ALIBABA CLOUD

Alibaba Cloud

Elastic Compute Service

Images

Document Version: 20201013

Alibaba Cloud

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.

2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company or individual in any form or by any means without the prior written consent of Alibaba Cloud.

3. The content of this document may be changed because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.

4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides this document based on the "status quo", "being defective", and "existing functions" of its products and services. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, special, or punitive damages, including lost profits arising from the use or trust in this document (even if Alibaba Cloud has been notified of the possibility of such a loss).

5. By law, all the contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of this document shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates.

6. Please directly contact Alibaba Cloud for any errors of this document.

Document conventions

Style	Description	Example
Danger	A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	Danger: Resetting will result in the loss of user configuration data.
Warning	A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	Warning: Restarting will cause business interruption. About 10 minutes are required to restart an instance.
Notice	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	Notice: If the weight is set to 0, the server no longer receives new requests.
Note	A note indicates supplemental instructions, best practices, tips, and other content.	Note: You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click **Settings**> **Network**> **Set network type**.
Bold	Bold formatting is used for buttons , menus, page names, and other UI elements.	Click **OK**.
`Courier font`	Courier font is used for commands	Run the `cd /d C:/window` command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	This format is used for an optional value, where only one item can be selected.	`ipconfig [-all|-t]`
{} or {a|b}	This format is used for a required value, where only one item can be selected.	`switch {active|stand}`

Table of Contents

1.Image overview

An ECS image stores information that you need for creating an ECS instance. You must select an image when you create an ECS instance. An image works as a copy that stores data from one or more disks. An ECS image may store data from a system disk or from both system and data disks.

Image types

The following table describes the types of ECS images based on their sources.

Type	Description	Price
Public image	Public images provided by Alibaba Cloud are licensed, secure, and stable. Public images include Windows Server system images and mainstream Linux system images. For more information, see Overview.	Only Windows Server and Red Hat Enterprise Linux public images are billed. Check the actual fees when you use them to create instances. The Windows Server and Red Hat Enterprise Linux public images are licensed and maintained by Microsoft and Red Hat, respectively. • Red Hat Enterprise Linux: Fees are calculated based on the instance type. • Windows Server: Fees are calculated based on the instance type. Other images: free of charge.

Custom image	Custom images are created from instances or snapshots, or imported from your local device. Only the creator of a custom image can use, share, copy, and delete the image. For more information, see Lifecycle of a custom image.	Custom image fees are billed in the following situations:
		• Daily-use fees. The daily-use fees are equal to the fees incurred by the snapshot where the custom image is created from. Snapshots are billed based on the storage space usage.
		• Instance creation fees. When you use a custom image to create an instance, fees are billed as follows:
		  ○ If the custom image is created based on an Alibaba Cloud Marketplace image, the custom image fees are equal to the total fees incurred by the Alibaba Cloud Marketplace image and the corresponding snapshot.
		  ○ If the custom image is created based on a free image, the custom image fees are equal to the fees of the corresponding snapshot.
		For more information, see Billing overview and Image FAQ.

Shared image	Shared images are images shared to you by other Alibaba Cloud accounts. For more information, see Share images.	If a shared image is provided by Alibaba Cloud Marketplace, the shared image is billed based on the pricing standards of the independent software vendors (ISVs).

Type	Description	Price
Alibaba Cloud Marketplace image	Alibaba Cloud Marketplace images are classified into the following types based on the ISVs: • Images provided by Alibaba Cloud accounts • Images provided by ISVs and licensed by Alibaba Cloud Marketplace An Alibaba Cloud Marketplace image contains an operating system and pre-installed software. The operating system and pre-installed software are tested and verified by the ISVs and Alibaba Cloud to ensure that the image is safe to use. For more information, see Marketplace images.	Alibaba Cloud Marketplace images are billed based on the pricing standards of the ISVs.

Lifecycle of a custom image

After you create or import a custom image, the image is in the **Available** state. You can then use the image to create ECS instances, share the image to another Alibaba Cloud account, or copy the image to another region. You can also delete images that you no longer need. The following figure shows the lifecycle of a custom image.

Create a custom image

After you create an ECS instance by using an existing image, you can configure the instance as needed. For example, you can install software and deploy projects on the instance, and create a custom image from the instance. For more information, see Create a custom image from an instance. Instances created from the custom image contain all the custom items that you have configured. For more information, see Create an ECS instance by using a custom image.

You can create a custom image from a system disk snapshot or from a system disk snapshot and one or more data disk snapshots. For more information, see Create a custom image from a snapshot.

You can also import a custom image from a local device. For more information, see Image import procedure.

Share and copy a custom image

Each image belongs to a region. For example, if you create a custom image in the China (Beijing) region, you can use the image to create ECS instances only in this region.

- When you share the image to another Alibaba Cloud account, this account can use the image only in the China (Beijing) region. If you want to share the image to an Alibaba Cloud account that needs to use the image in a different region, copy the image to the destination region, and then share the image to the target Alibaba Cloud account. For more information, see Share images.
- If you want to use the image in another region, copy the image to that region. The image copy is assigned a unique UID. It is independent of the original image. For more information, see Copy custom images.

Change the image of an ECS instance

After you create an ECS instance, you can change its operating system by replacing the image of the system disk.

- You can replace the image of the system disk with a public image. For more information, see Replace the system disk (public images).
- You can also replace the image of the system disk with a non-public image such as a custom, shared, or Alibaba Cloud Marketplace image. For more information, see Replace the system disk (non-public images).

Delete a custom image

You can delete customs images that you no longer need. After a custom image is deleted, you can no longer use it to created ECS instances. You cannot re-initialize disks of an ECS instance that is created from the image. For more information, see Re-initialize a system disk.

A custom image created from an ECS instance consists of the snapshots of disks that are attached to the instance. If you delete a custom image, snapshots contained in the image will not be deleted. If you do not want to keep the snapshots, navigate to the Snapshots page and delete the snapshots. For more information, see Delete a custom image.

API operations

You can also call API operations to manage images. For more information, see API overview.

2.Select an image

This topic describes how to select an appropriate image from multiple image types and operating systems to suit your business needs. You must select an image when you create an ECS instance.

When you select an image, you must consider the following factors:

- Region
- Image type
- Image fee
- Operating system
- Built-in software (such as MySQL and other applications)

Region

Each image is tied to its region and can only be used to create instances within the same region. For example, if you want to create an instance in China (Beijing), only images in the China (Beijing) region can be used. For more information about regions, seeRegions and zones.

If you want to use an image that belongs to a different region, you must copy the image to that region. For more information, see Copy custom images.

Image type

ECS images are classified into public images, custom images, shared images, and Alibaba Cloud Marketplace images based on image sources. For more information, see Image overview.

Image fee

You may be charged for images that you use. For more information, see Image overview.

Operating system

When you select an operating system, you must consider the following factors:

- Operating system architecture: 32-bit or 64-bit

Operating system architecture	Applicable memory	Limit
32-bit	A maximum of 4 GiB memory	◦ If the memory of an instance type is greater than 4 GiB, you cannot use a 32-bit operating system. ◦ A 32-bit Windows operating system supports a maximum of four CPU cores.
64-bit	A minimum of 4 GiB memory	If you want to use a memory of at least 4 GiB for your applications, use a 64-bit operating system.

- Operating system type such as Windows, Linux, or Unix-like

Operating system type	Logon mode	Feature	Scenario
Windows	Remote Desktop Connection	A Windows public image is installed with a genuine activated system.	◦ Applicable to programs developed based on Windows architectures such as .NET programs. ◦ Supports SQL Server and other databases (manual installation required).
Linux and Unix-like	SSH	◦ A common, stable, and secure server-side operating system. ◦ An open source operating system that provides fast deployment and easy source code compilation.	◦ Typically used for server applications, such as high-performance web servers, and supports common programming languages such as PHP and Python. ◦ Supports MySQL and other databases (manual installation required).

Alibaba Cloud provides a list of public images that run the Windows, Linux, or Unix-like operating systems. For more information, see Overview.

- Considerations for Windows

  We recommend that you use a recent version of Windows. More recent versions of Windows have fewer vulnerabilities than earlier versions. IIS 7.5 provides more features and a more convenient console than IIS 6.

  Read the following considerations and select the suitable hardware configuration and Windows version:

  - Instance types with one vCPU and 1 GiB memory do not support the MySQL database.
  - Windows instances that are used for website building and web environment deployment must have at least 2 GiB memory.
  - To ensure service availability, we recommend that you select an instance type that has at least 2 GiB of memory when you use Windows 2012.
  - You must select an instance type that has at least 2 GiB of memory if you want to use Windows 2016 or Windows 2019. If your selected instance type has memory of less than 2 GiB, Windows 2016 or Windows 2019 may not be displayed in the public image list on the buy page.
  - Alibaba Cloud no longer provides technical support for Windows Server 2003 system images.

- Considerations for Linux and Unix-like operating systems

  Alibaba Cloud Linux and Unix-like public images contain the following distributions:

- Alibaba Cloud Linux

  Alibaba Cloud Linux is an operating system that provides a safe, stable, and high-performance runtime environment for applications on ECS instances. Alibaba Cloud Linux 2 supports various cloud scenarios and instance types (excluding instances of the classic network type and non-I/O optimized instances). For more information, see Overview of Alibaba Cloud Linux 2.

- Red Hat series
  - CentOS
  - Red Hat

  The following table compares CentOS with Red Hat.

Operating system	Software package format	Package manager	Billing	Feature	Relationship
CentOS	.rpm	yum	Free usage	■ Has stable but less frequent patch updates than those of Red Hat. ■ Supports online and timely updates.	■ CentOS is an open source version of Red Hat. ■ They can use the same RPM package. ■ They can use the same commands.
Red Hat			Paid usage	Stable with enterprise-level technical support.	

- Debian series
  - Debian
  - Ubuntu

  The following table compares Debian with Ubuntu.

Operating system	Software package format	Package manager	Feature	Relationship
Debian	.deb	aptitude	Stable	Ubuntu is built on the Debian architecture and infrastructure. Ubuntu is the enhanced version of Debian.
Ubuntu		apt-get	■ User-friendly system configuration. ■ Timely software updates. ■ Easy to use and learn.	

- SUSE series
  - SUSE Linux
  - OpenSUSE

  The following table compares OpenSUSE with SUSE Linux.

Operating system	Feature	Relationship
OpenSUSE	■ OpenSUSE is the community edition of SUSE Linux. SUSE Linux Enterprise is the enterprise edition of SUSE Linux. ■ SUSE Linux Enterprise is more mature and stable, but its official distribution contains fewer software features than OpenSUSE. ■ OpenSUSE provides advanced software versions, better extensibility (desktop and server installation are supported), and free updates (you can also purchase official technical support). ■ SUSE Linux Enterprise is more suited for work and production environments, whereas OpenSUSE is more suited for personal entertainment and other professional purposes.	■ As of version 10.2, SUSE Linux is officially renamed OpenSUSE. ■ OpenSUSE uses the same kernel as SUSE Linux.
SUSE Linux		

- CoreOS

  CoreOS is an open source lightweight operating system based on the Linux kernel and designed to provide infrastructure for clustered deployments. CoreOS focuses on automation, ease of application deployment, security, reliability, and scalability. CoreOS provides the underlying functionality required for deploying applications inside software containers, together with a set of built-in tools for service discovery and configuration sharing.

- FreeBSD

  FreeBSD is a Unix-like operating system for a variety of platforms that focus on features, speed, and stability. FreeBSD provides advanced networking, performance, security, and compatibility features that are still missing from other operating systems, even some of the best commercial ones. For more information, visit FreeBSD Documentation.

Built-in software

Alibaba Cloud Marketplace images are typically pre-installed with a runtime environment or software applications. You can purchase appropriate images to create ECS instances based on your actual needs. For more information, see Alibaba Cloud Marketplace images.

What to do next

- Use an image to create an ECS instance. For more information, see Create an instance by using the provided wizard.
- Use an image to change the operating system. For more information, see Change the operating system.

3.Find an image

You can find an image based on its type, name, ID, or snapshot ID. After you find the image, you can use the image to create an instance or perform other operations. This topic describes how to find a specific image.

Methods

You can use one of the following methods to find an image:

- Find an image by using the console

  The following content lists three examples of this method:

  - Example 1: Find a Windows public image in the China (Beijing) region
  - Example 2: Find an image whose name contains mysql in the China (Hangzhou) region
  - Example 3: Find a custom image whose snapshot ID is s-2xxxxxxxxxxxxxxxxxxx in the China (Hong Kong) region

- Find an image by calling an API operation

Find an image by using the console

You can find the target image on the **Images** page in the ECS console.

1. Log on to the ECS console.
2. In the left-side navigation pane, choose **Instances & Images** > **Images**.
3. In the top navigation bar, select a region.
4. Select an image type.
5. Select a search item from the drop-down list.

   > **Note** You can select the image name, image ID, and snapshot ID as the search item.

6. Enter the corresponding value in the search bar.
7. Click **Search**.

Example 1

Example 1: Find a Windows public image in the China (Beijing) region

Perform the following operations on the **Images** page:

1. In the upper-left corner, select **China (Beijing)** from the drop-down list.
2. Click the **Public Image** tab.
3. Select **Image Name** from the drop-down list in the search bar.
4. Enter *win* in the search bar.
5. Click **Search**.

Example 2

Example 2: Find an image whose name contains mysql in the China (Hangzhou) region

Perform the following operations on the **Images** page:

1. In the upper-left corner, select **China (Hangzhou)** from the drop-down list.
2. Click the **Shared Images** tab.
3. Select **Image Name** from the drop-down list in the search bar.
4. Enter *mysql* in the search bar.
5. Click **Search**.

Example 3

Example 3: Find a custom image whose snapshot ID is s-2xxxxxxxxxxxxxxxxxx in the China (Hong Kong) region

Perform the following operations on the **Images** page:

1. In the upper-left corner, select **China (Hong Kong)** from the drop-down list.
2. Click the **Custom Images** tab.
3. Select **Snapshot ID** from the drop-down list in the search bar.
4. Enter *s-2xxxxxxxxxxxxxxxxxxx* in the search bar.
5. Click **Search**.

Find an image by calling an API operation

You can use OpenAPI Explorer or Alibaba Cloud CLI to call the DescribeImages operation and find a specific image. For more information about Alibaba Cloud CLI, see What is Alibaba Cloud CLI? This section describes how to use OpenAPI Explorer to call the API operation and find a specific image.

1. Go to OpenAPI Explorer.
2. Select a region from the **RegionId** drop-down list.
3. (Optional)Set other parameters such as ImageName and ImageId.

   > **Note** Image IDs are named in accordance with the following rules:
   >
   > - IDs of public images are named after the operating system version numbers, architectures, languages, and release dates. For example, win2008r2_64_ent_sp1_en-us_40G_alibase_20190318.vhd indicates that the image runs Windows Server 2008 R2 Enterprise 64-bit (English).
   > - IDs of custom images and Alibaba Cloud Marketplace images start with m.
   > - IDs of shared images are the same as those of the source custom images.

4. Click **Submit Request**.
5. Click the **Debugging Result** tab.

   If the target image is found, image information such as the image ID, description, and operating system is displayed on the **Debugging Result** tab. For more information, see DescribeImages.

What's next

After you find the target image, you may want to perform the following operations:

- Create an instance. For more information, see Create an instance by using the provided

wizard.

- Share the image. For more information, see Share or unshare custom images.
- Copy the image. For more information, see Copy custom images.
- Export the image. For more information, see Export a custom image.
- Delete the image. For more information, see Delete a custom image.
- Modify the description of the image. For more information, see Modify custom images.

Related information

- DescribeImages

4.Public image

4.1. Overview

This topic provides an overview of the public images provided by Alibaba Cloud, including Aliyun Linux images, third-party images, and open-source images. Public images are fully licensed to provide a secure and stable operating environment for applications on ECS instances.

Aliyun Linux Windows Server CentOS Ubuntu Debian CoreOS Red Hat OpenSUSE

Types of public images

The following table describes two types of public images provided by Alibaba Cloud. Windows Server and Red Hat Enterprise Linux images cannot be used free of charge. However, you can use other public images for free to create ECS instances. For more information, see Image overview.

Type	Description	Technical support
Aliyun Linux images	Aliyun Linux images are custom, proprietary operating systems provided by Alibaba Cloud to launch ECS instances. Aliyun Linux images are fully tested to guarantee its security, stability, and normal startup and operation.	Alibaba Cloud provides technical support for problems that occur when you use Aliyun Linux images.
Third-party images and open-source images	Third-party and open-source images are fully tested and released by Alibaba Cloud to guarantee their security, stability, and normal startup and operation. Such images include: • Windows: Windows Server • Linux: Ubuntu, CentOS, Red Hat Enterprise Linux, Debian, SUSE Linux, FreeBSD, and CoreOS	We recommend that you contact the corresponding operating system vendors or open-source communities for technical support. Alibaba Cloud also provides information about image- and system-related problems.

Aliyun Linux images

Aliyun Linux is a Linux public image independently developed by Alibaba Cloud. The following table describes the versions of Aliyun Linux images.

Operating system	Version	Description

Operating system	Version	Description
Aliyun Linux 2	Aliyun Linux 2.1903 64-bit	A next-generation operating system that supports various Alibaba Cloud instance types including ECS Bare Metal Instances. By default, Aliyun Linux 2 is also equipped with Alibaba Cloud CLI and other software packages. If you want to replace other Linux distributions with Aliyun Linux 2, you can select Public Image and then Aliyun Linux 2 when you create an ECS instance, or replace the system disk of an existing ECS instance with Aliyun Linux 2. For more information, see Aliyun Linux 2.

Third-party images and open-source images

Alibaba Cloud releases and updates public images of third-party and open-source image vendors on a regular basis. For more information, see Release notes. You can view all the available public images on the **Public Images** page in the corresponding region in the ECS console. For more information, see Find an image.

The following tables describe the versions of third-party and open-source public images for Windows and Linux provided by Alibaba Cloud.

- Windows images

Operating system	Version
Windows Server 2019	○ Windows Server 2019 Datacenter edition 64-bit (Chinese) ○ Windows Server 2019 Datacenter edition 64-bit (English)
Windows Server 2016	○ Windows Server 2016 Datacenter edition 64-bit (Chinese) ○ Windows Server 2016 Datacenter edition 64-bit (English)
Windows Server 2012	○ Windows Server 2012 R2 Datacenter edition 64-bit (Chinese) ○ Windows Server 2012 R2 Datacenter edition 64-bit (English)
Windows Server Version **** (Semi-Annual Channel)	○ Windows Server Version **** Datacenter edition 64-bit (Chinese) ○ Windows Server Version **** Datacenter edition 64-bit (English) The asterisks (****) indicate the latest version number of the Semi-Annual Channel release.

> **Note** From January 14, 2020, Microsoft stopped providing support for Windows Server 2008 and Windows Server 2008 R2 operating systems. Therefore, Alibaba Cloud no longer provides technical support for ECS instances that use the preceding operating systems. If you have ECS instances that use the preceding operating systems, upgrade them to Windows Server 2012 or later in a timely manner.

- Linux images

Operating system	Version
CentOS	○ CentOS 8.0 64-bit ○ CentOS 7.7 64-bit ○ CentOS 7.6 64-bit ○ CentOS 7.5 64-bit ○ CentOS 7.4 64-bit ○ CentOS 7.3 64-bit ○ CentOS 7.2 64-bit ○ CentOS 6.10 64-bit ○ CentOS 6.9 64-bit ○ CentOS 6.8 32-bit **Note** If you are using a 32-bit operating system, select instance types that have a memory capacity less than or equal to 4 GiB. For more information, see Select an image.
CoreOS	○ CoreOS 2303.3.0 64-bit ○ CoreOS 2247.6.0 64-bit ○ CoreOS 2023.4.0 64-bit ○ CoreOS 1745.7.0 64-bit
Debian	○ Debian 10.2 64-bit ○ Debian 9.11 64-bit ○ Debian 9.9 64-bit ○ Debian 9.8 64-bit ○ Debian 9.6 64-bit ○ Debian 8.11 64-bit ○ Debian 8.9 64-bit
FreeBSD	FreeBSD 11.2 64-bit
OpenSUSE	○ openSUSE 15.1 64-bit ○ openSUSE 42.3 64-bit

Operating system	Version
Red Hat	○ Red Hat Enterprise Linux 8.1 64-bit ○ Red Hat Enterprise Linux 8 64-bit ○ Red Hat Enterprise Linux 7.7 64-bit ○ Red Hat Enterprise Linux 7.6 64-bit ○ Red Hat Enterprise Linux 7.5 64-bit ○ Red Hat Enterprise Linux 7.4 64-bit ○ Red Hat Enterprise Linux 6.10 64-bit ○ Red Hat Enterprise Linux 6.9 64-bit Note You must check whether a Red Hat image is supported by the instance family before you use the Red Hat image. For more information, see Which instance families do Red Hat Enterprise Linux (RHEL) images support?.
SUSE Linux	○ SUSE Linux Enterprise Server 15 SP1 64-bit ○ SUSE Linux Enterprise Server 12 SP4 64-bit ○ SUSE Linux Enterprise Server 12 SP2 64-bit ○ SUSE Linux Enterprise Server 11 SP4 64-bit
Ubuntu	○ Ubuntu 18.04 64-bit ○ Ubuntu 16.04 64-bit ○ Ubuntu 16.04 32-bit ○ Ubuntu 14.04 64-bit ○ Ubuntu 14.04 32-bit Note If you are using a 32-bit operating system, select instance types that have a memory capacity less than or equal to 4 GiB. For more information, see Select an image.

4.2. Release notes

This topic describes the updates to the features of ECS public images in the order in which they were released

Background information

- Unless otherwise stated, the released updates apply to all Alibaba Cloud regions where ECS is provided.
- Public images are applicable to most instance families. For information about instance families that can use only specified public images, see the following sections:
  - Trusted images
  - AMD images

CentOS

Release	Image ID	Release date	Description
CentOS 8.2	*centos_8_2_x64_20G_alibase_20200824.vhd*	2020-08-24	• Kernel version: 4.18.0-193.14.2.el8_2.x86_64. • Changes: updated to include the latest patches.
CentOS 7.8	*centos_7_8_x64_20G_alibase_20200817.vhd*	2020-08-17	• Kernel version: 3.10.0-1127.18.2.el7.x86_64. • Changes: updated to include the latest patches.
CentOS 6.10	*centos_6_10_x64_20G_alibase_20200817.vhd*	2020-08-17	• Kernel version: 2.6.32-754.31.1.el6.x86_64. • Changes: updated to include the latest patches.
CentOS 8.2	*centos_8_2_x64_20G_alibase_20200717.vhd*	2020-07-17	• Kernel version: 4.18.0-193.6.3.el8_2.x86_64. • Changes: updated to include the latest patches.
CentOS 7.8	*centos_7_8_x64_20G_alibase_20200717.vhd*	2020-07-17	• Kernel version: 3.10.0-1127.13.1.el7.x86_64. • Changes: enabled IPv6 by default.
CentOS 6.10	*centos_6_10_x64_20G_alibase_20200717.vhd*	2020-07-17	• Kernel version: 2.6.32-754.30.2.el6.x86_64. • Changes: enabled IPv6 by default.
CentOS 7.8	*centos_7_8_x64_20G_alibase_20200622.vhd*	2020-06-22	• Kernel version: 3.10.0-1127.10.1.el7.x86_64. • Changes: updated to include the latest patches.
CentOS 8.2	*centos_8_2_x64_20G_alibase_20200616.vhd*	2020-06-16	• Kernel version: 4.18.0-193.el8.x86_64. • Changes: updated to include the latest patches.

Release	Image ID	Release date	Description
CentOS 6.10	*centos_6_10_x64_20G_alibase_20200616.vhd*	2020-06-16	• Kernel version: 2.6.32-754.30.2.el6.x86_64. • Changes: updated to include the latest patches.
CentOS 8.1	*centos_8_1_x64_20G_alibase_20200519.vhd*	2020-05-19	• Kernel version: 4.18.0-147.8.1.el8_1.x86_64. • Changes: updated to include the latest patches.
CentOS 7.8	*centos_7_8_x64_20G_alibase_20200519.vhd*	2020-05-19	• Kernel version: 3.10.0-1127.8.2.el7.x86_64. • Changes: updated to include the latest patches.
CentOS 6.10	*centos_6_10_x64_20G_alibase_20200519.vhd*	2020-05-19	• Kernel version: 2.6.32-754.29.2.el6.x86_64. • Changes: updated to include the latest patches.
CentOS 8.1	*centos_8_1_x64_20G_alibase_20200426.vhd*	2020-04-26	• Kernel version: 4.18.0-147.8.1.el8_1.x86_64. • Changes: updated to include the latest operating system patches.
CentOS 7.7	*centos_7_7_x64_20G_alibase_20200426.vhd*	2020-04-26	• Kernel version: 3.10.0-1062.18.1.el7.x86_64. • Changes: updated to include the latest operating system patches.
CentOS 6.10	*centos_6_10_x64_20G_alibase_20200426.vhd*	2020-04-26	• Kernel version: 2.6.32-754.28.1.el6.x86_64. • Changes: updated to include the latest operating system patches.
CentOS 8.1	*centos_8_1_x64_20G_alibase_20200329.vhd*	2020-03-29	• Kernel version: 4.18.0-147.5.1.el8_1.x86_64. • Changes: updated to include the latest operating system patches.

Release	Image ID	Release date	Description
CentOS 7.7	*centos_7_7_x64_20G_alibase_20200329.vhd*	2020-03-29	• Kernel version: 3.10.0-1062.18.1.el7.x86_64. • Changes: ◦ Updated to include the latest operating system patches ◦ Upgraded cloud-init to version 19.1 Note cloud-init dynamically generates network configurations. For more information about custom network configurations, see the "Optional. Customize network configuration" section in Install cloud-init.
CentOS 6.10	*centos_6_10_x64_20G_alibase_20200319.vhd*	2020-03-19	• Kernel version: 2.6.32-754.28.1.el6.x86_64. • Changes: updated to include the latest operating system patches.

Release	Image ID	Release date	Description

CentOS 8.0	*centos_8_0_x64_20G_alibase_20200218.vhd*	2020-02-18	• Kernel version: 4.18.0-147.5.1.el8_1.x86_64.
			• Changes:
			  ◦ Updated to include the latest operating system patches
			  ◦ Added the EPEL source and Chinese Simplified (zh-CN) language pack
			  ◦ Enabled IPv6 by default
			• Known issue: The system version of ECS instances created from the centos_8_0_x64_20G_alibase_20200218.vhd public image is CentOS 8.1. For more information about the issue, see the ""CentOS 8.0: The version update of the image in the public image list leads to the change of public image version number of created instances.

CentOS 7.7	*centos_7_7_x64_20G_alibase_20200220.vhd*	2020-02-20	• Kernel version: 3.10.0-1062.12.1.el7.x86_64. • Changes: updated to include the latest operating system patches.
CentOS 6.10	*centos_6_10_x64_20G_alibase_20200214.vhd*	2020-02-14	• Kernel version: 2.6.32-754.27.1.el6.x86_64. • Changes: updated to include the latest operating system patches.

Release	Image ID	Release date	Description
CentOS 6.10	*centos_6_10_x64_20G_alibase_20200103.vhd*	2020-01-03	• Kernel version: 2.6.32-754.25.1.el6.x86_64. • Changes: updated to include the latest operating system patches. • Applicable regions: China (Beijing), US (Virginia), China (Hong Kong), China (Zhangjiakou-Beijing Winter Olympics), China (Hohhot), China (Hangzhou), China (Qingdao), China (Chengdu), and Singapore.
CentOS 7.7	*centos_7_7_x64_20G_alibase_20191225.vhd*	2019-12-25	• Kernel version: 3.10.0-1062.9.1.el7.x86_64. • Changes: updated to include the latest operating system patches.
CentOS 8.0	*centos_8_0_x64_20G_alibase_20191225.vhd*	2019-12-25	• Kernel version: 4.18.0-80.11.2.el8_0.x86_64. • Changes: ◦ Updated to include the latest operating system patches ◦ Upgraded cloud-init to version 19.1 Note cloud-init dynamically generates network configurations. For more information about custom network configurations, see the "Optional. Customize network configuration" section in Install cloud-init.

Release	Image ID	Release date	Description
CentOS 6.10	*centos_6_10_x64_20G_alibase_20191223.vhd*	2019-12-25	• Kernel version: 2.6.32-754.24.3.el6.x86_64. • Changes: updated to include the latest operating system patches.
CentOS 7.7	*centos_7_7_64_20G_alibase_20191008.vhd*	2019-10-8	• Kernel version: 3.10.0-1062.1.2.el7.x86_64. • Changes: new release.
CentOS 7.6	*centos_7_06_64_20G_alibase_20190711.vhd*	2019-7-11	• Kernel version: 3.10.0-957.21.3.el7.x86_64. • Changes: updated to include the latest operating system patches.
CentOS 6.10	*centos_6_10_64_20G_alibase_20190709.vhd*	2019-7-9	• Kernel version: 2.6.32-754.17.1.el6.x86_64. • Changes: updated to include the latest operating system patches.
CentOS 6.10	*centos_6_10_64_20G_alibase_20190621.vhd*	2019-6-21	• Kernel version: 2.6.32-754.15.3.el6.x86_64. • Changes: updated to include the latest operating system patches and fixed the CVE-2019-11477 vulnerability.

CentOS 7.6	*centos_7_06_64_20G_alibase_20190619.vhd*	2019-6-19	• Kernel version: 3.10.0-957.21.3.el7.x86_64.
			• Changes:
			  ◦ Updated to include the latest patches and fixed the CVE-2019-11477 vulnerability
			  ◦ Set the default CPU mode to performance

CentOS 7.6	*centos_7_06_64_20G_alibase_20190218.vhd*	2019-2-18	• Kernel version: 3.10.0-957.5.1.el7.x86_64. • Changes: updated to include the latest operating system patches.

Release	Image ID	Release date	Description
CentOS 7.6	*centos_7_05_64_20G_alibase_20181212.vhd*	2018-12-12	• Kernel version: 3.10.0-957.1.3.el7.x86_64. • Changes: updated to include the latest operating system patches.
CentOS 7.5	*centos_7_05_64_20G_alibase_20181210.vhd*	2018-12-10	• Kernel version: 3.10.0-862.3.3.el7.x86_64. • Changes: ◦ Updated to include the latest operating system patches ◦ Upgraded the cloud-init version ◦ Enabled the chrony time synchronization service ◦ Disabled password authentication by default ◦ Set GRUB_TIMEOUT to 1

Debian

Release	Image ID	Release date	Description
Debian 10.5	*debian_10_5_x64_20G_alibase_20200819.vhd*	2020-08-19	• Kernel version: 4.19.0-10-amd64 • Changes: ◦ Updated to include the latest patches ◦ Updated network interface controller (NIC) configurations and configured DHCP for eight NICs by default
Debian 9.13	*debian_9_13_x64_20G_alibase_20200819.vhd*	2020-08-19	• Kernel version: 4.9.0-13-amd64 • Changes: ◦ Updated to include the latest patches ◦ Updated NIC configurations and configured DHCP for eight NICs by default

Release	Image ID	Release date	Description

Debian 9.13	*debian_9_13_x64_20G_alibase_20200730.vhd*	2020-07-30	• Kernel version: 4.9.0-13-amd64
			• Changes:
			  ◦ Updated to include the latest patches
			  ◦ Enabled IPv6 by default

Debian 10.4	*debian_10_4_x64_20G_alibase_20200717.vhd*	2020-07-17	• Kernel version: 4.19.0-10-amd64 • Changes: updated to include the latest patches
Debian 10.4	*debian_10_4_x64_20G_alibase_20200622.vhd*	2020-06-22	• Kernel version: 4.19.0-9-amd64 • Changes: updated to include the latest patches
Debian 9.12	*debian_9_12_x64_20G_alibase_20200622.vhd*	2020-06-22	• Kernel version: 4.9.0-12-amd64 • Changes: updated to include the latest patches
Debian 10.4	*debian_10_4_x64_20G_alibase_20200519.vhd*	2020-05-19	• Kernel version: 4.19.0-9-amd64 • Changes: updated to include the latest patches
Debian 9.12	*debian_9_12_x64_20G_alibase_20200519.vhd*	2020-05-19	• Kernel version: 4.9.0-12-amd64 • Changes: updated to include the latest patches
Debian 10.3	*debian_10_3_x64_20G_alibase_20200426.vhd*	2020-04-26	• Kernel version: 4.19.0-8-amd64 • Changes: updated to include the latest operating system patches
Debian 9.12	*debian_9_12_x64_20G_alibase_20200426.vhd*	2020-04-26	• Kernel version: 4.9.0-12-amd64 • Changes: updated to include the latest operating system patches

Release	Image ID	Release date	Description

Debian 10.3	*debian_10_3_x64_20G_alibase_20200329.vhd*	2020-03-29	• Kernel version: 4.19.0-8-amd64
			• Changes:
			  ◦ Updated to include the latest operating system patches
			  ◦ Enabled IPv6 by default

Debian 9.12	*debian_9_12_x64_20G_alibase_20200324.vhd*	2020-03-24	• Kernel version: 4.9.0-12-amd64 • Changes: updated to include the latest operating system patches
Debian 9.12	*debian_9_12_x64_20G_alibase_20200220.vhd*	2020-02-20	• Kernel version: 4.9.0-12-amd64 • Changes: updated to include the latest operating system patches
Debian 10.3	*debian_10_3_x64_20G_alibase_20200218.vhd*	2020-02-18	• Kernel version: 4.19.0-8-amd64 • Changes: updated to include the latest operating system patches
Debian 9.11	*debian_9_11_x64_20G_alibase_20191225.vhd*	2019-12-25	• Kernel version: 4.9.0-11-amd64 • Changes: updated to include the latest operating system patches

Release	Image ID	Release date	Description

Debian 10.2	*debian_10_2_x64_20G_alibase_20191223.vhd*	2019-12-24	• Kernel version: 4.19.0-6-amd64
			• Changes:
			  ◦ Updated to include the latest operating system patches
			  ◦ Upgraded cloud-init to version 19.1
			Note cloud-init dynamically generates network configurations. For more information about custom network configurations, see the "Optional. Customize network configuration" section in Install cloud-init.

Debian 9.9	*debian_9_09_64_20G_alibase_20190702.vhd*	2019-7-2	• Kernel version: 4.9.0-9-amd64 • Changes: updated to include the latest operating system patches
Debian 9.9	*debian_9_09_64_20G_alibase_20190510.vhd*	2019-5-10	• Kernel version: 4.9.0-9-amd64 • Changes: updated to include the latest operating system patches

Debian 8.11	*11_64_20G_alibase_20190311.vhd*	2019-3-11	• Kernel version: 3.16.0-7-amd64
			• Changes:
			  ◦ Updated to include the latest operating system patches
			  ◦ Fixed invalid apt source configurations in Debian 8.9

Debian 9.8	*debian_9_08_64_20G_alibase_20190225.vhd*	2019-2-25	• Kernel version: 4.9.0-8-amd64 • Changes: updated to include the latest operating system patches

Release	Image ID	Release date	Description
Debian 9.6	*debian_9_06_64_20G_alibase_20190103.vhd*	2019-1-3	• Kernel version: 4.9.0-8-amd64 • Changes: enabled the systemd-networkd service

Debian 9.6	*debian_9_06_64_20G_alibase_20181212.vhd*	2018-12-12	• Kernel version: 4.9.0-8-amd64
			• Changes:
			  ◦ Updated to include the latest operating system patches
			  ◦ Upgraded the cloud-init version
			  ◦ Enabled the chrony time synchronization service
			  ◦ Set GRUB_TIMEOUT to 1
			• Known issues: classic network configuration issues

FreeBSD

Release	Image ID	Release date	Description
FreeBSD 11.3	*freebsd_11_3_x64_30G_alibase_20200803.vhd*	2020-08-03	• Kernel version: 11.3-RELEASE • Changes: updated to include the latest patches
FreeBSD 11.3	*freebsd_11_3_x64_20G_alibase_20200420.vhd*	2020-04-20	• Kernel version: 11.3-RELEASE • Changes: updated to include the latest patches

FreeBSD 11.2	*freebsd_11_02_64_30G_alibase_20190806.vhd*	2019-8-6	• Kernel version: 11.2-RELEASE
			• Changes:
			  ◦ Fixed the clock offset issue
			  ◦ Fixed the error that causes the 30 GiB system disk to fail to be created

Ubuntu

Release	Image ID	Release date	Description
Ubuntu 18.04	*ubuntu_18_04_x64_20G_alibase_20200817.vhd*	2020-08-17	• Kernel version: 4.15.0-112-generic • Changes: updated to include the latest patches
Ubuntu 16.04	*ubuntu_16_04_x64_20G_alibase_20200817.vhd*	2020-08-17	• Kernel version: 4.4.0-187-generic • Changes: updated to include the latest patches
Ubuntu 18.04	*ubuntu_18_04_x64_20G_alibase_20200717.vhd*	2020-07-17	• Kernel version: 4.15.0-111-generic • Changes: updated to include the latest patches
Ubuntu 16.04	*ubuntu_16_04_x64_20G_alibase_20200717.vhd*	2020-07-17	• Kernel version: 4.4.0-185-generic • Changes: updated to include the latest patches
Ubuntu 18.04	*ubuntu_18_04_x64_20G_alibase_20200618.vhd*	2020-06-18	• Kernel version: 4.15.0-106-generic • Changes: updated to include the latest patches
Ubuntu 16.04	*ubuntu_16_04_x64_20G_alibase_20200618.vhd*	2020-06-18	• Kernel version: 4.4.0-184-generic • Changes: updated to include the latest patches
Ubuntu 20.04	*ubuntu_20_04_x64_20G_alibase_20200522.vhd*	2020-05-22	• New release • Kernel version: 5.4.0-31-generic
Ubuntu 16.04	*ubuntu_16_04_x64_20G_alibase_20200522.vhd*	2020-05-22	• Kernel version: 4.4.0-179-generic • Changes: updated to include the latest operating system patches

Release	Image ID	Release date	Description
Ubuntu 18.04	*ubuntu_18_04_x64_20G_alibase_20200521.vhd*	2020-05-21	• Kernel version: 4.15.0-101-generic • Changes: updated to include the latest operating system patches
Ubuntu 18.04	*ubuntu_18_04_x64_20G_alibase_20200426.vhd*	2020-04-26	• Kernel version: 4.15.0-96-generic • Changes: updated to include the latest operating system patches
Ubuntu 16.04	*ubuntu_16_04_x64_20G_alibase_20200426.vhd*	2020-04-26	• Kernel version: 4.4.0-177-generic • Changes: updated to include the latest operating system patches

Ubuntu 18.04	*ubuntu_18_04_x64_20G_alibase_20200329.vhd*	2020-03-29	• Kernel version: 4.15.0-91-generic
			• Changes:
			  ◦ Updated to include the latest operating system patches
			  ◦ Enabled IPv6 by default

Ubuntu 16.04	*ubuntu_16_04_x64_20G_alibase_20200319.vhd*	2020-03-19	• Kernel version: 4.4.0-176-generic • Changes: updated to include the latest operating system patches
Ubuntu 18.04	*ubuntu_18_04_x64_20G_alibase_20200220.vhd*	2020-02-20	• Kernel version: 4.15.0-88-generic • Changes: updated to include the latest operating system patches
Ubuntu 16.04	*ubuntu_16_04_x64_20G_alibase_20200220.vhd*	2020-02-20	• Kernel version: 4.4.0-174-generic • Changes: updated to include the latest operating system patches

Release	Image ID	Release date	Description
Ubuntu 18.04	*ubuntu_18_04_x64_20G_alibase_20191225.vhd*	2019-12-25	• Kernel version: 4.15.0-72-generic • Changes: updated to include the latest operating system patches
Ubuntu 16.04	*ubuntu_16_04_x64_20G_alibase_20191225.vhd*	2019-12-25	• Kernel version: 4.4.0-170-generic • Changes: updated to include the latest operating system patches
Ubuntu 18.04	*ubuntu_18_04_64_20G_alibase_20190624.vhd*	2019-6-24	• Kernel version: 4.15.0-52-generic • Changes: updated to include the latest operating system patches and fixed the CVE-2019-11477 vulnerability
Ubuntu 16.04	*ubuntu_16_04_64_20G_alibase_20190620.vhd*	2019-6-20	• Kernel version: 4.4.0-151-generic • Changes: updated to include the latest operating system patches and fixed the CVE-2019-11477 vulnerability
Ubuntu 16.04	*ubuntu_16_04_64_20G_alibase_20190513.vhd*	2019-5-13	• Kernel version: 4.4.0-146-generic • Changes: updated to include the latest operating system patches

Ubuntu 18.04	*ubuntu_18_04_64_20G_alibase_20190509.vhd*	2019-5-9	• Kernel version: 4.15.0-48-generic
			• Changes:
			  ◦ Upgraded cloud-init to speed up boot time
			  ◦ Updated to include the latest operating system patches

Release	Image ID	Release date	Description
Ubuntu 16.04	*ubuntu_16_04_64_20G_alibase_20190301.vhd*	2019-3-1	• Kernel version: 4.4.0-142-generic • Changes: updated to include the latest operating system patches
Ubuntu 18.04	*ubuntu_18_04_64_20G_alibase_20190223.vhd*	2019-2-23	• Kernel version: 4.15.0-45-generic • Changes: updated to include the latest operating system patches
Ubuntu 18.04	*ubuntu_18_04_64_20G_alibase_20181212.vhd*	2018-12-12	• Kernel version: 4.15.0-42-generic • Changes: ◦ Updated to include the latest operating system patches ◦ Upgraded the cloud-init version ◦ Enabled the chrony time synchronization service ◦ Set GRUB_TIMEOUT to 1

CoreOS

Note According to the end-of-life announcement for CoreOS Container Linux from the Fedora CoreOS community, updates are no longer provided for CoreOS Container Linux as of May 26, 2020. In view of this, Alibaba Cloud makes the following announcements:

- As of May 26, 2020, Alibaba Cloud no longer provides technical support for ECS instances that use the CoreOS Container Linux operating system. However, you can still use existing ECS instances that run this operating system.
- You can still obtain CoreOS Container Linux images from Alibaba Cloud before September 30, 2020. After September 30, 2020, you will be unable to use CoreOS Container Linux public images provided by Alibaba Cloud to create new ECS instances.
- As of May 26, 2020, you can still use the CoreOS Container Linux operating system that has already been installed. However, no security patches are available because the operating system has reached its end of life. For security concerns, Alibaba Cloud recommends that you do not use CoreOS Container Linux images any longer.
- The Fedora CoreOS community recommends that you use Fedora CoreOS as a replacement of CoreOS Container Linux. Alibaba Cloud will also bring Fedora CoreOS public images online soon.

