Image Management Service

FAQs

Issue   29
Date   2023-10-31

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process.* For details about this process, visit the following web page:
https://www.huawei.com/en/psirt/vul-response-process
For vulnerability information, enterprise customers can visit the following web page:
https://securitybulletin.huawei.com/enterprise/en/security-advisory

Contents

1 Image Consulting

1.1 Basic Concepts

Images are classified as public, private, KooGallery, and shared.

Image Type	Description
Public	A public image is a standard, widely used image. It contains an OS and preinstalled public applications and is available to all users. Public images are very stable and their OS and any included software have been officially authorized for use. If a public image does not contain the environments or software you need, you can use a public image to create an ECS and then deploy the required environments or software on it.

Public images include the following OSs to choose from: Huawei Cloud EulerOS, CentOS, Debian, openSUSE, Fedora, Ubuntu, EulerOS, and CoreOS.

For more information about public images, see **Managing Public Images**. |

Image Type	Description
Private	A private image contains an OS or service data, preinstalled public applications, and a user's personal applications. Private images are only available to the users who created them. A private image can be a system disk image, data disk image, ISO image, or full-ECS image. • A system disk image contains an OS and preinstalled software for various services. You can use a system disk image to create ECSs and migrate your services to the cloud. • A data disk image contains only service data. You can use a data disk image to create EVS disks and use them to migrate your service data to the cloud. • An ISO image is created from an external ISO image file. It is a special image that is not available on the ECS console. • A full-ECS image contains an OS, preinstalled software, and service data. A full-ECS image is created using differential backups and the creation takes less time than creating a system or data disk image that has the same disk capacity.
Shared	A shared image is a private image another user has shared with you. For more information about shared images, see **Sharing Images**.
KooGallery	KooGallery is an online store where you can purchase third-party images that have the OS, application environments, and software preinstalled. You can use these images to deploy websites and application development environments in just a few clicks. No additional configuration is required. KooGallery images are provided by service providers who have extensive experience in configuring and maintaining cloud servers. All the images are thoroughly tested and have been approved by Huawei Cloud KooGallery and service providers before being published.

You can modify an image, share images, export images, encrypt images, replicate images within a region, replicate images across regions, export an image list, and delete images.

Table 1-1 Managing private images

Feature	Description	Helpful Link
Modifying an image	To facilitate private image management, you can modify the following attributes of an image: name, description, minimum memory, maximum memory, and advanced functions such as NIC multi-queue and SR-IOV driver.	**Modifying an Image**
Sharing images	You can share an image with other Huawei Cloud accounts. These accounts can use your shared private image to quickly create ECSs or EVS disks.	• **Sharing Images** • **Image Sharing FAQs**
Exporting images	You can export private images to your OBS bucket and download them to your local PC for backup.	**Exporting an Image**
Encrypting images	You can create encrypted images to improve data security. The encryption mode is KMS envelope encryption. Encrypted images can be created from external image files or encrypted ECSs.	• **Encryption Method** • **Creating Encrypted Images**
Replicating images within a region	By replicating images within a region, you can convert encrypted and unencrypted images into each other or enable some advanced features, for example, quick instance provisioning.	**Replicating Images Within a Region**
Replicating images across regions	You can replicate private images created in one region to another region. Cross-region image replication is supported within a single account. Shared images can be replicated across regions between different accounts.	**Replicating Images Across Regions**
Tagging an image	You can tag your private images for easy management and search.	**Tagging an Image**
Exporting image list	You can export the public or private image list in a given region in CSV format, facilitating local maintenance and query.	**Exporting Image List**

Feature	Description	Helpful Link
Deleting images	You can delete images that will be no longer used. Deleting an image does not affect the ECSs created from that image.	**Deleting Images**

1.2 How Do I Select an Image?

When creating an ECS or a BMS, you can select an image based on the following factors:

- **Region and AZ**
- **Image Type**
- **Image Fee**
- **OS**

Region and AZ

An image is a regional resource. You cannot use an image to create an instance in a different region. For example, when creating an instance in region A, you can only select an image that is already in region A. For more regions, see **Region and AZ**.

If you want to use an image in another region to create an instance, copy the image to the current region first. For details, see **Replicating Images Across Regions**.

Image Type

Images are classified into public, private, KooGallery, and shared images.

Table 1-2 Image types

Image Type	Description	Availability/ Security	Billing
Public	A public image is a standard, widely used image. It contains an OS and preinstalled public applications and is available to all users. Public images are very stable and their OS and any included software have been officially authorized for use.	High	Free

Image Type	Description	Availability/ Security	Billing
KooGallery	KooGallery is an online store where you can purchase third-party images that have the OS, application environments, and software preinstalled. You can use these images to deploy websites and application development environments in just a few clicks. No additional configuration is required.	Medium high	Free/Charged
Private	A private image contains an OS or service data, preinstalled public applications, and a user's personal applications. Private images are only available to the users who created them.	Medium	Free
Shared	A shared image is a private image another user has shared with you.	Low	Free

You can select an image as follows:

- If you only need an OS, select a public image.
- If you need a complete software environment, such as a Magento e-commerce system, select a KooGallery image.
- If you want to clone an existing ECS, select a private image.
- If you want to use an image shared by others, select a shared image.

Image Fee

You may be billed for using an image. For details, see **What Are the Billing Standards of IMS?**

OS

When selecting an OS, consider the following factors:

- Architecture types

System Architecture	Applicable Memory	Constraints
32-bit	Smaller than 4 GB	• If the instance memory is greater than 4 GB, a 32-bit OS cannot be used. • A 32-bit OS only allows addressing within a 4 GB memory range. An OS with more than 4 GB memory cannot be accessed.
64-bit	4 GB or larger	If your application requires more than 4 GB of memory or the memory may need to be expanded to more than 4 GB, use a 64-bit OS.

● OS types

OS Type	Applicable Scenario	Constraints
Windows	• Programs developed for Windows (for example, .NET). • Databases such as SQL Server. (You need to install the database.)	The system disk must be at least 40 GB, and there must be at least 1 GB of memory.
Linux	• High-performance server applications (for example, Web) and working with common programming languages such as PHP and Python. • Databases such as MySQL. (You need to install the database.)	The system disk must be at least 40 GB, and there must be at least 512 MB of memory.

1.3 What Do I Do If I Cannot Find a Desired Image?

Huawei Cloud supports the following public images: CentOS, Debian, openSUSE, Fedora, Ubuntu, EulerOS, and CoreOS. You can view OS types and versions on the **Public Images** page on the management console. If you cannot find a desired image, you have the following options:

● Download an image file from the official OS website and then use the file to create a private image. For details, see **Creating a Windows System Disk Image from an External Image File** or **Creating a Linux System Disk Image from an External Image File.** The external image file can be in the VMDK, VHD, QCOW2, RAW, VHDX, QED, VDI, QCOW, ZVHD2, or ZVHD format.

- If you already have an ISO file and the OS is supported by the cloud platform (for details, see **External Image File Formats and Supported OSs**), you can create a private image as follows:

    a. Create a private image on the management console. For details, see **Creating a Windows System Disk Image from an ISO File** or **Creating a Linux System Disk Image from an ISO File**.

    b. Use VirtualBox to create a private image. For details, see **Creating a Windows Image Using VirtualBox and an ISO File** or **Creating a Linux Image Using VirtualBox and an ISO File**.

- If the image belongs to another tenant, ask the tenant to share it with you. For details about image sharing, see **Sharing Specified Images**.

- You can find private images in KooGallery.

If after trying all of these methods, you are still unable to obtain the desired image, you are advised to **create a service ticket** to contact Huawei Cloud technical support.

1.4 What Do I Do If I Want to Set Up an OpenVPN or PyTorch Environment But No Public Images Containing OpenVPN or PyTorch Are Available?

A public image does not contain applications such as OpenVPN and PyTorch. You need to manually set up the environment or install the applications from an image in KooGallery.

1.5 How Do I Increase the Image Quota?

What Is Quota?

Quotas can limit the number or amount of resources available to users, such as the maximum number of ECSs or EVS disks that can be created.

If the existing resource quota cannot meet your service requirements, you can apply for a higher quota.

How Do I View My Quotas?

1. Log in to the management console.

2. Click ⊙ in the upper left corner and select the desired region and project.

3. In the upper right corner of the page, choose **Resources** > **My Quotas**.

    The **Service Quota** page is displayed.

Figure 1-1 My Quotas
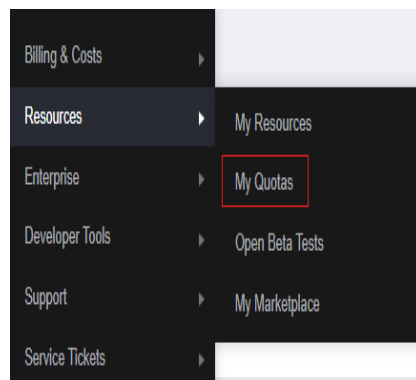
4. View the used and total quota of each type of resources on the displayed page.

    If a quota cannot meet service requirements, apply for a higher quota.

How Do I Apply for a Higher Quota?

1. Log in to the management console.
2. In the upper right corner of the page, choose **Resources** > **My Quotas**.

    The **Service Quota** page is displayed.

Figure 1-2 My Quotas
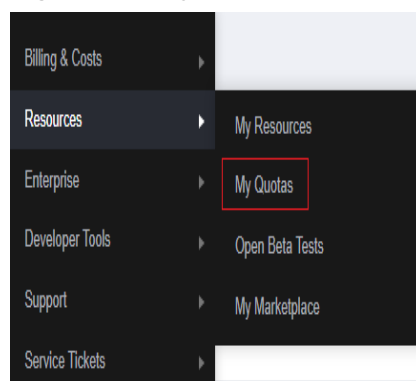
3. Click **Increase Quota** in the upper right corner of the page.

Figure 1-3 Increasing quota

4. On the **Create Service Ticket** page, configure parameters as required.

   In the **Problem Description** area, fill in the content and reason for adjustment.

5. After all necessary parameters are configured, select **I have read and agree to the Ticket Service Protocol and Privacy Statement** and click **Submit**.

1.6 What Are the Differences Between Images and Backups?

CBR and Image Management Service (IMS) have some complementary functions and can be used together in certain scenarios. Like CBR, IMS can also be used to back up ECSs.

Differences Between Backups and Images

Table 1-3 lists the differences between them.

Table 1-3 Differences between backups and images

Item	CBR	IMS
Concept	A backup contains the status, configuration, and data of a cloud server or disk stored at a specific time point for recovery in case of a fault. It is used to ensure data security and improve availability.	An image provides all information required for starting a cloud server. It is used to create a cloud server and deploy software environments in batches. A system disk image contains an OS and pre-installed application software for running services. A data disk image contains service data. A full-ECS image contains data of the system disk and data disks.

Item	CBR	IMS
Usage method	- Data storage location: Unlike server or disk data, backups are stored in OBS. Deleting a disk will not clear its backups. - Operation object: A server or disk can be backed up at a given point in time. CBR supports automatic backup and automatic deletion by configuring backup policies. - Usage: Backups can be used to restore data to the original server or disk, or to create a new disk or full-ECS image. - Support exporting to a local PC: No	- Data storage location: Unlike server or disk data, backups are stored in OBS. If a server or disk that is created using an image is deleted, the image will not be cleared. - Operation object: The system disk and data disks of a server can be used to create private images. You can also create private images using external image files. - Usage: System disk images or full-ECS images can be used to create new servers, and data disk images can be used to create new disks for service migration. - Support exporting to a local PC: Yes However, full-ECS images cannot be exported to a local PC.
Application scenarios	- Data backup and restoration - Rapid service deployment and migration	- Server migration to the cloud or between clouds - Deploying a specific software environment - Deploying software environments in batches - Backing up server operating environments
Advantages	Supports automatic backup. Data on a server or disk at a certain time point can be retained periodically or quantitatively. You can back up on-premises VMware VMs, synchronize the backups to the cloud, and then use the backups to restore data to new ECSs.	Supports system disk backup. You can import the data disk image of a local server or a server provided by another cloud platform to IMS and then use the image to create an EVS disk.

☐ NOTE

Although backups and images are stored in OBS, you cannot view backup and image data in OBS, because they do not occupy your resources. Backup fees are charged according to the CBR billing standards, and image storage fees are charged according to the OBS billing standards.

Relationship Between Backups and Images

1. You can use an ECS backup to create a full-ECS image.

2. Before creating a full-ECS image for an ECS, you need to back up the target ECS.

3. A backup is compressed when it is used to create an image, so the size of the generated image may be smaller than the backup size.

1.7 Can I Tailor an Image?

When you import an external image file, you are advised to import the image that contains the official OS release version. Do not tailor or highly customize the release version. Otherwise, problems may occur.

OS vendors do not always update OS release versions regularly. Some versions are no longer maintained, and these deprecated versions no longer receive security patches. Ensure that you read the update notifications from OS vendors and update your OS so that it runs properly.

1.8 How Do I Migrate an ECS to a Different Region of Another Account?

You can perform the migration in either of the following ways:

● You can use the ECS to create a private image, migrate the image to a different region of another account, and then use the image to create a new ECS. You can migrate a private image in either of the following ways:

– Replicate the image to another region of the same account and share it with another account.
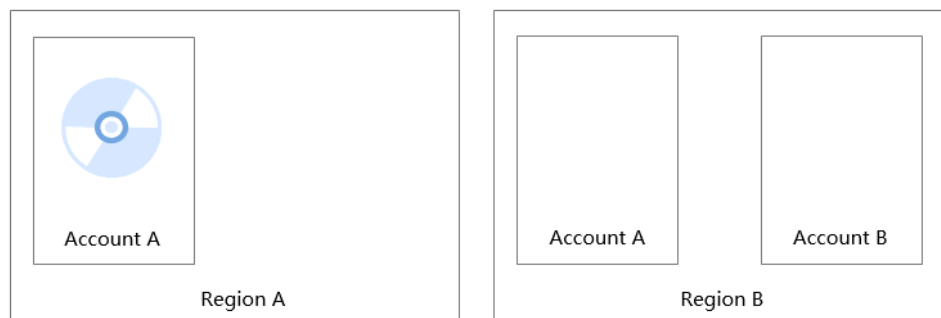
– Share the image with another account in the same region. Under the target account, accept the shared image, replicate it as a private image, and replicate it to another region.
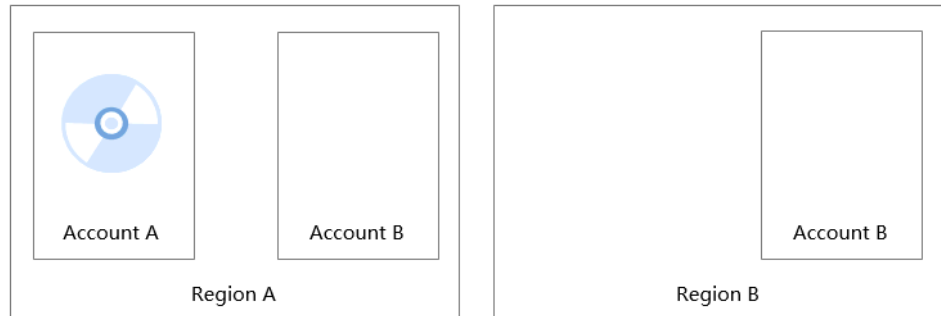
For details about cross-region image replication, image sharing, and replication of shared images, see **Replicating Images Across Regions**, **Sharing Specified Images**, **Replicating a Shared Image**.

- Server Migration Service (SMS):

  SMS is a Physical to Virtual (P2V) or Virtual to Virtual (V2V) migration service that migrates VMs on x86 physical servers, private cloud, or public cloud to Huawei Cloud ECSs. For details, see **Migrating Huawei Cloud ECSs from Multiple Accounts to a Single Account**.
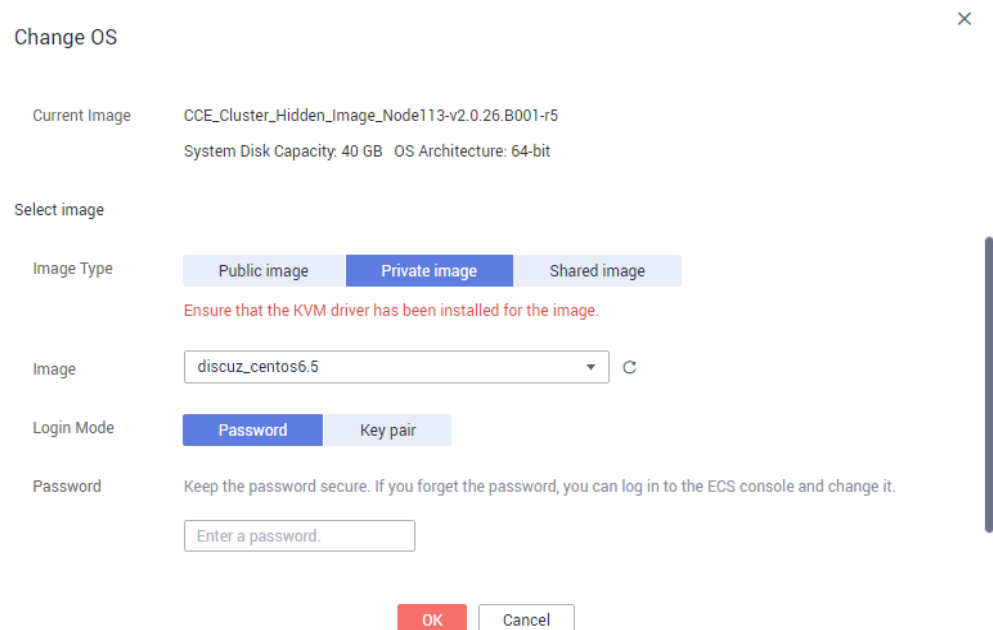
1.9 How Can I Back Up the Current Status of an ECS for Restoration in the Case of a System Fault?

You can back up the ECS in any of the following ways:

- (Recommended) Use CBR to create a scheduled backup task for the ECS. If the ECS fails, select a backup corresponding to the time you want the ECS to restore to, create a full-ECS image from the backup, and use the image to apply for a new ECS or to reinstall the OS.

- Create a system disk image from the ECS. If the ECS fails, use the system disk image to apply for a new ECS or to reinstall the OS.

- Create a snapshot for the system disk of the ECS. If the ECS fails, you can roll it back from the snapshot.

1.10 How Can I Apply a Private Image to an Existing ECS?

- You can change the OS of the ECS later if the created private image is in the same region as the ECS. When you change the OS, select the created private image, as shown in **Figure 1-4**. For details about how to change the OS, see **Changing the OS**.

Figure 1-4 Changing the OS

- If the created private image and the ECS are in different regions, replicate the private image to the region where the ECS is located, and then change the OS of the ECS as described in the previous item. For details about cross-region image replication, see **Replicating Images Across Regions**.

1.11 Can I Import Data from a Data Disk Image to a Data Disk?

No.

A data disk image can only be used to apply for a new disk and its data cannot be imported to a disk. To import the data, perform the following operations:

1. Use the data disk image to create a temporary disk.
2. Attach the temporary disk to the ECS where the target disk is located.
3. Copy data from the temporary disk to the target disk. Then, delete the temporary disk.

1.12 Can I Use Private Images of Other Tenants?

Yes.

Other tenants can share a private image with you. You can use it after accepting it. For details about image sharing, see **Sharing Specified Images**.

2 End-of-Support for OSs

2.1 What Do I Do If CentOS Linux Is No Longer Maintained?

CentOS has planned to stop maintaining CentOS Linux. Huawei Cloud will stop providing CentOS Linux public images. This section describes the impacts and tells you how to address the situation.

