Alibaba Cloud
Elastic Compute Service
Images

Issue: 20200403
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 due to product version upgrades, adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall 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 the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults" and "as available" basis. 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 bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequent
ial, exemplary, incidental, 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 contact Alibaba Cloud directly if you discover any errors in this document.
# Document conventions

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

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legal disclaimer</td>
<td>1</td>
</tr>
<tr>
<td>Document conventions</td>
<td>1</td>
</tr>
<tr>
<td>1 Image overview</td>
<td>1</td>
</tr>
<tr>
<td>2 Select an image</td>
<td>6</td>
</tr>
<tr>
<td>3 Search for an image</td>
<td>13</td>
</tr>
<tr>
<td>4 Public image</td>
<td>15</td>
</tr>
<tr>
<td>4.1 Public image overview</td>
<td>15</td>
</tr>
<tr>
<td>4.2 Release notes</td>
<td>19</td>
</tr>
<tr>
<td>4.3 Known issues</td>
<td>40</td>
</tr>
<tr>
<td>5 Aliyun Linux 2</td>
<td>49</td>
</tr>
<tr>
<td>5.1 Overview of Aliyun Linux 2</td>
<td>49</td>
</tr>
<tr>
<td>5.2 Release notes of Aliyun Linux 2</td>
<td>56</td>
</tr>
<tr>
<td>5.3 Known issues about Aliyun Linux 2</td>
<td>63</td>
</tr>
<tr>
<td>5.4 Features and interfaces supported by Aliyun Linux 2</td>
<td>65</td>
</tr>
<tr>
<td>5.4.1 Use the Aliyun Linux 2 image in an on-premises environment</td>
<td>65</td>
</tr>
<tr>
<td>5.4.2 Enable the cgroup writeback feature</td>
<td>70</td>
</tr>
<tr>
<td>5.4.3 Configure the weight-based throttling feature of blk-iocost</td>
<td>73</td>
</tr>
<tr>
<td>5.4.4 Enable the PSI feature for the cgroup v1 interface</td>
<td>79</td>
</tr>
<tr>
<td>5.4.5 Change the timeout period of TCP TIME-WAIT</td>
<td>81</td>
</tr>
<tr>
<td>5.4.6 Enhance the monitoring of block I/O throttling</td>
<td>82</td>
</tr>
<tr>
<td>5.4.7 Use the JBD2 optimization interface</td>
<td>84</td>
</tr>
<tr>
<td>5.4.8 Create a hard link across project quotas</td>
<td>87</td>
</tr>
<tr>
<td>5.4.9 Track I/O latency</td>
<td>88</td>
</tr>
<tr>
<td>5.4.10 Detect I/O hangs of file systems and block layers</td>
<td>90</td>
</tr>
<tr>
<td>5.5 Knowledge base about Aliyun Linux 2</td>
<td>92</td>
</tr>
<tr>
<td>5.6 FAQ about Aliyun Linux 2</td>
<td>93</td>
</tr>
<tr>
<td>6 Custom image</td>
<td>97</td>
</tr>
<tr>
<td>6.1 Create custom image</td>
<td>97</td>
</tr>
<tr>
<td>6.1.1 Create a custom image by using a snapshot</td>
<td>97</td>
</tr>
<tr>
<td>6.1.2 Create a custom image by using an instance</td>
<td>100</td>
</tr>
<tr>
<td>6.1.3 Use Packer to create a custom image</td>
<td>102</td>
</tr>
<tr>
<td>6.1.4 Create and import on-premises images by using Packer</td>
<td>106</td>
</tr>
<tr>
<td>6.2 Update a custom image</td>
<td>112</td>
</tr>
<tr>
<td>6.3 Modify custom images</td>
<td>117</td>
</tr>
<tr>
<td>6.4 Import images</td>
<td>118</td>
</tr>
<tr>
<td>6.4.1 Image import procedure</td>
<td>118</td>
</tr>
<tr>
<td>6.4.2 Use the image compliance tool</td>
<td>119</td>
</tr>
<tr>
<td>6.4.3 Instructions for importing images</td>
<td>125</td>
</tr>
<tr>
<td>6.4.4 Install cloud-init</td>
<td>128</td>
</tr>
</tbody>
</table>
6.4.5 Install virtio driver................................................................. 138
6.4.6 Customize Linux images....................................................... 144
6.4.7 Convert the image file format................................................. 150
6.4.8 Import custom images.......................................................... 152
6.5 Copy custom images.................................................................. 157
6.6 Share or unshare custom images............................................... 159
6.7 Export custom images............................................................... 162
6.8 Delete custom images............................................................... 165
7 Marketplace images.................................................................... 167
8 Open source tools...................................................................... 170
9 Change the operating system....................................................... 171
11 FAQ......................................................................................... 172
   11.1 Manage Windows Server Semi-Annual Channel images and instances.. 172
   11.2 Install GRUB v1.99 in a Linux server......................................... 178
   11.3 How do I enable or disable the Meltdown and Spectre patches for Linux images?.................................................. 180
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

ECS images are classified into the following types based on their sources. Fees are charged for ECS images. We recommend that you read and understand the pricing details of ECS before you use ECS images. For more information, see Billing overview.

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public image</td>
<td>Public images are licensed by Alibaba Cloud, which are highly secure and stable. Public images include Windows Server system images and mainstream Linux system images. For more information, see Public image overview.</td>
<td>Only Windows Server and Red Hat Enterprise Linux public images are charged. 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.</td>
</tr>
</tbody>
</table>
<pre><code>                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
</code></pre>
<p>|               |                                                                                                                                                                                                                                                                                                                                                                                                  | · Red Hat Enterprise Linux: Fees are calculated based on the instance specification.                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|               |                                                                                                                                                                                                                                                                                                                                                                                                  | · Windows Server: Fees are calculated based on the instance specification.                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|               |                                                                                                                                                                                                                                                                                                                                                                                                  | Other public images are free of charge.                                                                                                                                                                                                                                                                                                                                                                                                                       |</p>

Issue: 20200403
<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
<th>Price</th>
</tr>
</thead>
</table>
| 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 charged 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 charged based on the storage space usage.  
  - Instance creation fees. When you use a custom image to create an instance, fees are charged as follows:  
    - If the custom image is created based on an Alibaba Cloud Marketplace image, the custom image fees are equal to the total amount of 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*. |
<p>| Shared image | Shared images are images shared to you by other Alibaba Cloud accounts. For more information, see <em>Share images</em>. | If a shared image is provided by Alibaba Cloud Marketplace, the shared image is billed according to the pricing standards of the independent software vendor (ISV). |</p>
<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alibaba Cloud Marketplace image</td>
<td>Alibaba Cloud Marketplace images are classified into the following types based on the ISV.</td>
<td>Alibaba Cloud Marketplace images are billed according to the pricing standards of the ISV.</td>
</tr>
<tr>
<td></td>
<td>･ Images provided by Alibaba Cloud accounts</td>
<td></td>
</tr>
<tr>
<td></td>
<td>･ Images provided by ISVs and licensed by Alibaba Cloud Marketplace</td>
<td></td>
</tr>
<tr>
<td></td>
<td>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 ISV and Alibaba Cloud to ensure that the images are safe to use. For more information, see <em>Marketplace images</em>.</td>
<td></td>
</tr>
</tbody>
</table>

**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 an ECS instance, 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 then create a custom image for the instance. For more information, see Create a custom image by using an instance. Instances created from the custom image contain all the configuration items that you have defined. For more information, see #unique_10.

You can create a custom image by using the snapshot of the system disk or both the system and data disks. For more information, see Create a custom image by using a snapshot.

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

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 in this region only.

- When you share the image with another Alibaba Cloud account, this account can use the image in the China (Beijing) region only. To share the image to an Alibaba Cloud account who needs to use the image in a different region, copy the
image to the target region, and then share the image to the target Alibaba Cloud account. For more information, see *Share images*.

- If you need to use the image in another region, copy the image to that region. The image copy is signed a unique UID. It is independent of the original image. For more information, see *Copy custom images*.

**Change images for an ECS instance**

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

- You can replace the image of the system disk with a public image. For more information, see #unique_14.

- You can also replace the image of the system disk with a non-public image, for example, a custom, shared, or Alibaba Cloud Marketplace image. For more information, see #unique_15.

**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 #unique_16 of an ECS instance that is created from the image.

A custom image consists of snapshots of disks that are attached to an ECS instance. The delete operation does not delete snapshots contained in the image. To delete the snapshots, navigate to the Snapshots page and delete the target snapshots. For more information, see *Delete custom images*.

**API operations**

You can also perform API operations to manage an image. For more information, see *API overview*.
2 Select an image

This topic describes how to select an appropriate image for your instance.

We recommend that you take the following items into consideration when selecting an image for your instance:

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

Region

Images are regional resources. An image that is used to create instances must belong to the same region as the instances. For example, if you create an instance in China (Beijing), you can use images only in China (Beijing). For more information, see #unique_20.

To create an instance by using an image located in a different region, you must first copy the image to the current region. For more information, see Copy images.

Image types and billing methods

ECS images are classified into public images, custom images, shared images, and Marketplace images, according to the image source. For information about image types and billing methods, see Image overview.

Operating system

You must select an operating system (OS) during instance creation.

- OS architecture

  You can select a 32-bit or 64-bit OS architecture for your instance.

  - 32-bit OS architecture supports a maximum of 4 GiB memory. Additionally, a 32-bit Windows OS supports a maximum of four CPU cores.
  - 64-bit OS architecture supports at least 4 GiB memory and larger.
**OS type (Windows or Linux/Unix-like OS)**

<table>
<thead>
<tr>
<th>OS type</th>
<th>Logon mode</th>
<th>Feature</th>
<th>Scenario</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>Remote Desktop</td>
<td>A Windows public image is installed with a genuine activated system.</td>
<td>- Supporting programs developed based on Windows, such as .NET</td>
</tr>
<tr>
<td></td>
<td>Connection</td>
<td></td>
<td>- Supporting SQL Server and other databases (you need to manually install a database first.)</td>
</tr>
<tr>
<td>Linux/Unix-like</td>
<td>SSH</td>
<td>A common server-side open-source operating system that features high</td>
<td>- Generally used for server applications such as high-performance web servers</td>
</tr>
<tr>
<td></td>
<td></td>
<td>security and stability, fast deployment, and easy source code</td>
<td>- Supporting common programming languages such as PHP and Python</td>
</tr>
<tr>
<td></td>
<td></td>
<td>compilation.</td>
<td>- Supporting MySQL and other databases (you need to manually install a database first.)</td>
</tr>
</tbody>
</table>

Alibaba Cloud provides a list of public images that run Windows or Linux/Unix-like OS. For more information, see [Overview of public images](#).

**Considerations for Windows**

The following information is provided for your consideration if you select to run Windows on your instance. Generally, we recommend that you use a later version of Windows for ease of use and better security.

- Instance types with one vCPU core and 1 GiB memory cannot start the MySQL database.

- We recommend that your target instances have at least 2 GiB memory or larger if you want to host one or more websites, deploy web environments, or use Windows Server 2008, Windows Server 2012, Windows Server 2016, or
Windows Server 2019. Otherwise, the selected image may not be displayed on
the purchase page, instance performance may be degraded, or both.

- Alibaba Cloud no longer provides technical support for Windows Server 2003
  system images. For more information, see Offline announcement of Windows Server
  2003 system image.

• Considerations for Linux and Unix-like OSs

The following information is provided for your consideration if you run a Linux
or Unix-like operating system on your instance, and includes detailed informatio
n about the supported image versions.

- Aliyun Linux

  Aliyun Linux is an operating system developed by Alibaba Cloud that
  provides a safer, more stable, and high-performance running environment
  for applications on ECS instances. Aliyun Linux 2 supports various cloud
  scenarios and instance types (except for instances in a classic network and
non-I/O-optimized instances). For more information, see Overview of Aliyun Linux 2.

- Red Hat series
  ■ CentOS
  ■ Red Hat

The following table compares CentOS with Red Hat.

<table>
<thead>
<tr>
<th>OS</th>
<th>Software package format</th>
<th>Package manager</th>
<th>Billing method</th>
<th>Feature</th>
<th>Relationship</th>
</tr>
</thead>
<tbody>
<tr>
<td>CentOS</td>
<td>.rpm</td>
<td>yum</td>
<td>Free usage</td>
<td>■ Stable, but lower patch update speed than Red Hat</td>
<td>■ CentOS is an open-source version of Red Hat.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>■ Supporting online instant upgrades</td>
<td>■ They can use the same RPM package and commands.</td>
</tr>
</tbody>
</table>

Issue: 20200403
The following table compares Debian with Ubuntu.

<table>
<thead>
<tr>
<th>OS</th>
<th>Software package format</th>
<th>Package manager</th>
<th>Feature</th>
<th>Relationship</th>
</tr>
</thead>
<tbody>
<tr>
<td>Debian</td>
<td>.deb</td>
<td>aptitude</td>
<td>Stable</td>
<td>Ubuntu builds on the Debian architecture and infrastructure.</td>
</tr>
</tbody>
</table>
| Ubuntu     |                         | apt-get         |           | User-friendly system configuration
|            |                         |                | Timely software updates
|            |                         |                | Easy to use                                      |

The following table compares SUSE Linux with openSUSE.

- SUSE
  - SUSE Linux
  - openSUSE

Reducing complexity and improving stability with enterprise-level technical support.
<table>
<thead>
<tr>
<th>OS</th>
<th>Feature</th>
<th>Relationship</th>
</tr>
</thead>
<tbody>
<tr>
<td>openSUSE</td>
<td>■ openSUSE is the community version of SUSE Linux. It features advanced software versions, better extensibility (desktop and server installation are supported), and free updates (you can also purchase official technical support).</td>
<td>■ As of version 10.2, SUSE Linux was officially renamed openSUSE.</td>
</tr>
<tr>
<td>SUSE Linux</td>
<td>■ SUSE Linux Enterprise is the enterprise version of SUSE Linux. It is more mature and stable, but its official release contains fewer software features than openSUSE.</td>
<td>■ openSUSE uses the same kernel as SUSE Linux.</td>
</tr>
<tr>
<td></td>
<td>■ SUSE Linux Enterprise offers better work and production environments, whereas openSUSE delivers a superior entertainment experience and professional services.</td>
<td></td>
</tr>
</tbody>
</table>

- CoreOS

CoreOS is an open-source lightweight operating system based on the Linux kernel and designed to provide infrastructure for clustered deployments. It 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 which focuses on features, speed, and stability. FreeBSD offers advanced networking, performance, security and compatibility features today which are still missing in other operating systems, even some of the best commercial ones. For more information, see FreeBSD official documentation.
Built-in software

Alibaba Cloud Marketplace images are typically provided pre-installed with a running environment and software applications that you can apply to target ECS instances as needed. For more information, see Marketplace images.

What to do next

- Use a target image to create instances. For more information, see #unique_22.
- Use a target image to change the operating system of a current image. For more information, see Change the operating system.
3 Search for an image

This topic describes how to search for a specific image through the ECS console or by calling the related API action.

Use the ECS console

You can search for a specific image on the Images page of the ECS console.

Procedure

1. Log on to the ECS console.
2. In the top navigation bar, select a region.
3. In the left-side navigation pane, choose Instances & Images > Images.
4. Click the tab of a specific image type.
5. In the drop-down list, select a search item such as image name, image ID, or snapshot ID.
6. Enter one or more keywords in the search bar.
   
   For an ID search, you must enter an exact keyword item. For an image name search, you can enter partial keyword items (such as `win` to return Windows public image results).
7. Click Search.

Call an API action

You can call DescribeImages to search for an image through the API Explorer or Alibaba Cloud CLI. The following procedure uses the API Explorer as an example.

1. Log on to the API Explorer.
2. In the drop-down list of RegionId, select the target region.
3. Optional. Specify other parameters, such as ImageName and ImageId.

Note:

The naming rules of image IDs are as follows:

- Public image: The image ID is named by the version, architecture, language, and release date of the operating system. For example, the image ID of a 64-bit Windows Server 2008 R2 Enterprise Edition (English version) is `win2008r2_64_ent_sp1_en-us_40G_alibase_20190318.vhd`.
• Custom image and Marketplace image: The image ID starts with an m.
• Shared image: The image ID is the same as the ID of the source custom image.

4. Click Submit Request.

5. Click the Debugging Result tab.

If the required image is found, detailed information of the image, such as the image ID, image description, and operating system type is displayed on the Debugging Result tab. For more information, see #unique_25.

What to do next

After you find the required image, you can:

• Create an instance by using the wizard.
• Share custom images.
• Copy custom images.
• Export custom images.
• Delete custom images.
• Modify custom images.
4 Public image

4.1 Public image overview

Public images provided by Alibaba Cloud are fully licensed to provide a secure and stable operating environment for applications on ECS instances. This topic describes Aliyun Linux images and third-party and open-source images.

Types of public images

The following table describes two types of public images provided by Alibaba Cloud. You can use any public images for free to create ECS instances except for the Windows Server and Red Hat Enterprise Linux images. For more information, see Image overview.

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
<th>Technical support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aliyun Linux images</td>
<td>Aliyun Linux images are custom, native operating systems provided by Alibaba Cloud for you to launch ECS instances. Each Aliyun Linux image has been rigorously tested to guarantee its security, stability, and normal startup and operation.</td>
<td>Alibaba Cloud provides technical support if any problem occurs during the use of Aliyun Linux images.</td>
</tr>
</tbody>
</table>
| Third-party and open-source images | Third-party and open-source images have been rigorously 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 OS 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.
## Elastic Compute Service

### Images / 4 Public image

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aliyun Linux 2</td>
<td>Aliyun Linux 2.1903 64-bit</td>
<td>A next-generation OS that supports various Alibaba Cloud instance types including ECS Bare Metal Instances. Aliyun Linux 2 is also equipped with <em>Alibaba Cloud CLI</em> and other software packages by default. If you want to replace other Linux distributions with Aliyun Linux 2, you can select Public Image and then Aliyun Linux 2 when creating an ECS instance, or replace the system disk of an existing ECS instance with Aliyun Linux 2. For more information, see <em>Aliyun Linux 2</em>.</td>
</tr>
</tbody>
</table>

### Third-party and open-source images

Alibaba Cloud regularly releases and updates public images of third-party and open-source vendors. 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 *Search for an image*.

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

#### Windows images

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- Windows Server 2019 Datacenter Edition 64-bit (English)</td>
</tr>
<tr>
<td></td>
<td>- Windows Server 2016 Datacenter Edition 64-bit (English)</td>
</tr>
</tbody>
</table>
### Operating system

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- Windows Server 2012 R2 Datacenter Edition 64-bit (English)</td>
</tr>
<tr>
<td>**** (Semi-Annual</td>
<td>- Windows Server Version **** Datacenter Edition 64-bit (English)</td>
</tr>
<tr>
<td>Channel)</td>
<td>**** indicates the latest version of the Semi-Annual Channel images.</td>
</tr>
</tbody>
</table>

#### Note:

Support for Windows Server 2008 and Windows Server 2008 R2 was ended by Microsoft on January 14, 2020. Therefore, Alibaba Cloud does not provide technical support for ECS instances that use these operating systems. If you have an ECS instance that uses Windows Server 2008 or Windows Server 2008 R2, please change its operating system to Windows Server 2012 or a later version as soon as possible.