Release	Image ID	Release date	Description
CoreOS 2345_3.0	*coreos_2345_3.0_x64_30G_alibase_20200519.vhd*	2020-05-19	• Kernel version: 4.19.106-coreos • Changes: updated to include the latest patches
CoreOS 2345_3.0	*coreos_2345_3.0_x64_30G_alibase_20200423.vhd*	2020-04-23	• Kernel version: 4.19.106-coreos • Changes: updated to include the latest operating system patches
CoreOS 2345_3.0	*coreos_2345_3.0_x64_30G_alibase_20200325.vhd*	2020-03-25	• Kernel version: 4.19.106-coreos • Changes: updated to include the latest operating system patches
CoreOS 2303_4.0	*coreos_2303_4.0_x64_30G_alibase_20200217.vhd*	2020-02-17	• Kernel version: 4.19.95-coreos • Changes: updated to include the latest operating system patches
CoreOS 2303_3.0	*coreos_2303_3_x64_30G_alibase_20191223.vhd*	2019-12-23	• Kernel version: 4.19.86-coreos • Changes: updated to include the latest operating system patches

openSUSE

Release	Image ID	Release date	Description
openSUSE 15.2	*opensuse_15_2_x64_20G_alibase_20200818.vhd*	2020-08-18	• Kernel version: 5.3.18-lp152.33-default • Updated to include the latest patches
openSUSE 15.2	*opensuse_15_2_x64_20G_alibase_20200717.vhd*	2020-07-17	• Kernel version: 5.3.18-lp152.20.7-default • Updated to include the latest patches
openSUSE 15.1	*opensuse_15_1_x64_20G_alibase_20200623.vhd*	2020-06-23	• Kernel version: 4.12.14-lp151.28.52-default • Updated to include the latest patches

Release	Image ID	Release date	Description
openSUSE 15.1	*opensuse_15_1_x64_20G_alibase_20200520.vhd*	2020-05-20	• Kernel version: 4.12.14-lp151.28.48-default • Updated to include the latest patches
openSUSE 15.1	*opensuse_15_1_x64_20G_alibase_20200426.vhd*	2020-04-26	• Kernel version: 4.12.14-lp151.28.48-default • Changes: ◦ Enabled IPv6 by default ◦ Updated to include the latest operating system patches
openSUSE 15.1	*opensuse_15_1_x64_20G_alibase_20200331.vhd*	2020-03-31	• Kernel version: 4.12.14-lp151.28.44-default • Changes: updated to include the latest operating system patches
openSUSE 15.1	*opensuse_15_1_x64_20G_alibase_20200222.vhd*	2020-02-22	• Kernel version: 4.12.14-lp151.28.36-default • Changes: updated to include the latest operating system patches
openSUSE 15.1	*opensuse_15_1_x64_20G_alibase_20191219.vhd*	2019-12-19	• Kernel version: 4.12.14-lp151.28.36-default • Changes: ◦ Updated to include the latest operating system patches ◦ Upgraded cloud-init to version 19.1

SUSE Linux Enterprise Server

Release	Image ID	Release date	Description
SUSE Linux Enterprise Server 15 SP2	*sles_15_sp2_x64_20G_alibase_20200820.vhd*	2020-08-20	Updated to include the latest patches

Release	Image ID	Release date	Description
SUSE Linux Enterprise Server 12 SP5	*sles_12_sp5_x64_20G_alibase_20200819.vhd*	2020-08-19	Updated to include the latest patches
SUSE Linux Enterprise Server 15 SP1	*sles_15_sp1_x64_20G_alibase_20200717.vhd*	2020-07-17	Updated to include the latest patches
SUSE Linux Enterprise Server 12 SP5	*sles_12_sp5_x64_20G_alibase_20200717.vhd*	2020-07-17	Updated to include the latest patches
SUSE Linux Enterprise Server 15 SP1	*sles_15_sp1_x64_20G_alibase_20200617.vhd*	2020-06-17	Updated to include the latest patches
SUSE Linux Enterprise Server 12 SP5	*sles_12_sp5_x64_20G_alibase_20200617.vhd*	2020-06-17	Updated to include the latest patches
SUSE Linux Enterprise Server 15 SP1	*sles_15_sp1_x64_20G_alibase_20200520.vhd*	2020-05-20	Updated to include the latest patches
SUSE Linux Enterprise Server 12 SP5	*sles_12_sp5_x64_20G_alibase_20200520.vhd*	2020-05-20	Updated to include the latest patches
SUSE Linux Enterprise Server 15 SP1	*sles_15_sp1_x64_20G_alibase_20200426.vhd*	2020-04-26	• Enabled IPv6 by default • Updated to include the latest patches
SUSE Linux Enterprise Server 12 SP5	*sles_12_sp5_x64_20G_alibase_20200426.vhd*	2020-04-26	• Enabled IPv6 by default • Updated to include the latest patches
SUSE Linux Enterprise Server 15 SP1	*sles_15_sp1_x64_20G_alibase_20200329.vhd*	2020-03-29	Updated to include the latest patches

Release	Image ID	Release date	Description
SUSE Linux Enterprise Server 12 SP4	*sles_12_sp4_x64_20G_alibase_20200319.vhd*	2020-03-19	Updated to include the latest patches
SUSE Linux Enterprise Server 12 SP4	*sles_12_sp4_x64_20G_alibase_20200227.vhd*	2020-02-27	Updated to include the latest patches
SUSE Linux Enterprise Server 15 SP1	*sles_15_sp1_x64_20G_alibase_20200218.vhd*	2020-02-18	Updated to include the latest patches
SUSE Linux Enterprise Server 15 SP1	*sles_15_sp1_x64_20G_alibase_20200107.vhd*	2020-01-07	New release

Trusted images

Trusted images are applicable to only the following instance families and dedicated host types:

- Instance families: ecs.g6t and ecs.c6t
- Dedicated host types: ddh.g6t and ddh.c6t

Release	Image ID	Release date	Description

CentOS 7.8	*centos_7_8_tpm_x64_20G_alibase_20200810.vhd*	2020-08-10	• Released CentOS 7.8 trusted images.
			• Installed the following GRUB 2 and TPM-related RPM packages on trusted images:
			  ◦ grub2 (trust-customized version)
			  ◦ tpm2-abrmd
			  ◦ tpm2-tss
			  ◦ tpm2-tools
			• GRUB 2 packages are trust-customized. To enable trusted boot, we recommend that you do not upgrade GRUB 2 on your own.

AMD images

AMD images are applicable to only the ecs.ebmg6a, ecs.ebmc6a, and ecs.ebmr6a instance families.

Release	Image ID	Release date	Description
Ubuntu 18.04	*ubuntu_18_04_amd_x64_20G_alibase_20200804.vhd*	2020-08-04	• Released Ubuntu 18.04 AMD images. • Applicable regions: China (Beijing), China (Ulanqab), China (Shenzhen), China (Shanghai), China (Hangzhou), and China (Chengdu).

Windows Server 2012

Release	Image ID	Release date	Description
Windows Server 2012 R2 Datacenter Edition	• Chinese version: *win2012r2_9600_x64_dtc_zh-cn_40G_alibase_20200814.vhd* • English version: *win2012r2_9600_x64_dtc_en-us_40G_alibase_20200814.vhd*	2020-08-14	• Updated to include the KB4571703 and KB4569753 operating system patches released in August 2020. • Fixed the CVE-2020-1472, CVE-2020-1464, CVE-2020-1554, CVE-2020-1509, CVE-2020-1567, and CVE-2020-1380 vulnerabilities.
Windows Server 2012 R2 Datacenter Edition	• Chinese version: *win2012r2_9600_x64_dtc_zh-cn_40G_alibase_20200723.vhd* • English version: *win2012r2_9600_x64_dtc_en-us_40G_alibase_20200723.vhd*	2020-07-23	Updated to include the KB4566425, KB4565541, and KB4565635 operating system patches released in July 2020.
Windows Server 2012 R2 Datacenter Edition	• Chinese version: *win2012r2_9600_x64_dtc_zh-cn_40G_alibase_20200615.vhd* • English version: *win2012r2_9600_x64_dtc_en-us_40G_alibase_20200615.vhd*	2020-06-15	• Updated to include the KB4561666 operating system patch released in June 2020. • Fixed the CVE-2020-1301, CVE-2020-1239, CVE-2020-1300, CVE-2020-1281, and CVE-2020-1260 vulnerabilities.
Windows Server 2012 R2 Datacenter Edition	• Chinese version: *win2012r2_9600_x64_dtc_zh-cn_40G_alibase_20200516.vhd* • English version: *win2012r2_9600_x64_dtc_en-us_40G_alibase_20200516.vhd*	2020-05-16	• Updated to include the KB4556846 operating system patch released in May 2020. • Fixed the CVE-2020-1153, CVE-2020-1112, CVE-2020-1174, and CVE-2020-1062 vulnerabilities.

Release	Image ID	Release date	Description
Windows Server 2012 R2 Datacenter Edition	• Chinese version: *win2012r2_9600_x64_dtc_zh-cn_40G_alibase_20200416.vhd* • English version: *win2012r2_9600_x64_dtc_en-us_40G_alibase_20200416.vhd*	2020-04-16	• Updated to include the KB4550961 operating system patch released in April 2020. • Added disk drives for the Windows Recovery mode. • Fixed the CVE-2020-1020, CVE-2020-0687, CVE-2020-0938, CVE-2020-0965, and CVE-2020-0968 vulnerabilities.
Windows Server 2012 R2 Datacenter Edition	• Chinese version: *win2012r2_9600_x64_dtc_zh-cn_40G_alibase_20200314.vhd* • English version: *win2012r2_9600_x64_dtc_en-us_40G_alibase_20200314.vhd*	2020-03-14	• Updated to include the operating system patches released in March 2020. • Fixed the CVE-2020-0684, CVE-2020-0881, and CVE-2020-0787 vulnerabilities.
Windows Server 2012 R2 Datacenter Edition	• Chinese version: *win2012r2_9600_x64_dtc_zh-cn_40G_alibase_20200213.vhd* • English version: *win2012r2_9600_x64_dtc_en-us_40G_alibase_20200213.vhd*	2020-02-13	• Updated to include the operating system patches released in February 2020. • Fixed the CVE-2020-0738, CVE-2020-0689, CVE-2020-0681, CVE-2020-0683, CVE-2020-0686, CVE-2020-0674, and CVE-2020-0706 vulnerabilities.
Windows Server 2012 R2 Datacenter Edition	• Chinese version: *win201202r2_9600_x64_dtc_zh-cn_40G_alibase_20200116.vhd* • English version: *win2012r2_9600_x64_dtc_en-us_40G_alibase_20200116.vhd*	2020-01-16	• Updated to include the operating system patches released in January 2020. • Fixed the CVE-2020-0609, CVE-2020-0625, CVE-2020-0611, and CVE-2020-0640 vulnerabilities.
Windows Server 2012 R2 Datacenter Edition	• Chinese version: *win2012r2_9600_x64_dtc_zh-cn_40G_alibase_20191218.vhd* • English version: *win2012r2_9600_x64_dtc_en-us_40G_alibase_20191218.vhd*	2019-12-18	Updated to include the security patches released in December 2019.
Windows Server 2012 R2 Datacenter Edition	• Chinese version: *win2012r2_64_dtc_9600_zh-cn_40G_alibase_20191012.vhd* • English version: *win2012r2_64_dtc_9600_en-us_40G_alibase_20191012.vhd*	2019-10-12	Updated to include the security patches released in October 2019.

Release	Image ID	Release date	Description
Windows Server 2012 R2 Datacenter Edition	• Chinese version: *win2012r2_64_dtc_9600_zh-cn_40G_alibase_20190816.vhd* • English version: *win2012r2_64_dtc_9600_en-us_40G_alibase_20190816.vhd*	2019-8-16	• Updated to include the latest operating system patches released in August 2019. • Fixed the CVE-2019-1181 and CVE-2019-1182 vulnerabilities.
Windows Server 2012 R2 Datacenter Edition	• Chinese version: *win2012r2_64_dtc_9600_zh-cn_40G_alibase_20190718.vhd* • English version: *win2012r2_64_dtc_9600_en-us_40G_alibase_20190718.vhd*	2019-7-18	• Updated to include the latest operating system patches released in July 2019. • Upgraded .NET Framework to version 4.8.
Windows Server 2012 R2 Datacenter Edition	• Chinese version: *win2012r2_64_dtc_9600_zh-cn_40G_alibase_20190523.vhd* • English version: *win2012r2_64_dtc_9600_en-us_40G_alibase_20190523.vhd*	2019-5-23	Updated to include the operating system patches released in May 2019.
Windows Server 2012 R2 Datacenter Edition	• Chinese version: *win2012r2_64_dtc_9600_zh-cn_40G_alibase_20190318.vhd* • English version: *win2012r2_64_dtc_9600_en-us_40G_alibase_20190318.vhd*	2019-3-18	Updated to include the operating system patches released in March 2019.
Windows Server 2012 R2 Datacenter Edition	• Chinese version: *win2012r2_64_dtc_9600_zh-cn_40G_alibase_20181220.vhd* • English version: *win2012r2_64_dtc_9600_en-us_40G_alibase_20181220.vhd*	2018-12-20	• Updated to include the KB4471320 security patch released in December 2018. You must update Windows clients by using the latest patches to establish RDP connections. • Upgraded .NET Framework to version 4.7.2. • Used the Sysprep tool to generalize the image.

Windows Server 2016

Release	Image ID	Release date	Description
Windows Server 2016 Datacenter Edition	• Chinese version: *win2016_1607_x64_dtc_zh-cn_40G_alibase_20200814.vhd* • English version: *win2016_1607_x64_dtc_en-us_40G_alibase_20200814.vhd*	2020-08-14	• Updated to include the KB4571694 and KB4569746 operating system patches released in August 2020. • Fixed the CVE-2020-1472, CVE-2020-1464, CVE-2020-1554, CVE-2020-1509, CVE-2020-1567, and CVE-2020-1380 vulnerabilities.
Windows Server 2016 Datacenter Edition	• Chinese version: *win2016_1607_x64_dtc_zh-cn_40G_alibase_20200723.vhd* • English version: *win2016_1607_x64_dtc_en-us_40G_alibase_20200723.vhd*	2020-07-23	Updated to include the KB4565628, KB4486129, KB4565912, and KB4565511 operating system patches released in July 2020.
Windows Server 2016 Datacenter Edition	• Chinese version: *win2016_1607_x64_dtc_zh-cn_40G_alibase_20200615.vhd* • English version: *win2016_1607_x64_dtc_en-us_40G_alibase_20200615.vhd*	2020-06-15	• Updated to include the KB4561616 operating system patch released in June 2020. • Fixed the CVE-2020-1301, CVE-2020-1239, CVE-2020-1300, CVE-2020-1281, and CVE-2020-1260 vulnerabilities.
Windows Server 2016 Datacenter Edition	• Chinese version: *win2016_1607_x64_dtc_zh-cn_40G_alibase_20200516.vhd* • English version: *win2016_1607_x64_dtc_en-us_40G_alibase_20200516.vhd*	2020-05-16	• Updated to include the KB4556813 operating system patch released in May 2020. • Fixed the CVE-2020-1153, CVE-2020-1112, CVE-2020-1174, CVE-2020-1126, and CVE-2020-1062 vulnerabilities.
Windows Server 2016 Datacenter Edition	• Chinese version: *win2016_1607_x64_dtc_zh-cn_40G_alibase_20200416.vhd* • English version: *win2016_1607_x64_dtc_en-us_40G_alibase_20200416.vhd*	2020-04-16	• Updated to include the KB4550929 and KB4550994 operating system patches released in April 2020. • Added disk drives for the Windows Recovery mode. • Fixed the CVE-2020-1020, CVE-2020-0687, CVE-2020-0938, CVE-2020-0965, and CVE-2020-0968 vulnerabilities.

Release	Image ID	Release date	Description
Windows Server 2016 Datacenter Edition	• Chinese version: *win2016_1607_x64_dtc_zh-cn_40G_alibase_20200314.vhd* • English version: *win2016_1607_x64_dtc_en-us_40G_alibase_20200314.vhd*	2020-03-14	• Updated to include the operating system patches released in March 2020. • Fixed the CVE-2020-0684, CVE-2020-0801, CVE-2020-0881, and CVE-2020-0787 vulnerabilities.
Windows Server 2016 Datacenter Edition	• Chinese version: *win2016_1607_x64_dtc_zh-cn_40G_alibase_20200213.vhd* • English version: *win2016_1607_x64_dtc_en-us_40G_alibase_20200213.vhd*	2020-02-13	• Updated to include the operating system patches released in February 2020. • Fixed the CVE-2020-0738, CVE-2020-0689, CVE-2020-0681, CVE-2020-0683, CVE-2020-0686, CVE-2020-0674, and CVE-2020-0706 vulnerabilities.
Windows Server 2016 Datacenter Edition	• Chinese version: *win2016_1607_x64_dtc_zh-cn_40G_alibase_20200116.vhd* • English version: *win2016_1607_x64_dtc_en-us_40G_alibase_20200116.vhd*	2020-01-16	• Updated to include the operating system patches released in January 2020. • Fixed the CVE-2020-0609, CVE-2020-0601, CVE-2020-0625, CVE-2020-0611, and CVE-2020-0640 vulnerabilities.
Windows Server 2016 Datacenter Edition	• Chinese version: *win2016_1607_x64_dtc_zh-cn_40G_alibase_20191220.vhd* • English version: *win2016_1607_x64_dtc_en-us_40G_alibase_20191224.vhd*	2019-12-24	Updated to include the security patches released in December 2019.
Windows Server 2016 Datacenter Edition	• Chinese version: *win2016_64_dtc_1607_zh-cn_40G_alibase_20191012.vhd* • English version: *win2016_64_dtc_1607_en-us_40G_alibase_20191012.vhd*	2019-10-12	Updated to include the security patches released in October 2019.
Windows Server 2016 Datacenter Edition	• Chinese version: *win2016_64_dtc_1607_zh-cn_40G_alibase_20190816.vhd* • English version: *win2016_64_dtc_1607_en-us_40G_alibase_20190816.vhd*	2019-8-16	• Updated to include the latest operating system patches released in August 2019. • Fixed the CVE-2019-1181 and CVE-2019-1182 vulnerabilities.

Release	Image ID	Release date	Description
Windows Server 2016 Datacenter Edition	• Chinese version: *win2016_64_dtc_1607_zh-cn_40G_alibase_20190718.vhd* • English version: *win2016_64_dtc_1607_en-us_40G_alibase_20190718.vhd*	2019-7-18	• Updated to include the latest operating system patches released in July 2019. • Upgraded .NET Framework to version 4.8.
Windows Server 2016 Datacenter Edition	• Chinese version: *win2016_64_dtc_1607_zh-cn_40G_alibase_20190523.vhd* • English version: *win2016_64_dtc_1607_en-us_40G_alibase_20190523.vhd*	2019-5-23	Updated to include the operating system patches released in May 2019.
Windows Server 2016 Datacenter Edition	• Chinese version: *win2016_64_dtc_1607_zh-cn_40G_alibase_20190318.vhd* • English version: *win2016_64_dtc_1607_en-us_40G_alibase_20190318.vhd*	2019-3-18	Updated to include the operating system patches released in March 2019.
Windows Server 2016 Datacenter Edition	• Chinese version: *win2016_64_dtc_1607_zh-cn_40G_alibase_20181220.vhd* • English version: *win2016_64_dtc_1607_en-us_40G_alibase_20181220.vhd*	2018-12-20	• Updated to include the security patch KB4471321 released in December 2018. You must update Windows clients by using the latest patches to establish RDP connections. • Upgraded .NET Framework to version 4.7.2. • Used the Sysprep tool to generalize the image.

Windows Server 2019

Release	Image ID	Release date	Description
Windows Server 2019 Datacenter with Containers Edition	• Chinese version: *win2019_1809_x64_dtc_zh-cn_40G_container_alibase_20200814.vhd* • English version: *win2019_1809_x64_dtc_en-us_40G_container_alibase_20200814.vhd*	2020-08-14	• Updated to include the KB4565349, KB4566424, and KB4569750 operating system patches released in August 2020 • Fixed the CVE-2020-1472, CVE-2020-1464, CVE-2020-1554, CVE-2020-1509, CVE-2020-1567, and CVE-2020-1380 vulnerabilities

Release	Image ID	Release date	Description
Windows Server 2019 Datacenter Edition	• Chinese version: *win2019_1809_x64_dtc_zh-cn_40G_alibase_20200814.vhd* • English version: *win2019_1809_x64_dtc_en-us_40G_alibase_20200814.vhd*	2020-08-14	• Updated to include the KB4565349, KB4566424, and KB4569750 operating system patches released in August 2020 • Fixed the CVE-2020-1472, CVE-2020-1464, CVE-2020-1554, CVE-2020-1509, CVE-2020-1567, and CVE-2020-1380 vulnerabilities
Windows Server 2019 Datacenter with Containers Edition	• Chinese version: *win2019_1809_x64_dtc_zh-cn_40G_container_alibase_20200723.vhd* • English version: *win2019_1809_x64_dtc_en-us_40G_container_alibase_20200723.vhd*	2020-07-23	Updated to include the KB4558998, KB4558997, and KB4565632 operating system patches released in July 2020
Windows Server 2019 Datacenter Edition	• Chinese version: *win2019_1809_x64_dtc_zh-cn_40G_alibase_20200723.vhd* • English version: *win2019_1809_x64_dtc_en-us_40G_alibase_20200723.vhd*	2020-07-23	Updated to include the KB4558998, KB4558997, and KB4565632 operating system patches released in July 2020
Windows Server 2019 Datacenter with Containers Edition	• Chinese version: *win2019_1809_x64_dtc_zh-cn_40G_container_alibase_20200615.vhd* • English version: *win2019_1809_x64_dtc_en-us_40G_container_alibase_20200615.vhd*	2020-06-15	• Updated to include the KB4561608 operating system patch released in June 2020 • Fixed the CVE-2020-1301, CVE-2020-1286, CVE-2020-1292, CVE-2020-1239, CVE-2020-1300, CVE-2020-1281, and CVE-2020-1260 vulnerabilities
Windows Server 2019 Datacenter Edition	• Chinese version: *win2019_1809_x64_dtc_zh-cn_40G_alibase_20200615.vhd* • English version: *win2019_1809_x64_dtc_en-us_40G_alibase_20200615.vhd*	2020-06-15	• Updated to include the KB4561608 operating system patch released in June 2020 • Fixed the CVE-2020-1301, CVE-2020-1286, CVE-2020-1292, CVE-2020-1239, CVE-2020-1300, CVE-2020-1281, and CVE-2020-1260 vulnerabilities

Release	Image ID	Release date	Description
Windows Server 2019 Datacenter with Containers Edition	• Chinese version: *win2019_1809_x64_dtc_zh-cn_40G_container_alibase_20200516.vhd* • English version: *win2019_1809_x64_dtc_en-us_40G_container_alibase_20200516.vhd*	2020-05-16	• Updated to include the KB4551853 operating system patch released in May 2020 • Added the Docker runtime environment
Windows Server 2019 Datacenter Edition	• Chinese version: *win2019_1809_x64_dtc_zh-cn_40G_alibase_20200516.vhd* • English version: *win2019_1809_x64_dtc_en-us_40G_alibase_20200516.vhd*	2020-05-16	• Updated to include the KB4551853 operating system patch released in May 2020 • Fixed the CVE-2020-1153, CVE-2020-1112, CVE-2020-1174, CVE-2020-1126, CVE-2020-1118, and CVE-2020-1062 vulnerabilities
Windows Server 2019 Datacenter with Containers Edition	• Chinese version: *win2019_1809_x64_dtc_zh-cn_40G_container_alibase_20200416.vhd* • English version: *win2019_1809_x64_dtc_en-us_40G_container_alibase_20200416.vhd*	2020-04-16	• Updated to include the KB4549947 and KB4549949 operating system patches released in April 2020 • Added the Docker runtime environment • Added disk drives for the Windows Recovery mode • Fixed the CVE-2020-1020, CVE-2020-0687, CVE-2020-0910, CVE-2020-0938, CVE-2020-0965, and CVE-2020-0968 vulnerabilities
Windows Server 2019 Datacenter Edition	• Chinese version: *win2019_1809_x64_dtc_zh-cn_40G_alibase_20200416.vhd* • English version: none	2020-04-16	• Updated to include the KB4549947 and KB4549949 operating system patches released in April 2020 • Added disk drives for the Windows Recovery mode • Fixed the CVE-2020-1020, CVE-2020-0687, CVE-2020-0910, CVE-2020-0938, CVE-2020-0965, and CVE-2020-0968 vulnerabilities

Release	Image ID	Release date	Description
Windows Server 2019 Datacenter with Containers Edition	• Chinese version: *win2019_1809_x64_dtc_zh-cn_40G_container_alibase_20200314.vhd* • English version: *win2019_1809_x64_dtc_en-us_40G_container_alibase_20200314.vhd*	2020-03-14	• Updated to include the operating system patches released in March 2020 • Added the Docker runtime environment • Fixed the CVE-2020-0684, CVE-2020-0801, CVE-2020-0881, and CVE-2020-0787 vulnerabilities
Windows Server 2019 Datacenter Edition	• Chinese version: *win2019_1809_x64_dtc_zh-cn_40G_alibase_20200314.vhd* • English version: *win2019_1809_x64_dtc_en-us_40G_alibase_20200314.vhd*	2020-03-14	• Updated to include the operating system patches released in March 2020 • Fixed the CVE-2020-0684, CVE-2020-0801, CVE-2020-0881, and CVE-2020-0787 vulnerabilities
Windows Server 2019 Datacenter Edition	• Chinese version: *win2019_1809_x64_dtc_zh-cn_40G_alidocker_20200225.vhd* • English version: *win2019_1809_x64_dtc_en-us_40G_alidocker_20200225.vhd*	2020-02-25	• Updated to include the operating system patches released in February 2020 • Added the Docker runtime environment • Fixed the CVE-2020-0738, CVE-2020-0689, CVE-2020-0681, CVE-2020-0683, CVE-2020-0686, CVE-2020-0674, and CVE-2020-0706 vulnerabilities
Windows Server 2019 Datacenter Edition	• Chinese version: *win2019_1809_x64_dtc_zh-cn_40G_alibase_20200213.vhd* • English version: *win2019_1809_x64_dtc_en-us_40G_alibase_20200213.vhd*	2020-02-13	• Updated to include the operating system patches released in February 2020 • Fixed the CVE-2020-0738, CVE-2020-0689, CVE-2020-0681, CVE-2020-0683, CVE-2020-0686, CVE-2020-0674, and CVE-2020-0706 vulnerabilities
Windows Server 2019 Datacenter Edition	• Chinese version: *win2019_1809_x64_dtc_zh-cn_40G_alibase_20200116.vhd* • English version: *win2019_1809_x64_dtc_en-us_40G_alibase_20200116.vhd*	2020-01-16	• Updated to include the operating system patches released in January 2020 • Fixed the CVE-2020-0609, CVE-2020-0601, CVE-2020-0625, CVE-2020-0611, and CVE-2020-0640 vulnerabilities

Release	Image ID	Release date	Description
Windows Server 2019 Datacenter Edition	• Chinese version: *win2019_1809_x624_dtc_zh-cn_40G_alibase_20191220.vhd* • English version: *win2019_1809_x64_dtc_en-us_40G_alibase_20191220.vhd*	2019-12-20	Updated to include the security patches released in December 2019
Windows Server 2019 Datacenter Edition	• Chinese version: *win2019_64_dtc_1809_zh-cn_40G_alibase_20191012.vhd* • English version: *win2019_64_dtc_1809_en-us_40G_alibase_20191012.vhd*	2019-10-12	Updated to include the latest security patches released in October 2019
Windows Server 2019 Datacenter Edition	• Chinese version: *win2019_64_dtc_1809_zh-cn_40G_alibase_20190816.vhd* • English version: *win2019_64_dtc_1809_en-us_40G_alibase_20190816.vhd*	2019-8-16	• Updated to include the latest operating system patches released in August 2019 • Fixed the CVE-2019-1181 and CVE-2019-1182 vulnerabilities
Windows Server 2019 Datacenter Edition	• Chinese version: *win2019_64_dtc_1809_zh-cn_40G_alibase_20190718.vhd* • English version: *win2019_64_dtc_1809_en-us_40G_alibase_20190718.vhd*	2019-7-18	• Updated to include the latest operating system patches released in July 2019 • Upgraded .NET Framework to version 4.8
Windows Server 2019 Datacenter Edition	• Chinese version: *win2019_64_dtc_1809_zh-cn_40G_alibase_20190528.vhd* • English version: *win2019_64_dtc_1809_en-us_40G_alibase_20190528.vhd*	2019-5-28	Updated to include the latest operating system patches released in May 2019
Windows Server 2019 Datacenter Edition	• Chinese version: *win2019_64_dtc_1809_zh-cn_40G_alibase_20190318.vhd* • English version: *win2019_64_dtc_1809_en-us_40G_alibase_20190318.vhd*	2019-3-18	New release

Windows Server Version 1809

Release	Image ID	Release date	Description
Windows Server Version 1809 Datacenter Edition	• Chinese version: *winsvr_64_dtcC_1809_zh-cn_40G_alibase_20190528.vhd* • English version: *winsvr_64_dtcC_1809_en-us_40G_alibase_20190528.vhd*	2019-5-28	Updated to include the latest operating system patches released in May 2019
Windows Server Version 1809 Datacenter Edition	• Chinese version: *winsvr_64_dtcC_1809_zh-cn_40G_alibase_20190318.vhd* • English version: *winsvr_64_dtcC_1809_en-us_40G_alibase_20190318.vhd*	2019-3-18	Updated to include the operating system patches released in March 2019
Windows Server Version 1809 Datacenter Edition	• Chinese version: *winsvr_64_dtcC_1809_zh-cn_40G_alibase_20181222.vhd* • English Edition: *winsvr_64_dtcC_1809_en-us_40G_alibase_20181222.vhd*	2018-12-22	• Updated to include the latest patch KB4483235 released in December 2018 • Used the Sysprep tool to generalize the image

Windows Server Version 1903

Release	Image ID	Release date	Description
Windows Server Version 1903 Datacenter Edition	• Chinese version: *winsvr_64_dtcC_1903_zh-cn_40G_alibase_20191012.vhd* • English version: *winsvr_64_dtcC_1903_en-us_40G_alibase_20191012.vhd*	2019-10-12	Updated to include the latest security patches released in October 2019
Windows Server Version 1903 Datacenter Edition	• Chinese version: *winsvr_64_dtcC_1903_zh-cn_40G_alibase_20190816.vhd* • English version: *winsvr_64_dtcC_1903_en-us_40G_alibase_20190816.vhd*	2019-8-16	• Updated to include the latest operating system patches released in August 2019 • Fixed the CVE-2019-1181 and CVE-2019-1182 vulnerabilities
Windows Server Version 1903 Datacenter Edition	• Chinese version: *winsvr_64_dtcC_1903_zh-cn_40G_alibase_20190718.vhd* • English version: *winsvr_64_dtcC_1903_en-us_40G_alibase_20190718.vhd*	2019-7-18	• Updated to include the latest operating system patches released in July 2019 • Upgraded .NET Framework to version 4.8

Windows Server Version 1909

Release	Image ID	Release date	Description
Windows Server Version 1909 Datacenter with Containers Edition	• Chinese version: *wincore_1909_x64_dtc_zh-cn_40G_container_alibase_20200723.vhd* • English version: *wincore_1909_x64_dtc_en-us_40G_container_alibase_20200723.vhd*	2020-07-23	Updated to include the KB4565483, KB4565554, and KB4565633 operating system patches released in July 2020
Windows Server Version 1909 Datacenter Edition	• Chinese version: *wincore_1909_x64_dtc_zh-cn_40G_alibase_20200723.vhd* • English version: *wincore_1909_x64_dtc_en-us_40G_alibase_20200723.vhd*	2020-07-23	Updated to include the KB4565483, KB4565554, and KB4565633 operating system patches released in July 2020
Windows Server Version 1909 Datacenter with Containers Edition	• Chinese version: *wincore_1909_x64_dtc_zh-cn_40G_container_alibase_20200615.vhd* • English version: *wincore_1909_x64_dtc_en-us_40G_container_alibase_20200615.vhd*	2020-06-15	• Updated to include the KB4560960 operating system patch released in June 2020 • Fixed the CVE-2020-1301, CVE-2020-1286, CVE-2020-1292, CVE-2020-1248, CVE-2020-1239, CVE-2020-1300, and CVE-2020-1281 vulnerabilities
Windows Server Version 1909 Datacenter Edition	• Chinese version: *wincore_1909_x64_dtc_zh-cn_40G_alibase_20200615.vhd* • English version: *wincore_1909_x64_dtc_en-us_40G_alibase_20200615.vhd*	2020-06-15	• Updated to include the KB4560960 operating system patch released in June 2020 • Fixed the CVE-2020-1301, CVE-2020-1286, CVE-2020-1292, CVE-2020-1248, CVE-2020-1239, CVE-2020-1300, and CVE-2020-1281 vulnerabilities
Windows Server Version 1909 Datacenter Edition	• Chinese version: *wincore_1909_x64_dtc_zh-cn_40G_alibase_20200516.vhd* • English version: *wincore_1909_x64_dtc_en-us_40G_alibase_20200516.vhd*	2020-05-16	• Updated to include the KB4556799 operating system patch released in May 2020 • Fixed the CVE-2020-1153, CVE-2020-1112, CVE-2020-1174, CVE-2020-1126, and CVE-2020-1118 vulnerabilities

Release	Image ID	Release date	Description
Windows Server Version 1909 Datacenter with Containers Edition	• Chinese version: *wincore_1909_x64_dtc_zh-cn_40G_container_alibase_20200516.vhd* • English version: *wincore_1909_x64_dtc_en-us_40G_container_alibase_20200516.vhd*	2020-05-16	• Updated to include the KB4556799 operating system patch released in May 2020 • Added the Docker runtime environment
Windows Server Version 1909 Datacenter Edition	• Chinese version: *wincore_1909_x64_dtc_zh-cn_40G_alibase_20200416.vhd* • English version: *wincore_1909_x64_dtc_en-us_40G_alibase_20200416.vhd*	2020-04-16	• Updated to include the KB4549951 and KB4552152 operating system patches released in April 2020 • Added disk drives for the Windows Recovery mode • Fixed the CVE-2020-1020, CVE-2020-0687, CVE-2020-0910, CVE-2020-0938, CVE-2020-0965, and CVE-2020-0968 vulnerabilities
Windows Server Version 1909 Datacenter with Containers Edition	• Chinese version: *wincore_1909_x64_dtc_zh-cn_40G_container_alibase_20200416.vhd* • English version: *wincore_1909_x64_dtc_en-us_40G_container_alibase_20200416.vhd*	2020-04-16	• Updated to include the patches KB4549951 and KB4552152 released in April 2020 • Added the Docker runtime environment • Added disk drives for the Windows Recovery mode • Fixed the CVE-2020-1020, CVE-2020-0687, CVE-2020-0910, CVE-2020-0938, CVE-2020-0965, and CVE-2020-0968 vulnerabilities
Windows Server Version 1909 Datacenter Edition	• Chinese version: *wincore_1909_x64_dtc_zh-cn_40G_alibase_20200315.vhd* • English version: *wincore_1909_x64_dtc_en-us_40G_alibase_20200315.vhd*	2020-03-15	• Updated to include the operating system patches released in March 2020 • Fixed the CVE-2020-0684, CVE-2020-0801, CVE-2020-0881, CVE-2020-0787, and CVE-2020-0796 vulnerabilities

Release	Image ID	Release date	Description
Windows Server Version 1909 Datacenter Edition	• Chinese version: *wincore_1909_x64_dtc_zh-cn_40G_alibase_20200213.vhd* • English version: *wincore_1909_x64_dtc_en-us_40G_alibase_20200213.vhd*	2020-02-13	• Updated to include the operating system patches released in February 2020 • Fixed the CVE-2020-0738, CVE-2020-0689, CVE-2020-0681, CVE-2020-0683, CVE-2020-0686, CVE-2020-0674, and CVE-2020-0706 vulnerabilities
Windows Server Version 1909 Datacenter Edition	• Chinese version: *wincore_1909_x64_dtc_zh-cn_40G_alibase_20200116.vhd* • English version: *wincore_1909_x64_dtc_en-us_40G_alibase_20200116.vhd*	2020-01-16	• Updated to include the operating system patches released in January 2020 • Fixed the CVE-2020-0601, CVE-2020-0625, and CVE-2020-0611 vulnerabilities
Windows Server Version 1909 Datacenter Edition	• Chinese version: *wincore_1909_x64_dtc_zh-cn_40G_alibase_20191219.vhd* • English version: *wincore_1909_x64_dtc_en-us_40G_alibase_20191219.vhd*	2019-12-19	Updated to include the security patches released in December 2019

Windows Server Version 2004

Release	Image ID	Release date	Description
Windows Server Version 2004 Datacenter with Containers Edition	• Chinese version: *wincore_2004_x64_dtc_zh-cn_40G_container_alibase_20200814.vhd* • English version: *wincore_2004_x64_dtc_en-us_40G_container_alibase_20200814.vhd*	2020-08-14	• Updated to include the KB4566782, KB4570334, and KB4569745 operating system patches released in August 2020 • Fixed the CVE-2020-1472, CVE-2020-1464, CVE-2020-1554, CVE-2020-1509, CVE-2020-1567, and CVE-2020-1380 vulnerabilities
Windows Server Version 2004 Datacenter Edition	• Chinese version: *wincore_2004_x64_dtc_zh-cn_40G_alibase_20200814.vhd* • English version: *wincore_2004_x64_dtc_en-us_40G_alibase_20200814.vhd*	2020-08-14	• Updated to include the KB4566782, KB4570334, and KB4569745 operating system patches released in August 2020 • Fixed the CVE-2020-1472, CVE-2020-1464, CVE-2020-1554, CVE-2020-1509, CVE-2020-1567, and CVE-2020-1380 vulnerabilities

Windows Server 2008

Note On January 14, 2020, Microsoft stopped providing support for Windows Server 2008 and Windows Server 2008 R2 operating systems. Therefore, Alibaba Cloud no longer provides technical support for ECS instances that use the preceding operating systems. If you have ECS instances that use the preceding operating systems, upgrade them to Windows Server 2012 or later in a timely manner.

Release	Image ID	Release date	Description
Windows Server 2008 R2 Enterprise Edition	• Chinese version: *win2008r2_sp1_x64_ent_zh-cn_40G_alibase_20200116.vhd* • English version: *win2008r2_sp1_x64_ent_en-us_40G_alibase_20200116.vhd*	2020-01-16	• Updated to include the operating system patches released in January 2020. • Fixed the CVE-2020-0625, CVE-2020-0611, and CVE-2020-0640 vulnerabilities.
Windows Server 2008 R2 Enterprise Edition	• Chinese version: *win2008r2_sp1_x64_ent_zh-cn_40G_alibase_20191218.vhd* • English version: *win2008r2_sp1_x64_ent_en-us_40G_alibase_20191220.vhd*	2019-12-20	Updated to include the security patches released in December 2019.
Windows Server 2008 R2 Enterprise Edition	• Chinese version: *win2008r2_64_ent_sp1_zh-cn_40G_alibase_20191012.vhd* • English version: *win2008r2_64_ent_sp1_en-us_40G_alibase_20191012.vhd*	2019-10-12	Updated to include the latest security patches released in October 2019.
Windows Server 2008 R2 Enterprise Edition	• Chinese version: *win2008r2_64_ent_sp1_zh-cn_40G_alibase_20190816.vhd* • English version: *win2008r2_64_ent_sp1_en-us_40G_alibase_20190816.vhd*	2019-8-16	• Updated to include the latest operating system patches released in August 2019. • Fixed the CVE-2019-1181 and CVE-2019-1182 vulnerabilities.
Windows Server 2008 R2 Enterprise Edition	• Chinese version: *win2008r2_64_ent_sp1_zh-cn_40G_alibase_20190816.vhd* • English version: *win2008r2_64_ent_sp1_en-us_40G_alibase_20190816.vhd*	2019-8-16	• Updated to include the latest operating system patches released in August 2019. • Fixed the CVE-2019-1181 and CVE-2019-1182 vulnerabilities.

Release	Image ID	Release date	Description
Windows Server 2008 R2 Enterprise Edition	• Chinese version: *win2008r2_64_ent_sp1_zh-cn_40G_alibase_20190718.vhd* • English version: *win2008r2_64_ent_sp1_en-us_40G_alibase_20190718.vhd*	2019-7-18	• Updated to include the latest operating system patches released in July 2019. • Upgraded .NET Framework to version 4.8.
Windows Server 2008 Standard Edition SP2	• Chinese version: *win2008_32_std_sp2_zh-cn_40G_alibase_20190517.vhd* • English version: none	2019-5-17	• Updated to include the latest operating system patches released in May 2019. • Fixed the CVE-2019-0708 remote code execution vulnerability in Microsoft Windows Remote Desktop Services.
Windows Server 2008 R2 Enterprise Edition	• Chinese version: *win2008r2_64_ent_sp1_zh-cn_40G_alibase_20190515.vhd* • English version: *win2008r2_64_ent_sp1_en-us_40G_alibase_20190515.vhd*	2019-5-15	• Updated to include the latest operating system patches released in May 2019. • Fixed the CVE-2019-0708 remote code execution vulnerability in Microsoft Windows Remote Desktop Services.
Windows Server 2008 R2 Enterprise Edition	• Chinese version: *win2008r2_64_ent_sp1_zh-cn_40G_alibase_20190318.vhd* • English version: *win2008r2_64_ent_sp1_en-us_40G_alibase_20190318.vhd*	2019-3-18	Updated to include the latest operating system patches released in March 2019.
Windows Server 2008 R2 Enterprise Edition	• Chinese version: *win2008r2_64_ent_sp1_zh-cn_40G_alibase_20181220.vhd* • English version: none	2018-12-20	• Updated to include the security patch KB4471318 released in December 2018. You must update Windows clients by using the latest patches to establish RDP connections. • Upgraded .NET Framework to version 4.7.2. • Used the Sysprep tool to generalize the image.

4.3. Known issues

This topic describes known issues of Alibaba Cloud images for different operating systems, the scope of these issues, and their corresponding solutions.

SUSE Linux Enterprise Server 12 SP5: Kernel updates may lead to startup hangs

- Problem description: After an earlier kernel version is updated to SUSE Linux Enterprise Server (SLES) 12 SP5, or after an internal kernel version of SLES 12 SP5 is updated, instances may have the issue of startup hangs for some CPU types. These known CPU types are `Intel® Xeon® CPU E5-2682 v4 @ 2.50GHz` and `Intel® Xeon® CPU E7-8880 v4 @ 2.20GHz`. The following code describes the debugging result of the corresponding calltrace:

```
[    0.901281] CS:  0010 DS: 0000 ES: 0000 CR0: 0000000080050033
[    0.901281] CR2: ffffc90000d68000 CR3: 000000000200a001 CR4: 00000000003606e0
[    0.901281] DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000
[    0.901281] DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400
[    0.901281] Call Trace:
[    0.901281]  cpuidle_enter_state+0x6f/0x2e0
[    0.901281]  do_idle+0x183/0x1e0
[    0.901281]  cpu_startup_entry+0x5d/0x60
[    0.901281]  start_secondary+0x1b0/0x200
[    0.901281]  secondary_startup_64+0xa5/0xb0
[    0.901281] Code: 6c 01 00 0f ae 38 0f ae f0 0f 1f 84 00 00 00 00 00 0f 1f 84 00 00 00 00 00 90 31 d2 65 4
8 8b 34 25 40 6c 01 00 48 89 d1 48 89 f0 <0f> 01 c8 0f 1f 84 00 00 00 00 00 0f 1f 84 00 00 00 00 00 ** **
```

- Cause: The new kernel version is incompatible with the CPU microcode.
- Solution: In the `/boot/grub2/grub.cfg` file, add the `idle` kernel parameter to the row that begins with `linux` and set this parameter to nomwait. The following example shows how to modify the file:

```
menuentry 'SLES 12-SP5'  --class sles --class gnu-linux --class gnu --class os $menuentry_id_option '
gnulinux-simple-fd7bda55-42d3-4fe9-a2b0-45efdced****' {
        load_video
        set gfxpayload=keep
        insmod gzio
        insmod part_msdos
        insmod ext2
        set root='hd0,msdos1'
        if [ x$feature_platform_search_hint = xy ]; then
          search --no-floppy --fs-uuid --set=root --hint='hd0,msdos1'  fd7bda55-42d3-4fe9-a2b0-45efdce
d****
        else
          search --no-floppy --fs-uuid --set=root fd7bda55-42d3-4fe9-a2b0-45efdced****
        fi
        echo    'Loading Linux 4.12.14-122.26-default ...'
        linux   /boot/vmlinuz-4.12.14-122.26-default root=UUID=fd7bda55-42d3-4fe9-a2b0-45efdced****
net.ifnames=0 console=tty0 console=ttyS0,115200n8 mitigations=auto splash=silent quiet showopts
idle=nomwait
        echo    'Loading initial ramdisk ...'
        initrd  /boot/initrd-4.12.14-122.26-default
}
```

openSUSE 15: Kernel updates may lead to startup hangs

- Problem description: After openSUSE kernel versions are updated to `4.12.14-lp151.28.52-default`, instances may have the issue of startup hangs for some CPU types. These known CPU type is `Intel® Xeon® CPU E5-2682 v4 @ 2.50GHz`. The following code describes the debugging result of the corresponding calltrace:

```
[    0.901281] CS:  0010 DS: 0000 ES: 0000 CR0: 0000000080050033
[    0.901281] CR2: ffffc90000d68000 CR3: 000000000200a001 CR4: 00000000003606e0
[    0.901281] DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000
[    0.901281] DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400
[    0.901281] Call Trace:
[    0.901281]  cpuidle_enter_state+0x6f/0x2e0
[    0.901281]  do_idle+0x183/0x1e0
[    0.901281]  cpu_startup_entry+0x5d/0x60
[    0.901281]  start_secondary+0x1b0/0x200
[    0.901281]  secondary_startup_64+0xa5/0xb0
[    0.901281] Code: 6c 01 00 0f ae 38 0f ae f0 0f 1f 84 00 00 00 00 00 0f 1f 84 00 00 00 00 00 90 31 d2 65 4
8 8b 34 25 40 6c 01 00 48 89 d1 48 89 f0 <0f> 01 c8 0f 1f 84 00 00 00 00 00 0f 1f 84 00 00 00 00 00 ** **
```

- Cause: The new kernel version is incompatible with the CPU microcode. For more information, visit Issues of startup hangs.
- Involved image: opensuse_15_1_x64_20G_alibase_20200520.vhd
- Solution: In the */boot/grub2/grub.cfg* file, add the `idle` kernel parameter to the row that begins with `linux` and set this parameter to nomwait. The following example shows how to modify the file:

```
menuentry 'openSUSE Leap 15.1'  --class opensuse --class gnu-linux --class gnu --class os $menuent
ry_id_option 'gnulinux-simple-20f5f35a-fbab-4c9c-8532-bb6c66ce****' {
        load_video
        set gfxpayload=keep
        insmod gzio
        insmod part_msdos
        insmod ext2
        set root='hd0,msdos1'
        if [ x$feature_platform_search_hint = xy ]; then
          search --no-floppy --fs-uuid --set=root --hint='hd0,msdos1'  20f5f35a-fbab-4c9c-8532-bb6c66ce
****
        else
          search --no-floppy --fs-uuid --set=root 20f5f35a-fbab-4c9c-8532-bb6c66ce****
        fi
        echo    'Loading Linux 4.12.14-lp151.28.52-default ...'
        linux   /boot/vmlinuz-4.12.14-lp151.28.52-default root=UUID=20f5f35a-fbab-4c9c-8532-bb6c66ce*
*** net.ifnames=0 console=tty0 console=ttyS0,115200n8 splash=silent mitigations=auto quiet idle=n
omwait
        echo    'Loading initial ramdisk ...'
        initrd  /boot/initrd-4.12.14-lp151.28.52-default
}
```

CentOS 8.0: The version update of the image in the public image list leads to the change of public image version number of created instances

- Problem description: After you connect to an instance created from the centos_8_0_x64_20G_alibase_20200218.vhd public image, you check the system version of the instance, and find that the system version is CentOS 8.1.

```
root@ecshost:~$ lsb_release -a
LSB Version:    :core-4.1-amd64:core-4.1-noarch
Distributor ID:    CentOS
Description:    CentOS Linux release 8.1.1911 (Core)
Release:    8.1.1911
Codename:    Core
```

- Cause: The centos_8_0_x64_20G_alibase_20200218.vhd public image is in the public image list and was updated with the latest community update package. The image was upgraded and the actual system version is CentOS 8.1.

  centos_8_0_x64_20G_alibase_20200218.vhd

- Involved image: centos_8_0_x64_20G_alibase_20200218.vhd.
- Solution: You can call operations such as RunInstances with `ImageId set to centos_8_0_x64_20G_alibase_20191225.vhd` to create an instance whose system version is CentOS 8.0.