Background

On December 8, 2020, CentOS announced its plan to stop maintaining CentOS Linux and launched CentOS Stream. For more information, see **CentOS Project shifts focus to CentOS Stream**.

CentOS Linux 8 ended on December 31, 2021, and CentOS Linux 7 will end on June 30, 2024. CentOS Linux 9 and later versions will not be released, and patches will no longer be updated.

Impacts

CenterOS Linux users will be affected as follows:

- After December 31, 2021, CentOS Linux 8 users will not be able to obtain any maintenance or support services, including problem fixing and function updates.
- After June 30, 2024, CentOS Linux 7 users will not be able to obtain any maintenance or support services, including problem fixing and function updates.

Huawei Cloud users will be affected as follows:

- CentOS Linux 8 public images will continue for a certain time. ECSs created from CentOS Linux 8 images will not be affected, but the images will no longer be updated.
- Huawei Cloud will synchronize with CentOS for the support of CentOS Linux. After December 31, 2021, support services will no longer be available for CentOS 8. The support for CentOS 7 will continue until June 30, 2024.

Solution

You can change or migrate the OS so that the services originally running in CentOS Linux can continue to run in other OSs.

For details about how to change to Debian or Ubuntu, see **Changing the OS**.

- Change CentOS Linux to one of those listed in **Table 2-2**.

    If you want to change the ECS OS and the software is loosely coupled with the OS, change it. This does not affect the ECS configurations (such as NICs, disks, and VPNs).

    - For details about how to change to Huawei Cloud EulerOS, see **Changing an OS to Huawei Cloud EulerOS**.
    - For details about how to change to Debian or Ubuntu, see **Changing the OS**.

- Migrate CentOS Linux to Huawei Cloud EulerOS.

    If you want to change the OS but retain OS parameter settings, migrate the OS to Huawei Cloud EulerOS. This does not affect the ECS configurations (such as NICs, disks, and VPNs).

    For details, see **Migrating an OS to Huawei Cloud EulerOS**.

The following table describes the differences between the two methods.

Table 2-1 Differences between OS change and OS migration

Item	Changing the OS	Migrating the OS
Data backup	• Data in all partitions of the system disk will be cleared, so you are advised to back up the system disk data prior to an OS change. • Data in data disks remains unchanged.	• System disk data is not cleared, but you are still advised to back up the system disk data to prevent any exception in system software. • Data in data disks remains unchanged.
Custom settings	After the OS is changed, custom settings such as DNS and hostname will be reset and need to be reconfigured.	After the OS is migrated, custom settings such as DNS and hostname do not need to be reconfigured.

Table 2-2 Available OSs

OS	Description	Intended User
Huawei Cloud EulerOS	Huawei Cloud EulerOS (HCE OS) is an openEuler-based cloud operating system. Huawei Cloud EulerOS offers cloud native, high-performing, secure, and easy-to-migrate capabilities. This accelerates service migration to the cloud and promotes application innovation. You can use Huawei Cloud EulerOS to replace operating systems such as CentOS and EulerOS.	Individuals or enterprises that want to continue to use free images in an open source community
Debian and Ubuntu	They are Linux distributions that differ in use and compatibilities.	Individuals or enterprises that can afford the OS change costs

2.2 EOS Plan

If the End of Support (EOS) of an OS arrives, you can still use images containing this OS, but Huawei Cloud will no longer provide technical support for these images, such as locating new problems and rectifying defects.

This section provides the OS EOS plan.

- **HuaweiCloudEulerOS**
- **EulerOS**
- **CentOS**
- **Debian**
- **Ubuntu**
- **Red Hat**
- **FreeBSD**
- **OpenSUSE**
- **SUSELinux**
- **Fedora**
- **RockyLinux**
- **AlmaLinux**
- **WindowsServer**

📖 NOTE

- EulerOS and Huawei Cloud EulerOS are developed by Huawei which provides technical support for the OSs until their end of life (EOL).
- For third-party OSs, when their EOL arrives, Huawei Cloud will stop providing technical support for the images that contain these OSs.

OS EOS

- Huawei Cloud EulerOS

Version	EOS Date
Huawei Cloud EulerOS 2.0	2028-06-30
Huawei Cloud EulerOS 1.1	2026-06-30

- EulerOS

Version	EOS Date
EulerOS 2.0SP8	2024-06-30
EulerOS 2.0SP5	2023-06-30
EulerOS 2.0SP3	2022-09-30
EulerOS 2.0SP2	2021-12-30
EulerOS 2.0SP1	2020-12-30

- CentOS

Version	Mainstream End Date	Extended End Date
CentOS 8	2021-12-31	2021-12-31
CentOS 7	2020-08-06	2024-06-30
CentOS 6	2017-05-10	2020-11-30

- Debian

Version	EOS Date
Debian 13	Unknown
Debian 12	Unknown
Debian 11	Unknown
Debian 10	2022-09-10
Debian 9	2020-07-18
Debian 8	2018-06-17
Debian 7	2016-04-25

- Ubuntu

Version	EOS Date
Ubuntu 22.04 LTS	2032-04
Ubuntu 20.04 LTS	2030-04
Ubuntu 18.04 LTS	2028-04
Ubuntu 16.04 LTS	2026-04
Ubuntu 14.04 LTS	2024-04

● Red Hat

Version	EOS Date
Red Hat 9	2027-05-31
Red Hat 8	2024-05-31
Red Hat 7	2019-08-06
Red Hat 6	2016-05-10

● FreeBSD

Version	EOS Date
FreeBSD 13.0	Three months after the release of FreeBSD 13.1
FreeBSD 12.3	2022-08-21
FreeBSD 12.2	2022-03-31
FreeBSD 12.1	2021-01-31
FreeBSD 12.0	2020-02-04
FreeBSD 11.4	2021-09-30
FreeBSD 11.3	2020-09-30
FreeBSD 11.2	2019-10-31
FreeBSD 11.1	2018-09-30
FreeBSD 11.0	2017-11-30

● OpenSUSE

Version	EOS Date
OpenSUSE 15.3	2022-11-30
OpenSUSE 15.2	2022-01-04

Version	EOS Date
OpenSUSE 15.1	2021-02-02
OpenSUSE 15.0	2019-12-03
OpenSUSE 42.3	2019-07-01
OpenSUSE 42.2	2018-01-26
OpenSUSE 42.1	2017-05-17

- SUSE Linux

Version	Mainstream End Date	Extended End Date
SUSE Linux Enterprise Server 15 SP4	Six months after the release of SUSE Linux Enterprise Server 15 SP5	Unknown
SUSE Linux Enterprise Server 15 SP3	2022-12-31	2025-12-31
SUSE Linux Enterprise Server 15 SP2	2021-12-31	2024-12-31
SUSE Linux Enterprise Server 15 SP1	2021-01-31	2024-06-31
SUSE Linux Enterprise Server 15	2019-12-31	2022-12-31
SUSE Linux Enterprise Server 12 SP5	2024-10-31	2027-10-31
SUSE Linux Enterprise Server 12 SP4	2020-06-30	2023-06-30
SUSE Linux Enterprise Server 12 SP3	2019-06-30	2022-06-30
SUSE Linux Enterprise Server 12 SP2	2018-03-31	2021-03-31
SUSE Linux Enterprise Server 12 SP1	2017-05-31	2020-05-31
SUSE Linux Enterprise Server 12	2016-06-30	2019-07-01

- Fedora

Version	EOS Date
Fedora 35	2022-12-13

Version	EOS Date
Fedora 34	2022-06-07
Fedora 33	2021-11-30
Fedora 32	2021-05-25
Fedora 31	2020-11-24
Fedora 30	2020-05-26
Fedora 29	2019-11-26
Fedora 28	2019-05-28
Fedora 27	2018-11-30

- Rocky Linux

Version	EOS Date
Rocky Linux 8.5	2031-11-14

- AlmaLinux

Version	EOS Date
AlmaLinux 8.5	2031-11

- Windows Server

Version	Mainstream End Date	Extended End Date
Windows Server 2019	2024-01-09	2029-01-09
Windows Server 2016	2022-01-11	2027-01-12
Windows Server 2012	2018-10-09	2023-10-10
Windows Server 2012 R2	2018-10-19	2023-10-10
Windows Server 2008	Ended	Ended
Windows Server 2003	Ended	Ended

3 Image Creation

3.1 Image Creation FAQs

How Can I Use an ECS to Quickly Provision Identical ECSs?

If you have an ECS with applications deployed, you can use the ECS to create a private image and then use the image to create identical ECSs. In this way, you do not need to deploy applications repeatedly.

- **Creating a System Disk Image from a Windows ECS**
- **Creating a System Disk Image from a Linux ECS**
- **Creating an ECS from an Image**

How Many Private Images Can I Create Under an Account?

At present, you can create up to 50 private images under a given account within a region. If you need to create more than 50 private images, submit a service ticket to increase your quota. For details, see **How Do I Increase the Image Quota?**

Do I Have to Stop the ECS Before Using It to Create a Private Image?

No. You can create an image from a running ECS. However, if data is written to the ECS during image creation, that new data will not be included in the created image.

Where Can I View the Image Creation Progress? How Long Does It Take to Create an Image?

Log in to the management console. Choose **Compute** > **Image Management Service** and click the **Private Images** tab. Monitor the image creation progress in the **Status** column.

The image creation involves the installation of Xen and KVM drivers, OS kernel loading, and GRUB boot configuration, which may take a long time. In addition, the network speed, image file type, and disk size have an impact on how long image creation takes.

Can I Select a Private Image Created Under a Subaccount When Creating an ECS Under the Main Account?

Yes.

Private images created under a subaccount are visible to the main account and all the other subaccounts (if any) under the main account.

- If the private image is a system disk image or full-ECS image, you can select **Private Image** for **Image** when creating an ECS. Then, select this image from the drop-down list.
- If the private image is a data disk image, select **Create from image** for **Select Data Source** when creating an EVS disk. Then, select this image in the displayed dialog box.

In addition, private images created under the main account are visible to all of its subaccounts.

3.2 Full-ECS Image FAQs

What Is a Full-ECS Image?

A full-ECS image contains the OS, applications, and service data of an ECS. Generally, a full-ECS image is used to migrate all data of an ECS. For example:

- Sharing an ECS with other tenants
- Migrating an ECS from a region to another (for example, from CN East-Shanghai1 to CN South-Guangzhou)
- Migrating data from an old ECS to a new one

Why Do I Have to Select a Vault When Creating a Full-ECS Image? Do I Need to Pay for the Vault?

When creating a full-ECS image from a CBR backup, you must select a vault. The vault is where your images and backups are stored. You need to pay for the vault.

When creating a full-ECS image from a CSBS backup, the vaults storing CSBS backups are not open to users but still need to be billed.

Therefore, no matter which backup type you select, you need to pay for the vault. Selecting a vault does not mean that you need to pay extra fees.

Where Can I View the Data Disk Information of a Successfully Created Full-ECS Image?

After a full-ECS image is created, only the system disk information (**Disk Capacity**) is displayed in the image list and image details. You can view the data disk information on the CSBS or CBR console, depending on where the full-ECS image is created from.

The following describes how to view the data disk details in CBR:

1. In the private image list, click the full-ECS image name.

Image details are displayed.

2. Locate **Source** and click the backup ID following it.

The CBR details page is displayed.

Figure 3-1 Image details

Name	cbr_switch_test	ID	ecc65532-7431-49e0-971a-b1912f4e1e2b
Image Type	Full-ECS image	Disk Capacity (GB)	--
OS	Ubuntu 16.04 server 64bit	Status	✓ Normal
Minimum Memory	1 GB	Maximum Memory	4096 GB
Released ⊘	No	Created	2023/01/14 09:05:42 GMT+08:00
Completed	2023/01/14 09:05:50 GMT+08:00	Source	CBR backup manualbk_vault-d9cd-aaa0
Description	--	OS Type	Linux
NIC Multi-Queue	Supported	Enterprise Project	default

3. Click the **Disk Backup** tab. Details about the system disk and data disks are displayed.

Figure 3-2 Disk backup

Details	Disk Backup	Share List	Replication History		
Name	**Status**	**Disk Name**	**Used As**		**Disk Capacity (GB)**
manualbk_3c43_ecs-37389...	✓ Available	ecs-373896-volume-0000	System Disk		40
manualbk_3c43_ecs-37389...	✓ Available	ecs-373896-volume-0001	Data Disk		100

What Are the Restrictions on Using a Full-ECS Image?

- A full-ECS image cannot be published in KooGallery.
- A full-ECS image cannot be exported. You are advised to create images for the system disk and data disks separately and then export the images.
- A full-ECS image is shareable only when it is created from a CBR backup or from an ECS that has never had a CSBS backup.
- A full-ECS image cannot be replicated within the same region.

3.3 How Can I Use a Backup to Create an EVS Disk or ECS?

You can use CSBS backups to create ECSs and use VBS backups to create EVS disks.

- CSBS backups cannot be directly used to create ECSs. You need to use a backup to create a private image and then use the private image to create ECSs.

  For details about how to create a private image from a CSBS backup, see **Creating a Full-ECS Image from a CSBS Backup**. For details about how to create ECSs from a private image, see **Creating an ECS from an Image**.

- VBS backups can be directly used to create EVS disks. For details, see **Using a Backup to Create a Disk**.

3.4 Is There Any Difference Between the Image Created from a CSBS/CBR Backup and That Created from an ECS?

No.

You can create a full-ECS image from an ECS, a CSBS backup, or a CBR backup.

When you create a full-ECS image from an ECS, the system first creates a backup for the ECS and then uses the backup to create an image. Therefore, the image is essentially created from an ECS backup no matter you use an ECS or a CSBS/CBR backup.

3.5 Why Can't I Find an ISO Image When I Want to Use It to Create an ECS or Change the OS of an ECS?

- An ISO image created from an ISO file is used only for creating a temporary ECS. It will not be available on the ECS console. You cannot use it to create ECSs or change ECS OSs. You need to install an OS on the temporary ECS and use that ECS to create a system disk image which can be used to create ECSs or change ECS OSs.
- You are not advised to use a temporary ECS as a normal ECS because it has limited functionality. For example, disks cannot be attached to it.

For details about how to create a private image using an ISO file, see:

- **Creating a Windows System Disk Image from an ISO File**
- **Creating a Linux System Disk Image from an ISO File**

3.6 How Do I Create a Full-ECS Image Using an ECS That Has a Spanned Volume?

An ECS used to create a Windows full-ECS image cannot have a spanned volume. If you attempt to create an image from an ECS with a spanned volume, when the image is used to create new ECSs, data may be lost.

If an ECS has a spanned volume, back up data in the spanned volume and then delete this volume from the ECS. Use the ECS to create a full-ECS image. Use the full-ECS image to create an ECS. Then, use the backup to create a spanned volume for the new ECS if necessary.

◫ NOTE

If a Linux ECS has a volume group or a logical volume consisting of multiple physical volumes, to ensure you do not lose any data, back up data in the volume group or logical volume and delete the volume group or logical volume before using this ECS to create a full-ECS image.

3.7 Why Is Sysprep Required for Creating a Private Image from a Windows ECS?

Why Is Sysprep Required?

For a user that needs to be added to a domain and uses the domain account to log in to Windows, Sysprep is required before a private image is created. Otherwise, the image will contain information about the original ECS, especially the SID. ECSs with the same SID cannot be added to a domain. If Windows does not require any user or ECS to be added to a domain, you do not need to run Sysprep.

⚠ **CAUTION**

- Before running Sysprep, ensure that Windows is activated.
- For details about Sysprep, visit **https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-vista/cc721940(v=ws.10)?redirectedfrom=MSDN**.

Restrictions on Running Sysprep

Sysprep can only be used for configuring a new Windows installation. You can run Sysprep multiple times to install and configure Windows. However, you can reset and activate a Windows OS only three times, and you are not allowed to use Sysprep to re-configure an existing Windows OS.

📖 **NOTE**

In the Windows command line, enter the following command to check how many times you can run Sysprep in the displayed **Windows Script Host** dialog box:

slmgr /dlv

If the value of **Remaining Windows rearm count** is **0**, you cannot run Sysprep.

3.8 What Do I Do If an ECS Created from a Windows Image Failed to Start After Running Sysprep?

Symptom

1. After Sysprep is executed, the following message is displayed when you start the ECS.

Figure 3-3 Message displayed
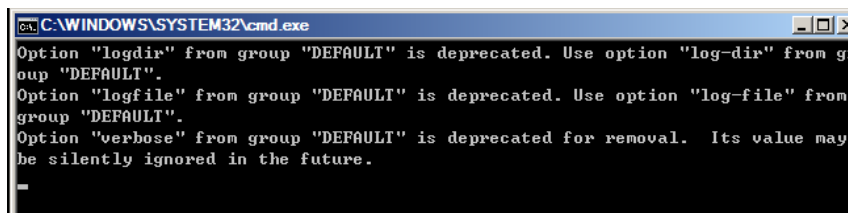
Then, the following information is displayed in the dialog box:

Windows could not parse or process the unattend answer file for pass [specialize]. A component or setting specified in the answer file does not exist. The error was detected while processing settings for component [Microsoft-Windows-Shell-Setup].

2. Click **OK**. The following information is displayed in the dialog box:
   The computer accidentally restarts or encounters an error. Windows installation cannot continue. Click OK to restart the computer and restart the installation.

3. Open **setupact.log** in **C:\Windows\Panther**. The log contains the following information.

Figure 3-4 Viewing ECS logs
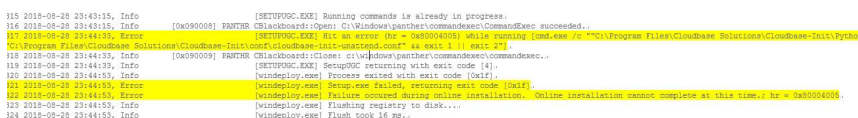
Solution

1. Create an ECS from a public image. (You are advised to use a public image to create another ECS because Sysprep can be executed only for certain times.)

2. Create an **Unattend.xml** file or modify the **Unattend.xml** file provided by the system.

   – If you create an **Unattend.xml** file, ensure that the created file is used when you run Sysprep. For details about the file, visit:

     ▪ **https://docs.microsoft.com/en-us/windows-hardware/ manufacture/desktop/update-windows-settings-and-scripts-create-your-own-answer-file-sxs**

     ▪ **https://docs.microsoft.com/en-us/windows-hardware/ manufacture/desktop/sysprep--system-preparation--overview**

   – If you modify the **Unattend.xml** file (in the **C:\Program Files\Cloudbase Solutions\Cloudbase-Init\conf** directory), delete the **RunSynchronous** part from the file.

Figure 3-5 Deleting the RunSynchronous part

3. Run Sysprep. For details, see **Running Sysprep**.

> **NOTICE**
>
> If you use the **Unattend.xml** file created by yourself, check the **Unattend.xml** path when running Sysprep to ensure that the newly created **Unattend.xml** file is used.

4. Create an image from the ECS where Sysprep has been executed.

3.9 What Do I Do If I Cannot Create an Image in ZVHD2 Format Using an API?

Symptom

When you create a ZVHD2 image using an API, the image is created in the ZVHD format.

Solution

Check whether your token contains the **op_gated_lld** role (**op_gated_lld** is the OBT tag, which can be viewed in the body of the response message of the API used to obtain a user token). The ZVHD2 image has the lazy loading feature. If the current environment does not support this feature or this feature is in the OBT phase, the ZVHD2 image will fail to be created.