- **Linux images**

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>CentOS</td>
<td>- CentOS 7.7 64-bit &lt;br&gt; - CentOS 7.6 64-bit &lt;br&gt; - CentOS 7.5 64-bit &lt;br&gt; - CentOS 7.4 64-bit &lt;br&gt; - CentOS 7.3 64-bit &lt;br&gt; - CentOS 7.2 64-bit &lt;br&gt; - CentOS 6.10 64-bit &lt;br&gt; - CentOS 6.9 64-bit &lt;br&gt; - CentOS 6.8 32-bit</td>
</tr>
</tbody>
</table>

#### Note:

If you are using a 32-bit operating system, do not select instance types that have a memory capacity exceeding 4 GiB. For more information, see Select an image.
<table>
<thead>
<tr>
<th>Operating system</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>CoreOS</td>
<td>- CoreOS 2023.4.0 64-bit</td>
</tr>
<tr>
<td></td>
<td>- CoreOS 1745.7.0 64-bit</td>
</tr>
<tr>
<td>Debian</td>
<td>- Debian 9.9 64-bit</td>
</tr>
<tr>
<td></td>
<td>- Debian 9.8 64-bit</td>
</tr>
<tr>
<td></td>
<td>- Debian 9.6 64-bit</td>
</tr>
<tr>
<td></td>
<td>- Debian 8.11 64-bit</td>
</tr>
<tr>
<td></td>
<td>- Debian 8.9 64-bit</td>
</tr>
<tr>
<td>FreeBSD</td>
<td>FreeBSD 11.2 64-bit</td>
</tr>
<tr>
<td>openSUSE</td>
<td>openSUSE 42.3 64-bit</td>
</tr>
<tr>
<td>Red Hat</td>
<td>- Red Hat Enterprise Linux 8 64-bit</td>
</tr>
<tr>
<td></td>
<td>- Red Hat Enterprise Linux 7.6 64-bit</td>
</tr>
<tr>
<td></td>
<td>- Red Hat Enterprise Linux 7.5 64-bit</td>
</tr>
<tr>
<td></td>
<td>- Red Hat Enterprise Linux 7.4 64-bit</td>
</tr>
<tr>
<td></td>
<td>- Red Hat Enterprise Linux 6.10 64-bit</td>
</tr>
<tr>
<td></td>
<td>- Red Hat Enterprise Linux 6.9 64-bit</td>
</tr>
<tr>
<td>SUSE Linux</td>
<td>- SUSE Linux Enterprise Server 12 SP4 64-bit</td>
</tr>
<tr>
<td></td>
<td>- SUSE Linux Enterprise Server 12 SP2 64-bit</td>
</tr>
<tr>
<td></td>
<td>- SUSE Linux Enterprise Server 11 SP4 64-bit</td>
</tr>
<tr>
<td>Ubuntu</td>
<td>- Ubuntu 18.04 64-bit</td>
</tr>
<tr>
<td></td>
<td>- Ubuntu 16.04 64-bit</td>
</tr>
<tr>
<td></td>
<td>- Ubuntu 16.04 32-bit</td>
</tr>
<tr>
<td></td>
<td>- Ubuntu 14.04 64-bit</td>
</tr>
<tr>
<td></td>
<td>- Ubuntu 14.04 32-bit</td>
</tr>
</tbody>
</table>

**Note:**
If you are using a 32-bit operating system, do not select instance types that have a memory capacity exceeding 4 GiB. For more information, see [Select an image](#).
4.2 Release notes

This topic describes the updates for the ECS image feature in the order of their release time. Unless otherwise stated, the released updates apply to all Alibaba Cloud ECS regions.
### Aliyun Linux 2

<table>
<thead>
<tr>
<th>Image ID</th>
<th>Release date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>aliyun_2_1 903_64_20G_alibase_2 0190829.vhd</code></td>
<td>August 29, 2019</td>
<td>- Updated to the latest software version</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>Kernel changes:</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Updated to the kernel version 4.19.57-15.1.x86_64 version</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Fixed the Spectre-V1 SWAPGS vulnerability</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Fixed the bio splitting code</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Set the default TCP congestion control algorithm to CUBIC</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Configured the network to 10-eth0. network</td>
</tr>
</tbody>
</table>

**Issue:** 20200403
<table>
<thead>
<tr>
<th>Image ID</th>
<th>Release date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aliyun_2_1903_64_20G</td>
<td>June 19, 2019</td>
<td>• Updated to the latest software version</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Kernel changes:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Updated to the kernel version</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4.19.43-13.2.17.x86_64 version</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Added support for the cgroup writeback feature</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Added support for policy-based routing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Added support for the <code>ss</code> command from the <code>iproute2</code> suite</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Fixed the following network-related CVEs:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ CVE-2019-11477</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ CVE-2019-11478</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ CVE-2019-11479</td>
</tr>
<tr>
<td>Image ID</td>
<td>Release date</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>aliyun-2.1903-x64-20G-alibase-20190507.vhd</td>
<td>May 7, 2019</td>
<td>• Updated to the latest software version</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Fixed the time synchronization delay that was present on instance startup</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Updated the kernel version to kernel-4.19.34-11.al7.x86_64 and fixed other issues</td>
</tr>
<tr>
<td>Image ID</td>
<td>Release date</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| `aliyun-2.1903-x64-20G-alibase-20190327.vhd` | March 27, 2019 | • Released Aliyun Linux 2  
• Used the kernel -4.19.24-9.al7.x86_64 kernel version in Aliyun Linux 2 |

**CentOS**

<table>
<thead>
<tr>
<th>Release</th>
<th>Image ID</th>
<th>Release date</th>
<th>Description</th>
</tr>
</thead>
</table>
| CentOS 7.7 | `centos_7_7_x64_20G-alibase_20191225.vhd`    | December 25, 2019 | • Kernel version: 3.10.0-1062.9.1.el7.x86_64  
• Changes: updated to include the latest operating system patches |
<table>
<thead>
<tr>
<th>Release</th>
<th>Image ID</th>
<th>Release date</th>
<th>Description</th>
</tr>
</thead>
</table>
| CentOS 8.0 | centos_8_0_x64_20Gアルバセ_20191225.vhd     | December 25, 2019 | - 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 Custom network configurations in Install cloud-init. |
| CentOS 6.10 | centos_6_10_x64_20Gアルバセ_20191223.vhd     | December 25, 2019 | - 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アルバセ_20191008.vhd     | October 8, 2019 | - Kernel version: 3.10.0-1062.1.2.el7.x86_64  
- Changes: new release  
| CentOS 7.6 | centos_7_06_64_20Gアルバセ_20190711.vhd     | July 11, 2019 | - Kernel version: 3.10.0-957.21.3.el7.x86_64  
- Changes: updated to include the latest operating system patches  

<table>
<thead>
<tr>
<th>Release</th>
<th>Image ID</th>
<th>Release date</th>
<th>Description</th>
</tr>
</thead>
</table>
| CentOS 6.10 | centos\_6\_10\_64\_20G\_a\_libase\_20190709.vhd | July 9, 2019 | - 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\_a\_libase\_20190621.vhd | June 21, 2019 | - 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\_a\_libase\_20190619.vhd | June 19, 2019 | - Kernel version: 3.10.0-957.21.3.el7.x86\_64  
- Changes:  
  - Updated to include the latest operating system patches and fixed the CVE-2019-11477 vulnerability  
  - Set the default CPU mode to performance |
| CentOS 7.6 | centos\_7\_06\_64\_20G\_a\_libase\_20190218.vhd | February 18, 2019 | - Kernel version: 3.10.0-957.5.1.el7.x86\_64  
- Changes: updated to include the latest operating system patches |
| CentOS 7.6 | centos\_7\_05\_64\_20G\_a\_libase\_20181212.vhd | December 12, 2018 | - Kernel version: 3.10.0-957.1.3.el7.x86\_64  
- Changes: updated to include the latest operating system patches |
<table>
<thead>
<tr>
<th>Release</th>
<th>Image ID</th>
<th>Release date</th>
<th>Description</th>
</tr>
</thead>
</table>
| CentOS 7.5 | centos\_7\_05\_64\_20G\_alibase\_20181210.vhd | December 10, 2018 | - Kernel version: 3.10.0-862 .3.3.el7.x86_64.  
- Changes:  
  - Updated to include the latest operating system patches  
  - Updated the cloud-init version  
  - Enabled the chrony time synchronization service  
  - Disabled password authentication by default  
  - Set GRUB\_TIMEOUT to 1 |
| Debian | | | |
| Debian 9.11 | debian\_9\_11\_x64\_20G\_alibase\_20191225.vhd | December 25, 2019 | - Kernel version: 4.9.0-11-amd64  
- Changes: updated to include the latest operating system patches |
<table>
<thead>
<tr>
<th>Release</th>
<th>Image ID</th>
<th>Release date</th>
<th>Description</th>
</tr>
</thead>
</table>
| Debian 10.2 | debian_10_2_x64_20G_alibase_20191223.vhd | December 24, 2019 | - 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 Custom network configurations in Install cloud-init. |
| Debian 9.9 | debian_9_09_64_20G_alibase_20190702.vhd | July 2, 2019 | - 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 | May 10, 2019 | - Kernel version: 4.9.0-9-amd64  
- Changes: updated to include the latest operating system patches |
<table>
<thead>
<tr>
<th>Release</th>
<th>Image ID</th>
<th>Release date</th>
<th>Description</th>
</tr>
</thead>
</table>
| Debian 8.11 | 11_64_20G_alibase_20190311.vhd | March 11, 2019 | - 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 | February 25, 2019 | - Kernel version: 4.9.0-8-amd64  
- Changes: updated to include the latest operating system patches |
| Debian 9.6 | debian_9_06_64_20G_alibase_20190103.vhd | January 3, 2019 | - Kernel version: 4.9.0-8-amd64  
- Changes: enabled the systemd-networkd service |
| Debian 9.6 | debian_9_06_64_20G_alibase_20181212.vhd | December 12, 2018 | - Kernel version: 4.9.0-8-amd64  
- Changes:  
  - Updated to include the latest operating system patches  
  - Updated the cloud-init version  
  - Enabled the chrony time synchronization service  
  - Set GRUB_TIMEOUT to 1  
- Known issues: Classic network configuration issues |
### FreeBSD

<table>
<thead>
<tr>
<th>Release</th>
<th>Image ID</th>
<th>Release date</th>
<th>Description</th>
</tr>
</thead>
</table>
| FreeBSD 11.2  | freebsd_11_02_64_30G_alibase_20190806.vhd        | August 6, 2019 | · Kernel version: 11.2-RELEASE  
· Changes:  
  - Fixed the clock offset issue  
  - Fixed the issue causing 30-GiB system disk creation to fail |

### Ubuntu

<table>
<thead>
<tr>
<th>Release</th>
<th>Image ID</th>
<th>Release date</th>
<th>Description</th>
</tr>
</thead>
</table>
| Ubuntu 18.04  | ubuntu_18_04_x64_20G_alibase_20191225.vhd        | December 25, 2019 | · 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        | December 25, 2019 | · 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         | June 24, 2019  | · Kernel version: 4.15.0-52-generic  
· Changes: updated to include the latest operating system patches and fixed the CVE-2019-11477 vulnerability |
<table>
<thead>
<tr>
<th>Release</th>
<th>Image ID</th>
<th>Release Date</th>
<th>Description</th>
</tr>
</thead>
</table>
| Ubuntu 16.04 | ubuntu_16_04_64_20G_alibase_20190620.vhd | June 20, 2019 | - 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 | May 13, 2019 | - 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 | May 9, 2019 | - Kernel version: 4.15.0-48-generic  
- Changes:  
  - Updated cloud-init to speed up boot time  
  - Updated to include the latest operating system patches |
| Ubuntu 16.04 | ubuntu_16_04_64_20G_alibase_20190301.vhd | March 1, 2019 | - 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 | February 23, 2019 | - Kernel version: 4.15.0-45-generic  
- Changes: updated to include the latest operating system patches |
<table>
<thead>
<tr>
<th>Release</th>
<th>Image ID</th>
<th>Release date</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Ubuntu 18.04** | ubuntu_18_04_64_2G_alibase_20181212.vhd     | December 12, 2018 | - Kernel version: 4.15.0-42-generic  
  - Changes:  
    - Updated to include the latest operating system patches  
    - Updated the cloud-init version  
    - Enabled the chrony time synchronization service  
    - Set GRUB_TIMEOUT to 1 |

**CoreOS**

<table>
<thead>
<tr>
<th>Release</th>
<th>Image ID</th>
<th>Release date</th>
<th>Description</th>
</tr>
</thead>
</table>
| **CoreOS 2303**  | coreos_2303_3_x64_30G_alibase_20191223.vhd   | December 24, 2019 | - Kernel version: 4.19.86-coreos  
  - Changes: updated to include the latest operating system patches |

**OpenSUSE**

<table>
<thead>
<tr>
<th>Release</th>
<th>Image ID</th>
<th>Release date</th>
<th>Description</th>
</tr>
</thead>
</table>
| **OpenSuse 15.1**| opensuse_15_1_x64_20G_alibase_20191219.vhd   | December 24, 2019 | - Kernel version: 4.12.14-lp151.28.36-default  
  - Changes:  
    - Updated to include the latest operating system patches  
    - Updated cloud-init to version 19.1 |
Windows Server 2008

**Note:**
Support for Windows Server 2008 and Windows Server 2008 R2 was ended by Microsoft on January 14, 2020. Therefore, Alibaba Cloud does not provide technical support for ECS instances that use these operating systems. If you have an ECS instance that uses Windows Server 2008 or Windows Server 2008 R2, please change its operating system to Windows Server 2012 or a later version as soon as possible.

<table>
<thead>
<tr>
<th>Release</th>
<th>Image ID</th>
<th>Release date</th>
<th>Description</th>
</tr>
</thead>
</table>
• English Edition: `win2008r2_64_ent_sp1_en-us_40G.ali_base_20190816.vhd` | August 16, 2019 | • Updated to include the latest operating system patches.  
• English Edition: `win2008r2_64_ent_sp1_en-us_40G.ali_base_20190816.vhd` | August 16, 2019 | • Updated to include the latest operating system patches.  
<table>
<thead>
<tr>
<th>Release</th>
<th>Image ID</th>
<th>Release date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Server 2008 R2 Enterprise Edition</td>
<td>• <strong>Chinese Edition:</strong> <code>win2008r2_64_ent_sp1_zh-cn_40G.ali base_20190718.vhd</code></td>
<td>July 18, 2019</td>
<td>• Updated to include the latest operating system patches.</td>
</tr>
<tr>
<td></td>
<td>• <strong>English Edition:</strong> <code>win2008r2_64_ent_sp1_en-us_40G.ali base_20190718.vhd</code></td>
<td></td>
<td>• Upgraded .NET Framework to version 4.8.</td>
</tr>
<tr>
<td>Windows Server 2008 Standard Edition SP2</td>
<td>• <strong>Chinese Edition:</strong> <code>win2008_32_std_sp2_zh-cn_40G.ali base_20190517.vhd</code></td>
<td>May 17, 2019</td>
<td>• Updated to include the latest operating system patches.</td>
</tr>
<tr>
<td></td>
<td>• <strong>English Edition:</strong></td>
<td></td>
<td>• Fixed the CVE-2019-0708 remote code execution vulnerability in Microsoft Windows Remote Desktop Services.</td>
</tr>
<tr>
<td>Windows Server 2008 R2 Enterprise Edition</td>
<td>• <strong>Chinese Edition:</strong> <code>win2008r2_64_ent_sp1_zh-cn_40G.ali base_20190515.vhd</code></td>
<td>May 15, 2019</td>
<td>• Updated to include the latest operating system patches.</td>
</tr>
<tr>
<td></td>
<td>• <strong>English Edition:</strong> <code>win2008r2_64_ent_sp1_en-us_40G.ali base_20190515.vhd</code></td>
<td></td>
<td>• Fixed the CVE-2019-0708 remote code execution vulnerability in Microsoft Windows Remote Desktop Services.</td>
</tr>
<tr>
<td>Windows Server 2008 R2 Enterprise Edition</td>
<td>• <strong>Chinese Edition:</strong> <code>win2008r2_64_ent_sp1_zh-cn_40G.ali base_20190318.vhd</code></td>
<td>March 18, 2019</td>
<td>Updated to include the latest operating system patches.</td>
</tr>
<tr>
<td></td>
<td>• <strong>English Edition:</strong> <code>win2008r2_64_ent_sp1_en-us_40G.ali base_20190318.vhd</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Release</td>
<td>Image ID</td>
<td>Release date</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>---------------------------------------------------------------------------</td>
<td>----------------</td>
<td>-----------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
• English Edition:                                                                 | December 20, 2018 | • Updated to include the latest security patch KB4471318. You must update Windows clients with the latest patches to establish RDP connections.  
• Upgraded .NET Framework to version 4.7.2.  
• Use the Sysprep tool to generalize the image. |
• English Edition: win2012r2_64_dtc_960_0_en-us_40G.ali base_20191012.vhd                                                                 | October 12, 2019 | Updated to include the latest security patches.                                                   |
• English Edition: win2012r2_64_dtc_960_0_en-us_40G.ali base_20190816.vhd                     | August 16, 2019 | • Updated to include the latest operating system patches.  
<table>
<thead>
<tr>
<th>Release</th>
<th>Image ID</th>
<th>Release date</th>
<th>Description</th>
</tr>
</thead>
</table>
• English Edition: `win2012r2_64_dtc_960_0_en-us_40G.ali base_20190718.vhd` | July 18, 2019 | • Updated to include the latest operating system patches.  
• Upgraded .NET Framework to version 4.8 |
• English Edition: `win2012r2_64_dtc_960_0_en-us_40G.ali base_20190523.vhd` | May 23, 2019 | Updated to include the latest operating system patches. |
• English Edition: `win2012r2_64_dtc_960_0_en-us_40G.ali base_20190318.vhd` | March 18, 2019 | Updated to include the latest operating system patches. |
• English Edition: `win2012r2_64_dtc_960_0_en-us_40G.ali base_20181220.vhd` | December 20, 2018 | • Updated to include the latest security patch KB4471320. You must update Windows clients with the latest patches to establish RDP connection s.  
• Upgraded .NET Framework to version 4.7 .2.  
• Use the Sysprep tool to generalize the image. |
## Windows Server 2016

<table>
<thead>
<tr>
<th>Release</th>
<th>Image ID</th>
<th>Release date</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Windows Server 2016 Datacenter Edition** | • **Chinese Edition:** `win2016_64_dtc_1607_zh-cn_40G_alibase_20191012.vhd`  
• **English Edition:** `win2016_64_dtc_1607_en-us_40G_alibase_20191012.vhd` | **October 12, 2019** | Updated to include the latest security patches. |
| **Windows Server 2016 Datacenter Edition** | • **Chinese Edition:** `win2016_64_dtc_1607_zh-cn_40G_alibase_20190816.vhd`  
• **English Edition:** `win2016_64_dtc_1607_en-us_40G_alibase_20190816.vhd` | **August 16, 2019** | • Updated to include the latest operating system patches.  
| **Windows Server 2016 Datacenter Edition** | • **Chinese Edition:** `win2016_64_dtc_1607_zh-cn_40G_alibase_20190718.vhd`  
• **English Edition:** `win2016_64_dtc_1607_en-us_40G_alibase_20190718.vhd` | **July 18, 2019** | • Updated to include the latest operating system patches.  
• Upgraded .NET Framework to version 4.8. |
| **Windows Server 2016 Datacenter Edition** | • **Chinese Edition:** `win2016_64_dtc_1607_zh-cn_40G_alibase_20190523.vhd`  
• **English Edition:** `win2016_64_dtc_1607_en-us_40G_alibase_20190523.vhd` | **May 23, 2019** | Updated to include the latest operating system patches. |
<table>
<thead>
<tr>
<th>Release</th>
<th>Image ID</th>
<th>Release date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Windows Server 2016 Datacenter Edition</strong></td>
<td>• Chinese Edition: win2016_64_dtc_1607_zh-cn_40G_alibase_20190318.vhd</td>
<td>March 18, 2019</td>
<td>Updated to include the latest operating system patches.</td>
</tr>
<tr>
<td></td>
<td>• English Edition: win2016_64_dtc_1607_en-us_40G_alibase_20190318.vhd</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Windows Server 2016 Datacenter Edition</strong></td>
<td>• Chinese Edition: win2016_64_dtc_1607_zh-cn_40G_alibase_20181220.vhd</td>
<td>December 20, 2018</td>
<td>• Updated to include the latest security patch KB4471321. You must update Windows clients with the latest patches to establish RDP connections.</td>
</tr>
<tr>
<td></td>
<td>• English Edition: win2016_64_dtc_1607_en-us_40G_alibase_20181220.vhd</td>
<td></td>
<td>• Upgraded .NET Framework to version 4.7.2.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Use the Sysprep tool to generalize the image.</td>
</tr>
</tbody>
</table>