Debian 9.6: Classic network-type instances have network configuration issues

- Problem description: Classic network-type instances created from Debian 9 public images cannot be pinged.
- Cause: Classic network-type instances created from Debian 9 public images cannot be automatically assigned IP addresses through the Dynamic Host Configuration Protocol (DHCP) because the systemd-networkd service is disabled by default in Debian 9.
- Involved image: debian_9_06_64_20G_alibase_20181212.vhd.
- Solution: Run the following commands:

```
systemctl enable systemd-networkd
```

```
systemctl start systemd-networkd
```

CentOS 6.8: An instance installed with the NFS client fails to respond

- Problem description: A CentOS 6.8 instance installed with the NFS client fails to respond and must be restarted.
- Cause: When you use the NFS service on instances whose operating system kernel versions are 2.6.32-696 to 2.6.32-696.10, the NFS client will attempt to end a TCP connection if a glitch occurs due to communication latency. Specifically, if the NFS server is delayed in sending a response to the NFS client, the connection initiated by the NFS client may be stalled in the FIN_WAIT2 state. Typically, the connection will expire and close a minute after the connection enters the FIN_WAIT2 state and the NFS client will initiate another connection. However, kernel versions 2.6.32-696 to 2.6.32-696.10 have issues with establishing TCP connections. As a result, the connection will remain in the FIN_WAIT2 state, the NFS client will be unable to recover the TCP connection, and a new TCP connection cannot be initiated. The requests will hang, and the only way to fix the issue is to restart the instance.
- Involved images: centos_6_08_32_40G_alibase_20170710.vhd and centos_6_08_64_20G_alibase_20170824.vhd.
- Solution: Run the **yum update** command to update the kernel to 2.6.32-696.11 or later.

  Notice Before you perform operations on the instance, you must create a snapshot to back up your data. For more information, see Create a normal snapshot.

CentOS 7: The hostname changes from uppercase to lowercase letters after an instance restarts

- Problem description: When ECS instances are restarted for the first time, the hostnames of some instances that run CentOS 7 change from uppercase to lowercase letters. The following table describes some examples.

Hostname	Hostname after the instance is restarted for the first time	Does the hostname remain in lowercase after the restart?
iZm5e1qe*****sxx1ps5zX	izm5e1qe*****sxx1ps5zx	Yes
ZZHost	zzhost	Yes
NetworkNode	networknode	Yes

- Involved images: the following CentOS public images and custom images derived from these public images:
  - centos_7_2_64_40G_base_20170222.vhd
  - centos_7_3_64_40G_base_20170322.vhd
  - centos_7_03_64_40G_alibase_20170503.vhd
  - centos_7_03_64_40G_alibase_20170523.vhd
  - centos_7_03_64_40G_alibase_20170625.vhd
  - centos_7_03_64_40G_alibase_20170710.vhd
  - centos_7_02_64_20G_alibase_20170818.vhd
  - centos_7_03_64_20G_alibase_20170818.vhd
  - centos_7_04_64_20G_alibase_201701015.vhd
- Involved hostnames: If the hostnames of your applications are case-sensitive, the availability of corresponding services may be affected when you restart such instances. The following table describes whether the hostname will change after an instance is restarted.

Current state of hostname	Will the hostname change after an instance restart?	When will the change occur?	Continue reading this section?
The hostname contains uppercase letters when you created the instance by using the ECS console or by calling ECS API operations.	Yes	When the instance is restarted for the first time	Yes
The hostname contains only lowercase letters when you created the instance by using the ECS console or by calling ECS API operations.	No	N/A	No
The hostname contains uppercase letters, and you modify the hostname after you log on to the instance.	No	N/A	Yes

- Solution: To retain uppercase letters in the hostname of an instance after you restart the instance, perform the following steps:

i. Connect to your instance. For more information, see Connection methods.

ii. View the existing hostname.

```
[root@izbp193*****3i161uynzzx ~]# hostname
izbp193*****3i161uynzzx
```

iii. Run the following command to staticize the hostname:

```
hostnamectl set-hostname --static iZbp193*****3i161uynzzX
```

iv. Run the following commands to view the updated hostname:

```
[root@izbp193*****3i161uynzzx ~]# hostname
iZbp193*****3i161uynzzX
```

- Additional actions: If you are using a custom image, we recommend that you update cloud-init to the latest version and create a custom image again to prevent the previous issue from occurring to the custom image. For more information, see Install cloud-init and Create a custom image from an instance.

Linux: Pip requests time out

- Problem description: Pip requests occasionally time out or fail.
- Involved images: CentOS, Debian, Ubuntu, SUSE, openSUSE, and Alibaba Cloud Linux.
- Cause: Alibaba Cloud provides three pip source addresses. The default address is mirrors.aliyun.com. To access this address, instances must be able to access the Internet. If your instance is not assigned a public IP address, pip requests will time out.
  - The Internet source address (default): mirrors.aliyun.com
  - The internal source address of VPCs: mirrors.cloud.aliyuncs.com
  - The internal source address of the classic network: mirrors.aliyuncs.com
- Solution: You can solve the problem by using one of the following methods:
  - Method 1

    Assign a public IP address to your instance by associating an elastic IP address (EIP) to your instance. For more information, see Overview.

    A subscription instance can also be reassigned a public IP address through configuration upgrade or downgrade. For more information, see Upgrade configurations of subscription instances.
  - Method 2

    If a pip request fails, you can run the *fix_pypi.sh* script in your ECS instance and retry the pip operation. Specifically, perform the following steps:

    a. Connect to your instance. For more information, see Connect to a Linux instance by using VNC.

    b. Run the following command to obtain the script file:

    ```
    wget http://image-offline.oss-cn-hangzhou.aliyuncs.com/fix/fix_pypi.sh
    ```

c. Run one of the following scripts based on the network type of the instance:
   - For instances in VPCs, run the `bash fix_pypi.sh "mirrors.cloud.aliyuncs.com"` script.
   - For instances in the classic network, run the `bash fix_pypi.sh "mirrors.aliyuncs.com"` script.

d. Retry the pip operation.

The following section describes the content of the *fix_pypi.sh* script:

```
#! /bin/bash

function config_pip() {
   pypi_source=$1

   if [[ ! -f ~/.pydistutils.cfg ]]; then
cat > ~/.pydistutils.cfg << EOF
[easy_install]
index-url=http://$pypi_source/pypi/simple/
EOF
   else
      sed -i "s#index-url.*#index-url=http://$pypi_source/pypi/simple/#" ~/.pydistutils.cfg
   fi

   if [[ ! -f ~/.pip/pip.conf ]]; then
   mkdir -p ~/.pip
cat > ~/.pip/pip.conf << EOF
[global]
index-url=http://$pypi_source/pypi/simple/
[install]
trusted-host=$pypi_source
EOF
   else
      sed -i "s#index-url.*#index-url=http://$pypi_source/pypi/simple/#" ~/.pip/pip.conf
      sed -i "s#trusted-host.*#trusted-host=$pypi_source#" ~/.pip/pip.conf
   fi
}

config_pip $1
```

5.Alibaba Cloud Linux 2

5.1. Overview of Alibaba Cloud Linux 2

Alibaba Cloud Linux 2 is a next-generation proprietary Linux distribution developed by Alibaba Cloud. It provides a safe, stable, and high-performance customized running environment for applications on ECS instances. Alibaba Cloud Linux 2 is optimized for cloud infrastructure and aims to deliver a better runtime experience. You can create an instance by using the Alibaba Cloud Linux 2 image. Alibaba Cloud Linux 2 is free to use, and Alibaba Cloud provides long-term technical support.

Alibaba Cloud alibaba cloud linux 2 ecs native Linux

Scenarios

Alibaba Cloud Linux 2 is suitable for the following scenarios:

- Various workloads in cloud environments, such as databases, cloud-native containers, data analytics, web applications, and other workloads in the production environment.
- Various instance families including ECS Bare Metal Instance families. For more information, see Instance families.
  - Alibaba Cloud Linux 2 supports instance types that have 1 to 160 vCPUs.
  - Alibaba Cloud Linux 2 supports instance types that have a memory of 0.5 GiB to 3,840 GiB.
  - Alibaba Cloud Linux 2 does not support non-I/O optimized instances.

Benefits

Compared with other Linux distributions, Alibaba Cloud Linux 2 has the following benefits:

- Alibaba Cloud provides long-term free software maintenance and technical support for Alibaba Cloud Linux 2.
- Alibaba Cloud Linux 2 is optimized through the combination with Alibaba Cloud infrastructure and features faster system startup and higher runtime performance.
- Alibaba Cloud Linux 2 provides the latest enhanced features of the Linux community to support cloud-based application environments.
- Alibaba Cloud Linux 2 is equipped with a custom Linux kernel, user mode packages, and toolkits that provide additional features to the operating system.
- Alibaba Cloud Linux 2 offers a streamlined kernel and increased protection against security risks. Alibaba Cloud Linux 2 provides policies to monitor and fix security vulnerabilities and ensures constant system security.

Features

- Alibaba Cloud Linux 2 is distributed with the latest version of the Alibaba Cloud kernel. The kernel provides the following features:
  - The Alibaba Cloud kernel is based on Linux kernel V4.19 with the long-term support (LTS) from the kernel community. It is optimized for cloud-based scenarios, improved performance, and bug fixes. For more information, see Release notes of Alibaba Cloud Linux 2.
  - Alibaba Cloud Linux 2 provides customized and optimized kernel startup parameters and system configuration parameters for the ECS instance environment.

  - Alibaba Cloud Linux 2 provides the kernel failure dumping mechanism kdump when the operating system fails. You can enable or disable this feature without the need to restart the operating system.
  - Alibaba Cloud Linux 2 provides Kernel Live Patching (KLP).
- Pre-installed software and updates are described as follows:
  - The user-mode package is compatible with the latest version of CentOS 7 and can run on Alibaba Cloud Linux 2.
  - Alibaba Cloud Linux 2 is pre-installed with Alibaba Cloud CLI.
  - The network module is changed from network.service to systemd-networkd.
  - Fixes for Common Vulnerabilities and Exposures (CVE) will be continuously updated until the end of life (EOL) of Alibaba Cloud Linux 2. For more information, see Alibaba Cloud Linux 2.1903 Security Advisories. Alibaba Cloud Linux 2 provides automatic solutions to automatically fix vulnerabilities. For more information, see Use YUM to perform security updates.
- Alibaba Cloud Linux 2 accelerates the startup process, improves runtime performance, and enhances system stability in the following ways:
  - Alibaba Cloud Linux 2 optimizes the startup speed for ECS instances. Tests have proven that Alibaba Cloud Linux 2 can save 60% of startup time compared with other operating systems.
  - Alibaba Cloud Linux 2 optimizes scheduling, memory, I/O, and network subsystems. In some open-source benchmark tests, Alibaba Cloud Linux 2 shows 10% to 30% performance improvement compared with other operating systems.
  - Alibaba Cloud Linux 2 features enhanced system stability. According to statistics, Alibaba Cloud Linux 2 can reduce the downtime by 50% compared with other operating systems.

Billing

Alibaba Cloud Linux 2 images are provided free of charge. However, you are charged for resources such as vCPUs, memory, storage, public bandwidth, and snapshots. For more information, see Billing overview.

Obtain Alibaba Cloud Linux 2

You can use the following methods to obtain and use Alibaba Cloud Linux 2:

- ECS instances
  - When you create an ECS instance, select **Public Image** and then select Alibaba Cloud Linux and its version. For more information, see Create an instance by using the provided wizard.
  - Update the operating system of an existing ECS instance to Alibaba Cloud Linux 2 by replacing the system disk. For more information, see Replace the system disk (public images).
- On-premises environments such as a KVM-based virtualization environment

  Download and install the Alibaba Cloud Linux 2 image, and restart the system. For more information, see Use Alibaba Cloud Linux 2 images in an on-premises environment.

Use Alibaba Cloud Linux 2

- View or modify system parameters

You can run the sysctl command to view or modify the runtime parameters of Alibaba Cloud Linux 2. Alibaba Cloud Linux 2 has updated the following kernel configuration parameters in the */etc/sysctl.d/50-aliyun.conf* file.

System parameter	Description
`kernel.hung_task_timeout_secs = 240`	Increases the kernel hung_task timeout seconds to avoid frequent hung_task prompts.
`kernel.panic_on_oops = 1`	Throws the kernel panic exception when the kernel is experiencing an Oops error. System failure details are automatically captured if kdump is configured.
`kernel.watchdog_thresh = 50`	Increases the thresholds for events such as hrtimer, NMI, soft lockup, and hard lockup to avoid potential kernel false positives.
`kernel.hardlockup_panic = 1`	Throws the kernel panic exception when the kernel is experiencing a hard lockup error. System failure details are automatically captured if kdump is configured.

- View kernel parameters

  Alibaba Cloud Linux 2 has updated the following kernel parameters. You can run the `cat /proc/cmdline` command to view the kernel parameters of Alibaba Cloud Linux 2 at runtime.

Kernel parameter	Description
`crashkernel=0M-2G:0M,2G-8G:192M,8G-:256M`	Reserves memory space for the kdump feature.
`cryptomgr.notests`	Disables crypto self-check during kernel startup to accelerate system startup.
`cgroup.memory=nokmem`	Disables the kernel memory statistics function of memory cgroup to avoid potential kernel instability.
`rcupdate.rcu_cpu_stall_timeout=300`	Increases the timeout threshold of RCU CPU Stall Detector to 300 seconds to avoid kernel false positives.

- Roll back the kernel version

  Alibaba Cloud Linux 2 is distributed with Alibaba Cloud kernel V4.19.y. The kernel version changes when you update the image. You can run the following commands to install and switch to a V3.10 series kernel that is compatible with CentOS 7 as required.

  > **Note** Replacing the kernel version may result in a boot failure. Exercise caution when you perform this operation.

  Run the following commands to roll back to the V3.10 kernel:

```
# Install a V3.10 kernel.
sudo yum install -y kernel-3.10.0
# Configure the GRUB driver.
sudo grub2-set-default "$(grep ^menuentry /boot/grub2/grub.cfg | grep 3.10.0 | awk -F\' '{ print $2 }'
)"
# Apply changes to the configuration file.
sudo grub2-mkconfig -o /boot/grub2/grub.cfg
# Restart the operating system for the new configurations to take effect.
sudo reboot
```

- Enable or disable kdump

  Alibaba Cloud Linux 2 provides the kdump service. After this service is enabled, kernel errors can be captured to help you analyze kernel failures.

  > **Note** If the memory of the selected instance type is less than or equal to 2 GiB, the kdump service cannot be used.

  - Run the following commands to enable the kdump service:

    ```
    # Enable the kdump service first.
    sudo systemctl enable kdump.service
    # Restart the kdump service.
    sudo systemctl restart kdump.service
    ```

  - Run the following commands to return the memory address space reserved by the kdump service to the operating system and disable the kdump service:

    ```
    # Modify the configuration in the /sys/kernel/kexec_crash_size file.
    sudo sh -c 'echo 0 > /sys/kernel/kexec_crash_size'
    # Disable the kdump service.
    sudo systemctl disable kdump.service
    # Stop the kdump service.
    sudo systemctl stop kdump.service
    ```

    > **Note** After the memory address space that is reserved by the kdump service is returned to the operating system, the operating system must be restarted to re-enable the kdump service.

- Configure the network

  By default, Alibaba Cloud Linux 2 uses systemd-networkd to configure the network. The configuration file for DHCP or static IP addresses is located in the */etc/systemd/network/* directory.

```
# Restart the network.
sudo systemctl restart systemd-networkd
```

- Obtain the Debuginfo package and the source code package
  - Run the following commands to obtain the Debuginfo package:

```
# Install yum-utils.
sudo yum install -y yum-utils
# Install the Debuginfo package by replacing packageName in the following command with the na
me of the target software package:
sudo debuginfo-install -y <packageName>
```

  - Run the following commands to obtain the source code package:

```
# Install the source code.
sudo yum install -y alinux-release-source
# Install yum-utils.
sudo yum install -y yum-utils
# Install the source code package by replacing sourcePackageName in the following command wit
h the name of the target software package:
sudo yumdownloader --source <sourcePackageName>
```

- Use experimental software packages

  Experimental software packages are provided by Alibaba Cloud, but are not fully tested. Alibaba Cloud does not guarantee the quality of these packages. Alibaba Cloud Linux 2 provides the following types of experimental packages:

  - Experimental software packages that serve common purposes
    - `Golang 1.12`
    - `Golang 1.13`

    Run the following commands to install an experimental software package that serves common purposes:

```
# Enable Yum repositories.
sudo yum install -y alinux-release-experimentals
# Install an experimental software package that serves common purposes by replacing packageN
ame in the following command with the name of the target software package:
sudo yum install -y <packageName>
```

- Development kits that support SCL plug-ins
  - The development kit that is based on `GCC-7.3.1` : devtoolset-7
  - The development kit that is based on `GCC-8.2.1` : devtoolset-8
  - The development kit that is based on `GCC-9.1.1` : devtoolset-9

  Run the following commands to install an experimental software package that supports SCL plug-ins:

```
# Install scl-utils.
sudo yum install -y scl-utils
# Enable Yum repositories.
sudo yum install -y alinux-release-experimentals
# Install the software packages that you need from the Yum repositories. The following sample c
ommands install all development kits that support SCL plug-ins:
sudo yum install -y devtoolset-7-gcc devtoolset-7-gdb devtoolset-7-binutils devtoolset-7-make
sudo yum install -y devtoolset-8-gcc devtoolset-8-gdb devtoolset-8-binutils devtoolset-8-make
sudo yum install -y devtoolset-9-gcc devtoolset-9-gdb devtoolset-9-binutils devtoolset-9-make
```

  After the installation is completed, you can use the later version of GCC and related tools. The sample code is as follows:

```
# Specify the repository name to view an existing SCL. The following command uses the devtools
et-7 repository as an example:
scl -l devtoolset-7
#Run the related SCL software.
scl enable devtoolset-7 'gcc --version'
```

Update history

- For more information about release notes of Alibaba Cloud Linux 2 images, see Release notes of Alibaba Cloud Linux 2.
- For more information about CVE updates of Alibaba Cloud Linux 2, see Alibaba Cloud Linux 2.1903 Security Advisories.

Technical support

Alibaba Cloud provides the following support for Alibaba Cloud Linux 2:

- 5-year long-term support (LTS) in terms of security updates and vulnerability fixes is provided until the version lifecycle ends on March 31, 2024. You can obtain free LTS in the following ways:
  - Submit a ticket
  - GitHub
- Images are updated every four months. Updates cover new features, security updates, and vulnerability fixes.
- Security updates are provided from Yum repositories. You can run the **yum update** command to

update security to the latest version.

5.2. Release notes of Alibaba Cloud Linux 2

This topic describes the feature updates of Alibaba Cloud Linux 2 images in the order in which they were released.

Background information

- Unless otherwise stated, the released updates apply to all Alibaba Cloud regions where ECS is provided.
- Alibaba Cloud Linux 2 images are applicable to most instance families. For information about instance families that do not support Alibaba Cloud Linux 2 images and can use only specified public images, see the Release notes of images that are applicable to some instance families section.

Release notes

Image ID	Release date	Description

Image ID	Release date	Description

aliyun_2_1903_x64_20G_alibase_20200904.vhd	2020-09-04	• Images are updated to the latest software version to be compatible with CentOS 7.8. Common Vulnerabilities and Exposures (CVEs) are fixed.
		• /etc/redhat-release is changed from Aliyun Linux release 7.2 LTS (Hunting Beagle) to Alibaba Cloud Linux (Aliyun Linux) release 2.1903 LTS (Hunting Beagle).
		• The image type information in /etc/image-id is optimized.
		• The tuned service is disabled by default.
		• Kernel updates:
		  ○ The kernel is updated to the *kernel-4.19.91-21.al7* version.
		  ○ Kernel bugs and security vulnerabilities are fixed.
		  ○ The io_uring bug is fixed and new features are added.
		  ○ THP fork optimization is added to accelerate the creation of memory intensive processes.
		  ○ Secure operations on Apache Pass (AEP) devices are supported.
		  ○ The TCP-RT feature developed by Alibaba Cloud is supported.
		  ○ The virtio-mem feature is supported.
		  ○ The PCIe Gen4 feature, RAS feature, and power management of Intel® IceLake processors are enhanced.
		  ○ The Intel® Speed Select Technology is supported.
		• Applicable regions: China (Hangzhou), China (Hong Kong), China (Zhangjiakou-Beijing Winter Olympics), and China (Chengdu).

aliyun_2_1903_x64_20G_qboot_alibase_20200904.vhd	2020-09-04	• Images are updated to the latest software version to be compatible with CentOS 7.8. CVEs are fixed. • This image is derived from the *aliyun_2_1903_x64_20G_alibase_20200904.vhd* image. • Quick boot by using qboot is supported. • Applicable regions: China (Hangzhou), China (Hong Kong), and China (Zhangjiakou-Beijing Winter Olympics).

Image ID	Release date	Description

aliyun_2_1903_x64_20G_alibase_20200529.vhd	2020-05-29	• Images are updated to the latest software version to be compatible with CentOS 7.8. CVEs are fixed.
		• /etc/image-id is added.
		• The tuned service is disabled by default.
		• Kernel updates:
		  ○ The kernel is updated to the *kernel-4.19.91-19.1.al7* version.
		  ○ The kernel interface support provided by Alibaba Cloud kernel on the statistics of scheduling and memory QoS metrics is open sourced to perform fine-grained monitoring of Service Level Indicators (SLIs) related to scheduling and memory.
		  ○ The kernel interface support provided by Alibaba Cloud kernel on priority control when a memcg is out of memory (OOM) is open sourced to improve protection on important processes during system OOM.
		  ○ AMD QoS is supported.
		  ○ The virtio pmem driver is supported.
		  ○ The free page reporting feature is supported to enhance the awareness of hypervisors about idle memory of a guest OS and efficiently manage and utilize physical memory resources.
		  ○ Memory compaction is optimized to alleviate memory fragmentation and improve the utilization of system memory.
		  ○ Kernel bugs and security vulnerabilities are fixed.

Image ID	Release date	Description

aliyun_2_1903_x64_20G_alibase_20200324.vhd	2020-03-24	• Images are updated to the latest software version to be compatible with CentOS 7.7. CVEs are fixed.
		• The latest fixes for CVEs can be obtained through YUM.
		• The LTS version of Alibaba Cloud Linux 2 is released and /etc/alinux-release is updated to Aliyun Linux release 2.1903 LTS (Hunting Beagle).
		• The tuned service is enabled by default.
		• Kernel updates:
		  ○ The kernel is updated to the *kernel-4.19.91-18.al7* version.
		  ○ NVMe devices are supported.
		  ○ The Transparent Huge Pages (THP) feature is enabled by default to improve application performance.
		  ○ io_uring is added.
		  ○ Intel_idle and guest halt polling are enabled to improve the guest CPU performance.
		  ○ ftrace syscalls is enabled to enhance the performance of the bpftrace tool.
		  ○ Multiple Alibaba Cloud optimizations and bug fixes to the kernel including subsystems such as schedulers, memory, file systems, and block layers are open sourced.
		  ○ Kernel security vulnerabilities are fixed.

Image ID	Release date	Description
aliyun_2_1903_x64_20G_alibase_20200221.vhd	2020-02-21	• Images are updated to the latest software version to be compatible with CentOS 7.7. CVEs are fixed. • IPv6 is supported by default. • Kernel updates: ◦ The kernel is updated to the *kernel-4.19.81-17.1.al7* version. ◦ Intel Cooper Lake CPU and Ice Lake CPU are supported. ◦ The support for the AMD and ARM 64-bit CPU architectures is enhanced. ◦ Persistent memory is supported. ◦ The blk-iocost feature is provided. It is based on the cost model and the weight-based throttling function of blkio cgroup controllers. For more information, see Configure the weight-based throttling feature of blk-iocost. ◦ The Pressure Stall Information (PSI) feature that is implemented based on cgroup v1 interfaces is supported. For more information, see Enable the PSI feature for the cgroup v1 interface. ◦ Multiple Alibaba Cloud optimizations and bug fixes to the kernel including subsystems such as schedulers, memory, file systems, and block layers are open sourced. ◦ Kernel security vulnerabilities are fixed.
aliyun_2_1903_x64_20G_alibase_20200114.qboot.vhd	2020-01-14	• Images are updated to the latest software version. • Kernel updates: ◦ The kernel is updated to the *4.19.81-17.al7.x86_64* version. ◦ Quick boot by using qboot is supported. • Applicable regions: China (Beijing), China (Hangzhou), and China (Hong Kong).
aliyun_2_1903_64_20G_alibase_20190829.vhd	2019-08-29	• Images are updated to the latest software version. • Kernel updates: ◦ The kernel is updated to the *kernel-4.19.57-15.1.al7.x86_64* version. ◦ The Spectre-V1 SWAPGS vulnerability is fixed. ◦ Issues with DM bio splitting code are fixed. ◦ The default TCP congestion control algorithm is set to CUBIC. ◦ The network is configured to 10-eth0.network.

Image ID	Release date	Description

aliyun_2_1903_64_20G_alibase_20190619.vhd	2019-06-19	• Images are updated to the latest software version.
		• Kernel updates:
		  ○ The kernel is updated to the *kernel-4.19.43-13.2.al7.x86_64* version.
		  ○ The cgroup writeback feature that is implemented based on cgroup v1 interfaces is supported.
		  ○ Policy-based routing is supported.
		  ○ The INET_DIAG kernel configuration item is enabled to support the ss command from the iproute2 suite.
		  ○ The configurable net.ipv4.tcp_tw_timeout kernel interface is supported.
		  ○ The following network-related CVEs are fixed:
		  ■ CVE-2019-11477
		  ■ CVE-2019-11478
		  ■ CVE-2019-11479

aliyun-2.1903-x64-20G-alibase-20190507.vhd	2019-05-07	• Images are updated to the latest software version. • The time synchronization delay that was presented on instance startup is fixed. • The kernel is updated to the *kernel-4.19.34-11.al7.x86_64* version and other issues are fixed.
aliyun-2.1903-x64-20G-alibase-20190327.vhd	2019-03-27	• Alibaba Cloud Linux 2 is released. • The *kernel-4.19.24-9.al7.x86_64* kernel version is used in Alibaba Cloud Linux 2.

Release notes of images that are applicable to some instance families

Image ID	Release date	Applicable instance family	Description

Image ID	Release date	Applicable instance family	Description
aliyun_2_1903_x64_20G_secured_alibase_20200904.vhd	2020-09-04	Trusted instance families: • ecs.g6t • ecs.c6t	• Images are updated to the latest software version to be compatible with CentOS 7.8. CVEs are fixed. • This image is derived from the *aliyun_2_1903_x64_20G_alibase_20200904.vhd* image. • Boot mode is changed to the Unified Extensible Firmware Interface (UEFI) mode. This is the only supported mode. • Trusted features are added. • Applicable regions: China (Hangzhou), China (Hong Kong), China (Zhangjiakou-Beijing Winter Olympics), and China (Chengdu).
aliyun_2_1903_x64_20G_uefi_alibase_20200904.vhd	2020-09-04	AMD instance families: • ecs.ebmg6a • ecs.ebmc6a • ecs.ebmr6a	• Images are updated to the latest software version to be compatible with CentOS 7.8. CVEs are fixed. • This image is derived from the *aliyun_2_1903_x64_20G_alibase_20200904.vhd* image. • Boot mode is changed to the UEFI mode. This is the only supported mode. • Applicable regions: China (Hangzhou), China (Hong Kong), China (Zhangjiakou-Beijing Winter Olympics), and China (Chengdu).

aliyun_2_1903_x64_20G_secured_alibase_20200622.vhd	2020-06-22	Trusted instance families:
		• ecs.g6t
		• ecs.c6t
			• Images are updated to the latest software version to be compatible with CentOS 7.8. CVEs are fixed.
			• This image is derived from the *aliyun_2_1903_x64_20G_alibase_20200529.vhd* image.
			• Boot mode is changed to the UEFI mode. This is the only supported mode.
			• Trusted features are added.
			• Kernel updates:
			  ◦ The kernel is updated to the *kernel-4.19.91-19.2.al7* version.
			  ◦ AMD IOMMU is supported.

Image ID	Release date	Applicable instance family	Description
aliyun_2_1903_x64_20G_uefi_alibase_20200616.vhd	2020-06-16	AMD instance families: • ecs.ebmg6a • ecs.ebmc6a • ecs.ebmr6a	• Images are updated to the latest software version to be compatible with CentOS 7.8. CVEs are fixed. • This image is derived from the *aliyun_2_1903_x64_20G_alibase_20200529.vhd* image. • Boot mode is changed to the UEFI mode. This is the only supported mode. • The kernel is updated to the *kernel-4.19.91-19.2.al7* version.

5.3. Known issues about Alibaba Cloud Linux 2

This topic describes known issues of Alibaba Cloud Linux 2 images, the scope of these issues, and their corresponding solutions.

Performance issues may occur after you enable the CONFIG_PARAVIRT_SPINLOCK kernel feature

- Problem description: After you enable the CONFIG_PARAVIRT_SPINLOCK kernel feature, application performance is significantly affected when an ECS instance has a large number of vCPUs and a large number of lock contentions exist in applications. For example, short-lived connections deteriorate the performance of a NGINX application.
- Solution: We recommend that you disable the CONFIG_PARAVIRT_SPINLOCK kernel feature for Alibaba Cloud Linux 2 (disabled by default). And if you are not sure how to resolve the kernel problem, do not enable the CONFIG_PARAVIRT_SPINLOCK feature.

System instability and performance issues may occur after you set the THP switch of kernel features to always

- Problem description: After you set the Transparent Hugepage (THP) switch in your production environment to *always*, the system becomes unstable and its performance is deteriorated.
- Solution: For information about how to optimize THP-related performance, see Transparent huge page THP-related performance optimization in Alibaba Cloud Linux 2.

A delegation conflict occurs in NFS v4.0

- Problem description: A delegation conflict occurs in NFS v4.0. For more information, see Delegation in NFS Version 4.
- Solution: We recommend that you disable the Delegation feature when you use NFS v4.0. For information about how to disable this feature at the server side, visit How to Select Different Versions of NFS on a Server.

Defects in NFS v4.1 or v4.2 cause failures to exit applications

- Problem description: In NFS v4.1 or v4.2, if you use Asynchronous I/O (AIO) in applications to distribute requests and close the corresponding file descriptors before all I/O operations are returned, a livelock may be triggered and the corresponding process cannot be ended.
- Solution: This problem was fixed in kernel versions 4.19.30-10.al7 and later. Application exit failure is not likely to occur. Decide whether you need to upgrade the kernel to fix this issue. To upgrade the kernel version, run the **sudo yum update kernel -y** command.

  > **Notice**
  > - The kernel upgrade may result in system boot failure. Exercise caution when you perform this action.
  > - Before you upgrade the kernel, make sure that you have created a snapshot or a custom image to back up data. For more information, see Create a normal snapshot or Create a custom image from an instance.

System performance is affected after security vulnerabilities such as Meltdown and Spectre are fixed

- Problem description: By default, the repair of important security vulnerabilities such as Meltdown or Spectre in processors is enabled in the kernel of Alibaba Cloud Linux 2. This affects system performance. Therefore, performance may be deteriorated during performance benchmark testing.
- Solution: Meltdown and Spectre are two important vulnerabilities in Intel chips. These vulnerabilities allow attackers to steal sensitive application data from the system memory. We recommend that you enable the repair feature. However, if you want to maximize system performance, you can disable the repair feature. For more information, see How to fix CPU vulnerabilities in the Alibaba Cloud Linux 2 system.

5.4. Features and interfaces supported by Alibaba Cloud Linux 2

5.4.1. Features and interfaces supported by Alibaba Cloud Linux 2

This topic summarizes the features and kernel interfaces supported by Alibaba Cloud Linux 2.

Use Alibaba Cloud Linux 2 images

The following table describes the operations on Alibaba Cloud Linux 2 images.

Documentation	Description
Use Alibaba Cloud Linux 2 images in an on-premises environment	Alibaba Cloud Linux 2 images can be downloaded to and used on local kernel-based virtual machines (KVMs).
Use YUM to perform security updates	You can use YUM to query, check, and install security updates for Alibaba Cloud Linux 2.

Function interfaces supported by Alibaba Cloud Linux 2

If you have knowledge about the Linux kernel and need to use Linux kernel features, you can perform operations based on the Alibaba Cloud Linux 2 kernel features and interfaces described in the following table.

Documentation	Description
Enable the cgroup writeback feature	Alibaba Cloud Linux 2 supports the cgroup writeback feature for the cgroup v1 kernel interface in the 4.19.36-12.al7 kernel version or later. This feature allows you to limit the buffered I/O rate when you use the cgroup v1 kernel interface.
Configure the weight-based throttling feature of blk-iocost	Alibaba Cloud Linux 2 provides the weight-based throttling feature (blk-iocost) based on the cost model in the 4.19.81-17.al7.x86_64 kernel version or later. This feature improves the weight-based disk throttling feature of the I/O subsystem (blkcg) within a kernel.
Enable the PSI feature for the cgroup v1 interface	Alibaba Cloud Linux 2 supports the Pressure Stall Information (PSI) feature for the cgroup v1 interface in the 4.19.81-17.al7 kernel version or later. This feature allows you to monitor the CPU, memory, and I/O performance.
Change the TCP TIME-WAIT timeout period	In the Linux kernel, TCP/IP connections remain in the TIME-WAIT state for 60 seconds. The length of this period cannot be changed. However, in some scenarios such as heavy TCP loads, network performance can be improved if this period is reduced. In this context, Alibaba Cloud Linux 2 provides a kernel interface in the 4.19.43-13.al7 kernel version or later to change the length of the TCP TIME-WAIT timeout period.
Enhance the monitoring of block I/O throttling	Alibaba Cloud Linux 2 provides interfaces in the 4.19.81-17.al7 kernel version or later to better monitor Linux block I/O throttling.
Use the JBD2 optimization interface	JBD2 is the kernel thread of the ext4 file system. It often experiences the shadow (BH_Shadow) state during its use, which can affect the system performance. To solve this problem, Alibaba Cloud Linux 2 provides an interface in the 4.19.81-17.al7 kernel version or later to optimize JBD2.
Create a hard link across project quotas	By default, the ext4 file system contains constraints. You are not allowed to create hard links across project quotas. However, in practice some scenarios require the creation of hard links. Alibaba Cloud Linux 2 provides a custom interface that can bypass the constraints of the ext4 file system to create hard links across project quotas.
Track I/O latency	Alibaba Cloud Linux 2 optimizes the /proc/diskstats interface, which is the raw data source of the I/O latency analysis tool iostat. Alibaba Cloud Linux 2 can calculate the duration of time in read, write and special I/O (discard) on the device. In addition, Alibaba Cloud Linux 2 provides the bcc tool to track I/O latency.

Documentation	Description
Detect I/O hangs of file systems and block layers	An I/O hang occurs when the system becomes unstable or even goes down due to time-consuming I/O requests. To accurately detect I/O hangs, Alibaba Cloud Linux 2 extends the core data structure and provides the feature to locate and detect I/O hangs with low system overheads.
Memcg global minimum watermark rating	Alibaba Cloud Linux 2 provides the memcg global minimum watermark rating feature. The global wmark_min of resource-consuming tasks is increased to trigger direct memory reclaim. The global wmark_min of latency-sensitive tasks is decreased to avoid direct memory reclaim. This way, when a resource-consuming task requests a large amount of memory, an increase in the global wmark_min throttles the resources used for the task for a short period to avoid direct memory reclaim for latency-sensitive tasks. After a certain amount of memory is reclaimed through global kswapd backend reclaim, the resource-consuming task is no longer throttled.
Memcg backend asynchronous reclaim	Alibaba Cloud Linux 2 provides the backend asynchronous reclaim feature for memcgs. This feature differs from the global kswapd kernel thread in that it uses the workqueue mechanism instead of a corresponding memcg kswapd kernel thread.
Memcg QoS feature of the cgroup v1 interface	The memory control group (memcg) quality of service (QoS) can be used to control locks and limits on memory usage in a memcg. Alibaba Cloud Linux 2 provides the memcg QoS feature in the 4.19.91-18.al7 kernel version or later.
Memcg Exstat feature	Alibaba Cloud Linux 2 provides the memcg exstat (Extend/Extra) feature in the 4.19.91-18.al7 kernel version or later.

5.4.2. Use Alibaba Cloud Linux 2 images in an on-premises environment

Alibaba Cloud Linux 2 provides local images in various formats that contain the built-in cloud-init package. This topic describes how to use Alibaba Cloud Linux 2 images in an on-premises environment.

Context

Alibaba Cloud Linux 2 images can only run on Kernel-based Virtual Machines (KVMs). Alibaba Cloud Linux 2 images cannot start KVMs directly. You must configure a boot image. In this topic, the local operating system is Linux. Alibaba Cloud Linux 2 is used to create a KVM, and cloud-init is used to initialize the system settings of the KVM. For more information about cloud-init, visit cloud-init official website - Alibaba Cloud (AliYun). The NoCloud data source is then used to create local configuration files. After the configuration files are attached to the KVM as a virtual disk, the KVM can be started.

This topic is applicable to users who are familiar with KVMs.

Step 1: Download the Alibaba Cloud Linux 2 image to your local computer

You can download the Alibaba Cloud Linux 2 image to your local computer from Alibaba Cloud Linux 2 On-premise Image. Alibaba Cloud Linux 2 images in the VHD or qcow2 format are available.

Step 2: Generate the seed.img boot image from your local computer

You must configure the network, account, and YUM repository of the boot image. Typically, the image name is set to seed.img. You can set another name for the image, but we recommend that you do not.

> **Notice** The seed.img image only contains the configuration files that are required to start cloud-init. The image does not contain Alibaba Cloud Linux 2 system files.

You can use one of the following methods to generate the seed.img image:

- Use the image file prepared by Alibaba Cloud Linux 2 to generate the seed.img image. You can download the image file from Alibaba Cloud Linux 2 On-premise Image. On the Alibaba Cloud Linux 2 On-premise Image page, click *seed.img* to download the image.

  You cannot change the configuration information in the boot image. Therefore, this image file is not ideal for all scenarios. Before you use this method to generate the seed.img image, make sure that you are already familiar with the image file.
- Use the NoCloud data source to manually generate the seed.img image. Perform the following steps:

  1. In the same local directory, create two configuration files `meta-data` and `user-data`.
     i. Create a directory named `seed` and go to the directory.

     ```
     mkdir seed
     cd seed/
     ```

ii. Create the `meta-data` configuration file.The following example describes the configuration file content. You can modify the configuration as needed.

```
#cloud-config
#vim:syntax=yaml

local-hostname: alinux-host
# FIXME: doesn't work for systemd-networkd
#network-interfaces: |
#  iface eth0 inet static
#  address 192.168.122.68
#  network 192.168.122.0
#  netmask 255.255.255.0
#  broadcast 192.168.122.255
#  gateway 192.168.122.1
```

iii. Create the `user-data` configuration file.The following example describes the configuration file content. You can modify the configuration as needed.

```
#cloud-config
#vim:syntax=yaml

# Create a user named alinux who is authorized to run sudo commands.
users:
 - default
 - name: alinux
   sudo: ['ALL=(ALL)  ALL']
   plain_text_passwd: aliyun
   lock_passwd: false

# Create the YUM repository for Alibaba Cloud Linux 2.
yum_repos:
   base:
      baseurl: https://mirrors.aliyun.com/alinux/$releasever/os/$basearch/
      enabled: true
      gpgcheck: true
      gpgkey: https://mirrors.aliyun.com/alinux/RPM-GPG-KEY-ALIYUN
      name: Aliyun Linux - $releasever - Base - mirrors.aliyun.com
   updates:
      baseurl: https://mirrors.aliyun.com/alinux/$releasever/updates/$basearch/
      enabled: true
      gpgcheck: true
```

```
      gpgkey: https://mirrors.aliyun.com/alinux/RPM-GPG-KEY-ALIYUN
      name: Aliyun Linux - $releasever - Updates - mirrors.aliyun.com
    extras:
      baseurl: https://mirrors.aliyun.com/alinux/$releasever/extras/$basearch/
      enabled: true
      gpgcheck: true
      gpgkey: https://mirrors.aliyun.com/alinux/RPM-GPG-KEY-ALIYUN
      name: Aliyun Linux - $releasever - Extras - mirrors.aliyun.com
    plus:
      baseurl: https://mirrors.aliyun.com/alinux/$releasever/plus/$basearch/
      enabled: true
      gpgcheck: true
      gpgkey: https://mirrors.aliyun.com/alinux/RPM-GPG-KEY-ALIYUN
      name: Aliyun Linux - $releasever - Plus - mirrors.aliyun.com

# Using cloud-init or systemd-networkd may cause the steps to fail when you create the met
a-data configuration file. The alternative network configurations are as follows:
write_files:
  - path: /etc/systemd/network/20-eth0.network
    permissions: 0644
    owner: root
    content: |
      [Match]
      Name=eth0

      [Network]
      Address=192.168. *. */24
      Gateway=192.168. *.1

# You can also use the following alternative network configurations:
runcmd:
  - ifdown eth0
  - systemctl restart systemd-networkd
```

2. Install the `cloud-utils` software package on your local computer.

```
yum install -y cloud-utils
```

3. In the `seed` directory, run the following command to generate the `seed.img` image.

```
cloud-localds seed.img user-data meta-data
```

Step 3: Start the KVM

You can use one of the following methods to start the KVM. Then, use the account information in the `user-data` configuration file to log on to the KVM.

- Use libvirt to start the KVM.
  i. Create a configuration file of the XML format on your local computer. The name of the sample file is `alinux2.xml`. The content of the file is as follows. You can modify the XML-formatted configuration file as needed.

```
<domain type='kvm'>
  <name>alinux2</name>
  <memory>1048576</memory> <! -- 1 GB memory. -->
  <vcpu>1</vcpu>
  <os>
    <type arch='x86_64'>hvm</type>
    <boot dev='hd'/>
  </os>
  <clock sync="localtime"/>
  <on_poweroff>destroy</on_poweroff>
  <on_reboot>restart</on_reboot>
  <on_crash>restart</on_crash>
  <devices>
    <emulator>/usr/bin/qemu-kvm</emulator>
    <disk type='file' device='disk'><! -- Specify the type parameter based on the image format.
Set type to qcow2 for the qcow2 format and vpc for the VHD format. -->
      <driver name='qemu' type='qcow2' cache='none' dataplane='on' io='native'/> <! -- If you
want to create a snapshot of the qcow2 format, you must disable dataplane. -->
      <source file='path'/> <! -- Enter the absolute path of the Alinyun Linux 2 image. -->
      <target dev='vda' bus='virtio'/>
    </disk>
    <! -- Add the information of seed.img. -->
    <disk type='file' device='disk'>
      <driver name='qemu' type='raw'/>
      <source file='/path/to/your/seed.img'/> <! -- Enter the absolute path of seed.img. -->
      <target dev='vdb' bus='virtio'/>
    </disk>
    <interface type='network'>
      <source network='default'/>
      <model type='virtio'/>
    </interface>
    <console type='pty'>
      <target type='virtio' port='0'/>
```

```
    </console>
    <video>
      <model type='cirrus' vram='9216' heads='1'/>
      <alias name='video0'/>
    </video>
    <input type='tablet' bus='usb'/>
    <input type='mouse' bus='ps2'/>
    <graphics type='vnc' port='-1' autoport='yes'/>
  </devices>
</domain>
```

ii. Run the `virsh` command to start the KVM. The sample command is as follows:

```
virsh define alinux2.xml
virsh start KVMName    # Enter the actual name of the KVM.
```

- Run the `qemu-kvm` command line to start the KVM. You must add the following parameter information to the command line. Change the `file` parameter to the actual absolute path of the seed.img image.

  ```
  -drive file=/path/to/your/seed.img,if=virtio,format=raw
  ```

  For more information about how to use the libvirt and qemu-kvm commands, visit Installing Virtualization Packages Manually.
- Use the graphical interface (virt-manager) to start the KVM. Before you start the KVM, find the configuration file of the KVM on your local computer and add the absolute path of the seed.img image file to the configuration file.

5.4.3. Use YUM to perform security updates

This topic describes how to use YUM to query, check, and install security updates for Alibaba Cloud Linux 2.

Background

To ensure system security, Alibaba Cloud Linux 2 stays up to date on Common Vulnerabilities and Exposures (CVE) as a community-based effort supported by the industry, promptly updates software packages including the kernel, and fix software defects and security vulnerabilities. For information about Alibaba Cloud Linux 2 security updates, see Alibaba Cloud Linux 2 security advisories.

Based on the Common Vulnerability Scoring System (CVSS3) for CVE, Alibaba Cloud Linux 2 divides security updates into the following severity levels:

- Critical: high-risk CVE, which you must update.
- Important: relatively high-risk CVE, which Alibaba Cloud strongly recommends you to update.
- Moderate: medium-risk CVE, which Alibaba Cloud recommends you to update.
- Low: low-risk CVE, which are optional for updates.