Contact the customer service to ensure that the current environment supports lazy loading, obtain a new token, and use the new token to create an image.

4 Image Sharing

4.1 Image Sharing FAQs

How Many Tenants, Projects, or Organizations Can I Share an Image with?

A system disk image or data disk image can be shared with up to 128 tenants, but a full-ECS image can only be shared with up to 10 tenants.

How Many Images Can Be Shared with Me?

There is no limit.

Can I Share Images Between My Accounts at the Chinese Mainland Website and International Website?

Yes. You can share images between your accounts of the Chinese Mainland and International websites, but only in regions that are available on both websites. For example, you cannot share images in the CN North-Beijing1 region of the Chinese Mainland website with your account of the International website which does not have this region.

Do Shared Images Affect My Private Image Quota?

No.

I Shared an Image to an Account But the Account Did Not Accept or Reject the Image. Will My Image Sharing Quota Be Consumed?

No.

Where Can I View the Images Shared with Me?

Switch to the region where the shared image is located, choose **Service List** > **Compute** > **Image Management Service** > **Images Shared with Me**.

If you are a multi-project user, make clear which of your projects will receive the shared image. Switch to the region where the project resides and select the

project. Then, choose **Service List** > **Compute** > **Image Management Service** > **Images Shared with Me**.

If the image is not accepted, a red dot is displayed on the **Images Shared with Me** tab page (as shown in **Figure 4-1**) and a message is displayed, asking you whether to accept the shared image. After the image is accepted, it is displayed in the list on the **Images Shared with Me** tab page.

Figure 4-1 Images Shared with Me
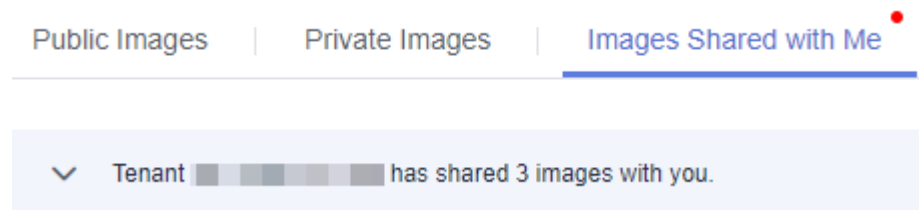
If I Want to Share a System Disk Image with Another Account, Should the Account Purchase an ECS in Advance?

No. The account can use the shared image to apply for ECSs.

Is There Any Restriction on the Region When I Create ECSs Using a Shared Image?

Yes. You can only create ECSs in the same region as the shared image.

Can I Share Images Shared with Me with Other Tenants?

You cannot directly share such images with other tenants. If you do need to do so, you can replicate a shared image to a private image and then share the private image.

Can I Use an Image I Have Shared with Others to Create an ECS?

Yes. After sharing an image with other tenants, you can still use the image to create an ECS and use the created ECS to create a private image.

What Are the Risks of Creating ECSs Using a Shared Image?

The image owner can view, stop sharing, or delete the image at any time. After the shared image is deleted, you will be unable to use the shared image to reinstall the OSs of the ECSs created from the shared image or create ECSs with the same configurations.

The cloud platform does not ensure the integrity or security of images shared by other accounts. For security reasons, you are advised to choose only images shared by trusted accounts.

What Are the Risks of Sharing Images with Other Tenants?

Data, files, and software may be disclosed. Before sharing an image, you must take care to delete any sensitive data or important files from the image. The

image recipient can use the shared image to create ECSs and use the created ECSs to create private images. If the created private images are shared with other tenants, any data leakage that occurs can be quite widespread.

How Do I Replicate an Image Between Projects in a Region?

Cross-region image replication allows you to replicate images between regions. Image sharing allows you to replicate images between projects in the same region.

In the **Share Image** dialog box, enter target project IDs, and click **OK**, as instructed in **Sharing Specified Images**. After the image is shared, switch to the target projects. On the **Image Management Service** > **Images Shared with Me** page, you can view the shared image to be accepted.

How Do I Share an Image Across Regions?

To share an image across regions, you can use either of the following methods:

- Replicate the image to the destination region and then share it.
- Share the image and then replicate it to the destination region.

For example, if you want to share a private image in the CN-Hong Kong region to the CN East-Shanghai2 region with another account, use either of the following methods:

Method 1:

1. Replicate the private image from the CN-Hong Kong region to the CN East-Shanghai2 region. In the CN East-Shanghai2 region, the image is named **copy_image**.

   For details, see **Replicating Images Across Regions**.

2. Share **copy_image** with the target account.

   For details, see **Sharing Specified Images**.

Method 2:

1. Share the private image with the target account in the CN-Hong Kong region.

   For details, see **Sharing Specified Images**.

2. After accepting the shared image, the account replicates it as **copy_image**.

   For details, see **Replicating a Shared Image**.

3. The account replicates **copy_image** from the CN-Hong Kong region to the CN East-Shanghai2 region.

   For details, see **Replicating Images Across Regions**.

Can I Specify a Region or an AZ for Sharing an Image?

No. When sharing an image, you can only specify a project ID. You cannot specify a region or an AZ. An image can only be shared within a given region, but once shared, it can be used in any AZ in that region.

Can I Restore My Data Disks from a Data Disk Image Shared by Another Account?

No. You can only use the shared image to apply for a new data disk and cannot use it to restore your existing data disks. However, you can use the new data disk for restoration by referring to **Can I Import Data from a Data Disk Image to a Data Disk?**

Can I Share My ECS and Its EIP with Another Account?

You can share an ECS through full-ECS image sharing but cannot share the EIP.

What Can I Do If I Want to Use a Rejected Image?

If you have rejected an image shared by another tenant, but now want to use it, two methods are available:

- Method 1

  Ask the image owner to add you to the tenants the image is shared with. For details, see **Adding Tenants Who Can Use Shared Images**.

- Method 2

  Accept the rejected image again. For details, see **Accepting Rejected Images**.

  ◯ NOTE

  If the image is also shared with your account or organization and is not refused, you can still use the image under the account or organization.

4.2 How Will I Be Billed for Sharing an Image?

- If it is a system or data disk image, the OBS storage is free.
- If it is a full-ECS image, you will be billed for the space used to store the CBR backup.

  ◯ NOTE

  Full-ECS images created from a CBR backup can be shared but those created from a CSBS backup cannot.

4.3 What Are the Differences Between Sharing Images and Replicating Images?

- Sharing images:

  You can only share images within a region with other users. To share an image across regions, replicate the image to the target region and then share it. For details, see **Sharing Images**.

- Replicating images:

  - In-region: You can convert encrypted and unencrypted images into each other or enable some advanced features (such as fast ECS creation from an image) using the in-region image replication function.

– Cross-region: Cross-region replication is applicable to cross-region server deployment or data backup. It is often used together with image sharing for cross-region, cross-account image replication.

The following table describes the details.

Scenario	Operation	Description	Helpful Links
Sharing	Share	The image is shared with another user in the same region. The target user can use the image (with the same ID as the source image) but the image owner is still the user who shared it.	For details, see **Sharing Specified Images**.
In-region replication under the same account	Replicate	This is used for conversion between encrypted images and unencrypted images or for enabling advanced features (such as fast ECS creation from an image).	For details, see **Replicating Images Within a Region**.
Cross-region replication under the same account	Replicate	After the replication is complete, a new image is generated in the target region. The new image has an ID that is different from the source image ID.	For details, see **Replicating Images Across Regions**.
Cross-region, cross-account replication	Replicate and share	Replicate the image to the target region and share it with other accounts.	For details, see **Replicating Images Across Regions** and **Sharing Specified Images**

4.4 What Do I Do If I Cannot Share My Images?

- Some images cannot be shared. Therefore, the **Share** option is not provided for them in the **Operation** column. The following images cannot be shared:
  - KooGallery images
  - Encrypted images
  - Full-ECS images created from a CSBS backup
- Images can only be shared within the same region. If you are attempting to share an image across regions, your attempt will fail.

  Solutions:
  - Solution 1: Replicate the image to the target region and then share it.
  - Method 2: Export the image and then import it to the target region.

Export the image to a local directory and then upload it to the account in the target region.

5 OS

5.1 How Do I Select an OS?

- Windows

  Used for development platforms or services that run Windows.

  The system disk must be at least 40 GB, and there must be at least 1 GB of memory.

  Internet Information Services (IIS) and SQL Server can be installed.

- Linux

  Used for development platforms or services that run Linux. CentOS and Ubuntu are provided. CentOS is recommended.

  The system disk must be no less than 40 GB, and the memory must be no less than 512 MB.

- OS selection for servers that require memory greater than 4 GB

  Because 32-bit OSs allow addressing only within a 4 GB memory range, if the required memory capacity is 4 GB or larger, select a 64-bit OS.

5.2 How Is BIOS Different from UEFI?

Table 5-1 Differences between the UEFI and BIOS boot modes

Boot Mode	Description	Highlight
BIOS	Basic Input Output System (BIOS) stores important basic input/output programs of ECSs, system settings, self-test programs upon system startup, and automatic startup programs.	Provides basic settings and control for ECSs.

Boot Mode	Description	Highlight
UEFI	Unified Extensible Firmware Interface (UEFI) is a specification that defines a software interface between an OS and platform firmware. UEFI can be used to automatically load an OS from a pre-boot operating environment.	Boots up or recovers from sleep state faster.

5.3 What Do I Do If I Cannot Change the Resolution of a Windows OS Booted in UEFI Mode?

Symptoms

The resolution of a Windows OS booted in UEFI mode cannot be changed in display settings.

Possible Causes

By default, x86 Windows cloud servers on Huawei Cloud are booted in BIOS mode. If users migrate Windows servers from other vendors or a local IDC, the servers may be booted in UEFI mode. The resolution of servers booted in UEFI mode cannot be changed in display settings.

Solutions

1. Log in to the Windows cloud server using VNC. Open the **Start** menu, click the **Power** button, and choose **Restart**. During the restart, press **Esc** on your keyboard quickly and repeatedly to enter the BIOS configuration.

```
OpenStack Nova
pc-i440fx-2.8                          2.00 GHz
0.0.0                                  8192 MB RAM


     Select Language          <Standard English>      This is the option
                                                       one adjusts to change
  ▶ Device Manager                                     the language for the
  ▶ Boot Manager                                       current system
  ▶ Boot Maintenance Manager

     Continue
     Reset




   ↑↓=Move Highlight        <Enter>=Select Entry
```
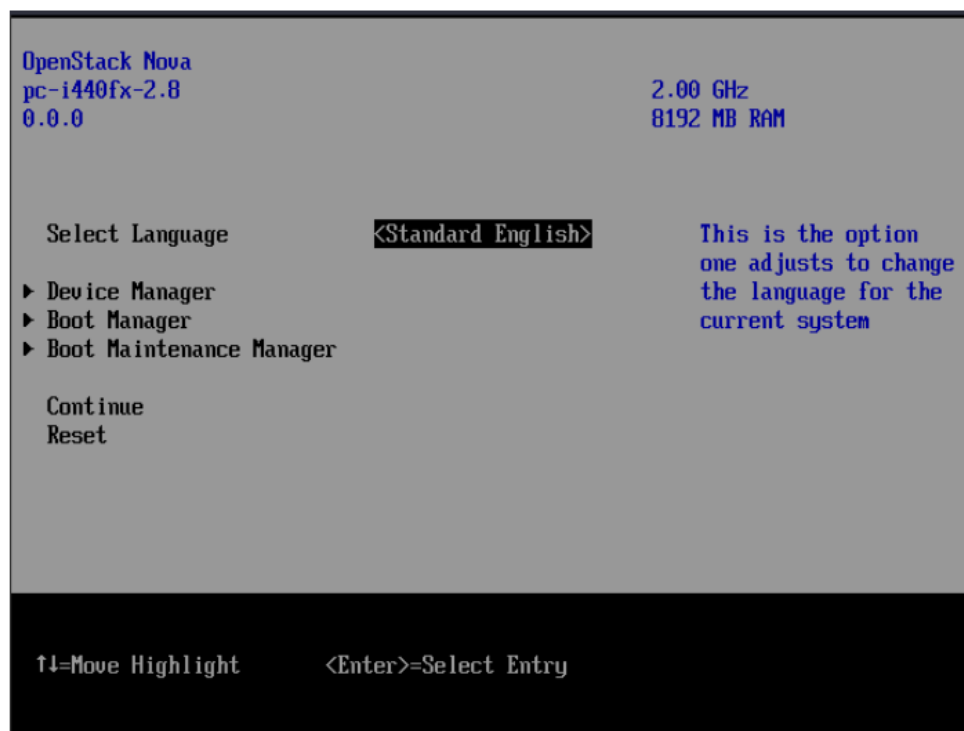
2. Use the up and down arrow keys on the keyboard to select **Device Manager** and press **Enter**.

```
                          Device Manager

     Devices List                                      List all the Driver
  ▶ Driver Health Manager                              Health instances to
  ▶ RAM Disk Configuration                             manage
  ▶ OVMF Platform Configuration
  ▶ iSCSI Configuration
  ▶ Network Device List


     Press ESC to exit.






   ↑↓=Move Highlight        <Enter>=Select Entry       Esc=Exit
```
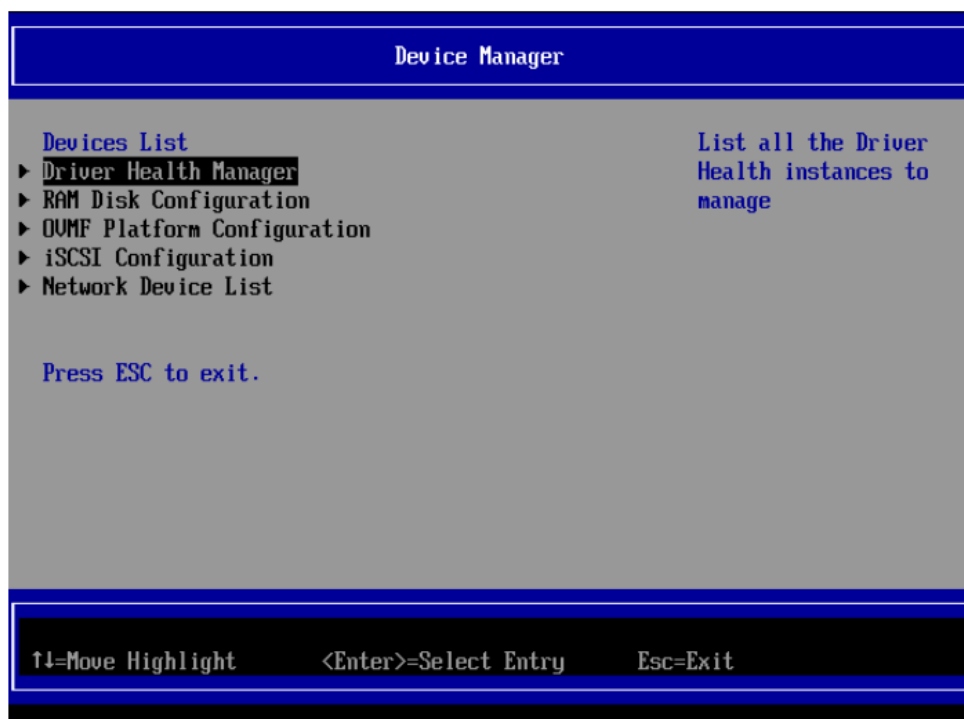
3. Use the up and down arrow keys to select **OVMF Platform Configuration** and press **Enter**.

Device Manager

Devices List
▶ Driver Health Manager
▶ RAM Disk Configuration
▶ OVMF Platform Configuration
▶ iSCSI Configuration
▶ Network Device List

Press ESC to exit.

Change various OVMF
platform settings.

↑↓=Move Highlight   <Enter>=Select Entry   Esc=Exit
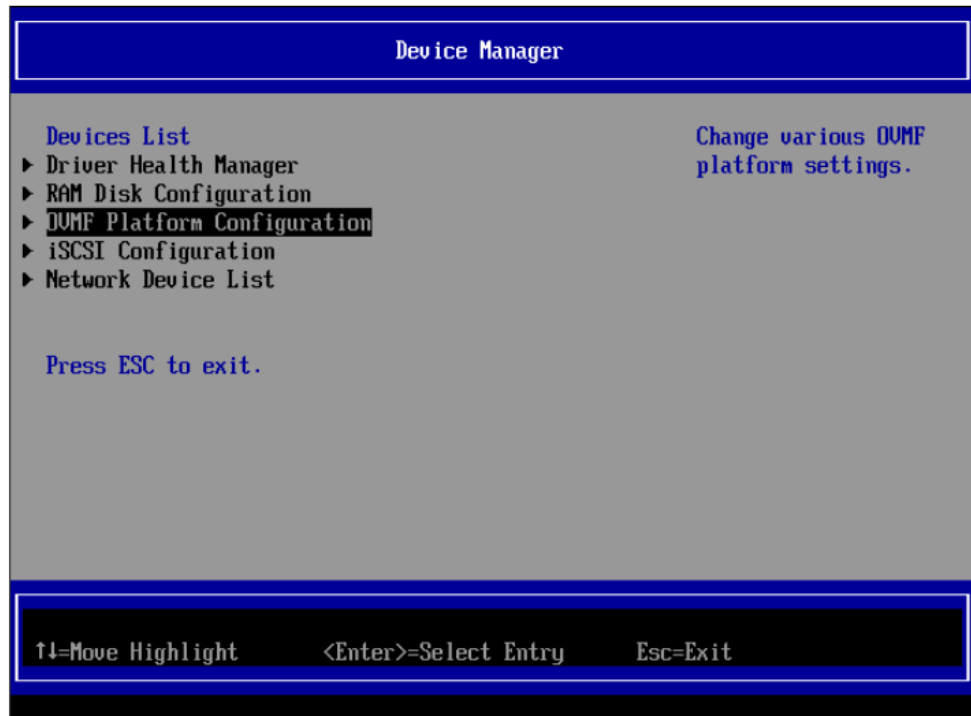
4. Use the up and down arrow keys to select **Change Preferred** (it is selected by default).

OVMF Settings

Preferred Resolution at   800x600
Next Boot
Change Preferred   <800x600>
Resolution for Next Boot
Commit Changes and Exit
Discard Changes and Exit

You can specify a new
preference for the
Graphics Console
here. The list is
filtered against the
video RAM size.

