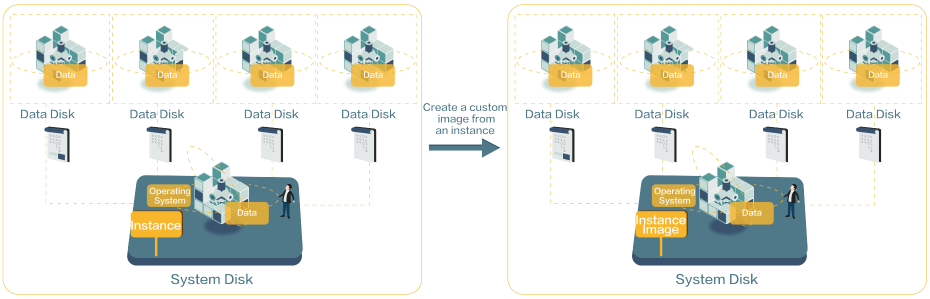
Relevant configuration files

Before creating an image, ensure the key configuration files from the following table have not been modified; otherwise, the new instance will not be able to start.

Configuration File	Purpose	Risks if changed
/etc/issue, /etc/-release, /etc/*_version	For system release and version	Modifying /etc/issue will make the system release version unidentifiable, and cause instance creation failure.
/boot/grub/menu.lst, /boot/grub/grub.conf	For system boot	Modifying /boot/grub/menu.lst will result in kernel loading failure, and the system will not be able to start.
/etc/fstab	For mounting partitions during boot.	Modifying it will cause partition mounting failure, and the system will not be able to start.
/etc/shadow	For storing system passwords.	If this file is set to read-only, the password file cannot be edited, and instance creation will fail.
/etc/selinux/config	For system security policies	Modifying /etc/selinux/config and enabling SELinux will result in start failure.

Create a custom image using an instance

You can create a custom image using an instance by selecting its disks, including the system disk and data disks, and pack them into an image. During this process, snapshots are automatically created for all disks of the instance. It is these snapshots that are then used to compose the new image.



Note:

- Before creating a custom image, ensure no confidential data is accessible on the disks being used.
- To create a custom image from snapshots, see Create a custom image from snapshots.

To create a custom image, follow these steps:

Log on to the ECS Console。

Click **Instances** on the left navigation bar.

Select your desired region.

Select the target instance, and then click **More** > **Create Custom Image**.

Enter a name and description for the image, and then click **Create**.

When all snapshots have been successfully created, the custom image will be ready for use.

Copy an image or not

Copying an image allows you to use images across regions.

Open a ticket to activate this feature. State the size of the image you want to copy.

By default, custom images cannot be used across regions. However, you can copy a custom image from one region to another. This allows you to deploy a backup image system, or an identical application environment, in another region.

Copy an image

To copy an image, perform the following:

Log on to the ECS Management Console.

Click **Images** in the left-side navigation bar.

Select your desired region.

Select the image you want to copy.
Note: The image type must be Custom Image.

Click **Copy Image**. In the displayed dialog box, you can view the image ID.

Specify the target region to which you want to copy the image.

Enter a name and description for the target image.

8. Click **OK**.

A snapshot and a custom image will be automatically created in the target region. Ensure the status of the new image is available before using it to create ECS instances.

Cancel the copying of an image

If you do not need an image currently being copied, cancel the copying operation as follows:

Log on to the ECS Management Console.

Select **Images** in the left navigation bar.

Select the target region of the image being created. The image list is displayed.

Select the image that is being created and click **Cancel Copy**.

The system will prompt you to confirm cancel image copying. Click **OK**.

Share an image, cancel sharing, and view shared images

Share an image

You can share your custom images with other users. Through the ECS Management Console or ECS Open API, you can query images shared by other accounts with your own account, and select images shared by other accounts to create ECS instances.

Note:

- Alibaba Cloud does not guarantee the integrity or security of images shared by Alibaba Cloud users. Ensure that you use only images shared by trusted accounts.
- Before using shared images to create ECS instances, log on to the ECS instances to which the shared images belong and verify that the images are secure and complete.
- Before sharing an image, ensure no confidential data is accessible on the disks to be shared.

Considerations

Restrictions

- One account can obtain a maximum of **30** shared images.
- One image can be shared with a maximum of **50** accounts.
- Shared images do not count towards your image quota.
- Shared images can only be used to create instances in the same region as the source image.
- Only image owners can share images with other accounts.

Impact of deleting shared images

- You can delete a custom image even you have shared it with other accounts. Before deleting the shared image, however, you need to unassociate it from other accounts.
- If you delete an account that has shared a custom image, the users who are using the shared image can no longer find the image through the ECS Management Console or ECS Open API, or use the image to create ECS instances.
- Deleting shared custom images may cause system disk re-initialization to fail for ECS instances created from these images.

Operating procedure

Log on to the ECS Management Console.

Click **Images** in the left-side navigation bar.

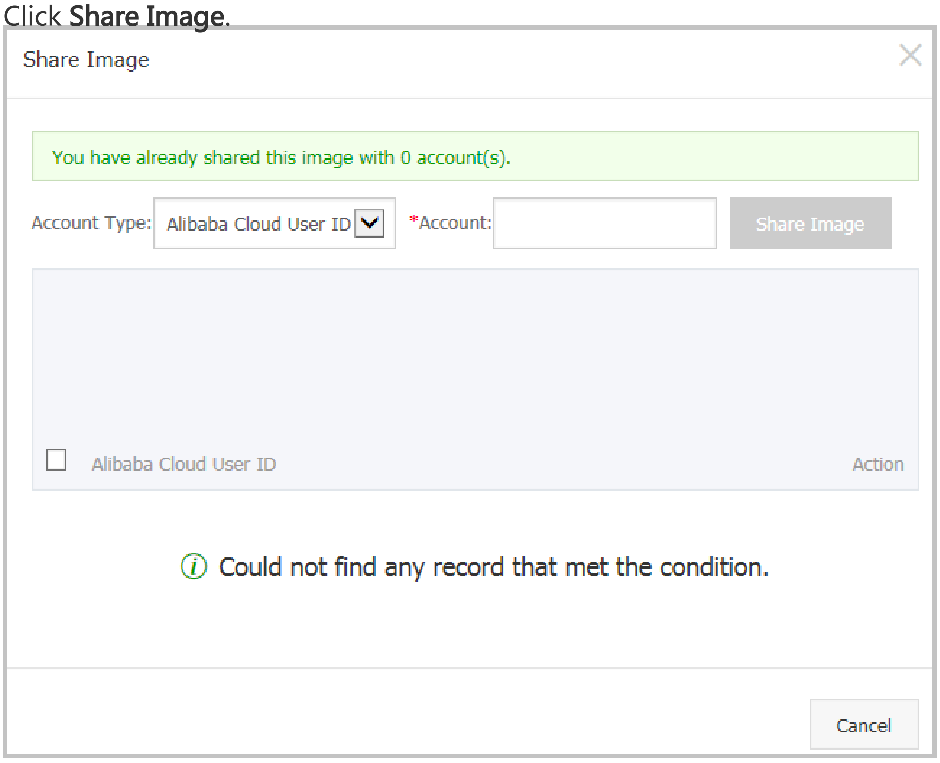
Select your desired region.

Select the image you want to share.
Note: The image type must be **Custom Image**.

Click **Share Image**.

In the displayed dialog box, select the **Account Type** and enter the Alibaba Cloud ID of the account you want to share the image with.
Note: The **Account ID** can be obtained from the **Account Management** > **Security Settings** on the Alibaba Cloud website by logging on to https://account-intl.console.aliyun.com/#/secure.

Click **Share Image**.



Share Image

You have already shared this image with 0 account(s).

Account Type: Alibaba Cloud User ID *Account:

□ Alibaba Cloud User ID Action

Could not find any record that met the condition.

View accounts using your shared images

You can view which accounts are using your shared images.

To view accounts using your shared images, perform the following:

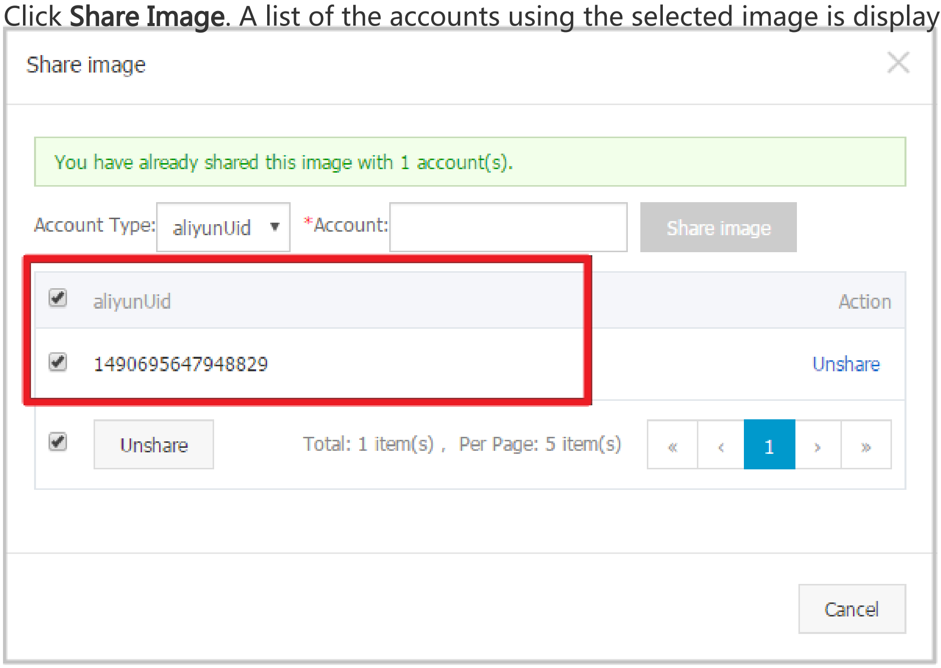
Log on to the ECS Management Console.

Click **Images** in the left-side navigation bar.

Select your desired region.

Select the image you want to check.

Click **Share Image**. A list of the accounts using the selected image is displayed.



Share image

You have already shared this image with 1 account(s).

Account Type: aliyunUid *Account:

☑ aliyunUid	Action
☑ 1490695647948829	Unshare

Total: 1 item(s) , Per Page: 5 item(s)

Cancel the sharing of an image

You can cancel the sharing of an image to specific accounts at any time.

Note: When the sharing of an image is cancelled:

- Any accounts currently using the image will no longer be able to use the image. Therefore, you must disassociate the image from other accounts before cancelling it being shared.
- Any instances using the image, including instances of other accounts using the shared image, will not be able to reinitialize the system disk.

Operating procedure

To cancel the sharing of an image, perform the following:

Log on to the ECS Management Console.