Query security updates

You can run the following command to query security updates:

```
yum updateinfo <command> [option]
```

The following table describes the parameters of the command.

Variable name	Value
command	• `list` : queries the list of available security updates. • `info <update_id>` : queries details about a specific security update. The value of `<update_id>` is an advisory ID in Alibaba Cloud Linux 2 security advisories.
option	• `--sec-severity=<SEVS>` or `--secseverity=<SEVS>` : specifies the security update severity level through the `<SEVS>` parameter. Notice The values of security update severity levels are case-sensitive. • `--cve=<CVES>` : specifies the CVE IDs. You can obtain the CVE IDs from Alibaba Cloud Linux 2 security advisories.

Usage examples of the commands used to query security updates are as follows:

- You can run the `yum updateinfo --help` command to obtain the help information about the command.
- You can run the `yum updateinfo` command to query all available security updates. Example:

```
# yum updateinfo
Loaded plugins: fastestmirror
Determining fastest mirrors
base                                                     | 3.1 kB  00:00
:00
extras                                                   | 2.5 kB  00:0
0:00
plus                                                     | 2.5 kB  00:00:
00
updates                                                  | 2.9 kB  00:
00:00
(1/6): extras/2.1903/x86_64/primary_db
| 149 kB  00:00:00
(2/6): base/2.1903/x86_64/group_gz
| 101 kB  00:00:00
(3/6): updates/2.1903/x86_64/updateinfo
|  81 kB  00:00:00
(4/6): plus/2.1903/x86_64/primary_db
| 1.5 MB  00:00:00
(5/6): base/2.1903/x86_64/primary_db
| 4.9 MB  00:00:00
(6/6): updates/2.1903/x86_64/primary_db
| 6.1 MB  00:00:00
Updates Information Summary: updates
   17 Security notice(s)
       7 Important Security notice(s)
       6 Moderate Security notice(s)
       4 Low Security notice(s)
updateinfo summary done
```

- You can run the `yum updateinfo list` command to query the list of available security updates. Example:

```
# yum updateinfo list
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
ALINUX2-SA-2019:0055 Moderate/Sec.  binutils-2.27-41.base.1.al7.x86_64
ALINUX2-SA-2019:0058 Low/Sec.       curl-7.29.0-54.1.al7.x86_64
ALINUX2-SA-2019:0059 Low/Sec.       elfutils-default-yama-scope-0.176-2.1.al7.n
...
```

- You can run the `yum updateinfo info <update_id>` command to query the details of a specified security update. Example:

```
# yum updateinfo info ALINUX2-SA-2020:0005
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile


==============================================================================
 ALINUX2-SA-2020:0005: nss, nss-softokn, nss-util security update (Important)
==============================================================================
  Update ID : ALINUX2-SA-2020:0005
    Release : Alibaba Cloud Linux 2.1903
       Type : security
     Status : stable
     Issued : 2020-01-03
       CVEs : CVE-2019-11729
            : CVE-2019-11745
Description : Package updates are available for Alibaba Cloud Linux 2.1903 that fix
            : the following vulnerabilities:
            :
            : CVE-2019-11729:
            : Empty or malformed p256-ECDH public keys may
            : trigger a segmentation fault due values being
            : improperly sanitized before being copied into
            : memory and used. This vulnerability affects
            : Firefox ESR < 60.8, Firefox < 68, and Thunderbird
            : < 60.8.
            :
            : CVE-2019-11745:
            : When encrypting with a block cipher, if a call to
            : NSC_EncryptUpdate was made with data smaller than
            : the block size, a small out of bounds write could
            : occur. This could have caused heap corruption and
            : a potentially exploitable crash. This
            : vulnerability affects Thunderbird < 68.3, Firefox
            : ESR < 68.3, and Firefox < 71.
            :
    Severity : Important
updateinfo info done
```

Check security updates

You can run the `yum check-update --security` command to check for security updates available for the system. By appending `--secseverity=<SEVS>` to the command, you can check for security updates of a specific severity level. The `<SEVS>` parameter specifies the security update severity level.

> **Notice** You can specify multiple security update severity levels and separate them with commas (,). The values of security update severity levels are case-sensitive.

Usage examples of checking for security updates are as follows:

- Example 1:

```
# yum check-update --security |grep available
49 package(s) needed for security, out of 183 available
```

- Example 2:

```
# yum check-update --security --secseverity=Critical,Important |grep available
30 package(s) needed for security, out of 183 available
```

Install security updates

You can use the `yum upgrade` command to install security updates in one of the following ways:

- You can run the `yum upgrade --security` command to install security updates. By appending `secseverity=<SEVS>` to the command, you can install security updates of a specific severity level. The `<SEVS>` parameter specifies the security update severity level.

  > **Notice** You can specify multiple security update severity levels and separate them with commas (,). The values of security update severity levels are case-sensitive.

  Example:

```
# yum upgrade --security --secseverity=Critical,Important
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
...
[snipped]
...
Transaction Summary
================================================================================
================================================================================
===============
Upgrade  30 Packages (+1 Dependent package)

Total download size: 91 M
Is this ok [y/d/N]:
```

- You can run the `yum upgrade -cves=<CVES>` command to install security updates of a specific CVE. The `<CVES>` parameter specifies the CVE ID.

  > **Notice** You can specify multiple CVE IDs and separate them with commas (,). The values of CVE IDs are case-sensitive.

  Example:

```
# yum upgrade --cve=CVE-2019-11729,CVE-2019-11745
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
...
[snipped]
...
Dependencies Resolved

================================================================================
================================================================================
===============
 Package                 Arch              Version                 Repository
Size
================================================================================
================================================================================
===============
Updating:
 nss                     x86_64            3.44.0-7.1.al7          updates
854 k
```

```
 nss-softokn                 x86_64                 3.44.0-8.1.al7                  updates
330 k
 nss-softokn-freebl          x86_64                 3.44.0-8.1.al7                  updates
225 k
 nss-sysinit                 x86_64                 3.44.0-7.1.al7                  updates
65 k
 nss-tools                   x86_64                 3.44.0-7.1.al7                  updates
528 k
 nss-util                    x86_64                 3.44.0-4.1.al7                  updates
79 k
Updating for dependencies:
 nspr                        x86_64                 4.21.0-1.1.al7                  updates
127 k

Transaction Summary
================================================================================
================================================================================
===============
Upgrade  6 Packages (+1 Dependent package)

Total download size: 2.2 M
Is this ok [y/d/N]:
```

Note The output of the `man yum` command shows that the `yum upgrade` command is equivalent to the `yum update --obsoletes` command. The `yum upgrade` command is also equivalent to the `yum update` command because `obsoletes` is enabled in the */etc/yum.conf* configuration file by default.

5.4.4. Enable the cgroup writeback feature

Alibaba Cloud Linux 2 supports the cgroup writeback feature for the cgroup v1 kernel interface in the kernel version 4.19.36-12.al7. This feature allows you to limit buffered I/O when you use the cgroup v1 kernel interface.

Context

cgroup refers to control group and consists of v1 and v2. For more information, visit What are Control Groups. This topic describes how to enable the cgroup writeback feature for cgroup v1 to limit buffered I/O of processes.

Limits

After you enable cgroup writeback, check whether the mapping between the memory subsystem (memcg) and the I/O subsystem (blkcg) conforms to the following rule. If yes, limit buffered I/O of processes.

memcg and blkcg must work together to enable the cgroup writeback feature. Then the cgroup writeback feature limits buffered I/O. However, by default, the control subsystems of the cgroup v1 kernel interface do not work together. Therefore, memcg and blkcg must be associated together through a certain rule. The rule is: each memcg must map a unique blkcg. The mapping between memcg and blkcg can be one-to-one or many-to-one, but can never be one-to-many or many-to-many.

For example, to limit buffered I/O of Processes A and B, you must take note of the following items:

- If A and B belong to two different memcg subsystems, the two memcg subsystems can each be mapped to different blkcg subsystems. For example, A belongs to `memcg1` and `blkcg1`. B belongs to `memcg2` and `blkcg0`.
- If A and B belong to two different memcg subsystems, the two memcg subsystems can also be mapped to the same blkcg subsystem. For example, A belongs to `memcg1` and B belongs to `memcg2`. Both A and B can be mapped to `blkcg2`.
- If A and B belong to the same memcg, the memcg can only be mapped to the same blkcg. For example, assume both A and B belong to `memcg0` and are mapped to `blkcg3`.

After you enable the cgroup writeback feature and before you limit buffered I/O of a process, we recommend that you configure the `cgroup.procs` interface of blkcg by writing a process ID to this interface to avoid exceptions and ensure that the memcg maps to a unique blkcg. You can also use a tool to view the mapping between memcg and blkcg. For more information, see Verify the mapping between memcg and blkcg.

During O&M, a process may move to another cgroup. Based on the preceding rule, if the process moves between two memcg subsystems, no issue occurs. If the process moves between two blkcg subsystems, an exception occurs. To avoid exceptions, the code of the cgroup writeback feature defines the following rule: If a process in a running blkcg moves between two blkcg subsystems, the original memcg maps to the root blkcg. Typically, no throttling threshold is set for the root blkcg. When the original memcg maps to the root blkcg, the throttling does not take effect.

> **Notice** Although the kernel code defines the rule to avoid exceptions, we recommend that you prevent processes from moving between two blkcg subsystems.

Enable cgroup writeback

The cgroup writeback feature in the cgroup v1 interface is disabled by default. To enable this feature, complete the following steps:

1. Add the `cgwb_v1` field to the `grubby` command to enable the cgroup writeback feature.In this example, the kernel version is `4.19.36-12.al7.x86_64`. Enter your actual kernel version during this operation. To query your kernel version, run the `uname -a` command.

```
sudo grubby --update-kernel="/boot/vmlinuz-4.19.36-12.al7.x86_64" --args="cgwb_v1"
```

2. Restart the system to allow the cgroup writeback feature to take effect.

```
sudo reboot
```

3. Run the following command to read the `/proc/cmdline` kernel file. You can see that the command line parameter of the kernel contains the `cgwb_v1` field. This indicates that the `blkio.throttle.write_bps_device` and `blkio.throttle.write_iops_device` interfaces in blkcg can limit buffered I/O.

```
cat /proc/cmdline | grep cgwb_v1
```

Verify the mapping between memcg and blkcg

Before you limit buffered I/O of a process, you can use one of the following methods to check whether the mapping between memcg and blkcg is one-to-one or many-to-one.

- Run the following command to view the mapping between memcg and blkcg.

```
sudo cat /sys/kernel/debug/bdi/bdi_wb_link
```

The following sample response shows that the mapping between the memcg and blkcg conforms to the one-to-one mapping rule.

```
memory    <--->    blkio
memcg1:   35 <---> blkcg1:   48
```

- Use the ftrace kernel monitoring tool.
  i. Enable the ftrace tool.

```
sudo bash -c "echo 1 > /sys/kernel/debug/tracing/events/writeback/insert_memcg_blkcg_link/enable"
```

  ii. View the output interface.

```
sudo cat /sys/kernel/debug/tracing/trace_pipe
```

The following sample response contains `memcg_ino=35 blkcg_ino=48`, which indicates that the mapping between the memcg and blkcg conforms to the one-to-one mapping rule.

```
<... >-1537  [006] ....   99.511327: insert_memcg_blkcg_link: memcg_ino=35 blkcg_ino=48 old_blkcg_ino=0
```

Verify whether cgroup writeback is effective

In this example, two processes that generate I/O are simulated to verify whether the cgroup writeback feature is effective.

> **Note**
>
> - Because the `dd` command is responding quickly and the screen rolls too fast to view, run the `iostat` command to view the result.
> - Because the `dd` command displays response data in sequence, 1 MB of data is generated for sequential I/O refresh. Therefore, you must set the threshold of `blkio.throttle.write_bps_device` to a value no less than 1 MB (1048576 bytes). If you set blkio.throttle.write_bps_device to a value less than 1 MB, I/O hangs may occur.

1. Simulate two processes that generate I/O, and firstly set the `cgroup.procs` interface of blkcg based on the preceding limits.

```
sudo mkdir /sys/fs/cgroup/blkio/blkcg1
sudo mkdir /sys/fs/cgroup/memory/memcg1
sudo bash -c "echo $$ > /sys/fs/cgroup/blkio/blkcg1/cgroup.procs"  # $$ is your process ID.
sudo bash -c "echo $$ > /sys/fs/cgroup/memory/memcg1/cgroup.procs"  # $$ is your process ID.
```

2. Use the `blkio.throttle.write_bps_device` interface in blkcg to limit buffered I/O.

```
sudo bash -c "echo 254:48 10485760 > /sys/fs/cgroup/blkio/blkcg1/blkio.throttle.write_bps_device
"  # Configure writeback throttling of the disk to 10 MB/s based on the device number.
```

3. Use the `dd` command that does not contain the `oflag=sync` parameter to generate buffered I/O.

```
sudo dd if=/dev/zero of=/mnt/vdd/testfile bs=4k count=10000
```

4. Use the iostat tool to query results. View the `wMB/s` output column. If the value is 10 MB/s, the cgroup writeback feature has taken effect.

```
iostat -xdm 1 vdd
```

5.4.5. Configure the weight-based throttling feature of blk-iocost

Alibaba Cloud Linux 2 provides the weight-based throttling feature (blk-iocost) based on the cost model in the kernel version 4.19.81-17.al7.x86_64 and later. blk-iocost improves the weight-based disk throttling feature of the I/O subsystem (blkcg) within a kernel. Both cgroup v1 and cgroup v2 interfaces support blk-iocost in Alibaba Cloud Linux 2. This topic describes the interfaces that implement throttling.

Interface description

Interface	Description	Configuration item

Interface	Description	Configuration item
cost.qos	A read/write interface whose file is stored only in the root group of blkcg. The full name of the file is `blkio.cost.qos` in cgroup v1 and `io.cost.qos` in cgroup v2. This interface provides the blk-iocost feature and limits the rate of I/O quality of service (QoS) based on the latency weight. After blk-iocost is enabled, the kernel calculates the proportion of requests that exceed the read and write latency `rlat|wlat` in all requests. When the proportion is greater than `rlat|wlat`, the kernel considers the disk to be saturated and reduces the number of requests sent to the disk. By default, the value of `rlat|wlat` is set to 0, indicating that the blk-iocost feature is disabled.	Each line of configuration in the interface file starts with the Major and Minor numbers of the disk in the `MAJ:MIN` format, followed by the following configuration items: • enable: specifies whether to enable the blk-iocost controller to enable blk-iocost. The default value 0 indicates that blk-iocost is disabled. A value of 1 indicates that blk-iocost is enabled. • ctrl: the control mode. Valid values: `auto` and `user`. When the control mode is set to `auto`, the kernel automatically detects the disk type and uses built-in parameters. When the control mode is set to `user`, you must specify the following QoS control parameters: • rpct: the read latency percentile. Valid values: 0 to 100. • rlat: the read latency threshold. Unit: microseconds. • wpct: the write latency percentile. Valid values: 0 to 100. • wlat: the write latency threshold. Unit: microseconds. • min: the minimum scaling percentage. Valid values: 1 to 10000. • max: the maximum scaling percentage. Valid values: 1 to 10000.

Interface	Description	Configuration item

cost.model	A read/write interface whose file is stored only in the root group of blkcg. The full name of the interface file is `blkio.cost.model` in cgroup v1 and `io.cost.model` in cgroup v2. The interface is used to set the cost model.	Each line of configuration in the interface file starts with the Major and Minor numbers of the disk in the `MAJ:MIN` format, followed by the following configuration items:
		• ctrl: the control mode. It specifies whether to allow the user to enter model parameters. Valid values: `auto` and `user`.
		• model: the model parameter. Valid value: `linear`. You must define the following modeling parameters when the value of the model parameter is `linear`:
		  ○ [r|w]bps: the maximum sequential I/O throughput.
		  ○ [r|w]seqiops: the sequential input/output operations per second (IOPS).
		  ○ [r|w]randiops: the random IOPS.
		Note You can use the *tools/cgroup/iocost_coef_gen.py* script in the kernel source code to generate the preceding parameters and then write these parameters to the interface file of cost.model to configure the cost model.

Interface	Description	Configuration item
cost.weight	A read/write interface whose file is stored only in the sub-group of blkcg. The full name of the interface file is `blkio.cost.weight` in cgroup v1 and `io.cost.weight` in cgroup v2. This interface is used to set the weight of a sub-group. Default value: 100. Valid values: 1 to 10000. The interface can be used to set a weight for each disk or change the default weight of a sub-group.	• If you set the weight of the interface to `<weight>`, the default weight of blkcg is changed to <weight>. • If you set the port number and weight of the interface to `MAJ:MIN <weight>`, the weight of blkcg on the MAJ:MIN disk is changed to <weight>.

Precautions

The blk-iocost feature allows the system to automatically configure IO monitoring (`ctrl=auto`). To use this feature, you must disable the `rotational` interface (echo 0 >) for ultra disks, standard SSDs, enhanced SSDs, or local NVMe SSDs.

```
echo 0 > /sys/block/[$DISK_NAME]/queue/rotational  # Replace [$DISK_NAME] with the actual disk name.
```

Example 1

Use the *cost.qos* interface to enable the blk-iocost feature for the `254:48` disk. If more than 95% of requests have a latency `(rlat|wlat)` of more than 5 milliseconds, the disk is considered to be saturated. The kernel will adjust the speed of the disk to send requests to fall within the interval from 50% to 150% of the original speed. The following commands are used for the cgroup v1 and cgroup v2 interfaces:

- The command for cgroup v1:

  ```
  echo "254:48 enable=1 ctrl=user rpct=95.00 rlat=5000 wpct=95.00 wlat=5000 min=50.00 max=150.00" > /sys/fs/cgroup/blkio/blkio.cost.qos
  ```

- The command for cgroup v2:

  ```
  echo "254:48 enable=1 ctrl=user rpct=95.00 rlat=5000 wpct=95.00 wlat=5000 min=50.00 max=150.00" > /sys/fs/cgroup/io.cost.qos
  ```

Example 2

Use the `cost.model` interface to configure a model on the `254:48` disk based on the `linear` modeling parameters. The following commands are used for the cgroup v1 and cgroup v2 interfaces:

- The command for cgroup v1:

```
echo "254:48 ctrl=user model=linear rbps=2706339840 rseqiops=89698 rrandiops=110036 wbps=10631
26016 wseqiops=135560 wrandiops=130734" > /sys/fs/cgroup/blkio/blkio.cost.model
```

- The command for cgroup v2:

```
echo "254:48 ctrl=user model=linear rbps=2706339840 rseqiops=89698 rrandiops=110036 wbps=10631
26016 wseqiops=135560 wrandiops=130734" > /sys/fs/cgroup/io.cost.model
```

Example 3

Use the `cost.weight` interface to change the default weight of blkcg1 to 50 and then set the weight of blkcg1 on the `254:48` disk to 50. The following commands are used for the cgoup v1 and cgoup v2 interfaces:

- The command for cgroup v1:

```
echo "50" > /sys/fs/cgroup/blkio/blkcg1/blkio.cost.weight    # Change the default weight to 50.
echo "254:48 50" > /sys/fs/cgroup/blkio/blkcg1/blkio.cost.weight    # Set the weight of blkcg1 on the
disk to 50.
```

- The command for cgroup v2:

```
echo "50" > /sys/fs/cgroup/cg1/io.cost.weight    # Change the default weight to 50.
echo "254:48 50" > /sys/fs/cgroup/cg1/io.cost.weight    # Set the weight of blkcg1 on the disk to 50.
```

Common monitoring tools

- iocost monitor script

  The `tools/cgroup/iocost_monitor.py` script in the kernel source code uses the drgn debugger to directly obtain kernel parameters and then provides the I/O performance monitoring data. For more information about drgn, visit drgn. The script is used in the following manner:

  Run the following command to monitor the I/O performance data of the *vdd* disk:

```
./iocost_monitor.py vdd
```

  A response similar to the following one is returned:

```
vdd RUN  per=500.0ms cur_per=3930.839:v14620.321 busy= +1 vrate=6136.22% params=hdd
                 active    weight     hweight% inflt% dbt  delay usages%
blkcg1                *    50/   50   9.09/  9.09   0.00   0  0*000 009:009:009
blkcg2                *   500/  500  90.91/ 90.91   0.00   0  0*000 089:091:092
```

- The blkio.cost.statcost.stat interface file of cgroup v1

  The Alibaba Cloud Linux 2 kernel provides the blk-iocost interface file of the cgroup v1 interface. This interface file records the QoS data of each controlled device. Run the following command to view the interface file:

```
cat /sys/fs/cgroup/blkio/blkcg1/blkio.cost.stat
```

A response similar to the following one is returned:

```
254:48 is_active=1 active=50 inuse=50 hweight_active=5957 hweight_inuse=5957 vrate=159571
```

- ftrace monitoring tool

  The Alibaba Cloud Linux 2 kernel provides the ftrace tool related to blk-iocost for kernel-side analytics. The ftrace monitoring tool is used in the following manner:

  i. Set the `enable` attribute to 1 to enable the ftrace tool.

  ```
  echo 1 > /sys/kernel/debug/tracing/events/iocost/enable
  ```

  ii. View the output information.

  ```
  cat /sys/kernel/debug/tracing/trace_pipe
  ```

  A response similar to the following one is returned:

  ```
    dd-1593  [008] d...   688.565349: iocost_iocg_activate: [vdd:/blkcg1] now=689065289:579865876
  62878 vrate=137438 period=22->22 vtime=0->57986365150756 weight=50/50 hweight=65536/6553
  6
    dd-1593  [008] d.s.   688.575374: iocost_ioc_vrate_adj: [vdd] vrate=137438->137438 busy=0 miss
  ed_ppm=0:0 rq_wait_pct=0 lagging=1 shortages=0 surpluses=1
  <idle>-0     [008] d.s.   688.608369: iocost_ioc_vrate_adj: [vdd] vrate=137438->137438 busy=0 miss
  ed_ppm=0:0 rq_wait_pct=0 lagging=1 shortages=0 surpluses=1
    dd-1594  [006] d...   688.620002: iocost_iocg_activate: [vdd:/blkcg2] now=689119946:579940996
  11644 vrate=137438 period=22->26 vtime=0->57993412421644 weight=250/250 hweight=65536/65
  536
  <idle>-0     [008] d.s.   688.631367: iocost_ioc_vrate_adj: [vdd] vrate=137438->137438 busy=0 miss
  ed_ppm=0:0 rq_wait_pct=0 lagging=1 shortages=0 surpluses=1
  <idle>-0     [008] d.s.   688.642368: iocost_ioc_vrate_adj: [vdd] vrate=137438->137438 busy=0 miss
  ed_ppm=0:0 rq_wait_pct=0 lagging=1 shortages=0 surpluses=1
  <idle>-0     [008] d.s.   688.653366: iocost_ioc_vrate_adj: [vdd] vrate=137438->137438 busy=0 miss
  ed_ppm=0:0 rq_wait_pct=0 lagging=1 shortages=0 surpluses=1
  <idle>-0     [008] d.s.   688.664366: iocost_ioc_vrate_adj: [vdd] vrate=137438->137438 busy=0 miss
  ed_ppm=0:0 rq_wait_pct=0 lagging=1 shortages=0 surpluses=1
  ```

5.4.6. Enable the PSI feature for the cgroup v1 interface

In the Linux kernel, only the cgroup v2 interface supports the Pressure Stall Information (PSI) feature. Alibaba Cloud Linux 2 supports the PSI feature for the cgroup v1 interface in the kernel version 4.19.81-17.al7 to allow you to monitor the CPU, memory, and I/O performance. This topic describes how to enable the PSI feature in the cgroup v1 interface and query relevant information.

Context

PSI is a kernel feature that can be used to monitor the CPU, memory, and I/O performance. For more information about the PSI feature, see the kernel document `Documentation/accounting/psi.txt`. The kernel document is contained in the Debuginfo package and source code package of Alibaba Cloud Linux 2. For information about how to download the Debuginfo package and source code package, see Use Alibaba Cloud Linux 2.

Enable the PSI feature for the cgroup v1 interface

By default, the PSI feature of the cgroup v1 interface is disabled. You can complete the following steps to enable the PSI feature:

1. Run the `grubby` command to change the startup parameter.The default value of the `args` parameter is `"psi=1"`, which indicates that the PSI feature has been enabled for cgroup v2. Change the value of the parameter to `"psi=1 psi_v1=1"`, which indicates that the PSI feature is enabled for cgroup v1 in Alibaba Cloud Linux 2. In this example, the kernel version is `4.19.81-17.al7.x86_64`. You must use your actual kernel version during the operation. To query the kernel version, run the `uname -a` command.

   ```
   sudo grubby --update-kernel="/boot/vmlinuz-4.19.81-17.al7.x86_64" --args="psi=1 psi_v1=1"
   ```

2. Restart the system to apply the change.

   ```
   sudo reboot
   ```

Verify that the PSI feature has been enabled for the cgroup v1 interface

After the system restarts, you can run the following command to verify that the PSI feature has been enabled for the cgroup v1 interface in `/proc/cmdline` of the kernel.

```
cat /proc/cmdline | grep "psi=1 psi_v1=1"
```

Query the monitoring data of the CPU, memory, and I/O performance

When you enable the PSI feature for the cgroup v1 interface, the PSI monitoring data of the CPU, memory, and I/O performance are all transferred to the cpuacct controller. You can query detailed monitoring data by running the following commands:

```
cat /sys/fs/cgroup/cpuacct/cpu.pressure
cat /sys/fs/cgroup/cpuacct/memory.pressure
cat /sys/fs/cgroup/cpuacct/io.pressure
```

5.4.7. Change the TCP TIME-WAIT timeout period

In the Linux kernel, TCP/IP connections stay in the TIME-WAIT state for 60 seconds, and this period cannot be changed. However, in some scenarios such as heavy TCP loads, network performance can be improved if this period can be reduced. In this context, Alibaba Cloud Linux 2 provides a kernel interface in the 4.19.43-13.al7 kernel version to change the TCP TIME-WAIT timeout period. This topic describes how to use the kernel interface.

Context

The TIME-WAIT state is a mechanism in TCP/IP stacks that keeps sockets open after an application has shut down the sockets. By default, this state lasts for 60 seconds to ensure complete data transmission between the server and the client. If a large number of connections are in the TIME-WAIT state, network performance may be compromised. Therefore, Alibaba Cloud Linux 2 provides an interface to change the TIME-WAIT timeout period to improve network performance in high-concurrency scenarios. The value range of this interface is 1 to 600 seconds. The default value of the TIME-WAIT timeout period is 60 seconds.

Precautions

A timeout period of less than 60 seconds may violate the TCP/IP quiet time restriction and may cause some old data to be accepted as new or duplicated new data rejected as old. Therefore, we recommend that you adjust the TIME-WAIT timeout period on the advice of Alibaba Cloud technicians. For more information about the TCP/IP quiet time concept, visit IETF RFC 793.

Configuration methods

You can use one of the following methods to change the TIME-WAIT timeout period. In both methods, the `[$TIME_VALUE]` parameter specifies the new timeout period that you want to set.

- Run the `sysctl` command to change the TIME-WAIT timeout period.

  ```
  sysctl -w "net.ipv4.tcp_tw_timeout=[$TIME_VALUE]"
  ```

- Run the `echo` command as the root user and change the TIME-WAIT timeout period in the `/proc/sys/net/ipv4/tcp_tw_timeout` interface.

  ```
  echo [$TIME_VALUE] > /proc/sys/net/ipv4/tcp_tw_timeout
  ```

5.4.8. Enhance the monitoring of block I/O throttling

Alibaba Cloud Linux 2 provides interfaces in the 4.19.81-17.al7 kernel version to better monitor Linux block I/O throttling. This topic describes how to use the interfaces.

Context

Linux block I/O throttling (bit/s or IOPS) is required in multiple scenarios, especially those where cgroup writeback is enabled. You can perform I/O throttling related operations in a more convenient manner if block I/O throttling is well monitored. In this context, Alibaba Cloud Linux 2 provides interfaces to enhance the monitoring of block I/O throttling.

Interface description

Interface	Description
blkio.throttle.io_service_time	The total amount of time between request dispatch and request completion for I/O operations. Unit: nanoseconds.
blkio.throttle.io_wait_time	The total amount of time the I/O operations wait in the scheduler queues. Unit: nanoseconds.
blkio.throttle.io_completed	The total number of completed I/O operations. The parameter is used to calculate the average latency of the block I/O throttling layer.
blkio.throttle.total_io_queued	The number of I/O operations that were throttled in the past. The number of I/O operations that were throttled in the current cycle can be calculated based on periodic monitoring and be used to analyze whether an I/O latency is related to throttling.
blkio.throttle.total_bytes_queued	The total bytes of I/O that were throttled in the past. Unit: bytes.

The path of the preceding interfaces is */sys/fs/cgroup/blkio/<cgroup>/*, where `<cgroup>` is the control group.

Example

You can obtain the average I/O latency of a disk by using the interface that enhances the monitoring of block I/O throttling. In this example, the average I/O write latency of the *vdd* disk is monitored at an interval of five seconds. Then, the average I/O latency of the *vdd* disk is calculated. The following table describes relevant parameters.

Parameter	Description
write_wait_time<N>	Obtains the duration of block I/O throttling.
write_service_time<N>	Obtains the total amount of time between request dispatch and request completion for I/O operations.
write_completed<N>	Obtains the number of completed I/O operations.

1. Obtain the monitoring data at the T1 time.

```
write_wait_time1 = `cat /sys/fs/cgroup/blkio/blkcg1/blkio.throttle.io_wait_time | grep -w "254:48 Write" | awk '{print $3}'`
write_service_time1 = `cat /sys/fs/cgroup/blkio/blkcg1/blkio.throttle.io_service_time | grep -w "254:48 Write" | awk '{print $3}'`
write_completed1 = `cat /sys/fs/cgroup/blkio/blkcg1/blkio.throttle.io_completed | grep -w "254:48 Write" | awk '{print $3}'`
```

2. Wait five seconds and obtain the monitoring data at the T2 (T1 + 5s) time.

```
write_wait_time2 = `cat /sys/fs/cgroup/blkio/blkcg1/blkio.throttle.io_wait_time | grep -w "254:48 Write" | awk '{print $3}'`
write_service_time2 = `cat /sys/fs/cgroup/blkio/blkcg1/blkio.throttle.io_service_time | grep -w "254:48 Write" | awk '{print $3}'`
write_completed2 = `cat /sys/fs/cgroup/blkio/blkcg1/blkio.throttle.io_completed | grep -w "254:48 Write" | awk '{print $3}'`
```

3. Calculate the average I/O latency during the five seconds based on the following formula:Average I/O latency = (Total I/O duration at the T2 time - Total I/O duration at the T1 time)/(Number of completed I/O operations at the T2 time - Number of completed I/O operations at the T1 time).

```
avg_delay = `echo "((write_wait_time2 + write_service_time2) - (write_wait_time1+write_service_time1)) / (write_completed2 - write_completed1)" | bc`
```

5.4.9. Use the JBD2 optimization interface

As the kernel thread of the ext4 file system, JBD2 often experiences the shadow (BH_Shadow) state during its use, which can affect the system performance. To solve this problem, Alibaba Cloud Linux 2 provides an interface in the 4.19.81-17.al7 kernel version to optimize JBD2. This topic describes this interface.

Context

ext4 is one of the most common journaling file systems. The kernel thread of ext4 for updating journals is JBD2. JBD2 is a global resource for the ext4 file system. When the JBD2 kernel thread attempts to obtain access permissions from the cache, the cache page may be in the BH_Shadow state. In this case, JBD2 may wait an extended period of time for the cache page to write back to the disk, which can affect the system performance. To solve this problem, Alibaba Cloud Linux 2 provides the `force_copy` kernel interface to optimize JBD2. The system then copies the cache page to reduce the time that JBD2 requires to wait for the cache page in the BH_Shadow state to write back to the disk. In addition, Alibaba Cloud Linux 2 provides the `stats` interface to help analyze quality of service (QoS) issues related to the file system.

Interface description

Interface	Description
force_copy	The interface file is stored in */proc/fs/jbd2/<device>-8/force_copy*, where the `device` variable indicates the name of the Block Storage device. After you enable the force_copy interface, the system will force copy data, which reduces the waiting time of JBD2. **Notice** Running the interface will consume memory.
stats	The interface file is stored in */proc/fs/jbd2/<device>-8/stats*. The interface helps determine whether QoS issues in the file system are caused by JBD2.

Examples

The following examples show how to implement the `force_copy` and `stats` interfaces:

- By default, the `force_copy` interface is disabled. You can set the value of the interface to 1 to enable the interface or set the value to 0 to disable the interface.

  ```
  echo 1 > /proc/fs/jbd2/nvme0n1-8/force_copy    # Call the interface.
  ```

- Run the following command to query the `stats` interface:

  ```
  cat /proc/fs/jbd2/nvme0n1-8/stats
  ```

  The following sample response is returned:

  ```
  337 336 65536 0 14837 1701504 16 0 20058 5 33082732 605 942 1000 1000
  ```

  The following table describes the fields in the preceding sample response.

Field	Description
The first field	The ID of the transaction.
The second field	The number of transactions requested.
The third field	The maximum number of cached transactions.
The fourth field	The transaction wait time.
The fifth field	The latency of the transaction request.
The sixth field	The amount of time that the transaction ran.
The seventh field	The amount of time that the transaction was locked.

Field	Description
The eighth field	The amount of time that it took to refresh the transaction.
The ninth field	The transaction logging time.
The tenth field	The average transaction commit time.
The eleventh field	The number of handles contained in the transaction.
The twelfth field	The number of blocks contained in the transaction.
The thirteenth field	The number of blocks recorded for the transaction.
The fourteenth field	The time constant of the kernel configuration, in Hertz.
The fifteenth field	The period of the time constant of the kernel configuration in milliseconds.

5.4.10. Create a hard link across project quotas

By default, the ext4 file system contains constraints. You are not allowed to create hard links across project quotas. However, in practice certain scenarios will require the creation of hard links. Alibaba Cloud Linux 2 provides a custom interface that can bypass the constraints of the ext4 file system to create hard links across project quotas. This topic describes the interface for the function and the sample interface.

Context

Linux distributions support the following disk quota modes: user quota, group quota, and project quota. Compared with user quota and group quota, project quota provides a more fine-grained disk quota. Project quota identifies directories and files within the file system by project ID. This topic describes how to create a hard link across project ID directories in the ext4 file system.

Interface description

The default value of the */proc/sys/fs/hardlink_cross_projid* interface is 0. In this case, hard links cannot be created across project quotas. If the */proc/sys/fs/hardlink_cross_projid* interface is set to 1, you can bypass the constraints of the ext4 file system to create hard links across project quotas.

For more information about the interface, see `Documentation/sysctl/fs.txt`. You can obtain the kernel document from the Debuginfo package and the source code package provided by Alibaba Cloud Linux 2. For more information, see Use Alibaba Cloud Linux 2.

Example

You can run the following command to query the value of the */proc/sys/fs/hardlink_cross_projid* interface:

```
cat /proc/sys/fs/hardlink_cross_projid
```

A value of `0` is returned, indicating that hard links cannot be created across project quotas.

You can change the value from 0 to 1 to create hard link across project quotas.

```
echo 1 > /proc/sys/fs/hardlink_cross_projid
```

5.4.11. Track I/O latency

Alibaba Cloud Linux 2 optimizes the `/proc/diskstats` interface, which is the raw data source of the I/O latency analysis tool iostat. Alibaba Cloud Linux 2 can calculate the duration of time in read, write and special I/O (discard) on the device. In addition, Alibaba Cloud Linux 2 provides the bcc tool to track I/O latency. This topic describes the optimized `/proc/diskstats` interface and the bcc tool.

Interface description

The */proc/diskstats* interface in Alibaba Cloud Linux 2 allows you to query the I/O information on a disk and the amount of time spent on read, write, and discard operations on a device.

Example: query the */proc/diskstats* interface as a root user.

```
cat /proc/diskstats
```

A sample response is as follows:

```
254       0 vda 6328 3156 565378 2223 1610 424 25160 4366 0 1358 5332 0 0 0 0 2205 3347 0
```

In the response, the last three domains are new domains added in Alibaba Cloud Linux 2. The following table describes the three domains:

Domain	Description
The sixteenth domain	The read duration on the device. Unit: milliseconds.
The seventeenth domain	The write duration on the device. Unit: milliseconds.
The eighteenth domain	The discard duration on the device. Unit: milliseconds.

Note For information about other domains, see the kernel document `Documentation/iostats.txt`. You can obtain the kernel document from the Debuginfo package and the source code package of Alibaba Cloud Linux 2. For more information, see Use Alibaba Cloud Linux 2.

bcc

Alibaba Cloud Linux 2 provides the bcc tool that helps you track I/O latency. You must download the tool before you use it. The download command is as follows:

```
yum install -y bcc-tools
```

You can run one of the following commands to query the description of the bcc tool.

- Run the following command to query the description of the bcc tool.

  ```
  /usr/share/bcc/tools/alibiolatency -h
  ```

  The description is as follows:

```
usage: alibiolatency [-h] [-d DEVICE] [-i [DIS_INTERVAL]]
                     [-t [AVG_THRESHOLD_TIME]] [-T [THRESHOLD_TIME]] [-r]

Summarize block device I/O latency

optional arguments:
  -h, --help            show this help message and exit
  -d DEVICE, --device DEVICE
                        inspect specified device
  -i [DIS_INTERVAL], --dis_interval [DIS_INTERVAL]
                        specify display interval
  -t [AVG_THRESHOLD_TIME], --avg_threshold_time [AVG_THRESHOLD_TIME]
                        display only when average request process time is
                        greater than this value
  -T [THRESHOLD_TIME], --threshold_time [THRESHOLD_TIME]
                        dump request life cycle when single request process
                        time is greater than this value
  -r, --dump_raw        dump every io request life cycle

examples:
    ./alibiolatency        # summarize block I/O latency(default display interval is 2s)
    ./alibiolatency -d sda3  # inspect specified device /dev/sda3
    ./alibiolatency -i 2     # specify display interval, 2s
    ./alibiolatency -t 10    # display only when average request process time is greater than 10ms
    ./alibiolatency -T 20    # dump request life cycle when single request process time is greater than
20ms
    ./alibiolatency -r       # dump every io request life cycle
```

- Run the `man` command to query the description of the bcc tool.

```
man bcc-alibiolatency
```

5.4.12. Detect I/O hangs of file systems and block layers

An I/O hang occurs when the system becomes unstable or even goes down due to time-consuming I/O requests. To accurately detect I/O hangs, Alibaba Cloud Linux 2 extends the core data structure and provides the function to quickly locate and detect I/O hangs with low system overheads. This topic describes the interfaces for this function and the usage examples of these interfaces.

Interface description

Interface	Description
/sys/block/<device>/queue/hang_threshold	The interface can detect the threshold for I/O hangs. Unit of the threshold: milliseconds. Default value: 5000. The interface allows you to define the threshold for I/O hangs.
/sys/block/<device>/hang	The interface can return the number of I/O operations that exceeds the threshold for I/O hangs on the device.
/sys/kernel/debug/block/<device>/rq_hang	The interface can query details about I/O hangs.
/proc/<pid>/wait_res	The interface can query information about the resources that a process is waiting for.
/proc/<pid>/task/<tid>/wait_res	The interface can query information about the resources that a thread is waiting for.

The following table describes variables in the preceding interfaces.

Variable	Description
<device>	The name of the Block Storage device.
<pid>	The ID of the process.
<tid>	The ID of the thread.

Example 1

You can call the `/sys/block/<device>/queue/hang_threshold` interface to change the threshold for I/O hangs. In this example, the threshold is changed from 5,000 ms (the default value) to 10,000 ms.

1. Change the threshold for the *vdb* disk to 10,000 ms.

   ```
   echo 10000 > /sys/block/vdb/queue/hang_threshold
   ```

2. View the result of the threshold change.

   ```
   cat /sys/block/vdb/queue/hang_threshold
   ```

   A response similar to the following one is returned:

   ```
   10000
   ```

Example 2

You can call the `/sys/block/<device>/hang` interface to query the number of I/O operations that have I/O hangs on a disk. In this example, the queried disk is *vdb*.

The following query command is used:

```
cat /sys/block/vdb/hang
```

A response similar to the following one is returned:

```
0     1    # The value on the left indicates the number of read operations that have I/O hangs. The val
ue on the right indicates the number of write operations that have I/O hangs.
```

Example 3

You can call the `/sys/kernel/debug/block/<device>/rq_hang` interface to query the details of I/O hangs. In this example, the *vdb* disk is used.

The following query command is used:

```
cat /sys/kernel/debug/block/vdb/rq_hang
```

A response similar to the following one is returned:

```
ffff9e50162fc600 {.op=WRITE, .cmd_flags=SYNC, .rq_flags=STARTED|ELVPRIV|IO_STAT|STATS, .state=in_f
light, .tag=118, .internal_tag=67, .start_time_ns=1260981417094, .io_start_time_ns=1260981436160, .curr
ent_time=1268458297417, .bio = ffff9e4907c31c00, .bio_pages = { ffffc85960686740 }, .bio = ffff9e4907c31
500, .bio_pages = { ffffc85960639000 }, .bio = ffff9e4907c30300, .bio_pages = { ffffc85960651700 }, .bio = f
fff9e4907c31900, .bio_pages = { ffffc85960608b00 }}
```

The preceding response shows the details of an I/O operation. `io_start_time_ns`, which indicates the start time of the I/O request, is assigned a value. This indicates that the I/O request was not processed in time, leading to prolonged I/O consumption.

Example 4

You can call the `/proc/<pid>/wait_res` interface to query information about the resources that a process is waiting for. In this example, the `577` process is used.

The following query command is used:

```
cat /proc/577/wait_res
```

A response similar to the following one is returned:

```
1 0000000000000000 4310058496 4310061448    # 1 is the value of Field 1, 0000000000000000 the value of
Field 2, 4310058496 the value of Field 3, and 4310061448 the value of Field 4.
```

The following table describes the parameters in the sample responses.

Parameter	Description

Parameter	Description
Field 1	The type of the resource that the process is waiting for. A value of 1 indicates pages in the file system. A value of 2 indicates the block I/O layer.
Field 2	The address of the resource (page or block I/O layer) that the process is waiting for.
Field 3	The time at which the process began waiting for the resource.
Field 4	The time when the file is read. The difference between Field 4 and Field 3 is the time consumed while the process waits for the resource.

5.4.13. Memcg global minimum watermark rating

This topic describes the memcg global minimum watermark rating feature provided in Alibaba Cloud Linux 2 kernel version `4.19.91-18.al7` or later.

Context

Global memory reclaim has a great impact on system performance of the Linux kernel. When latency-sensitive tasks and resource-consuming tasks are deployed together, resource-consuming tasks request a large amount of memory instantly, causing the free memory of the system to reach the global minimum watermark (global wmark_min). As a result, direct memory reclaim is enabled for all system tasks, causing performance jitters for latency-sensitive tasks. Neither global kswapd backend reclaim nor memcg backend reclaim can resolve this problem.

In this context, Alibaba Cloud Linux 2 provides the memcg global minimum watermark rating feature. The global wmark_min of resource-consuming tasks is increased to trigger direct memory reclaim. The global wmark_min of latency-sensitive tasks is decreased to avoid direct memory reclaim. In this way, when a resource-consuming task requests a large amount of memory instantly, an increase in the global wmark_min throttles the resources used for the task for a short period to avoid direct memory reclaim for latency-sensitive tasks. After a certain amount of memory is reclaimed through global kswapd backend reclaim, the throttling of the resource-consuming task is stopped.

Interface files

The interface file that implements the memcg global minimum watermark rating feature is memory.wmark_min_adj. The value of this interface file indicates a percent of adjustment over the global minimum watermark (global wmark_min). Valid values: -25 to 50.

- This interface file inherits a value of 0 from its parent group when the interface file is created. The default value is 0.
- A negative value is a percent of adjustment over the range `[0, WMARK_MIN]`, where `WMARK_MIN` is the value of global wmark_min. Example:

  ```
  memory.wmark_min_adj=-25, memcg WMARK_MIN is "WMARK_MIN + (WMARK_MIN - 0) * (-25%)"
  ```

> **Note** A negative value also indicates a decrease of global wmark_min to increase the memcg QoS of latency-sensitive tasks.

- A positive value is a percent of adjustment over the range `[WMARK_MIN, WMARK_LOW]`, where `WMARK_MIN` and `WMARK_LOW` are values of global wmark_min and global wmark_low. Example:

  ```
  memory.wmark_min_adj=50, memcg WMARK_MIN is "WMARK_MIN + (WMARK_LOW - WMARK_MIN) * 50%
  "
  ```

  > **Note** A positive value also indicates an increase of global wmark_min to decrease the memcg QoS of resource-consuming tasks.

- When the offset global wmark_min is triggered, throttling is performed, and the throttling time is linearly proportional to the excessive memory usage. Valid values of throttling time: 1 to 1000. Unit: ms.

> **Note** This interface file is not stored in the memcg root directory.

Precautions

A multi-level memcg includes `effective memory.wmark_min_adj`, which is the final effective value of memory.wmark_min_adj. The values of memory.wmark_min_adj at all levels are traversed to obtain the maximum value. Intermediate nodes with the default value 0 are excluded. The following hierarchy shows an example.

```
    root
    / \
   A   D
  / \
 B   C
/ \
E   F
```

The following table describes the mapping between the values of memory.wmark_min_adj at each level and the final effective value.