**Windows Server 2019**

<table>
<thead>
<tr>
<th>Release</th>
<th>Image ID</th>
<th>Release date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Windows Server 2019 Datacenter Edition</strong></td>
<td>• Chinese Edition: win2019_64_dtc_1809_zh-cn_40G_alibase_20191012.vhd</td>
<td>October 12, 2019</td>
<td>Updated to include the latest security patches</td>
</tr>
<tr>
<td></td>
<td>• English Edition: win2019_64_dtc_1809_en-us_40G_alibase_20191012.vhd</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Release</td>
<td>Image ID</td>
<td>Release date</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>--------------------------------------------------------------------------</td>
<td>--------------</td>
<td>-----------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Windows Server 2019 Datacenter Edition</td>
<td>- Chinese Edition: <code>win2019_64_dtc_1809_zh-cn_40G_alibase_20190816.vhd</code></td>
<td>August 16, 2019</td>
<td>Updated to include the latest operating system patches</td>
</tr>
<tr>
<td>Windows Server 2019 Datacenter Edition</td>
<td>- Chinese Edition: <code>win2019_64_dtc_1809_zh-cn_40G_alibase_20190718.vhd</code></td>
<td>July 18, 2019</td>
<td>Updated to include the latest operating system patches</td>
</tr>
<tr>
<td></td>
<td>- English Edition: <code>win2019_64_dtc_1809_en-us_40G_alibase_20190718.vhd</code></td>
<td></td>
<td>Upgraded .NET Framework to version 4.8</td>
</tr>
<tr>
<td></td>
<td>- English Edition: <code>win2019_64_dtc_1809_en-us_40G_alibase_20190528.vhd</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- English Edition: <code>win2019_64_dtc_1809_en-us_40G_alibase_20190318.vhd</code></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Windows Server Version 1809

<table>
<thead>
<tr>
<th>Release</th>
<th>Image ID</th>
<th>Release date</th>
<th>Description</th>
</tr>
</thead>
</table>
• English Edition: win2019_64_dtc_1809_en-us_40G_alibase_20190\_528.vhd | May 28, 2019 | Updated to include the latest operating system patches. |
|                              | • Chinese Edition: winsvr_64_dtcC_1809_zh-cn_40G_alibase_20190\_318.vhd  
• English Edition: winsvr_64_dtcC_1809_en-us_40G_alibase_20190\_318.vhd | March 18, 2019 | Updated to include the latest operating system patches. |
|                              | • Chinese Edition: winsvr_64_dtcC_1809_zh-cn_40G_alibase_20181\_222.vhd  
• English Edition: winsvr_64_dtcC_1809_en-us_40G_alibase_20181\_222.vhd | December 22, 2018 | • Updated to include the latest patch KB4483235.  
• By default, the image is generalized by the Sysprep tool. |
### Windows Server Version 1903

<table>
<thead>
<tr>
<th>Release</th>
<th>Image ID</th>
<th>Release date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Server Version 1903 Datacenter Edition</td>
<td>Chinese Edition: <code>winsvr_64_dtcC_1903_zh-cn_40G_alibase_20190718.vhd</code> English Edition: <code>winsvr_64_dtcC_1903_en-us_40G_alibase_20190718.vhd</code></td>
<td>July 18, 2019</td>
<td>• Updated to include the latest operating system patches • Upgraded .NET Framework to version 4.8</td>
</tr>
</tbody>
</table>

### 4.3 Known issues

This topic describes known issues of Alibaba Cloud images on different platforms, the scope of these issues, and their corresponding solutions.

**Debian 9.6: Classic network configuration**

The following section describes the issue details, involved images, and solution.

- Problem description: Classic network-type instances created from Debian 9 public images cannot be pinged.
• Cause: Instances in classic networks cannot automatically obtain IP addresses through the Dynamic Host Configuration Protocol (DHCP) because Debian 9 disables the systemd-networkd service by default.
• Image: debian_9_06_64_20G_alibase_20181212.vhd
• Solution: Run the following commands:

```bash
systemctl enable systemd-networkd
systemctl start systemd-networkd
```

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

The following section describes the issue details, involved images, and solution.

• Problem description: An instance that is running CentOS 6.8 and has an installed NFS client fails to respond and must be restarted.
• Cause: When you use the NFS service, the NFS client attempts 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. Normally, a connection expires and closes one 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 is unable to recover the TCP connection, and a new TCP connection cannot be initiated.
• 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 upgrade the kernel to versions 2.6.32-696.11 or later.

⚠️ Notice:
Before you perform any operations on the instance, you must #unique_33 to back up your data.

CentOS 7: The hostname changes from uppercase to lowercase letters after the instance is restarted

The following section describes the issue details, involved images, and solution.
Problem description: After 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.

<table>
<thead>
<tr>
<th>Hostname</th>
<th>Hostname after the instance is restarted for the first time</th>
<th>Does the hostname remain in lowercase after the restart?</th>
</tr>
</thead>
<tbody>
<tr>
<td>iZm5e1qe****sxx1ps5zx</td>
<td>izm5e1qe****sxx1ps5zx</td>
<td>Yes</td>
</tr>
<tr>
<td>ZZHost</td>
<td>zzhost</td>
<td>Yes</td>
</tr>
<tr>
<td>NetworkNode</td>
<td>networknode</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Images: The following CentOS public images and custom images created from these public images are affected:

- 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_02_64_20G_alibase_20170818.vhd
- centos_7_03_64_20G_alibase_20170818.vhd
- centos_7_04_64_20G_alibase_20170105.vhd

Hostname: If the hostnames of your applications are case-sensitive, restarting such instances may affect the availability of corresponding services. The
The following table describes whether the hostname will change after an instance is restarted.

<table>
<thead>
<tr>
<th>Current state of hostname</th>
<th>Will the hostname change after an instance restart?</th>
<th>When will the change take effect?</th>
<th>Continue reading this section?</th>
</tr>
</thead>
<tbody>
<tr>
<td>The hostname contains uppercase letters at the time of instance creation</td>
<td>Yes</td>
<td>When the instance is restarted for the first time.</td>
<td>Yes</td>
</tr>
<tr>
<td>(either in the ECS console or through ECS API operations).</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The hostname contains no uppercase letters at the time of instance creation</td>
<td>No</td>
<td>N/A</td>
<td>No</td>
</tr>
<tr>
<td>(either in the ECS console or through ECS API operations).</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>You log on to the instance and modify its hostname so that the hostname contains uppercase letters.</td>
<td>No</td>
<td>N/A</td>
<td>Yes</td>
</tr>
</tbody>
</table>

- **Solution:** To retain uppercase letters in a hostname after you restart an instance, follow these steps:

1. Connect to the instance. For more information, see #unique_34.
2. View the existing hostname.

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

3. Run the following command to staticize the hostname.

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

4. 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 image. For more information, see Install cloud-init and Create a custom image by using an instance.
Linux: Pip requests time out

The following section describes the issue details, involved images, and solution.

- Problem description: Pip requests occasionally time out or fail.
- Images: CentOS, Debian, Ubuntu, SUSE, openSUSE, and Aliyun 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 has no public IP address assigned, a pip request will time out.
  - (Default) Public network: mirrors.aliyun.com
  - VPCs: mirrors.cloud.aliyuncs.com
  - Classic networks: mirrors.aliyuncs.com
Solution: You can solve the problem through one of the following methods:

- **Method 1**
  
  Assign a public IP address to your instance by associating an Elastic IP Address (EIP) with your instance. For more information, see #unique_35.

  A subscription instance can also be reassigned a public IP address by changing its specifications. For more information, see #unique_36.

- **Method 2**
  
  If a pip request fails, you can run the `fix_pypi.sh` script in your ECS instance and retry the pip operation. The procedure is as follows:

  1. Connect to the instance. For more information, see #unique_37.
  2. Run the following command to obtain the script file.

    ```bash
    ```

  3. Run the script based on the network type of your instance.

    - **For instances in VPCs**, run the `bash fix_pypi.sh "mirrors.cloud.aliyuncs.com"` command.

    - **For instances in classic networks**, run the `bash fix_pypi.sh "mirrors.aliyuncs.com"` command.

  4. Retry the pip operation.

The content of `fix_pypi.sh` is as follows:

```bash
#!/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://$pypi_source/pypi/simple/
    EOF
```
```
trusted-host=$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
}
```

Aliyun Linux 2: Enabling the CONFIG_PARAVIRT_SPINLOCK kernel feature causes performance issues

The following section describes the issue details, involved images, and solution.

- **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, timed-out connections deteriorate the performance of an NGINX application.
- **Image:** Aliyun Linux 2
- **Solution:** We recommend that you keep the `CONFIG_PARAVIRT_SPINLOCK` kernel feature disabled for Aliyun 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.

Aliyun Linux 2: Setting the THP switch to always affects system stability and causes performance issues

The following section describes the issue details, involved images, and solution.

- **Problem description:** After you set the Transparent Hugepage (THP) switch in your production environment to **always**, the system becomes unstable and performance is deteriorated.
- **Image:** Aliyun Linux 2
- **Solution:** Set the THP switch to `madvise`. In scenarios such as when running performance benchmark testing by using test suites, system performance is deteriorated if this switch is set to `madvise` compared with `always`. However, these testing results might not be reliable or match real-world conditions. Therefore, we recommend that you retain the `madvise` setting to prevent the system from being affected by other contentions.
Aliyun Linux 2: A delegation conflict occurred in NFS V4.0

The following section describes the issue details, involved images, and solution.

- **Problem description:** A delegation conflict occurred in NFS V4.0. For more information, see *Delegation in NFS Version 4*.
- **Image:** Aliyun Linux 2
- **Solution:** We recommend that you do not enable the Delegation feature when you use NFS V4.0. For information about how to disable this feature at the server side, see *How to Select Different Versions of NFS on a Server*.

Aliyun Linux 2: NFS V4.1 or V4.2 has a defect that can prevent applications from logging out

The following section describes the issue details, involved images, and solution.

- **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.
- **Image:** Aliyun Linux 2
- **Solution:** This problem has been 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:

- Upgrading the kernel may result in system boot failure. Exercise caution when performing this action.
- Before you upgrade the kernel, make sure you have created a snapshot or custom image to back up data. For more information, see *Create a custom image by using an instance*.

Aliyun Linux 2: System performance is affected when important security vulnerabilities such as Spectre or Meltdown are fixed

The following section describes the issue details, involved images, and solution.

- **Problem description:** In the kernel of Aliyun Linux 2, the repair of important security vulnerabilities such as Meltdown or Spectre in processors is enabled
by default, which affects system performance. As a result, performance may be
deteriorated during performance benchmark testing.

- **Image:** Aliyun Linux 2

- **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 in normal circumstances you do not disable the repair function. However, if you need to maximize system performance, you can run the following commands to disable the repair function:

1. Run the following commands to add nopti nospectre_v2 to the kernel startup parameters.

   ```bash
   sudo sed -i 's/(GRUB_CMDLINE_LINUX=).*"/\1 nopti nospectre_v2 "/ /etc/default/grub
   
   sudo grub2-mkconfig -o /boot/grub2/grub.cfg
   ``

2. Run the following command to restart the system.

   ```bash
   sudo reboot
   ```
5 Aliyun Linux 2

5.1 Overview of Aliyun Linux 2

Aliyun Linux 2 is a next-generation operating system developed by Alibaba Cloud. It provides a safe, stable, and high-performance customized running environment for applications on ECS instances. Aliyun Linux 2 is a Linux distribution that is deeply optimized for cloud infrastructure to offer unparalleled runtime experience. You can create an instance by using the Aliyun Linux 2 public image for free, and obtain long-term technical support for the operating system from Alibaba Cloud.

For more information, visit the Aliyun Linux 2 product page.

Scenarios

Aliyun 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 #unique_39.
  - Aliyun Linux 2 supports instance types that have 1 to 160 vCPUs.
  - Aliyun Linux 2 supports instance types that have memory of 0.5 GiB to 3,840 GiB.
  - Aliyun Linux 2 does not support non-I/O optimized instances.

Benefits

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

- It is optimized for ECS instances, and features faster system startup and better runtime performance.
- It provides the latest enhanced features of the Linux community to power cloud-based application environments.
- It features an updated Linux kernel, user mode packages, and toolkits that provide additional features to the operating system.
· It has streamlined the kernel and reduced potential security risks.
· It is free to use and is provided with Alibaba Cloud technical support.

Features

· Aliyun Linux 2 is distributed with the latest version of the Alibaba Cloud kernel. The kernel provides the following features:
  - Customization based on the V4.19 kernel that has been supported by the kernel community, more new features for cloud scenarios, improved performance, and bug fixes.
  - Customized and optimized kernel startup parameters and system configuration parameters for the ECS instance environment.
  - kdump. You can enable or disable this feature without the need to restart the operating system.
  - Kernel Live Patching (KLP).

· Pre-installed software and updates:
  - Aliyun Linux 2 is pre-installed with Alibaba Cloud CLI.
  - The network module is changed from network.service to systemd-networkd.
  - The user-mode package keeps compatible with the latest CentOS 7 and can run on Aliyun Linux 2.
  - Fixes for Common Vulnerabilities and Exposures (CVE) are continuously updated until the end of life (EOL) of Aliyun Linux 2. For information about the release notes of Aliyun Linux 2, see Release notes of CVE.

· Aliyun Linux 2 speeds up the boot process and improves system performance at runtime in the following ways:
  - It has an optimized startup speed to better fit in with ECS instance environments.
  - It is optimized for multi-threaded scenarios in ECS instance environments and delivers improved multi-threaded performance for high-specification instances.
  - It is optimized holistically to better fit in with MySQL database scenarios and can be used in combination with enhanced SSDs to deliver significantly improved performance.
Billing

Aliyun Linux 2 images are provided for free. However, you must pay for other resources such as vCPUs, memory, storage, public bandwidth, and snapshots. For more information, see #unique_4.

Obtain Aliyun Linux 2

You can use the following methods to obtain Aliyun Linux 2:

- **ECS instances**
  - When creating an ECS instance, select Public Image and then select Aliyun Linux and its version. For more information, see #unique_22.
  - Replace the operating system of an existing ECS instance to Aliyun Linux 2 by replacing the instance system disk. For more information, see #unique_14.

- **On-premises environment such as a KVM-based virtualization environment**
  Download the Aliyun Linux 2 VM image, install the image, and start the system. For more information, see *Use the Aliyun Linux 2 image in an on-premises environment*.

Use Aliyun Linux 2

- **View or modify system parameters**

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

<table>
<thead>
<tr>
<th>System parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>kernel.hung_task_timeout_secs = 240</code></td>
<td>Increases the kernel hung_task timeout seconds to avoid frequent hung_task prompts.</td>
</tr>
<tr>
<td><code>kernel.panic_on_oops = 1</code></td>
<td>Throws the kernel panic exception when the kernel is experiencing an Oops error. Crash details are automatically captured if kdump is configured.</td>
</tr>
<tr>
<td><code>kernel.watchdog_thresh = 50</code></td>
<td>Increases the thresholds for events such as hrtimer, NMI, soft lockup, and hard lockup to avoid possible kernel false positives.</td>
</tr>
<tr>
<td><code>kernel.hardlockup_panic = 1</code></td>
<td>Throws the kernel panic exception when the kernel is experiencing a hard lockup error. Crash details are automatically captured if kdump is configured.</td>
</tr>
</tbody>
</table>
· View kernel parameters

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

<table>
<thead>
<tr>
<th>Kernel parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crashkernel=0M-2G:0M, 2G-8G:192M, 8G-:256M</td>
<td>Reserves memory space for the kdump feature.</td>
</tr>
<tr>
<td>cryptomgr.notests</td>
<td>Disables crypto self-check during kernel startup to speed up startup.</td>
</tr>
<tr>
<td>cgroup.memory=nokmem</td>
<td>Disables the kernel memory statistics function of memory cgroup to avoid potential kernel instability.</td>
</tr>
<tr>
<td>rcupdate.rcu_cpu_stall_timeout=300</td>
<td>Increases the timeout threshold of RCU CPU Stall Detector to 300 seconds to avoid kernel false positives.</td>
</tr>
</tbody>
</table>

· Roll back the kernel version

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

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

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

```bash
# 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 }')"
# Update the changes into the configuration file.
sudo grub2-mkconfig -o /boot/grub2/grub.cfg
# Restart the operating system for the new configurations to take effect.
```
Elastic Compute Service

Images / 5 Aliyun Linux 2

- Enable or disable kdump

Aliyun 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:

```
# Change 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 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, Aliyun 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` with the name of the target software package in the following command:
```
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` with the name of the target software package in the following command:
sudo yumdownloader --source <sourcePackageName>
```