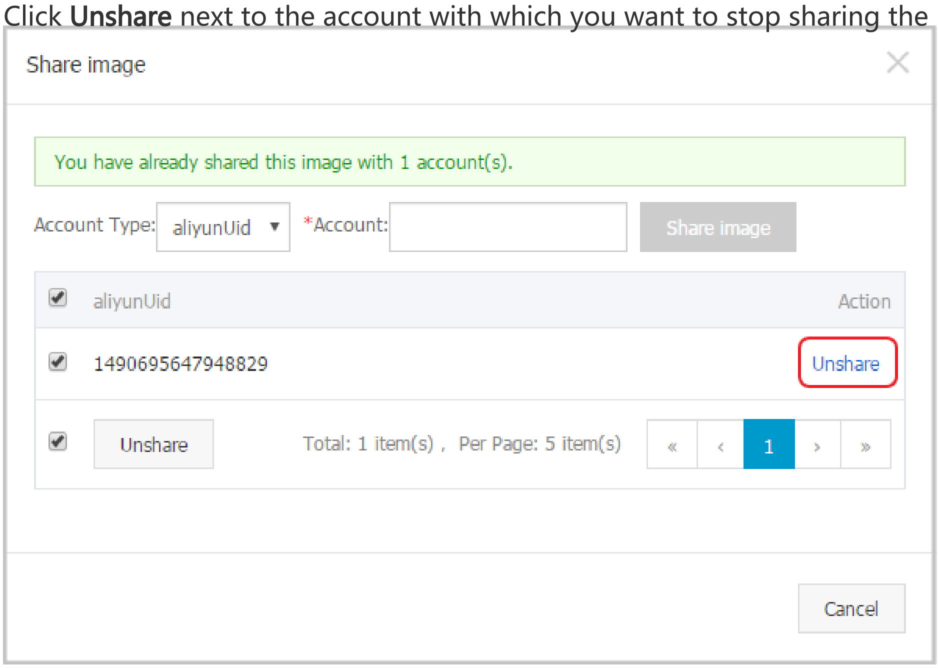
Click **Images** in the left-side navigation bar.

Select your desired region.

Select the image you want to cancel sharing.

Click **Share Image**.

Click **Unshare** next to the account with which you want to stop sharing the image.



Share image

You have already shared this image with 1 account(s).

Account Type: aliyunUid ▾ *Account:

☑	aliyunUid	Action
☑	1490695647948829	Unshare

☑ Unshare Total: 1 item(s) , Per Page: 5 item(s)

View the shared images you are using

You can view a list of the shared images from other accounts that you are using.

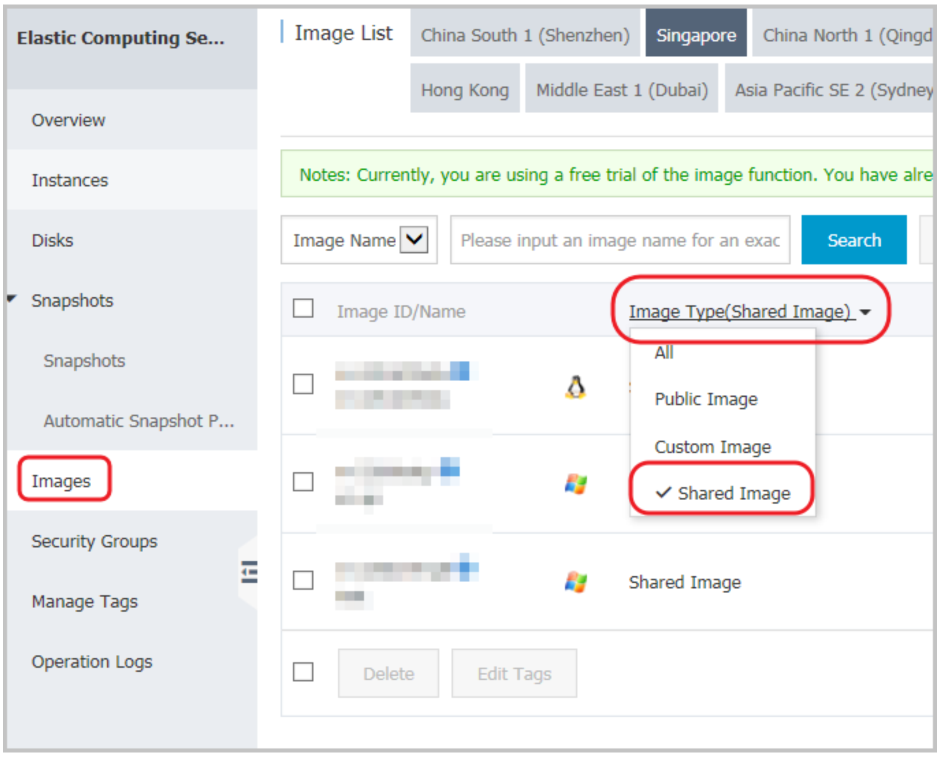
To view a list of the shared images you are using, perform the following:

Log on to the ECS Management Console.

Click **Images** in the left-side navigation bar.

Select your desired region.

In the image type dropdown, select **Shared Image** as the **Image Type**.



Notes: Currently, you are using a free trial of the image function. You have alre

A list of the shared images you are using will be displayed.

Import an image

You can import image files to the ECS environment to create custom images. You can then use these image to create ECS instances.

Note: You need to open a ticket first to apply for ECS image import permissions. Once the permission is granted, the **Import Image** button will appear.

Requirements

Supported Windows (32-bit and 64-bit) operating systems

- Microsoft Windows Server 2012 R2 (Standard Edition)
- Microsoft Windows Server 2012 (Standard Edition, Data Center Edition)
- Microsoft Windows Server 2008 R2 (Standard Edition, Data Center Edition, Enterprise Edition)
- Microsoft Windows Server 2008 (Standard Edition, Data Center Edition, Enterprise Edition)
- Microsoft Windows Server 2003 R2 (Standard Edition, Data Center Edition, Enterprise Edition)
- Microsoft Windows Server 2003 with Service Pack 1 (SP1) (Standard Edition, Data Center Edition, Enterprise Edition)

- Windows 7 Professional Edition and Enterprise Edition

Note: Windows XP, Windows 8, and Windows 10 are not supported.

Supported Linux (32-bit and 64-bit) operating systems

- Red Hat Enterprise Linux (RHEL) 5, 6, 7
- CentOS 5, 6, 7
- Ubuntu 10, 12, 13, 14
- Debian 6, 7
- OpenSUSE 13.1
- SUSE Linux 10, 11, 12
- CoreOS 681.2.0+

Supported image formats

- RAW
- Virtual hard disk (VHD)

Supported file systems

Windows (32-bit and 64-bit)
Supports NTFS format and MBR partition.

Linux/Unix (32- bit and 64-bit)
Supports ext3 and ext4 file system format and MBR partition.

Windows-specific requirements

- Recommended system disk size: 40 GB ~ 500 GB.
- Imported Windows images must provide Windows activation service.
- The firewall must be disabled. Otherwise, remote login is not possible. Port 3389 must be enabled.
- Disable user account control (UAC) to enable changes to be made to the system.

Linux-specific requirements

- Recommended system disk size: 40 GB ~ 500 GB.
- SELinux is not activated.
- The firewall is disabled; port 22 is enabled by default.
- Imported Red Hat Enterprise Linux (RHEL) images must be activated with a BYOL. You must buy your own product serial numbers and services from the manufacturer.

Restrictions

- Images can only be imported from the system disk. You cannot import images from data disks.
- Image import does not support the use of multiple network interfaces or IPv6 addresses.
- Passwords must be 8 ~ 30 characters in length and contain three types of characters (uppercase, lowercase, numbers, and special characters).
- It is recommended that you install the XEN and KVM virtualization platform drivers.

Importing images using the ECS Management Console

Prerequisites

- OSS must be activated before images can be imported.
- OSS access permissions must be manually granted to the official ECS service account before images are imported.
- Use an OSS third-party tool client, OSS API or OSS SDK, to upload the file to a bucket in the same region as the ECS custom image to import.
- Ensure images are being created in accordance with image restrictions and requirements.

Operating procedure

To import images using the management console, perform the following:

Log on to the ECS Management Console.

Click **Images** in the left-side navigation bar.

Select the image you want to import, and click **Import Image** next to that image. Ensure the image you want to import meets the preceding requirements. If you have not granted the official ECS service account access to your OSS, image import may fail.

Complete the image import form using the following information:

Region
Select the region where you want to deploy the application.

Image File OSS Address
Copy the object address taken from the OSS console.

Image Name
The length should be 2 ~ 128 characters. It can contain uppercase letters, lowercase letters or Chinese characters. It cannot contain numbers, underscores (_), or hyphens (-).

System Disk Size
Windows system disk size: 40-500 GB; Linux system disk size: 20- 500 GB.

System Architecture
64-bit OS: x86_64. 32-bit OS: i386.

Operating System Type
Currently supported OS releases are:

- Windows: Windows Server 2003, 2008, 2012, and Windows 7.
- Linux: CentOS, Red Hat, SUSE, Ubuntu, Debian, FreeBSD, and CoreOS.
  Note:
    - **(Linux only)** Open a ticket to Alibaba Cloud to confirm the selected edition is supported.
    - If your image OS is a custom edition developed on a Linux core, open a ticket to Alibaba Cloud.

Image Format
Supports RAW and VHD format. RAW format is recommended.
Note: You cannot use qemu-image to create VHD images.

Image Description
Enter a description of the image.

Click **Submit**. You can view the task progress in the image list of the import region.

Image importing takes time, usually several hours. The duration of the task depends on the size of your image file and how many other import tasks are running. You can view the task progress in the image list of the import region.

You can also find and cancel the image import task in the task manager.

Modify custom image names and description

You can modify the names and descriptions of custom images at any time.

To modify the names and descriptions of custom images, perform the following:

Log on to the ECS Management Console.

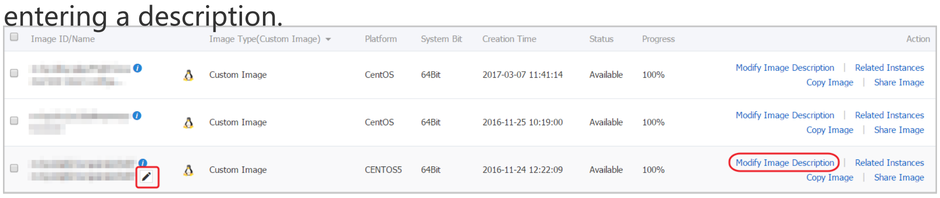
Click **Images** in the left-side navigation bar.

Select your desired region.

Select the image to edit.
Note: The image type must be **Custom Image**.

Modify the image name by hovering the cursor over the image name, and then clicking the **pen icon** that appears.

Modify the description of an image by clicking **Modify Image Description**, and then entering a description.



□	Image ID/Name	Image Type(Custom Image)	Platform	System Bit	Creation Time	Status	Progress	Action
□	[redacted]	Custom Image	CentOS	64Bit	2017-03-07 11:41:14	Available	100%	Modify Image Description Related Instances Copy Image Share Image
□	[redacted]	Custom Image	CentOS	64Bit	2016-11-25 10:19:00	Available	100%	Modify Image Description Related Instances Copy Image Share Image
□	[redacted]	Custom Image	CENTOS5	64Bit	2016-11-24 12:22:09	Available	100%	Modify Image Description Related Instances Copy Image Share Image

Click **OK**.

Delete a custom image

You can delete custom images that you no longer require. To ensure successful deletion, check that you do not currently have any ECS instances created from this custom image.

To delete a custom image, perform the following:

Log on to the ECS Management Console.

Click **Images** in the left-side navigation bar.

Select your desired region.

Select the image you want to delete.
Note: The image type must be **Custom Image**.

Click **Delete**.

In the dialog box, click **OK**.

Security groups

Usage scenarios

The following scenarios apply to **Classic Networks**. If you want to know how to use security groups together with VPC, refer to Use security groups to control ECS instances’ access to public cloud for a VPC.