Level	Value	Final effective value
A	-10	-10
B	-25	-10
C	0	0
D	50	50

Level	Value	Final effective value
E	-25	-10
F	50	50

Note

- The value displayed in the output of the **cat /sys/fs/cgroup/memory/<memcg path>/memory.wmark_min_adj** command is the final effective value. In the command, `<memcg path>` indicates the root path of the memcg.
- We recommend that you use the global minimum watermark rating feature together with global wmark_min. For example, you can set global wmark_min to 2 GB or more in */proc/sys/vm/min_free_kbytes*.

Configuration examples

Example 1: Configure global minimum watermark rating for the memcg of latency-sensitive tasks.

1. Run the **mkdir /sys/fs/cgroup/memory/test-lc** command to create a test file.
2. Run the **echo -25 > /sys/fs/cgroup/memory/test-lc/memory.wmark_min_adj** command to write the value `-25` to the interface file to increase the memcg QoS of latency-sensitive tasks.

Example 2: Configure global minimum watermark rating for the memcg of resource-consuming tasks.

1. Run the **mkdir /sys/fs/cgroup/memory/test-be** command to create a test file.
2. Run the **echo 25 > /sys/fs/cgroup/memory/test-be/memory.wmark_min_adj** command to write the value `25` to the interface file to decrease the memcg QoS of resource-consuming tasks.

5.4.14. Memcg backend asynchronous reclaim

The memory control group (memcg) backend asynchronous reclaim feature is provided in Alibaba Cloud Linux 2 kernel version `4.19.81-17.al7` or later. This topic describes the interface files that implement the memcg backend asynchronous reclaim feature.

Context

In community versions of the Linux kernel, the system allocates memory and triggers memcg-level direct memory reclaim when the memory reaches a limit set by a memcg. Direct memory reclaim is synchronous reclaim that occurs in the context of memory allocation and affects performance of the current process.

To resolve this problem, Alibaba Cloud Linux 2 provides the backend asynchronous reclaim feature for memcgs. This feature differs from the global kswapd kernel thread in that it uses the workqueue mechanism instead of a corresponding memcg kswapd kernel thread. Additionally, four memcg interface files are added in each of the cgroup v1 and cgroup v2 interfaces.

Precautions

- Memory allocation of the current memcg may recursively trigger the backend asynchronous reclaim of the parent group.
- When triggered, backend asynchronous reclaim starts from the memcg on which the feature is triggered and is performed in sequence down the hierarchy.
- When memory.high is configured and the value of memory.high is smaller than that of memory.limit_in_bytes, the values of memory.wmark_high and memory.wmark_low are calculated based on memory.high instead of memory.limit_in_bytes.

Interface files

Interface file	Description
memory.wmark_ratio	Specifies whether to enable the memcg backend asynchronous reclaim feature and sets the memcg memory watermark where asynchronous reclaim starts. Unit: percent of the memcg memory limit. Valid values: 0 to 100. • The default value is 0, which indicates that the memcg backend asynchronous reclaim feature is disabled. • When the value is not 0, the memcg backend asynchronous reclaim feature is enabled and the corresponding watermark is set.
memory.wmark_high	A read-only interface file. • When the memcg memory usage exceeds the value of this interface file, backend asynchronous reclaim is started. • The value of this interface file is calculated based on the following formula: `(memory.limit_in_bytes × memory.wmark_ratio/100)`. • When the memcg backend asynchronous reclaim feature is disabled, the default value of memory.wmark_high is the maximum value and the backend asynchronous reclaim feature is never triggered. • This interface file is not stored in the memcg root directory.
memory.wmark_low	A read-only interface file. • When the memcg memory usage is less than the value of this interface file, backend asynchronous reclaim is ended. • The value of this interface file is calculated based on the following formula: `memory.wmark_high - memory.limit_in_bytes × memory.wmark_scale_factor/10000`. • This interface file is not stored in the memcg root directory.
memory.wmark_scale_factor	Controls the gap between memory.wmark_high and memory.wmark_low. Unit: 0.01% of the memcg memory limit. Valid values: 1 to 1000. • This interface file inherits the value of its parent group when the interface file is created. The value of this interface file is 50, which indicates 0.50% of the memcg memory limit. This is the default value. • This interface file is not stored in the memcg root directory.

Configuration examples

1. Create a test file.

```
mkdir /sys/fs/cgroup/memory/test/
```

2. Specify the value of memory.limit_in_bytes.In this example, the value is 1 GiB.

```
echo 1G > /sys/fs/cgroup/memory/test/memory.limit_in_bytes
```

3. Configure memory.wmark_ratio.In this example, the memcg memory watermark where asynchronous reclaim starts is set to 95% of the memcg memory limit.

```
echo 95 > /sys/fs/cgroup/memory/test/memory.wmark_ratio
```

4. Run the **cat /sys/fs/cgroup/memory/test/memory.wmark_scale_factor** command to query the value of memory.wmark_scale_factor.The default value is 0.50% of the memcg memory limit.

```
50
```

5. Query the values of memory.wmark_high and memory.wmark_low.If the following values are displayed for memory.wmark_high and memory.wmark_low in the command outputs, the configurations are correct.
   - If the following value is displayed for memory.wmark_high in the **cat /sys/fs/cgroup/memory/test/memory.wmark_high** command output:

     ```
     1020051456
     ```

   - If the following value is displayed for memory.wmark_low in the **cat /sys/fs/cgroup/memory/test/memory.wmark_low** command output:

     ```
     1014685696
     ```

5.4.15. Memcg QoS feature of the cgroup v1 interface

The memory control group (memcg) quality of service (QoS) can be used to control locks and limits on memory usage in a memcg. In community versions of the Linux kernel, this feature is supported only in the `cgroup v2` interface, whereas in Alibaba Cloud Linux 2 kernel version `4.19.91-18.al7` or later, this feature is also supported in the `cgroup v1` interface.

Background information

In the Alibaba Cloud Linux 2 kernel, the `memcg QoS` feature is enabled in the `cgroup v1` interface by default. For more information about `memcg QoS`, visit `Documentation/admin-guide/cgroup-v2.rst`. You can obtain the kernel document from the Debuginfo package and the source code package of Alibaba Cloud Linux 2. For more information, see Use Alibaba Cloud Linux 2.

Precautions

When you use the memcg QoS feature of the `cgroup v1` interface, we recommend that you place your tasks in a memcg leaf node such as */sys/fs/cgroup/memory/<intermediate node>/<leaf node>/tasks*.

Interface files

This section describes the interface files that implement the memcg QoS feature of the `cgroup v1` interface in the Alibaba Cloud Linux 2 kernel.

Interface file	Description
memory.min	Absolutely locks the memory. Memory locked by this interface file is not reclaimed even if the system has no memory to reclaim. You can perform the following read and write operations on this file: • Read the size of locked memory from this interface file. • Write the size of locked memory to this interface file.
memory.low	Relatively locks the memory. Memory locked by this interface file may be partially reclaimed if the system has no other memory to reclaim. You can perform the following read and write operations on this file: • Read the size of locked memory from this interface file. • Write the size of locked memory to this interface file.
memory.high	Limits the memory usage. You can perform the following read and write operations on this file: • Read the usage limits on the memcg from this interface file. • Write the usage limits on the memcg to this interface file.

Examples

Create a test memcg at the memcg mount point such as */sys/fs/cgroup/memory/*, and ensure that the memcg includes the memory.min, memory.low, and memory.high interface files.

The following sample commands are provided for your reference:

```
mkdir /sys/fs/cgroup/memory/test
ls /sys/fs/cgroup/memory/test | grep -E "memory.(min|low|high)"
```

Sample command outputs:

```
memory.high
memory.low
memory.min
```

5.4.16. Memcg Exstat feature

This topic describes the memcg exstat (Extend/Extra) feature provided in Alibaba Cloud Linux 2 kernel version `4.19.91-18.al7` or later.

Context

Compared with the memcg exstat feature provided in community versions of the Linux kernel, the memcg exstat feature supported by the Alibaba Cloud Linux 2 kernel provides the following additional memcg statistical items:

- Interface files supported by the cgroup v1 interface: memory.events, memory.events.local, and memory.stat.
- Statistics on latency caused by adjustment of the global minimum watermark.
- Statistics on latency caused by backend asynchronous reclaim.

Features

Alibaba Cloud Linux 2 kernel features are implemented based on kernel interfaces. This topic describes the implementation methods for each feature.

Feature	Description
Statistics on memory events	The cgroup v2 interface of community versions of the Linux kernel supports the memory.events and memory.events.local interface files to show the number of times certain memory events have occurred in a memcg. For more information, see cgroup-v2.rst. The cgroup v1 interface of the Alibaba Cloud Linux 2 kernel supports the memory.events and memory.events.local interface files. **Note** The interface files are not stored in the memcg root directory.

Feature	Description
Statistics on memory workingsets	The cgroup v2 interface of community versions of the Linux kernel supports the memory.stat interface file. The interface file includes the following statistical items: `workingset refault`, `workingset activate`, and `workingset nodereclaim`. For more information, visit cgroup-v2.rst. The cgroup v1 interface of the Alibaba Cloud Linux 2 kernel supports the memory.stat interface file. The interface file includes the following statistical items: `workingset refault`, `workingset activate`, `workingset nodereclaim`, and `workingset restore`. The official description of `workingset restore` is as follows: + workingset_restore + Number of restored pages which have been detected as an active + workingset before they got reclaimed.
Statistics on latency caused by adjustment of the global minimum watermark	Alibaba Cloud Linux 2 provides the memcg global minimum watermark rating feature. For more information, see Memcg global minimum watermark rating. Alibaba Cloud Linux 2 provides statistics on the throttling time resulted when the offset global minimum watermark in the memcg.exstat interface file is exceeded. The statistical item is `wmark_min_throttled_ms`. Note This statistical item is recursive to the parent group, and the interface file is not stored in the memcg root directory. Statistics description: • Interface file: *memory.exstat* • Statistical item: `wmark_min_throttled_ms` • Unit: ms

Feature	Description
Statistics on latency caused by backend asynchronous reclaim	Alibaba Cloud Linux 2 provides the backend asynchronous reclaim feature, memcg kswapd. For more information, see Memcg backend asynchronous reclaim. Alibaba Cloud Linux 2 provides statistics on latency caused by backend asynchronous reclaim in the memcg.exstat interface file. Such statistics include the block time and actual working time during reclaim. The statistical item is `wmark_reclaim_work_ms`. **Note** This statistical item is recursive to the parent group, and the interface file is not stored in the memcg root directory. Statistics description: • Interface file: *memory.exstat* • Statistical item: `wmark_reclaim_work_ms` • Unit: ms

Examples

Create a test file at the */sys/fs/cgroup/memory* memcg mount point, and ensure that the test file path includes the memory.events, memory.events.local, and memory.exstat interface files, and that the memory.stat interface file includes the `workingset` statistical item.

1. Run the **mkdir /sys/fs/cgroup/memory/test** command to create the test file.
2. Query the memory.events, memory.events.local, and memory.exstat interface files.
   i. Run the **cat /sys/fs/cgroup/memory/test/memory.events** command to query the memory.events interface file.
   An example of the query result is shown as follows:

   ```
   low 0
   high 0
   max 0
   oom 0
   oom_kill 0
   ```

   ii. Run the **cat /sys/fs/cgroup/memory/test/memory.events.local** command to query the memory.events.local interface file.
   An example of the query result is shown as follows:

   ```
   low 0
   high 0
   max 0
   oom 0
   oom_kill 0
   ```

iii. Run the **cat /sys/fs/cgroup/memory/test/memory.exstat** command to query the memory.exstat interface file.
An example of the query result is shown as follows:

```
wmark_min_throttled_ms 0
wmark_reclaim_work_ms 0
```

3. Run the **cat /sys/fs/cgroup/memory/test/memory.stat | grep workingset** command to check whether the memory.stat interface file includes the `workingset` statistical item.
A command output similar to the following one indicates that the interface file includes the `workingset` statistical item.

```
workingset_refault 0
workingset_activate 0
workingset_restore 0
workingset_nodereclaim 0
total_workingset_refault 0
total_workingset_activate 0
total_workingset_restore 0
total_workingset_nodereclaim 0
```

5.5. Knowledge base about Alibaba Cloud Linux 2

This topic provides the troubleshooting information and solutions about Alibaba Cloud Linux 2 issues.

- How do I configure the Kdump file in a Alibaba Cloud Linux 2 system?
- There is a delay in system time synchronization after the ECS instance Alibaba Cloud Linux 2.1903 the image is started or restarted.
- You cannot run the yum command on Alibaba Cloud Linux 2 ECS instances of the classic network system.
- A segfault error occurs when the ECS instances of the Alibaba Cloud Linux 2 system are running Docker images of earlier versions.
- The route information cannot be queried or configured on the ECS instance of the Alibaba Cloud Linux 2 system.
- The application on the ECS instance occasionally suffers packet loss and the kernel Log (dmesg) contains the error message "kernel: nf_conntrack: table full, dropping packet".
- Alibaba Cloud Linux 2 ECS instances fail to create a large number of processes after a large number of processes are created.
- Influence of TCP congestion control algorithm BBR on network performance in Alibaba Cloud Linux 2 system
- The Buffer I/O write performance of the Ext4 file system in the ECS instance of the Alibaba Cloud Linux 2 is not as expected.
- The Alibaba Cloud Linux 2 field value returned when the ECS instance of the Send-Q system

runs the ss command is 0
- Transparent huge page THP-related performance optimization in Alibaba Cloud Linux 2

5.6. FAQ about Alibaba Cloud Linux 2

This topic describes the frequently asked questions (FAQ) about Alibaba Cloud Linux 2 images and their solutions.

What are the differences between Aliyun Linux and Alibaba Cloud Linux 2?

Alibaba Cloud Linux 2 differs in the following aspects:

- Alibaba Cloud Linux 2 is optimized for containers to better support cloud-native applications.
- Alibaba Cloud Linux 2 is equipped with an updated Linux kernel and updated user-mode packages.

How do I use Alibaba Cloud Linux 2 in Alibaba Cloud public cloud?

Alibaba Cloud provides public images for Alibaba Cloud Linux 2. You can choose **Public Image** > **Alibaba Cloud Linux**, and then select a version of Alibaba Cloud Linux 2 image when you create an ECS instance.

Will I be charged for using Alibaba Cloud Linux 2 in Alibaba Cloud ECS?

No, Alibaba Cloud Linux 2 images are free of charge. You will only be charged for the ECS instances to which the images are applied.

Which ECS instance types does Alibaba Cloud Linux 2 support?

Alibaba Cloud Linux 2 supports most ECS instance types, including ECS Bare Metal Instance types.

> **Note** Alibaba Cloud Linux 2 does not support instances on the Xen virtual machine monitor.

Does Alibaba Cloud Linux 2 support 32-bit applications or libraries?

No. Alibaba Cloud Linux 2 does not support 32-bit applications or libraries.

Does Alibaba Cloud Linux 2 provide a graphical user interface (GUI) desktop?

No. Alibaba Cloud Linux 2 does not provide a GUI desktop.

Can I view the source code of Alibaba Cloud Linux 2 components?

Yes. Alibaba Cloud Linux 2 is open source. You can use the yumdownloader tool or visit the official Alibaba Cloud download pages to download the source code package. You can also download the source code tree of the Aliyun Linux kernel from GitHub. For more information, visit Github.

Is Alibaba Cloud Linux 2 backward-compatible with the current Aliyun Linux version?

Yes. Alibaba Cloud Linux 2 is compatible with Aliyun Linux 17.01.

> **Note** You may need to re-compile a compiled kernel module on Alibaba Cloud Linux 2 before it can be used.

Can I use Alibaba Cloud Linux 2 on an on-premises environment?

Yes, you can use Alibaba Cloud Linux 2 on an on-premises environment. Alibaba Cloud Linux 2 provides local images in the qcow2 format. These images are supported only for Kernel-based virtual machines (KVMs). For more information, see Use Alibaba Cloud Linux 2 images in an on-premises environment.

Which third-party applications can run on Alibaba Cloud Linux 2?

Alibaba Cloud Linux 2 is binary compatible with CentOS 7.6.1810. Applications that can run on CentOS can also run on Alibaba Cloud Linux 2.

What are the advantages of Alibaba Cloud Linux 2 compared with other Linux operating systems?

Alibaba Cloud Linux 2 is binary compatible with CentOS 7.6.1810 and provides differentiated operating system features.

Compared with CentOS and RHEL, Alibaba Cloud Linux 2 has the following advantages:

- Updates are released at a faster pace. Updated Linux kernels, user-mode software, and toolkits are provided.
- Alibaba Cloud Linux 2 works out of the box and requires minimal configuration.
- Alibaba Cloud Linux 2 is optimized to work with the optimized hypervisor and maximizes performance for users.

- Unlike RHEL, Alibaba Cloud Linux 2 does not have any runtime charges. Different from CentOS, Alibaba Cloud provides commercial support for Alibaba Cloud Linux 2.

How does Alibaba Cloud Linux 2 protect data security?

Alibaba Cloud Linux 2 is binary compatible with CentOS 7.6.1810 and RHEL 7.6 and complies with the RHEL safety specifications. Alibaba Cloud Linux 2 uses the following tools to protect your data:

- Uses industry-standard vulnerability scan and security test tools to perform periodical security scanning.
- Periodically assesses the CVE patch updates of CentOS 7 to fix operating system security vulnerabilities.
- Supports existing solutions of Alibaba Cloud for operating system security hardening.
- Uses the same mechanism as CentOS 7 to release user security alerts and patch updates.

Does Alibaba Cloud Linux 2 support data encryption?

Yes. Alibaba Cloud Linux 2 uses the CentOS 7 data encryption toolkit implemented by Key Management Service (KMS) to encrypt data.

How do I grant permissions to manage Alibaba Cloud Linux 2?

You can grant management permissions in Alibaba Cloud Linux 2 in the same manner as you would in CentOS 7. This means the same commands can be used to grant management permissions in both Alibaba Cloud CentOS 7 images and Alibaba Cloud Linux 2.

6.Custom image

6.1. Create custom image

6.1.1. Create a custom image from a snapshot

You can create a custom image from a snapshot that contains the operating system and data of an ECS instance. Then, you can use the custom image to create multiple identical instances.

custom image duplicate environment preparation deployment with source code ECS

Prerequisites

A system disk snapshot is created. For more information, see Create a normal snapshot.

Context

Before you create custom images from snapshots, take note of the following points:

- Notes on snapshots used to create custom images:
  - A custom image can be created from a system disk snapshot or from a system disk snapshot and one or more data disk snapshots. Data disk snapshots alone cannot be used to create custom images.
  - Both encrypted and unencrypted snapshots can be used to create custom images.
  - If the ECS instance from which a snapshot was created expires or is released, the custom image created from the snapshot and the ECS instance created from the image are not affected.
- Notes on custom images:
  - Custom images cannot be used across regions. However, you can copy custom images from one region to another for later use. For more information, see Copy custom images.
  - Custom images are independent of the billing methods of the ECS instances from which the custom images were created. For example, custom images created from subscription ECS instances can be used to create pay-as-you-go instances.
- Notes on ECS instances created from custom images:
  - You can upgrade the configurations of ECS instances created from custom images, such as vCPUs, memory, bandwidth, and disks.
  - You can replace the operating systems of ECS instances created from custom images, and the custom image remains usable. For more information, see Replace the system disk (non-public images).
  - Unreachable network errors may occur after you use a custom image to create VPC-type ECS instances that run the Linux operating system. The errors may be caused by the configurations in */etc/sysconfig/network*. For more information, see How to solve unreachable network errors when a VPC-type instance is created from a custom image.
- Recommendations for data security:
  - For information about how to enhance the security of custom images, see Security suggestions for Alibaba Cloud custom images.

- Delete sensitive data from a snapshot in advance to enhance data security.

Procedure

1. Log on to the ECS console.
2. Use one of the following methods to find the system disk snapshot from which you want to create a custom image:
   - On the Instances page
     a. In the left-side navigation pane, choose **Instances & Images > Instances**.
     b. In the top navigation bar, select a region.
     c. Find the target instance. Click the instance ID or click **Manage** in the **Actions** column to go to the Instance Details page.
     d. In the left-side navigation pane, click **Snapshots**. Find the target snapshot whose **Disk Type(All)** is **System Disk**. Click **Create Custom Image** in the **Actions** column.
   - On the Snapshots page
     a. In the left-side navigation pane, choose **Storage & Snapshots > Snapshots**.
     b. In the top navigation bar, select a region.
     c. Find the target snapshot whose **Disk Type(All)** is **System Disk**. Click **Create Custom Image** in the Actions column.

3. In the **Create Custom Image** dialog box that appears, configure the following parameters.

Parameter	Description	Reference
System Snapshot ID	The snapshot must be a system disk snapshot.	N/A
Custom Image Name and Custom Image Description	Enter a name and description for the custom image to be created.	N/A
Add Data Disk Snapshot	Optional. Select **Add Data Disk Snapshot**, click **Add**, and then select the ID of a data disk snapshot. ○ If you do not select the ID of any data disk snapshot, an empty data disk is created with a default capacity of 5 GiB. ○ If you select the ID of a data disk snapshot, the resulting disk capacity is the same as the snapshot size.	快照概述

Parameter	Description	Reference
Tag	Select a tag. ○ Optional: In most scenarios, the tag is optional. ○ Required: When you log on as a RAM user bound with an authorization policy that requires tags, you must specify a tag. Otherwise, an error is reported, indicating insufficient permissions.	Create a resource with a specific tag

4. Click Create.

What's next

After the custom image is created, you can perform the following operations:

- Create an ECS instance by using a custom image
- Replace the system disk (non-public images)

Related information

- CreateImage

6.1.2. Create a custom image from an instance

After you create an instance, you can perform operations to customize the instance such as installing software and deploying application environments and create a custom image for the updated instance. Instances created from the custom image will contain all of the configured items, saving you the trouble of configuring these items for each new instance.

Prerequisites

Sensitive data is deleted from the instance to enhance data security.

Before you create a custom image from a Linux instance, check the following items:

- Check the network configuration of the instance. based on your Linux version. For more information, see How to solve unreachable network errors when a VPC-type instance is created from a custom image.
- The system disk has a sufficient amount of free space.

Context

When you create a custom image from an instance, a snapshot is generated for each disk in the instance. Together, all of the snapshots constitute a complete custom image, as shown in the following figure.

Before you create a custom image from an instance, note the following points:

- When you create a custom image from an instance, you do not need to stop the instance.

- When you create a custom image from an instance, the status of the instance cannot be changed. For example, if you stop, start, or restart an instance, the custom image creation will fail.
- You cannot create images for expired subscription instances. You can create a snapshot for the system disk of an instance and then use the snapshot to create a custom image.
- You cannot create images for released instances. If you have saved a system disk snapshot for an instance, you can use the snapshot to create a custom image.
- Custom images are located within the same region as the instances from which the images are created. For example, if an instance is located in the China (Hangzhou) region, the image created from the instance is also located in the China (Hangzhou) region. For more information about how to use images across regions, see Copy custom images.
- The amount of time it takes to create an image depends on the size of the disk from which the image is created.

When you create a custom image from a Linux instance, note the following points:

- Do not upload data disk information to the */etc/fstab* file. Otherwise, instances created from the image cannot be started.
- Do not upgrade the kernel or operating system version.
- Do not adjust the system disk partitions. Only disks with a single root partition are supported.
- Do not modify critical system files such as */sbin*, */bin*, and */lib*.
- Do not modify the default logon username root.

Procedure

1. Log on to the ECS console.
2. In the left-side navigation pane, choose **Instances & Images > Instances**.
3. In the top navigation bar, select a region.
4. Find the instance for which you want to create a custom image. In the **Actions** column, choose **More > Disk and Image > Create Custom Image**.
5. Enter the image name and description.
6. Click **Create**. The image can be used only after snapshots of all disks have been created. Image creation may take a while.

What's next

After you create a custom image, you can:

- Create an instance by using a custom image
- Share custom images
- Export a custom image

Related information

- Create a custom image from a snapshot
- Modify custom images

6.1.3. Create a custom image by using Packer

Packer is a lightweight open source tool for creating images and runs on commonly used mainstream operating systems such as Windows, Linux, and macOS. This topic describes how to install and use Packer to create a custom image.

Context

A Linux instance is used in these examples. For more information about how to install Packer in Windows, visit Packer documentation.

Step 1. Install Packer

1. Connect to a Linux instance. For more information, see Connect to a Linux instance by using a username and password.
2. Run the `cd /usr/local/bin` command to access the */usr/local/bin* directory.

   > **Note** The */usr/local/bin* directory is an environment variable directory. You can install Packer to this directory or the directory that is added to environment variables.

3. Run the `wget https://releases.hashicorp.com/packer/1.1.1/packer_1.1.1_linux_amd64.zip` command to download the Packer package. You can go to the Download Packer page to download other versions of Packer packages.
4. Run the `unzip packer_1.1.1_linux_amd64.zip` command to decompress the package.
5. Run the `packer -v` command to verify the installation status of Packer.
   - If the Packer version number is returned, Packer is installed.
   - If the `command not found` error is returned, Packer is not installed properly.

Step 2. Define a Packer template

If you want to use Packer to create a custom image, you must create a template in the JSON format. In the template, you must specify the image builder and provisioner. For more information, visit Alicloud Image Builder and Provisioners. Packer provides a variety of provisioners that allow you to configure the content generation mode for custom images. A Shell provisioner is used to define a Packer template in the following example.

Create a JSON file named *alicloud* in the Linux instance and paste the following information to the file:

```
{
    "variables": {
      "access_key": "{{env `ALICLOUD_ACCESS_KEY`}}",
      "secret_key": "{{env `ALICLOUD_SECRET_KEY`}}"
    },
    "builders": [{
      "type":"alicloud-ecs",
      "access_key":"{{user `access_key`}}",
      "secret_key":"{{user `secret_key`}}",
      "region":"cn-beijing",
      "image_name":"packer_basic",
      "source_image":"centos_7_02_64_20G_alibase_20170818.vhd",
      "ssh_username":"root",
      "instance_type":"ecs.n1.tiny",
      "internet_charge_type":"PayByTraffic",
      "io_optimized":"true"
    }],
    "provisioners": [{
      "type": "shell",
      "inline": [
        "sleep 30",
        "yum install redis.x86_64 -y"
      ]
    }]
  }
```

The following table describes the parameters that you must specify.

Parameter	Description
access_key	Your AccessKey ID. For more information, see Create an AccessKey. Note To avoid disclosing the AccessKey pair of your Alibaba Cloud account, we recommend that you create a RAM user and use the credentials of the RAM user to create an AccessKey pair. For more information, see Create a RAM user and Create an AccessKey.
secret_key	Your AccessKey secret. For more information, see Create an AccessKey.

Parameter	Description
region	The region of the temporary instance used to create the custom image.
image_name	The name of the custom image.
source_image	The name of the source image used to create the custom image. You can obtain the name from the public image list of Alibaba Cloud.
instance_type	The type of the temporary instance used to create the custom image.
internet_charge_type	The billing method for network usage of the temporary instance used to create the custom image.
provisioners	The provisioner used to create the custom image. For more information, visit Provisioners.

Step 3. Create a custom image by using Packer

Perform the following operations to create a custom image by using the Packer template file that you specified:

1. Run the `export ALICLOUD_ACCESS_KEY=<Your AccessKey ID>` command to import your AccessKey ID.
2. Run the `export ALICLOUD_SECRET_KEY=<Your AccessKey secret>` command to import your AccessKey secret.
3. Run the `packer build alicloud.json` command to create a custom image.

The command output is as follows. The following section describes how to create a custom image that contains ApsaraDB for Redis:

```
alicloud-ecs output will be in this color.
==> alicloud-ecs: Prevalidating alicloud image name...
alicloud-ecs: Found image ID: centos_7_02_64_20G_alibase_20170818.vhd
==> alicloud-ecs: Start creating temporary keypair: packer_59e44f40-c8d6-0ee3-7fd8-b1ba08ea94b8
==> alicloud-ecs: Start creating alicloud vpc
----------------------------
==> alicloud-ecs: Provisioning with shell script: /var/folders/3q/w38xx_js6cl6k5mwkrqsnw7w0000gn/T
/packer-shell257466182
alicloud-ecs: Loaded plugins: fastestmirror
----------------------------
alicloud-ecs: Total                                 1.3 MB/s | 650 kB 00:00
alicloud-ecs: Running transaction check
----------------------------
==> alicloud-ecs: Deleting temporary keypair...
Build 'alicloud-ecs' finished.
==> Builds finished. The artifacts of successful builds are:
--> alicloud-ecs: Alicloud images were created:
cn-beijing: m-2ze12578be1oa4ovs6r9
```

What's next

Create an ECS instance by using a custom image

Related information

- packer-provider
- Packer Documentation

6.1.4. Create and import an on-premises image by using Packer

Packer is a lightweight open source tool for creating images and runs on commonly used mainstream operating systems such as Windows, Linux, and macOS. This topic describes how to create an on-premises image for CentOS 6.9 and upload the image to Alibaba Cloud. You can create a Packer template to create images for other operating systems.

Prerequisites

- An AccessKey pair is created. For more information, see Create an AccessKey.

  > **Note** To avoid disclosing the AccessKey pair of your Alibaba Cloud account, we recommend that you create a RAM user and use the credentials of the RAM user to create an AccessKey pair. For more information, see Create a RAM user.

- The OSS service is activated. For more information, see Activate OSS.

Context

The following software versions are used in this topic. The operations may vary depending on your software version.

- Operating system of the on-premises server: Ubuntu 16.04
- Operating system from which to create an image: CentOS 6.9

Example

CentOS 6.9 is used in this example. Perform the following operations to create an on-premises image:

1. Run the `egrep "(svm|vmx)" /proc/cpuinfo` command to check whether your on-premises server or virtual machine supports Kernel-based Virtual Machine (KVM).
   If the following command output is returned, KVM is supported:

   ```
   pat pse36 clflush dts acpi mmx fxsr sse sse2 ss ht tm pbe syscall nx pdpe1gb rdtscp lm constant_t
   sc art arch_perfmon pebs bts rep_good nopl xtopology nonstop_tsc aperfmperf tsc_known_freq p
   ni pclmulqdq dtes64 monitor ds_cpl vmx est tm2 ssse3 sdbg fma cx16 xtpr pdcm pcid sse4_1 sse4_2
   x2apic movbe popcnt tsc_deadline_timer aes xsave avx f16c rdrand lahf_lm abm 3dnowprefetch ep
   b intel_pt tpr_shadow vnmi flexpriority ept vpid fsgsbase tsc_adjust bmi1 avx2 smep bmi2 erms inv
   pcid mpx rdseed adx smap clflushopt xsaveopt xsavec xgetbv1 xsaves dtherm ida arat pln pts hw
   p hwp_notify hwp_act_window hwp_epp
   flags       : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov
   ```

2. Run the following commands in sequence to install KVM if your on-premises server or virtual machine supports KVM:

   ```
   sudo apt-get install qemu-kvm qemu virt-manager virt-viewer  libvirt-bin bridge-utils  #Install
   KVM and related controls.
   ```

   ```
   sudo virt-manager  #Enable virt-manager.
   ```

   If you can create a virtual machine on the Graphical User Interface (GUI), KVM is installed.

3. Install Packer. For more information, see Use Packer to create a custom image.
4. Run the following commands in sequence to create a Packer template.

   > **Note** The following sample commands are based on the CentOS 6.9 operating system. If you want to create on-premises images for other operating systems, customize the *centos.json* configuration file. For more information, see Create a Packer template.

   ```
   cd /usr/local  #Switch the directory.
   ```

```
wget https://raw.githubusercontent.com/alibaba/packer-provider/master/examples/alicloud/local/centos.json  #Download the centos.json configuration file that is released by Alibaba Cloud.
```

```
wget https://raw.githubusercontent.com/alibaba/packer-provider/master/examples/alicloud/local/http/centos-6.9/ks.cfg  #Download the ks.cfg configuration file that is released by Alibaba Cloud.
```

```
mkdir -p http/centos-6.9  #Create a directory.
```

```
mv ks.cfg http/centos-6.9/  #Move the ks.cfg file to the http/centos-6.9 directory.
```

5. Run the following commands in sequence to create and import an on-premises image:

```
export ALICLOUD_ACCESS_KEY=<Your AccessKey ID>     #Import your AccessKey ID.
```

```
export ALICLOUD_SECRET_KEY=<Your AccessKey secret>  #Import your AccessKey secret.
```

```
packer build centos.json                    #Create an on-premises image and import it to Alibaba Cloud.
```

A command output similar to the following one is displayed:

```
qemu output will be in this color.
 ==> qemu: Downloading or copying ISO
    qemu: Downloading or copying: http://mirrors.aliyun.com/centos/6.9/isos/x86_64/CentOS-6.9-x86_64-minimal.iso
 ..................................................
 ==> qemu: Running post-processor: alicloud-import
    qemu (alicloud-import): Deleting import source https://oss-cn-beijing.aliyuncs.com/packer/centos_x86_64
 Build 'qemu' finished.
 ==> Builds finished. The artifacts of successful builds are:
 --> qemu: Alicloud images were created:
 cn-beijing: XXXXXXXX
```

6. Wait for a few minutes and go to the Images page in the ECS console to view the custom image in the corresponding region such as China (Beijing).

Create a Packer template

CentOS 6.9 is used in the preceding example to create an on-premises image. For more information, see Example. The following JSON file shows how to create a Packer template based on CentOS 6.9:

```
{"variables": {
```

```
    "box_basename": "centos-6.9",
    "build_timestamp": "{{isotime \"20060102150405\"}}",
    "cpus": "1",
    "disk_size": "4096",
    "git_revision": "__unknown_git_revision__",
    "headless": "",
    "http_proxy": "{{env `http_proxy`}}",
    "https_proxy": "{{env `https_proxy`}}",
    "iso_checksum_type": "md5",
    "iso_checksum": "af4axxxxxxxxxxxxxxxx192a2",
    "iso_name": "CentOS-6.9-x86_64-minimal.iso",
    "ks_path": "centos-6.9/ks.cfg",
    "memory": "512",
    "metadata": "floppy/dummy_metadata.json",
    "mirror": "http://mirrors.aliyun.com/centos",
    "mirror_directory": "6.9/isos/x86_64",
    "name": "centos-6.9",
    "no_proxy": "{{env `no_proxy`}}",
    "template": "centos-6.9-x86_64",
    "version": "2.1.TIMESTAMP"
  },
 "builders":[
   {
    "boot_command": [
     "<tab> text ks=http://{{ .HTTPIP }}:{{ .HTTPPort }}/{{user `ks_path`}}<enter><wait>"
    ],
    "boot_wait": "10s",
    "disk_size": "{{user `disk_size`}}",
    "headless": "{{ user `headless` }}",
    "http_directory": "http",
    "iso_checksum": "{{user `iso_checksum`}}",
    "iso_checksum_type": "{{user `iso_checksum_type`}}",
    "iso_url": "{{user `mirror`}}/{{user `mirror_directory`}}/{{user `iso_name`}}",
    "output_directory": "packer-{{user `template`}}-qemu",
    "shutdown_command": "echo 'vagrant'|sudo -S /sbin/halt -h -p",
    "ssh_password": "vagrant",
    "ssh_port": 22,
    "ssh_username": "root",
    "ssh_wait_timeout": "10000s",
    "type": "qemu",
```

```
        "vm_name": "{{ user `template` }}.raw",
        "net_device": "virtio-net",
        "disk_interface": "virtio",
        "format": "raw"
      }
    ],
   "provisioners": [{
        "type": "shell",
        "inline": [
            "sleep 30",
            "yum install cloud-util cloud-init -y"
          ]
      }],
     "post-processors":[
      {
        "type":"alicloud-import",
        "oss_bucket_name": "packer",
        "image_name": "packer_import",
        "image_os_type": "linux",
        "image_platform": "CentOS",
        "image_architecture": "x86_64",
        "image_system_size": "40",
        "region":"cn-beijing"
      }
     ]
}
```

QEMU builder is used in the preceding example to create a virtual machine image. The following table describes the required parameters for the Packer builder. For more information about other optional parameters, visit QEMU Builder.

Required parameters for the Packer builder

Parameter	Type	Description
iso_checksum	string	The checksum for the ISO file of the operating system. Packer verifies this parameter before a virtual machine with the ISO file attached is started. Make sure that you specify at least one of the iso_checksum and iso_checksum_url parameters. If you specified the iso_checksum parameter, the value of iso_checksum_url is automatically ignored.

Parameter	Type	Description
iso_checksum_type	string	The checksum type of the ISO file of the specified operating system. Valid values: • none: If you set iso_checksum_type to none, the checksum process is ignored. This value is not recommended. • md5 • sha1 • sha256 • sha512
iso_checksum_url	string	A URL that points to a GNU- or BSD- style checksum file that contains the ISO file checksum of an operating system. Make sure that you specify at least one of the iso_checksum and iso_checksum_url parameters. If you specified the iso_checksum parameter, the value of iso_checksum_url is automatically ignored.
iso_url	string	A URL that points to the ISO file and contains the installation image. This URL can be an HTTP URL or file path: • If it is an HTTP URL, Packer downloads the file from the HTTP URL and caches the file for running it later. • If it is a file path to the IMG or QCOW2 file, QEMU builder uses the file to create a custom image. If you specified the file path, set disk_image to *true*.
headless	boolean	By default, Packer starts the GUI to build a QEMU virtual machine. If you set headless to *True*, a virtual machine without any console is started.

The provisioner used in the preceding example contains a Post-Processor module that enables automated upload of on-premises images to Alibaba Cloud. The following table describes the required parameters for the Packer provisioner. For more information about other optional parameters, visit Alicloud Import Post-Processor.

Required parameters for the Packer provisioner

Parameter	Type	Description
access_key	string	Your AccessKey ID.
secret_key	string	Your AccessKey secret.
region	string	The ID of the region where you want to upload your on-premises image. `cn-beijing` is used in this example. For more information about regions, see Regions and zones.

Parameter	Type	Description
image_name	string	The name of your on-premises image. • The name must be 2 to 128 characters in length. • The name must start with a letter. • The name can contain letters, digits, underscores (_), and hyphens (-). • The name cannot start with http:// or https://.
oss_bucket_name	string	The name of your OSS bucket. If you specify a bucket name that does not exist, Packer automatically creates a bucket with the specified name when Packer uploads the image.
image_os_type	string	The type of the image. Valid values: • linux • windows
image_platform	string	The distribution of the image. CentOS is used in this example.
image_architecture	string	The architecture of the image. Valid values: • i386 • x86_64
format	string	The format of the image. Valid values: • RAW • VHD

What's next

You can use the custom image uploaded to Alibaba Cloud to create ECS instances. For more information, see Create an ECS instance by using a custom image.

Related information

References

- Packer Documentation
- packer
- opstools
- packer-provider
- Anaconda Kickstart

6.2. Import images

6.2.1. Image import procedure

Importing a local image file is applicable to scenarios where your business is deployed on the cloud. You can use the imported custom image to create an ECS instance or replace the system disk. This topic describes how to import an image.

Linux image import procedure

The Linux image import procedure is as follows:

1. Complete the following preparations on the source server before creating a custom image:
   i. Install an image compliance tool and use it to automatically check whether Linux settings meet the import requirements. For more information, see Use the image compliance tool.
   ii. Install cloud-init to allow instances running the image to complete the initialization configuration. For more information, see Install cloud-init.
   iii. Install VirtIO drivers to allow ECS instances created from the image to start. For more information, see Install a virtio driver.
2. Read Instructions for importing images.
3. Convert the image file format (except for RAW, VHD, and qcow2 image files). For more information, see Convert the image file format.
4. Import custom images.

   If the operating system of the custom image is not supported by Alibaba Cloud and cloud-init cannot be installed, you can select Customized Linux when importing a custom image. For more information, see Customize Linux images.

Windows Image import procedure

The Windows image import procedure is as follows:

1. Install a virtio driver
2. Instructions for importing images
3. Convert the image file format
4. Import custom images

6.2.2. Use the image compliance tool

Before you import custom images, we recommend that you use the image compliance tool to check whether the Linux operating system configurations meet import requirements. This topic describes how to use the image compliance tool provided by Alibaba Cloud to check the validity of a custom Linux image.

Background information

ECS allows you to create instances from imported custom images. You must import custom images to ECS before you can create instances from them. Custom images can be created based on on-premises servers, virtual machines (VMs), or cloud servers of other service providers. Custom images must meet certain requirements before they can be used in Alibaba Cloud. For more information, see Instructions for importing images.

We recommend that you use the image compliance tool of ECS to reduce the time needed to create a custom image. The image compliance tool is designed to automatically validate configuration items in a Linux server environment to identify non-compliant items, generate detection reports in TXT and JSON formats, and provide troubleshooting actions if required.

This topic uses a server running the CentOS 7.4 64-bit OS as an example.

Application scope

The image compliance tool only supports Linux images, such as Ubuntu, CentOS, Debian, Red Hat, SUSE Linux Enterprise Server (SLES), openSUSE, FreeBSD, and CoreOS.

Procedure

1. Log on to your server, VM, or cloud server.
2. Run the following command to download the image compliance tool to the current directory of your server:

   ```
   wget http://docs-aliyun.cn-hangzhou.oss.aliyun-inc.com/assets/attach/73848/cn_zh/1557459863884/image_check
   ```

   You can also download the image compliance tool directly.
3. Run the image compliance tool with root privileges to ensure that it can read permission-restricted configuration files.

   ```
   chmod +x image_check
   sudo <Path of the image compliance tool>/image_check -p [Destination path]
   ```

   In the preceding code example, *<Path of the image compliance tool>* is also the path where to generate the detection report. Therefore, run the following command to start the image compliance tool:

   ```
   sudo ./image_check
   ```

   > **Note** You can use `-p [Destination path]` to specify the path where to generate the detection report. If this parameter is not specified, the detection report will be generated in the same path as the image compliance tool.
4. Wait for the image compliance tool to check the system configurations.

```
Begin check your system.....
The report is generating.
----------------------------------------
The infomation you need to input when you import your image to Alibaba Cloud website:
Current system: CentOS
Architecture: x86_64
System disk size: 42 GB
----------------------------------------
Check driver                    [ OK ]
Check shadow file authority          [ OK ]
Check security                  [ OK ]
Check qemu-ga                    [ OK ]
Check network                   [ OK ]
Check ssh                      [ OK ]
Check firewall                  [ OK ]
Check filesystem                 [ OK ]
Check device id                 [ OK ]
Check root account               [ OK ]
Check password                  [ OK ]
Check partition table            [ OK ]
Check lib                      [ OK ]
Check disk size                 [ OK ]
Check disk use rate              [ OK ]
Check inode use rate             [ OK ]
----------------------------------------
16 items are OK.
0 items are failed.
0 items are warning.
----------------------------------------
The report is generated: /root/image_check_report_2019-05-10_13-28-21.txt
Please read the report to check the details.
```

5. View the detection report.

   The path of the detection report is displayed in the output of tool execution. In this example, the report is stored in the /root directory. The report is named in the format of `image_check_report_date_time.txt` or `image_check_report.json`.

Detection items

The compliance tool detects the following configuration items to ensure that ECS instances created from your custom image will be fully functional.

Detection item	Non-compliance issue	Suggestion
driver	The ECS instance cannot start correctly.	Install the virtualization driver. For more information, see Install cloud-init.
/etc/shadow	The password file cannot be modified. As a result, you cannot create an ECS instance from the custom image.	Do not run the `chattr` command to lock the */etc/shadow* file.
SElinux	The ECS instance cannot start correctly.	Do not start SELinux by modifying */etc/selinux/config*.
qemu-ga	Some services required by ECS are unavailable, and the instance is not fully functional.	Uninstall qemu-ga.
network	Network functions of the ECS instance are unstable.	Disable or delete Network Manager and enable the network service.
ssh	You cannot connect to the ECS instance from the console.	Enable the SSH service and do not set PermitRootLogin.
firewall	The system does not automatically configure your ECS instance environment.	Disable firewalls such as iptables, firewalld, IPFilter (IPF), IPFireWall (IPFW), or PacketFilter (PF).
file system	You cannot resize the disk.	• We recommend that you use the XFS, ext3, and ext4 file systems. • The ext2, UFS, and UDF file systems are supported. • Do not use the `64 bit` feature for the ext4 file system. **Note** The `64 bit` feature is one feature of the ext4 file system. You can run the **man ext4** command to view detailed descriptions.
device id	The ECS instance cannot start correctly.	Clean up the *fstab* file and remove unneeded device IDs from the file to make sure that the device IDs in use appear in the output of the **blkid** command.
root	The username and password cannot be used to connect to the ECS instance.	Reserve the root account.

Detection item	Non-compliance issue	Suggestion
passwd	You cannot add users to the ECS instance.	Retain the passwd command or reinstall the password file.
Partition table	The ECS instance cannot start correctly.	Use MBR partitioning.
/lib	The ECS instance cannot be configured automatically.	The */lib* and */lib64* files cannot be stored in absolute paths. Modify the storage paths of the */lib* and */lib64* files to their relative paths.
system disk	N/A	Increase the system disk capacity. The optimal system disk capacity is 40 GiB to 500 GiB. When you import images, configure the system disk capacity based on the virtual file size of images, instead of the size of images.
disk usage	Required drivers or services cannot be installed for the ECS instance.	Make sure that sufficient disk space is available.
inode usage	Required drivers or services cannot be installed for the ECS instance.	Make sure that sufficient inode resources are available.

The image compliance tool provides `OK`, `FAILED`, or `WARNING` detection result based on detection items.