                    F9=Reset to Defaults   F10=Save
↑↓=Move Highlight   <Enter>=Select Entry   Esc=Exit

5. In the **Change Preferred** line, use the up and down arrow keys to change the resolution (for example, the resolution is changed from 800x600 to 1280x760), and press **Enter**.
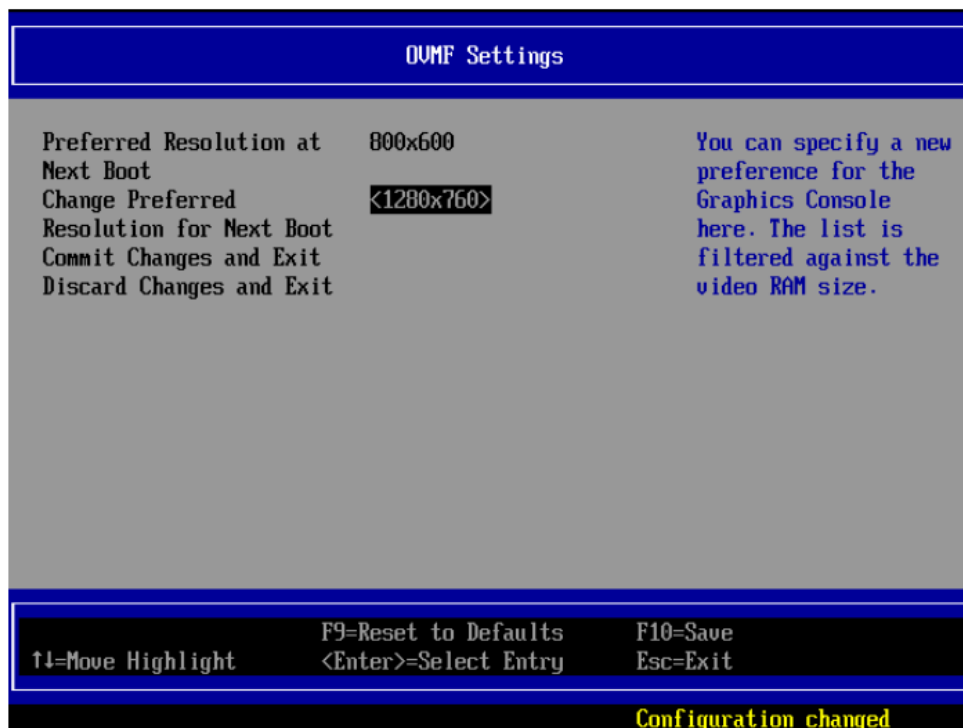
6. Use the up and down arrow keys to select **Commit Changes and Exit** and press **Enter** to save the settings and exit. Then, press **Esc** to exist the BIOS configuration.
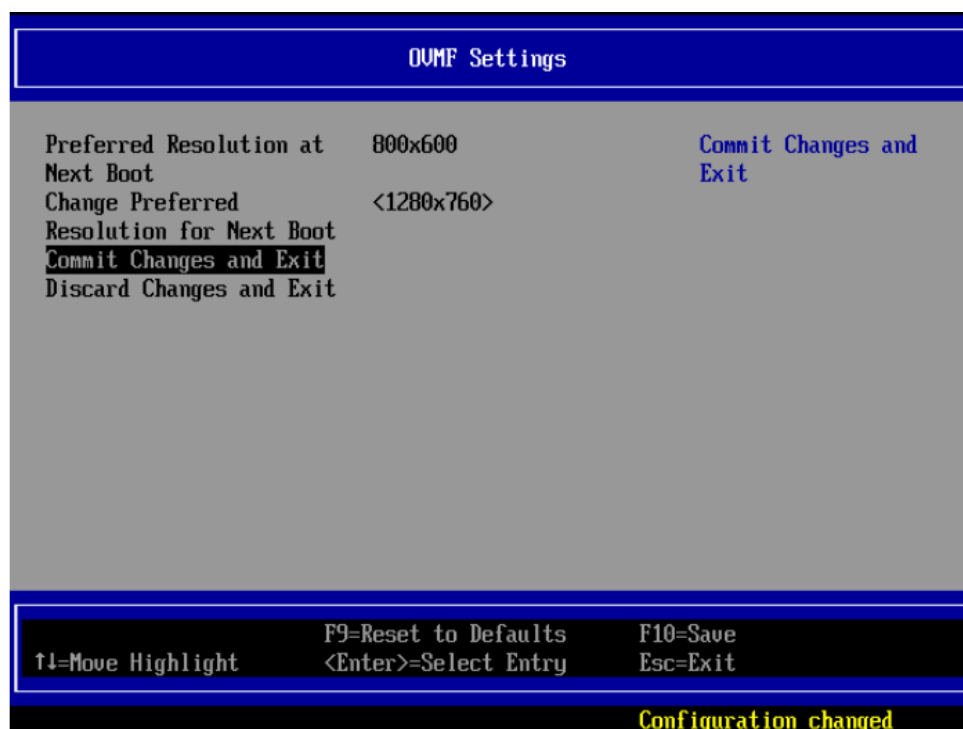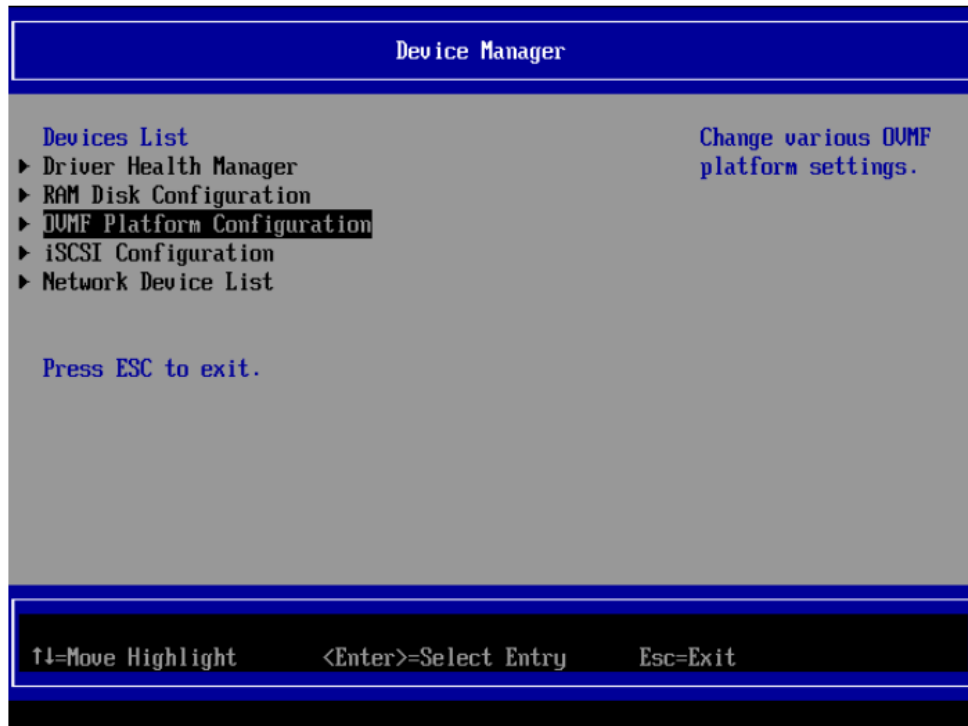
7. Use the up and down arrow keys to select **Reset** and press **Enter** to restart the cloud server.

 📖 **NOTE**

> You must select **Reset**. If you select **Continue**, you need to restart the cloud server again to make the BIOS configuration take effect.
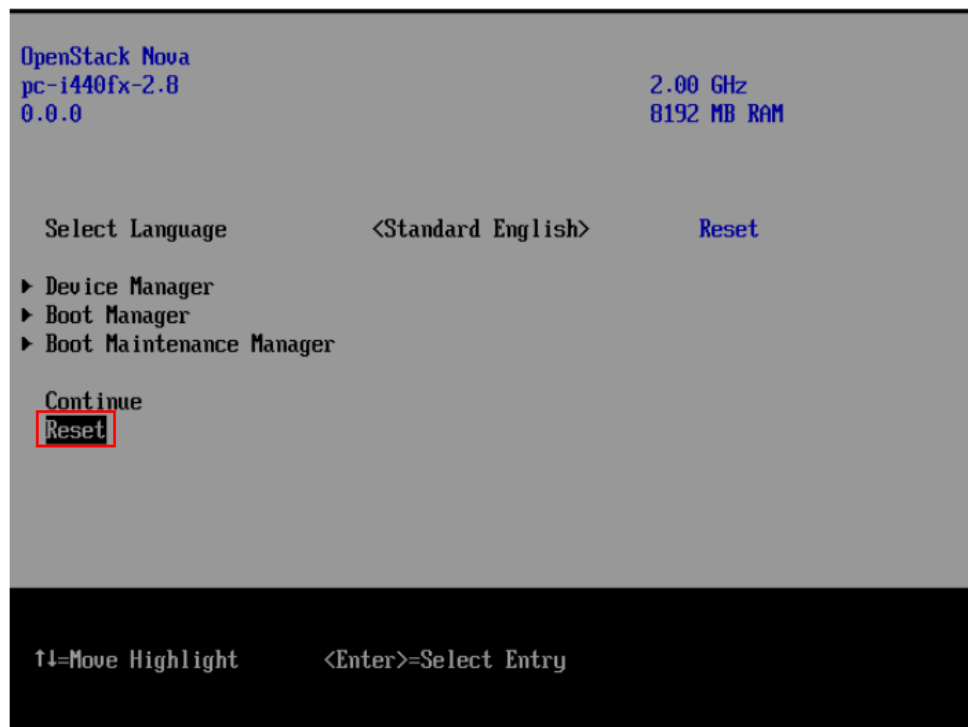
8. Log in to the cloud server and check the desktop resolution.

After logging in to the cloud server, right-click the desktop and choose **Display settings** from the shortcut menu. The desktop resolution is 1280x760 which is the same as that configured in BIOS.

5.4 How Do I Delete Redundant Network Connections from a Windows ECS?

Method 1

1. Press **Win+R**. In the displayed dialog box, enter **regedit** and press **Enter** to open the registry editor.

   📖 **NOTE**

   > Modifying a registry may cause a system startup failure. So, back up the registry before modifying it.

2. Open the following registry key:

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT \CurrentVersion\NetworkList\Profiles

   Click each item under **Profiles** and query the **Data** column of **ProfileName** in the right pane.

3. Double-click **ProfileName** and set **Value Data** to the name of a new network.

4. Restart the ECS for the change to take effect.

Method 2

1. Press **Win+R**. In the displayed dialog box, enter **regedit** and press **Enter** to open the registry editor.

   📖 **NOTE**

   > Modifying a registry may cause a system startup failure. So, back up the registry before modifying it.

2. Open the following registry keys:

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT \CurrentVersion\NetworkList\Profiles

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT \CurrentVersion\NetworkList\Signatures\Unmanaged

3. Delete the directories shown in the following figure.

Figure 5-1 Registry directory
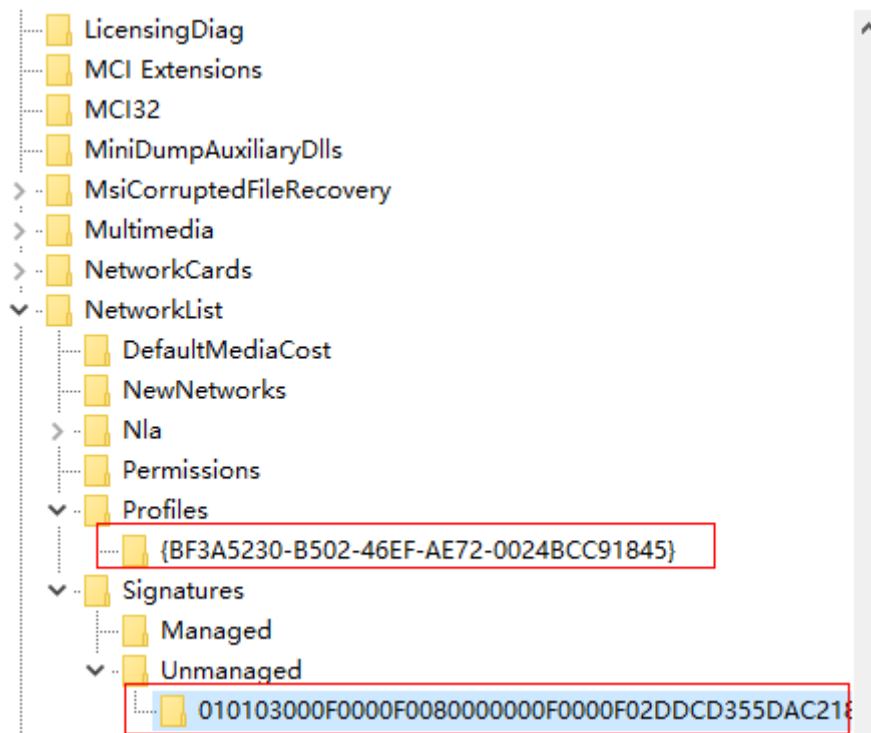
5.5 What Do I Do If an ECS Starts Slowly?

Symptom

If an ECS starts slowly, you can change the default timeout duration to speed up the startup.

Solution

1. Log in to the ECS.

2. Run the following command to switch to user **root**:

   sudo su

3. Run the following command to query the version of the GRUB file:

   rpm -qa | grep grub

   Figure 5-2 Querying the GRUB file version

4. Set **timeout** in the GRUB file to **0**.

   – If the GRUB file version is earlier than 2:

   Open **/boot/grub/grub.cfg** or **/boot/grub/menu.lst** and set **timeout** to **0**.

   – If the GRUB file version is 2:

   Open **/boot/grub2/grub.cfg** and set the value of **timeout** to **0**.

Figure 5-3 Modifying the timeout duration

5.6 What Do I Do If the One-Click Password Resetting Plug-In Failed to Start?

Symptom

The one-click password reset plug-in failed to start after it is installed.

Solution

Add the following content to the ECS configuration (the configuration file path varies depending on the OS. For details, see **Procedure**):

/CloudrResetPwdAgent/bin/cloudResetPwdAgent.script start

📖 NOTE

- If **exit 0** is displayed at the end of the file, add the preceding content to the line just before **exit 0**. If **exit 0** is not displayed, add the preceding content to the end of the file.
- ECSs created from a SUSE 11 SP4 image must have 4 GB or a larger memory.

Procedure

- CoreOS

  Run the following commands to start the plug-in:
  ```
  cat >/etc/systemd/system/cloudResetPwdAgent.service <<EOT
  [Unit]
  Description=cloudResetPwdAgent service
  Wants=local-fs.target
  Requires=local-fs.target
  [Service]
  Type=simple
  ExecStart=/CloudrResetPwdAgent/bin/cloudResetPwdAgent.script start
  RemainAfterExit=yes
  ExecStop=/CloudrResetPwdAgent/bin/cloudResetPwdAgent.script stop
  KillMode=none
  [Install]
  WantedBy=multi-user.target
  EOT
  systemctl enable cloudResetPwdAgent.service
  ```

- SUSE, Ubuntu, and Debian

  a. Run the following command to open the **rc** file:

     vi /etc/init.d/rc

  b. Press **i** to enter the editing mode and add the following content to the end of the file:
     ```
     /CloudrResetPwdAgent/bin/cloudResetPwdAgent.script start
     ```

   c. Press **Esc**, enter **:wq**, and press **Enter** to save the configuration and exit.

- CentOS Linux 7

  a. Run the following commands to make **rc.local** executable, and then to open the file:

   chmod +x /etc/rc.d/rc.local

   vi /etc/rc.d/rc.local

  b. Press **i** to enter the editing mode and add the following content to the end of the file:
```
/CloudrResetPwdAgent/bin/cloudResetPwdAgent.script start
```

  c. Press **Esc**, enter **:wq**, and press **Enter** to save the configuration and exit.

- openSUSE 13

  a. Run the following command to open the **boot.local** file:

   vi /etc/init.d/boot.local

  b. Press **i** to enter the editing mode and add the following content to the end of the file:
```
/CloudrResetPwdAgent/bin/cloudResetPwdAgent.script start
```

  c. Press **Esc**, enter **:wq**, and press **Enter** to save the configuration and exit.

- Debian 8

  a. Run the following command to open the **rc.local** file:

   vi /etc/rc.local

  b. Press **i** to enter the editing mode and add the following content to the end of the file:
```
/CloudrResetPwdAgent/bin/cloudResetPwdAgent.script start
```

  c. Press **Esc**, enter **:wq**, and press **Enter** to save the configuration and exit.

- Fedora 20

  a. Run the following commands to open the **rc.local** file:

   touch /etc/rc.d/rc.local

   chmod +x /etc/rc.d/rc.local

   vi /etc/rc.d/rc.local

  b. Press **i** to enter the editing mode and add the following content to the end of the file:
```
/CloudrResetPwdAgent/bin/cloudResetPwdAgent.script start
```

  c. Press **Esc**, enter **:wq**, and press **Enter** to save the configuration and exit.

- Other OSs

  a. Run the following command to open the **rc.local** file:

   vi /etc/rc.d/rc

  b. Press **i** to enter the editing mode and add the following content to the end of the file:
```
/CloudrResetPwdAgent/bin/cloudResetPwdAgent.script start
```

  c. Press **Esc**, enter **:wq**, and press **Enter** to save the configuration and exit.

5.7 Why Can't I Find My Private Image When I Want to Use It to Create an ECS or Change the OS of an ECS?

When you create an ECS or change the OS of an existing ECS, some of your private images are not shown. One possible cause is that the x86 and Arm architectures are incompatible with each other, or that there is an incompatibility issue between UEFI and BIOS boot modes.

- If a private image is created from a x86 ECS, this image will be invisible to you when you create an Arm (Kunpeng) ECS or change the OS of an Arm (Kunpeng) ECS, and vice versa.

- If you use an external image file to create a private image and select the x86 architecture, this image will be invisible to you when you create an Arm (Kunpeng) ECS or change the OS of an Arm (Kunpeng) ECS, and vice versa.

- If a private image is created from an ECS in BIOS boot mode, this image will be invisible to you when you create an ECS in UEFI boot mode or change the OS of an ECS in UEFI boot mode, and vice versa.

- If you use an external image file to create a private image and select the BIOS boot mode, this image will be invisible to you when you create an ECS in UEFI boot mode or change the OS of an ECS in UEFI boot mode, and vice versa.

6 Image Importing

6.1 Can I Use Images in Formats Other Than the Specified Ones?

No. Currently, only the VMDK, VHD, RAW, QCOW2, VHDX, QED, VDI, QCOW, ZVHD2, ISO, and ZVHD formats are supported.

Images of the -flat.vmdk format and image file packages containing snapshot volumes or delta volumes are not supported. You can use **qemu-img** to convert an image to one of the supported formats before uploading it to the cloud platform.

> ☐ **NOTE**
>
> For details about image file format conversion, see **Converting the Image Format Using qemu-img**.

6.2 What Are the Impacts If I Do Not Pre-configure an ECS Used to Create a Private Image?

Before using an ECS or external image file to create a private image, you need to pre-configure the ECS or the source VM of the image file. If you do not perform the pre-configuration, there will be the following impacts:

1. If you do not delete residual rule files from the **udev** directory, new ECSs will retain the configurations of the source ECS or image file. If you do not set the IP address assignment mode to DHCP, NICs of new ECSs will not start from eth0. You need to remotely log in to the new ECSs to perform configurations.

2. For Linux, the following issues may occur during the ECS creation:
   - Custom passwords cannot be injected.
   - Certificates cannot be injected.
   - Other custom configurations cannot be applied on new ECSs.

3. If you do not delete information about automatic disk attachment detection from the **fstab** file, new ECSs may fail to start.

6.3 How Do I Import an OVF or OVA File to the Cloud Platform?

Scenarios

Open Virtualization Appliance (OVA) is a single file (with the .ova extension) that archives all the files making up an Open Virtualization Format (OVF). OVF is a folder that contains the files required for defining and deploying VMs. An OVF folder always includes .ovf, .mf, and .vmdk files.

- An .ovf file is an XML descriptor that defines metadata of a VM, such as the name and hardware requirements, and contains reference information about other files in the OVF folder.
- An .mf file contains the SHA hash codes of all the files in the folder and is used to prevent the image file from being tampered with.
- A .vmdk file is a virtual disk file that is used to create a disk image. An OVF folder may contain multiple .vmdk files.

This section describes how to import OVF and OVA files to the cloud platform.

Procedure

Manually extract VMDK files from an OVF or OVA template and upload them to an OBS bucket. Then, you can select one from the bucket when you use an external file to create a system or data disk image.