Security groups provide security assurance to networks. They can be used to:

- Provide secure intranet communication.
- Block access to instances from specified IP addresses.
- Allow remote logins using only a specified IP address.
- Permit an instance to access only a specified IP address.

Scenario 1: Provide secure intranet communication

In a classic network, you can use security groups for Intranet communication between:

- ECS instances belonging to the same account in the same region.
- ECS instances belonging to different accounts in the same region.

ECS instances belonging to the same account in the same region

By setting security group rules, you can allow classic network instances belonging to the same account in the same region to communicate via intranet.

By default, ECS instances in the same security group can communicate through the intranet, but instances in different security groups cannot communicate through the intranet.

There are two ways to allow communication between ECS instances in different security groups. You can:

- Place the instances in the same security group to allow intranet communication.
- Authorize intranet communication between the two security groups by setting access-type

security group rules. In **Authorization Type**, select **Security Group Access**, and then select the security group of each other for the **Authorization Object**.

Instances belonging to different accounts in the same region

By setting security group rules, you can allow classic network ECS instances belonging to different accounts in the same region to communicate via intranet.

To achieve intranet communication between instances belonging to different accounts in the same region, each user must perform the following:

- Add the other user’ s security group to its inbound intranet.
- Authorize the ECS instances of the other user’ s security group to access all instances in the their account.

Notice: To ensure the security of your instances, when you are configuring an intranet inbound rule for a security group of classic network type, **Security Group Access** is the top priority for **Authorization Type**. If you want to select **Address Field Access**, you must enter an IP address with CIDR prefix, “/32”, in the format of a.b.c.d/32. Only IPv4 is supported.

Block access to an ECS instance from an IP address

You can use security groups to block access to an ECS instance or a port of an ECS instance from specified IP addresses.

To block access to an instance from a specific IP address, perform the following:

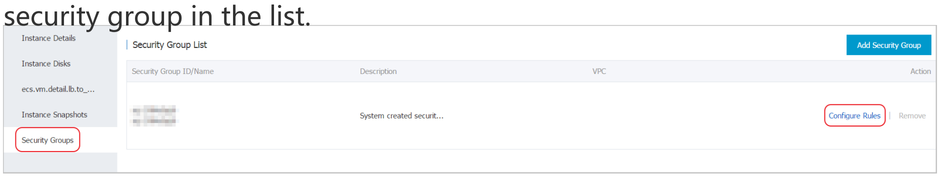
Log on to the ECS Management Console.

Click **Instances** in the left-side navigation bar.

Select your desired region.

Select your desired instance, and click **Manage**.

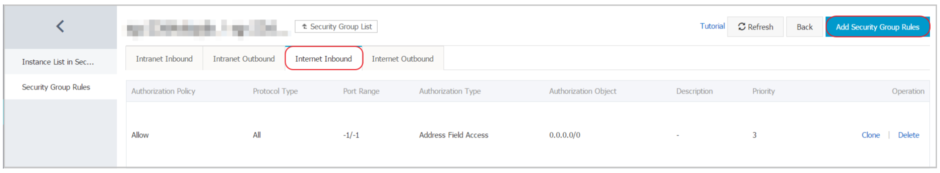
Select **Security Groups** in the left-side navigation bar, and click **Configure Rules** of one security group in the list.



Security Group List

Security Group ID/Name	Description	VPC	Action
[redacted]	System created securit...		Configure Rules | Remove

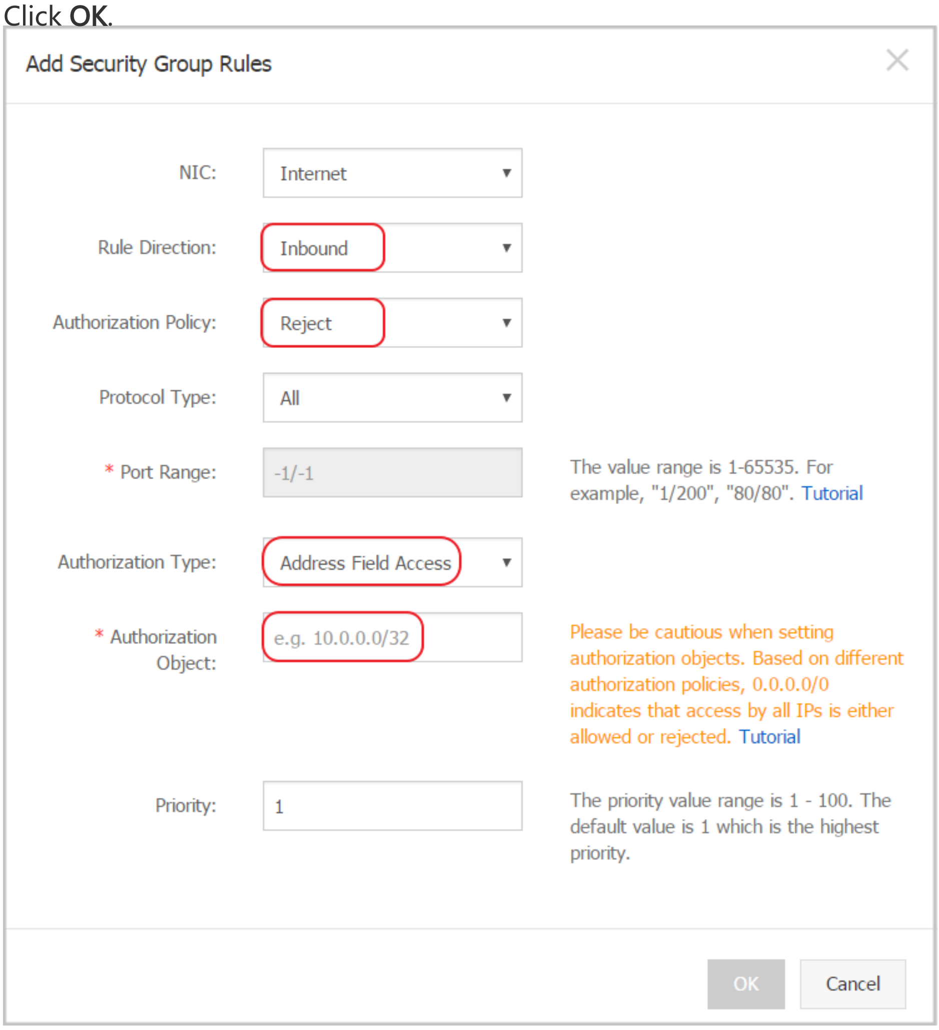
Click **Internet Inbound** and then click **Add Security Group Rules**.



Authorization Policy	Protocol Type	Port Range	Authorization Type	Authorization Object	Description	Priority	Operation
Allow	All	-1/-1	Address Field Access	0.0.0.0/0	-	3	Clone | Delete

If you want to reject access from an IP address, on the **Add Security Group Rules** dialog box:

- Select **Reject** for the **Authorization Policy**.
- Select **All** for the **Protocol Type**.
- Select **Address Field Access** for the **Authorization Type** and enter an IP address with or without a CIDR prefix, for example 1.2.3.4 or 1.2.3.4/24, as the **Authorization Object**.
- Enter **1** for **Priority**.
- Click **OK**.



NIC: Internet

Rule Direction: Inbound

Authorization Policy: Reject

Protocol Type: All

* Port Range: -1/-1 The value range is 1-65535. For example, "1/200", "80/80". Tutorial

Authorization Type: Address Field Access

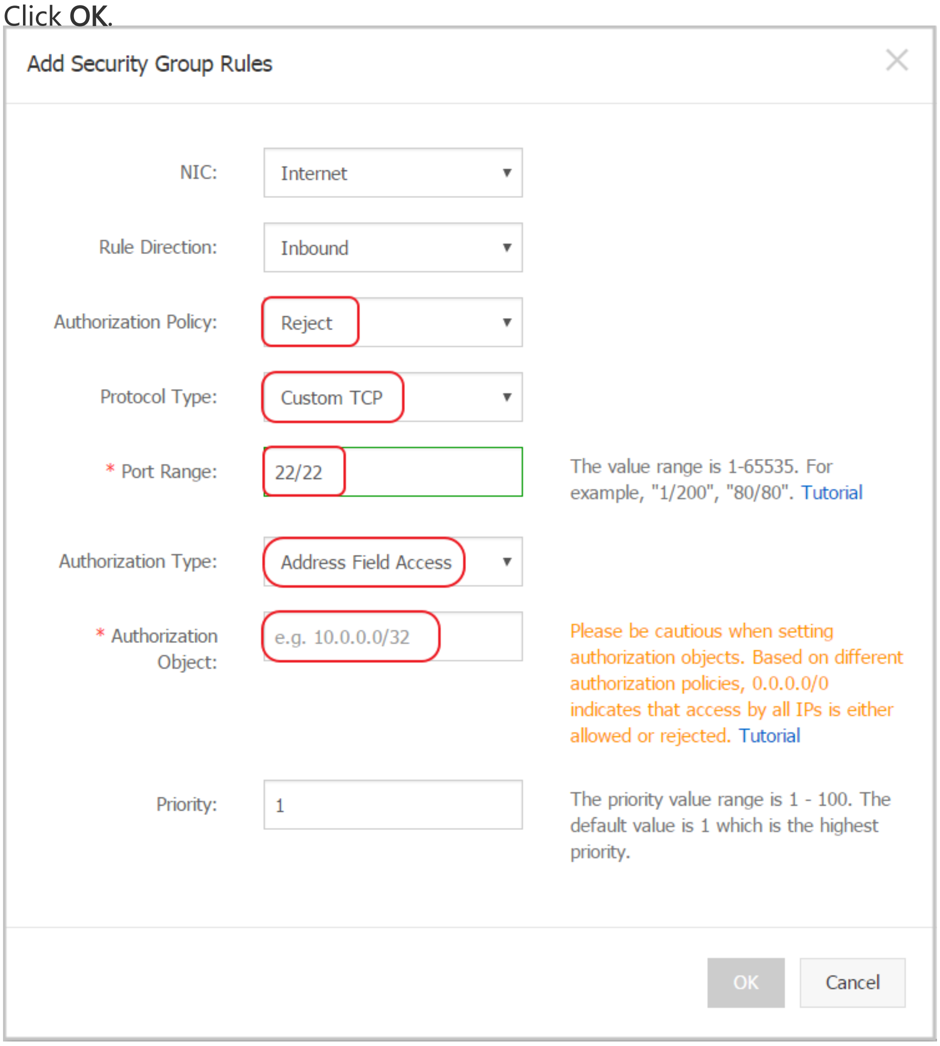
* Authorization Object: e.g. 10.0.0.0/32 Please be cautious when setting authorization objects. Based on different authorization policies, 0.0.0.0/0 indicates that access by all IPs is either allowed or rejected. Tutorial

Priority: 1 The priority value range is 1 - 100. The default value is 1 which is the highest priority.

If you want to reject an IP address to access to Port 22 of your ECS instance, on the **Add Security Group Rules** dialog:

- Select **Reject** for the **Authorization Policy**.
- Select **Custom TCP** for the **Protocol Type**.

- Enter **22/22** as the **Port Range**.
- Select **Address Field Access** for the **Authorization Type** and enter an IP address with or without a CIDR prefix, for example 1.2.3.4 or 1.2.3.4/24, as the **Authorization Object**.
- Enter **1** for **Priority**.
- Click **OK**.