- `OK`: The detection items all comply with requirements.
- `FAILED`: The detection items do not comply with requirements, which means ECS instances created from the custom image will not be able to start correctly. We recommend that you rectify the non-compliant items and create a new image to improve instance startup efficiency.
- `WARNING`: The detection items do not comply with requirements, which means ECS instances created from the custom image will be able to start correctly, but ECS cannot use valid methods to configure your instance. You can choose to immediately rectify the non-compliant items or temporarily retain the items and create an image.

Output items

The image compliance tool generates detection reports in both TXT and JSON formats in the destination path.

> **Note** You can use `-p [Destination path]` to specify the path where to generate the detection report. If this parameter is not specified, the detection report will be generated in the same path as the compliance tool.

- Reports in TXT format are named `image_check_report_date_time.txt`. The reports include server configuration information and detection results. The following example uses a server running the CentOS 7.4 64-bit OS.

```
The information you need to input when you import your image to Alibaba Cloud Website:
 Current system is: CentOS #Server operating system
 Architecture: x86_64 #System architecture
 System disk size: 42 GB #Server system disk capacity
 ----------------------------------------
 Check driver #Detection item name
 Pass: kvm drive is exist #Detection result
 Alibaba Cloud supports kvm virtualization technology
 We strongly recommend installing kvm driver.
```

- Reports in JSON format are named `image_check_report.json`. The reports include server configuration information and detection results. The following example uses a server running the CentOS 7.4 64-bit OS.

```
"platform": "CentOS", \\Server operating system
 "os_big_version": "7", \\Operating system version number (major)
 "os_small_version": "4", \\Operating system version number (minor)
 "architecture": "x86_64", \\System architecture
 "system_disk_size": "42", \\Server system disk capacity
 "version": "1.0.2", \\Compliance tool version
 "time": "2018-05-14_19-18-10", \\Detection time
 "check_items": [{
    "name": "driver", \\Detection item name
    "result": "OK", \\Detection result
    "error_code": "0", \\Error code
    "description": "Pass: kvm driver exists.", \\Description
    "comment": "Alibaba Cloud supports kvm virtualization technology. We strongly recommend insta
lling kvm driver."
 }]
}
```

What to do next

1. View Instructions for importing images.
2. Install a virtio driver.
3. Optional. Convert the image file format.
4. Import custom images.
5. Create an ECS instance by using a custom image.

6.2.3. Instructions for importing images

Before you import an image, we recommend that you read the following instructions to improve the efficiency of importing images and the availability of imported images.

Windows Server images

Before you begin

- Verify the integrity of the file system.
- Do not modify critical system files.
- Ensure that the system disk has sufficient free space.
- Configure the system disk size based on the virtual disk size rather than the image size. The system disk size can be 40 GiB to 500 GiB.
- Disable the firewall and allow traffic on RDP port 3389.
- Ensure that the logon password for the administrator account meets the password complexity requirements. The password must be 8 to 30 characters in length and must contain at least three of the following character types: uppercase letters, lowercase letters, digits, and special characters. Special characters include `( ) ` ~ ! @ # $ % ^ & * - _ + = | { } [ ] : ; ' < > , . ? /` The password cannot start with a forward slash (/).

Items not supported

- ISO images. Before you import ISO images to ECS, use tools such as VirtualBox installed on premises to convert the images to the RAW, VHD, or QCOW2 format.
- Installation of qemu-ga in images. If qemu-ga is installed, some of the services that ECS requires may be unavailable.
- Images that run the following operating system versions:
  - Windows XP
  - Windows 7
  - Windows 8
  - Windows 8.1
  - Windows 10
- Installation of a Community Edition virtio driver in Windows Server operating systems. If a Community Edition virtio driver is installed, remove the read-only attribute of the following files:
  - *C:\Windows\System32\drivers\netkvm.sys*
  - *C:\Windows\System32\drivers\balloon.sys*
  - *C:\Windows\System32\drivers\vioser.sys*
  - *C:\Windows\System32\drivers\viostor.sys*
  - *C:\Windows\System32\drivers\pvpanic.sys*

Items supported

- Multi-partition system disks.
- NTFS file systems and MBR partitions.
- Images in the RAW, QCOW2, or VHD format. If the image to be imported is not in the preceding formats, convert the image to a supported format before you import the image. For more information, see Convert the image format.
- Images that run the following operating systems:
  - Microsoft Windows Server 2016
  - Microsoft Windows Server 2012 R2

- Microsoft Windows Server 2012
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2008
- Windows Server 2003 Service Pack 1 or later

Linux images

Before you begin

- Verify the integrity of the file system.
- Do not modify critical system files such as */sbin*, */bin*, and */lib**.
  - Do not modify */etc/issue**. Otherwise, the system distribution cannot be identified by ECS and system creation errors will occur.
  - Do not modify */boot/grub/menu.lst*. Otherwise, the ECS instance cannot be started.
  - Do not modify */etc/fstab*. Otherwise, the exception partition cannot be loaded and ECS instances cannot be started.
  - Do not configure */etc/shadow* to be **read-only**. Otherwise, the password file cannot be modified and system creation errors will occur.
  - Do not modify */etc/selinux/config* to enable SELinux. Otherwise, the system cannot be started. If you must enable SELinux, see Enable or disable SELinux.
- Ensure that the system disk has sufficient free space.
- Disable the firewall and allow traffic on SSH port 22.
- Enable Dynamic Host Configuration Protocol (DHCP).
- Install XEN or KVM virtualization drivers. For more information, see Install a virtio driver.
- Install cloud-init to configure the hostname, NTP source, and YUM source. For more information, see Install cloud-init.
- Ensure that the logon password for the root account meets the password complexity requirements. The password must be 8 to 30 characters in length and must contain three of the following character types: lowercase letters, uppercase letters, digits, and special characters.Special characters include `( ) ` ~ ! @ # $ % ^ & * - _ + = | { } [ ] : ; ' < > , . ? /`

Items not supported

- ISO images. Before you import ISO images to ECS, use tools such as VirtualBox installed on premises to convert the images to the RAW, VHD, or QCOW2 format.
- Multiple network interfaces.
- IPv6 addresses.
- Adjustment of system disk partitions. Only disks with a single root partition are supported.
- Installation of qemu-ga in images. If qemu-ga is installed, some of the services that ECS requires may be unavailable.

Items supported

- Images in the RAW, QCOW2, or VHD format. If the image to be imported is not in the preceding formats, convert the image to a supported format before you import the image. For more information, see Convert the image format.
- MBR partitions and xfs, ext3, and ext4 file systems.
- Ext4 file system. However, the ext4 file system cannot contain the `64bit` feature, and the `pr`

oject and quota features cannot be used together. You can run the following command to view the list of features contained in the ext4 file system:

```
tune2fs -l <ext4 file system disk directory> | grep features
```

- Images that run the following operating systems:
  - Alibaba Cloud Linux
  - CentOS 5, 6, and 7
  - CoreOS 681.2.0+
  - Debian 6/7
  - FreeBSD
  - OpenSUSE 13.1
  - RedHat
  - Red Hat Enterprise Linux (RHEL)
  - SUSE Linux 10, 11, and 12
  - Ubuntu 10, 12, 13, 14, 16, and 18

Non-standard Linux images

Linux images that are not listed as ECS public images are considered non-standard images. Such images are developed on a standard OS platform, but none of their critical system configuration files, basic system environments, and applications comply with ECS requirements for a standard operating system. If you want to use a non-standard platform image, select one of the following image types and perform corresponding operations:

- Others Linux: ECS identifies all images of this type as other Linux systems. If you import an Others Linux image and then use it to create instances, ECS does not process the created instances. If DHCP is disabled in the Others Linux image, you must connect to the instances by using the remote connection feature in the ECS console, and then manually configure IP addresses, routes, and passwords for the instances. If DHCP is enabled in the Others Linux image, networks are automatically configured for the instances when you log on to the instances.
- Customized Linux: After a Customized Linux image is imported, you can create instances from this image and configure networks and passwords for the instances in the same way as you do with instances created from standard ECS images. For more information, see Customize Linux images.

6.2.4. Install cloud-init

To ensure that the ECS instance running an image can complete the initialization configuration, we recommend that you install cloud-init on the server when you create a custom Linux image. This topic describes how to install Alibaba Cloud cloud-init and the native cloud-init.

cloud-init Alibaba Cloud image custom configuration

Context

cloud-init is open-source software used by cloud platforms to initialize Linux virtual machines. All major public cloud platforms such as Alibaba Cloud, Amazon Web Services (AWS), Microsoft Azure, and OpenStack support cloud-init. Alibaba Cloud cloud-init initializes the configurations of instances during their startup and executes user data scripts. These configurations include NTP, software sources, hostname, and SSH key pairs. For more information, visit cloud-init Documentation.

By default, cloud-init is installed for all Alibaba Cloud public images. To ensure that instances created from custom images can automatically initialize system configurations, we recommend that you install Alibaba Cloud cloud-init on your Linux server in the following scenarios:

- Linux servers will be migrated to the cloud but are not installed with cloud-init.

  > **Note** Proceed with caution when you install cloud-init on servers that you do not plan to migrate to the cloud.

- Linux servers are installed with cloud-init of versions earlier than 0.7.9.
- Alibaba Cloud ECS instances are not installed with cloud-init.

Description of cloud-init version

Different cloud platforms may use different versions of cloud-init. Select the appropriate version and configure it with the appropriate data source (datasource). The latest version of Alibaba Cloud cloud-init is 19.1.2, and the data source is `Aliyun`.

> **Notice** After cloud-init has been installed, it will automatically start during startup. If the installed version of cloud-init is not compatible with the operating system of the server or the data source is not configured properly, cloud-init may not run normally and the instance may start slowly or even fail to start the next time you restart the instance. Therefore, you must select a later version of cloud-init and an appropriate data source such as `Aliyun`.

When you use cloud-init, note the following differences among different versions:

- 0.7.6a: the initial version of Alibaba Cloud cloud-init, which depends on python2.7 for the Python environment. Some early public images still use cloud-init 0.7.6a.

  > **Note** The Python community no longer provides technical support for python2.7. Therefore, we recommend that you use later versions of cloud-init to avoid potential risks associated with the dependency library.

- 0.7.9 and earlier: initial versions of the native cloud-init, which are not applicable to initialize ECS instances and must be upgraded.
- 18: cloud-init 18 and later automatically initialize network configurations. The code for network configuration is `BOOTPROTO=dhcp DEVICE=eth0 ONBOOT=yes STARTMODE=auto TYPE=Ethernet USERCTL=no`. If you want to customize network configurations after you install cloud-init, see the Optional. Customize network configuration. section in this topic.
- 19.1: Alibaba Cloud public images are upgrading to be installed with cloud-init 19.1, which depends on python3.6 for the Python environment.

Check the cloud-init version

1. Log on to the source server.
2. Run the following command to check whether cloud-init is installed:

   ```
   which cloud-init
   ```

   If the output contains no path information, cloud-init is not installed. Install Alibaba Cloud cloud-init first.
3. Run the following command to check the version of cloud-init:

   ```
   cloud-init --version
   ```

   If the returned version is earlier than 0.7.9, install Alibaba Cloud cloud-init.
4. Back up data on the server.

Recommended. Install Alibaba Cloud cloud-init

Perform the following operations to download cloud-init 19.1.2 whose source code is `Aliyun`:

1. Ensure that the python-pip dependency library is installed on the source server. Run the following commands to install the python3-pip dependency library for some Linux distributions:
   - CentOS and Red Hat Enterprise Linux:

     ```
     yum -y install python3-pip
     ```
   - Ubuntu and Debian:

     ```
     apt-get -y install python3-pip
     ```
   - openSUSE and SUSE:

     ```
     zypper -n install python3-pip
     ```
2. Run the following command to install Alibaba Cloud cloud-init:

   ```
   wget https://ecs-image-utils.oss-cn-hangzhou.aliyuncs.com/cloudinit/cloud-init-19.1.2.tgz
   ```
3. Run the following command to decompress the cloud-init installation package to the current directory:

   ```
   tar -zxvf cloud-init-19.1.2.tgz
   ```
4. Go to the *tools* directory of the *cloud-init* file.
5. Run the following command to execute the *deploy.sh* script to install cloud-init:

   ```
   bash ./deploy.sh <issue> <major_version>
   ```

   The following table describes the parameters and values in the *deploy.sh* script.

Parameter	Description	Example

Parameter	Description	Example
issue	The type of the operating system. Valid values: *centos*, *redhat*, *rhel*, *debian*, *ubuntu*, *opensuse*, and *sles*. The parameter values are case-sensitive. *sles* stands for SUSE and SLES.	centos
major_version	The major version number of the operating system.	The major version number of CentOS 6.5 is *6*.

6. Check whether cloud-init is installed.
   If `"description": "success"` is returned, Alibaba Cloud cloud-init is installed.

The following sample shell scripts used to install Alibaba Cloud cloud-init are provided for your reference. Adapt the scripts based on your actual operation system.

- CentOS 6 and CentOS 7:

```
# Check whether the python3-pip dependency library has been installed. If not, install it.
if ! python3 -c 'import setuptools' >& /dev/null; then
  yum -y install python3-pip
fi
# Back up cloud-init of an earlier version.
test -d /etc/cloud && mv /etc/cloud /etc/cloud-old
# Download and decompress Alibaba Cloud cloud-init.
wget https://ecs-image-utils.oss-cn-hangzhou.aliyuncs.com/cloudinit/cloud-init-19.1.2.tgz
tar -zxvf ./cloud-init-19.1.2.tgz
# Install cloud-init.
issue_major=$( cat /etc/redhat-release | grep -Eo '[0-9]+\.?[ 0-9]+' | head -1 | awk -F'.' '{printf $1}')
bash ./cloud-init-*/tools/deploy.sh centos "$issue_major"
```

- Red Hat Enterprise Linux 6 and Red Hat Enterprise Linux 7:

```
# Check whether the python3-pip dependency library has been installed. If not, install it.
if ! python3 -c 'import setuptools' >& /dev/null; then
  yum -y install python3-pip
fi
# Back up cloud-init of an earlier version.
test -d /etc/cloud && mv /etc/cloud /etc/cloud-old
# Download and decompress Alibaba Cloud cloud-init.
wget https://ecs-image-utils.oss-cn-hangzhou.aliyuncs.com/cloudinit/cloud-init-19.1.2.tgz
tar -zxvf ./cloud-init-19.1.2.tgz
# Install cloud-init.
issue_major=$( cat /etc/os-release | grep VERSION_ID | grep -Eo '[0-9]+\.?[ 0-9]+' | head -1 | awk -F'.' '{
printf $1}')
bash ./cloud-init-*/tools/deploy.sh rhel "$issue_major"
```

- Ubuntu 14, Ubuntu 16, and Ubuntu 18:

```
# Check whether the python3-pip dependency library has been installed. If not, install it.
if ! python3 -c 'import setuptools' >& /dev/null; then
  apt-get install python36 python3-pip -y
fi
# Back up cloud-init of an earlier version.
test -d /etc/cloud && mv /etc/cloud /etc/cloud-old
# Download and decompress Alibaba Cloud cloud-init.
wget https://ecs-image-utils.oss-cn-hangzhou.aliyuncs.com/cloudinit/cloud-init-19.1.2.tgz
tar -zxvf ./cloud-init-19.1.2.tgz
# Install cloud-init.
issue_major=$( cat /etc/os-release | grep VERSION_ID | grep -Eo '[0-9]+\.?[ 0-9]+' | head -1 | awk -F'.' '{
printf $1}')
bash ./cloud-init-*/tools/deploy.sh ubuntu "$issue_major"
```

- Debian 8 and Debian 9:

```
# Check whether the python3-pip dependency library has been installed. If not, install it.
if ! python3 -c 'import setuptools' >& /dev/null; then
  apt-get -y install python3-pip
fi
# Back up cloud-init of an earlier version.
test -d /etc/cloud && mv /etc/cloud /etc/cloud-old
# Download and decompress Alibaba Cloud cloud-init.
wget https://ecs-image-utils.oss-cn-hangzhou.aliyuncs.com/cloudinit/cloud-init-19.1.2.tgz
tar -zxvf ./cloud-init-19.1.2.tgz
# Install cloud-init.
issue_major=$( cat /etc/os-release | grep VERSION_ID | grep -Eo '[0-9]+\.?[ 0-9]+' | head -1 | awk -F'.' '{
printf $1}')
bash ./cloud-init-*/tools/deploy.sh debian "$issue_major"
```

- SUSE 11 and SUSE 12:

```
# Check whether the python3-pip dependency library has been installed. If not, install it.
if ! python3 -c 'import setuptools'>& /dev/null; then
  zypper -n install python3-pip
fi
# Back up cloud-init of an earlier version.
test -d /etc/cloud && mv /etc/cloud/etc/cloud-old
# Download and decompress Alibaba Cloud cloud-init.
wget https://ecs-image-utils.oss-cn-hangzhou.aliyuncs.com/cloudinit/cloud-init-19.1.2.tgz
tar -zxvf ./cloud-init-19.1.2.tgz
# Install cloud-init.
issue_major=$( cat /etc/os-release | grep VERSION_ID | grep -Eo '[0-9]+\.?[ 0-9]+' | head -1 | awk -F'.' '{
printf $1}')
bash ./cloud-init-*/tools/deploy.sh sles "$issue_major"
```

- openSUSE 13 and openSUSE 42:

```
# Check whether the python3-pip dependency library has been installed. If not, install it.
if ! python3 -c 'import setuptools'>& /dev/null; then
  zypper -n install python3-pip
fi
# Back up cloud-init of an earlier version.
test -d /etc/cloud && mv /etc/cloud/etc/cloud-old
# Download and decompress Alibaba Cloud cloud-init.
wget https://ecs-image-utils.oss-cn-hangzhou.aliyuncs.com/cloudinit/cloud-init-19.1.2.tgz
tar -zxvf ./cloud-init-19.1.2.tgz
# Install cloud-init.
issue_major=$( cat /etc/os-release | grep VERSION_ID | grep -Eo '[0-9]+\.?[ 0-9]+' | head -1 | awk -F'.' '{
printf $1}')
bash ./cloud-init-*/tools/deploy.sh opensuse"$issue_major"
```

Optional. Install the native cloud-init

1. Make sure that you have installed the Git, Python, and python-pip dependency libraries for the source server. Run the following commands to install Git, python3.6, and python3-pip dependency libraries for some Linux distributions:
   - CentOS and Red Hat Enterprise Linux:

     ```
     yum -y install git python36 python3-pip
     ```
   - Ubuntu and Debian:

     ```
     apt-get -y install git python36 python3-pip
     ```
   - openSUSE and SUSE:

     ```
     zypper -n install git python36 python3-pip
     ```
2. Run the following command to download the cloud-init source code package from Git:

   ```
   git clone https://git.launchpad.net/cloud-init
   ```
3. Go to the cloud-init directory.

   ```
   cd ./cloud-init
   ```
4. Run the following command to install all the dependency libraries:

   ```
   pip3 install -r ./requirements.txt
   ```
5. Run the following command to install cloud-init:

   ```
   python3 setup.py install
   ```
6. Modify the *cloud.cfg* configuration file.

i. Open the configuration file.

```
vi /etc/cloud/cloud.cfg
```

ii. Modify the configuration before `cloud_init_modules:` as follows:

```
# Example datasource config
# The top level settings are used as module
# and system configuration.
# A set of users which may be applied and/or used by various modules
# when a 'default' entry is found it will reference the 'default_user'
# from the distro configuration specified below
users:
  - default
user:
   name: root
   lock_passwd: False
# If this is set, 'root' will not be able to ssh in and they
# will get a message to login instead as the above $user
disable_root: false
# This will cause the set+update hostname module to not operate (if true)
preserve_hostname: false
syslog_fix_perms: root:root
datasource_list: [ AliYun ]
# Example datasource config
datasource:
   AliYun:
      support_xen: false
      timeout: 5 # (defaults to 50 seconds)
      max_wait: 60 # (defaults to 120 seconds)
#     metadata_urls: [ 'blah.com' ]
# The modules that run in the 'init' stage
cloud_init_modules:
```

Optional. Customize network configuration.

1. After cloud-init is installed, open the */etc/cloud/cloud.cfg* file.

```
vim /etc/cloud/cloud.cfg
```

2. Add the disabled configuration before `Example datasource config` .

```
network:
 config: disabled
```

Note After the configuration is added, you must manage the network configuration under the */etc/sysconfig/network-scripts/* directory.

Troubleshooting

- The libraries that are missing may vary with images. You can use pip to install the libraries and then install cloud-init again.
- If the default software package manager (such as **yum**) and the **pip** manager have been installed with different versions of dependency libraries, library version conflicts may occur and cause cloud-init to run abnormally. We recommend that you download the dependency libraries based on the error message.

Error message	Cause	Troubleshooting command
`no setuptools module in python`	The python setuptools module is not installed.	The following example uses python3.6: • CentOS and Red Hat: `yum -y install python3-pip` • Ubuntu and Debian: `apt-get -y install python3-pip` • openSUSE and SUSE: `zypper -n install python3-pip`

`File "/root/cloud-init/cloudinit/log.py", line 19, in <module>`
`import six`
`ImportError: No module named six )`
	The six dependency library is not installed.	`pip3 install six`

`File "/root/cloud-init/cloudinit/url_helper.py", line 20, in <module>`
`import oauthlib.oauth1 as oauth1`
`ImportError: No module named oauthlib.oauth1 )`
	The oauthlib dependency library is not installed.	`pip3 install oauthlib`

Error message	Cause	Troubleshooting command
No uninstalled dependency libraries specified	The error message is not mapped.	Run the following command to install all dependency libraries that are listed in the *requirements.txt* file of cloud-init: `pip3 install -r requirements.txt`

What's next

- For Linux servers that will be migrated to the cloud:

  You can migrate the servers by using the Cloud Migration tool or importing the custom images. For more information, see Migrate your server to Alibaba Cloud by using the Cloud Migration tool or Import custom images.

- For Alibaba Cloud ECS instances that already run Linux custom images:

  You can restart the system to check the installation result. If the system automatically configures the hostname, software sources, and NTP, cloud-init is installed. For example, if the network configuration file shows the following content, cloud-init is installed:

```
[root@iZbp1ios3psx4hoi******Z ~]# cat /etc/sysconfig/network-scripts/ifcfg-eth0
# Created by cloud-init on instance boot automatically, do not edit.
#
BOOTPROTO=dhcp
DEVICE=eth0
ONBOOT=yes
STARTMODE=auto
TYPE=Ethernet
USERCTL=no
```

Related information

- cloud-init official website - Alibaba Cloud (AliYun)

6.2.5. Install a virtio driver

In some scenarios, you may want to use the operating system data of a source server such as a server, virtual machine or cloud web host to create a custom image, and import the custom image to Alibaba Cloud to create an ECS instance. If the source server is not installed with the virtio driver, the created ECS instance may be unable to be started. To avoid this problem, you must check whether a virtio driver is installed in the source server before you import the custom image to Alibaba Cloud.

virtio import a custom image manually install a virtio driver custom image

Context

You can determine whether to manually install the virtio driver based on the operating system of your source server.

Operating system	Description
• Windows Server 2008 • Windows Server 2012 • Windows Server 2016 • Windows Server Version **** (Semi-Annual Channel) • Windows Server 2019 and later • CentOS 6, CentOS 7, CentOS 8, and later • Ubuntu 12, Ubuntu 14, Ubuntu 16, Ubuntu 18, and later. • Debian 7, Debian 8, Debian 9, Debian 10, and later • SUSE 11, SUSE 12, SUSE 15, and later	If the source server runs one of the operating systems listed on the left, when you import the custom image to Alibaba Cloud, Alibaba Cloud automatically adds a virtio driver to the server. You do not need to manually install the virtio driver on the source server before you create the custom image. You must fix the temporary file systems of the servers that are pre-installed with a virtio driver when the temporary file system does not contain the configuration description of the driver. For more information, see Step 2: Fix the temporary file system.
Other operating systems	If your source server runs a Linux-like operating system that is not included in the preceding list, perform the following steps to install the virtio driver: 1. Step 1: Check whether the operating system kernel supports the virtio driver 2. Step 2: Fix the temporary file system 3. Step 3: Download the kernel installation package 4. Step 4: Compile the kernel

Step 1: Check whether the operating system kernel supports the virtio driver

1. Run the `grep -i virtio /boot/config-$(uname -r)` command to check whether the kernel of the current operating system supports the virtio driver.

   Check the CONFIG_VIRTIO_BLK and CONFIG_VIRTIO_NET parameters.

Check result	Description
The two parameters do not exist.	The virtio driver is not installed on the operating system and a custom image cannot be directly imported to Alibaba Cloud. You must compile the kernel and install the virtio driver for the source server. For more information, see Step 3: Download the kernel installation package and Step 4: Compile the kernel.
The parameter values are both m.	Go to the next step.

Check result	Description
The parameter values are both Y.	The virtio driver is installed on the operating system and a custom image can be directly imported to Alibaba Cloud. For more information, see Instructions for importing images and Import custom images.

2. Run the `lsinitrd /boot/initramfs-$(uname -r).img | grep virtio` command to check whether the virtio driver is included in the initramfs or initrd temporary file system.

> **Note**
>
> - The preceding figure shows that initramfs contains the virtio_blk installation file, and the virtio.ko, virtio_pci.ko, and virtio_ring.ko dependencies. Therefore, you can directly import your custom images to Alibaba Cloud. For more information, see Instructions for importing images and Import custom images.
> - If initramfs does not contain the virtio_blk installation file, you must fix the temporary file system before you import custom images to Alibaba Cloud.

Step 2: Fix the temporary file system

If the check result shows that the kernel of operating system supports virtio drivers but the initramfs or initrd temporary file system does not contain the virtio_blk installation file, you must fix the temporary file system. Operating systems such as CentOS are used in the following examples:

- CentOS/RedHat 5

```
mkinitrd -f --allow-missing \
        --with=xen-vbd  --preload=xen-vbd \
        --with=xen-platform-pci --preload=xen-platform-pci \
        --with=virtio_blk --preload=virtio_blk \
        --with=virtio_pci --preload=virtio_pci \
        --with=virtio_console --preload=virtio_console \
```

- CentOS/RedHat 6/7

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

- Debian/Ubuntu

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

Step 3: Download the kernel installation package

Note The *linux-4.4.24.tar.gz* kernel version is used in the following example. You must change the commands based on the kernel version of your operating system.

1. Run the `yum install -y ncurses-devel gcc make wget` command to install required components for the compilation of the kernel.
2. Run the `uname -r` command to query the kernel version of your operating system. In this example, the kernel version is 4.4.24-2.a17.x86_64.
3. Go to the Index of pub/linux/kernel to check the download link of the kernel version source code. The download link of *linux-4.4.24.tar.gz* is `https://www.kernel.org/pub/linux/kernel/v4.x/linux-4.4.24.tar.gz` as shown in the following figure.
4. Run the `cd /usr/src/` command to switch the directory.
5. Run the `wget https://www.kernel.org/pub/linux/kernel/v4.x/linux-4.4.24.tar.gz` command to download the installation package.
6. Run the `tar -xzf linux-4.4.24.tar.gz` command to decompress the installation package.
7. Run the `ln -s linux-4.4.24 linux` command to build a link.
8. Run the `cd /usr/src/linux` command to switch the directory.

Step 4: Compile the kernel

1. Run the following commands in sequence to compile the kernel:

```
make mrproper
symvers_path=$(find /usr/src/ -name "Module.symvers")
test -f $symvers_path && cp $symvers_path .
cp /boot/config-$(uname -r) . /.config
make menuconfig
```

2. Start to perform virtio-related configurations when the following page is displayed:

Note If you select the configurations that have the asterisks (*), the virtio driver is directly compiled into the kernel. If you select configurations that have *M*, the virtio driver is compiled into a module, and then the module is inserted into the kernel when the driver is to start.

i. Select Virtualization.

Select the Kernel-based Virtual Machine (KVM) support option.

```
Processor type and features  --->
  [*] Paravirtualized guest support  --->
    --- Paravirtualized guest support
(128)   Maximum allowed size of a domain in gigabytes
[*]   KVM paravirtualized clock
[*]   KVM Guest support
```

```
Device Drivers  --->
 [*] Block devices  --->
<M>   Virtio block driver (EXPERIMENTAL)
-*- Network device support  --->
   <M>   Virtio network driver (EXPERIMENTAL)
```

ii. Press the Esc key to exit the kernel configuration window and save the *.config* file.

iii. Check whether virtio-related configurations are complete. For more information, see the Step 1: Check whether the operating system kernel supports the virtio driver section.

iv. (Optional)If virtio-related configurations are not complete, run the following commands to manually edit the *.config* file:

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

v. Run the following commands to check the installation status of the virtio driver:

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

If one of the command outputs contains virtio-related files such as virtio_blk and virtio_pci.virtio_console, the virtio driver is installed.

What's next

After you install the virtio driver, you can perform the following operations:

- Migrate servers
- Import custom images

6.2.6. Customize Linux images

If the selected OS is not supported by Alibaba Cloud and cloud-init cannot be installed, you can select Customized Linux when you import a custom image. Alibaba Cloud regards customized Linux images as an unrecognized OS type. You must add a parsing script to the custom image before the import to automatically configure the instance when it is first started.

Limits

Customized Linux images have the following limits:

- The first partition must be writable.
- The type of the first partition must be FAT32, ext2, ext3, ext4, or UFS.
- The size of the virtual file of the customized Linux image must be larger than 5 GiB.

Customized Linux images have the following security requirements:

- No important vulnerabilities can be remotely exploited.
- When you log on to an instance for the first time through the management terminal of the ECS console, you are required to change the initial password (if there is any) before you can perform any other actions. For more information, see Connect to a Linux instance by using VNC.
- SSH key pairs are not supported. The initial SSH private key pair must be randomly generated by Alibaba Cloud.

Configuration method

Before you create and import a customized Linux image, you must perform the following operations:

1. Create the *aliyun_custom_image* directory in the root directory of the first partition of the server from which the image is created.

   When the instance created from the customized Linux image is started for the first time, Alibaba Cloud writes instance configurations to the *os.conf* file in the *aliyun_custom_image* directory. If the *os.conf* file does not exist, Alibaba Cloud will create one.

2. Create a parsing script in the image to parse the *os.conf* file to implement instance configurations.

   For more information about how to compile a script, see Considerations for the parsing script and Example of the parsing script.

Example of the os.conf file

- *os.conf* file for instances in the classic network

```
hostname=<yourHostName>
password=<yourPassword>
eth0_ip_addr=10.0.0.2
eth0_mac_addr=00:xx:xx:xx:xx:23
eth0_netmask=255.255.255.0
eth0_gateway=10.0.0.1
eth0_route="10.0.0.0/8 10.0.0.1;172.16.0.0/12 10.0.0.1"
eth1_ip_addr=42.0.0.2
eth1_mac_addr=00:xx:xx:xx:xx:24
eth1_netmask=255.255.255.0
eth1_gateway=42.0.0.1
eth1_route="0.0.0.0/0 42.0.0.1"
dns_nameserver="7.7.7.7 8.8.8.8"
```

The following table describes the parameters in the preceding example.

Parameter	Description
hostname	The name of the host.
password	The password, which is a Base64-encoded string.
eth0_ip_addr	The IP address of the eth0 NIC.
eth0_mac_addr	The MAC address of the eth0 NIC.
eth0_netmask	The network mask of the eth0 NIC.
eth0_gateway	The default gateway of the eth0 NIC.
eth0_route	The eth0 internal routes that are separated by semicolons (;) by default.
eth1_ip_addr	The IP address of the eth1 NIC.
eth1_mac_addr	The MAC address of the eth1 NIC.
eth1_netmask	The network mask of the eth1 NIC.
eth1_gateway	The default gateway of the eth1 NIC.
eth1_route	The eth1 Internet routes that are separated by semicolons (;) by default.
dns_nameserver	The DNS address list, in which addresses are separated by spaces by default.

- *os.conf* file for instances in VPCs

```
hostname=<yourHostName>
password=<yourPassword>
eth0_ip_addr=10.0.0.2
eth0_mac_addr=00:xx:xx:xx:xx:23
eth0_netmask=255.255.255.0
eth0_gateway=10.0.0.1
eth0_route="0.0.0.0/0 10.0.0.1"
dns_nameserver="7.7.7.7 8.8.8.8"
```

The following table describes the parameters in the preceding example.

Parameter	Description
hostname	The name of the host.
password	The password, which is a Base64-encoded string.
eth0_ip_addr	The IP address of the eth0 NIC.
eth0_mac_addr	The MAC address of the eth0 NIC.
eth0_netmask	The network mask of the eth0 NIC.
eth0_gateway	The default gateway of the eth0 NIC.
eth0_route	The eth0 internal routes that are separated by semicolons (;) by default.
dns_nameserver	The DNS address list, in which addresses are separated by spaces by default.

Considerations for the parsing script

Typically, when an instance is started for the first time, Alibaba Cloud writes instance configurations to the *os.conf* file. The os.confn file is in the *aliyun_custom_image* directory in the root directory of the first partition. However, you must create a predefined parsing script for a customized Linux image. The script will read the configurations from the *os.conf* file to configure the instance.

The parsing script must meet the following conditions:

Condition	Description
Automatic start at system startup	Set the parsing script to be automatically started at system startup by placing the script in the */etc/init.d/* directory.
Values for configuration items	As shown in Example of the os.conf file, instances in the classic network and instances in VPCs differ in the number of configuration items and values of some configuration items.

Condition	Description
Path for the configuration file	Device names allocated to the first partition for instances created from the customized Linux image vary depending on whether the instances are I/O optimized. We recommend that you use `uuid` or `label` in your parsing code to identify the device allocated for the first partition. The user password is a Base64-encoded string. Therefore, it must also be Base64-encoded in the parsing script.
Network type	When determining the network type, the parsing script can check whether there are eth1_route or eth1-related configuration items. The script will parse and process the instance accordingly based on the network type. • Instances within VPCs are configured with the default Internet route specified by the eth0_route parameter in the *os.conf* file. • Instances within the classic network are configured with the default Internet route specified by the eth1_route parameter in the *os.conf* file, and with the default internal route specified by the eth0_route parameter.
Configuration optimization	Configurations in the *os.conf* file are executed only once during the instance lifecycle. We recommend that you delete the *os.conf* file after the parsing script is executed. The parsing script will not execute the configurations in the *os.conf* file if the script does not read any.
Customized image processing	When a custom image is created based on a customized Linux image, the automatic startup script is also included. Alibaba Cloud will write configurations to the *os.conf* file when the instance is started for the first time. Then, the parsing script will immediately execute the configurations upon detection.
Configuration change processing	When instance configurations are changed through the Alibaba Cloud console or API operations, Alibaba Cloud writes new configurations to the *os.conf* file. Then, the parsing script will run again to issue the changes.

Example of the parsing script

A parsing script for CentOS is used in this example. You must change the script content based on your operating system and debug the script before you execute it.

```
#! /bin/bash


### BEGIN INIT INFO
# Provides:         os-conf
# Required-Start:    $local_fs $network $named $remote_fs
# Required-Stop:
# Should-Stop:
# Default-Start:     2 3 4 5
# Default-Stop:      0 1 6
# Short-Description: The initial os-conf job, config the system.
### END INIT INFO
```

```
first_partition_dir='/boot/'
os_conf_dir=${first_partition_dir}/aliyun_custom_image
os_conf_file=${os_conf_dir}/os.conf

load_os_conf() {
   if [[ -f $os_conf_file ]]; then
      . $os_conf_file
      return 0
   else
      return 1
   fi
}

cleanup() {
   # ensure $os_conf_file is deleted, to avoid repeating config system
   rm $os_conf_file >& /dev/null
   # ensure $os_conf_dir exists
   mkdir -p $os_conf_dir
}

config_password() {
   if [[ -n $password ]]; then
      password=$(echo $password | base64 -d)
      if [[ $? == 0 && -n $password ]]; then
         echo "root:$password" | chpasswd
      fi
   fi
}

config_hostname() {
   if [[ -n $hostname ]]; then
      sed -i "s/^HOSTNAME=. */HOSTNAME=$hostname/" /etc/sysconfig/network
      hostname $hostname
   fi
}

config_dns() {
   if [[ -n $dns_nameserver ]]; then
      dns_conf=/etc/resolv.conf
      sed -i '/^nameserver.*/d' $dns_conf
```

```
        for i in $dns_nameserver; do
            echo "nameserver $i" >> $dns_conf
        done
    fi
}

is_classic_network() {
    # vpc: eth0
    # classic: eth0 eth1
    grep -q 'eth1' $os_conf_file
}

config_network() {
    /etc/init.d/network stop
    config_interface eth0 ${eth0_ip_addr} ${eth0_netmask} ${eth0_mac_addr}
    config_route eth0 "${eth0_route}"
    if is_classic_network ; then
        config_interface eth1 ${eth1_ip_addr} ${eth1_netmask} ${eth1_mac_addr}
        config_route eth1 "${eth1_route}"
    fi
    /etc/init.d/network start
}

config_interface() {
    local interface=$1
    local ip=$2
    local netmask=$3
    local mac=$4
    inteface_cfg="/etc/sysconfig/network-scripts/ifcfg-${interface}"
    cat << EOF > $inteface_cfg
DEVICE=$interface
IPADDR=$ip
NETMASK=$netmask
HWADDR=$mac
ONBOOT=yes
BOOTPROTO=static
EOF
}

config_default_gateway() {
    local gateway=$1
```

```
    sed -i "s/^GATEWAY=. */GATEWAY=$gateway/" /etc/sysconfig/network
}

config_route() {
    local interface=$1
    local route="$2"
    route_conf=/etc/sysconfig/network-scripts/route-${interface}
    > $route_conf
    echo $route | sed 's/;/\n/' | \
        while read line; do
            dst=$(echo $line | awk '{print $1}')
            gw=$(echo $line | awk '{print $2}')
            if ! grep -q "$dst" $route_conf 2> /dev/null; then
                echo "$dst via $gw dev $interface" >> $route_conf
            fi
            if [[ "$dst" == "0.0.0.0/0" ]]; then
                config_default_gateway $gw
            fi
        done
}

################### sysvinit service portal ######################

start() {
    if load_os_conf ; then
        config_password
        config_network
        config_hostname
        config_dns
        cleanup
        return 0
    else
        echo "not load $os_conf_file"
        return 0
    fi
}

RETVAL=0

case "$1" in
    start)
```

```
    start
    RETVAL=$?
  ;;
  *)
    echo "Usage: $0 {start}"
    RETVAL=3
  ;;
esac

exit $RETVAL
```

6.2.7. Convert the image file format

ECS can only import image files in the RAW, VHD, or qcow2 formats. If you want to import image files in other formats, you must first convert their formats. This topic describes how to use the qemu-img tool to convert other image file formats to VHD or RAW. Using qemu-img, you can convert qcow2, VMDK, VDI, VHD (vpc), VHDX, qcow1, or QED to VHD, or implement conversion between RAW and VHD.

Windows

To install qemu-img and convert the image file format, perform the following steps:

1. Download and install qemu-img. This example uses installation path *C:\Program Files\qemu*. Visit qemu-img to download the qemu-img tool.
2. Create an environment variable for qemu-img:
   i. Choose **Start** > **Computer**, right-click Computer, and choose **Properties** from the shortcut menu.
   ii. In the left-side navigation pane, click **Advanced System Settings**.
   iii. In the **System Properties** dialog box that appears, click the **Advanced** tab and then click **Environment Variables**.
   iv. In the **Environment Variables** dialog box that appears, find the **Path** variable from the **System Variables** section and then click **Edit**. If the **Path** variable does not exist, click **New**.
   v. Add a system variable value.
      - In the **Edit System Variable** dialog box that appears, add *C:\Program Files\qemu* to the **Variable Value** field. Use semicolons (;) to separate different variable values.
      - In the **New System Variable** dialog box that appears, enter *Path* in the **Variable Name** field and enter *C:\Program Files\qemu* in the **Variable Value** field.
3. Check whether the environment variable is properly configured: Open **Command Prompt** in Windows and run the `qemu-img --help` command. If the output is displayed correctly, the environment variable was properly configured.
4. In the **Command Prompt** window, run the **cd [Directory of the source image file]** command to switch to a new file directory, for example, `cd D:\ConvertImage` .

5. Run the `qemu-img convert -f qcow2 -O raw centos.qcow2 centos.raw` command to convert the image file format.
   - The -f parameter is followed by the source image format.
   - The -O parameter (uppercase is required) is followed by the destination image format, source file name, and destination file name.

When the conversion is complete, the destination file will appear in the directory where the source image file is located.

Linux

To install qemu-img and convert the image file format, perform the following steps:

1. Install the qemu-img tool.
   - For Ubuntu, run the `apt-get install qemu-utils` command.

     If the error `Unable to locate package qemu-utils` is returned during the installation on Ubuntu, run the following commands to install the qemu-img tool:

     ```
     apt-get update #Update the package list.
     apt-get install qemu-utils #Install the qemu-img tool.
     ```

   - For CentOS, run the `yum install qemu-img` command.

     Run `pip install -r requirements.txt` to install all of the dependent libraries based on the libraries contained in the requirements.txt file of cloud-init.
2. Run the `qemu-img convert -f qcow2 -O raw centos.qcow2 centos.raw` command to convert the image file format.
   - The -f parameter is followed by the source image format.
   - The -O parameter (uppercase is required) is followed by the destination image format, source file name, and destination file name.

When the conversion is complete, the destination file will appear in the directory where the source image file is located.

What's next

Import custom images

6.2.8. Import custom images

When you deploy your services in the cloud, you can manually import image files of your servers. You can also use ECS images that are automatically generated by Alibaba Cloud for your servers. This topic describes the application scenarios and operation procedures of the two methods.

Prerequisites

Before you manually import custom images, make sure that the following requirements have been met:

- You understand the limits and requirements related to images as specified in Instructions for importing images, Customize Linux images, and Convert the image file format.

- OSS is activated. For more information, see Activate OSS.
- If you are using a RAM user, use your Alibaba Cloud account to grant permissions to the RAM user by attaching the `AliyunECSImageImportDefaultRole` policy to the user.

Context

The following table lists the scenarios in which you can import custom images.

Feature	Scenario	Procedure
Auto-import	Migrate one or more servers such as IDC servers, virtual machines, and cloud servers on other cloud platforms to Alibaba Cloud.	Auto-import
Manual import	The operating system that you require is not available in Alibaba Cloud. Possible cases are as follows: • The specified operating system type does not exist in Alibaba Cloud. • The specified operating system version has been discontinued in Alibaba Cloud. • The specified operating system is a custom operating system. The manual import feature allows you to select a license type to activate the source operating system. This can reduce your costs when you use images on the cloud. For more information about license types, see Parameters for image import.	Manual import

Auto-import

Follow these steps to use Server Migration Center (SMC) to generate ECS images for your server:

1. Log on to the ECS console.
2. In the left-side navigation pane, choose **Instances & Images > Images**.
3. In the top navigation bar, select a region.
4. In the upper-right corner of the **Images** page, choose > **Auto Import**.

   The **Server Migration Center console** is displayed.
5. Complete the operations as instructed. For more information, see Migration process.
   After the migration is complete, SMC will generate a custom image for your server. The image name starts with `IMAGE_FROM_SMC` .

Manual import

Follow these steps to manually import a local image to Alibaba Cloud ECS:

1. Use a third-party OSS client or call an API operation to upload the custom image that you have prepared. For information about how to upload an image file larger than 5 GiB, see Multipart upload and resumable upload.
2. Log on to the ECS console.

3. In the left-side navigation pane, choose **Instances & Images > Images**.
4. In the top navigation bar, select a region.
5. Authorize ECS to access your OSS resources.
   i. On the **Images** page, choose > **Manually Import**.
   ii. In the **Import Image** dialog box that appears, click **Confirm Address** in Step 3 shown in the following figure.
   iii. On the **Cloud Resource Access Authorization** page that appears, select `AliyunECSImageImportDefaultRole` and `AliyunECSExportDefaultRole`. Click **Confirm Authorization Policy**.
6. Import the custom image.
   i. On the **Images** page, choose > **Manually Import** again.
   ii. In the **Import Image** dialog box that appears, configure the parameters listed in the following table.

Parameter	Required	Description
Region of Image	Yes	This field is automatically set to the current region. To change the region, close the Import Image dialog box and select a new region in the top navigation bar. You can then choose Import Image > Manually Import to open the **Import Image** dialog box again to configure other parameters.
OSS Object Address	Yes	Copy the URL of the image object from the OSS console. For more information about how to obtain an object URL, see Download objects.
Image Name	Yes	Enter a name for the custom image. The name must be 2 to 128 characters in length and must start with a letter. It can contain letters, digits, periods (.), underscores (_), colons (:), and hyphens (-).
Operating System	Yes	Select the operating system of your image. Valid values: **Windows** | **Linux**. If you want to import a non-standard platform image, select **Linux**.
System Disk Size (GiB)	No	Specify the system disk size. Valid values: 40 GiB to 500 GiB.
System Architecture	Yes	Select **x86_64** for 64-bit operating systems and **i386** for 32-bit operating systems.

Parameter	Required	Description
Platform	Yes	The options depend on your selected **Operating System**. Select a system platform to import the image. ■ Windows: Windows Server 2003, Windows Server 2008, and Windows Server 2012. ■ Linux: CentOS, SUSE, Ubuntu, Debian, FreeBSD, CoreOS, Aliyun, Customized Linux, and Others Linux. (Submit a ticket to confirm whether the selected edition is supported.) ■ If your image operating system is a custom edition based on the Linux kernel, Submit a ticket.
Image Format	No	The RAW, qcow2, and VHD formats are supported. We recommend that you use the qcow2 and VHD formats. **Note** The ISO format is not supported and must be converted to the RAW, VHD, or qcow2 format. You can also use Packer to create and import a local image. For more information, see Create and import on-premises images by using Packer and Configure DevOps parameters by using Packer.