☐ NOTE

The following assumes that the OVF or OVA template contains only one VMDK file. If there are multiple VMDK files (for example, there are three VMDK files, one used as a system disk image file and the others as data disk image files), upload them to an OBS bucket and register them as a system disk image and data disk images, respectively.

- The source VM runs the Windows OS.
  - If you choose to export an OVF template named **MyVm** and save it to the **OvfLib** folder in drive C, the following files will be generated in the folder (the VMDK file can be uploaded to the cloud platform):
    ```
    ├C
    │ ├OvfLib
    │     ├MyVm
    │         ├MyVm.ovf
    │     ├MyVm.mf
    │     ├MyVm-disk1.vmdk
    ```
  - If you choose to export an OVA template and name it **MyVm**, the **C:\MyVm.ova** file will be generated. The VMDK file extracted from **MyVm.ova** can be uploaded to the cloud platform.

    ### ☐ NOTE

    You can import an image file in the VHD, VMDK, QCOW2, RAW, VHDX, QCOW, VDI, QED, ZVHD, or ZVHD2 format to create a private image.

    For details, see **Creating a Windows System Disk Image Using an External Image File** or **Creating a Data Disk Image Using an External Image File**.

- The source VM runs the Linux OS.

  - If you choose to export an OVF template, upload the VMDK file generated in the folder to the cloud platform.

  - If you choose to export an OVA template and name it **MyVm**, perform the following operations:

    i. Run the following command to view the OVA file:

    file MyVm.ova

    The command output is as follows:

    ```
    MyVm.ova: POSIX tar archive (GNU)
    ```

    MyVm.ova contains the following two files:

    ```
    $tar tf MyVm.ova
    MyVm.ovf
    MyVm.vmdk
    ```

    ii. Run the following command to decompress **MyVm.ova**:

    tar xvf MyVm.ova

    The extracted folder contains the following files:

    ```
    MyVm.ovf
    MyVm.vmdk
    ```

    The image file in the VMDK format can be uploaded to the cloud platform.

    ◯◯ NOTE

    You can import an image file in the VHD, VMDK, QCOW2, RAW, VHDX, QCOW, VDI, QED, ZVHD, or ZVHD2 format to create a private image.

    For details, see **Creating a Linux System Disk Image Using an External Image File** or **Creating a Data Disk Image Using an External Image File**.

6.4 What Do I Do If I Configured an Incorrect OS or System Disk Capacity During Private Image Registration Using an Image File?

If you selected an incorrect OS, ECSs may fail to be created from the private image. If the configured system disk capacity is less than the one in the image file, image registration will fail.

In such cases, delete the incorrect image and create a new one using correct parameter settings.

6.5 What Do I Do If the System Disk Capacity in a VHD Image File Exceeds the One I Have Specified on the Management Console When I Use This File to Register a Private Image?

The possible causes may be:

1. You have specified a small value.

   Check the system disk capacity in the VHD image file. Specify a value no less than this value when you use the VHD image file to register an image.

2. After being converted using **qemu-img** or a similar tool, the VHD's virtual disk size becomes smaller than the actual system disk size. For details, see **https://bugs.launchpad.net/qemu/+bug/1490611**.

   Run the following command to check the VHD image file information:

   ```
   [xxxx@xxxxx test]$ qemu-img info 2g.vhd
   image: 2g.vhd
   file format: vpc
   virtual size: 2.0G (2147991552 bytes)
   disk size: 8.0K
   cluster_size: 2097152
   ```

   The virtual size is converted from the actual size (unit: byte) to an integer in GB. After the conversion, the output virtual size **2 GB** is smaller than the input actual size **2.0004 GB** (**2147991552 bytes**). You need to specify an integer larger than the actual size 2.0004 GB on the management console.

6.6 How Do I Import Existing Huawei Cloud Private Images to a Specified Region?

Scenarios

You can import existing private images on Huawei Cloud to a specified region, migrating them between regions. In addition to **cross-region image replication**, you can export and import the images. This section describes how to import an image from a **CN North** to a **CN South** region.

Procedure

1. Export the image from the **CN North** region.

   a. Log in to the management console.

   b. Under **Compute**, click **Image Management Service**.

      The IMS console is displayed.

   c. Locate the row that contains the image to be exported, click **More** in the **Operation** column and select **Export**.

   d. In the displayed **Export Image** dialog box, set the following parameters:

      - **Fast Export**: To export an image larger than 128 GB, you must enable fast export, and you cannot specify the format of the exported image. After the image is exported, you can convert it to a common format. For details, see **Converting the Image Format Using qemu-img-hw**.

      - **Format**: Select one from **qcow2**, **vmdk**, **vhd**, and **zvhd** as you need.

      - **Name**: Enter a name that is easy to identify.

      - **Storage Path**: Click to expand the bucket list and select an OBS bucket for storing the exported image.

e. Click **OK**.

You can view the image export progress in the **Task Center**. After the image is successfully exported, you can download the image from the OBS bucket on the OBS console or OBS Browser.

2. Create an OBS bucket in the **CN South** region. Upload the image file downloaded in step **1** to the OBS bucket in the **CN South** region.

3. Register the image file in the OBS bucket as a private image.

7 Image Exporting

7.1 Can I Download My Private Images to a Local PC?

Yes. You can download private images in VMDK, VHD, QCOW2, or ZVHD format as instructed in **Exporting an Image**.

7.2 Can I Use the System Disk Image of an ECS on a BMS After I Export It from the Cloud Platform?
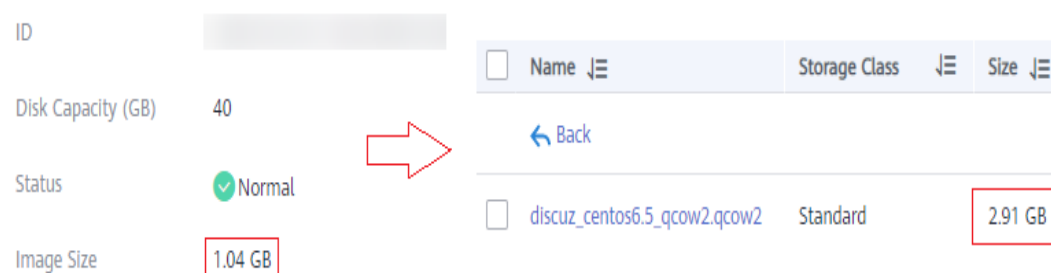
No. The system disk image of an ECS is a VM file that contains a system running environment and does not have an installation boot program. Therefore, it cannot be used on a BMS.

7.3 Why Is the Image Size in an OBS Bucket Different from That Displayed in IMS?

Symptom

After a private image is exported to an OBS bucket, the image size in the bucket is different from that displayed in IMS. For example, the size of a private image is 1.04 GB on the IMS console. After it is exported to an OBS bucket, the size is displayed as 2.91 GB.

Figure 7-1 Example

Cause Analysis

The size of an image in an OBS bucket varies depending on the file's storage format in the bucket.

7.4 Can I Download a Public Image to My Local PC?

Currently, you cannot directly download a public image. You can use the public image to create an ECS, use the ECS to create a private image, export the private image to your OBS bucket, and download the private image to your local PC.

Helpful links:

- **Creating a System Disk Image from a Windows ECS** or **Creating a System Disk Image from a Linux ECS**

- **Exporting an Image**

📖 NOTE

- Windows, SUSE, Red Hat, Ubuntu, and Oracle Linux public images and the private images created from these public images cannot be exported.

- However, if a Windows, SUSE, Red Hat, Ubuntu, or Oracle Linux private image is created from an external image file, this private image can be exported.

7.5 What Are the Differences Between Import/Export and Fast Import/Export?

Item	Description	Helpful Link
Import	Import an external image file to the Huawei Cloud management console for creating a private image. External image files in the following formats can be imported: VMDK, VHD, QCOW2, RAW, VHDX, QED, VDI, QCOW, ZVHD2, and ZVHD. Maximum file size: 128 GB During the import, operations such as driver injection will be performed in the background. Therefore, the import takes a longer time than fast import.	• **Creating a Windows System Disk Image from an External Image File** • **Creating a Linux System Disk Image from an External Image File** • **Creating a Data Disk Image from an External Image File**

Item	Description	Helpful Link
Fast import	When importing an external image file in the RAW or ZVHD2 format to the Huawei Cloud management console, you can select **Enable Fast Create**, as shown in **Figure 7-2**. The system does not perform any operations such as driver injection. Verify that: ● The image file converted to the RAW format has been optimized as required and a bitmap file has been generated for it. ● The image file converted to the ZVHD2 format has been optimized as required. Maximum file size: 1 TB	**Quickly Importing an Image File**
Export	You can export private images to OBS buckets and download them to your local PC for further use on other cloud platforms. Maximum file size: 128 GB (If an image file is larger than 128 GB, use fast export to export it.) You can specify the format of the exported image file. Currently, only QCOW2, VMDK, VHD, and ZVHD are supported.	**Exporting an Image**
Fast export	On the **Export Image** page, select **Enable** following **Fast Export**, as shown in **Figure 7-3**. You cannot specify the format of the exported image file. After the export is complete, you can use a tool to convert the exported image to your desired format. The file size is not limited. Encrypted images do not support fast export.	**Exporting an Image**

Figure 7-2 Fast import

Figure 7-3 Fast export

7.6 What Do I Do If the Export Option Is Unavailable for My Image?

Some images cannot be exported. Therefore, the **Export** option is not provided for them in the **Operation** column. The following images cannot be exported:

- Public images
- Full-ECS images
- ISO images
- Private images created from a Windows or SUSE public image
- Private images created from a KooGallery image

8 Image Optimization

8.1 Must I Install Guest OS Drivers on an ECS?

Installing Guest OS drivers on an ECS improves your experience in using the ECS. In addition, it also ensures high reliability and stability of ECSs.

- Windows ECSs: Install PV and VirtIO drivers on ECSs.
- Linux ECSs: Install Xen PV and VirtIO drivers and add them to initrd.

8.2 Why Do I Need to Install and Update VirtIO Drivers for Windows?

Why Do I Need to Install VirtIO Drivers?

VirtIO drivers are paravirtualized drivers that provide high-performance disks and NICs for ECSs.

- A standard Windows OS does not have VirtIO drivers.
- Public images have VirtIO drivers by default.
- You need to install VirtIO drivers for private images. For details, see **Installing VirtIO Drivers**.

Why Do I Need to Update VirtIO Drivers?

This ensures that known issues identified in the community or R&D tests can be avoided on the latest drivers.

When Do I Need to Update VirtIO Drivers?

After a major error is fixed, you are advised to update VirtIO drivers immediately. (This has not happened by now.)

After other issues are fixed, decide whether to update VirtIO drivers based on your needs.

What Do I Need to Do?

- Upgrade VirtIO drivers in Windows private images or running Windows ECSs.
- If you have any technical issue or question, contact the customer service.

8.3 What Will the System Do to an Image File When I Use the File to Register a Private Image?

You are advised to enable automatic configuration when registering a private image using an image file. Then, the system will perform the following operations:

Linux

- Check whether any PV drivers exist. If yes, the system deletes them.
- Modify the **grub** and **syslinux** configuration files to add the OS kernel boot parameters and change the disk partition name (**UUID=**_UUID of the disk partition_).
- Change the names of the disk partitions in the **/etc/fstab** file (**UUID=**_UUID of the disk partition_).
- Check whether the initrd file has Xen and IDE drivers. If no, the system will load the Xen and IDE drivers.
- Modify the X Window configuration file **/etc/X11/xorg.conf** to prevent display failures.
- Delete services of VMware tools.
- Record the latest automatic modification made to the image into **/var/log/rainbow_modification_record.log**.
- Copy built-in VirtIO drivers to **initrd** or **initramfs**. For details, see **External Image File Formats and Supported OSs**.

📖 **NOTE**

For the following image files, the system does not copy this driver after **Enable automatic configuration** is selected:

- Image files whose **/usr** directory is an independent partition
- Fedora 29 64bit, Fedora 30 64bit, and CentOS 8.0 64bit image files that use the XFS file system
- SUSE 12 SP4 64bit image files that use the ext4 file system

Windows

- Restore the IDE driver so that the OS can use this driver for its initial start.
- Delete the registry keys of the mouse and keyboard and generate the registry keys again to ensure that the mouse and keyboard are available on the new cloud platform.
- Restore the PV driver registry key to rectify driver installation failures and Xen driver conflicts.
- Inject VirtIO drivers offline so that the OS can start properly.
- Restore DHCP. The OS will dynamically obtain information such as the IP address based on the DHCP protocol.

8.4 How Do I Configure an ECS, BMS, or Image File Before I Use It to Create an Image?

ECS or Image File Configurations

Table 8-1 ECS configurations

OS	Configuration	Reference
Windows	- Set the NIC to DHCP. - Enable remote desktop connection. - Install the one-click password reset plug-in. (Optional) Install Cloudbase-Init. - Install Guest OS drivers (PV and VirtIO drivers). - Run Sysprep.	**Creating a System Disk Image from a Windows ECS**
Linux	- Set the NIC to DHCP. - Install the one-click password reset plug-in. (Optional) Install Cloud-Init. - Delete files from the network rule directory. - Change the disk identifier in the GRUB configuration file to UUID. - Change the disk identifier in the fstab file to UUID. - Install native Xen and KVM drivers. - Detach data disks from the ECS.	**Creating a System Disk Image from a Linux ECS**

Table 8-2 Image file configurations

OS	Configuration	Reference
Windows	- Set the NIC to DHCP. - Enable remote desktop connection. - Install Guest OS drivers (PV and VirtIO drivers). (Optional) Install Cloudbase-Init. (Optional) Enable NIC multi-queue. (Optional) Configure an IPv6 address.	**Preparing an Image File (Windows)**
Linux	- Delete files from the network rule directory. - Set the NIC to DHCP. - Install native Xen and KVM drivers. - Change the disk identifier in the GRUB configuration file to UUID. - Change the disk identifier in the fstab file to UUID. - Delete the automatic attachment information of non-system disks from the **/etc/fstab** file. (Optional) Install Cloud-Init. (Optional) Enable NIC multi-queue. (Optional) Configure an IPv6 address.	**Preparing an Image File (Linux)**

☐ NOTE

- When registering an external image file as a private image, you are advised to perform the preceding operations on the VM where the external image file is located.
- When registering a Windows external image file as a private image, if the Guest OS drivers are installed, the cloud platform will check the image file after you select **Enable automatic configuration**. If the GuestOS drivers are not installed, the cloud platform will try to install them.

BMS or Image File Configurations

Table 8-3 BMS configurations

OS	Configuration	Reference
Windows	• Install the **bms-network-config** package. • Install Cloudbase-Init. • Delete residual files from the OS.	**Creating a Private Image from a BMS**
Linux	• Install software in the **bms-network-config** package. • Install Cloud-Init. • Delete residual files from the OS.	**Creating a Private Image from a BMS**

Table 8-4 Image file configurations

OS	Configuration	Reference
Windows	• Install drivers for x86 V5 BMSs. • Install Cloudbase-Init. • Install software in the **bms-network-config** package. • (Optional) Install the SDI iNIC driver. • (Optional) Install the one-click password reset plug-in. • Set the Windows time zone. • Set the virtual memory. • (Optional) Configure automatic Windows update. • Configure SID.	**Private Image Creation Guide**

OS	Configuration	Reference
Linux	- Install and configure Cloud-Init. - Modify the hardware device driver that boots the OS. - Install software in the **bms-network-config** package. (Optional) Install the SDI iNIC driver. (Optional) Install the Hi1822 NIC driver. (Optional) Install the IB driver. (Optional) Install drivers for x86 V5 BMSs. (Optional) Install the UltraPath software. (Optional) Install the one-click password reset plug-in. - Perform security configuration. - Configure remote login to the BMS. - Configure automatic root partition expansion.	**Private Image Creation Guide**

8.5 What Do I Do If a Windows Image File Is Not Pre-Configured When I Use It to Register a Private Image?

If an image file is not configured as instructed in **Windows image file requirements** before it is exported from the original platform, configure it by referring to **Figure 8-1**.

> ⚠ **CAUTION**
>
> An ECS can run properly only after Xen Guest OS drivers (PV drivers) and KVM Guest OS drivers (VirtIO drivers) are installed on it. Without these drivers, the performance of this ECS will be affected and some functions will be unavailable. Ensure that the driver installation has been completed for the image file before it is exported from the original platform. Otherwise, the ECSs created from the image will fail to start.
>
> - Install PV drivers. For details, see **Installing PV Drivers**.
> - Install VirtIO drivers. For details, see **Installing VirtIO Drivers**.

Figure 8-1 Image creation process
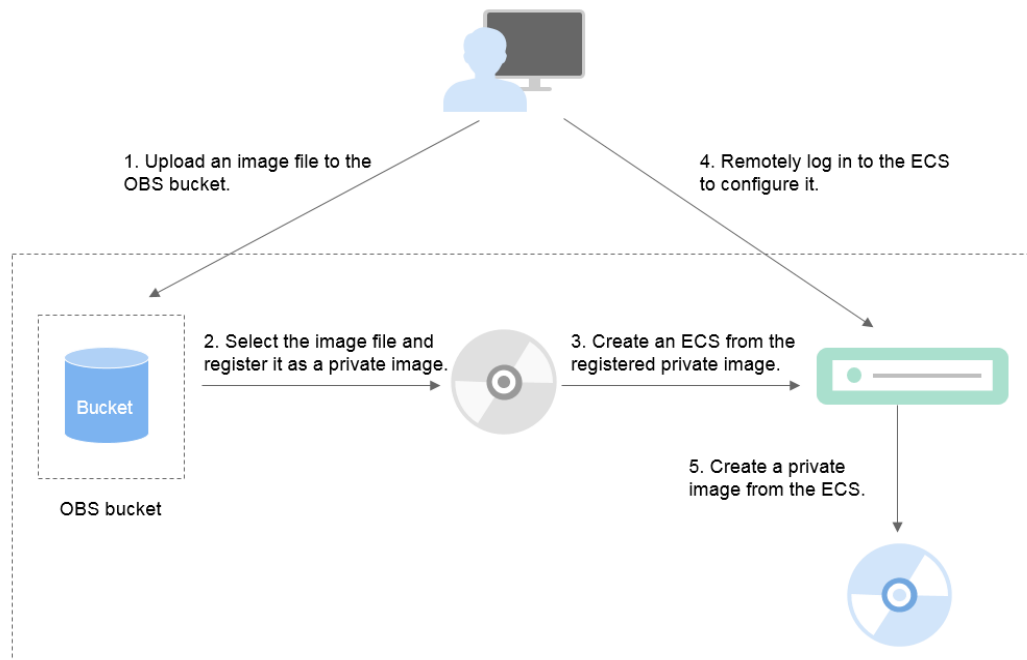
Step 1: Upload the Image File

Upload the external image file to an OBS bucket. For details, see **Uploading an External Image File (Windows)**.

Step 2 Register the Image File as a Private Image

On the management console, select the uploaded image file and register it as a private image. For details, see **Registering an External Image File as a Private Image (Windows)**.

Step 3: Create an ECS

1. Access the IMS console.

   a. Log in to the management console.

   b. Under **Compute**, click **Image Management Service**.

      The IMS console is displayed.

2. Click the **Private Images** tab.

3. Locate the row that contains the private image and click **Apply for Server** in the **Operation** column.

4. Set parameters as promoted to create an ECS. Pay attention to the following:
   - You are advised to select **Pay-per-use** for **Billing Mode** because the ECS will be deleted when you finish with it.
   - Bind an EIP to the ECS so that you can upload installation packages to the ECS or download installation packages from the ECS.
   - You must add inbound rules for security groups of the ECS to ensure that the ECS can be accessed.