Add Security Group Rules

NIC: Internet

Rule Direction: Inbound

Authorization Policy: Reject

Protocol Type: Custom TCP

* Port Range: 22/22

The value range is 1-65535. For example, "1/200", "80/80". Tutorial

Authorization Type: Address Field Access

* Authorization Object: e.g. 10.0.0.0/32

Please be cautious when setting authorization objects. Based on different authorization policies, 0.0.0.0/0 indicates that access by all IPs is either allowed or rejected. Tutorial

Priority: 1

The priority value range is 1 - 100. The default value is 1 which is the highest priority.

Allow remote login from a specific IP address

Take a Linux instance as an example. Configure to allow a specific IP address to access port 22.

A Linux instance is used in the following example. Allow a specific IP address to SSH the instance.

To allow remote login from a specific IP address, perform the following:

Log on to the ECS Management Console.

Click **Instances** in the left-side navigation bar.

Select your desired region.

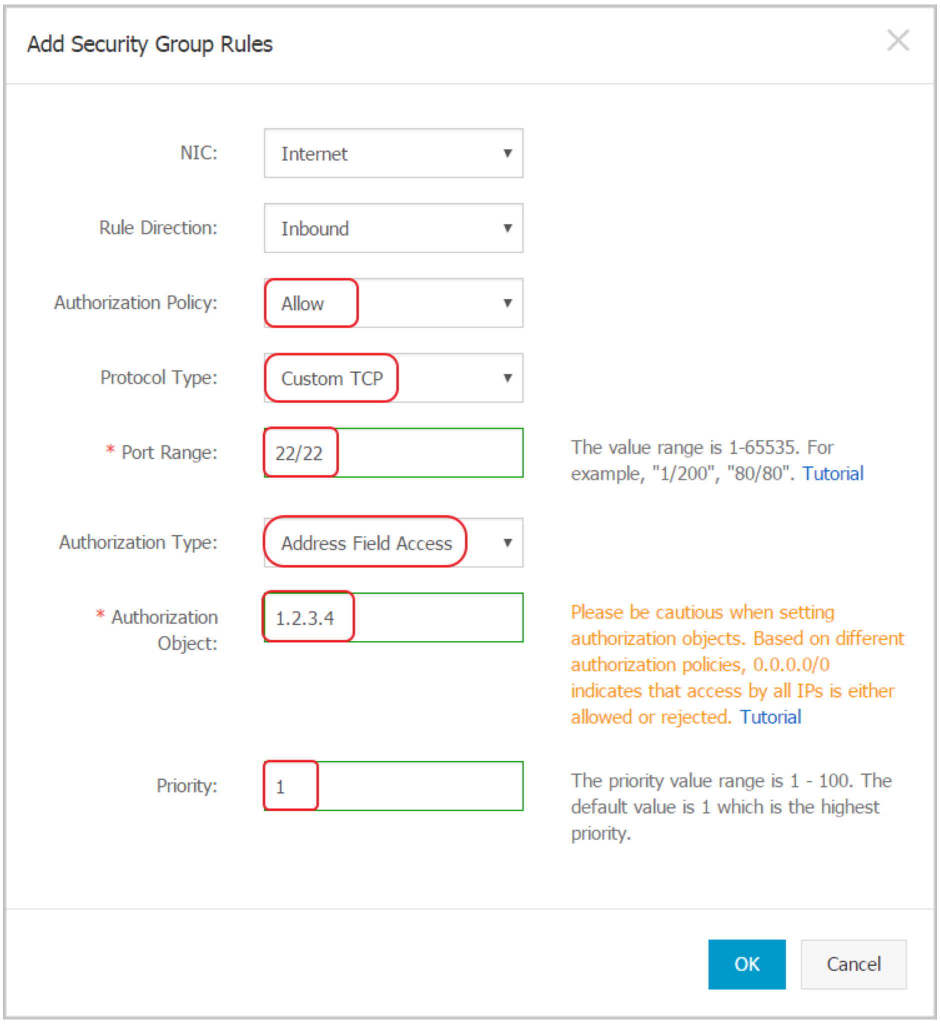
Select your desired instance, and click **Manage**.

Select **Security Groups** in the left-side navigation bar, and click **Configure Rules** of one security group in the list.

Click **Internet Inbound** and then click **Add Security Group Rules**.

On the **Add Security Group Rules** dialog box:

- Select **Allow** for the **Authorization Policy**.
- Select **Custom TCP** for the **Protocol Type**.
- Enter **22/22** as the **Port Range**.
- Select **Address Field Access** for the **Authorization Type** and enter an IP address with or without a CIDR prefix, for example 1.2.3.4 or 1.2.3.4/24, as the **Authorization Object**.
- Enter **1** for **Priority**.
- Click **OK**.



Add Security Group Rules

NIC:	Internet
Rule Direction:	Inbound
Authorization Policy:	Allow
Protocol Type:	Custom TCP
* Port Range:	22/22
Authorization Type:	Address Field Access
* Authorization Object:	1.2.3.4
Priority:	1

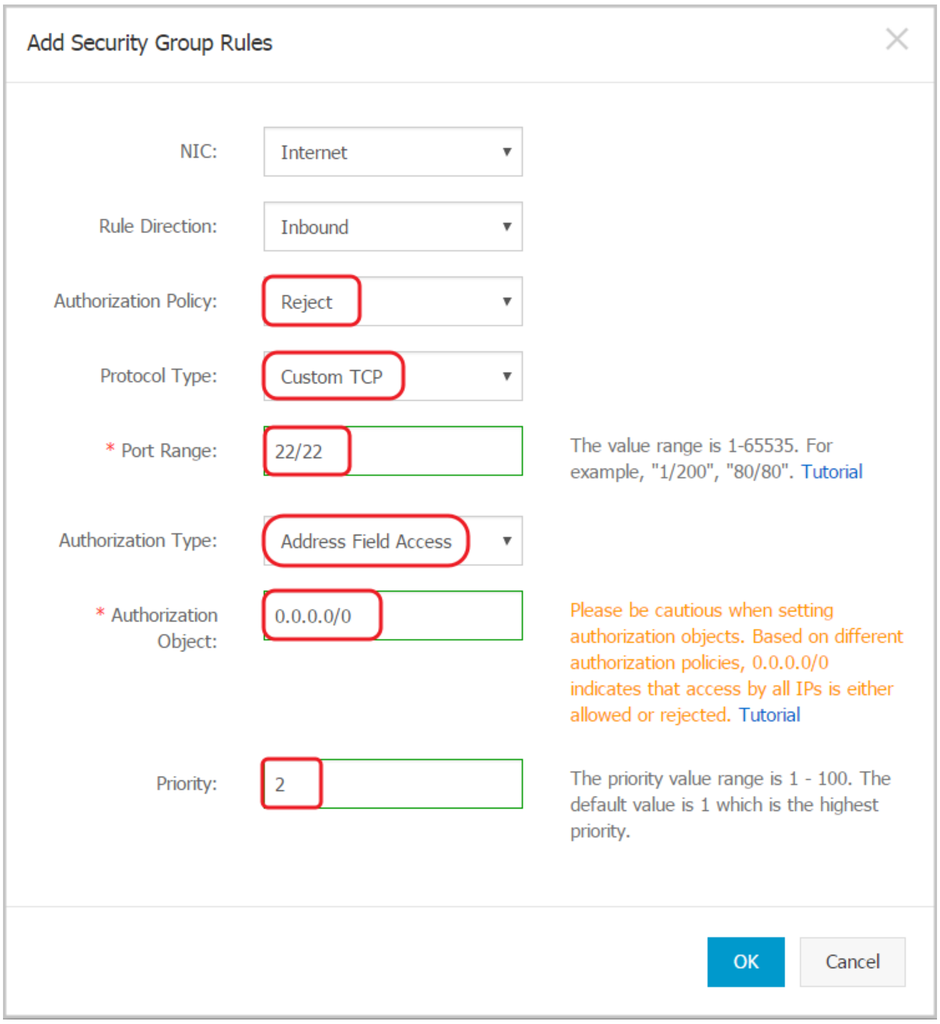
The value range is 1-65535. For example, "1/200", "80/80". Tutorial

Please be cautious when setting authorization objects. Based on different authorization policies, 0.0.0.0/0 indicates that access by all IPs is either allowed or rejected. Tutorial

The priority value range is 1 - 100. The default value is 1 which is the highest priority.

Add another security group rule:

- Select **Reject** for the **Authorization Policy**.
- Select **Custom TCP** for the **Protocol Type**.
- Enter **22/22** as the **Port Range**.
- Select **Address Field Access** for the **Authorization Type** and enter **0.0.0.0/0** as the **Authorization Object**.
- Enter **2** for **Priority**.
- Click **OK**.



Add Security Group Rules

NIC: Internet

Rule Direction: Inbound

Authorization Policy: Reject

Protocol Type: Custom TCP

* Port Range: 22/22

The value range is 1-65535. For example, "1/200", "80/80". Tutorial

Authorization Type: Address Field Access

* Authorization Object: 0.0.0.0/0

Please be cautious when setting authorization objects. Based on different authorization policies, 0.0.0.0/0 indicates that access by all IPs is either allowed or rejected. Tutorial

Priority: 2

The priority value range is 1 - 100. The default value is 1 which is the highest priority.

When both security rules are successfully configured, the following results are be displayed:

- The request to access port 22 from 1.2.3.4 is allowed, according to the rule configured as priority 1.
- The request to access port 22 from other IP addresses is rejected, according to the rule configured as priority 2.

Allow instance access to specific IP addresses

You can allow instance access to specified IP addresses.

To allow access to an instance for only specific IP addresses, perform the following:

Log on to the ECS Management Console.

Click **Instances** in the left-side navigation bar.

Select your desired region.

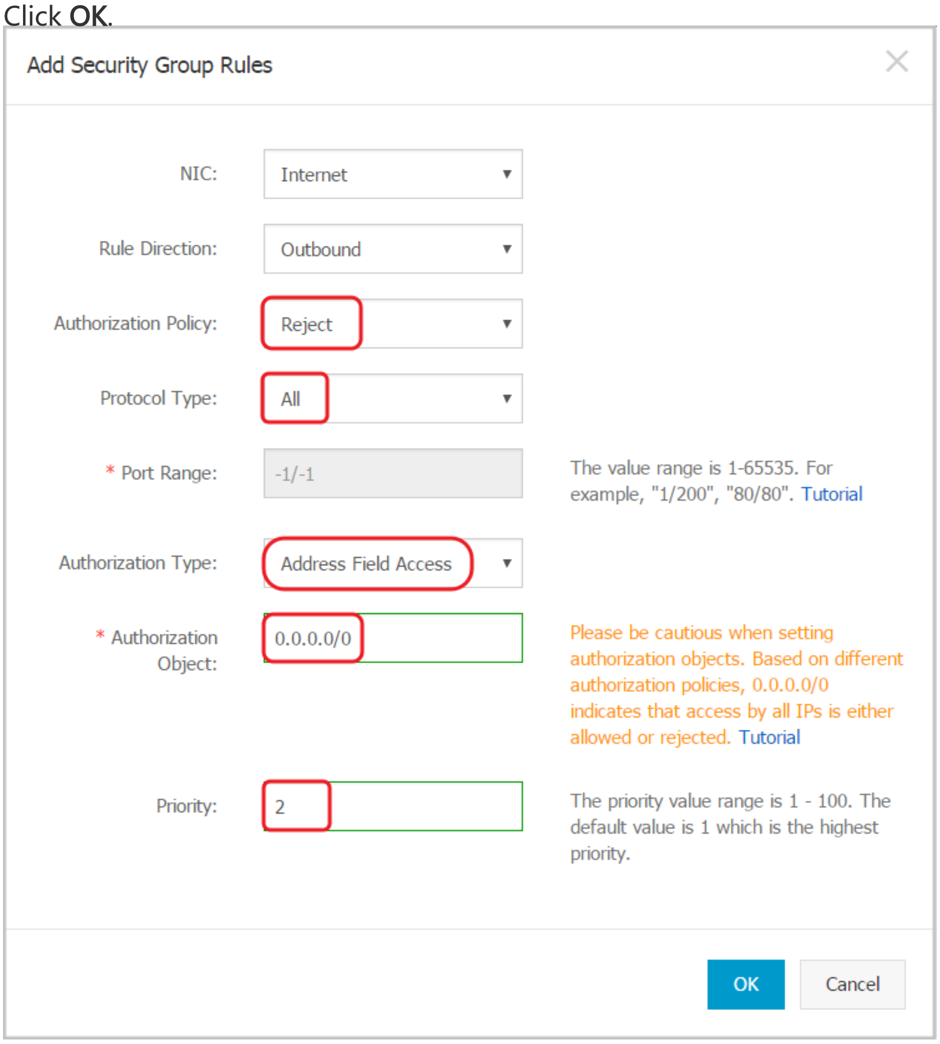
Select your desired instance, and click **Manage**.