License Type	No	Select a license type to activate the source operating system after the image has been imported. Valid values:
		■ **BYOL**: the license provided by the source operating system. When this option is selected, make sure that your license key can be used by Alibaba Cloud.
		■ **Aliyun**: the Alibaba Cloud software license. When this option is selected, the Alibaba Cloud license is applied to your selected **Platform**.
		■ **Auto**: the default value. When this option is selected, Alibaba Cloud will automatically detect the source operating system and allocate a license. In this mode, the system automatically checks whether an Alibaba Cloud software license exists in your selected **Platform** and then performs the following actions:
		  ■ If a license exists, the system allocates the license to the imported image.
		  ■ If no license exists, the system switches the license type to **BYOL**.

Image Description	No	Enter a description for the custom image.

Parameter	Required	Description
Add Data Disk Image	No	Select this option if you want to import an image that contains data of data disks. Supported data disk capacity ranges from 5 GiB to 2,000 GiB.

iii. Click **OK**. The system will create a task to import the custom image.

7. (Optional)You can view the task progress in the image list of the destination region. Before the task is complete, you can find the imported custom image on the Tasks page in the ECS console and cancel the import task if needed. For more information, see Tasks.

   The amount of time it takes to import a custom image depends on the size of the image and the number of ongoing import tasks in the queue.

   When you import an custom image, a snapshot is automatically generated. You can view the snapshot information on the **Snapshots** page in the ECS console. Before the image import task is complete, the status of the snapshot is displayed as **Failed**. After the image import task is complete, the status of both the snapshot and image is updated to **Available**. The snapshot capacity is the size of the imported image file, regardless of the system disk size that you set when you import the image. The snapshot service is a paid service. For more information, see Snapshot billing.

What's next

Create an instance by using a custom image

Related information

References

- ImportImage
- Create and import an on-premises image by using Packer
- Change the operating system
- Image FAQ
- What is SMC?

6.3. Copy custom images

This topic describes how to copy a custom image under your Alibaba Cloud account to other regions. This action enables you to create identical ECS instances across regions, and implement data backups of target instances.

image environment deployment copy ECS

Context

The following table lists various scenarios for copying custom images.

Business requirement	Procedure	Reference
Copy images across regions under the same account	1. Create a custom image from an instance 2. Copy images to a different region.	1. CreateImage 2. CopyImage
Copy images across regions under different accounts	1. Create a custom image from an instance 2. Copy images to a different region. 3. Share images.	1. CreateImage 2. CopyImage 3. ModifyImageSharePermission
Share images in the same region under different accounts	You can share images without the need to copy images. For more information, see Share images.	ModifyImageSharePermission
Change the encryption status of a custom image, encrypt a system disk, or encrypt operation system data	Select Encrypt when you copy a custom image. The encryption feature is in public review. public preview	CopyImage

Before you copy a custom image, note the following points:

- The following fees may be incurred:
  - The copied snapshot will consume snapshot capacity. For more information, see Billing overview.

    > **Note** When an image is copied, a corresponding snapshot is generated in the destination region. The custom image is generated in the destination region based on this snapshot.

  - Fees for traffic between the two regions. Currently, no fees are charged for this traffic. For the latest billing details, see the official Alibaba Cloud website for announcements.
- The time it takes to complete the task depends on the image size, network transmission speed, and the number of concurrent tasks in the queue.
- The role authorization information, service authorization information, and instance user data of the source image are not copied to the target image.

Procedure

1. Log on to the ECS console.
2. In the left-side navigation pane, choose **Instances & Images** > **Images**.
3. In the top navigation bar, select a region.
4. On the **Images** page, click the **Custom Images** tab.
5. Select the custom image that you want to copy and click **Copy Image** in the **Actions** column.

> Note If the size of your custom image is greater than 500 GiB, you are directed to open a ticket to complete the operation when you click **Copy Image**.

6. In the **Copy Image**dialog box, specify the following parameters.
   i. Confirm the custom image ID.
   ii. In the **Destination Region** drop-down list, select a region. The selected region must be different from the current region.
   iii. Enter the **Custom Image Name** to be displayed in the destination region.
   iv. Enter the **Custom Image Description** to be displayed in the destination region.
   v. (Optional)Select **Encrypt** and then select a key from the drop-down list.
      - **Default CMK**: The default key generated by Key Management Service (KMS).
      - Other types of keys: These types of keys include all user-imported keys. If this is the first time that you select Encrypt, click **Go to Authorize** and select AliyunECSEncryptDefaultRole to allow ECS to access your KMS resources.

      > Note The encryption feature is in public preview in certain regions.

   vi. Click **OK**.
7. Query the results and manage the tasks.
   i. In the upper-left corner of the top navigation bar, switch to the destination region and view the copy progress of the custom image.
   When the progress reaches 100%, the image enters the **Available** state, indicating that the task is complete. An image is created in the destination region and has a unique image ID.
   ii. (Optional)If the **Progress** has not reached 100% and the **Status** is **Creating**, you can cancel the copy task by clicking **Cancel Copy**.

What's next

You can use the copied image to create an instance or change the system disk:

- Create an ECS instance
- Replace the system disk (non-public images)

Related information

- CopyImage
- CancelCopyImage

6.4. Share or unshare custom images

This topic describes how to share or unshare custom images. After you create a custom image, you can share it with other Alibaba Cloud accounts. The Alibaba Cloud accounts can create ECS instances from the shared image. You can also unshare custom images from Alibaba Cloud accounts to which they were shared.

share images unshare images share images across regions

Prerequisites

Before you share an image, ensure that all sensitive data and files have been removed from the image.

Context

Images shared to an account are not counted against the image quota assigned to the account. Alibaba Cloud does not charge an account for images shared to it.

Only users who create an ECS instance from the shared custom image are charged. For more information about the billing of shared images, see Images.

Users can only use the shared image and cannot delete it directly. If you want to delete the shared image, you must first unshare and then delete it. For more information, see Delete a custom image.

Before you share a custom image with an Alibaba Cloud account, note the following limitations:

- You can share only the custom images created under your account. You cannot share custom images that were created and shared by other accounts.
- Each custom image can be shared with up to 50 accounts.
- You can share images between the accounts on the China (aliyun.com), International (alibabacloud.com), and Japan (jp.alibabacloud.com) sites. However, the custom images that were created from Alibaba Cloud Marketplace images cannot be shared.
- Custom images cannot be shared across regions. If you want to share a custom image across regions, you must copy the image to the target region first. For more information, see Copy custom images.
- ECS cannot guarantee the integrity and security of shared images. Before you use the shared images, ensure that the images are from trusted users or accounts. You must assume all risks.

Share custom images

You can perform the following steps to share your custom image with an Alibaba Cloud account.

1. Log on to the ECS console.
2. In the left-side navigation pane, choose **Instances & Images** > **Images**.
3. In the top navigation bar, select a region.
4. On the **Custom Images** tab, select the custom image that you want to share. Choose **More** > **Share Image** in the **Actions** column.
5. In the **Share Image** dialog box that appears, select **Alibaba Cloud Account ID** from the **Account Type** drop-down list, enter the account ID with which you want to share images in the **Account** field, and click **Share Image**.

   How to obtain the account ID: Move the pointer over the profile picture in the upper-right corner of the Alibaba Cloud console. Select **Security Settings** from the drop-down list. The account ID is displayed on the **Security Settings** page.

   After you share a custom image with an account, the account can view the shared image from the ECS console by choosing **Instances & Images** > **Images** > **Shared Images** in the same region. The account that receives the shared image can perform the following operations:

   - Create one or more ECS instances from the shared image.

When you create an ECS instance, you can select Shared Image in the Image section. For more information, see Create an instance by using the provided wizard.

- Replace the system disk of an ECS instance with the shared image.

  For more information, see Replace the system disk (non-public images).

Unshare custom images

You can perform the following steps to unshare your custom image from an Alibaba Cloud account.

> **Notice** After you unshare the custom images:
>
> - The account that received the shared image cannot query the image from the ECS console or by calling the API operation.
> - The account that received the shared image cannot create ECS instances or replace the system disk by using the image.
> - The system disks of ECS instances that were created from the shared image cannot be reinitialized.

1. Log on to the ECS console.
2. In the left-side navigation pane, choose **Instances & Images > Images**.
3. In the top navigation bar, select a region.
4. On the **Custom Images** tab, select the custom image that you want to unshare. Choose **More > Share Image** in the **Actions** column.
5. In the **Share Image** dialog box that appears, select the account ID and click **Unshare**.

Related information

- ModifyImageSharePermission
- DescribeImageSharePermission

6.5. Export a custom image

You can export custom images that you created to OSS buckets, and then download the images to local computers. This topic describes the considerations for exporting custom images and how to export custom images.

Prerequisites

- An OSS bucket is available within the same region as the custom image to be exported.

  If you have not created any OSS buckets, create one. For more information, see Create buckets.

  > **Note** Exporting a custom image will incur OSS storage fees and traffic fees. For more information, see Overview.

- The custom image to be exported meets the following requirements:
  - It was not created based on an Alibaba Cloud Marketplace image.
  - It does not contain a Windows Server operating system.

- It does not contain snapshots of more than four data disks. The size of each data disk does not exceed 500 GiB.

Context

Before you export a custom image, note the following points:

- The time it takes to export a custom image depends on the size of the image and the number of ongoing export tasks in the queue.
- If an exported custom image contains data disk snapshots, multiple objects appear in your OSS bucket.

  Objects whose names contain *system* are system disk snapshots. Objects whose names contain *data* are data disk snapshots. The identifier of a data disk snapshot is the mount point of the source data disk, such as xvdb and xvdc.
- To use the exported image to create identical Linux instances, make sure that the storage location and storage space division of files recorded in */etc/fstab* are consistent with the exported data disk snapshot information.
- If the cloud disk does not contain any data when the custom image is created, the decompressed image file will not contain any data either.

Procedure

1. Log on to the ECS console.
2. In the left-side navigation pane, choose **Instances & Images > Images**.
3. In the top navigation bar, select a region.
4. Authorize ECS to access OSS.
   i. In the **Actions** column corresponding to a custom image, choose **More > Export Image**.
   ii. In the **Export Image** dialog box that appears, click **Verify**.

   
   iii. In the **Cloud Resource Access Authorization** dialog box, click **Confirm Authorization Policy** to allow ECS to access your OSS resources.
5. In the left-side navigation pane, choose **Instances & Images > Images**.
6. On the **Custom Images** tab, find the target image. In the **Actions** column corresponding to the image, choose **More > Export Image**.
7. In the **Export Image** dialog box, set the following parameters:
   - Image Format: Select a format in which to export the custom image. Valid values: RAW, VHD, QCOW2, VDI, and VMDK.

     > **Note** This feature is available in some regions and will be available in more regions soon.
   - OSS Bucket Address: Select an OSS bucket that belongs to the same region as the custom image.
   - OSS Object Prefix: Set the prefix of the object name for the custom image. For example, if you set OSS Object Prefix to Demo, the exported image is named *Demo-[automatically generated object name]* in the OSS bucket.

8. Click **OK** to export the custom image.

   You can cancel an image export task at any time before the task is complete. Go to the **Tasks** page in the ECS console, find the corresponding task in the specified region, and cancel the task.

What's next

Download the custom image. For more information, see Download objects.

> **Note** If you select the RAW image format, the default file name extension of the exported custom image is *.raw.tar.gz*, and the file name extension of the decompressed image is *.raw*. If your local computer runs a Mac OS X system, we recommend that you use GNU Tar to decompress the image.

Related information

- ExportImage
- CancelTask

6.6. Modify custom images

This topic describes how to modify the name and description of a custom image.

Prerequisites

A custom image is created or a custom image creation request is submitted.

Procedure

1. Log on to the ECS console.
2. In the left-side navigation pane, choose **Instances & Images** > **Images**.
3. In the top navigation bar, select a region.
4. Find the custom image to be modified.
5. Click the icon. In the **Image Name** dialog box that appears, enter the new image name and click **OK**.

   
6. Click **Modify Description** in the **Actions** column corresponding to the target image.
7. In the **Modify Description** dialog box that appears, enter the new image description and click **OK**.

Related information

- ModifyImageAttribute

6.7. Delete a custom image

You can delete custom images that are no longer needed. If you delete a custom image, the instances created from the image will not be affected.

Context

- After you delete a custom image, you will no longer be able to create instances from the image.
- After you delete a custom image:
  - The ECS instances that were created from the image can still be used and will continue to incur fees.
  - The system disks of ECS instances that were created from the image cannot be re-initialized.
- Before you delete a shared image, you must unshare the image. After you delete a shared image:
  - Accounts to which the image was shared will no longer be able to query the image from the ECS console or by calling an API operation.
  - Accounts to which the image was shared will no longer be able to create ECS instances or replace the system disk by using the image.
  - The system disks of ECS instances that were created from the shared image cannot be re-initialized.
- If you delete the source image, the copied image will not be affected. Similarly, if you delete the copied image, the source image will not be affected.

Procedure

1. Log on to the ECS console.
2. In the left-side navigation pane, choose **Instances & Images > Images**.
3. In the top navigation bar, select a region.
4. Select one or more custom images to be deleted. Click **Delete Image**.

   
5. In the dialog box that appears, select **Proceed to Forcibly Delete**.
6. Click **OK**.

Related information

- DeleteImage

7.Alibaba Cloud Marketplace images

You can purchase Alibaba Cloud Marketplace images to create ECS instances that are equipped with pre-installed runtime environments or software applications. These images can be used for scenarios such as website building, application development, and visualized management. The created ECS instances can be used out-of-the-box, which is time-saving and convenient.

Alibaba Cloud Marketplace is a network platform established by Alibaba Cloud. On the network platform, independent software vendors (ISVs) provide their images and relevant services to users. Alibaba Cloud Marketplace images integrate specific software environments and features such as the PHP runtime environment and the control panel into the operating system. You can select images based on these environments and features when you create instances.

If you create an instance from an Alibaba Cloud Marketplace image, your license may become invalid. If you encounter this problem, contact the image vendor for technical support.

Create an instance from an Alibaba Cloud Marketplace image

You can use one of the following methods to create an instance from Alibaba Cloud Marketplace image. For more information, see Create an ECS instance.

- Method 1: Select an Alibaba Cloud Marketplace image when you create an instance.
- Method 2: Go to Alibaba Cloud Marketplace to purchase an image and then create an instance.

> **Note** If you create an instance from an Alibaba Cloud Marketplace image, your license may become invalid. If you encounter this problem, contact the image vendor for technical support.

Change the operating system of an instance by using an Alibaba Cloud Marketplace image

If you have purchased an ECS instance and you want to replace the image of the instance with an Alibaba Cloud Marketplace image, you can replace the system disk.

To replace the system disk, On the **Replace Operating System** page, select **Marketplace Image** for **Image** and then click Select from Image Market (Including Operating System). In the **Marketplace Image** dialog box, select the desired image. For more information, see Replace the system disk (non-public images).

8.Change the operating system

You can change the operating system of an instance such as from Linux to Windows or from Ubuntu to CentOS.

change the operating system of an ECS instance change the operating system of an ECS instance from Linux to Windows change the operating system of an ECS instance from Ubuntu to CentOS custom image non-public image public image system disk

You can change the operating system of an instance by changing its system disk.

- Change the image of the system disk to a non-public image. For more information, see Replace the system disk (non-public images).
- Change the image of the system disk to a public image. For more information, see Replace the system disk (public images).

> **Note** In regions outside mainland China, you can only change the operating system of an ECS instance between Linux editions or between Windows editions. You cannot change the instance type between Linux and Windows.

9.End of support for operating systems

Due to reasons such as product lifecycle, third-party support, and evolution of open-source projects, Alibaba Cloud may stop providing technical support for some services after a period of time since the release of the services. Understanding the technical support plans of services or software can help you update the services or software to general availability (GA) versions in a timely manner. When you use ECS, you need to pay attention to the lifecycle plans of image operating systems. These plans are published in the official website of the operating systems.

> **Note** When an operating system version comes to the end-of-life (EOL), Alibaba Cloud will stop providing support for the ECS instances that use the operating system version.

EOL plan of Alibaba Cloud Linux 2

Version	End-of-support date
Alibaba Cloud Linux 2	March 31, 2024

EOL plans of third-party operating systems

The following tables describe the EOL plans of some third-party operating system versions:

- CentOS

Version	End-of-update date	End-of-maintenance date
CentOS 8	May 2024	May 31, 2029
CentOS 7	Q4 2020	June 30, 2024
CentOS 6	May 10, 2017	November 30, 2020
CentOS 5	April 12, 2007	March 31, 2017

- Debian

Version	Code	Release date	End-of-support date	EOL LTS	EOL ELTS
Debian 12	Bookworm	Unknown	To be decided	To be decided	To be decided
Debian 11	Bullseye	Unknown	To be decided	To be decided	To be decided
Debian 10	Buster	July 6, 2019	2022	To be decided	To be decided

Version	Code	Release date	End-of-support date	EOL LTS	EOL ELTS
Debian 9	Stretch	June 17, 2017	2020	2022	To be decided
Debian 8	Jessie	April 25, 2015	June 17, 2018	June 30, 2020	To be decided
Debian 7	Wheezy	May 4, 2013	April 25, 2016	May 31, 2018	December 31, 2019
Debian 6.0	Squeeze	February 6, 2011	May 31, 2014	February 29, 2016	To be decided
Debian 5.0	Lenny	February 14, 2009	February 6, 2012	To be decided	To be decided

- Ubuntu

Version	End-of-support date
Ubuntu 18.04 LTS	April 2028
Ubuntu 16.04 LTS	April 2024
Ubuntu 14.04 LTS	April 2022

- Windows Server

Version	End-of-update date	End-of-maintenance date
Windows Server 2019 Datacenter	January 9, 2024	January 9, 2029
Windows Server 2016 Datacenter	January 11, 2022	January 12, 2027
Windows Server 2012 Datacenter	October 9, 2018	October 10, 2023
Windows Server 2012 R2 Datacenter	October 19, 2018	October 10, 2023
Windows Server 2008	Stopped	Stopped
Windows Server 2003	Stopped	Stopped

For information about the detailed EOL plans for third-party operating system versions, visit corresponding official websites.

- CentOS
- CoreOS

- Debian
- FreeBSD
- Microsoft Windows Server
- OpenSUSE
- Red Hat
- SUSE
- Ubuntu

10.Image FAQ

This topic provides answers to commonly asked questions about ECS images.

- Common FAQ
  - Can I replace the selected image of an ECS instance?
  - Do the system disks of ECS instances support Key Management Service (KMS) encryption? How do I use KMS encryption through Terraform or Packer?
  - What are the differences between snapshots and images? How are snapshots and images related?
  - Which instance families do Red Hat Enterprise Linux (RHEL) images support?
- FAQ about custom images
  - Can I use a snapshot of a data disk to create a custom image?
  - How do I view data disk usage?
  - How do I unmount file systems and delete disk table data?
  - How do I confirm that a data disk has been unmounted and that a new custom image can be created?
  - Does a custom image still exist after the instance from which the image was created is released?
  - When an instance expires or its data is deleted, are custom images that were created from the instance affected? Are instances created from the custom images affected?
  - Can I replace the operating system of an instance created from a custom image? Can the custom image still be used after the operating system is replaced?
  - Can I select a custom image with a different operating system when I replace the system disk of an instance?
  - Can I use a custom image to overwrite the system disk data of an ECS instance?
  - Can I upgrade the CPU, memory, bandwidth, and hard disks of an ECS instance that was created from a custom image?
  - Can I use a custom image across regions?
  - Can a custom image created from a subscription instance be used to create a pay-as-you-go instance?
  - I created an ECS instance from a custom image and specified a system disk capacity greater than that in the image. However, the system disk capacity of the new ECS instance is the same as that in the image. What can I do?
  - Why do I need to comment out mounted items when I create a custom image or an ECS instance?
  - How do I configure and use a private Docker image registry?
  - How do I clone an ECS instance?
  - Some custom images cannot be used to create I/O optimized instances. What can I do?
  - Where do I view the progress of an image being imported? How long does it take to import an image?
  - Where do I view the progress of an image being created? How long does it take to create an image?

- FAQ about copying images
  - When do I need to copy a custom image?
  - Which images can be copied?
  - Which regions support copying custom images?
  - How long does it take to copy a custom image?
  - How am I charged when I copy a custom image?
  - What limits apply to the original and new images during the copy process?
  - How do I copy images in my Alibaba Cloud account to other regions in other Alibaba Cloud accounts?
  - Do size limits apply to copying an image?
  - Can I copy a custom image created from an Alibaba Cloud Marketplace image across regions?
  - How do I migrate data from regions outside mainland China to regions inside mainland China?
- FAQ about sharing images
  - How many images can be shared to me?
  - To how many users can an image be shared?
  - I have accounts on different Alibaba Cloud sites. Can I share images between these accounts?
  - Do shared images consume my image quota?
  - Do geographical limits apply to creating instances from shared images?
  - What are the risks of creating an instance from a shared image?
  - What are the risks if I share a custom image to other accounts?
  - After an account shares an image to me, can I share this image to another account?
  - After I share an image, can I still use this image to create an instance?
  - Can an image created from Instance A in one region be used by Instance B in a different region?
- FAQ about importing images
  - Is Bring Your Own License (BYOL) supported when I import custom images?
  - What kinds of licenses can be used when I import custom images?
  - How are images imported with BYOL licenses charged?
  - How are BYOL licenses authenticated and subscribed through Alibaba Cloud when their subscription expires?
- FAQ about exporting images
  - I want to export an image to my local computer for testing. What can I do?
- FAQ about deleting images
  - Can I delete a custom image after it is used to create an ECS instance?
  - Can I delete a custom image from my account after the image is shared to another account?
  - If I unshare Custom Image M to Account A, what will happen?
  - When I attempt to delete an image, I am prompted with a message similar to "The specified image cannot be deleted because it is associated with instances." Why?

- FAQ about replacing images or operating systems
  - When I replace a system disk, can I select an image that contains data disk snapshots?
  - I want to replace the operating system of my ECS instance by using an existing image. What can I do?
  - Can an image created from an instance in Account A be used to replace a system disk in Account B?
- FAQ about image pricing
  - I am creating an ECS instance. Why is the total instance cost displayed when I select a custom image higher than that displayed when I select a public image?
- FAQ about commercial availability of images
  - What features do Alibaba Cloud Marketplace images provide?
  - What are the benefits of Alibaba Cloud Marketplace images?
  - What server environments and scenarios do Alibaba Cloud Marketplace images support?
  - Are Alibaba Cloud Marketplace images safe?
  - What do I do if I encounter a problem when I am installing or using an Alibaba Cloud Marketplace image?
  - How do I purchase an Alibaba Cloud Marketplace image?
  - How long can I use a purchased image?
  - Are Alibaba Cloud Marketplace images refundable?
  - Are any free Alibaba Cloud Marketplace images available after Alibaba Cloud Marketplace images are commercially available?
  - I bought an Alibaba Cloud Marketplace image in the China (Hangzhou) region. Can I use it to create an ECS instance or replace a system disk in the China (Beijing) region?
  - I have an instance created from an Alibaba Cloud Marketplace image. Do I need to make further payments when I renew the instance or upgrade its configurations?
  - I have an ECS instance created from an Alibaba Cloud Marketplace image. After the instance is released, can I continue to use that image free of charge when I purchase a new ECS instance?
  - I created an ECS instance from an Alibaba Cloud Marketplace image and then created a custom image from the instance. Do I need to pay for the custom image when I use it to create an ECS instance?
  - If I copy an Alibaba Cloud Marketplace image that I bought to another region to create an ECS instance, do I need to pay for the image?
  - I created an ECS instance from an Alibaba Cloud Marketplace image and then created a custom image from that instance. If I share the custom image to Account B, does Account B need to pay for the custom image when it uses this image to create an ECS instance?
  - Is a fee charged if I replace a system disk by using an Alibaba Cloud Marketplace image or an image derived from an Alibaba Cloud Marketplace image?
  - My ECS instance is using an Alibaba Cloud Marketplace image. Is a fee charged if I replace the system disk of the instance?
  - How do I call an ECS API operation to use an Alibaba Cloud Marketplace image or a custom or shared image that derives from an Alibaba Cloud Marketplace image to create an ECS instance or replace a system disk?

- If I do not purchase an Alibaba Cloud Marketplace image or an image that derives from an Alibaba Cloud Marketplace image, will an error be reported when I call an ECS API operation to use the image to create an ECS instance or replace a system disk?
- I have configured a scaling group with the minimum number of instances set to 10 and the maximum number of instances set to 100. What can I do with Alibaba Cloud Marketplace images to ensure that ECS instances are created to suit my computing needs?
- Can I purchase multiple Alibaba Cloud Marketplace images at a time?
- If an image (such as jxsc000010 or jxsc000019) that was in use within a scaling configuration no longer exists in Alibaba Cloud Marketplace, what can I do to ensure that ECS instances can continue to be created properly based on the scaling configuration in the corresponding scaling group?
- Can one product code support images in different regions?
- I bought 100 images with the same product code. Can I use them within any region?
- After I select I/O Optimized, I cannot select Alibaba Cloud Marketplace images when I purchase an ECS instance. What is the cause and how can I resolve this problem?

- FAQ about subscription Alibaba Cloud Marketplace images
  - What are yearly, monthly, and weekly subscription Alibaba Cloud Marketplace images?
  - On which ECS instances can I use a subscription image?
  - How do I purchase a subscription image? Can I purchase it separately?
  - How do I pay for subscription images?
  - Can I use a subscription image after it expires? How do I continue to use it?
  - After I purchase a subscription image, can I request a refund if I no longer want to use it?
  - What can I expect when a refund is made?
  - Can a subscription image be converted to a pay-as-you-go image?
  - Can I replace a subscription image with an image of another type or vice versa? How is the fee calculated?
  - Where do I view and manage the subscription images that I purchased?
  - Is a fee charged for a custom image derived from a subscription image? How will the custom image be affected if the subscription image expires?
- FAQ about ECS instances and operating system images
  - How do I install patches to compile the kernel on FreeBSD?
  - Why does the load average become high on ECS instances that run Ubuntu operating systems of specific versions after the Server Guard process is started on the instances?
  - Why am I unable to select a Windows operating system for ECS instances?
  - Does Alibaba Cloud support Windows Server 2008 and Windows Server 2008 R2?
  - The operating system of my instance is Windows Server. I am prompted with a message indicating that the operating system is not genuine. What can I do?
  - Are fees charged for the images used by ECS instances?
  - Can I install or upgrade my operating system?
  - Do operating systems have a graphical interface?
  - How do I choose an operating system?
  - Do public images come with the FTP service?

Can I replace the selected image of an ECS instance?

Yes, you can replace the image of your ECS instance by selecting Replace System Disk in the ECS console. Note that if you replace an image, data stored on the system disk may be lost. Make sure that you have backed up your data before you replace the system disk. For more information, see Change the operating system.

Do the system disks of ECS instances support Key Management Service (KMS) encryption? How do I use KMS encryption through Terraform or Packer?

- The system disks of ECS instances can be encrypted by using BYOK and CMKs hosted in KMS. For more information, see Encryption overview.
- Support for Packer-based encryption will be added soon.
- In Terraform, you can set the encrypted parameter to enable or disable KMS encryption. For more information, see alicloud_disks.

What are the differences between snapshots and images? How are snapshots and images related?

Images and snapshots differ in the following ways:

- Images can be used to create ECS instances, whereas snapshots cannot.
- A snapshot can be a data backup of either the system disk or a data disk of an ECS instance, whereas an image must contain the system disk data of an ECS instance.

- Snapshots can be used only to restore data of existing instance disks, whereas images can be used to replace the system disks of any instances or create instances.
- Snapshots cannot be used across regions. To restore instance data in other regions, you can use a custom image. For more information, see Copy custom images.
- Images and snapshots apply to different scenarios. Here are some scenarios to which snapshots and custom images are suited:

  Scenarios for snapshots

  - Back up data on a regular basis: Automatically create snapshots to back up data on a daily, weekly, or monthly basis based on automatic snapshot policies.
  - Temporarily back up data. Examples:
    - Manually create a snapshot to back up the system data before a temporary system change such as system update or application release.
    - Create a snapshot to back up data before the system disk is resized.
    - To migrate data from a disk, create a snapshot for the disk and use the snapshot to create a new disk.

  Scenarios for custom images

  - Back up systems that will not change in a short term, such as applications and systems that are released or updated.
  - Create new ECS instances. For example, you can use a custom image to create an ECS instance that has multiple applications deployed.
  - Migrate systems and data. For example, you can migrate ECS instances from the classic network to VPCs.
  - Restore systems across regions and zones.

Snapshots and images have the following relationships:

- When you create a custom image from an instance, ECS creates a snapshot for each disk of the instance. The created custom image contains the snapshots of all the disks of this instance. For more information, see Create a custom image from an instance.
- You can also create custom images from system disk snapshots. For more information, see Create a custom image from a snapshot.

Which instance families do Red Hat Enterprise Linux (RHEL) images support?

RHEL images support the following instance families. For more information, see Instance families.

- ecs.r6 (supports only RHEL 7.7 and later)
- ecs.c6 (supports only RHEL 7.7 and later)
- ecs.g6 (supports only RHEL 7.7 and later)
- ecs.r5
- ecs.c5
- ecs.g5
- ecs.re4
- ecs.t5
- ecs.hfc5

- ecs.hfg5
- ecs.i2
- ecs.sn1ne
- ecs.sn2ne
- ecs.se1ne
- ecs.sn1
- ecs.sn2
- ecs.se1

For more information, see the following topics:

- RHEL certification
- Red Hat certified instance types

Can I use a snapshot of a data disk to create a custom image?

No, you cannot use data disk snapshots to create custom images. Only system disk snapshots can be used to create custom images.

However, you can add a snapshot of a data disk when you use a snapshot of a system disk to create a custom image. For more information, see Create a custom image from a snapshot.

How do I view data disk usage?

You can run the **df** command to check data disk usage and the locations where file systems are mounted. Example: **df -lh**.

You can run the **fdisk** command to view the partition information of a data disk. Example: **fdisk -l**.

How do I unmount file systems and delete disk table data?

Assume that */dev/hda5* is mounted to the */mnt/hda5* directory. You can run one of the following commands to unmount the file system:

```
umount /dev/hda5
```

```
umount /mnt/hda5
```

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

/etc/fstab is an important configuration file in Linux systems. It contains detailed information about file systems and storage devices mounted to the system upon system startup.

If you do not want to mount a partition when you start an instance, you must delete the corresponding statement from the /etc/fstab file. For example, after the following statement is deleted from the /etc/fstab file, *xvdb1* will not be loaded upon system startup.

```
/dev/xvdb1 /leejd ext4 defaults 0 0
```

The following table lists other important configuration files in Linux systems.

Configuration file	Description	Risk of modifying the file
/etc/issue*, /etc/*-release, /etc/*_version	The system distribution configuration file	Modifications to */etc/issue** cause failures to recognize system distributions and to create the system.
/boot/grub/menu.lst, /boot/grub/grub.conf	The system boot configuration file	Modifications to */boot/grub/menu.lst* cause kernel load and system boot failures.
/etc/fstab	The configuration file for mounting partitions upon system startup	Modifications to /etc/fstab cause partition load and system boot failures.
/etc/shadow	The system password-related configuration file	Changes of /etc/shadow to read-only cause failures to modify password files and create the system.
/etc/selinux/config	The system security policy configuration file	Modifications to */etc/selinux/config* to enable SELinux cause system boot failures.

How do I confirm that a data disk has been unmounted and that a new custom image can be created?

1. Confirm that the statement used to automatically mount data disk partitions has been deleted from the */etc/fstab* file.
2. Run the **mount** command to view the mount information of all devices. Confirm that the information about corresponding data disk partitions is not displayed in the command output.

Does a custom image still exist after the instance from which the image was created is released?

Yes, the custom image still exists after the instance from which the image was created is released.

When an instance expires or its data is deleted, are custom images that were created from the instance affected? Are instances created from the custom images affected?

No, the custom images and instances created from them are not affected.

Can I replace the operating system of an instance created from a custom image? Can the custom image still be used after the operating system is replaced?

Yes, you can replace the operating system of an instance created from a custom image. The custom image can still be used after the operating system is replaced.

Can I select a custom image with a different operating system when I replace the system disk of an instance?

Yes, you can select a custom image with a different operating system when you replace the system disk of an instance. For more information, see Replace the system disk (non-public images).

> Note When a custom image is used to replace a system disk, all data on the original system disk is overwritten.

Can I use a custom image to overwrite the system disk data of an ECS instance?

Yes, you can use a custom image to overwrite the system disk data of an ECS instance. For more information, see Replace the system disk (non-public images).

> Note The custom image will overwrite all data on the system disk of the ECS instance.

Can I upgrade the CPU, memory, bandwidth, and hard disks of an ECS instance that was created from a custom image?

Yes, you can upgrade the CPU, memory, bandwidth, and hard disks of an ECS instance that was created from a custom image. For more information, see Overview of instance upgrade and downgrade.

Can I use a custom image across regions?

No, custom images cannot be used across regions. For example, a custom image created from an instance in the China (Hangzhou) region cannot be used to create an ECS instance in the China (Shanghai) region.

If you want to use a custom image across regions, you can copy the image to the destination region. For more information, see Copy custom images.

Can a custom image created from a subscription instance be used to create a pay-as-you-go instance?

Yes, a custom image created from a subscription instance can be used to create a pay-as-you-go instance. The usage of custom images has nothing to do with the billing methods of instances.

I created an ECS instance from a custom image and specified a system disk capacity greater than that in the image. However, the system disk capacity of the new ECS instance is the same as that in the image. What can I do?

The system disk capacity of an instance created from a custom image may fail to expanded due to one of the following reasons: The cloud-init service is not installed, the cloud-init service has failed, or the file systems do not support the capacity expansion.

You can manually expand the system disk capacity.

Why do I need to comment out mounted items when I create a custom image or an ECS instance?

When you create an ECS instance from a custom image, the following conditions can cause disks to fail to be mounted:

- The created ECS instance does not have data disks.
- Data disks are new disks and are not formatted or partitioned.
- The entries for the mounted data disks are not commented out in the */etc/fstab* file of the custom image.

The following example shows a data disk mount failure. In this example, a data disk of an ECS instance that was created from a custom image is not partitioned, and the entry for this data disk is not commented out in the */etc/fstab* file of the custom image.

1. A data disk of the ECS instance is not partitioned, as shown in the following figure.

   

2. In the ECS instance, the entry for the data disk is not commented out in the */etc/fstab* file, as shown in the following figure.

   

3. When the instance starts, the system attempts to mount the data disk based on the configurations in the */etc/fstab* file. However, the mount operation fails because the data disk is not partitioned, as shown in the following figure.

   

You do not need to comment out the entries for the mounted data disks in the following situation: When you create an ECS instance, you choose to add data disks and create data disks from snapshots of partitioned and formatted data disks.

If you have further questions, submit a ticket.

How do I configure and use a private Docker image registry?

Image management is at the core of Docker. To allow organizations to share images internally, Docker has created the open source docker-registry on GitHub to act as a repository of private Docker images.

Start docker-registry that supports Alibaba Cloud OSS. You can download docker-registry from GitHub and install it, and run the **pip install docker-registry-driver-alioss** command to install the OSS driver.

1. Run Docker registry.

   ```
   docker run -e OSS_BUCKET=-e STORAGE_PATH=/docker/ -e OSS_KEY=-e OSS_SECRET=-p 5000:500
   0 -d chrisjin/registry:ali_oss
   ```

2. Configure *config.yml*.

```local: &local
<<: *common
storage: alioss
storage_path: _env:STORAGE_PATH:/devregistry/
oss_bucket: _env:OSS_BUCKET[:default_value]
oss_accessid: _env:OSS_KEY[:your_access_id]
oss_accesskey: _env:OSS_SECRET[:your_access_key]```

3. Start Docker registry.

```
DOCKER_REGISTRY_CONFIG= [your_config_path] gunicorn -k gevent -b 0.0.0.0:5000 -w 1 docker_r
egistry.wi:application
```

If you have further questions, submit a ticket.

How do I clone an ECS instance?

You can clone the environment and data of an existing ECS instance in your account to create identical ECS instances within the same region.

1. Log on to the ECS console.
2. Select the ECS instance that you want to clone and create snapshots for its system disk and data disks. For more information, see Create a normal snapshot.

   > **Note** To ensure data consistency, create snapshots only when the instance is in the **Stopped** state.

3. Use the system disk snapshot to create a custom image. In the Create Custom Image dialog box, select **Add Data Disk Snapshot** and click **Add** to add one or more data disk snapshots to the image. For more information, see Create a custom image from a snapshot.
4. Create an ECS instance by following the instructions in Create an instance by using the provided wizard. During the creation process, note the following parameters:
   - Region: You must select the same region as that of the cloned instance.
   - Image: Select **Custom Image** as the image type. Then, select the custom image that you created in the previous step from the drop-down list.

     > **Note** If the selected custom image contains one or more data disk snapshots, an equal number of data disks are automatically created from these snapshots. Each disk has the same size as the snapshot from which it is created. You can extend a data disk but cannot shrink it.

Some custom images cannot be used to create I/O optimized instances. What can I do?

Some custom images cannot be used to create I/O optimized instances. If you want to use such a custom image to create an I/O optimized instance, we recommend that you submit a ticket that contains the image name.
```

Where do I view the progress of an image being imported? How long does it take to import an image?

You can view the progress of an image being imported on the Images page in the ECS console. It may take an extended period of time to import a custom image. The amount of time it takes to import an image depends on the image size and the number of concurrent import tasks in the queue.

Where do I view the progress of an image being created? How long does it take to create an image?

You can view the progress of an image being created on the Images page in the ECS console. The amount of time it takes to create an image depends on the size of the disk from which the image is created.

When do I need to copy a custom image?

Custom images can be used only within the same region and cannot be used across regions. You can copy custom images to achieve the following goals:

- Deploy applications in ECS instances to multiple regions.
- Migrate ECS instances to other regions.
- Use custom images across regions.

You can copy a custom image from one region to another and use the custom image to deploy the same application environment in the destination region.

Which images can be copied?

Only custom images can be copied. Public images, Alibaba Cloud Marketplace images, and images shared by other accounts cannot be copied.

Which regions support copying custom images?

All Alibaba Cloud regions support copying custom images.

How long does it take to copy a custom image?

When you copy a custom image across regions, the image file is transmitted from one region to another. The amount of time it takes to copy a custom image depends on the network transmission speed and the number of transmission tasks in the queue.

How am I charged when I copy a custom image?

You must perform the following operations to copy a custom image:

1. Copy the snapshot from which the custom image was created from the source region to the destination region.
2. Create a custom image from the snapshot in the destination region.

You may be charged the following fees for the preceding operations:

- Fees for traffic between the two regions. Alibaba Cloud does not charge you for cross-region traffic. For the latest billing details, see the official Alibaba Cloud website for announcements.
- The copied snapshot consumes snapshot capacity. Snapshot capacity is billed. For more information, see Snapshot billing.

What limits apply to the original and new images during the copy process?

The original image cannot be deleted during the copy process. The copy process can be canceled, but the new image cannot be used to replace a system disk or create an ECS instance.

How do I copy images in my Alibaba Cloud account to other regions in other Alibaba Cloud accounts?

You must copy your own images to the destination regions and then share the images to the intended Alibaba Cloud accounts. After the images are shared, they will be displayed in the shared image lists of those accounts.

Do size limits apply to copying an image?

No, no size limits apply to copying an image. However, if you click **Copy Image** in the ECS console to copy an image whose size exceeds 500 GiB, you will be prompted to submit a ticket.

Can I copy a custom image created from an Alibaba Cloud Marketplace image across regions?

If an Alibaba Cloud Marketplace image is available in the destination region, you can copy the custom image derived from the Alibaba Cloud Marketplace image to the destination region. Otherwise, the following error message will be displayed when you copy the custom image.

How do I migrate data from regions outside mainland China to regions inside mainland China?

You can migrate data from regions outside mainland China to regions inside mainland China by copying images. For more information, see Copy custom images.

How many images can be shared to me?

A maximum of 100 images can be shared to you.

To how many users can an image be shared?

An image can be shared to a maximum of 50 users.

I have accounts on different Alibaba Cloud sites. Can I share images between these accounts?

Yes, you can share images between the accounts. Images (except for custom images derived from Alibaba Cloud Marketplace images) can be shared between your accounts on the China site (aliyun.com), International site (alibabacloud.com), and Japan site (jp.alibabacloud.com).

Do shared images consume my image quota?

No, shared images do not consume your image quota.

Do geographical limits apply to creating instances from shared images?

Yes, instances can be created only within the same region as the shared images from which to create the instances.

What are the risks of creating an instance from a shared image?

The image owner can check how the image is shared and can delete the image. After a shared image is deleted by its owner, the system disks of ECS instances that use this image cannot be re-initialized.

Alibaba Cloud does not guarantee the integrity and security of images shared by other accounts. We recommend that you only select images shared by trusted accounts. After an ECS instance is created from a shared image, you must log on to the ECS instance to check the security and integrity of the shared image.

What are the risks if I share a custom image to other accounts?

If you share a custom image to other accounts, data and software may be leaked or stolen. Before you share a custom image to other accounts, check whether the image contains any sensitive or important data. After the image is shared to other accounts, they can use the shared image to create ECS instances, which can then be used to create more custom images. During this process, data can be spread repeatedly, creating a risk of data being disclosed beyond your original intentions.

After an account shares an image to me, can I share this image to another account?

No, only the owner of an image can share it to other accounts.

After I share an image, can I still use this image to create an instance?

Yes, after you share an image to another account, you can still use the image to create an ECS instance and then create a custom image from the instance.

Can an image created from Instance A in one region be used by Instance B in a different region?

- If Instances A and B belong to the same account, you can copy the image to the region of Instance B and apply it to Instance B. For more information, see Copy custom images.
- If instances A and B belong to different accounts, you can copy the image to the region of Instance B and share the image to the account of Instance B. For more information, see Copy custom images and Share or unshare custom images.

Is Bring Your Own License (BYOL) supported when I import custom images?

Yes, BYOL is supported when you import custom images. You can configure the license types by using the image import feature in the ECS console or by calling the ImportImage operation. For more information, see Import custom images and ImportImage.

What kinds of licenses can be used when I import custom images?

When you import custom images, you can select one of the following license types:

- Aliyun

Aliyun licenses are provided by Alibaba Cloud and are mainly the licenses for Windows Server operating systems. If cloud-init is installed on the imported images, Alibaba Cloud will use KMS to activate the operating systems and provide Windows Server Update Services (WSUS).

- BYOL

  Microsoft BYOL licenses are used in the following scenarios:

  - BYOL implemented through SA

    BYOL can be implemented for software programs such as SQL Server and SharePoint that support License Mobility when ECS instances are created.

  - Windows operating systems

    Windows client access licenses (CALs) do not support License Mobility. Therefore, existing Windows licenses cannot be used within shared hardware environments. You must deploy Windows operating systems within a dedicated physical environment, which can be an Alibaba Cloud dedicated host or an ECS bare metal instance. For more information, see the dedicated host documentation and ECS bare metal instance documentation.

    For this kind of ECS instances, Alibaba Cloud does not provide KMS, WSUS, or software technical support. You can contact Microsoft for software technical support.

  - BYOL implemented through SA is not supported and No SA

    This scenario is similar to the Windows operating system scenario. You can reuse software licenses that you have purchased and download and deploy software programs in a dedicated hardware environment.

- Auto

  Auto is the default value for License Type. When Auto is selected, a license type is automatically configured based on the operating system distribution to be imported.

  - For operating systems such as Windows Server for which Alibaba Cloud has a signed licensing agreement and provide official licenses, the license type will be Aliyun.
  - For other operating systems such as noncommercial Linux images, the license type will be BYOL. Alibaba Cloud does not provide software technical support for these operating systems.

How are images imported with BYOL licenses charged?

No fees are charged for operating system components of images that are imported with BYOL licenses. This rule is applicable to newly created, renewed, or re-initialized ECS instances as well as ECS instances that have their configurations upgraded or downgraded.

How are BYOL licenses authenticated and subscribed through Alibaba Cloud when their subscription expires?

You can change images imported with BYOL licenses to public images provided by Alibaba Cloud or Alibaba Cloud Marketplace images.

- For Windows Server operating systems, you can use the public images provided by Alibaba Cloud. For more information, see Overview.
- You can obtain SQL Server and Red Hat images in the Alibaba Cloud Marketplace. For more information, see Alibaba Cloud Marketplace images.

I want to export an image to my local computer for testing. What can I do?

By default, images are exported as .raw.tar.gz files from which you can extract .raw files. You can search for the relevant documentation for using images in the .raw format. Alibaba Cloud has no limits on how to use images in the .raw format.

Can I delete a custom image after it is used to create an ECS instance?

You can select **Proceed to Forcibly Delete** in the Delete Image dialog box to forcibly delete the image. However, after the image is deleted, the disks of the ECS instances created from the image cannot be re-initialized. For more information, see Reinitialize a cloud disk.

Can I delete a custom image from my account after the image is shared to another account?

Yes, you can delete a custom image from your account after the image is shared to another account. However, after the shared image is deleted, the system disks of all ECS instances created from the image cannot be re-initialized. We recommend that you unshare the custom image before you delete it.

If I unshare Custom Image M to Account A, what will happen?