        – If the image file has Cloudbase-Init installed, set a password and log in to the ECS using the password as prompted. If Cloudbase-Init is not installed, use the password or certificate contained in the image file to log in the ECS.

For details, see **Purchasing an ECS**.

5. Perform the following steps to check whether the private image has been pre-configured:

    a. Check whether the ECS can be successfully started. If the start succeeds, Guest OS drivers have been installed for the image file on the original platform or the drivers have been automatically installed for the private image on the cloud platform. If the start failed, install Guest OS drivers for the image file on the original platform and start from **Step 1: Upload the Image File** again.

    b. Check whether you can log in to the ECS using your configured password or key. If you can, Cloudbase-Init has been installed. If you cannot, use the password or key contained in the image file to log in to the ECS and install Cloudbase-Init as instructed in **Installing and Configuring Cloudbase-Init**.

    c. Check whether NICs are set to DHCP by referring to **2** in **Step 4: Configure the ECS**.

    d. Use MSTSC to log in to the ECS. If the login is successful, remote desktop connection is enabled on the ECS. If the login fails, enable remote desktop connection by referring to **3** in **Step 4: Configure the ECS**.

If the ECS meets the preceding requirements, the private image has been pre-configured. Skip **Step 4: Configure the ECS** and **Step 5: Create a Private Image from the ECS**.

Step 4: Configure the ECS

Remotely log in to the ECS created in **Step 3: Create an ECS** to configure it.

1. Log in to the ECS.
2. Check whether NICs are set to DHCP. If the ECS is configured with a static IP address, change its IP address assignment mode to DHCP as instructed in **Setting the NIC to DHCP**.
3. Enable remote desktop connection for the ECS as needed. For details about how to enable this function, see **Enabling Remote Desktop Connection**.
4. (Optional) Configure value-added functions.

    – Install and configure Cloudbase-Init. For details, see **Installing and Configuring Cloudbase-Init**.

    – Enable NIC multi-queue. For details, see **How Do I Enable NIC Multi-Queue for an Image?**

    – Configure an IPv6 address. For details, see **How Do I Configure an ECS to Dynamically Acquire IPv6 Addresses?**

Step 5: Create a Private Image from the ECS

For details, see **Creating a System Disk Image from a Windows ECS**.

(Optional) Clear the Environment

After the image registration is complete, delete the image file as well as the intermediate private image and ECS to avoid generating any additional charges.

- Delete the image registered in **Step 2 Register the Image File as a Private Image**.
- Delete the ECS created in **Step 3: Create an ECS**.
- Delete the image file from the OBS bucket.

8.6 What Do I Do If a Linux Image File Is Not Pre-Configured When I Use It to Register a Private Image?

If an image file is not configured as instructed in **Linux image file requirements** before it is exported from the original platform, configure it by referring to **Figure 8-2**.

⚠ **CAUTION**

An ECS can run properly only after Xen and KVM drivers are installed on it. If no such drivers are installed, the performance of the ECS will be affected and some functions will be unavailable. Ensure that KVM drivers have been installed for the image file before it is exported from the original platform. Otherwise, the ECSs created from the image will fail to start.

- For Xen, install native Xen and KVM drivers. For details, see **How Do I Install Native Xen and KVM Drivers?**
- For KVM, install native KVM drivers. For details, see **Installing Native KVM Drivers**.

Figure 8-2 Image creation process
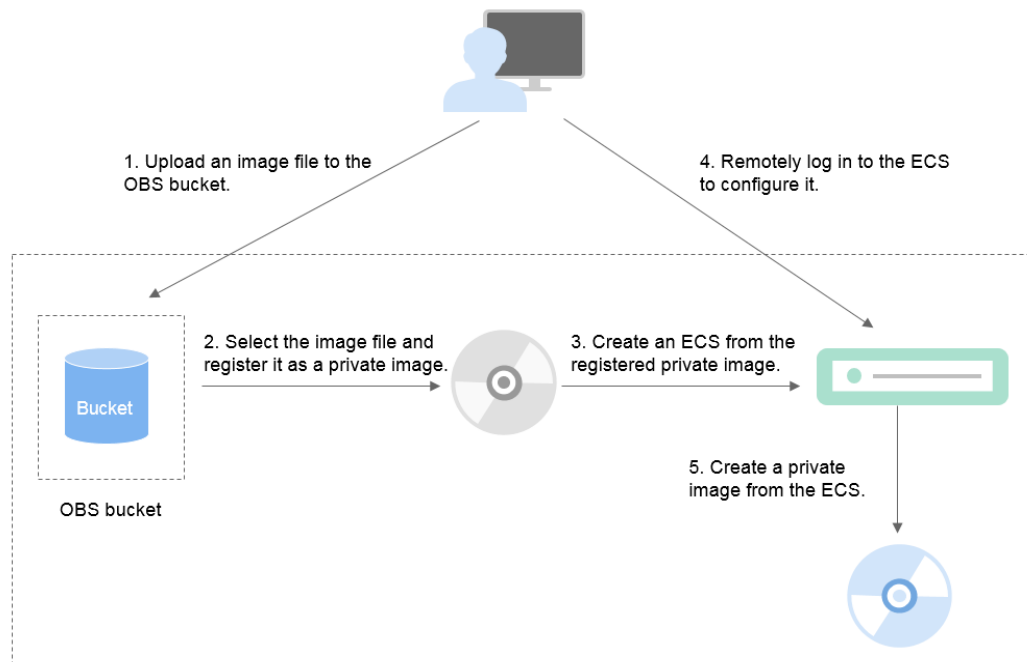
Step 1: Upload the Image File

Upload the external image file to an OBS bucket. For details, see **Uploading an External Image File (Linux)**.

Step 2 Register the Image File as a Private Image

On the management console, select the uploaded image file and register it as a private image. For details, see **Registering an External Image File as a Private Image (Linux)**.

Step 3: Create an ECS

Create an ECS from the private image.

1. Access the IMS console.

   a. Log in to the management console.

   b. Under **Compute**, click **Image Management Service**.

      The IMS console is displayed.

2. Click the **Private Images** tab.

3. Locate the row that contains the private image and click **Apply for Server** in the **Operation** column.

4. Set parameters as promoted to create an ECS. Pay attention to the following:

   – You are advised to select **Pay-per-use** for **Billing Mode** because the ECS will be deleted when you finish with it.

   – You must add inbound rules for security groups of the ECS to ensure that the ECS can be accessed.

–   If Cloud-Init has been installed in the image file, set a login password as prompted. If Cloud-Init is not installed, use the password or certificate contained in the image file to log in.

For details, see **Purchasing an ECS**.

5.   Perform the following steps to check whether the private image has been pre-configured:

a.   Check whether the ECS can be successfully started. If the start succeeds, Xen and KVM drivers have been installed for the external image file on the original platform or the drivers have been automatically installed for the private image on the cloud platform. If the start failed, install Xen and KVM drivers for the image file and start from **Step 1: Upload the Image File** again.

b.   Check whether you can log in to the ECS using your configured password or key. If you can, Cloud-Init has been installed. If you cannot, use the password or key contained in the image file to log in to the ECS and install Cloud-Init as instructed in **Installing Cloud-Init**.

c.   Check the network configuration by referring to **Step 4: Configure the ECS**.

If the ECS meets the preceding requirements, the private image has been pre-configured. Skip **Step 4: Configure the ECS** and **Step 5: Create a Private Image from the ECS**.

Step 4: Configure the ECS

Remotely log in to the ECS created in **Step 3: Create an ECS** to configure it.

1.   Log in to the ECS.

2.   Configure the network.

–   Run the **ifconfig** command to check whether the private IP address of the ECS is the same as that displayed on the console. If they are inconsistent, delete files from the network rule directory as instructed in **Deleting Files from the Network Rule Directory**.

–   Check whether NICs are set to DHCP. If the ECS is configured with a static IP address, change its IP address assignment mode to DHCP as instructed in **Setting the NIC to DHCP**.

–   Run the **service sshd status** command to check whether SSH is enabled. If it is disabled, run the **service sshd start** command to enable it. Ensure that your firewall (for example, Linux iptables) allows SSH access.

3.   Configure a file system.

–   Change the disk identifier in the GRUB configuration file to UUID. For details, see **Changing the Disk Identifier in the GRUB Configuration File to UUID**.

–   Change the disk identifier in the fstab file to UUID. For details, see **Changing the Disk Identifier in the fstab File to UUID**.

–   Clear the automatic attachment information of non-system disks in the **/etc/fstab** file to prevent impacts on subsequent data disk attachment. For details, see **Detaching Data Disks from an ECS**.

4.   (Optional) Configure value-added functions.

- – Install and configure Cloud-Init. For details, see **Installing Cloud-Init** and **Configuring Cloud-Init**.
- – Enable NIC multi-queue. For details, see **How Do I Enable NIC Multi-Queue for an Image?**
- – Configure an IPv6 address. For details, see **How Do I Configure an ECS to Dynamically Acquire IPv6 Addresses?**

Step 5: Create a Private Image from the ECS

Create a private image from the ECS. For details, see **Creating a System Disk Image from a Linux ECS**.

(Optional) Clear the Environment

After the image registration is complete, delete the image file as well as the intermediate private image and ECS to avoid generating any additional charges.

- Delete the image registered in **Step 2 Register the Image File as a Private Image**.
- Delete the ECS created in **Step 3: Create an ECS**.
- Delete the image file from the OBS bucket.

8.7 How Do I Optimize an Image?

Scenarios

The general-purpose second-generation ECS uses KVM. To create this type of ECS from an image, you must ensure that the image has KVM drivers installed. Otherwise, you may fail to start or log in to the ECSs created from the image.

To help you better use general-purpose second-generation ECSs, IMS provides the automatic image optimization function.

📖 NOTE

- Only some images can be optimized. You can check whether an image can be optimized on the console.

Constraints

- After an image is automatically optimized, a new private image will be generated.
- Only Linux images can be optimized automatically.

  For details about how to manually optimize a Linux private image, see **Optimizing a Linux Private Image**.
- After an image is optimized, a new image will be generated and it can be used to create general-purpose second-generation ECSs. After the optimization is complete, you can delete the original image.

Procedure

1. Log in to the management console.
2. Under **Compute**, click **Image Management Service**.
3. Click the **Private Images** tab.
4. Locate the image to be optimized, click **More** in the **Operation** column, and select **Optimize** from the drop-down list.

   📖 **NOTE**

   In the **Operation** column of the target image, if you cannot find **Optimize** from **More**, optimization is not supported for this image.

5. In the displayed dialog box, select **Yes. I have optimized the image.** if you have optimized the image. Otherwise, select **No. Help me optimize the image.**

Figure 8-3 Optimize Image

6. Click **OK**.

8.8 How Do I Use a Private Image Created from a First-Generation ECS to Create a Second-Generation ECS?

Scenario

For general-purpose and memory-optimized ECSs, the second generation has a different virtualization architecture and driver type from the first generation. Therefore, you must optimize a private image created from a first-generation ECS before using it to create a second-generation ECS.

Procedure

The following operations use a general-purpose ECS as an example.

Method 1: automatic image optimization

1. Log in to the management console.
2. Under **Compute**, click **Image Management Service**.
3. On the **Image Management Service** page, click **Private Images** to display the image list.
4. Automatically optimize the image. For details, see **How Do I Optimize an Image?**.

   📖 NOTE

   > Only Linux images can be optimized automatically.

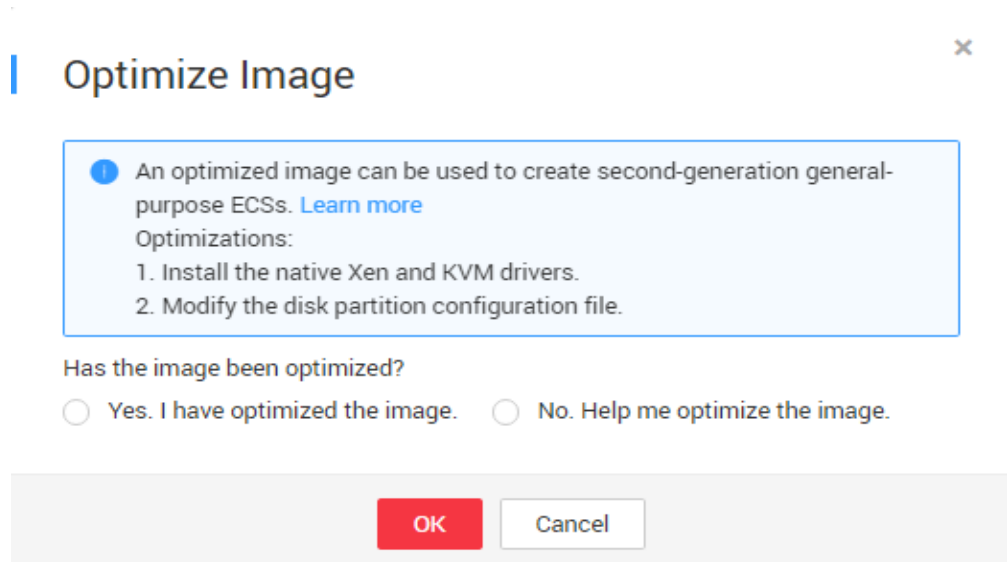5. Use the optimized private image to create a second-generation ECS.

Method 2: manual image optimization

1. Log in to the management console.
2. Under **Compute**, click **Image Management Service**.
3. On the **Image Management Service** page, click **Private Images** to display the image list.
4. Use this image to create a first-generation ECS.

   📖 NOTE

   > If first-generation ECSs have been sold out, use method 1.

5. Optimize the image.
   – For Windows, see **Optimizing a Windows Private Image**.
   – For Linux, see **Optimizing a LinuxPrivate Image**.
6. Use the optimized general-purpose first-generation ECS to create a private image.
7. Use the private image to create a second-generation ECS.

8.9 How Do I Enable NIC Multi-Queue for an Image?

Scenarios

With the increase of network I/O bandwidth, a single vCPU cannot meet the requirement of processing NIC interruptions. NIC multi-queue allows multiple vCPUs to process NIC interruptions, thereby improving network PPS and I/O performance.

ECSs Supporting NIC Multi-Queue

NIC multi-queue can be enabled on an ECS only when the ECS specifications, virtualization type, and image meet the requirements described in this section.

- For details about the ECS specifications that support NIC multi-queue, see **ECS Types**.

  📖 NOTE

  > If the number of NIC queues is greater than 1, NIC multi-queue is supported.

- Only KVM ECSs support NIC multi-queue.

- The Linux public images listed in **Table 8-6** support NIC multi-queue.

  □ NOTE

  - Windows OSs have not commercially supported NIC multi-queue. If you enable NIC multi-queue for a Windows image, starting an ECS created using such an image may be slow.

  - You are advised to upgrade the kernel version of Linux ECSs to 2.6.35 or later. Otherwise, NIC multi-queue is not supported.

    Run the **uname -r** command to check the kernel version. If the version is earlier than 2.6.35, contact technical support to upgrade it.

Table 8-5 Windows ECSs that support NIC multi-queue

OS	Image	Supported By
Windows	Windows Server 2008 WEB R2 64bit	Private images
	Windows Server 2008 Enterprise SP2 64bit	Private images
	Windows Server 2008 R2 Standard/Datacenter/Enterprise 64bit	Private images
	Windows Server 2008 R2 Enterprise 64bit_WithGPUdriver	Private images
	Windows Server 2012 R2 Standard 64bit_WithGPUdriver	Private images
	Windows Server 2012 R2 Standard/Datacenter 64bit	Private images

Table 8-6 Linux ECSs that support NIC multi-queue

OS	Image	Supported By	NIC Multi-Queue Enabled by Default
Linux	Ubuntu 14.04/16.04 Server 64bit	Public images	Yes
	openSUSE 42.2 64bit	Public images	Yes
	SUSE Enterprise 12 SP1/SP2 64bit	Public images	Yes
	CentOS 6.8/6.9/7.0/7.1/7.2/7.3/7.4/7.5/7.6 64bit	Public images	Yes
	Debian 8.0.0/8.8.0/8.9.0/9.0.0 64bit	Public images	Yes

OS	Image	Supported By	NIC Multi-Queue Enabled by Default
	Fedora 24/25 64bit	Public images	Yes
	EulerOS 2.2 64bit	Public images	Yes

Operation Instructions

Assume that an ECS has the required specifications and virtualization type.

- If the ECS was created using a public image listed in **ECSs Supporting NIC Multi-Queue**, NIC multi-queue has been enabled on the ECS by default. Therefore, you do not need to manually enable NIC multi-queue for it.

- If the ECS was created using an external image file with an OS listed in **ECSs Supporting NIC Multi-Queue**, perform the following operations to enable NIC multi-queue:

  a. **Register the External Image File as a Private Image**.

  b. **Set NIC Multi-Queue for the Image**.

  c. **Create an ECS from the Private Image**.

  d. **Run the Script for Configuring NIC Multi-Queue**.

Register the External Image File as a Private Image

For details, see **Registering an External Image File as a Private Image (Linux)**. After the image file is imported, view the value of **NIC Multi-Queue** on the image details page.

- If the value is **Supported**, go to **Create an ECS from the Private Image**.

- If the value is **Not supported**, go to **Set NIC Multi-Queue for the Image**.

Set NIC Multi-Queue for the Image

Windows OSs have not commercially supported NIC multi-queue. If you enable NIC multi-queue for a Windows image, starting an ECS created using such an image may be slow.

Use either of the following methods to set NIC multi-queue.

Method 1:

1. Access the IMS console.

   a. Log in to the management console.

   b. Under **Compute**, click **Image Management Service**.
      The IMS console is displayed.

2. On the displayed **Private Images** page, locate the row that contains the target image and click **Modify** in the **Operation** column.

3. Set NIC multi-queue for the image.

Method 2:

1. Access the IMS console.

   a. Log in to the management console.

   b. Under **Compute**, click **Image Management Service**.

   The IMS console is displayed.

2. On the displayed **Private Images** page, click the name of the target image.

3. In the upper right corner of the displayed image details page, click **Modify**. In the displayed **Modify Image** dialog box, set NIC multi-queue for the image.

Method 3: Add **hw_vif_multiqueue_enabled** to the image using an API.

1. Obtain a token. For details, see **Authentication**.

2. Call an API to update image information. For details, see **Updating Image Information (Native OpenStack API)**.

3. Add **X-Auth-Token** to the request header.

   The value of **X-Auth-Token** is the token obtained in step **1**.

4. Add **Content-Type** to the request header.

   The value of **Content-Type** is **application/openstack-images-v2.1-json-patch**.

   The request URI is in the following format:

   PATCH /v2/images/{*image_id*}

   The request body is as follows:

```
[
    {
     "op":"add",
     "path":"/hw_vif_multiqueue_enabled",
     "value": "true"
    }
]
```

   Figure 8-4 shows an example request body for setting NIC multi-queue.