Select **Security Groups** in the left-side navigation bar, and click **Configure Rules**.

Click **Internet Outbound** and then click **Add Security Group Rules**.

On the **Add Security Group Rules** dialog box:

- Select **Reject** for the **Authorization Policy**.
- Select **All** for the **Protocol Type**.
- Select **Address Field Access** for the **Authorization Type** and enter **0.0.0.0/0** as the **Authorization Object**.
- Enter **2** for **Priority**.
- Click **OK**.



Add Security Group Rules

NIC: Internet

Rule Direction: Outbound

Authorization Policy: Reject

Protocol Type: All

* Port Range: -1/-1

The value range is 1-65535. For example, "1/200", "80/80". Tutorial

Authorization Type: Address Field Access

* Authorization Object: 0.0.0.0/0

Please be cautious when setting authorization objects. Based on different authorization policies, 0.0.0.0/0 indicates that access by all IPs is either allowed or rejected. Tutorial

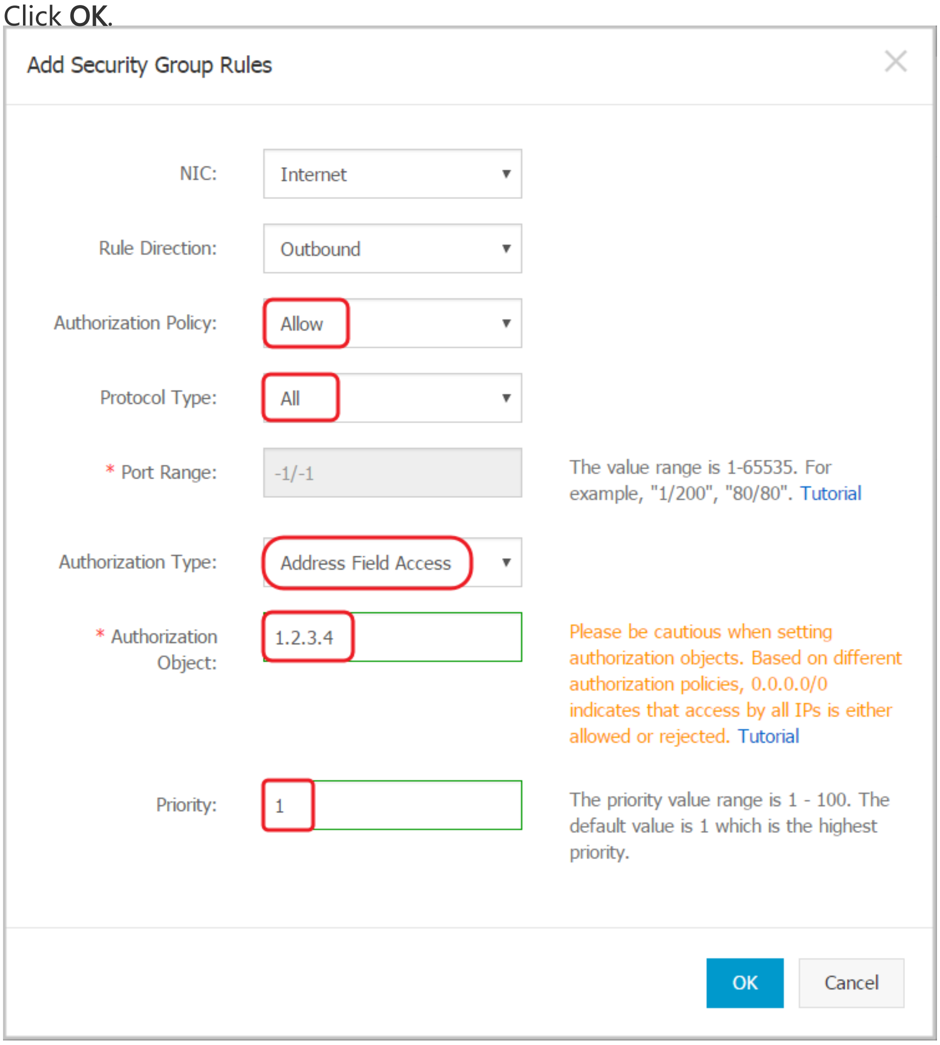
Priority: 2

The priority value range is 1 - 100. The default value is 1 which is the highest priority.

Add another security group rule:

- Select **Allow** for the **Authorization Policy**.
- Select **All** for the **Protocol Type**.

- Select **Address Field Access** for the **Authorization Type** and enter an IP address with or without a CIDR prefix, for example 1.2.3.4 or 1.2.3.4/24, as the **Authorization Object**.
- Enter **1** for **Priority**.
- Click **OK**.



Add Security Group Rules

NIC: Internet

Rule Direction: Outbound

Authorization Policy: Allow

Protocol Type: All

* Port Range: -1/-1

The value range is 1-65535. For example, "1/200", "80/80". Tutorial

Authorization Type: Address Field Access

* Authorization Object: 1.2.3.4

Please be cautious when setting authorization objects. Based on different authorization policies, 0.0.0.0/0 indicates that access by all IPs is either allowed or rejected. Tutorial

Priority: 1

The priority value range is 1 - 100. The default value is 1 which is the highest priority.

To check that the rules were successfully configured, log on to the instance and runping or telnet. If you do not have access to IP addresses except for the IP address previously specified for access authorization, the configuration is successful.

Default security group rules

For classic network

For a classic network, the default rules of the default security group are as follows:

- Reject all for intranet inbound traffic, and allow all for intranet outbound traffic.
- Allow all for Internet outbound traffic, and allow access for Internet inbound traffic at the

following ports:

- Port 22 of TCP protocol for SSH.
- Port 3389 of TCP protocol for remote access.
- ICMP protocol for remote access.

For VPC network

The default rules of the default security group are as follows:

- Allow all for 0.0.0.0/0 for both intranet inbound and intranet outbound traffic, that is, allows all instances in the VPC to communicate with each other.
- All rules can be set for the inbound and outbound traffic, regardless of intranet or Internet.

For user-defined security groups

For user-defined security groups, the default rules of the default security group are as follows:

- Allow all for outbound traffic.
- Reject all for inbound traffic, for both intranet and Internet.

Create a security group

A security group functions similarly to virtual firewalls, and is used to set network access controls for one or more ECS instances. When creating instances, you must select a security group. You can also add security group rules to control outbound and inbound network access for all ECS instances in the security group.

To create a security group, perform the following:

Log on to the ECS Management Console.

Click **Security Groups** in the left-side navigation bar.

Select your desired region.

Click **Create Security Group**. In the displayed dialog box, enter the following:

Security Group Name
The length must be 2 ~ 128 characters. It can contain uppercase letters, lowercase letters, and Chinese characters. It cannot contain numbers, underscores (_), or hyphens (-).

Description
The length must be 2 ~ 256 characters. Do not start with http:// or https://.

- **Network Type**
There are two network types, Classic network and VPC. If you select VPC, you must select a specific VPC. If no VPCs have been created in the current region, you must create one first.

Click **OK**.

Configure security group rules

Security group rules are designed to allow or reject inbound and outbound Internet or intranet access for ECS instances in a security group. You can authorize or cancel security group rules at any time. Any changes you make to security group rules will automatically apply to instances associated with the security group.

If two security groups have identical rules, but different access rules, rules for rejecting access will be valid, but rules for allowing access will be invalid.

Operating procedure

To configure security group rules, perform the following:

Log on to the ECS Management Console.

Click **Security Groups** in the left-side navigation bar.

Select your desired region.

Select the security group to authorize and click **Configure Rules**.

Click **Add Security Group Rule**. In the displayed dialog box, specify the following:

NIC type
The type can be **Internet** or **Intranet**. If this security group belongs to a VPC, select **Intranet**.

Rule Direction

The type can be **Inbound** or **Outbound**.

Authorization Policy
The policy can be **Allow** or **Reject**.

Protocol Type
The type can be All, Custom TCP, Custom UDP, All ICMP, All GRE, SSH (22), telnet (23), HTTP (80), HTTPS (443), MS SQL (1433), Oracle (1521), MySQL (3306), RDP (3389), PostgreSQL (5432), and Redis (6379).

Port Range
The range can be 1 ~ 65535, in the format of “Start Port/End Port”, for example, “1/200”. If you want to set it to a specific port, you must set Start Port and End Port to the desired port number, for example, “80/80”. If you set it to “-1/-1”, it means all ports.

Authorization Type
The type can be **Address Field Access** or **Security Group Access**.

Authorization Object

- If you select **Address Field Access** for **Authorization Type**, enter an IP address with or without a CIDR prefix. Only IPv4 addresses are supported.
- If you select **Security Group Access** for **Authorization Type**, select a security group of your account or other account. If you want to authorize a security group of other account, specify the **Account** ID, which you can get on **Account Management** > **Security Settings**.

Notice: To ensure the security of your instances, when you are configuring an intranet inbound rule for a security group of classic network type, **Security Group Access** is the top priority for **Authorization Type**. If you want to select **Address Field Access**, you must enter an IP address with the CIDR prefix, “/32”, in the format of a.b.c.d/32.

Priority
The range can be 1 ~ 100, in descending order of priority.

Click **OK**.

ECS security group rule priority explanation

Newer security groups have a higher priority than older security groups if they have the same **Priority** value, but have conflict between them.

However, security group priorities should not be regarded as only comparable within a security group, because they also apply when the policies of different security groups are applied to the same instance. Therefore, if there is a conflict between rules in different security groups, the rule with the highest rule priority will apply.

If there are security group rules with the same priority, the rule for rejection will prevail.

Examples

Scenario 1

- Security group A, created in 2015, rule 100: reject Port 80.
- Security group B, created in 2014, rule 100: allow Port 80.

Result: no connection with Port 80.

Scenario 2

- Security group A, created in 2015, rule 100: allow Port 80.
- Security group B, created in 2014, rule 90: reject Port 80.

Result: connection is successful with Port 80.

Scenario 3

- Security group A, created in 2015, rule 90: reject Port 80.
- Security group B, created in 2014, rule 100: allow Port 80.