Account A will be unable to query Image M either by using the ECS console or by calling ECS API operations, and cannot use Image M to create ECS instances or replace system disks. If Account A has created ECS instances from Image M before the image is unshared, the system disks of these instances cannot be re-initialized.

When I attempt to delete an image, I am prompted with a message similar to "The specified image cannot be deleted because it is associated with instances." Why?

You may have created the image from a snapshot. To delete this image, you must select **Proceed to Forcibly Delete**. After the image is forcibly deleted, instances created from it are still available, but their cloud disks cannot be re-initialized. For more information, see Delete a custom image.

When I replace a system disk, can I select an image that contains data disk snapshots?

No, you cannot select an image that contains data disk snapshots when you replace a system disk. If you want to use such an image to replace a system disk, we recommend that you use the image to create a pay-as-you-go instance and create a snapshot for the system disk of the new instance. You can then use the snapshot to create a custom image that contains only a system disk snapshot, and use the created custom image to replace the system disk of the target instance.

I want to replace the operating system of my ECS instance by using an existing image. What can I do?

For information about how to use an existing image to replace the operating system of an ECS instance, see Change the operating system.

> **Note** We recommend that you create snapshots to back up data before you proceed.

Can an image created from an instance in Account A be used to replace a system disk in Account B?

Yes, you can share the image to Account B and then replace the system disk. For more information, see Share or unshare custom images.

> **Notice** To use an image to replace a system disk, make sure that the image contains only a system disk snapshot.

I am creating an ECS instance. Why is the total instance cost displayed when I select a custom image higher than that displayed when I select a public image?

This situation may occur in the following circumstances:

- The custom image contains data disk snapshots. When such an image is selected, the costs of the data disks cause the total cost of the instance to be higher than that of an instance created from a public image.
- The custom image was created based on a paid public image such as Windows Server or RHEL.

What features do Alibaba Cloud Marketplace images provide?

A software environment such as the PHP, .NET, JAVA, or LAMP runtime environment and a variety of features such as control panel and website building systems are pre-installed on the operating systems in Alibaba Cloud Marketplace images. You can use Alibaba Cloud Marketplace images to deploy runtime environments or software applications to ECS instances.

What are the benefits of Alibaba Cloud Marketplace images?

You can use an Alibaba Cloud Marketplace image to create an ECS instance and deploy the pre-installed system environment or software of the image to the ECS instance. This eliminates the need to configure the environment or install software manually and enables you to create a ready-to-run runtime environment and conveniently build and manage services.

What server environments and scenarios do Alibaba Cloud Marketplace images support?

Alibaba Cloud Marketplace provides hundreds of high-quality third-party images. These images not only cover the deployment of runtime environments such as PHP, .NET, JAVA, LAMP, and Docker virtual containers, but can also meet personalized demands for website building, application development, and visual management.

Are Alibaba Cloud Marketplace images safe?

All image service providers in Alibaba Cloud Marketplace have a wealth of experience in system maintenance and environment configuration. All images are made based on the official Alibaba Cloud operating systems that are installed with Alibaba Cloud Security. All images have passed strict security reviews and are safe to use.

What do I do if I encounter a problem when I am installing or using an Alibaba Cloud Marketplace image?

You can view the service information on the buy page and contact the image service provider by TradeManager, phone, or email. They will answer your questions as soon as possible.

How do I purchase an Alibaba Cloud Marketplace image?

You can purchase an Alibaba Cloud Marketplace image either from Alibaba Cloud Marketplace or from the ECS instance buy page when you create an ECS instance.

How long can I use a purchased image?

Theoretically, a purchased image can be used indefinitely. However, an image is a piece of software and has its own lifecycle. In addition, image providers only provide services over a limited period of time, which is described in the commodity details.

Are Alibaba Cloud Marketplace images refundable?

Alibaba Cloud Marketplace images support money-back guarantee within a certain period of time based on the Alibaba Cloud Marketplace rules. However, you will be ineligible for a refund in the following situations:

- You have deployed the purchased image to an ECS instance within the money-back guarantee period.
- You have deployed the purchased image to an ECS instance before your application for a refund for this image is approved.
- You can receive refunds only for images that have not been used.

Are any free Alibaba Cloud Marketplace images available after Alibaba Cloud Marketplace images are commercially available?

Free Alibaba Cloud Marketplace images are still available. However, you must purchase them at a price of USD 0.00 before you can use them.

I bought an Alibaba Cloud Marketplace image in the China (Hangzhou) region. Can I use it to create an ECS instance or replace a system disk in the China (Beijing) region?

No, Alibaba Cloud Marketplace images are region-specific. You can use an Alibaba Cloud Marketplace image that you purchased in a region to create ECS instances or replace system disks only within that region.

I have an instance created from an Alibaba Cloud Marketplace image. Do I need to make further payments when I renew the instance or upgrade its configurations?

No, you do not need to make any further payments. You can use a purchased image to create as many instances as you like.

I have an ECS instance created from an Alibaba Cloud Marketplace image. After the instance is released, can I continue to use that image free of charge when I purchase a new ECS instance?

Yes, you can continue to use that image free of charge when you purchase a new ECS instance.

I created an ECS instance from an Alibaba Cloud Marketplace image and then created a custom image from the instance. Do I need to pay for the custom image when I use it to create an ECS instance?

Yes, you must pay the original price of the Alibaba Cloud Marketplace image.

If I copy an Alibaba Cloud Marketplace image that I bought to another region to create an ECS instance, do I need to pay for the image?

Yes, you must pay the original price of the Alibaba Cloud Marketplace image.

I created an ECS instance from an Alibaba Cloud Marketplace image and then created a custom image from that instance. If I share the custom image to Account B, does Account B need to pay for the custom image when it uses this image to create an ECS instance?

Yes, Account B must pay the original price of the Alibaba Cloud Marketplace image.

Is a fee charged if I replace a system disk by using an Alibaba Cloud Marketplace image or an image derived from an Alibaba Cloud Marketplace image?

It depends. If the current image of your ECS instance is a different version of the replacement image, no fees are charged. Otherwise, a fee is charged.

My ECS instance is using an Alibaba Cloud Marketplace image. Is a fee charged if I replace the system disk of the instance?

No, no fees are charged if you replace the system disk of the instance.

How do I call an ECS API operation to use an Alibaba Cloud Marketplace image or a custom or shared image that derives from an Alibaba Cloud Marketplace image to create an ECS instance or replace a system disk?

1. Check whether the image in use is an Alibaba Cloud Marketplace image or an image that derives from an Alibaba Cloud Marketplace image. You can call the DescribeImages operation to query the image information.

   If the product ID (`ProductCode`) of your image is not empty, your image is an Alibaba Cloud Marketplace image or a custom or shared image that derives from an Alibaba Cloud Marketplace image. For example, if the `ProductCode` of your image is `abcd000111` , you can access the image at `http://market.aliyun.com/products/123/abcd000111.html` .

2. Select the version and region of the image and then purchase the image.

An image can only be used on ECS instances that are deployed within the same region in which the image was purchased. In addition, you can purchase only one image at a time. If you need to create multiple ECS instances, you must purchase multiple images.

3. You can use the image that you purchase to create an ECS instance or replace a system disk.

If I do not purchase an Alibaba Cloud Marketplace image or an image that derives from an Alibaba Cloud Marketplace image, will an error be reported when I call an ECS API operation to use the image to create an ECS instance or replace a system disk?

Yes, an error will be reported with the `QuotaExceed.BuyImage` error code.

I have configured a scaling group with the minimum number of instances set to 10 and the maximum number of instances set to 100. What can I do with Alibaba Cloud Marketplace images to ensure that ECS instances are created to suit my computing needs?

If you want to automatically create n instances that use the same image, you must purchase the image n times from Alibaba Cloud Marketplace in advance.

Can I purchase multiple Alibaba Cloud Marketplace images at a time?

No, you cannot purchase multiple Alibaba Cloud Marketplace images at a time.

If an image (such as jxsc000010 or jxsc000019) that was in use within a scaling configuration no longer exists in Alibaba Cloud Marketplace, what can I do to ensure that ECS instances can continue to be created properly based on the scaling configuration in the corresponding scaling group?

We recommend that you select a suitable replacement image from Alibaba Cloud Marketplace to ensure that ECS instances are properly created in your scaling group.

Can one product code support images in different regions?

Yes, one product code can support images in different regions as long as the regions already support the images.

I bought 100 images with the same product code. Can I use them within any region?

Alibaba Cloud Marketplace images are region-specific. If you want to use an image within a specific region, we recommend that you purchase the image within that region.

After I select I/O Optimized, I cannot select Alibaba Cloud Marketplace images when I purchase an ECS instance. What is the cause and how can I resolve this problem?

View the details about and solution to this problem.

- Problem description: When you purchase an ECS instance on the official Alibaba Cloud

website, you cannot select any Alibaba Cloud Marketplace images.

- Cause: If you select **I/O Optimized** when you purchase an ECS instance, you cannot select Alibaba Cloud Marketplace images.

  I/O optimized ECS instances provide better network capabilities between instances and disks compared with non-I/O optimized ECS instances, maximizing the storage performance of standard SSDs. However, not all images support I/O optimized instances because the related optimization operations involve networks, storage, and internal drivers.

- Solution: When you purchase an I/O optimized instance, we recommend that you select an official standard image supported by the instance and then deploy your business environment on the instance.

If the problem persists, we recommend that you submit a ticket.

What are yearly, monthly, and weekly subscription Alibaba Cloud Marketplace images?

Yearly, monthly, or weekly subscription Alibaba Cloud Marketplace images are images that are purchased from Alibaba Cloud Marketplace and billed on a subscription basis. These images are developed and maintained by image providers, who are responsible for both pre-sales consultation and after-sales services. In this topic, these images are collectively referred to as subscription images.

On which ECS instances can I use a subscription image?

A subscription image can only be used on a subscription instance with the same subscription duration.

How do I purchase a subscription image? Can I purchase it separately?

No, you cannot purchase a subscription image separately.

You can use one of the following methods to purchase a subscription image:

- When you create an ECS instance, set Billing Method to **Subscription**, select an **Alibaba Cloud Marketplace** image, and then specify a subscription duration by setting Duration.

  > **Note** In this case, you must pay for both the instance and image. The instance is created upon successful payment for both the image and instance.

- To use a subscription image on an existing subscription ECS instance, you can use this image to replace the operating system of the instance. In this case, you must select the image subscription duration based on the instance subscription duration. For more information, see Replace the system disk (non-public images).

  > **Note** In this case, you only need to pay for the image.

How do I pay for subscription images?

Subscription images require payment upfront. The subscription duration of a subscription image must be the same as that of the subscription instance on which the image is used.

Image prices are set by the image providers.

Can I use a subscription image after it expires? How do I continue to use it?

When a subscription image expires, it cannot be used unless it is renewed in a timely manner.

You cannot renew a subscription image separately. If you want to continue using the image, you must renew the image together with the corresponding ECS instance. You can resume use of the image after it is renewed.

After I purchase a subscription image, can I request a refund if I no longer want to use it?

The image provider will determine whether to make a refund. You can consult the image provider before you purchase the image.

What can I expect when a refund is made?

If a refund is available, the image provider will make the refund based on your usage.

Can a subscription image be converted to a pay-as-you-go image?

Subscription images cannot be converted to pay-as-you-go images. This conversion function is currently under development for release in the future. Stay updated on the official Alibaba Cloud website.

Can I replace a subscription image with an image of another type or vice versa? How is the fee calculated?

Yes, you can replace images when you replace system disks of ECS instances. You can make the following replacements:

- Replace an image of another type (such as public image, custom image, or shared image) with a subscription image. After the image is replaced, the system will calculate the actual cost based on the image cost and the remaining subscription duration of the ECS instance.
- Replace a subscription image with an image of another type (such as public image, custom image, or shared image). If the image provider allows for refunds, a refund will be made based on your actual usage.
- Replace Subscription Image A with Subscription Image B. If a refund is available after the image is replaced, the refund will be made based on the refund policy. The actual cost of Image B will be calculated based on the image price and the remaining subscription duration of the ECS instance.

Where do I view and manage the subscription images that I purchased?

You can log on to the ECS console. In the left-side navigation pane, choose **Instances & Images** > **Images**. Then, click the Marketplace Images tab to view and manage the subscription images that you purchased.

Is a fee charged for a custom image derived from a subscription image? How will the custom image be affected if the subscription image expires?

When you use a custom image derived from a subscription image to create an instance or replace a system disk, you are re-ordering the subscription image on Alibaba Cloud Marketplace. The custom image will not be affected regardless of whether the original subscription image expires.

How do I install patches to compile the kernel on FreeBSD?

1. Access the */usr/src* directory to download the FreeBSD kernel source code.

```
cd /usr/src
git clone https://github.com/freebsd/freebsd.git
```

2. Download patches.

   In this example, the following patches to virtio drivers are downloaded: `0001-virtio.patch`.

```
cd /usr/src/sys/dev/virtio/
wget https://ecs-image-tools.oss-cn-hangzhou.aliyuncs.com/0001-virtio.patch
patch -p4 < 0001-virtio.patch
```

3. Copy the kernel files and compile and install the kernel.

   N in the `make -j<N>` command indicates the number of jobs that run in parallel. Set N based on your compiling environment. The ratio of the number of vCPUs to the N value must be `1:2`. For example, for a single-vCPU environment, set -j<N> to `-j2`.

```
cd /usr/src
cp ./sys/amd64/conf/GENERIC .
make -j2 buildworld KERNCONF=GENERIC
make -j2 buildkernel KERNCONF=GENERIC
make -j2 installkernel KERNCONF=GENERIC
```

4. After the kernel is compiled, delete the source code.

```
rm -rf /usr/src/*
rm -rf /usr/src/. *
```

Why does the load average become high on ECS instances that run Ubuntu operating systems of specific versions after the Server Guard process is started on the instances?

After the Server Guard (AliYunDun) process is started on ECS instances that run Ubuntu operating systems of specific versions such as Ubuntu 18.04, the load average of the instances becomes high. After the Server Guard process is terminated, the load average drops to normal levels.

For the causes of and solutions to this problem, see The system load is high after the Server Guard process is started on an ECS instance that runs an Ubuntu 18.04 operating system.

Why am I unable to select a Windows operating system for ECS instances?

When you create an ECS instance based on a Windows operating system, make sure that the instance memory is greater than or equal to 1 GiB. For ECS instances that have less than 1 GiB of memory, you can only select Linux and Windows Server 1709 images.

Does Alibaba Cloud support Windows Server 2008 and Windows Server 2008 R2?

On January 14, 2020, Microsoft stopped providing support for Windows Server 2008 and Windows Server 2008 R2 operating systems. Therefore, Alibaba Cloud no longer provides technical support for ECS instances that use the preceding operating systems. If you have ECS instances that use the preceding operating systems, upgrade them to Windows Server 2012 or later in a timely manner.

The operating system of my instance is Windows Server. I am prompted with a message indicating that the operating system is not genuine. What can I do?

Activate the Windows operating system. For more information, see How to activate the VPC-type Windows instances by using KMS servers.

Are fees charged for the images used by ECS instances?

The Windows Server and Red Hat public images are charged. The fees depend on instance types. Other public images are free of charge. For more information about the fees for other types of images, see Image types.

Can I install or upgrade my operating system?

No, you cannot install or upgrade your operating system. An ECS instance must use an image that is provided by Alibaba Cloud, which you cannot add or upgrade on your own. However, you can perform the following operations:

- Replace a system disk and select a new operating system. For more information, see Change the operating system.
- Create an ECS instance from a custom image that is imported from a local computer. For more information about how to import an image, see Instructions for importing images. For more information about how to create an ECS instance by using a custom image, see Create an instance by using a custom image.
- Patch the operating system.

Do operating systems have a graphical interface?

Windows operating systems except for Windows Server Semi-Annual Channel offer a management desktop. For more information about how to use Windows Server Semi-Annual Channel operating systems, see Manage Windows Server Semi-Annual Channel images and instances.

Linux operating systems offer a command line interface. You can install a graphical desktop.

How do I choose an operating system?

For more information about how to choose an operating system, see Select an image.

Do public images come with the FTP service?

No, public images do not come with the FTP service. You must configure the FTP service on your own. For more information, see Manually build an FTP site on a Windows instance and Manually build an FTP site on a CentOS 7 instance.

Which SUSE versions do Alibaba Cloud public images support?

Alibaba Cloud public images support SUSE versions. For the SUSE versions that Alibaba Cloud public images support, see the "Aliyun Linux images" section in Overview.

What service support is available for SUSE operating systems?

SUSE Linux Enterprise Server (SLES) operating systems that are sold on Alibaba Cloud Marketplace are synchronized with SUSE update sources on a regular basis. For instances created from Alibaba Cloud SLES public images, the support for their operating systems is covered by the Alibaba Cloud enterprise-level support service. If you have purchased the enterprise-level support service and encounter a problem when you use an SLES operating system, submit a ticket to contact Alibaba Cloud technical support personnel.

If an image was manually created from an ECS instance, can I retrieve the instance data after the instance is released upon expiration?

Yes, you can retrieve instance data in one of the following ways:

- Create a new instance from the previously created image. For more information, see Create an ECS instance by using a custom image.
- Use the previously created image to replace the system disk of the current instance. For more information, see Replace the system disk (non-public images).

> **Notice** When you replace a system disk, take note of the following items:
>
> - All data on the current system disk will be lost, and the system disk will be restored to the state of the image.
> - The image must be in the same region as the current instance.

I have an ECS instance and I want to create another ECS instance from the image of the current ECS instance. What can I do?

You can create a custom image from the current ECS instance and then use the custom image to create a new ECS instance. For more information, see Create a custom image from an instance and Create an ECS instance by using a custom image.

I have purchased an ECS instance. How do I restore my shared image to the newly purchased instance?

Make sure that you have shared the image to the account of the newly purchased instance. Use one of the following methods to restore the image to the instance:

- If the shared image and the instance are located in the same region, replace the system disk of the instance and select the shared image for the new system disk. For more information, see Replace the system disk (non-public images).
- If the shared image and the instance are not located in the same region, copy the image to

the region where the instance is located. Then replace the system disk of the instance, and select this image for the new system disk. For more information, see Copy custom images and Replace the system disk (non-public images).

> **Notice** The following risks are associated with the replacement of the system disk of an instance:
>
> - The original system disk will be released. We recommend that you create a snapshot to back up your data in advance.
> - You must stop the instance before you can replace its system disk. When the instance is stopped, the services that are running on the instance are interrupted.
> - After you replace the system disk, you must re-deploy the service environment on the new system disk. This may cause services on the instance to be interrupted for an extended period of time.
> - During the replacement, a new system disk with a different disk ID is allocated to the instance. The snapshots of the original system disk cannot be used to roll back the new system disk.

I have multiple Alibaba Cloud accounts. I want to transfer an instance from Account A to Account B or migrate the environment and applications of an instance in Account A to an instance in Account B. What can I do?

You can perform the following steps:

1. Create a custom image from the instance in Account A. For more information, see Create a custom image from an instance.
2. Share the image to Account B. For more information, see Share or unshare custom images.
3. Create an instance in Account B from the shared image. For more information, see Create an ECS instance by using a custom image.

How do I migrate data between ECS instances?

You can perform the following steps to migrate data from one ECS instance to another:

1. Create a custom image from the source ECS instance.
2. Copy or share the custom image.
   - If the source and destination instances are located within the same region and belong to the same account, go to the next step.
   - If the source and destination instances are located in different regions but belong to the same account, copy the image to the region where the destination instance is located. For more information, see Copy custom images.
   - If the source and destination instances are located within the same region but belong to different accounts, share the custom image to the account of the destination instance. For more information, see Share or unshare custom images.
   - If the source and destination instances are located in different regions and belong to different accounts, copy the image to the region where the destination instance is located, and then share the image to the account of the destination instance. For more information, see Copy custom images and Share or unshare custom images.

3. Use the shared image to create an ECS instance or replace the image of the destination instance. For more information, see Create an ECS instance by using a custom image or Change the operating system.

   > Note If you want to replace the image of the destination instance, make sure that the original image does not contain any data disk snapshots.

If the preceding steps are not applicable, see Migrate your instance within Alibaba Cloud ECS for more information about how to migrate data between ECS instances.

Can ECS instances in different VPCs communicate with each other?

Express Connect and Cloud Enterprise Network (CEN) can be used to allow VPCs to connect to each other. For more information, see Step 1: Network planning in *CEN documentation*.

How do I handle a CentOS DNS resolution timeout?

View the details about and solution to the CentOS DNS resolution timeout problem.

- Cause

  The DNS resolution mechanism of CentOS 6 and CentOS 7 has changed. A DNS resolution timeout may occur in CentOS 6 or CentOS 7 instances that were created before February 22, 2017 or created from custom images that were created before February 22, 2017.

- Solution

  You can perform the following steps to fix this problem:

  i. Download the fix_dns.sh script.
  ii. Place the downloaded script in the */tmp* directory of the CentOS system.
  iii. Run the **bash /tmp/fix_dns.sh** command to execute the script.

- Script role

  The script determines whether the */etc/resolv.conf* file contains the `options` > `single-request-reopen` configuration. For more information, see resolv.conf - resolver configuration file.

  The DNS resolution mechanism of CentOS 6 and CentOS 7 uses the same 5-tuple to send IPv4 and IPv6 DNS requests, for which the `single-request-reopen` option must be added. When two requests from the same port need to be handled after the option is added, the resolver closes the socket after the resolver sends the first request and then opens a new socket before the resolver sends the second request. The option will take effect immediately after it is added. You do not need to restart the instance.

- Script logic

  i. Determine whether the operating system of the instance is CentOS.
     - If the operating system is not CentOS (for example, the operating system is Ubuntu or Debian), the script stops running.
     - If the operating system is CentOS, the script continues to run.
  ii. Check the */etc/resolv.conf* file for the `options` configuration.

- If the `options` configuration is unavailable:

  Use the Alibaba Cloud `options` configuration (`options timeout:2 attempts:3 rotate single-request-reopen`) by default.

- If the `options` configuration is available:
  - If the `single-request-reopen` option does not exist, append this option to the `options` configuration.
  - If the `single-request-reopen` option exists, the script stops running and the DNS nameserver configuration does not change.

Why does ECS disable virtual memory and leave swap partitions unconfigured by default?

When physical memory is insufficient, the memory manager will save memory data that has been inactive for an extended period of time to a swap partition or virtual memory file. This mechanism helps increase the available memory.

However, if memory usage is already high and I/O performance is poor, the mechanism will decrease the available memory instead. Alibaba Cloud ECS cloud disks use distributed file systems for storage and provide multiple strongly consistent replicas for each piece of data. This mechanism ensures the security of user data but deteriorates the storage and I/O performance of local disks by tripling the number of I/O operations.

Because of this, virtual memory is not enabled for Windows and swap partitions are not configured for Linux by default to avoid further decreasing I/O performance when system resources are insufficient.

How do I enable the kdump service in a public image?

By default, the kdump service is disabled in public images. If you want your instance to generate a core file when the instance is down so that you can analyze the downtime cause based on the file, you can perform the following steps to enable the kdump service. The CentOS 7.2 public image is used in the following example:

1. Configure the directory in which to generate the core file.
   i. Run the **vim /etc/kdump.conf** command to open the kdump configuration file.
   ii. Run the path command to configure the directory in which to generate the core file. In this example, the directory is */var/crash*, and the following path command is used:

   ```
   path /var/crash
   ```

   iii. Save and close the */etc/kdump.conf* file.
2. Enable the kdump service.

   Use one of the following methods based on the operating system to enable the kdump service. In this example, the kdump service is enabled in CentOS 7.2 by using Method 1.

   - Method 1: Run the following commands to enable the kdump service:

     ```
     systemctl enable kdump.service
     ```

```
systemctl start kdump.service
```

- Method 2: Run the following commands to enable the kdump service:

```
chkconfig kdump on
```

```
service kdump start
```

3. Run the following command to simulate the scenario where the instance is down:

```
echo c > /proc/sysrq-trigger
```

> **Note** After the command is run, the instance is disconnected from the network. You must reconnect the instance to the network to perform the subsequent operations.

4. Analyze the core file.
   i. Run the following command to install the Crash analysis tool:

```
yum install crash
```

   ii. Download the debuginfo installation package.

   Run the **uname -r** command to view the operating system kernel version and download the debuginfo installation package that matches the kernel version.

   - *kernel-debuginfo-common-x86_64-<Kernel version>.rpm*
   - *kernel-debuginfo-<Kernel version>.rpm*

   > **Note** The download links for the debuginfo package vary with the CentOS versions. You can find the download link that corresponds to your kernel version on the official CentOS website . For more information, see CentOS debuginfo packages.

   In this example, the kernel version is `3.10.0-514.26.2.el7.x86_64`. The following download commands are used:

```
wget http://debuginfo.centos.org/7/x86_64/kernel-debuginfo-common-x86_64-3.10.0-514.26.2.el7.x86_64.rpm
```

```
wget http://debuginfo.centos.org/7/x86_64/kernel-debuginfo-3.10.0-514.26.2.el7.x86_64.rpm
```

   iii. Run the following commands to install the debuginfo package:

```
rpm -ivh kernel-debuginfo-common-x86_64-3.10.0-514.26.2.el7.x86_64.rpm
```

```
rpm -ivh kernel-debuginfo-3.10.0-514.26.2.el7.x86_64.rpm
```

iv. Run the following commands to use the Crash analysis tool to analyze the core file:

```
cd <core file directory>
```

```
crash /usr/lib/debug/lib/modules/<Kernel version>/vmlinux vmcore
```

In this example, the core file directory is */var/crash/127.0.0.1-2019-07-08-15:52:25*, and the kernel version is `3.10.0-514.26.2.el7.x86_64`. The following commands are used:

```
cd /var/crash/127.0.0.1-2019-07-08-15:52:25
```

```
crash /usr/lib/debug/lib/modules/3.10.0-514.26.2.el7.x86_64/vmlinux vmcore
```

How do I obtain the dump file for RHEL images?

Some RHEL images do not have the kdump service enabled by default. You can submit a ticket to obtain the dump file. For instances that have a memory of greater than 16 GiB, you may fail to obtain the dump file by submitting a ticket. Details on the ticket shall prevail.

How do I enable or disable the Meltdown and Spectre patches for Linux images?

For information about the security vulnerabilities and public images involved as well as how to enable or disable security vulnerability patches, see How do I enable or disable the Meltdown and Spectre patches for Linux images?.

After I use an ECS instance for an extended period of time without restarting it, the instance is disconnected from the network, the network is no longer available, or the public or private IP address of the instance cannot be pinged. What can I do?

For more information about the cause of and solution to this issue, see Troubleshoot IP address faults in CentOS 7 instances and Windows instances.

How do I upgrade RHEL 7 to RHEL 8?

For more information about how to upgrade RHEL 7 to RHEL 8, see Upgrading from RHEL 7 to RHEL 8.

11.FAQ

11.1. Manage Windows Server Semi-Annual Channel images and instances

This topic describes how to manage an ECS instance that is created from a Windows Server Semi-Annual Channel image.

Windows Server Semi-Annual Channel instance management ECS Alibaba Cloud

Context

Windows Server Semi-Annual Channel runs in Server Core mode and is entirely command-line based. Windows Server Semi-Annual Channel offers some significant advantages, such as support for remote management, lower requirements for hardware, and a reduction in the need for updates. Windows Server Semi-Annual Channel instances exclude Resource Manager, Control Panel, and Windows Explorer. The instances do not support the *.msc command-line option such as devmgmt.msc. You can manage servers by using tools such as Sconfig, Server Manager, PowerShell, and Windows Admin Center.

When you create an instance, you can view the following Windows Server Semi-Annual Channel images in the public images list:

- Windows Server Version 1809 Datacenter Edition
- Windows Server Version 1709 Datacenter Edition
- Windows Server Version 1903 Datacenter Edition
- Windows Server Version 1909 Datacenter Edition

Windows Server Semi-Annual Channel runs in Server Core mode. We recommend that you use advanced management tools such as PowerShell and Windows Admin Center. For more information, visit Manage a Server Core server in Microsoft Docs.

Manage an instance by using PowerShell

PowerShell runs on .NET Framework and uses object-oriented scripts, allowing you to manage Windows instances in the same manner as you do with SSH. For example, if the public IP address of your instance is 172.16.1XX.183, you can perform the following steps to manage your instance by using PowerShell:

1. Connect to a Windows instance. For more information, see Connect to a Windows instance from a local client.
2. Enter **PowerShell** on the command line to start PowerShell.
3. Run the following commands in PowerShell:

```
Enable-PSRemoting -Force
Set-NetFirewallRule -Name "WINRM-HTTP-In-TCP-PUBLIC" -RemoteAddress Any
```

4. Add rules to the security group to which the instance belongs to allow access over HTTP port 5985 and HTTPS port 5986. For more information about how to add rules to a security group, see Add security group rules.
5. Enter **PowerShell** on the command line of the client to start PowerShell.

6. Run the following command in PowerShell:

```
Set-Item WSMan:localhost\client\trustedhosts -value 172.16.1XX.183 -Force
```

> Note `172.16.1XX.183` indicates that only your instance is trusted. You can use `*` to indicate that all PCs are trusted.

7. Run `Enter-PSSession '172.16.1XX.183' -Credential:'administrator'` in PowerShell and enter the password of the instance as prompted.

Now you can manage your Windows instances on the client PC.

Install Windows Admin Center

Windows Admin Center is a browser-based GUI management tool. It can replace server management tools or Microsoft Management Console (MMC) when the Server Core mode is used. For example, if the public IP address of your instance is 172.16.1XX.183, you can use one of the following methods to install Windows Admin Center:

- Use commands
  i. Connect to a Windows instance. For more information, see Connect to a Windows instance from a local client.
  ii. Add rules to the security group to which the instance belongs to allow access over HTTP port 5985 and HTTPS port 5986. For more information, see Add security group rules.
  iii. Enter **PowerShell** on the command line to start PowerShell.
  iv. Run the following commands in PowerShell:

```
Enable-PSRemoting -Force
Set-NetFirewallRule -Name "WINRM-HTTP-In-TCP-PUBLIC" -RemoteAddress Any
```

  v. Run the following commands to download Windows Admin Center:

```
wget -Uri http://download.microsoft.com/download/E/8/A/E8A26016-25A4-49EE-8200-E4BCBF292C4A/HonoluluTechnicalPreview1802.msi -UseBasicParsing -OutFile c:\HonoluluTechnicalPreview1802.msi
msiexec /i c:\HonoluluTechnicalPreview1802.msi /qn /L*v log.txt SME_PORT=443 SSL_CERTIFICATE_OPTION=generate
```

  vi. Run the *cat log.txt* command to check the download progress.

  When information similar to the following content is displayed in the log file, Windows Admin Center is installed:

```
MSI (s) (14:44) [09:48:37:885]: Product: Project 'Honolulu'(Technical Preview) -- Installation completed successfully.
MSI (s) (14:44) [09:48:37:885]: Windows Installer installed this product. Product name: Project 'Honolulu' (Technical Preview). Product version: 1.1.10326.0. Product language: 1033. Manufacturer: Microsoft Corporation. Installation success or error status: 0.
```

- Use a browser
  - Prerequisites

    PowerShell is configured and can be used to manage instances. If you want to install Windows Admin Center by using a browser, you must complete the installation on the client PC. For more information, see Manage an instance by using PowerShell.
  - Procedure
    a. Download and install Windows Admin Center.
    b. Open https://localhost/ after the installation is complete.
    c. Click **Add**. In the dialog box that appears, add the IP address of the instance.

  Now you can use Windows Admin Center to manage instances by using Microsoft Edge or Chrome.

FAQ

Question 1: How do I copy files to a Windows Server Semi-Annual Channel instance?

If the files to be copied are stored on your client PC, and Windows Admin Center is installed, or PowerShell is configured to manage instances, you can copy files to the instance by using one of the following methods:

- Use a Remote Desktop (RDP) application
  i. Connect to a Windows instance. For more information, see Connect to a Windows instance from a local client.
  ii. Copy the target files on the client PC.
  iii. Enter *notepad* on the command line of the instance.
  iv. Choose **File** > **Open**. In the dialog box that appears, right-click the destination directory and choose **Paste** from the shortcut menu.
- Use PowerShell
  i. Start the target Windows instance.
  ii. Enter **PowerShell** on the command line of the client PC to start PowerShell.
  iii. Use PowerShell to manage the target instance. For more information, see Manage an instance by using PowerShell.
  iv. Run the following commands on the client PC:

```
$session = New-PSSession -ComputerName 172.16.1XX.183
Copy-Item -ToSession $session -Path C:\1.txt -Destination c:\2.txt
```

  > **Note** *C:\1.txt* is the source file directory on the client PC. *C:\2.txt* is the destination file directory on the Windows instance.

- Use Windows Admin Center
  i. Start the target Windows instance.
  ii. Configure Windows Admin Center. For more information, see Install Windows Admin Center.
  iii. Start Windows Admin Center and click the target instance. Click **File**, select the file, and

then click **Upload**.

Question 2: How do I stop or restart a Windows Server Semi-Annual Channel instance?

- Use an RDP application
  i. Connect to a Windows instance. For more information, see Connect to a Windows instance from a local client.
  ii. Enter *sconfig* on the command line, select `13` to restart the instance or `14` to stop the instance, and then press the Enter key.
- Use PowerShell
  i. Connect to a Windows instance. For more information, see Connect to a Windows instance from a local client.
  ii. Enter **PowerShell** on the command line to start PowerShell.
  iii. Run one of the following commands to restart or stop the instance:

```
shutdown -r -t 00 :: This command will restart the instance in 0 seconds.
shutdown -s -t 00 :: This command will stop the instance in 0 seconds.
Stop-Computer -Force # This PowerShell command will stop the instance instantly.
Restart-Computer -Force # This PowerShell command will restart the instance instantly.
```

- Use PowerShell
  i. Start the target Windows instance.
  ii. Enter **PowerShell** on the command line of the client PC to start PowerShell.
  iii. Use PowerShell to manage the target instance. For more information, see Manage an instance by using PowerShell.
  iv. Run the following commands to restart or stop the instance:

```
Enter-PsSession -ComputerName 172.16.1XX.183
Restart-Computer -Force # Restart the instance.
Stop-Computer -Force # Stop the instance.
```

- Use Windows Admin Center
  i. Start the target Windows instance.
  ii. Configure Windows Admin Center. For more information, see Install Windows Admin Center.
  iii. Start Windows Admin Center and select the target instance. Click **Overview** in the left-side navigation pane. On the Overview page that appears, click **Restart** or **Shutdown**.

Question 3: How do I install the IIS service?

- Use an RDP application
  i. Connect to a Windows instance. For more information, see Connect to a Windows instance from a local client.
  ii. Enter **PowerShell** on the command line to start PowerShell.
  iii. Run the following commands to install IIS:

```
Import-Module ServerManager
Add-WindowsFeature Web-Server, Web-CGI, Web-Mgmt-Console
```

- Use PowerShell
  i. Start the target Windows instance.
  ii. Enter **PowerShell** on the command line of the client PC to start PowerShell.
  iii. Use PowerShell to manage the target instance. For more information, see Manage an instance by using PowerShell.
  iv. Run the following PowerShell commands on the client PC:

```
Enter-PsSession -ComputerName 172.16.1XX.183
Import-Module ServerManager
Add-WindowsFeature Web-Server, Web-CGI, Web-Mgmt-Console
```

- Use Windows Admin Center
  i. Start the target Windows instance.
  ii. Configure Windows Admin Center. For more information, see Install Windows Admin Center.
  iii. Start Windows Admin Center and select the target instance. Click **Roles and Features** in the left-side navigation pane. On the Roles and Features page that appears, click **Web Server**. Choose the suitable features based on your needs and click **Yes**.

Question 4: How do I reopen a command line window that I accidentally closed during an RDP session?

If a command line window is accidentally closed during an RDP session, the remote application shows a black screen and operations cannot be performed. In this case, you can perform the following steps:

1. Press Ctrl+Alt+End if an MSTSC connection is used. In other cases, press Ctrl+Alt+Del.
2. Select **Task Manager** on the page that appears, and press the Enter key.
3. In Task Manager, choose **File** > **New Task**. Enter cmd and click **OK**.

Related information

References

- Windows Server Semi-Annual Channel overview
- Introducing Windows Server, version 1709
- Windows Admin Center
- About Remote Troubleshooting

11.2. Install GRUB on a Linux server

To migrate a Linux server to Alibaba Cloud by using Server Migration Center (SMC), you must upgrade the system boot program GRand Unified Bootloader (GRUB) of the server to version 2.02 or later if the following conditions are met: The server runs an early Linux distribution such as CentOS 5 or Debian 7, the GRUB version is earlier than 2.02, and the "Do Grub Failed" error message appears in the log file.

Context

This topic describes how to install GRUB on a Linux server. GRUB version 2.02 is used in the example. The procedure to install GRUB of other versions is similar. The source code package may vary with different GRUB versions. For more information, visit Index of /gnu/grub.

Procedure

1. Log on to the Linux server.
2. Run the following commands to find the paths of the grub, grub-install, and grub-mkconfig files:

   > Note If you are prompted that one or more of these paths do not exist, go to the next step.

   ```
   which grub
   ```

   ```
   which grub-install
   ```

   ```
   which grub-mkconfig
   ```

3. Run the `mv` command to rename the grub, grub-install, and grub-mkconfig files.

   > Note If you are prompted that one or more of these files do not exist, go to the next step.

   After you use SMC to migrate the server, you can restore the files by changing their names back to the original ones.

   ```
   mv /sbin/grub /sbin/grub-old
   ```

   ```
   mv /sbin/grub-install /sbin/grub-install-old
   ```

   ```
   mv /sbin/grub-mkconfig /sbin/grub-mkconfig-old
   ```

4. Install the GRUB dependencies including bison, gcc, and make.

   ```
   yum install -y bison gcc make
   ```

5. Perform the following operations to install flex:
   i. Check whether the tools folder exists. If the folder does not exist, create it.

      ```
      test -d /root/tools || mkdir -p /root/tools
      ```

   ii. Go to the tools folder and download the flex installation package.

      ```
      cd /root/tools
      wget https://github.com/westes/flex/releases/download/v2.6.4/flex-2.6.4.tar.gz
      ```

iii. Decompress the flex installation package.

```
tar xzf flex-2.6.4.tar.gz
```

iv. Go to the directory to which the flex installation package is decompressed, and create a folder named build.

```
cd flex-2.6.4
mkdir -p build
```

v. Go to the build folder, and compile and install flex.

```
cd build
../configure
```

```
make && make install
```

vi. Create a symbolic link.

```
ln -s /usr/local/bin/flex /usr/bin/flex
```

6. Perform the following operations to install GRUB:Upgrade GRUB to version 2.02 or later if you are using an early distribution of the Linux operating systems such as CentOS 5, Red Hat Enterprise Linux 5, Debian 7, Amazon Linux, or Oracle Linux.

i. Check whether the tools folder exists. If the folder does not exist, create it.

```
test -d /root/tools || mkdir -p /root/tools
```

ii. Go to the tools folder and download the GRUB installation package.

```
cd /root/tools
wget https://alpha.gnu.org/gnu/grub/grub-2.02~rc1.tar.gz
```

iii. Decompress the GRUB installation package.

```
tar xzf grub-2.02~rc1.tar.gz
```

iv. Go to the directory to which the GRUB installation package is decompressed, and create a folder named build.

```
cd grub-2.02~rc1
mkdir -p build
```

v. Go to the build folder, and compile and install GRUB.

```
cd build
../configure
```

```
sed -i -e "s/-Werror//" ./grub-core/Makefile
sed -i -e "s/-Werror//" . /Makefile
make && make install
```

vi. Create symbolic links.

```
ln -s /usr/local/sbin/grub-install /sbin/grub-install
ln -s /usr/local/sbin/grub-mkconfig /sbin/grub-mkconfig
```

> **Note** If the `-Werror` error is reported during compilation, find the *makefile* file, remove the `-Werror` option from the file, and then try again.

7. Run the `grub-install --version` command to check the GRUB version.

What's next

- If the GRUB version that you installed appears in the command output, you can use SMC to migrate the server to Alibaba Cloud. For more information, see Migration process in *Server Migration Center User Guide*.
- (Optional) After the migration is complete, run the following commands to restore GRUB to the original version:

```
rm /sbin/grub-install
rm /sbin/grub-mkconfig
rm /boot/grub/grub.cfg
mv /sbin/grub-old /sbin/grub
mv /sbin/grub-install-old /sbin/grub-install
```

11.3. How do I enable or disable the Meltdown and Spectre patches for Linux images?

This topic describes how Alibaba Cloud ECS responds to the Meltdown and Spectre vulnerabilities and how to protect ECS instances against these vulnerabilities.

Background information

The Meltdown and Spectre vulnerabilities were exposed in Intel processor chips. These vulnerabilities are caused by design flaws at the chip hardware layer. Exploitation of these vulnerabilities can result in security problems such as kernel data leaks of operating systems and unauthorized access to system kernel data by applications. You can go to the CVE website to check the vulnerability IDs:

- CVE-2017-5753
- CVE-2017-5715
- CVE-2017-5754

On January 20, 2018, Alibaba Cloud released a vulnerability notice to describe the details and impacts of the vulnerabilities.

This topic describes the Alibaba Cloud public images that have been patched against these vulnerabilities and how to configure the operating system. The default security policy is as follows:

- To protect against the Meltdown vulnerability, Page Table Isolation (PTI) is enabled.
- To protect against the Spectre vulnerability, No Indirect Branch Restricted Speculation (NOIBRS) is enabled and is integrated with Retpoline and Indirect Branch Prediction Barriers (IBPB).

How to enable or disable the Meltdown patch

The following public images have the Meltdown patch enabled (PTI On):

- CentOS 7.5/7.6
- Debian 9.6/8.10
- Red Hat 7.5/7.6
- SUSE Linux 15
- Ubuntu 18.04
- CoreOS 1911.3.0
- FreeBSD 11.2
- OpenSUSE 15

The preceding list is subject to change due to updates to Alibaba Cloud public images.

If you find that enabling PTI affects the performance of your instances, or if you have other protective measures, you can take the following steps to disable PTI:

1. Connect to your instance.
2. Perform one of the following operations based on your Linux distribution:
   - CentOS, Debian, OpenSUSE, Red Hat, SUSE Linux, and Ubuntu: Add the `nopti` kernel parameter.
   - CoreOS: Run the `vi /usr/share/oem/grub.cfg` command, add the `pti` parameter to the GRUB configuration file, and set the parameter to off.
   - FreeBSD: Run the `vi /boot/loader.conf` command, add the `vm.pmap.pti` parameter to the configuration file, and set the parameter to 0.
3. Restart the instance.

How to enable or disable the Spectre patch

Alibaba Cloud currently allows you to configure Indirect Branch Restricted Speculation (IBRS) and IBPB. By default, public images are protected against the Spectre vulnerability through Reptpoline and IBPB. You can disable IBRS by using the noibrs parameter. The following public images have the Spectre patch enabled:

- CentOS 7.5/7.6
- Debian 9.6/8.10
- Red Hat 7.5/7.6
- SUSE Linux 15
- Ubuntu 18.04
- CoreOS 1911.3.0
- FreeBSD 11.2
- OpenSUSE 15

The preceding list is subject to change due to updates to Alibaba Cloud public images.

If you want to restore the default settings of your operating system, find that the current setting affects the performance of your instances, or want to implement other protective measures, you can take the following steps to disable the Spectre patch:

1. Connect to your instance.
2. Perform one of the following operations based on your Linux distribution as described in the following table.

<table>
<tr><th>Linux distribution</th><th>How to restore the default settings of Alibaba Cloud images</th><th>How to restore the default settings of the operating system</th><th>How to disable the Spectre patch</th></tr>
<tr><td>CentOS</td><td rowspan="2">Add the noibrs kernel parameter.</td><td rowspan="2">Remove the noibrs kernel parameter.</td><td rowspan="6">Add the spectre_v2 kernel parameter and set it to off.</td></tr>
<tr><td>Red Hat</td></tr>
<tr><td>CoreOS</td><td>Run the <code>vi /usr/oem/share/grub.cfg</code> command, add the spectre_v2 kernel parameter to the GRUB configuration file, and set the parameter to off.</td><td rowspan="3">Remove the disabled spectre_v2 kernel parameter.</td></tr>
<tr><td>OpenSUSE</td><td>Add the spectre_v2 kernel parameter and set it to off.</td></tr>
<tr><td>Debian</td><td rowspan="2">Retpoline and IBPB are enabled by default.</td><td rowspan="3">No modification is required.</td></tr>
<tr><td>Ubuntu</td></tr>
<tr><td>SUSE Linux</td><td>Retpoline is enabled by default.</td></tr>
</table>

Linux distribution	How to restore the default settings of Alibaba Cloud images	How to restore the default settings of the operating system	How to disable the Spectre patch
FreeBSD	Add the hw.ibrs_disable kernel parameter.	Remove the hw.ibrs_disable kernel parameter.	Add the hw.ibrs_disable kernel parameter.

> **Note** The `noibrs` kernel parameter does not work for OpenSUSE and CoreOS. You must set the `spectre_v2` parameter to off for them.

3. Restart the instance.

How to check whether the Meltdown or Spectre patch is enabled

1. Connect to your instance.
2. Obtain the spectre-meltdown-checker.sh script from GitHub spectre-meltdown-checker Repo.
3. Run the following commands in your instance:

```
chmod +x spectre-meltdown-checker.sh
sudo bash spectre-meltdown-checker.sh
```

4. Determine whether the Meltdown or Spectre patch is enabled based on the script prompts.

References

For the following operating systems, you can go to their official websites for more details:

- Red Hat
- SUSE Linux
- Ubuntu