- Use experimental software packages

Experimental software packages are provided by Alibaba Cloud, but are not rigorously tested. Alibaba Cloud does not guarantee the quality of these packages. Aliyun 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 `packageName` with the name of the target software package in the following command:
sudo yum install -y <packageName>
  ```

- Developments kits that support SCL plug-ins

  - The developments kit based on GCC-7.3.1 (devtoolset-7)
  - The development kit based on GCC-8.2.1 (devtoolset-8)
  - The development kit 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 packages that you need from the YUM repositories. The following sample commands also install all development kits supported by the SCL plug-ins.
  ```
```bash
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 complete, you can use the later version of GCC and related tools. The sample code is as follows:

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

Change history

- For the information about release notes of Aliyun Linux 2 images, see [Release notes of Aliyun Linux 2](#).
- For the information about updates of Aliyun Linux 2 CVE, see [Release notes of CVE](#).

Technical support

- Alibaba Cloud provides the following technical support for Aliyun Linux 2:
  - Long-term supports up to 5 years such as security updates and vulnerability fixes are provided until the version lifecycle ends on March 31, 2024. You can obtain free technical support in the following ways:
    - submit a ticket.
    - GitHub
  - Images are updated every four months. Updates include new features, security updates, and vulnerability fixes.
  - Security updates are provided from YUM repositories. You can run the `yum update` command to update to the latest version.
5.2 Release notes of Aliyun Linux 2

This topic describes the feature updates of Aliyun Linux 2 images in the order of their release time. Unless otherwise stated, the released updates apply to all Alibaba Cloud regions where Elastic Compute Service (ECS) is provided.
<table>
<thead>
<tr>
<th>Image ID</th>
<th>Release date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aliyun_2_1</td>
<td>March 24, 2020</td>
<td>• Images are updated to the latest software versions to be compatible with CentOS 7.7. Common Vulnerabilities and Exposures (CVEs) are fixed.</td>
</tr>
<tr>
<td>903_x64_20</td>
<td></td>
<td>• The latest fixes for CVEs can be obtained through yum. /etc/alinux-release is updated to Aliyun Linux release 2.1903 LTS (Hunting Beagle).</td>
</tr>
<tr>
<td>G_alibase_</td>
<td></td>
<td>• The tuned service is enabled by default. Kernel changes: - The kernel is updated to the kernel-4.19.91-18.al7 version. The NVMe driver is enabled.</td>
</tr>
<tr>
<td>20200324.vhd</td>
<td></td>
<td>- THP support is enabled by default. - The io_uring interface is supported. - The Hygon CPU support is added. - The intel_idle driver is enabled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- guest halt polling is enabled. - ftrace syscalls is enabled. - Multiple Alibaba Cloud optimizations and bug fixes to the kernel including subsystems such as schedulers, memory, file systems, and block layers are open sourced.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Kernel security vulnerabilities are fixed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Applicable regions: China (Zhangjiako-Beijing Winter Olympics), China (Hohhot), China (Heyuan), and China (Chengdu).</td>
</tr>
<tr>
<td>Image ID</td>
<td>Release date</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>aliyun_2_1903_x64_20G_alibase_20200221.vhd</td>
<td>February 21, 2020</td>
<td>• Images are updated to the latest software versions to be compatible with CentOS 7.7.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• IPv6 is enabled by default.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Kernel changes:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- The kernel is updated to the kernel 4.19.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Intel Cooper Lake CPU and Ice Lake CPU are supported.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- The support for the AMD and ARM 64-bit CPU architectures is enhanced.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Persistent memory is supported.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- The blk-iocost feature is provided.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- The Pressure Stall Information (PSI) feature is supported for the cgroup v1 interface. For more information, see Enable the PSI feature for the cgroup v1 interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Multiple Alibaba Cloud optimizations and bug fixes to the kernel including subsystems such as</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Kernel security vulnerabilities are fixed.</td>
</tr>
</tbody>
</table>


<table>
<thead>
<tr>
<th>Image ID</th>
<th>Release date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aliyun_2_1903_x64_20G_alibase_20200114.qboot.vhd</td>
<td>January 14, 2020</td>
<td>• Images are updated to the latest software version.&lt;br&gt;• Kernel changes:&lt;br&gt;  - The kernel is updated to the 4.19.81-17 al7 x86_64 version.&lt;br&gt;  - Quick boot with qboot is supported.</td>
</tr>
<tr>
<td>Image ID</td>
<td>Release date</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>aliyun_2_1</td>
<td>August 29, 2019</td>
<td>- Images are updated to the latest software version.</td>
</tr>
<tr>
<td>903_64_20G</td>
<td></td>
<td>- Kernel changes:</td>
</tr>
<tr>
<td>_alibase_2</td>
<td></td>
<td>- The kernel is updated to the kernel version.</td>
</tr>
<tr>
<td>0190829.vhd</td>
<td></td>
<td>- The Spectre-V1 SWAPGS vulnerability is fixed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Issues with bio-splitting code are fixed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- The default TCP congestion control algorithm is set to CUBIC.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- The network is configured to 10-eth0. network.</td>
</tr>
<tr>
<td>Image ID</td>
<td>Release date</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>--------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| aliyun_2_1 903_64_20G _alibase_2 0190619.vhd | June 19, 2019 | - Images are updated to the latest software version.  
- Kernel changes:  
  - The kernel is updated to the kernel version.  
  - The cgroup writeback feature is supported for the cgroup v1 interface.  
  - The policy-based routing is supported.  
  - The ss command from the iproute2 suite is supported by enabling the INET_DIAG kernel configuration.  
  - The configurable net.ipv4.tcp_tw_reuse kernel interface is supported.  
- The following network-related CVEs are fixed:  
  - CVE-2019-11477.  
<table>
<thead>
<tr>
<th>Image ID</th>
<th>Release date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aliyun-2.1903-x64-20G-alibase-20190507.vhd</td>
<td>May 7, 2019</td>
<td>• Images are updated to the latest software version.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The time synchronization delay that was present on instance startup is fixed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The kernel is updated to kernel-4.19.34-11.al7.</td>
</tr>
</tbody>
</table>
5.3 Known issues about Aliyun Linux 2

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

Enabling the CONFIG_PARAVIRT_SPINLOCK kernel feature causes performance issues

- **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, timed-out connections deteriorate the performance of an NGINX application.
• Solution: The CONFIG_PARAVIRT_SPINLOCK kernel feature for Aliyun Linux 2 is disabled by default. And if you are not sure how to resolve the kernel problem, we recommend that you do not enable the CONFIG_PARAVIRT_SPINLOCK feature.

Setting the THP switch of kernel features to always causes affect system stability and performance issues

• Problem description: After you set the Transparent Hugepage (THP) switch in your production environment to always, the system becomes unstable and performance is deteriorated.

• Solution: Set the THP switch to madvise. In scenarios such as running performance benchmark testing by using test suites, system performance is deteriorated if this switch is set to madvise compared with always. However, these testing results might not be reliable or match real-world conditions. Therefore, we recommend that you retain the madvise setting to prevent the system from being affected by other contentions.

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 do not enable the Delegation feature when you use NFS V4.0. For information about how to disable this feature at the server side, see How to Select Different Versions of NFS on a Server.

Defects in NFS V4.1 or V4.2 cause applications not to exit

• 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 descriptor s 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:
- Upgrading the kernel may result in system boot failure. Exercise caution when you perform this action.
- Before you upgrade the kernel, make sure you have created a snapshot or a custom image to back up data. For more information, see #unique_33 or Create a custom image by using an instance.

Fixing security vulnerabilities such as Meltdown and Spectre affects system performance

- Problem description: In the kernel of Aliyun Linux 2, the repair of important security vulnerabilities such as Meltdown or Spectre in processors is enabled by default, which affects system performance. As a result, performance may be deteriorated during performance benchmark testing.
- Solution: Meltdown and Spectre are two critical vulnerabilities in Intel chips. These vulnerabilities allow attackers to steal sensitive application data from the system memory. We recommend that you do not disable the repair function. However, if you need to maximize system performance, you can run the following commands to disable the repair function:

1. Run the following commands to add nopti nospectre_v2 to the kernel startup parameters.

```
sudo sed -i 's/\(GRUB_CMDLINE_LINUX=".*\)"/\1 nopti nospectre_v2"/' /etc/default/grub
```
```
sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

2. Run the following command to restart the system.

```
sudo reboot
```

5.4 Features and interfaces supported by Aliyun Linux 2

5.4.1 Use the Aliyun Linux 2 image in an on-premises environment

Aliyun Linux 2 provides a local image in the qcow2 format with built-in cloud-init. This topic describes how to use the Aliyun Linux 2 image in an on-premises environment.
The Aliyun Linux 2 image can run only on Kernel-based Virtual Machines (KVMs). The Aliyun Linux 2 image cannot start KVMs directly. You must configure a boot image. In this topic, the local operating system is Linux. Aliyun 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).

Then the NoCloud data source is used to create local configuration files. After the configuration files have been 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 Aliyun Linux 2 image to your local computer

Download the Aliyun Linux 2 image at Aliyun Linux 2 image to your local machine.

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 do so.

Notice:

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

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

• Download the image files of seed.img prepared by Aliyun Linux 2 from seed.img. You cannot change the configuration information in the boot image. Therefore, the 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. The procedure is as follows:

In the same local directory, create two configuration files meta-data and user-data.

a) Create a directory named seed and go to the directory.
b) Create the **meta-data** configuration file.

An example of the file content is as follows. You can change the configuration as needed.

```yaml
#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
```

c) Create the **user-data** configuration file.

An example of the file content is as follows. You can change the configuration as needed.

```yaml
#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 Aliyun 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
  updates:
    baseurl: https://mirrors.aliyun.com/alinux/$releasever/updates/$basearch/
    enabled: true
    gpgcheck: true
    gpgkey: https://mirrors.aliyun.com/alinux/RPM-GPG-KEY-ALIYUN
  extras:
    baseurl: https://mirrors.aliyun.com/alinux/$releasever/extras/$basearch/
    enabled: true
```

```
gpgcheck: true

gpgkey: https://mirrors.aliyun.com/alinux/RPM-GPG-KEY-

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-

name: Aliyun Linux - $releasever - Plus - mirrors.aliyun.
.com

# Using cloud-init or systemd-networkd may cause configurations in
metadata to fail. 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

d) Install the cloud-utils software package on your local computer.

    yum install -y cloud-utils

e) 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.

  1. 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 change the configuration file of the XML format as needed.

    <domain type='kvm'>
2. Run the `virsh` command to start the KVM. The sample command is as follows:

```bash
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 parameters to the command line. Change the `file` parameter to the actual absolute path of the seed.img image.

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

For more information about the `libvirt` and `qemu-kvm` commands, click `Installing Virtualization Packages Manually`. 
• Use the graphical interface (virt-manager) to start the KVM. Before you start the
KVM, you must 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.

5.4.2 Enable the cgroup writeback feature

Aliyun 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.

   ```bash
   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.**

   ```bash
   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.

  1. Enable the ftrace tool.
  ```
sudo bash -c "echo 1 > /sys/kernel/debug/tracing/events/writeback/insert_memcg_blkcg_link/enable"
  
  2. 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
```

5.4.3 Configure the weight-based throttling feature of blk-iocost

Aliyun Linux 2 provides the weight-based throttling feature (blk-iocost) based on the cost model since the kernel version 4.19.81-17.al7.x86_64. 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 Aliyun Linux 2. This topic describes the interfaces that implement throttling.
## Interface description

<table>
<thead>
<tr>
<th>Interface</th>
<th>Description</th>
<th>Configuration item</th>
</tr>
</thead>
</table>
| cost.qos    | A read/write interface whose file is only stored 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 to all requests. When the proportion is greater than rlat|wlat, the kernel considers the device 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 rlat|wlat feature is disabled. Each line of configuration in the interface file starts with the Major and Minor numbers of the device in the MAJ:MIN format, followed by other configuration items. The following describes configuration items:  
· enable: specifies whether to enable the blk-iocost controller, that is, whether 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 device type and uses built-in parameters. When the control mode is set to user, you must specify the following QoS control parameters.  
· rpct: read latency percentile. Valid values: 0 to 100.  
· rlat: read latency threshold. Unit: microseconds.  
· wpct: write latency percentile. Valid values: [0,100].  
· wlat: write latency threshold. Unit: microseconds.  
· min: minimum scaling percentage. Valid values: 1 to 10000.  
· max: maximum scaling percentage. Valid values: 1 to 10000. |
<table>
<thead>
<tr>
<th>Interface</th>
<th>Description</th>
<th>Configuration item</th>
</tr>
</thead>
</table>
| cost.model  | A read/write interface whose file is only stored 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 device in the MAJ:MIN format, followed by other configuration items. The following describes configuration items:  
  · ctrl: the control mode. Specifies whether to enter model parameters by the user. 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. |
<table>
<thead>
<tr>
<th>Interface</th>
<th>Description</th>
<th>Configuration item</th>
</tr>
</thead>
</table>
| cost.weight | A read/write interface whose file is only stored 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 device 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 device MAJ:MIN is changed.                                                                 |

Precautions

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

```bash
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` device. If over 95% of requests have a latency (rlat|wlat) of over 5 milliseconds, the disk is considered saturated. The kernel will adjust the speed of the disk to send requests at a speed between 50% and 150% of the original speed. The commands for the cgroup v1 and cgroup v2 interfaces are as follows:
• The command for cgroup v1:

```bash
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:

```bash
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 device 254:48 based on the linear modeling parameters. The commands for the cgroup v1 and cgroup v2 interfaces are as follows:

• The command for cgroup v1:

```bash
echo "254:48 ctrl=user model=linear rbps=2706339840 rseqiops=89698
rrandiops=110036 wbps=1063126016 wseqiops=135560 wrandiops=130734"
> /sys/fs/cgroup/blkio/blkio.cost.model
```

• The command for cgroup v2:

```bash
echo "254:48 ctrl=user model=linear rbps=2706339840 rseqiops=89698
rrandiops=110036 wbps=1063126016 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 device 254:48 to 50. The commands for the cgroup v1 and cgroup v2 interfaces are as follows:

• The command for cgroup v1:

```bash
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 device to 50.
```

• The command for cgroup v2:

```bash
echo "50" > /sys/fs/cgroup/cg1/io.cost.weight    # Change the default weight 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, see [drgan](#). The script is used as follows:

  Run the following command to monitor the I/O performance data of the `vdd` disk.

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

  A sample response is as follows:

  ```plaintext
  vdd RUN  per=500.0ms cur_per=3930.839:v14620.321 busy= +1 vrate=6136 .22% params=hdd
  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 under cgroup v1**

  The Aliyun Linux 2 kernel provides the blk-iocost statistics interface under the cgroup v1 interface. The interface file of the statistics interface records the QoS
data of each controlled device. Run the following command to view the interface document:

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

A sample response is as follows:

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

- **ftrace monitoring tool**

  The Aliyun Linux 2 kernel provides the ftrace tool related to blk-iocost for kernel-side analytics. The ftrace monitoring tool is used as follows:

  1. Set the `enable` property to 1 to enable the ftrace tool.

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

  2. View the output information.

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

A sample response is as follows:

```
<idle>-0 [008] d... 688.565349: iocost_iocg_activate: [vdd ...
```

5.4.4 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. Aliyun 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 Aliyun Linux 2. For information about how to download the Debuginfo package and source code package, see Use Aliyun 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 Aliyun 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
```

5.4.5 Change the timeout period of TCP TIME-WAIT

In the Linux kernel, the TIME-WAIT state of TCP/IP lasts for 60 seconds and the period cannot be changed. However, in some scenarios such as when the TCP load is heavy, being able to shorten this period will greatly improve network performance. Therefore, Aliyun Linux 2 has added a kernel interface to the kernel version 4.19.43-13. al7 to change the timeout period of TCP TIME-WAIT. This topic describes how to use the kernel interface.

Context

By default, the TCP/IP stack keeps the socket open for 60 seconds after an application sends a request to close the socket. This state is the TCP/IP TIME-WAIT state and ensures that data transmission between the server and the client is complete. However, if too many connections are in the TIME-WAIT state, network performance can be compromised. Therefore, Aliyun Linux 2 provides an
interface that can change the timeout period of TIME-WAIT and improve network performance in scenarios such as high-concurrency business. The value range of the interface is 1 to 600 seconds. The default value of the timeout period of TIME-WAIT is 60 seconds.

Precautions

Setting a timeout period less than 60 seconds contradicts the quiet time concept of TCP/IP and may result in the system receiving old data as new data or rejecting copied new data as old data. Make adjustments based on the advice of network technicians of Alibaba Cloud. For information about the quiet time of TCP/IP, see IETF RFC 793.

Configuration methods

You can use one of the following methods to change the timeout period of TIME-WAIT. Specify the \([$TIME\_VALUE]\) parameter to set a new timeout period for TIME-WAIT.

- Run the \texttt{sysctl} command to change the timeout period of TIME-WAIT:
  \[
  \texttt{sysctl \textemdash w "net.ipv4.tcp_tw_timeout=[$TIME\_VALUE"]}
  \]
- Run the \texttt{echo} command as the root user and change the timeout period in the \texttt{/proc/sys/net/ipv4/tcp_tw_timeout} interface.
  \[
  \texttt{echo \[$TIME\_VALUE]\ > /proc/sys/net/ipv4/tcp_tw_timeout}
  \]

5.4.6 Enhance the monitoring of block I/O throttling

To better monitor Linux block I/O throttling, Aliyun Linux 2 provides an interface in the kernel version 4.19.81-17.al7 to collect more statistics on block I/O throttling. This topic describes the new interface and how to use it.

Context

Linux block I/O throttling (bit/s or IOPS) is required in multiple scenarios, especially those where cgroup writeback is enabled. Aliyun Linux 2 provides an interface that enhances the monitoring of block I/O throttling to facilitate your operations.
# Interface description

<table>
<thead>
<tr>
<th>Interface</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>blkio.throttle.io_service_time</td>
<td>The duration of time from when I/O operations are issued from the block I/O throttling layer to when the operations are completed. Unit: ns.</td>
</tr>
<tr>
<td>blkio.throttle.io_wait_time</td>
<td>The duration of throttling at the block I/O throttling layer. Unit: ns.</td>
</tr>
<tr>
<td>blkio.throttle.io_completed</td>
<td>The number of completed I/O operations. The parameter is used to calculate the average latency of the block I/O throttling layer. Unit: counts.</td>
</tr>
<tr>
<td>blkio.throttle.total_io_queued</td>
<td>The number of I/O operations that were throttled in the history. 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. Unit: counts.</td>
</tr>
<tr>
<td>blkio.throttle.total_bytes_queued</td>
<td>The total bytes of I/O that were throttled in the history. Unit: bytes.</td>
</tr>
</tbody>
</table>

The path of the preceding parameters 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 between two points in time five seconds away from each other is monitored. Then the average I/O latency of the vdd disk is calculated. The following table describes relevant parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>write_wait_time&lt;N&gt;</td>
<td>Obtains the duration of throttling at the block I/O throttling layer.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>write_service_time&lt;N&gt;</td>
<td>Obtains the duration of time from when I/O operations are issued from the block I/O throttling layer to when the operations are completed.</td>
</tr>
<tr>
<td>write_completed&lt;N&gt;</td>
<td>Obtains the number of completed I/O operations.</td>
</tr>
</tbody>
</table>

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 for 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.

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`
```

5.4.7 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 that can affect system performance. To solve this problem, Aliyun Linux 2 optimizes JBD2. This topic describes the interfaces that optimize JBD2.

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 write access permissions from the cache, the cache page may be in the shadow state. Because of this, JBD2 may take an extended period of time waiting for the cache page to write back to the disk. To solve this problem, Aliyun Linux 2 adds the kernel interface force_copy to JBD2. The interface allows you to enable the optimization function. The system then copies cache pages, reducing the time that JBD2 has to wait for cache pages while in the shadow state to write back to the disk. In addition, to analyze the QoS issues related to the file system, Aliyun Linux 2 added the information statistics interface stats to JBD2.

### Interface description

<table>
<thead>
<tr>
<th>Interface</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>force_copy</td>
<td>The interface file is stored in <code>/proc/fs/jbd2/&lt;device&gt;-8/force_copy</code>, where the variable device indicates the name of the block storage device. Valid values: 1 and 0. After you enable the force_copy interface, the system will force copy data, which reduces the waiting time of JBD2. <strong>Notice:</strong> Running the interface will consume memory.</td>
</tr>
<tr>
<td>stats</td>
<td>The interface file is stored in <code>/proc/fs/jbd2/&lt;device&gt;-8/stats</code>. The interface helps to determine whether quality of service (QoS) issues in the file system are caused by JBD2.</td>
</tr>
</tbody>
</table>

### Examples

The examples of force_copy and stats interfaces are as follows:
- By default, the `force_copy` interface is disabled. You can set the value of the interface to 1 to call 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
```

A sample response is as follows:

```
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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>The first field</td>
<td>The ID of the event.</td>
</tr>
<tr>
<td>The second field</td>
<td>The number of events requested.</td>
</tr>
<tr>
<td>The third field</td>
<td>The maximum number of cached events.</td>
</tr>
<tr>
<td>The fourth field</td>
<td>The event wait time.</td>
</tr>
<tr>
<td>The fifth field</td>
<td>The latency of the event request.</td>
</tr>
<tr>
<td>The sixth field</td>
<td>The amount of time that the event ran.</td>
</tr>
<tr>
<td>The seventh field</td>
<td>The amount of time that the event was locked.</td>
</tr>
<tr>
<td>The eighth field</td>
<td>The amount of time that it took to refresh the event.</td>
</tr>
<tr>
<td>The ninth field</td>
<td>The amount of time that it took to log on to the event.</td>
</tr>
<tr>
<td>The tenth field</td>
<td>The average submission time.</td>
</tr>
<tr>
<td>The eleventh field</td>
<td>The number of handles contained in the event.</td>
</tr>
<tr>
<td>The twelfth field</td>
<td>The number of blocks contained in the event.</td>
</tr>
<tr>
<td>The thirteenth field</td>
<td>The number of blocks recorded for the event.</td>
</tr>
<tr>
<td>The fourteenth field</td>
<td>The time constant of the kernel configuration, in Hertz.</td>
</tr>
</tbody>
</table>
5.4.8 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. Aliyun 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 Aliyun Linux 2. For more information, see `Use Aliyun 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
```

### 5.4.9 Track I/O latency

Aliyun Linux 2 optimizes the `/proc/diskstats` interface, which is the raw data source of the I/O latency analysis tool `iostat`. Aliyun Linux 2 can calculate the duration of time in read, write and special I/O (discard) on the device. In addition, Aliyun 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 Aliyun 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 Aliyun Linux 2.

The following table describes the three domains:

<table>
<thead>
<tr>
<th>Domain</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>The sixteenth domain</td>
<td>The read duration on the device. Unit: milliseconds.</td>
</tr>
<tr>
<td>The seventeenth domain</td>
<td>The write duration on the device. Unit: milliseconds.</td>
</tr>
<tr>
<td>The eighteenth domain</td>
<td>The discard duration on the device. Unit: milliseconds.</td>
</tr>
</tbody>
</table>

**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 Aliyun Linux 2. For more information, see Use Aliyun Linux 2.

bcc

Aliyun 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:

```bash
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.