Figure 8-4 Example request body
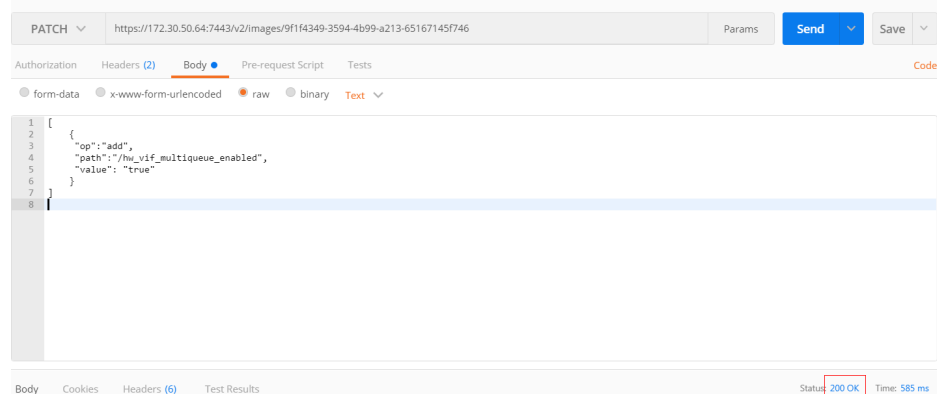
Create an ECS from the Private Image

Use the registered private image to create an ECS. For details, see **Purchasing an ECS**. Note the following when setting the parameters:

- **Region**: Select the region where the private image is located.
- **Image**: Select **Private image** and then the desired image from the drop-down list.

Run the Script for Configuring NIC Multi-Queue

Windows OSs have not commercially supported NIC multi-queue. If you enable NIC multi-queue for a Windows image, starting an ECS created using such an image may be slow.

For Linux OSs, the script for automatically configuring NIC multi-queue is provided. If an ECS has multiple NICs, running the script will automatically enable multi-queue for all the NICs.

1. Log in to the ECS and run the following command to check the number of queues supported by and enabled for a NIC:

   ethtool -l *NIC*

   Example:

   ```
   [root@localhost ~]# ethtool -l eth0   #View the number of queues used by NIC eth0.
   Channel parameters for eth0:
   Pre-set maximums:
   RX:             0
   TX:             0
   Other:          0
   Combined:       4   #The NIC supports a maximum of four queues.
   Current hardware settings:
   RX:             0
   TX:             0
   Other:          0
   Combined:       1   #One queue has been enabled for the NIC.
   ```

   If the values of the two **Combined** fields are the same, NIC multi-queue has been enabled. No further action is required.

2. Run the following command to download the configuration script **multi-queue-hw**:

   wget https://ecs-instance-driver.obs.cn-north-1.myhuaweicloud.com/multi-queue-hw

   The download path is **https://ecs-instance-driver.obs.cn-north-1.myhuaweicloud.com/multi-queue-hw**.

3. Run the following command to make the script executable:

   chmod +x multi-queue-hw

4. Run the following command to place the **multi-queue-hw** script in the **/etc/init.d** directory:

   mv multi-queue-hw /etc/init.d

   Enter **y** when the following information is displayed:

   ```
   mv: overwrite '/etc/init.d/multi-queue-hw'?
   ```

5. Run the following command to run the script:

   /etc/init.d/multi-queue-hw start

   NIC multi-queue script takes effect immediately after the script is executed but becomes invalid once the ECS stops.

6. Add a startup item for each OS so that NIC multi-queue is automatically enabled upon the ECS startup.

- For CentOS, Red Hat, Fedora, EulerOS, SUSE, and openSUSE, run the following command:

  chkconfig multi-queue-hw on

- For Ubuntu, run the following command:

  update-rc.d multi-queue-hw defaults 90 10

- For Debian, run the following command:

  systemctl enable multi-queue-hw

8.10 How Do I Configure an ECS to Dynamically Acquire IPv6 Addresses?

Scenarios

IPv6 addresses are used to deal with IPv4 address exhaustion. If an ECS uses an IPv4 address, the ECS can run in dual-stack mode after IPv6 is enabled for it. Then, the ECS will have two IP addresses to access the intranet and Internet: an IPv4 address and an IPv6 address.

In some cases, an ECS cannot dynamically acquire an IPv6 address even if it meets all the requirements in **Constraints**. You need to configure the ECS to dynamically acquire IPv6 addresses. For public images:

- By default, dynamic IPv6 address assignment is enabled for Windows public images. You do not need to configure it. The operations in **Windows Server 2012** and **Windows Server 2008** are for your reference only.

- Before enabling dynamic IPv6 address assignment for a Linux public image, check whether IPv6 has been enabled and then whether dynamic IPv6 address assignment has been enabled. Currently, IPv6 is enabled for all Linux public images.

Constraints

- Ensure that IPv6 has been enabled on the subnet where the ECS works.

  If IPv6 is not enabled on the subnet, enable it by referring to **Enabling IPv6 for an ECS**. IPv6 cannot be disabled once it is enabled.

- Ensure that the ECS flavor supports IPv6.

  The ECS flavors that support IPv6 vary depending on regions and AZs. Check whether an ECS flavor supports IPv6 after you select a region and AZ on the management console.

Figure 8-5 Checking whether an ECS flavor supports IPv6
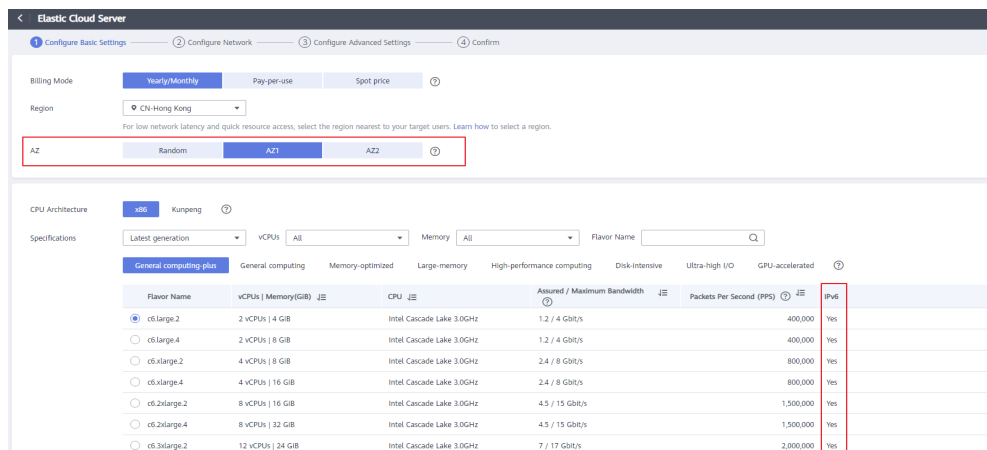
If the value of **IPv6** is **Yes** for an ECS flavor, the flavor supports IPv6.

📖 **NOTE**

> **AZ** and **Flavor** determine whether IPv6 is supported.
>
> After you select an AZ, if **IPv6** is not displayed or the value of **IPv6** is **No**, IPv6 is not supported by any or certain flavors in the AZ.

- Ensure that **Self-assigned IPv6 address** is selected during ECS creation.

Figure 8-6 Self-assigned IPv6 address
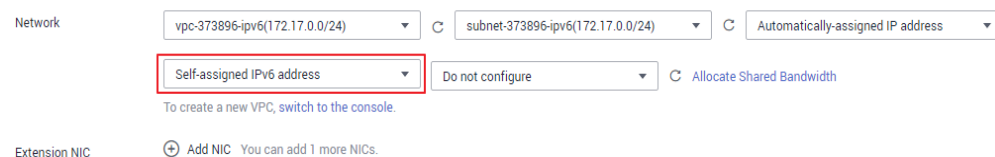
- After the ECS is started, its hot-swappable NICs cannot automatically acquire IPv6 addresses.
- Only ECSs can work in dual-stack mode and BMSs cannot.
- Only one IPv6 address can be bound to a NIC.

Procedure

- Windows: Windows Server 2012/2008 is used as an example to describe how to enable dynamic assignment of IPv6 addresses in Windows.
- Linux: Dynamic assignment of IPv6 addresses can be enabled automatically (recommended) or manually.

  If a private image created from a CentOS 6.x or Debian ECS with automatic IPv6 address assignment enabled is used to create an ECS in an environment that does not support IPv6, the ECS may start slow because of IPv6 address assignment timeout. You can set the timeout duration for assigning IPv6 addresses by referring to **Setting the Timeout Duration for IPv6 Address Assignment**.

Table 8-7 Enabling dynamic assignment of IPv6 addresses for different OSs

OS	Automatically/ Manually Enabling	Reference
Windows Server 2012	Automatically	**Windows Server 2012**
Windows Server 2008	Automatically	**Windows Server 2008**
Linux	Automatically (recommended)	**Linux (Automatically Enabling Dynamic Assignment of IPv6 Addresses)**
Linux	Manually	**Linux (Manually Enabling Dynamic Assignment of IPv6 Addresses)**

Enabling IPv6 for an ECS

NOTE

> After IPv6 is enabled on the subnet where the ECS works, an IPv6 CIDR block is automatically assigned to the subnet. IPv6 cannot be disabled once it is enabled.

1. Log in to the management console.

2. Click ⊙ in the upper left corner and select the desired region and project.

3. Click ☰ . Under **Compute**, click **Elastic Cloud Server**.

4. Click the target ECS to go to the detail page.

5. In the **ECS Information** area, click the VPC name.

6. Click the number in the **Subnets** column.

   The **Subnets** page is displayed.

7. In the subnet list, locate the target subnet and click its name.

   The subnet details page is displayed.

8. In the **Subnet Information** area, click **Enable** for **IPv6 CIDR Block**.

9. Click **Yes**.

Windows Server 2012

Step 1 Check whether IPv6 is enabled for the ECS.

Run the following command in the CMD window to check it:

ipconfig

- If an IPv6 address and a link-local IPv6 address are displayed, IPv6 is enabled and dynamic IPv6 assignment is also enabled.

Figure 8-7 Querying the IPv6 address
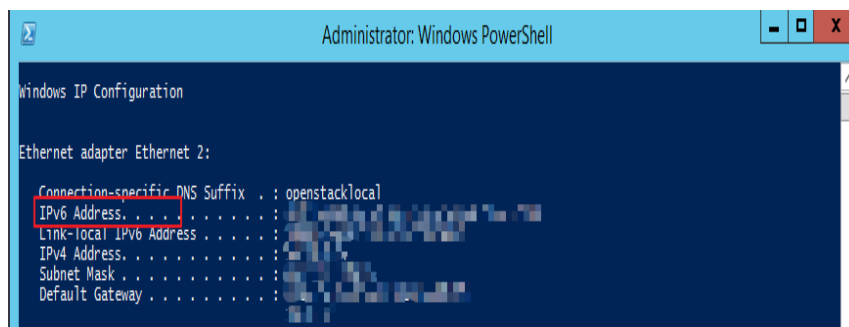
- If only a link-local IPv6 address is displayed, IPv6 is enabled but dynamic IPv6 assignment is not enabled. Go to **Step 2**.

Figure 8-8 Link-local IPv6 address
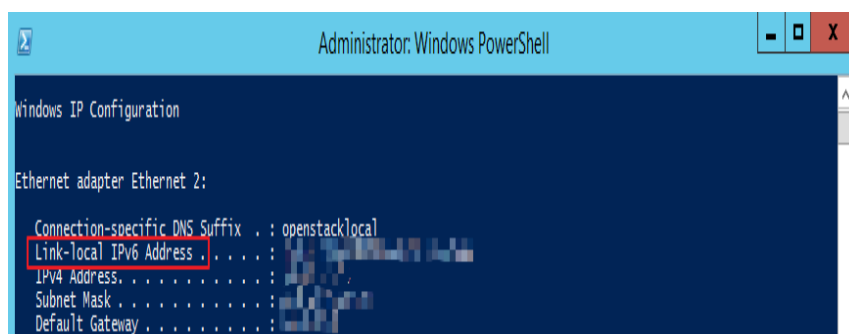
- If neither an IPv6 address nor link-local IPv6 address is displayed, IPv6 is disabled. Go to **Step 3**.

Figure 8-9 IPv6 disabled
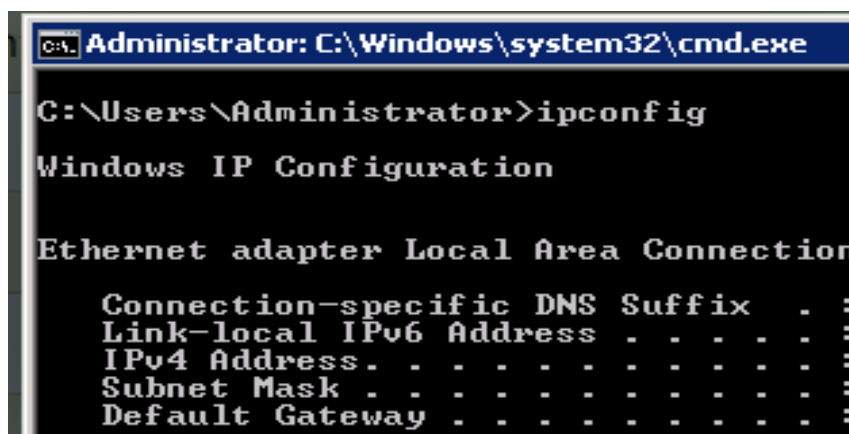
☐ **NOTE**

By default, dynamic IPv6 address assignment is enabled for Windows public images, as shown in **Figure 8-7**. No additional configuration is required.

Step 2 Enable dynamic IPv6 address assignment.

1. Choose **Start** > **Control Panel**.

2. Click **Network and Sharing Center**.

3. Click the Ethernet connection.

Figure 8-10 Ethernet connection
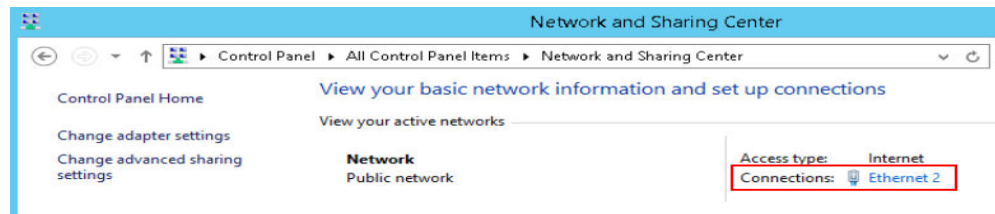
4. In the **Ethernet Status** dialog box, click **Properties** in the lower left corner.

5. Select **Internet Protocol Version 6 (TCP/IPv6)** and click **OK**.

Figure 8-11 Configuring dynamic IPv6 address assignment
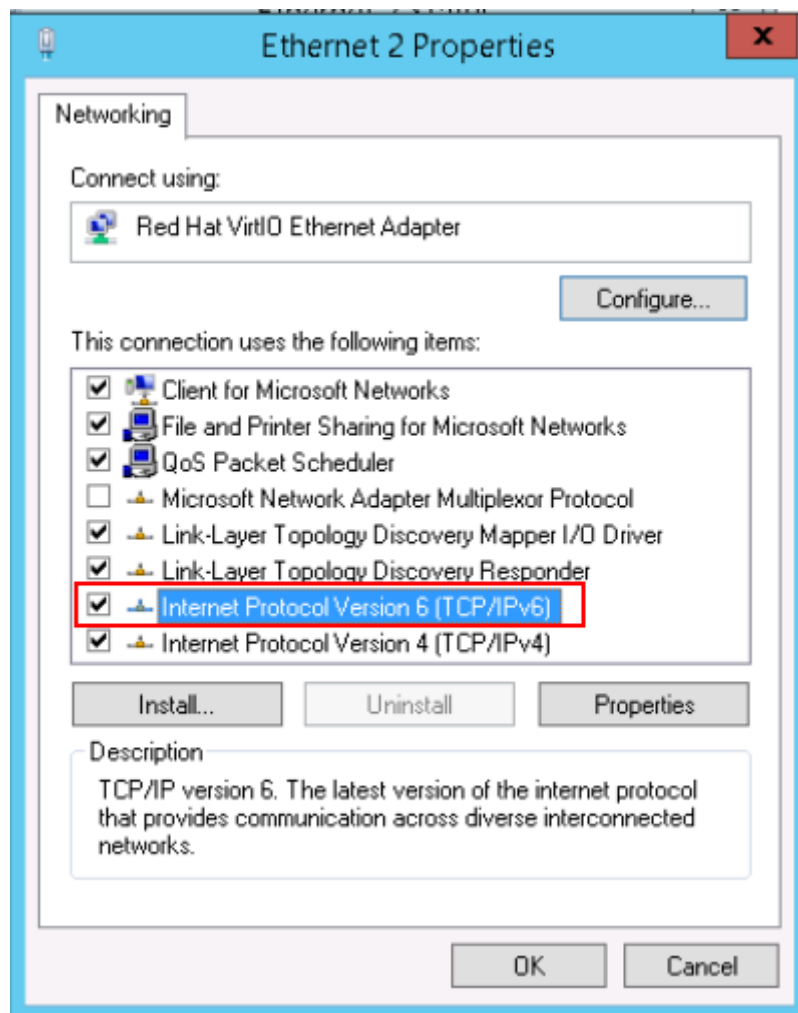
6. Perform **Step 1** to check whether dynamic IPv6 address assignment is enabled.

Step 3 Enable and configure IPv6.

1. In the **Internet Protocol Version 6 (TCP/IPv6) Properties** dialog box, configure an IPv6 address and a DNS server address.

- **IPv6 address**: IPv6 address allocated during ECS creation. Obtain the value from the ECS list on the console.
- **Subnet prefix length**: **64**
- **Preferred DNS server**: **240c::6666** (recommended)

Figure 8-12 Configuring an IPv6 address and a DNS server address

2. (Optional) Run the following command depending on your ECS OS.

   For Windows Server 2012, run the following command in PowerShell or CMD:

   Set-NetIPv6Protocol -RandomizeIdentifiers disabled

3. Perform **Step 1** to check whether dynamic IPv6 address assignment is enabled.

   ----End

Windows Server 2008

Step 1 Check whether IPv6 is enabled for the ECS.

Run the following command in the CMD window to check it:

ipconfig

- If an IPv6 address and a link-local IPv6 address are displayed, IPv6 is enabled and dynamic IPv6 assignment is also enabled.

Figure 8-13 Querying the IPv6 address
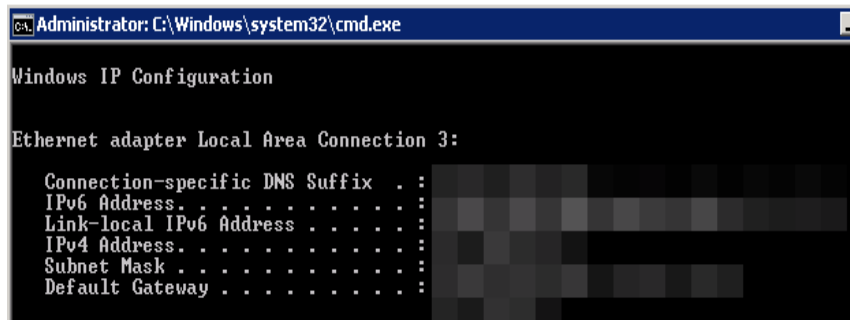
- If only a link-local IPv6 address is displayed, IPv6 is enabled but dynamic IPv6 assignment is not enabled. Go to **Step 2**.

Figure 8-14 Link-local IPv6 address
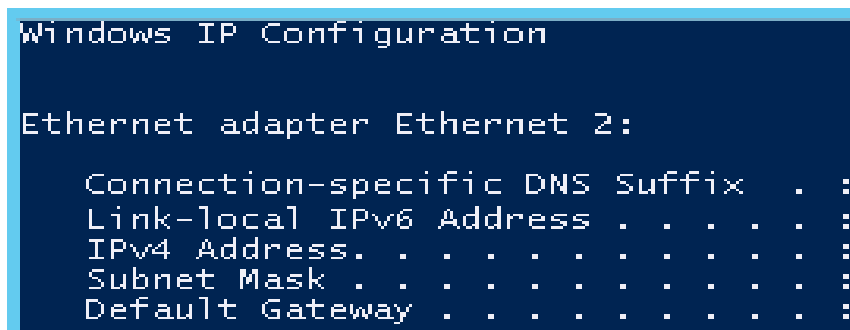
- If neither an IPv6 address nor link-local IPv6 address is displayed, IPv6 is disabled. Go to **Step 3**.