Result: no connection with Port 80.

Solution for ineffective security policies

If packets are transmitted at short intervals throughout the security policy change process, the security group policy will not apply the new rules straight away.

To make the new rules take effect, disconnect from the instance for a short period of time, and then log on again.

View the security group list

You can view the security groups on the ECS Management Console at any time.

To view the security groups list, perform the following:

Log on to the ECS Management Console.

Click **Security Groups** in the left-side navigation bar.

Select your desired region. A list of all the security groups in the specified region will be displayed.

(Optional) You can select VPC ID in the filter input box, and then search for a specific ID, to list all the security groups under this VPC.

Modify security group properties

You can modify the name and description of a security group at any time.

To modify the name and description of a security group, perform the following:

Log on to the ECS Management Console.

Click **Security Groups** in the left-side navigation bar.

Select your desired region. A list of all the security groups in this region will be displayed.

Modify properties of your desired security group:

- Modify the name: Hover the cursor over the group’ s name, and then click the pen icon that appears.
- Modify the name and description: Click **Modify**, and then enter a new name and description in the dialog box.

Click **OK**.

View the rules of a security group

You can view the rules of a security group at any time.

To view the rules of a security group, perform the following:

Log on to the ECS Management Console.

Click **Security Groups** in the left-side navigation bar.

Select your desired region.

Select your desired security group.

Click **Configure Rules**. The following security group rule tabs will be displayed for Classic Networks and VPCs:

- For Classic networks
  - Internet Inbound
  - Internet Outbound
  - Intranet Inbound
  - Intranet Outbound
- For VPCs
  - Intranet Inbound
  - Intranet Outbound (Egress)

Click a tab to view the security group rules for that type.

Delete a security group rule

You can delete security group rules if you no longer need them.

To delete rules in a security group, perform the following:

Log on to the ECS Management Console.

Click **Security Groups** in the left-side navigation bar.

Select your desired region.

Select the security group where you want to delete rules.

Click **Configure Rules**.

On the security group management page, select the type of rule you want to delete.

Select the rule you want to delete.

Click **Delete**.

In the dialog box, click **OK**.

Delete a security group

You can delete security groups, if you no longer require them.

Note:

- Before deleting a security group, ensure it does not contain instances and is not referenced in the rules of another security group.
- Deleting a security group will delete all its rules.

To delete a security group, perform the following:

Log on to the ECS Management Console.

Click **Security Groups** in the left-side navigation bar.

Select your desired region. You can then view a list of all the security groups in the region.

Select one or more security groups.

Click **Delete**.

In the displayed dialog box, click **OK**.

Key Pairs

Introduction to SSH key pairs

Alibaba Cloud offers two authentication approaches for remote logon to ECS instances:

- Password logon: The traditional authentication approach using the administrator password. It applies to both Windows instances and Linux instances.
- SSH key pair logon: This approach only applies to Linux instances. It is recommended that you choose this authentication approach to protect your instance’ s security.

What is an SSH key pair?

An SSH key pair is a pair of keys generated through an encryption algorithm: one key is made public, known as the **public key**, and the other is kept private, known as the **private key**.

If you have placed the public key in a Linux instance, you can use the private key to log on to the instance via SSH commands or related tools locally or in another instance without the need to enter a password.

Advantages

SSH keys have the following advantages:

High security:

- The key security strength is much higher than regular user passwords and can help to eliminate brute force password-cracking threats;
- It is not possible to deduce the private key using the public key.

Ease-of-use and convenience: You can log on to the instance remotely through simple configuration in the console and on the local client. No password is required for the logon next time. If you need to maintain multiple ECS instances in batch, this logon method is recommended.

Alibaba Cloud SSH key pairs

There are two methods to generate key pairs:

- Alibaba Cloud generating a key pair, 2048-bit RSA keys by default.
- Importing the public key of a key pair that is generated by other key pair generation tools. The key pair must be one of the following types:
  - rsa
  - dsa

- ssh-rsa
- ssh-dss
- ecdsa
- ssh-rsa-cert-v00@openssh.com
- ssh-dss-cert-v00@openssh.com
- ssh-rsa-cert-v00@openssh.com
- ssh-dss-cert-v00@openssh.com
- ssh-rsa-cert-v01@openssh.com
- ssh-dss-cert-v01@openssh.com
- ecdsa-sha2-nistp256-cert-v01@openssh.com
- ecdsa-sha2-nistp384-cert-v01@openssh.com
- ecdsa-sha2-nistp521-cert-v01@openssh.com

If your key pair is generated by Alibaba Cloud, you must download the private key when you generate the key for the first time. If you do not have the private key, you cannot ever log on to your ECS instance that is bound to this key pair.

You can allocate a key pair to an instance when you create the Linux instance, or you can allocate it after the instance is created.

If you use an SSH key pair to log on to a Linux instance, password authentication is disabled by default to improve security.

The limitations for using SSH keys are as follows:

- Only Linux instances are supported: Windows instances are not supported.
- An account can have up to 500 key pairs in a region.
- A Linux instance can only bind one SSH key pair. If your instance has already bound a key pair, the new key pair will replace the original key pair.
- Within the lifecycle of a Linux instance, you can re-bind the SSH key pair and instance. After re-binding, the key pair will take effect without the need to restart the instance.
- All instances of any instance type family, except those I/O optimized instances of Generation I, support SSH key pairs.

Operate an SSH key pair

- If you do not have an SSH key pair, log on to the ECS Management Console to create an SSH key pair.
- If you have had an SSH key pair generated by other tools, import an SSH key pair.
- If you do not need an SSH key pair any more, log on to the ECS Management Console to delete an SSH key pair.
- If you want to enable or disable SSH key pair authentication to log on to a Linux ECS instance, bind or unbind an SSH key pair.
- Allocate an SSH key pair when creating an ECS instance.
- Log on to an instance using an SSH key pair.

Create an SSH key pair

Currently, Alibaba Cloud only supports the creation of 2048-bit RSA key pairs.

- Alibaba Cloud will save the public key of the key pair.
- After the key pair is created successfully, you need to download the private key.
- The private key follows the unencrypted PEM-encoded PKCS#8 format.

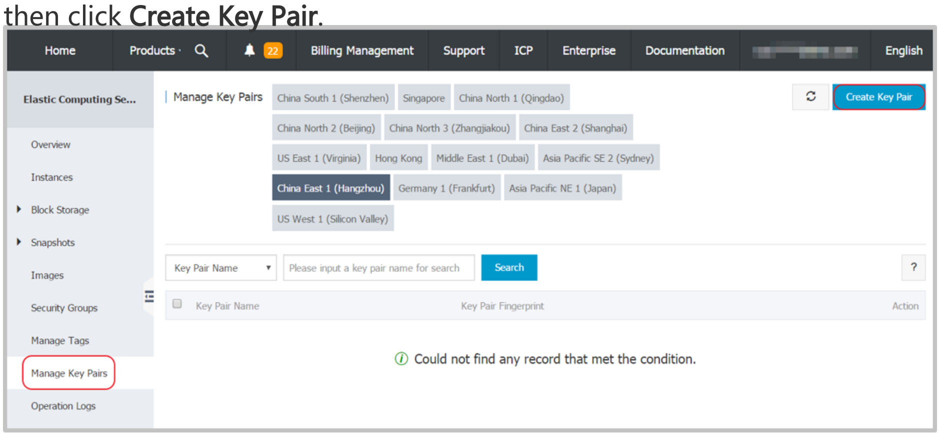
An account can have up to 500 key pairs per region.

Follow the steps below to create an SSH key pair.

Log on to ECS Management Console.

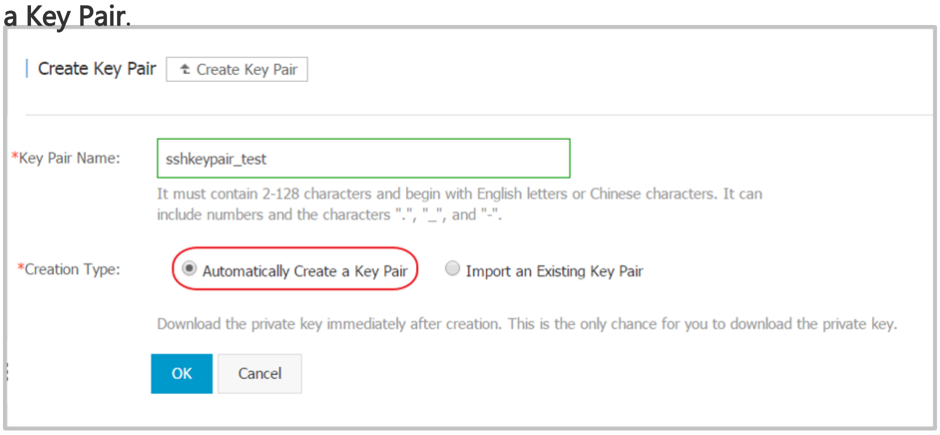
In the navigation pane, click **Manage Key Pairs**.

On the **Manage Key Pairs** page, select the region that you want to create a key pair, and then click **Create Key Pair**.



Could not find any record that met the condition.

On the **Create Key Pair** page, enter a name for the key pair, and select **Automatically Create a Key Pair**.



*Key Pair Name: sshkeypair_test

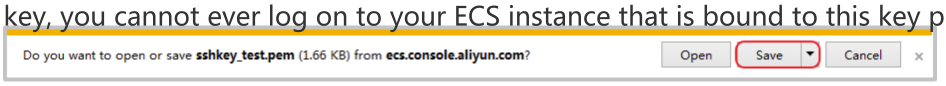
It must contain 2-128 characters and begin with English letters or Chinese characters. It can include numbers and the characters ".", "_", and "-".

*Creation Type: ● Automatically Create a Key Pair ○ Import an Existing Key Pair

Download the private key immediately after creation. This is the only chance for you to download the private key.

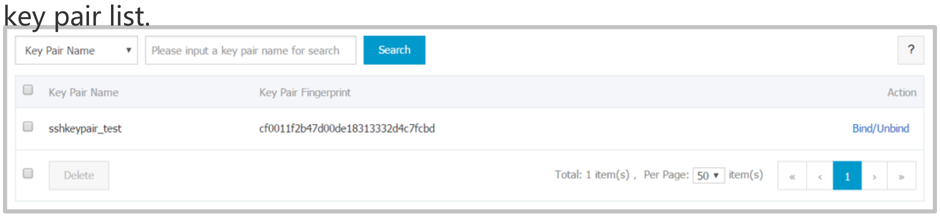
Click **OK** to start creating a key pair.

Download the private key. You may be notified by a pop-up window like the screenshot. **Note:** Alibaba Cloud will not save your private key, and only allows you to download your private key when a key pair is generated for the first time. If you do not have the private key, you cannot ever log on to your ECS instance that is bound to this key pair.



Do you want to open or save **sshkey_test.pem** (1.66 KB) from **ecs.console.aliyun.com**?

After creation, you can view the information, including **Key Pair Name** and **Key Pair Fingerprint**, in the key pair list.



□	Key Pair Name	Key Pair Fingerprint	Action
□	sshkeypair_test	cf0011f2b47d00de18313332d4c7fcbd	Bind/Unbind

□ Delete Total: 1 item(s) , Per Page: 50 ▾ item(s)

Import an SSH key pair

You can use other tools to generate an RSA key pair and import its public key into Alibaba Cloud. Refer to Introduction to SSH key pairs for the types of the imported key pair.