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

The description is as follows:

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

```
man bcc-alibiolatency
```

### 5.4.10 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, Aliyun Linux 2 extends the core data structure and provides the function to quickly locate and detect I/O hangs with low system overhead. This topic describes the interfaces for this function and the usage examples of these interfaces.

#### Interface description

<table>
<thead>
<tr>
<th>Interface</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>/sys/block/&lt;device&gt;/queue/hang_thres</code>&lt;br&gt;<code>hold</code></td>
<td>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 detecting I/O hangs.</td>
</tr>
<tr>
<td><code>/sys/block/&lt;device&gt;/hang</code></td>
<td>The interface can return the number of I/O operations that exceeds the threshold for I/O hangs on the device.</td>
</tr>
<tr>
<td><code>/sys/kernel/debug/block/&lt;device&gt;/rq_hang</code></td>
<td>The interface can query details about I/O hangs.</td>
</tr>
<tr>
<td><code>/proc/&lt;pid&gt;/wait_res</code></td>
<td>The interface can query the information about the resources that a process is waiting for.</td>
</tr>
<tr>
<td><code>/proc/&lt;pid&gt;/task/&lt;tid&gt;/wait_res</code></td>
<td>The interface can query the information about the resources that a thread is waiting for.</td>
</tr>
</tbody>
</table>

#### Variables in the interface.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;device&gt;</code></td>
<td>The name of the Block Storage device.</td>
</tr>
<tr>
<td><code>&lt;pid&gt;</code></td>
<td>The ID of the process.</td>
</tr>
<tr>
<td><code>&lt;tid&gt;</code></td>
<td>The ID of the thread.</td>
</tr>
</tbody>
</table>
Example 1

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

1. Change the detection threshold for the `vdb` disk to 10,000 ms.
   ```bash
echo 10000 > /sys/block/vdb/queue/hang_threshold
```

2. View the result of the detection threshold change.
   ```bash
cat /sys/block/vdb/queue/hang_threshold
```

A sample response is as follows:

```
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 query command is as follows:

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

A sample response is as follows:

```
0     1       # The value on the left indicates the number of read operations that have I/O hangs. The value 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 query command is as follows:

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

A sample response is as follows:

```
ffff9e50162fc600 {.op=WRITE, .cmd_flags=SYNC, .rq_flags=STARTED| ELVPRIV|IO_STAT|STATS, .state=in_flight, .tag=118, .internal_tag=67 , .start_time_ns=1260981417094, .io_start_time_ns=1260981436160, . current_time=1268458297417, .bio = ffff9e4907c31c00, .bio_pages = { ffffc8596086740 }, .bio = ffff9e4907c31500, .bio_pages = { ffffc8596
```
The preceding response shows the details of an I/O operation. The start time of the I/O request, `io_start_time_ns` 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 resources that a process is waiting for. In this example, the 577 process is used.

The query command is as follows:

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

A sample response is as follows:

```
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.
```

Response parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Field 1</td>
<td>The type of the resources for which the process is waiting. A value of 1 indicates pages in the file system. A value of 2 indicates the block I/O layer.</td>
</tr>
<tr>
<td>Field 2</td>
<td>The address of the resource (page or block I/O layer) for which the process is waiting.</td>
</tr>
<tr>
<td>Field 3</td>
<td>The time at which the process began waiting for resources.</td>
</tr>
<tr>
<td>Field 4</td>
<td>The current time when the file is read. The difference between Field 4 and Field 3 is the time consumed while waiting for the resource.</td>
</tr>
</tbody>
</table>

5.5 Knowledge base about Aliyun Linux 2

This topic provides the troubleshooting and solutions about Aliyun Linux 2 issues.

- How do I configure the Kdump file in a Aliyun Linux 2 system?
- There is a delay in system time synchronization after the ECS instance Aliyun Linux 2.1903 the image is started or restarted.

- You cannot run the yum command on Aliyun Linux 2 ECS instances of the classic network system.

- A segfault error occurs when the ECS instances of the Aliyun Linux 2 system are running Docker images of earlier versions.

- The route information cannot be queried or configured on the ECS instance of the Aliyun 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".

- Aliyun 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 Aliyun Linux 2 system.

- The Buffer I/O write performance of the Ext4 file system in the ECS instance of the Aliyun Linux 2 is not as expected.

- The Aliyun Linux 2 field value returned when the ECS instance of the Send-Q system runs the ss command is 0

### 5.6 FAQ about Aliyun Linux 2

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

- What are the differences between Aliyun Linux and Aliyun Linux 2?

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

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

- Which ECS instance types does Aliyun Linux 2 support?

- Does Aliyun Linux 2 support 32-bit applications or libraries?

- Does Aliyun Linux 2 provide a graphical user interface (GUI) desktop?

- Can I view the source code of Aliyun Linux 2 components?

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

- Can I use Aliyun Linux 2 on an on-premises environment?

- Which third-party applications can run on Aliyun Linux 2?

- What are the advantages of Aliyun Linux 2 compared with other Linux operating systems?

- How does Aliyun Linux 2 protect data security?
· Does Aliyun Linux 2 support data encryption?
· How do I grant permissions to manage Aliyun Linux 2?

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

Aliyun Linux 2 differs in the following aspects:

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

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

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

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

No, Aliyun 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 Aliyun Linux 2 support?

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

Note:
Aliyun Linux 2 does not support instances on the Xen virtual machine monitor.

Does Aliyun Linux 2 support 32-bit applications or libraries?

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

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

No. Aliyun Linux 2 does not provide a GUI desktop.

Can I view the source code of Aliyun Linux 2 components?

Yes. Aliyun 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 Aliyun Linux 2 backward-compatible with the current Aliyun Linux version?

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

Note:
You may need to re-compile a compiled kernel module on Aliyun Linux 2 before it can be used.

Can I use Aliyun Linux 2 on an on-premises environment?

Yes, you can use Aliyun Linux 2 on an on-premises environment. Aliyun 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 the Aliyun Linux 2 image in an on-premises environment.

Which third-party applications can run on Aliyun Linux 2?

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

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

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

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

- Updates are released at a faster pace. Updated Linux kernels, user-mode software, and toolkits are provided.
- Aliyun Linux 2 works out of the box and requires minimal configuration.
- Aliyun Linux 2 is optimized to work with the optimized hypervisor and maximizes performance for users.
- Unlike RHEL, Aliyun Linux 2 does not have any runtime charges. Different from CentOS, Alibaba Cloud provides commercial support for Aliyun Linux 2.

How does Aliyun Linux 2 protect data security?

Aliyun Linux 2 is binary compatible with CentOS 7.6.1810 and RHEL 7.6 and complies with the RHEL safety specifications. Aliyun 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 Aliyun Linux 2 support data encryption?

Yes. Aliyun 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 Aliyun Linux 2?

You can grant management permissions in Aliyun 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 Aliyun Linux 2.
6 Custom image

6.1 Create custom image

6.1.1 Create a custom image by using a snapshot

This topic describes how to create a custom image by using a snapshot. A custom image typically contains the operating system and data environment of an ECS instance that you can use to create multiple, identical ECS instances. You can also change the configurations of ECS instances created by a custom image as needed.

You can also use an instance to create an image. For more information, see Create a custom image by using an instance.

To enhance the security of custom images created from snapshots, see Security suggestions for Alibaba Cloud custom image.

Limits

Before you proceed, note the following:

- Custom images must be created from system disk snapshots (or system disk snapshots and 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.
- Custom images cannot be used across regions. However, you can copy custom images to the destination region for later use. For more information, see Copy custom images.
- Custom images are created independently from the billing methods of the instances from which they were created. For example, custom images created...
from Subscription instances can be used for creating Pay-As-You-Go instances. The converse method also applies.

- You can upgrade the instance created from a custom image, including upgrading the CPU, memory, bandwidth, and disks.
- You can change the operating system of an instance created from a custom image, and the custom image remains usable. For more information, see Change the system disk (custom image).
- If the ECS instance used for creating a custom image expires or is released, the custom image and the ECS instances created from the custom image are not affected. However, automatic snapshots are cleared when an ECS instance is released.

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 target instance and click its instance ID, or click Manage in the Actions column.
5. In the left-side navigation pane, click Instance Snapshots. Find a snapshot whose Disk Type is system disk and then click Create Custom Image in the Actions column.
6. In the Create Custom Image dialog box, complete the following:
   - Confirm the snapshot ID.
   - Enter a name and description of the custom image.
   - (Optional) Check Add Data Disk Snapshot, select multiple snapshots of data disks for the image, and click Add.

**Note:**

- If no data disk snapshot is selected (namely, no data disk snapshot ID is selected), an empty data disk is created with a default capacity of 5 GiB.
- If a data disk snapshot is selected, the disk size is the same as the snapshot size.
We recommend that you remove sensitive data from the data disk before creating a custom image to guarantee data security.

- (Optional) Attach tags to custom images for classification. For more information, see Tags.

You can also choose Storage & Snapshots > Snapshots, and select a snapshot whose Disk Type is System Disk to create a custom image.
What to do next

After you create a custom image, you can:

- Use it to create instances. For more information, see Create an instance by using a custom image.
- Use it to replace the system disk of an instance. For more information, see Replace a system disk (non-public image).

6.1.2 Create a custom image by using an instance

This topic describes how to create a custom image by using an instance. After creating an instance, you can customize the instance according to your service needs and create a custom image for it. New instances created from the custom image inherit all the customizations you have made for the original instance.

During custom image creation, snapshots are automatically created for all disks of the instance, including the system disk and data disks. All the created snapshots compose a new custom image. The following figure details this process.
The instance and the custom image that is created from this instance must belong to the same region. For example, if the instance is located in China East 1, the custom image must also be located in China East 1. If you need to use the image in another region, you must first copy the image to that region. For more information, see *Copy custom images*.

If your instance expired or is released, you can also use the system disk snapshots of the instance to create a custom image, and then use this image to create a new instance to retrieve data in the original instance. For more information, see *Create a custom image by using a snapshot*.

**Considerations**

- Make sure you have deleted all confidential data in the ECS instance before creating a custom image to guarantee data security.
- You can create a custom image without stopping the instance. During creation, do not change the status of the instance. Specifically, do not stop, start, or restart the instance.
- The time required for creating a custom image depends on the disk size of the instance.
- If your custom image contains snapshots of data disks, new data disks are created based on the snapshots. If you create a data disk along with an ECS instance, data on the new data disk duplicates the data disk snapshot according to the mount device.

**Precautions for Linux instances**

Before creating a custom image using a Linux instance, follow these instructions:

- Do not load data disk information to the `/etc/fstab` directory. Otherwise, instances created from the custom image cannot be started.
- We strongly recommended that you umount all the file systems mounted on the Linux instance before creating a custom image. Otherwise, instances created from the custom image may not be started or used.
- Do not upgrade the kernel or operating system unless other required.
- Do not adjust system disk partitions. Currently, the system disk supports only one root partition.
- Ensure that the system disk has available space.
• Do not modify key system files such as /sbin, /bin, and /lib.
• Do not modify the default login username root.

Procedure

1. Find the target instance.
2. In the Actions column, choose More > Disk and Image > Create Custom Image.
3. In the displayed dialog box, enter a name and description for the image.
4. Click Create.

The image is available after all snapshots of all disks have been created.

What to do next

Create an instance by using the custom image.

6.1.3 Use Packer to create a custom image

This topic provides information about how to install and use Packer to create a custom image.

Prerequisites

You must have an AccessKey.
Do not use the AccessKey of your Alibaba Cloud account. Instead, create a RAM user and use the RAM account to create the necessary AccessKey to maintain account security.

Step 1. Install Packer

Go to the official Packer download page where you can choose required version of Packer for your operating system.

To install Packer on a Linux server

1. Connect and log on to the Linux server. If the server you want to connect to is an ECS Linux instance, see connect to a Linux instance by using a password.
2. Run `cd /usr/local/bin` to go to the `/usr/local/bin` directory.

   **Note:**
   The `/usr/local/bin` directory is an environment variable directory. You can install Packer to this directory or another directory that has been added to the environment variable.

3. Run `wget https://releases.hashicorp.com/packer/1.1.1/packer_1.1.1_linux_amd64.zip` to download the Packer installer. You can visit the official download page of Packer to download installers for other versions of Packer.
4. Run `unzip packer_1.1.1_linux_amd64.zip` to unzip the package.
5. Run `packer -v` to verify Packer’s installation status. If the Packer version number is returned, you have successfully installed Packer. If error command not found is returned, Packer has not been correctly installed.

To install Packer on a Windows server

The following examples uses Windows Server 2012 64-bit:

1. Connect and log on to the Windows server. If the server you want to connect to is an ECS Windows instance, see connect to a Windows instance.
2. Open the official download page of Packer and select an appropriate Packer installer for 64-bit Windows.
3. Unzip the package to a specified directory and install Packer.
4. Define the directory for Packer in the PATH environment variable.
   a. Open the Control Panel.
   b. Select All Control Panel Items > System > Advanced System Settings.
   c. Click Environment Variable.
   d. Find Path in the system variable list.
   e. Add the Packer installation directory to the Variable Value, such as C:\Packer as seen in this example. Separate multiple directories with half-width semicolons (;). Click OK.

5. Run `packer.exe -v` in CMD to verify Packer’s installation status. If the Packer version number is returned, you have successfully installed Packer. If error command not found prompt is returned, Packer has not been correctly installed.

Step 2. Define a Packer template

**Note:**

To create a custom image by using Packer, you must first create a JSON format template file. In the template, you must specify the Alibaba Cloud Image Builder and Provisioner for the custom image to be created. Packer offers a diverse range of provisioners for you to choose from when configuring the content generation mode of the custom image. In the following JSON file example, the Shell provisioner is used as an example to illustrate how to define a Packer template.

Create a JSON file named `alicloud` and paste the following content:

```json
{
  "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"
    ]
  }]
}
```
Note:
Customize the values of the following parameters according to your actual requirements.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>access_key</td>
<td>Your AccessKey ID. For more details, see <a href="#">create an AccessKey</a>.</td>
</tr>
<tr>
<td>secret_key</td>
<td>Your AccessKey Secret. For more information, see <a href="#">create an AccessKey</a>.</td>
</tr>
<tr>
<td>region</td>
<td>The region of the temporary instance used to create the custom image.</td>
</tr>
<tr>
<td>image_name</td>
<td>The custom image’s name</td>
</tr>
<tr>
<td>source_image</td>
<td>The name of the basic image name retrieved from Alibaba Cloud public image list.</td>
</tr>
<tr>
<td>instance_type</td>
<td>Type of temporary instance generated to create the custom image.</td>
</tr>
<tr>
<td>internet_charge_type</td>
<td>The Internet bandwidth billing method for the temporary instance generated for creating the custom image.</td>
</tr>
<tr>
<td>provisioners</td>
<td>Type of Negot Provider used for creating the custom image</td>
</tr>
</tbody>
</table>

Step 3. Create a custom image by using Packer

To specify the Packer template file and create a custom image, follow these steps:

1. Run `export ALICLOUD_ACCESS_KEY=your AccessKeyID` to import your AccessKey ID.
2. Run `export ALICLOUD_SECRET_KEY=your AccessKeySecret` to import your AccessKey Secret.
3. Run `packer build alicloud.json` to create the custom image.
The following example creates a custom image containing ApsaraDB for Redis and runs as follows:

```
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 to do next

Use this custom image to create an ECS instance. For more information, see create an instance from a custom image.

References

- For more information, visit packer-provider, the Packer repository of Alibaba Cloud Github.
- See the Packer official documents to learn more about how to use Packer.

6.1.4 Create and import on-premises images by using Packer

Packer is a convenient open-source tool to create on-premises image files. It runs on the most major operating systems.

By using Packer, you can create identical on-premises images for multiple platforms from a single source configuration. This topic details steps to create an on-premises image for CentOS 6.9 on an Ubuntu 16.04 server and to upload it to Alibaba Cloud. For actual scenarios, you can customize your Packer templates as required.
Prerequisites

- You must have an AccessKey for the configuration file.

Note:
Do not use the AccessKey of your Alibaba Cloud account. Instead, create a RAM user and use the RAM account to create the necessary AccessKey to maintain account security.

- You must have purchased OSS.

Example of creating and importing an on-premises image

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

```
pat pse36 clflush dts acpi mmx fxsr sse sse2 ss ht tm pbe syscall nx pdpe1gb rdtscl pse36 clflush dts acpi mmx fxsr sse sse2 ss ht tm pbe syscall nx pdpe1gb rdtscl pmtdt 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 epb intel_pt tpr_shadow vnmi flexpriority ept vpid fsgsbase tsc_adjust bmi1 avx2 smep bmi2 erms invpcid mpx rdseed adx xsaveopt xsaves dtherm ida arat pln pts hwp hwp_notif 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 to install the KVM:

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

If a GUI runs in the VM console window, you have successfully installed the KVM.

3. Install Packer.

To install Packer, see use Packer to create a custom image.

4. Run the following commands to define a Packer template.

Note:
The on-premises image created in the following configuration is for the CentOS 6.9 operating system only. To create images for other operating systems, customize the configuration file centos.json as required.

```
 cd /user/local # Switch the directory.
```
wget https://raw.githubusercontent.com/alibaba/packer-provider/master/examples/alicloud/local/centos.json # Download file centos.json 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 file ks.cfg that is released by Alibaba Cloud.
mkdir -p http/centos-6.9 # Create a directory.
mv ks.cfg http/centos-6.9/ # Move file ks.cfg to the http/centos-6.9 directory.

5. Run the following commands to create an on-premises image.

export ALICLOUD_ACCESS_KEY= SpecifyYourAccessKeyIDHere # Import your AccessKeyID,
export ALICLOUD_SECRET_KEY= SpecifyYourAccessKeySecretHere # Import your AccessKeySecret.
packer build centos.json # Create an on-premises image.

An example result is as follows.

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, log on to the ECS console and check your custom image in the image list that is in the corresponding region. In this example, the region is cn-beijing, i.e. China (Beijing).

Customize a Packer template

In this example, the following JSON file is customized based on the template used to create an image for the 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": "af4axxxxxxxxxxxxxxxxx192a2",
  "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"
      }
    ]
  ]
}

Parameters in a Packer builder

QEMU builder is used in the preceding example to create a virtual machine image.

Required parameters for the builder are as follows.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>iso_checksum</td>
<td>String</td>
<td>The checksum for the OS ISO file. Packer verifies this parameter before starting a virtual machine with the ISO attached. Make sure you specify at least one of the iso_checksum or iso_checksum_url parameters. If you have specified the iso_checksum parameter, the iso_checksum_url parameter is automatically ignored.</td>
</tr>
<tr>
<td>iso_checksum_type</td>
<td>String</td>
<td>The type of the checksum specified in iso_checksum. Optional values:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• none: If you specify none for iso_checksum_type, the checksuming is ignored. This value is not recommended.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• md5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• sha1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• sha256</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• sha512</td>
</tr>
<tr>
<td>iso_checksum_url</td>
<td>String</td>
<td>A URL that points to a GNU or BSD style checksum file that contains the ISO file checksum of an operating system. It may come in either the GNU or BSD pattern. Make sure you specify either the iso_checksum or the iso_checksum_url parameter. If you specify the iso_checksum parameter, the iso_checksum_url parameter is automatically ignored.</td>
</tr>
<tr>
<td>iso_url</td>
<td>String</td>
<td>A URL that points to the ISO file, and contains the installation image. This URL may be an HTTP URL or a file path:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• If it is an HTTP URL, Packer downloads the file from the HTTP link and caches the file for later.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• If it is a file path to the IMG or QCOW2 file, QEMU directly starts the file. If you have the file path specified, set parameter disk_image to true.</td>
</tr>
<tr>
<td>headless</td>
<td>boolean</td>
<td>By default, Packer starts the virtual machine GUI to build a QEMU virtual machine. If you set headless to True, a virtual machine without any console is started.</td>
</tr>
</tbody>
</table>
For more information, see Packer QEMU Builder.

Parameters in a Packer provisioner

The provisioner in the preceding example contains a Post-Processor module that enables automated upload of on-premises images to Alibaba Cloud. Required parameters for the provisioner are as follows:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>access_key</td>
<td>String</td>
<td>Your AccessKeyID. The AccessKey has a high privilege. We recommend that you first create a RAM user and use the RAM account to create an AccessKey to maintain security of your Alibaba Cloud account.</td>
</tr>
<tr>
<td>secret_key</td>
<td>String</td>
<td>Your AccessKeySecret. The AccessKey has a high privilege. We recommend that you first create a RAM user and use the RAM account to create an AccessKey to maintain security of your Alibaba Cloud account.</td>
</tr>
<tr>
<td>region</td>
<td>String</td>
<td>Select the region where you want to upload your on-premises image. In this example, the region is cn-beijing. For more information, see regions and zones.</td>
</tr>
<tr>
<td>image_name</td>
<td>String</td>
<td>The name of your on-premises image. The name is must be 2 to 128 characters in length and can contain letters, numbers, Chinese characters, periods (.), colons (:), underscores (_), and hyphens (-). It must start with a letter or a Chinese character.</td>
</tr>
<tr>
<td>oss_bucket_name</td>
<td>String</td>
<td>The OSS bucket name. If you specify a bucket name that does not exist, Packer creates a bucket automatically with the specified oss bucket name when uploading the image.</td>
</tr>
<tr>
<td>image_os_type</td>
<td>String</td>
<td>Image type. Optional values:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>· linux</td>
</tr>
<tr>
<td></td>
<td></td>
<td>· windows</td>
</tr>
<tr>
<td>image_platform</td>
<td>String</td>
<td>Distribution of the image. For example, CentOS.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>---------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>image_architecture</td>
<td>String</td>
<td>The instruction set architecture of the image. Optional values:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• i386</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• x86_64</td>
</tr>
<tr>
<td>format</td>
<td>String</td>
<td>Image format. Optional values:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• RAW</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• VHD</td>
</tr>
</tbody>
</table>

For more information, see Packer *Alicloud Post-Processor*.

Next step

You can use the created image to create an ECS instance. For more information, see *create an instance from a custom image*.

References

- For more information about how to use Packer, see *Packer documentation*.
- For more information about release information, visit the Packer repository on GitHub *packer*.
- For more information about Alibaba Cloud open source tools, visit the Alibaba Cloud repository on GitHub *opstools*.
- For more information about Alibaba Cloud and Packer project, visit the Alibaba Cloud & Packer repositories on GitHub *packer-provider*.
- For more information about configuration file ks.cfg, see *Anaconda Kickstart*.

6.2 Update a custom image

This topic describes how to update custom images by using Operation Orchestration Service (OOS). OOS provides public templates to automate image updating. To create a random or scheduled O&M task, you only need to select a source image and specify required parameters, such as the Cloud Assistant scripts in a public template. The O&M task is then automatically executed based on the definitions in the template.

Context
The ACS-ECS-UpdateImage template defines the order in which the following tasks are executed to update the image:

1. Check whether the name of the new custom image exists and make sure that it complies with the naming conventions.
2. Create and launch a temporary ECS instance based on parameters such as the instance type, source image ID, and security group ID you have configured.
3. Check whether the Cloud Assistant client has been installed on the temporary ECS instance. If not, install the Cloud Assistant client.
4. Run scripts by using the Cloud Assistant client to update the system environment of the instance.

Note:
OOS calls Cloud Assistant API operations to run Shell, Bat, or PowerShell scripts to update the system environment of ECS instances. For more information, see #unique_68.

5. Stop the temporary ECS instance.
6. Create a custom image from the temporary ECS instance.
7. Release the temporary ECS instance.

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 and find the target image. In the Actions column, choose More > Update Image.
5. Go to the OOS console and perform the following operations:

a) In the Basic Information step, retain the default settings and click Next: Parameter Settings.

b) In the Parameter Settings step, specify parameters to automate the creation or updating of custom images. The following table describes these parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>targetImageName</td>
<td>The name for the new custom image. The name must comply with the regular expression /^[A-Za-z0-9-_]*$/ and cannot be the same as an existing image name.</td>
<td>add_testtxt_20191010</td>
</tr>
<tr>
<td>sourceImageId</td>
<td>The ID of the image you want to update.</td>
<td>m-bp13y4of6m doqw******</td>
</tr>
<tr>
<td>instanceType</td>
<td>The type of the temporary ECS instance to create. For more information, see #unique_39.</td>
<td>ecs.g5.xlarge</td>
</tr>
<tr>
<td>securityGroupId</td>
<td>The ID of the security group to which the temporary ECS instance belongs.</td>
<td>sg-bplazkttqpl dxg******</td>
</tr>
<tr>
<td>vSwitchId</td>
<td>The ID of the VSwitch to which the temporary ECS instance belongs. The VSwitch and security group must be in the same VPC.</td>
<td>vsw-bp1s5fnvk4 gn2tw******</td>
</tr>
</tbody>
</table>

Note: If you have not created a custom image, you can use a public image, such as centos_7_06_64_20G_a libase_20190711.vhd.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>commandType</td>
<td>The type of script you plan to execute by using the Cloud Assistant client. • RunShellScript: Shell script for Linux-based instances. • RunBatScript: Bat script for Windows-based instances. • RunPowerShellScript: PowerShell script for Windows-based instances.</td>
<td>RunShellScript</td>
</tr>
<tr>
<td>commandContent</td>
<td>The content of the script to execute on the temporary ECS instance.</td>
<td>echo &quot;hello world&quot; &gt; /root /test.txt.</td>
</tr>
<tr>
<td>Permissions</td>
<td>Optional. Valid values: • Use Existing Permissions of Current Account: This is the default value. You have all the permissions granted to your account. Make sure that you have the permissions to call the ECS API operations required for creating custom images. • Specify RAM Role and Use Permissions Granted to This Role: If a RAM role is specified, OOS performs O&amp;M tasks by assuming that RAM role.</td>
<td>Use Existing Permissions from a Current Account</td>
</tr>
</tbody>
</table>
c) Click Next: Preview.

d) Confirm O&M task details and high-risk operations. Then, click Confirm and Create.

6. In the left-side navigation pane, click Executions to view the created O&M task.

Result

If the O&M task is created and its execution status is Running, the custom image is being updated. If Execution Status changes to Succeeded, the image is updated. You can view the ID of the new image on the Execution Result page.
To view the progress of the image updating operations, click Details of the O&M task to view Execution Logs.

References
Introduction to OOS

6.3 Modify custom images

This topic describes how to modify the name and description of your custom images.

Procedure

To modify the name and description of a custom image, follow these steps:

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 target custom image and then click the icon.
5. Enter a new name for the custom image.
6. In the Actions column, click Modify Description.

7. In the displayed dialog box, enter a Custom Image Description

8. Click Save.

Alternatively, you can modify the name and description of a custom image by calling the ECS API `ModifyImageAttribute`.

6.4 Import images

6.4.1 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:
   a. 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.
   b. Install cloud-init to allow instances running the image to complete the initialization configuration. For more information, see Install cloud-init.
   c. Install VirtIO drivers to allow ECS instances created from the image to start. For more information, see Install 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 virtio driver
2. Instructions for importing images
3. Convert the image file format
4. Import custom images

**6.4.2 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 information 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 ]
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.

<table>
<thead>
<tr>
<th>Detection item</th>
<th>Non-compliance issue</th>
<th>Suggestion</th>
</tr>
</thead>
<tbody>
<tr>
<td>driver</td>
<td>The ECS instance cannot start correctly.</td>
<td>Install the virtualization driver. For more information, see Install cloud-init.</td>
</tr>
<tr>
<td>/etc/shadow</td>
<td>The password file cannot be modified. As a result, you cannot create an ECS instance from the custom image.</td>
<td>Do not run the chattr command to lock the /etc/shadow file.</td>
</tr>
<tr>
<td>SELinux</td>
<td>The ECS instance cannot start correctly.</td>
<td>Do not start SELinux by modifying /etc/selinux/config.</td>
</tr>
<tr>
<td>qemu-ga</td>
<td>Some services required by ECS are unavailable, and the instance is not fully functional.</td>
<td>Uninstall qemu-ga.</td>
</tr>
<tr>
<td>Detection item</td>
<td>Non-compliance issue</td>
<td>Suggestion</td>
</tr>
<tr>
<td>----------------</td>
<td>-----------------------</td>
<td>------------</td>
</tr>
<tr>
<td>network</td>
<td>Network functions of the ECS instance are unstable.</td>
<td>Disable or delete Network Manager and enable the network service.</td>
</tr>
<tr>
<td>ssh</td>
<td>You cannot <em>connect</em> to the ECS instance from the console.</td>
<td>Enable the SSH service and do not set PermitRootLogin.</td>
</tr>
<tr>
<td>firewall</td>
<td>The system does not automatically configure your ECS instance environment.</td>
<td>Disable firewalls such as iptables, firewalld, IPFilter (IPF), IPFireWall (IPFW), or PacketFilter (PF).</td>
</tr>
</tbody>
</table>
| 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. |
<p>| device id      | The ECS instance cannot start correctly. | Clean up the <code>fstab</code> file and remove unneeded device IDs from the file to make sure that the device IDs in use appear in the output of the <code>blkid</code> command. |
| root           | The username and password cannot be used to connect to the ECS instance. | Reserve the root account. |
| 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. |</p>
<table>
<thead>
<tr>
<th>Detection item</th>
<th>Non-compliance issue</th>
<th>Suggestion</th>
</tr>
</thead>
<tbody>
<tr>
<td>/lib</td>
<td>The ECS instance cannot be configured automatically.</td>
<td>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.</td>
</tr>
<tr>
<td>system disk</td>
<td>N/A</td>
<td>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.</td>
</tr>
<tr>
<td>disk usage</td>
<td>Required drivers or services cannot be installed for the ECS instance.</td>
<td>Make sure that sufficient disk space is available.</td>
</tr>
<tr>
<td>inode usage</td>
<td>Required drivers or services cannot be installed for the ECS instance.</td>
<td>Make sure that sufficient inode resources are available.</td>
</tr>
</tbody>
</table>

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 installing kvm driver."
]
```

What to do next

1. View Instructions for importing images.

2. Install virtio driver.

3. Optional. Convert the image file format.

4. Import custom images.

5. #unique_10.
6.4.3 Instructions for importing images

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

Windows images

Considerations

- Verify the integrity of the file system.
- Do not modify critical system files.
- Make sure that the system disk has sufficient storage 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 access to RDP port 3389.
- The logon password for the administrator account 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 \( ( ) ~ ! @ # $ % ^ & * - _ + = | \{ \} [ ] : ; ' < > , . ? / \). In addition, the password cannot start with a forward slash (/).

Items not supported

- ISO image files are not supported. Before importing ISO images to ECS, use tools such as VirtualBox installed on premises to create ISO images, and then convert the images to RAW, VHD, or qcow2 format.
- Do not install qemu-ga in an imported image. If it is installed, some of the services that ECS needs may be unavailable.
- Images running the following operating systems cannot be imported: Windows XP, Windows 7 (professional and enterprise editions), Windows 8, and Windows 10.

Items supported

- Multi-partition system disks.
- NTFS file systems and MBR partitions.
- Images in RAW, qcow2, or VHD format. If the target image is not in one of the preceding formats, convert the image file format before you import it. For more information, see Convert image formats.
• Images running 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

Considerations

• 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 release cannot be identified by ECS, leading to system creation failures.
  - 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 the ECS instance cannot be started.
  - Do not change /etc/shadow to read-only. Otherwise, the password file cannot be modified, leading to system creation failures.
  - Do not enable SELinux by modifying /etc/selinux/config. Otherwise, the system cannot start.

• Make sure that the system disk has sufficient storage space.
• Disable the firewall and allow access to SSH port 22.
• Enable Dynamic Host Configuration Protocol (DHCP).
• Install XEN or KVM virtualization drivers. For more information, see Install the virtio driver.
• We recommend that you use cloud-init to configure the hostname, NTP source, and yum source. For more information, see Install cloud-init.
• The logon password for the root account 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 ( ) ~ ! @ # $ % ^ & * - _ + = | { } [ ] : ; ' < > , . ? /.
Items not supported

- ISO image files are not supported. Before importing ISO images to ECS, use tools such as VirtualBox installed on premises to create ISO images, and then convert the images to RAW, VHD, or qcow2 format.
- Multiple network interfaces.
- IPv6 addresses.
- Do not adjust system disk partitions. Only disks with a single root partition are supported.
- Do not install qemu-ga in an imported image. If it is installed, some of the services that ECS needs may be unavailable.

Items supported

- Images in RAW, qcow2, or VHD format. If the target image is not in one of the preceding formats, convert the image file format before you import it. For more information, see Convert image formats.
- xfs, ext3, and ext4 file systems, and MBR partitions.

Note:
The ext4 file system cannot contain the 64bit feature. The project and quota features cannot appear in pairs. To view the list of features contained in the ext4 file system, run the `tune2fs -l ext4 file system disk directory | grep features` command.

- Images running the following operating systems:
  - Aliyun Linux
  - CentOS 5/6/7
  - CoreOS 681.2.0 or later
  - Debian 6/7
  - FreeBSD
  - OpenSUSE 13.1
  - Red Hat
  - Red Hat Enterprise Linux (RHEL)
  - SUSE Linux 10/11/12
  - Ubuntu 10/12/13/14/16/18
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 do not comply with ECS requirements for a standard operating system, such as critical system configuration files, basic system environments, and applications. 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 and does not process the instances created from such images. If you enable DHCP before you create an image, ECS automatically configures your network. If DHCP is not enabled, you must connect to the created instance by using the Management Terminal in the ECS console, and then manually configure the IP address, IP route, and password.
- Customized Linux: After importing a customized Linux image, configure the network and password of the instance according to the standard system configuration of ECS. For more information, see Customize Linux images.

6.4.4 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 on-premise server when you create a custom Linux image. This topic describes how to install Alibaba Cloud cloud-init and Community cloud-init.

Prerequisites

To install Alibaba Cloud cloud-init, ensure that the python-pip dependency library is installed on the source server.

To install the Community cloud-init, ensure that the Git, Python 2.7, and python-pip dependency libraries are installed on the source server.

Installation commands for some Linux distributions are shown as follows:
Elastic Compute Service

Images / 6 Custom image

- CentOS/Red Hat Enterprise Linux:
  - yum -y install git python python-pip

- Ubuntu/Debian:
  - apt-get -y install git python python-pip

- openSUSE/SUSE:
  - zypper -n install git python python-pip

Context

cloud-init is an open-source software used by cloud platforms to configure system initialization of Linux virtual machines. All major public cloud platforms such as Alibaba Cloud, Amazon Web Services (AWS), Microsoft Azure, and OpenStack support cloud-init. For more information, see cloud-init Documentation.

Alibaba Cloud cloud-init initializes the configurations of instances during their startup, including NTP, software source, hostname, and SSH key pair. It also executes user data scripts.

Note:
cloud-init later than v18 automatically initializes network configurations. The code for network configuration is

```
BOOTPROTO=dhcp DEVICE=eth0 ONBOOT=yes STARTMODE=auto TYPE=Ethernet USERCTL=no.
```

Some public images have been upgraded to v19.1. If you want to customize network configurations after you install cloud-init, see (Optional) Customize network configuration below in this topic.

Scenarios

By default, cloud-init is installed for all Alibaba Cloud public images. If you use a custom image in the following scenarios, we recommend that you install Alibaba Cloud cloud-init for your Linux server to ensure that the created instance can automatically initialize system configurations:

- Linux servers that will be migrated to the cloud but are not installed with cloud-init.
- Linux servers that are installed with cloud-init whose version is earlier than v0.7 .9.
- Alibaba Cloud ECS instances that are not installed with cloud-init.
Check the 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 version of Alibaba Cloud cloud-init is 0.7.6a, and the data source is Aliyun.

After cloud-init is installed, it starts automatically during startup by default. If the installed cloud-init version is not suitable or the data source is not configured properly, cloud-init may run abnormally and the instance may start slowly or even fail to be started the next time you restart the instance.

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

   ```bash
   which cloud-init
   ```

   If no information in the output indicates that cloud-init is installed, install Alibaba Cloud cloud-init.

3. Run the following command to check the version of cloud-init:

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

   If the version is earlier than the Community v0.7.9 (except for v0.7.6 a), you must install Alibaba Cloud cloud-init.

4. Complete the data backup.

   **Note:**
   We recommend that you proceed with caution when you install Alibaba Cloud cloud-init on servers that will not be migrated to the cloud.

(Recommended) Install Alibaba Cloud cloud-init

1. Run the following command to download Alibaba Cloud cloud-init:

   ```bash
   ```

2. Run the following command to download and decompress the cloud-init installation package to the current directory.

   ```bash
   tar -zxvf alibaba-cloud-init-latest.tgz
   ```

3. Access the `tools` directory of `cloud-init`.
4. Run the following command to execute the `deploy.sh` script to install cloud-init:

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

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>issue</td>
<td>The type of the operating system. Valid values: centos, redhat, rhel, debian,</td>
<td>centos</td>
</tr>
<tr>
<td></td>
<td>ubuntu, opensuse, and sles. The parameter values are case-sensitive. sles stands for</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SUSE and SLES.</td>
<td></td>
</tr>
<tr>
<td>major_version</td>
<td>The major version number of the operating system.</td>
<td></td>
</tr>
</tbody>
</table>

5. Check whether cloud-init is installed.

If "description": "success" is returned, Alibaba Cloud cloud-init is installed.

```json
{
  "status_code": 0,
  "description": "success"
}
```

Installation commands for different Linux distributions are shown as follows: You may need to adapt the script to your operating system.

- **CentOS 6 and 7**

  ```bash
  # Check whether the python-pip dependency library is installed. If no, install it.
  if ! python -c 'import setuptools' >& /dev/null; then
    yum -y install python-pip
  fi
  # Back up cloud-init of the earlier version.
  test -d /etc/cloud && mv /etc/cloud /etc/cloud-old
  # Download and decompress Alibaba Cloud cloud-init.
  tar -zxvf ./ali-cloud-init-latest.tgz
  # Install cloud-init.
  issue_major=$( cat /etc/redhat-release | grep -Eo '[0-9]+\.[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 7**

  ```bash
  # Check whether the python-pip dependency library is installed. If no, install it.
  if ! python -c 'import setuptools' >& /dev/null; then
    yum -y install python-pip
  ```
# Back up cloud-init of the earlier version.
test -d /etc/cloud & mv /etc/cloud /etc/cloud-old
# Download and decompress Alibaba Cloud cloud-init.
ali-cloud-init-latest.tgz
tar -zxvf ./ali-cloud-init-latest.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, 16, and 18

# Check whether the python-pip dependency library is installed. If no, install it.
if ! python -c 'import setuptools' >& /dev/null; then
    apt-get install python-pip -y
fi
# Back up cloud-init of the earlier version.
test -d /etc/cloud & mv /etc/cloud /etc/cloud-old
# Download and decompress Alibaba Cloud cloud-init.
ali-cloud-init-latest.tgz
tar -zxvf ./ali-cloud-init-latest.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 9

# Check whether the python-pip dependency library is installed. If no, install it.
if ! python -c 'import setuptools' >& /dev/null; then
    apt-get install python-pip -y
fi
# Back up cloud-init of the earlier version.
test -d /etc/cloud & mv /etc/cloud /etc/cloud-old
# Download and decompress Alibaba Cloud cloud-init.
ali-cloud-init-latest.tgz
tar -zxvf ./ali-cloud-init-latest.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 12

# Check whether the python-pip dependency library is installed. If no, install it.
if ! python -c 'import setuptools' >& /dev/null; then
    zypper -n install python-pip
fi
# Back up cloud-init of the earlier version.
test -d /etc/cloud & mv /etc/cloud /etc/cloud-old
# Download and decompress Alibaba Cloud cloud-init.
ali-cloud-init-latest.tgz
tar -zxvf ./ali-cloud-init-latest.tgz
# Install cloud-init.
issue_major=$( cat /etc/os-release | grep VERSION_ID | grep -Eo '[0-9]+\.[0-9]+\.[0-9]+' | head -1 | awk -F'.' '{printf $1}')
bash ./cloud-init-*/*tools/deploy.sh sles "$issue_major"

- openSUSE 13 and 42

# Check whether the python-pip dependency library is installed. If no, install it.
if ! python -c 'import setuptools'>& /dev/null; then
  zypper -n install python-pip
fi
# Back up cloud-init of the earlier version.
test -d /etc/cloud && mv /etc/cloud/etc/cloud-old
# Download and decompress Alibaba Cloud cloud-init.
tar -zxvf ./ali-cloud-init-latest.tgz
# Install cloud-init.
issue_major=$( cat /etc/os-release | grep VERSION_ID | grep -Eo '[0-9]+\.[0-9]+\.[0-9]+' | head -1 | awk -F'.' '{printf $1}')
bash ./cloud-init-*/tools/deploy.sh opensuse"$issue_major"

(Optional) Install Community cloud-init

1. Run the following command to download the cloud-init source code package from Git:

   ```bash
git clone https://git.launchpad.net/cloud-init
   ```

2. Access the cloud-init directory.

   ```bash
cd ./cloud-init
   ```

3. Run the following command to install all the dependency libraries:

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

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

   ```bash
python setup.py install
   ```

5. Modify the configuration file `cloud.cfg`.

   a) Open the configuration file.