Note: Please keep the private key of the key pair secure and do not import the private key to Alibaba Cloud.

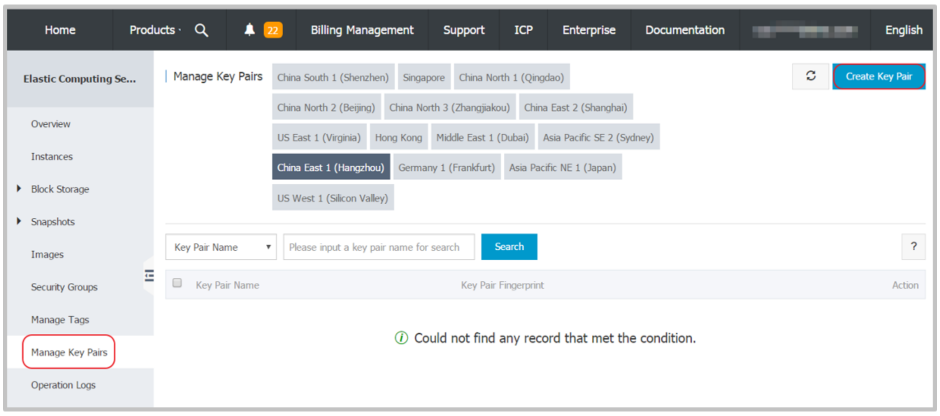
To import an SSH key pair, you must have a key pair generated by other tools, and the public key to be imported into Alibaba Cloud must be Base64-encoded.

Follow the steps below to import an SSH key pair.

Log on to ECS Management Console.

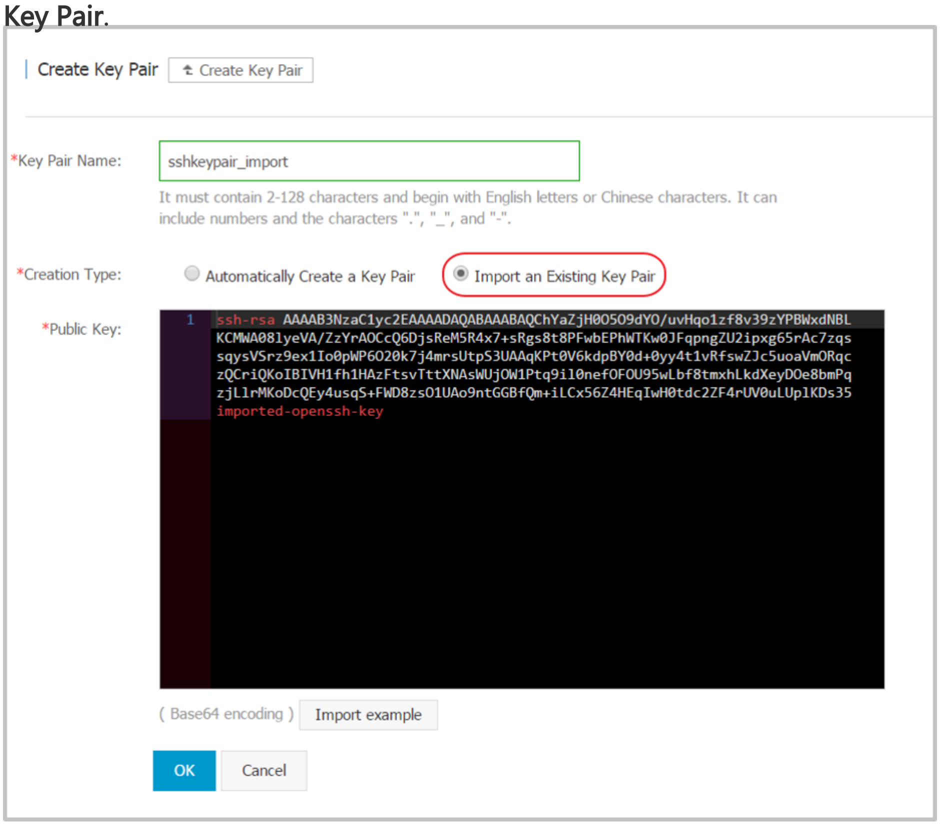
In the navigation pane, click **Manage Key Pair**.

On the **Manage Key Pair** page, select the region that you want to import a key pair, and then click **Create Key Pair**.



Could not find any record that met the condition.

On the **Create Key Pair** page, enter a name for the key pair, and select **Import an Existing Key Pair**.



Create Key Pair | Create Key Pair

*Key Pair Name: sshkeypair_import

It must contain 2-128 characters and begin with English letters or Chinese characters. It can include numbers and the characters ".", "_", and "-".

*Creation Type: ○ Automatically Create a Key Pair ● Import an Existing Key Pair

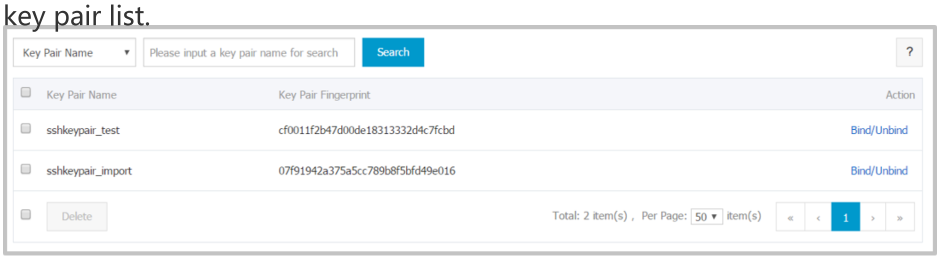
*Public Key:

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQChYaZjH0O5O9dYO/uvHqo1zf8v39zYPBWxdNBL
KCMWA08lyeVA/ZzYrAOCcQ6DjsReM5R4x7+sRgs8t8PFwbEPhWTKw0JFqpngZU2ipxg65rAc7zqs
sqysVSrz9ex1Io0pWP6O20k7j4mrsUtpS3UAAqKPt0V6kdpBY0d+0yy4t1vRfswZJc5uoaVmORqc
zQCriQKoIBIVH1fh1HAzFtsvTttXNAsWUjOW1Ptq9il0nefOFOU95wLbf8tmxhLkdXeyDOe8bmPq
zjLlrMKoDcQEy4usqS+FWD8zsO1UAo9ntGGBfQm+iLCx56Z4HEqIwH0tdc2ZF4rUV0uLUplKDs35
imported-openssh-key
```

(Base64 encoding) Import example

Click **OK** to start importing the key pair.

After creation, you can view the information, including **Key Pair Name** and **Key Pair Fingerprint**, in the key pair list.



□	Key Pair Name	Key Pair Fingerprint	Action
□	sshkeypair_test	cf0011f2b47d00de18313332d4c7fcbd	Bind/Unbind
□	sshkeypair_import	07f91942a375a5cc789b8f5bfd49e016	Bind/Unbind

□ Delete   Total: 2 item(s) , Per Page: 50 item(s)

Bind or unbind an SSH key pair

You can bind a key pair to a Linux instance. One instance can only bind one key pair.

- If the instance is running, the bound key pair will take effect immediately without the need to restart the instance.
- If your instance is using password-based authentication, Alibaba Cloud will automatically disable the password authentication feature after the key pair is bound.
- After a key pair is unbound, Alibaba Cloud will automatically enable the password authentication feature. **Note:** If you did not set a password, you need to reset the instance password and then try to log on again.
- If your instance is stopped, the bound key pair will take effect after the instance is restarted.
- If the instance already has a key pair, it will be replaced with the new key pair.

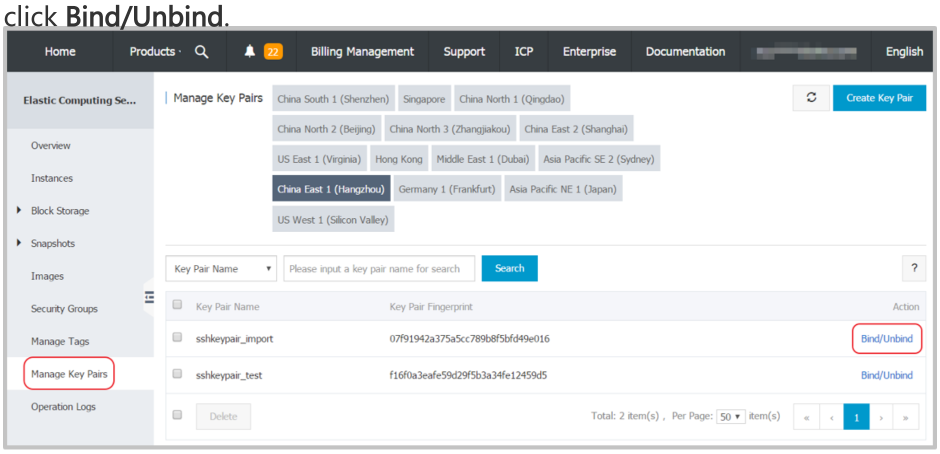
You can also unbind a key pair from an instance. The unbinding will take effect in real time.

Follow the steps below to bind an SSH key pair to an ECS instance or unbind it from an ECS instance.

Log on to ECS Management Console.

In the navigation pane, click **Manage Key Pairs**.

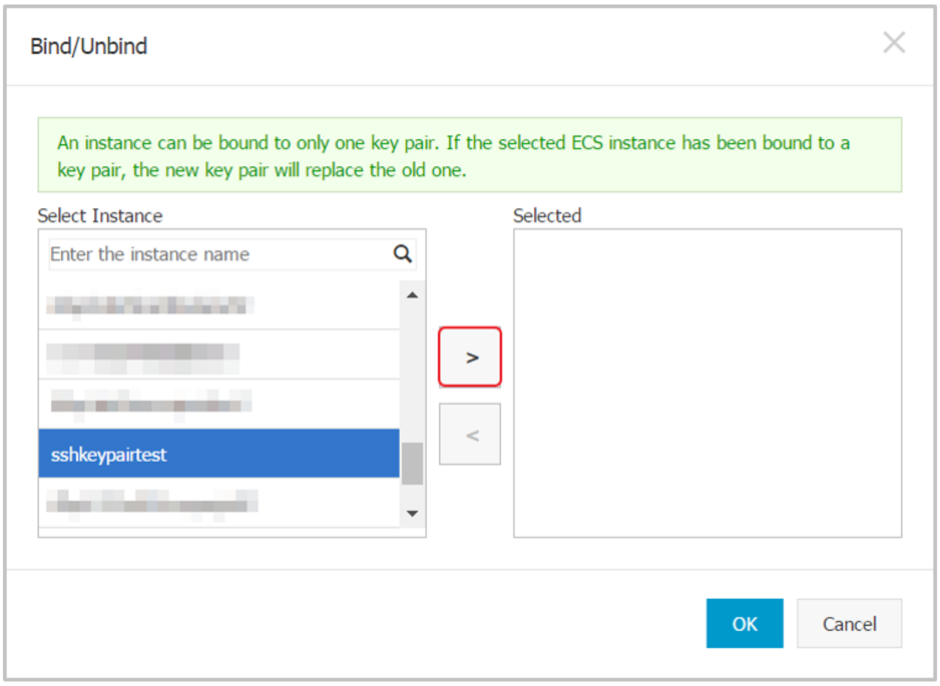
On the **Manage Key Pairs** page, select the desired region, find the desired key pair, and then click **Bind/Unbind**.



□	Key Pair Name	Key Pair Fingerprint	Action
□	sshkeypair_import	07f91942a375a5cc789b8f5bfd49e016	Bind/Unbind
□	sshkeypair_test	f16f0a3eafe59d29f5b3a34fe12459d5	Bind/Unbind

On the **Bind/Unbind** dialog,

- To bind the desired key pair to an ECS instance: select the desired instance in the **Select Instance** box, and then click the **>** icon.
- To unbind the desired key pair from an ECS instance, select the desired instance in the **Selected** box, and then click the **<** icon.



Bind/Unbind

An instance can be bound to only one key pair. If the selected ECS instance has been bound to a key pair, the new key pair will replace the old one.

Select Instance

Enter the instance name

[redacted]

[redacted]

[redacted]

sshkeypairtest

[redacted]

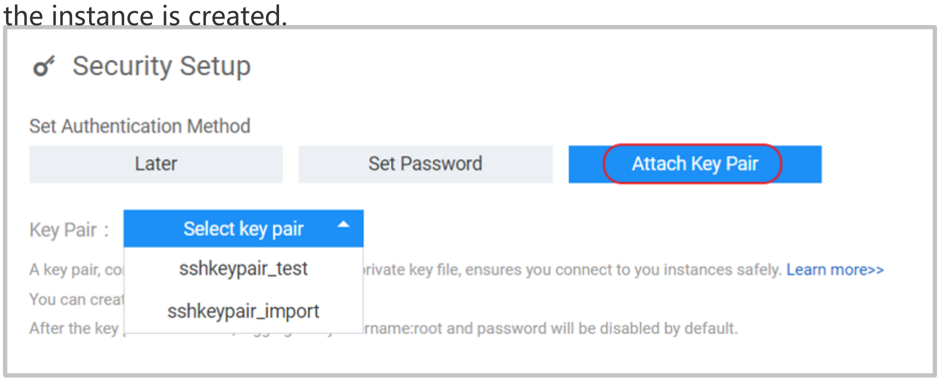
Selected

Click **OK** to start binding or unbinding the key pair.

Allocate an SSH key pair when creating an instance

There must be at least one key pair available for your account.

When you are creating an instance, you can select an existing key pair, and Alibaba Cloud will embed the public key into the instance. As a result, you can use the key pair to connect to an instance after the instance is created.



Security Setup

Set Authentication Method

Key Pair : Select key pair

sshkeypair_test

sshkeypair_import

A key pair, co rivate key file, ensures you connect to you instances safely. Learn more>>

You can creat

After the key rname:root and password will be disabled by default.

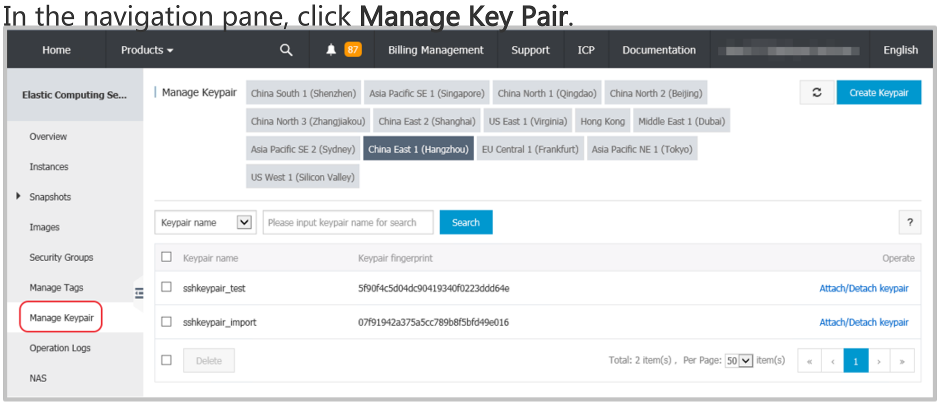
Delete an SSH key pair

You can delete a key pair if you no longer need it. The delete operation will completely remove the key pair and it cannot be recovered. Existing instances that have used the key pair will not be affected, and the deleted key pair name will remain associated to the instance.

Follow the steps below to delete one or more key pairs.

Log on to ECS Management Console.

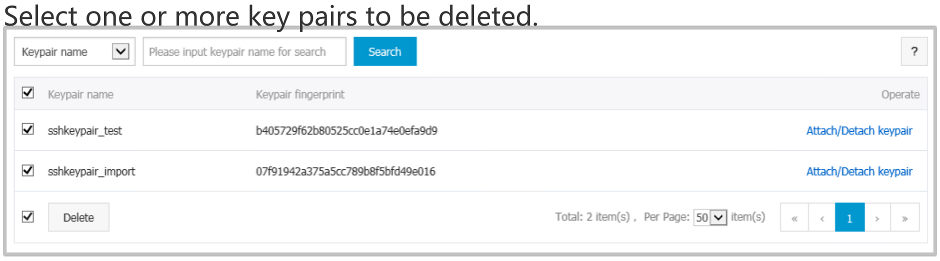
In the navigation pane, click **Manage Key Pair**.



□	Keypair name	Keypair fingerprint	Operate
□	sshkeypair_test	5f90f4c5d04dc90419340f0223ddd64e	Attach/Detach keypair
□	sshkeypair_import	07f91942a375a5cc789b8f5bfd49e016	Attach/Detach keypair

□ Delete Total: 2 item(s) , Per Page: 50 item(s) « ‹ 1 › »

Select one or more key pairs to be deleted.



☑	Keypair name	Keypair fingerprint	Operate
☑	sshkeypair_test	b405729f62b80525cc0e1a74e0efa9d9	Attach/Detach keypair
☑	sshkeypair_import	07f91942a375a5cc789b8f5bfd49e016	Attach/Detach keypair

☑ Delete Total: 2 item(s) , Per Page: 50 item(s) « ‹ 1 › »

Click **Delete** to start deleting the selected key pair.

Tags

As of January 2017, the ECS Management Console only supports adding tags to instances.

Each tag is composed of a key-value pair.

Up to 10 tags can be bound to a single instance.

For a single instance, the tag key for each tag must be unique. Tags with identical tag keys will be overwritten.

Tag information cannot be transmitted across regions.

A tag will be automatically deleted when it is not bound to any instance.

Add a tag to an instance

If you have a large number of instances, you can add tags to them to facilitate unified management and allow you to group different instances easily.

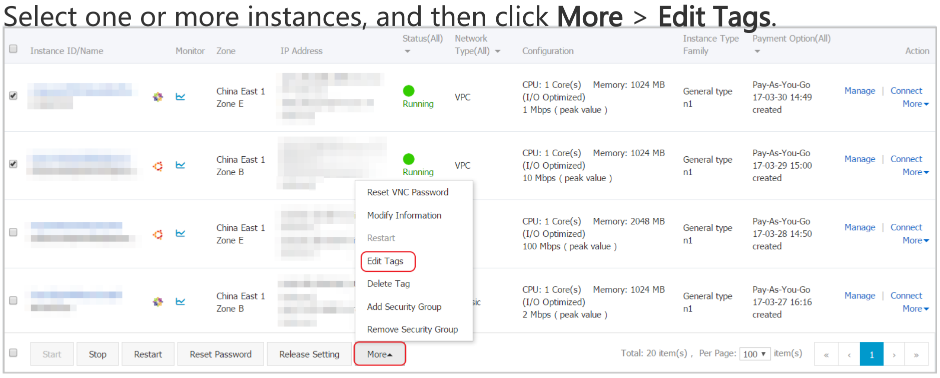
To add a tag to an instance, perform the following:

Log on to the ECS Management Console.

Click **Instances** in the left-side navigation bar.

Select your desired region.

Select one or more instances, and then click **More** > **Edit Tags**.



□	Instance ID/Name	Monitor	Zone	IP Address	Status(All)	Network Type(All)	Configuration	Instance Type Family	Payment Option(All)	Action
☑	[redacted]		China East 1 Zone E	[redacted]	● Running	VPC	CPU: 1 Core(s) Memory: 1024 MB (I/O Optimized) 1 Mbps (peak value)	General type n1	Pay-As-You-Go 17-03-30 14:49 created	Manage | Connect More
☑	[redacted]		China East 1 Zone B	[redacted]	● Running	VPC	CPU: 1 Core(s) Memory: 1024 MB (I/O Optimized) 10 Mbps (peak value)	General type n1	Pay-As-You-Go 17-03-29 15:00 created	Manage | Connect More
□	[redacted]		China East 1 Zone E	[redacted]			CPU: 1 Core(s) Memory: 2048 MB (I/O Optimized) 100 Mbps (peak value)	General type n1	Pay-As-You-Go 17-03-28 14:50 created	Manage | Connect More
□	[redacted]		China East 1 Zone B	[redacted]		sic	CPU: 1 Core(s) Memory: 1024 MB (I/O Optimized) 2 Mbps (peak value)	General type n1	Pay-As-You-Go 17-03-27 16:16 created	Manage | Connect More

Total: 20 item(s) , Per Page: 100 item(s)

In the dialog box, click **Create**.

Enter your custom tag key and value, and then click **Confirm**.

Your tag will then be added to the available tag selection. Click **Confirm** to add the created tag to the instance.

Delete a tag

You can delete tags if you no longer require them.

To delete a tag, perform the following:

Log on to the ECS Management Console.

Click **Instances** in the left navigation bar.

Select your desired region.

Select the instance you want to remove tag from.

Click **More** > **Edit Tag**.

In the dialog box, enter the tag key you want to delete, and then click **OK**.

Click **OK** to delete the tag.

Search for instances by tags

You can search for instances by tags.

To search for instances by tags, perform the following:

Log on to the ECS Management Console.

Click **Instances** in the left-side navigation bar.

Select your desired region.

Click **Tag** above the instance list.

Select the tag key you want to use for the instance search.

The instances that use the specified tag are displayed.

Monitoring

You can monitor the operating statuses of instances to ensure optimal performance.

You can monitor the status of instances using the following two portals:

- Instance Details page
- CloudMonitor

Monitor the status of an instance using Instance Details page

To monitor the Status of an instance using Instance Details, perform the following:

Log on to the ECS Management Console.

Click **Instances** in the left navigation bar.

Select your desired region.

Click the instance you want to monitor.

On the **Instance Details** page, you can view the monitoring information, including CPU usage and outbound/inbound network traffic information.

- Information about CPU monitoring:
  - For Linux instances, use the top command to view CPU usage details. Log on to the instance and execute the top command in the command line. Then, pressShift+P key to list programs by CPU usage to view which processes are using the most CPU resources.
  - For Windows instances, use the **Task Manager** on an instance to view the CPU usage to view which programs are using the CPU resources of the server.
- The displayed monitoring data shows the Internet traffic of the instance in Kbps (1 Mbps = 1,024 Kbps). The monitoring data shows inbound and outbound instance traffic. For 1 Mbps of bandwidth, the bandwidth is working at full capacity if the outbound network traffic reaches 1,024 Kbps.

CloudMonitor

To install a CloudMonitor, perform the following:

On the Alibaba Cloud Console, select **Products and Services** > **CloudMonitor**.

Click **Host Monitoring** on the left-side navigation bar, and then select the name of the instance you wish to monitor.

Click **Click to Install** to monitor the instance OS. Click **Monitoring Chart** to view basic parameters. Click **Alarm Rules** to set alarm rules.

Note: For more information about CloudMonitor, see CloudMonitor Product Documentation.