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

   b) Modify the configuration before `cloud_init_modules`: as follows:

   ```bash
# 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
# This will cause the setupupdate hostname module to not operate (if true)
preserve_hostname: false
# Example datasource config
datasource:
  # Eucalyptus
  ec2:
      'metadataиныз?all=search?all=metadata']
timeout: 5
  max_wait: 10
  # (defaults to 50 seconds)
cloud_init_modules:
```
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, cloud-init v19.1 does not manage the network configuration under `/etc/sysconfig/network-scripts/` and you must manage the network configuration manually.

# 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 default $user
disable_root: false

# This will cause the set-update hostname module to not operate (if true)
preserve_hostname: false

manage_etc_hosts: localhost

network:
  config: disabled

datasource_list: [ AliYun ]

# Example datasource config

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 as needed based on the error message.
<table>
<thead>
<tr>
<th>Error message</th>
<th>Cause</th>
<th>Troubleshooting command</th>
</tr>
</thead>
<tbody>
<tr>
<td>no setuptools module in python</td>
<td>The python setuptools module is not installed.</td>
<td>• CentOS/Red Hat: yum -y install python-pip</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Ubuntu/Debian: apt-get -y install python-pip</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• openSUSE/SUSE: zypper -n install python-pip</td>
</tr>
<tr>
<td>File &quot;/root/cloud-init/cloudinit/log.py&quot;, line 19, in &lt;module&gt; import six ImportError: No module named six )</td>
<td>The six dependency library is not installed.</td>
<td>pip install six</td>
</tr>
<tr>
<td>File &quot;/root/cloud-init/cloudinit/url_helper.py&quot;, line 20, in &lt;module&gt; import oauthlib.oauth1 as oauth1 ImportError: No module named oauthlib.oauth1 )</td>
<td>The oauthlib dependency library is not installed.</td>
<td>pip install oauthlib</td>
</tr>
<tr>
<td>Error messages do not indicate the libraries that are not installed.</td>
<td>The error message is not mapped.</td>
<td>Run the following command to install all dependency libraries that are listed in the requirements.txt file of cloud-init: pip install -r requirements.txt</td>
</tr>
</tbody>
</table>

What's next

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

  You can migrate the server to the cloud by using the Cloud Migration tool or importing the custom image. 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 source, 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 topics
cloud-init official website - Alibaba Cloud (AliYun)

6.4.5 Install virtio driver

This topic details which images do and do not require the virtio driver to be installed on the source server before import.

Images requiring no manual installation

After you import custom images, if the operating systems of your images are listed as follows, Alibaba Cloud automatically processes the virtio driver for you:

- Windows Server 2008
- Windows Server 2012
- Windows Server 2016
- CentOS 6/7
- Ubuntu 12/14/16
- Debian 7/8/9
- SUSE 11/12

You can skip to recover the temporary root file system of initramfs or initrd.

Images requiring manual installation

For Linux images that are not included in the preceding list, you must install the virtio driver on-premises before importing the images.

To check the availability of virtio driver on a server
1. Run `grep -i virtio /boot/config-$\text{uname -r}` to inspect whether the virtio driver is already built in the kernel of your server.

![Image of grep output]

**Note:**
- If VIRTIO_BLK and VIRTIO_NET do not exist in the output, the virtio driver is not built in the kernel. You must install and configure the virtio driver on your server to compile and install virtio driver.
- If the values of parameter `CONFIG_VIRTIO_BLK` and parameter `CONFIG_VIRTIO_NET` are y, the virtio driver is already built in the kernel. For more information, see notes for importing images and import custom images.
- If the values of parameter `CONFIG_VIRTIO_BLK` and parameter `CONFIG_VIRTIO_NET` are m, continue to step 2.

2. Run `lsinitrd /boot/initramfs-$\text{uname -r}.img | grep virtio` to make sure the virtio driver has been compiled in the temporary root file system of initramfs or initrd.

![Image of lsinitrd output]

**Note:**
- According to the preceding figure, the virtio_blk driver, including its dependency virtio.ko, virtio_pci.ko and virtio_ring.ko, has been compiled in

---

**Issue:** 20200403
Elastic Compute Service

Images / 6 Custom image

the temporary root file system initramfs. For more information, see notes for importing images and import custom images.

• If virtio driver is unavailable in the initramfs, you must recover the temporary root file system of initramfs or initrd before importing images or migration.

To recover the temporary root file system

If the virtio driver is supported by the kernel but not compiled in the temporary root file system, you must recover the temporary root file system. The following example uses CentOS:

• 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)
```

To compile and install virtio driver

The following example uses a Red Hat server:

To download the kernel package

1. Run `yum install -y ncurses-devel gcc make wget` to install necessary components to compile the kernel.

2. Run `uname -r` to query the kernel version of your server, such as 4.4.24-2.a17.x86_64.
3. Visit published Linux Kernel Archives to download the source codes of kernel, for example, the download link of kernel version starting with 4.4.24 is https://www.kernel.org/pub/linux/kernel/v4.x/linux-4.4.24.tar.gz.

4. Run `cd /usr/src/` to change the directory.


6. Run `tar -xzf linux-4.4.24.tar.gz` to decompress the package.

7. Run `ln -s linux-4.4.24 linux` to establish a link.

8. Run `cd /usr/src/linux` to change the directory.

To compile the kernel

1. Run the following commands to compile the driver into the kernel.

   ```bash
   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. Configure the corresponding settings of virtio driver in the following windows:

   **Note:**
Select * to build the driver in the kernel, select m to compile it as a module.

a. Press the space bar to select Virtualization.

Make sure that you have selected the option of KVM (Kernel-based Virtual Machine).

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)

b. Press the Esc key to exit the kernel configuration windows, and save changes to file .config according to the dialog box.
c. Inspect whether all the corresponding settings of virtio driver has been correctly configured or not.
d. (Optional) If no configuration of virtio driver is settled after the inspect, run the following commands to edit the file .config manually.

   make oldconfig
   make prepare
   make scripts
   make
   make install
e. Run the following commands to check whether the virtio driver is installed.

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

Note:
If any of the output includes virtio_blk and virtio_pci.virtio_console, your server has correctly installed the virtio driver.

What to do next

After compiling the virtio driver, you can migrate your server to Alibaba Cloud by using the Cloud Migration Tool.
6.4.6 Customize Linux images

If the selected OS is not supported by Alibaba Cloud and cloud-int cannot be installed, you can select Customized Linux when importing 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 logging 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.
- There is no default SSH key pair. The initial SSH private key pair must be randomly generated by Alibaba Cloud.

Procedure

Before creating and importing a customized Linux image, you must make the following configurations:

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 automatically 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

The following section shows examples of the os.conf files for instances in classic networks and instances in VPCs.

- Instances in classic networks:

```plaintext
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.

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

- Instances in VPCs:

```plaintext
hostname=<yourHostName>
password=<yourPassword>
```
The following table describes the parameters in the preceding example.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hostname</td>
<td>The hostname.</td>
</tr>
<tr>
<td>password</td>
<td>The password, which is a Base64-encoded string.</td>
</tr>
<tr>
<td>eth0_ip_addr</td>
<td>The IP address of the eth0 NIC.</td>
</tr>
<tr>
<td>eth0_mac_addr</td>
<td>The MAC address of the eth0 NIC.</td>
</tr>
<tr>
<td>eth0_netmask</td>
<td>The network mask of the eth0 NIC.</td>
</tr>
<tr>
<td>eth0_gateway</td>
<td>The default gateway of the eth0 NIC.</td>
</tr>
<tr>
<td>eth0_route</td>
<td>The eth0 internal and internet routes that are separated by semicolons (;) by default.</td>
</tr>
<tr>
<td>dns_nameserver</td>
<td>The DNS address list, in which addresses are separated by spaces by default.</td>
</tr>
</tbody>
</table>

Considerations for the parsing script

In normal cases, when an instance is started for the first time, Alibaba Cloud automatically writes instance configurations to the os.conf file. The os.conf 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:

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatic start at system startup</td>
<td>Set the parsing script to be automatically started at system startup by placing the script in the /etc/init.d/ directory.</td>
</tr>
<tr>
<td>Values for configuration items</td>
<td>As shown in Example of the os.conf file, instances in classic networks and instances in VPCs differ in the number of configuration items and values of some configuration items.</td>
</tr>
<tr>
<td>Condition</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>Path for the configuration file</td>
<td>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. As a best practice, include <code>uuid</code> or <code>label</code> in your parsing code to identify the device allocated for the first partition. Because the user password is a Base64-encoded string, it must also be Base64-encoded in the parsing script.</td>
</tr>
<tr>
<td>Network type</td>
<td>When determining the network type, the parsing script can check whether there are <code>eth1_route</code> or other <code>eth1</code>-related configuration items. The script will parse and process the instance accordingly based on the network type.</td>
</tr>
<tr>
<td></td>
<td>• Instances in VPCs are configured with the default Internet route and default internal route that are specified by the <code>eth0_route</code> parameter in the <code>os.conf</code> file.</td>
</tr>
<tr>
<td></td>
<td>• Instances in classic networks are configured with the default Internet route that is specified by the <code>eth1_route</code> parameter in the <code>os.conf</code> file, and with the default internal route that is specified by the <code>eth0_route</code> parameter.</td>
</tr>
<tr>
<td>Configuration optimization</td>
<td>Configurations in the <code>os.conf</code> file are executed only once during the instance lifecycle. We recommend that you delete the <code>os.conf</code> file after the parsing script is executed. The parsing script will not execute the configurations in the <code>os.conf</code> file if the script does not read any.</td>
</tr>
<tr>
<td>Customized image processing</td>
<td>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 <code>os.conf</code> file when the instance is started for the first time. Then, the parsing script immediately executes the configurations upon detection.</td>
</tr>
<tr>
<td>Configuration change processing</td>
<td>When instance configurations are changed through the Alibaba Cloud console or API operations, Alibaba Cloud writes new configurations to the <code>os.conf</code> file. Then, the parsing script runs again to issue the changes.</td>
</tr>
</tbody>
</table>

Example of the parsing script

This section uses a parsing script for CentOS as an example. You must change the script content based on your operating system. Make sure to debug the script before you execute it.

```bash
#!/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
}

config_hostname() {
  if [[ -n $hostname ]]; then
    sed -i "s/^HOSTNAME=. */HOSTNAME=$hostname/" /etc/sysconfig/network
    hostname $hostname
  
}

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=$4
    interface_cfg="/etc/sysconfig/network-scripts/ifcfg-${interface}
    cat << EOF > $interface_cfg
    DEVICE=$interface
    IPADDR=$ip
    NETMASK=$netmask
    HWADDR=$mac
    ONBOOT=yes
    BOOTPROTO=static
    EOF
    DEVICE=$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 $route | sed 's;/\n/' | \n        while read line; do
            dst=$(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
    }

    start() {
        if load_os_conf ; then
            config_password
            config_network
            config_hostname
            config_dns
            cleanup
            return 0
        else
            return 1
        fi
    }
}
Elastic Compute Service

Images / 6 Custom image

```bash
    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
```

6.4.7 Convert the image file format

ECS can only import image files in the RAW, VHD, or qcow2 format. 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.

Context

The qemu-img tool supports the following formats:

- Convert images from the RAW, qcow2, qcow1, VMDK, VDI, VHD (VPC), VHDX, or QED format to the VHD format.
- Convert between RAW and VHD.

Note:
The qemu-img tool cannot convert ISO images to the VHD or RAW format. To convert the image format, install the ISO image to VHD or RAW media, and then create an image in the specified format.

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.
   a) Choose Start > Computer, right-click Computer, and choose Properties from the shortcut menu.
   b) In the left-side navigation pane, click Advanced System Settings.
   c) In the System Properties dialog box that appears, click the Advanced tab and then click Environment Variables.
   d) 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.
   e) 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.
   a) Open Command Prompt in Windows.
   b) Run the `qemu-img --help` command.
      If the command output is displayed, the environment variable is properly configured.

4. In Command Prompt, 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 target image format, source file name, and target file name.

      When the conversion is complete, the target 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.

   Example:
   
   • 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 target image format, source file name, and target file name.

   When the conversion is complete, the target file will appear in the directory where the source image file is located.

What's next

#unique_83

6.4.8 Import custom images

   This topic describes how to import on-premises image files to your ECS environment. You can use imported images to create ECS instances or change the system disks of ECS instances.

Prerequisites

Before importing custom images, make sure that the following requirements have been met:

• You understand the limits for importing an on-premises image specified in `Instructions for importing images`, `Customize Linux images`, and `Convert the image file format`.
- You have #unique_64.

- If you are using a RAM user account, ensure that this account has been granted the permission for the AliyunECSImageImportDefaultRole role by the corresponding Alibaba Cloud account.

**Context**

When you import an image, a snapshot is automatically generated. You can view the snapshot information on the Snapshots page of the ECS console. Before the import image task is complete, the status of the snapshot is displayed as Failed. After the task is complete, the status automatically changes to Successful. The snapshot capacity is the size of the imported image file, regardless of the system disk size that was set when you import the image. The snapshot service is a paid service. For more information, see #unique_84.

The import image function allows you to select a license type to activate the source operating system. This can reduce your image usage costs on the cloud. For more information about license types, see *Parameters for image import*.

**Procedure**

1. Use a third-party OSS client or the OSS API to upload the prepared custom image file. If the file is larger than 5 GiB, see #unique_85.

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.
   a) On the Images page, click Import Image.
   b) In the Import Image dialog box, click Confirm Address in step 3 shown in the following figure.
   c) On the Cloud Resource Access Authorization page, select AliyunECSImageImportDefaultRole and AliyunECSExportDefaultRole and click Confirm Authorization Policy.

6. Import the custom image.
   a) Go back to the Images page and click Import Image.
   b) In the Import Image dialog box, configure the following parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Region of Image</td>
<td>Yes</td>
<td>This field is automatically populated with the current region. To change the region, close the Import Image dialog box and select a new region in the top navigation bar of the Images page. You can then click Import Image again to configure other parameters.</td>
</tr>
<tr>
<td>OSS Object Address</td>
<td>Yes</td>
<td>Copy the object address of the image file from the OSS console. For more information, see #unique_86.</td>
</tr>
<tr>
<td>Image Name</td>
<td>Yes</td>
<td>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 (-).</td>
</tr>
<tr>
<td>Operating System</td>
<td>Yes</td>
<td>Select the operating system of your image. Valid values: Windows</td>
</tr>
<tr>
<td>Parameter</td>
<td>Required</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>System Disk Size</td>
<td>Yes</td>
<td>Specify the system disk size. Valid values: 40 GiB to 500 GiB.</td>
</tr>
<tr>
<td>System Architecture</td>
<td>Yes</td>
<td>Select x86_64 for 64-bit operating systems and i386 for 32-bit operating systems.</td>
</tr>
</tbody>
</table>
| Platform                 | Yes      | The options depend on your selected Operating System. Select a system platform for the image to be imported.  
- Linux: CentOS, SUSE, Ubuntu, Debian, FreeBSD, CoreOS, Aliyun, Customized Linux, and Others Linux. *(open a ticket to confirm the selected edition is supported.)*  
- If your image operating system is a custom edition developed from Linux kernel, *open a ticket.* |
| Image Format             | No       | The qcow2, RAW, and VHD formats are supported. We recommend that you use the qcow2 and VHD formats.  
**Note:**  
The ISO format is not supported. You can use offline tools such as VirtualBox to create an ISO image file and convert it 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 #unique_87. |
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
</table>
| License Type         | No       | Select a license type to activate the source operating system after the image is imported. Valid values:  
|                      |          | • BYOL: the license that is provided by the source operating system. When this option is selected, make sure that your license key can be used by Alibaba Cloud.  
|                      |          | • Alibaba Cloud: the Alibaba Cloud software license. When this option is selected, the Alibaba Cloud license is applied to your selected Platform.  
|                      |          | • Automatic: 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.                                  |
| Add Images of Data Disks | No   | Select this option if you want to import an image that contains data disks. Supported data disk capacity ranges from 5 GiB to 2,000 GiB. |

c) 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 file and the number of image import tasks in the queue.

What's next

#unique_10
6.5 Copy custom images

This topic describes how to copy a custom image that is under your Alibaba Cloud account. This action enables you to create identical ECS instances across regions, allowing you to implement seamless data backups of the target instances.

Background information

An image is a regional resource, and a custom image belongs to the region where it is created. The following table lists the different scenarios of using custom images.

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Procedure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Copy images across regions under the same account</td>
<td>See Copy images.</td>
<td>When an image is copied, the corresponding snapshot is generated in the target region at the same time. After the copy operation is completed, a new image is generated in the target region, and it has a unique image ID.</td>
</tr>
<tr>
<td>Copy images across regions under different accounts</td>
<td>See Copy images and Share images.</td>
<td>An image is copied to the target region and then shared with the target account.</td>
</tr>
<tr>
<td>Share images in the same region under different accounts</td>
<td>See Share images.</td>
<td>This operation does not create a new image. The shared image still belongs to you.</td>
</tr>
</tbody>
</table>

Limits

Before you copy a custom image, note the following:

- Only custom images can be copied across regions. If you need to copy an image of another type, you need to first use that image to create an instance and then use that instance to create a custom image. Afterwards, you can copy the newly created custom image to the target region.
When an image is copied, a corresponding snapshot is generated in the target region at the same time, and then a custom image is generated based on the snapshot. Therefore, data traffic occurs between the source and target regions. Currently, no fees are charged for this traffic. For the latest billing details, see the official Alibaba Cloud website for announcements.

The created custom image in the target region has the same configuration as the original custom image. However, the related role authorization and service authorization information is not copied, nor are the settings of instance user data.

The task completion time depends on the image size, the network transmission speed, and the number of concurrent tasks in the queue.

Images with encrypted snapshots cannot be copied across regions.

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 the custom image to be copied. Note that Type must be Custom Image. Then, in the Actions column, click Copy Image.

Note: If your custom image is larger than 500 GiB, when you click Copy Image, you will be directed to open a ticket to complete the operation.

5. In the Copy Image dialog box, verify the ID of the selected image is the target image, and then complete the following configurations:
   a. Select the Target Region.
   b. Enter Custom Image Name and Custom Image Description that are shown in the target region.
   c. Click OK.
6. (Optional) Switch to the target region and check the progress. When 100% is displayed, the image is copied successfully.

Note:
If Progress is not 100%, Status is Creating. In this case, you can click Cancel Copy to cancel the operation. After the operation is canceled, the image information is removed from the target region.

You can also call the CopyImage and CancelCopyImage API actions to perform the preceding operations.

What to do next

When a copied image is in the Available state, you can use it to create an instance or change the system disk.

You can also view the copied snapshot in the target region.

6.6 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.

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 custom images.
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 #unique_22.

- Replace the system disk of an ECS instance with the shared image.
  
  For more information, see #unique_15.

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.

6.7 Export custom images

This topic describes considerations for exporting images and how to export Alibaba Cloud custom images.

Prerequisites

- Make sure that you have enabled OSS, and that an OSS bucket is available in the same region as your custom image. For more information, see #unique_95.

Note:

Exporting a custom image will incur OSS storage and traffic download fees. For more information, see #unique_96.

- This operation cannot export custom images that were created from Alibaba Cloud Marketplace images.
- Custom images to be exported cannot contain Windows Server operating systems.
· Custom images to be exported can only contain snapshots of up to four data disks. The size of each data disk cannot exceed 500 GiB.

Context

Before you export a custom image, note the following considerations:

· If an exported custom image contains data disk snapshots, multiple objects appear in your OSS. Objects whose name contains system are system disk snapshots. Objects whose name contains data are data disk snapshots. The identifier of a data disk snapshot is the mount point of the source data disk, for example, xvdb and xvdc.

· When using exported images to create instances with the same configurations, you must confirm that the storage location and storage space division of files recorded in /etc/fstab are consistent with the exported data disk snapshot information.

· 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.

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 you want to export. In the Actions column corresponding to the image, click More and choose Export Image from the shortcut menu.

   a) In the Export Image dialog box that appears, click Confirm Address.

   b) On the Cloud Resource Access Authorization page, click Confirm Authorization Policy to allow ECS to access your OSS resources.

5. Return to the ECS console homepage and go to the Images page again. Find the custom image you want to export. In the Actions column corresponding to the image, click More and choose Export Image from the shortcut menu.
6. In the Export Image dialog box, configure the following parameters:

- **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 Demo as the prefix, the exported image displayed in the OSS bucket is named `Demo-[Automatically generated object name]`.

7. Click OK to export the custom image.

You can cancel an export task at any time before the task is completed. Go to the Tasks page in the ECS console, find the task in the specified region, and cancel the task.

What's next

- Log on to the OSS console to query the result of the export task.
- Download the custom image. For more information, see "#unique_86".

![Note:]
The default format of exported custom images is `.raw.tar.gz`, and the format of the decompressed images is `.raw`. If your local computer runs on a Mac OS X system, we recommend that you use GNU Tar to decompress the images.

Related topics
- "#unique_97"
- "#unique_98"

6.8 Delete custom images

This topic describes how to delete a custom image. You can delete a custom image if you no longer need it. Deleting a custom image does not impact the instances created from the image or images copied from this image. Similarly, deleting image copies of a custom image has no impact on this custom image.

**Limits**

- After a custom image is deleted, it cannot be used to create new ECS instances. However, ECS instances created from the deleted custom image can still run normally (that is, continue to incur fees), but these instances cannot reinitialize their cloud disks.
If the to be deleted custom image has been shared to other accounts, you must remove all permissions that allow shared access to the custom image before you can delete the image. After a shared image is deleted:

- Users who are using the shared image will no longer be able to find the image through the ECS console or ECS API, nor can they use the image to create ECS instances or replace cloud disks.
- ECS instances that are created from the shared image cannot reinitialize their cloud disks.

**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 Custom Images tab page, select the image you want to delete. Note that the image type must be Custom Image.
5. Click Delete Image.
6. In the displayed dialog box, select the deletion method.
   - **Delete**: Delete a custom image by following the general procedures.
   - **Force Delete**: Forcibly delete a customer image. Select this option if you have created ECS instances by using this image.

   **Notice:**

   After a custom image is forcibly deleted, instances created by using this image cannot *reinitialize their cloud disks*.

7. Click OK.

You can also call *DeleteImage* to delete a custom image.
7 Marketplace images

This topic provides an overview of Alibaba Cloud Marketplace images and the related operations. You can use Marketplace images to obtain a pre-installed running environment or application on an ECS instance.

Background information

Alibaba Cloud Marketplace offers a variety of pre-installed, secure images and related services that are provided by independent software vendors (ISVs). These images integrate software and functions such as Hypertext Preprocessor (PHP) and control panel into operating systems.

Note:
After you create an ECS instance from a Marketplace image, the system may send you a message stating that your license has expired. In this case, contact your image provider for technical support.

Purchase a Marketplace image

1. Log on to the ECS console.
2. In the left-side navigation pane, choose Instances & Images > Instances.
3. Select a region.
4. On the Instances page, click Create Instance to go to the ECS purchase page.
5. Complete basic configurations.

Note that in the Image section you need to click Marketplace Image and then Select from image market (including operating system).

6. In the dialog box that is displayed, select the image you need, or enter keywords in the search bar to search for the image.

7. Complete the other configurations as prompted and click Create Order. Then, you can create an ECS instance according to #unique_92.

Create an ECS instance from a Marketplace image

1. Log on to the Alibaba Cloud Marketplace.

2. Select the image you need, and click Deploy Now.

3. Optional. If you have not logged on to the Alibaba Cloud console, log on before you can proceed.

4. Finish the other configurations as prompted and click Create Order. Then, create an ECS instance according to #unique_92.

Note:
On the Pay page that is displayed after you click Create Order, you must confirm and pay off the required fees before you can create the ECS instance from the image.

After you purchase a Marketplace image, you can go to the Account Overview page to view your bill.

Change the system disk of an ECS instance by using a Marketplace image

To change the image of an ECS instance you have purchased to a Marketplace image, you must change the system disk of this ECS instance.

Note:
After you change the image, the data on the system disk is lost. Therefore, we recommend that you back up the data before you change the system disk. For more information, see #unique_33.

To change the system disk, you need to navigate to the Replace System Disk page, select Marketplace Image in the Image Type section, click Select from image market (including operating system) in the Image Name section, and then in the displayed Image market dialog box select the image you need. For more information, see #unique_15.
8 Open source tools
9 Change the operating system

You can convert the OS running on your ECS instance to another supported OS through the ECS console.

To change the operating system, you must change the system disk of an instance:

- If you want to use a custom image, see change the system disk (custom image).
- If you want to use a public image, see change a system disk (public image).

Note:
Currently, instances that are hosted in regions outside of mainland China do not support swapping between Linux and Windows OSs. If your instance is hosted in one of these regions, you can only change its version of Windows OS to another version of Windows, or replace its current Linux OS with another Linux OS.
11 FAQ

11.1 Manage Windows Server Semi-Annual Channel images and instances

This topic describes the various methods you can use to manage an Alibaba Cloud ECS instance created from a Windows Server Semi-Annual Channel image.

Image overview

ECS now supports Windows Server Semi-Annual Channel images. When creating an instance, you can find the Version 1809 Datacenter image in the list of Windows Server public images. Windows Server Semi-Annual Channel images are operating system images running in pure Server Core mode and do not provide a graphical user interface. Windows Server Semi-Annual Channel images have much looser requirements for hardware, thus reducing the update frequency and supporting remote management. Alibaba Cloud ECS currently supports the following Windows Server Semi-Annual Channel versions:

- Windows Server 1809 Datacenter edition
- Windows Server 1709 Datacenter edition

Instance management tools

Instances that run Windows Server Semi-Annual Channel are not provided with the resource manager or control panel functions, or Windows Explorer, and do not support any .msc features (such as devmgmt.msc). However, you can manage Windows Server Semi-Annual Channel instances by using such tools as Sconfig, Server Manager, PowerShell, and Windows Admin Center.

Additionally, Windows Server Semi-Annual Channel instances run in Server Core mode. In this case, we recommend that you use PowerShell and Windows Admin Center to manage your instances. Procedures for the preceding management tools are provided in the following sections. For more information, see Manage a Server Core server.
PowerShell

In the following example, assume that the public IP address of your instance is 172.16.1XX.183. To implement PowerShell for remote management, follow these steps:

1. Connect to the target instance. For more information, see #unique_62.
2. Enter PowerShell in the command line of the target instance.
3. Run the following command in PowerShell:

   ```
   Enable-PSRemoting -Force
   Set-NetFirewallRule -Name "WINRM-HTTP-In-TCP-PUBLIC" -RemoteAddress Any
   ```

4. Add a rule to the security group of the target instance to allow access to the HTTP port 5985 and the HTTPS port 5986. For more information, see Add security group rules.

5. Enter PowerShell in the command line of your client.
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 also use * to indicate that all computers are trusted.

7. Run Enter-PSSession '172.16.1XX.183' -Credential:'administrator' in PowerShell and enter the instance password as prompted.

Now you can manage your Windows instance on your client computer.

Windows Admin Center

In the following examples, assume that the public IP address of your instance is 172.16.1XX.183. You can install Windows Admin Center either by using the command line or by downloading the installation package from the official website.
• Install Windows Admin Center through the command line

1. Connect to the target instance. For more information, see #unique_62.

2. Add a rule to the security group of the target instance to allow access to the HTTP 5985 and the HTTPS port 5986. For more information, see Add security group rules.

3. Enter PowerShell in the command line of the target instance.

4. Run the following command in PowerShell:

   ```
   Enable-PSRemoting -Force
   Set-NetFirewallRule -Name "WINRM-HTTP-In-TCP-PUBLIC" -RemoteAddress Any
   ```

5. Run the following command to download Windows Admin Center.

   ```
   msiexec /i c:\HonoluluTechnicalPreview1802.msi /qn /L*v log.txt
   SME_PORT=443 SSL_CERTIFICATE_OPTION=generate
   ```

6. Run the `cat log.txt` command to check the download progress. When the following information appears 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.
   ```

• Download and install Windows Admin Center through a browser

**Prerequisites**

Make sure that you are using a browser in the target client where Windows Admin Center is to be downloaded. PowerShell is configured. For more information, see PowerShell remote management.

**Procedure**

1. Download and install Windows Admin Center.

2. Open https://localhost/.

3. Click Add to add the instance IP address in the displayed window.

   Now you can manage your instance through Microsoft Edge or Chrome from the client computer of Windows Admin Center.
FAQ

How do I copy files to a Windows Server Semi-Annual Channel instance?

You can use RDP applications, PowerShell, or the Windows Admin Center to copy files from a client to a Windows Server Semi-Annual Channel instance.

• Through RDP applications
  1. Connect to the target instance. For more information, see #unique_62.
  2. On the client, copy the target files.
  3. In the CMD utility of your instance, enter notepad.
  4. Click File > Open. In the displayed window, select the destination directory for the files, then right-click and choose Paste.

• Through PowerShell
  1. Start the target instance.
  2. Open the CMD utility on the client, and enter PowerShell.
  3. Access the target instance remotely through PowerShell. For more information, see PowerShell remote management.
  4. Run the following command on the client:

```
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 computer, while -C:\2.txt is the target file directory on the Windows instance.

• Through Windows Admin Center
  1. Start the target instance.
  2. Configure Windows Admin Center. For more information, see Windows Admin Center.
  3. Open Windows Admin Center, and click the managed instance.
  4. Click File, select the target files and then click Upload.

How do I shut down or restart a Windows Server Semi-Annual Channel instance in the instance itself?
• Through RDP applications
  1. Connect to the target instance. For more information, see #unique_62.
  2. In the CMD utility, enter `sconfig`. Then, enter 13 to restart your instance or 14 to shut it down, and press Enter.

• Through PowerShell
  1. Connect to the target instance. For more information, see #unique_62.
  2. In the CMD utility, enter `PowerShell`.
  3. Enter one of the following commands to restart or shut down your instance:

        shutdown -r -t 00 :: # Restart your instance in 0 seconds through the command-line command
        shutdown -s -t 00 :: # Shut down your instance in 0 seconds through the command-line command
        Stop-Computer -Force # Shut down your instance immediately through the PowerShell command
        Restart-Computer -Force # Restart your instance immediately through the PowerShell command

• Through PowerShell remote management
  1. Start the target instance.
  2. Open the CMD utility on the client, and enter `PowerShell`.
  3. Access the target instance remotely through PowerShell. For more information, see `PowerShell remote management`.
  4. Enter one of the following commands on the client:

        Enter-PsSession -ComputerName 172.16.1XX.183
        Restart-Computer -Force #Restart
        Stop-Computer -Force #Shut down

• Through Windows Admin Center
  1. Start the target instance.
  2. Configure Windows Admin Center. For more information, see `Windows Admin Center`.
  3. Open Windows Admin Center, and click the managed instance. Then, click Overview, and select Restart or Shut down.

How do I install the IIS service?
Through RDP applications

1. Connect to the target instance. For more information, see #unique_62.
2. In the CMD utility, enter PowerShell.
3. Run the following command to install IIS:

   ```
   Import-Module ServerManager
   Add-WindowsFeature Web-Server, Web-CGI, Web-Mgmt-Console
   ```

Through PowerShell remote management

1. Start the target instance.
2. Open the CMD utility on the client, and enter PowerShell.
3. Access the target instance remotely through PowerShell. For more information, see PowerShell remote management.
4. Run the following command on the client:

   ```
   Enter-PsSession -ComputerName 172.16.1XX.183
   Import-Module ServerManager
   Add-WindowsFeature Web-Server, Web-CGI, Web-Mgmt-Console
   ```

Through Windows Admin Center

1. Start the target instance.
2. Configure Windows Admin Center. For more information, see Windows Admin Center.
3. Open Windows Admin Center, and click the managed instance. Click Roles and Features and Web Server in sequence, select the desired function, and click Yes.

How do I re-open a command line window that was accidentally closed in an RDP session?

To re-open a command line window, follow these steps:

1. Press Ctrl + Alt + End. If the preceding combination does not work, press Ctrl + Alt + Del.
2. In the interface that appears, select Task Manager and press Enter.
3. Click File > New Task, enter cmd, and click OK.

References

- Windows Server Semi-Annual Channel overview.
- Introducing Windows Server, version 1709
11.2 Install GRUB v1.99 in a Linux server

This topic describes how to install GRand Unified Bootloader (GRUB) in a Linux server by using GRUB v1.99 as an example. To install GRUB of a later version, you need to download the relevant GRUB package.

Background information

When you migrate a source Linux server by using the Cloud Migration tool, if the source Linux server has a low kernel version (such as CentOS 5 and Debian 7), and the version of the built-in system boot program GRUB is lower than v1.99, the log file indicates Do Grub Failed. In this case, you need to upgrade GRUB to v1.99 or later.

Procedure

1. Log on to the source Linux server.

2. Run the following commands to view the directories of the original grub, grub-install, and grub-mkconfig:

   ```bash
   # which grub
   # which grub-install
   # which grub-mkconfig
   ```

3. Run the mv command to rename the original grub, grub-install, and grub-mkconfig files for backup.

   ```bash
   # mv /sbin/grub /sbin/grub-old
   # mv /sbin/grub-install /sbin/grub-install-old
   # mv /sbin/grub-mkconfig /sbin/grub-mkconfig-old
   ```

   **Note:**
   After you migrate your server by using the Cloud Migration tool, you can reinstate the original files by changing their names back to the original ones.

4. Run the yum install -y bison gcc make command to install the dependencies of GRUB, which include bison, gcc, and make.

5. Run the following commands to install flex.

   ```bash
   # test -d /root/tools || mkdir -p /root/tools
   # cd /root/tools
   ```
6. Run the following commands to install the dependencies of GRUB v1.99.

```bash
# wget https://alpha.gnu.org/gnu/grub/grub-1.99-rc1.tar.gz
# tar xzf grub-1.99-rc1.tar.gz
# cd grub-1.99-rc1
# mkdir -p build
# cd build
# ../configure
# sed -i -e "s/-Werror//" ./grub-core/Makefile
# sed -i -e "s/-Werror//" ./Makefile
# make && make install
# ln -s /usr/local/sbin/grub-install /sbin/grub-install
# ln -s /usr/local/sbin/grub-mkconfig /sbin/grub-mkconfig
```

**Note:**

If the error `-Werror` occurs, we recommend that you locate the error in the `makefile`, remove the `-Werror` option, and then try again.

7. Run the `grub-install --version` command to verify GRUB is updated to v1.99.

What to do next

1. After you update GRUB to v1.99, you can migrate your server to Alibaba Cloud by using the Cloud Migration tool.

2. (Optional) After your servers are successfully migrated to Alibaba Cloud, run the following commands to use the earlier version of GRUB.

```bash
# rm /sbin/grub-install
# rm /sbin/grub-mkconfig
# rm /boot/grub/grub.cfg
# mv /sbin/grub-old /sbin/grub
```
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. You can learn about our measures for protecting ECS instances against these vulnerabilities.

Context

The Meltdown and Spectre vulnerabilities exist in the Intel chips. Caused by the design flaw of the chip hardware, the vulnerabilities may lead to problems such as leakage of operating system kernel information, unauthorized access to system kernel data by applications, and more. 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 security vulnerability notice, describing the vulnerability details and impacts.

This topic describes the Alibaba Cloud public images that have been patched against these vulnerabilities, and how to disable the patches for better instance performance. The default security policy is as follows:

- To protect against the Meltdown vulnerability, Page Table Isolation (PTI) is enabled by default.
- To protect against the Spectre vulnerability, by default 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 enabled the Meltdown patch (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 above list is subject to change due to updates of Alibaba Cloud public images.

If you find enabling PTI impacts your instance performance, or you have other protective measures, you can disable PTI by following the steps below:

1. Connect to your instance.
2. Do the following according to your Linux distribution:
   - CentOS, Debian, OpenSUSE, Red Hat, SUSE Linux and Ubuntu: Add the kernel parameter `nopti`.
   - CoreOS: Run `vi /usr/share/oem/grub.cfg` to configure `pti=off`.
   - FreeBSD: Run `vi /boot/loader.conf` to configure `vm.pmap.pti=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 Spectre through Reptpoline and IBPB. Moreover, IBRS is disabled through the `noibrs` parameter. The following public images are involved:

• 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 above list is subject to change due to updates of Alibaba Cloud public images.

If you need to restore the default settings of your operating system, or you find the current settings impact your instance performance, or you have other protective measures, you can disable the Spectre patch by following the steps below:
1. Connect to your instance.

2. Perform the corresponding operation according to the instructions in the following table.

<table>
<thead>
<tr>
<th>Linux distribution</th>
<th>To restore the default settings of Alibaba Cloud images</th>
<th>To restore the default settings of operating systems</th>
<th>To disable the Spectre patch</th>
</tr>
</thead>
<tbody>
<tr>
<td>CentOS</td>
<td>Add the kernel parameter noibrs.</td>
<td>Remove the kernel parameter noibrs.</td>
<td>Add the kernel parameter spectre_v2=off.</td>
</tr>
<tr>
<td>Red Hat</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CoreOS</td>
<td>Run vi /usr/oem/share/grub.cfg to add the kernel parameter spectre_v2=off.</td>
<td>Remove the kernel parameter spectre_v2=off.</td>
<td></td>
</tr>
<tr>
<td>OpenSUSE</td>
<td>Add the kernel parameter spectre_v2=off.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Debian</td>
<td>Retpoline and IBPB are enabled by default.</td>
<td>No need to modify the settings.</td>
<td></td>
</tr>
<tr>
<td>Ubuntu</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SUSE Linux</td>
<td>Retpoline is enabled by default.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FreeBSD</td>
<td>Add the kernel parameter hw. ibrs_disable.</td>
<td>Remove the kernel parameter hw. ibrs_disable.</td>
<td>Add the kernel parameter hw. ibrs_disable.</td>
</tr>
</tbody>
</table>

Note:
The kernel parameter noibrs does not work for OpenSUSE and CoreOS. You need to set spectre_v2=off for them.

3. Restart the instance.

How to detect whether protections are enabled

1. Connect to your instance.

2. From GitHub spectre-meltdown-checker Repo, obtain the spectre-meltdown-checker.sh script.

3. Run the following commands in your instance:

```
chmod +x spectre-meltdown-checker.sh
```
4. Judge whether the Meltdown or Spectre patch has been enabled according to the script prompts.

Reference

For the following operating systems, you can go to their website for more details:

- Red Hat
- SUSE Linux
- Ubuntu