Figure 8-15 IPv6 disabled
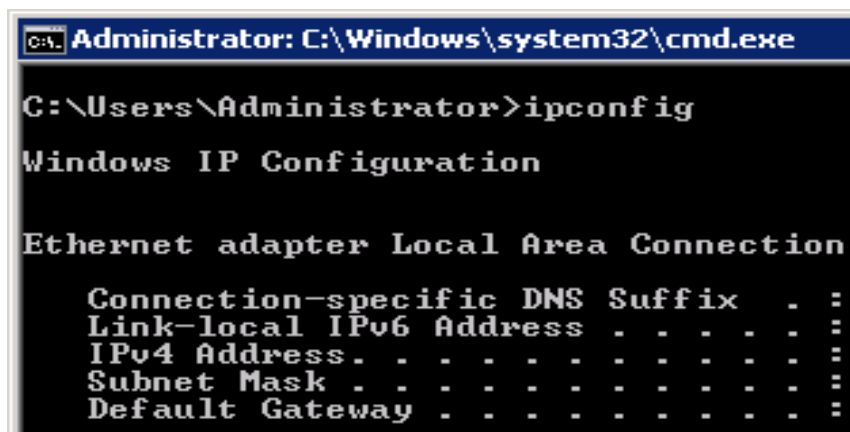
☐ **NOTE**

By default, dynamic IPv6 address assignment is enabled for Windows public images, as shown in **Figure 8-13**. No additional configuration is required.

Step 2 Enable dynamic IPv6 address assignment.

1. Choose **Start** > **Control Panel**.

2. Click **Network and Sharing Center**.

3. Click **Change adapter settings**.

4. Right-click the local network connection and choose **Properties**.

5. Select **Internet Protocol Version 6 (TCP/IPv6)** and click **OK**.

Figure 8-16 Configuring dynamic IPv6 address assignment

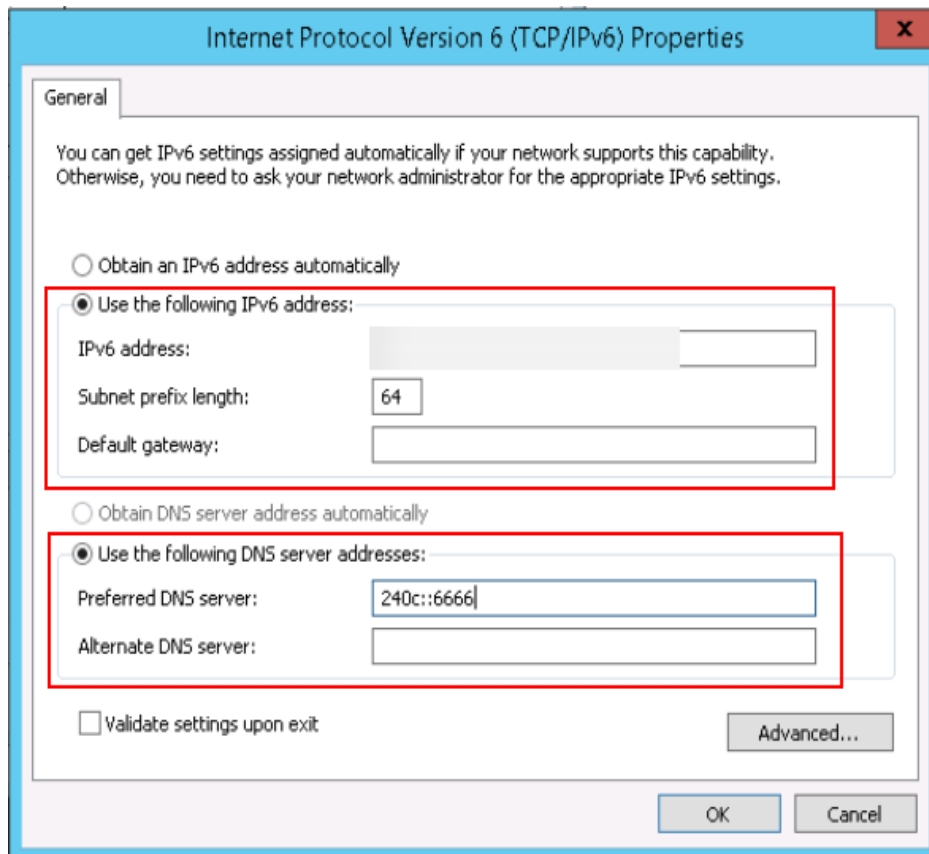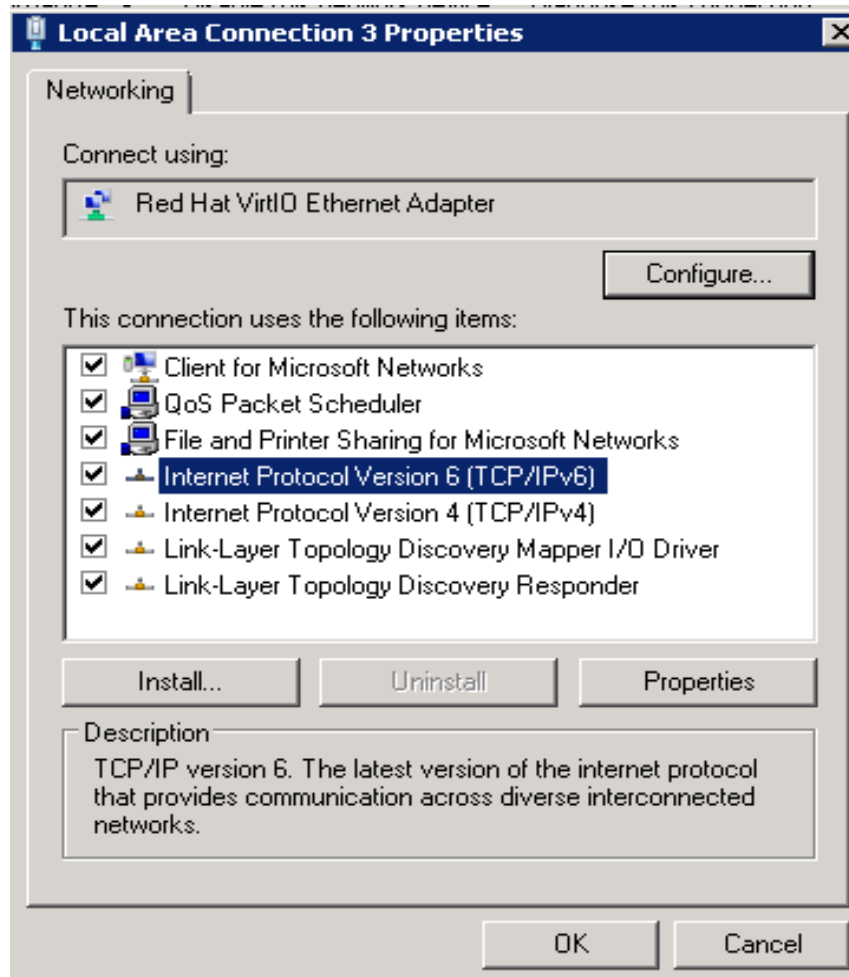6. Perform **Step 1** to check whether dynamic IPv6 address assignment is enabled.

Step 3 Enable and configure IPv6.

1. Choose **Start** > **Control Panel** > **Network Connection** > **Local Connection**.

2. Select **Properties**, select the following options, and click **Install**.

Figure 8-17 Enabling and configuring IPv6
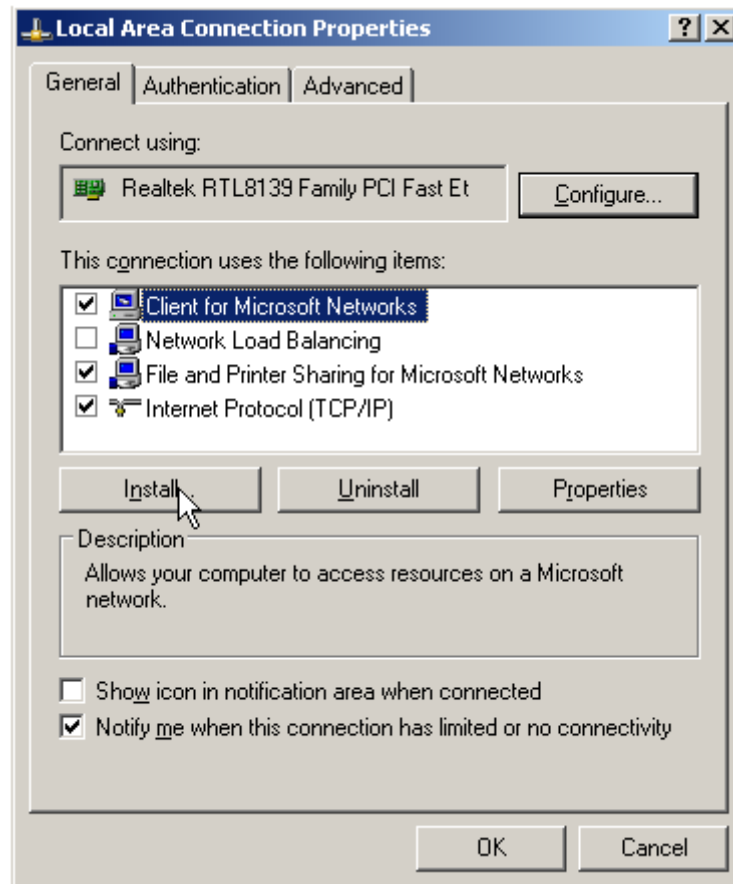
3. Select **Protocol** and click **Add**.

Figure 8-18 Adding the protocol
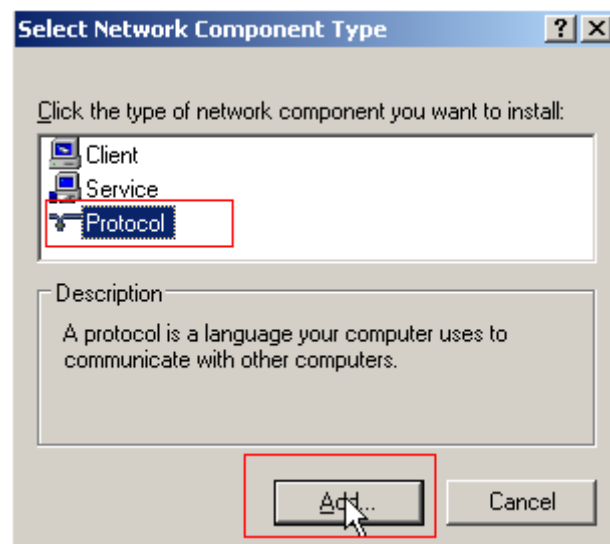
4. Select **Microsoft TCP/IP Version 6** and click **OK**.

Figure 8-19 Network protocols
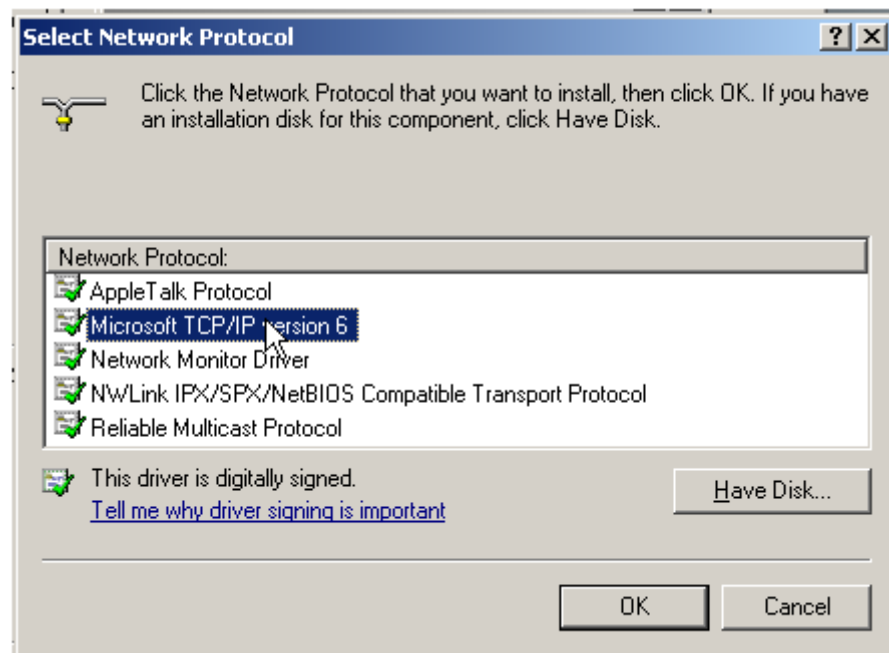
5. (Optional) Run the following commands depending on your ECS OS.

   For Windows Server 2008, run the following command in PowerShell or CMD:

   netsh interface ipv6 set global randomizeidentifiers=disable

   Disable the local connection and then enable it again.

   To disable the local connection, choose **Start** > **Control Panel** > **Network and Internet** > **Network and Sharing Center** > **Change Adapter Options**. Right-click the local connection and choose **Disable** from the shortcut menu.

   To enable the local connection, choose **Start** > **Control Panel** > **Network and Internet** > **Network and Sharing Center** > **Change Adapter Options**. Right-click the local connection and choose **Enable** from the shortcut menu.

6. Perform **Step 1** to check whether dynamic IPv6 address assignment is enabled.

   ----End

Linux (Automatically Enabling Dynamic Assignment of IPv6 Addresses)

The **ipv6-setup-**_xxx_ tool can be used to enable Linux OSs to automatically acquire IPv6 addresses. _xxx_ indicates a tool, which can be rhel or debian.

You can also enable dynamic IPv6 address assignment by following the instructions in **Linux (Manually Enabling Dynamic Assignment of IPv6 Addresses)**.

> **CAUTION**
>
> - When you run **ipv6-setup-**_xxx_, the network service will be automatically restarted. As a result, the network is temporarily disconnected.
> - If a private image created from a CentOS 6.x or Debian ECS with automatic IPv6 address assignment enabled is used to create an ECS in an environment that does not support IPv6, the ECS may start slow because of IPv6 address assignment timeout. Set the timeout duration for assigning IPv6 addresses to 30s by referring to **Setting the Timeout Duration for IPv6 Address Assignment** and try to create a new private image again.

Step 1 Run the following command to check whether IPv6 is enabled for the ECS:

ip addr

- If only an IPv4 address is displayed, IPv6 is disabled. Enable it by referring to **Setting the Timeout Duration for IPv6 Address Assignment**.

  Figure 8-20 IPv6 disabled

  ```
  eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP qlen 1000
  link/ether fa:16:3e:          brd ff:ff:ff:ff:ff:ff
  inet              brd              scope global noprefixroute dynamic eth0
      valid_lft 1193sec preferred_lft 1193sec
  ```

- If a link-local address (starting with fe80) is displayed, IPv6 is enabled but dynamic assignment of IPv6 addresses is not enabled.

  Figure 8-21 IPv6 enabled

  ```
  eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
  link/ether fa:16:3e:          brd ff:ff:ff:ff:ff:ff
  inet              brd              scope global noprefixroute dynamic eth0
      valid_lft 76391sec preferred_lft 76391sec
  inet6 fe80::f816:              /64 scope link
      valid_lft forever preferred_lft forever
  ```

- If the following address is displayed, IPv6 is enabled and an IPv6 address has been assigned:

  Figure 8-22 IPv6 enabled and an IPv6 address assigned

  ```
  eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
  link/ether fa:16:3e:75:af:4c brd ff:ff:ff:ff:ff:ff
  inet              brd              scope global noprefixroute dynamic eth0
      valid_lft 86395sec preferred_lft 86395sec
  inet6 2407:c080:802:                         /128 scope global dynamic
      valid_lft 7496sec preferred_lft 7196sec
  inet6 fe80::f816:3eff:          /64 scope link noprefixroute
      valid_lft forever preferred_lft forever
  ```

> **NOTE**
>
> IPv6 is enabled for Linux public images by default, as shown in **Figure 8-21**.

Step 2 Enable IPv6 for the ECS.

1. Run the following command to check whether IPv6 is enabled for the kernel:

   sysctl -a | grep ipv6

   – If a command output is displayed, IPv6 is enabled.

   – If no information is displayed, IPv6 is disabled. Go to **Step 2.2** to load the IPv6 module.

2. Run the following command to load the IPv6 module:

   modprobe ipv6

3. Add the following content to the **/etc/sysctl.conf** file:

   net.ipv6.conf.all.disable_ipv6=0

4. Save the configuration and exit. Then, run the following command to load the configuration:

   sysctl -p

Step 3 Enable dynamic IPv6 address assignment for the ECS.

1. Download **ipv6-setup-rhel** or **ipv6-setup-debian** with a required version and upload it to the target ECS.

   ipv6-setup-*xxx* modifies the configuration file of a NIC to enable dynamic IPv6 address assignment or adds such a configuration file for a NIC, and then restarts the NIC or network service. **Table 8-8** lists the download paths of **ipv6-setup-rhel** and **ipv6-setup-debian**.

   Table 8-8 Download paths of ipv6-setup-rhel and ipv6-setup-debian

Series	Release Version	How to Obtain
RHEL	– CentOS 6/7 – EulerOS 2.2/2.3 – Fedora 25	**https://ecs-instance-driver.obs.cn-north-1.myhuaweicloud.com/ipv6/ipv6-setup-rhel**
Debian	– Ubuntu 16/18 – Debian 8/9/10	**https://ecs-instance-driver.obs.cn-north-1.myhuaweicloud.com/ipv6/ipv6-setup-debian**

2. Run the following command to make **ipv6-setup-***xxx* executable:

   chmod +x ipv6-setup-*xxx*

3. Run the following command to enable dynamic IPv6 address assignment for a NIC:

   ./ipv6-setup-*xxx* **--dev** [*dev*]

   Example:

   ./ipv6-setup-*xxx* **--dev eth0**

   ▢ NOTE

   – To enable dynamic IPv6 address assignment for all NICs, run the **./ipv6-setup-***xxx* command.

   – To learn how to use **ipv6-setup-***xxx*, run the **./ipv6-setup-***xxx* **--help** command.

----End

Linux (Manually Enabling Dynamic Assignment of IPv6 Addresses)

> ⚠️ **CAUTION**
>
> If a private image created from a CentOS 6.x or Debian ECS with automatic IPv6 address assignment enabled is used to create an ECS in an environment that does not support IPv6, the ECS may start slow because of IPv6 address assignment timeout. Set the timeout duration for assigning IPv6 addresses to 30s by referring to **Setting the Timeout Duration for IPv6 Address Assignment** and try to create a new private image again.

Step 1 Run the following command to check whether IPv6 is enabled for the ECS:

ip addr

- If only an IPv4 address is displayed, IPv6 is disabled. Enable it by referring to **Step 2**.

  Figure 8-23 IPv6 disabled

  ```
  eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP qlen 1000
      link/ether fa:16:3e:          brd ff:ff:ff:ff:ff:ff
      inet                   brd                  scope global noprefixroute dynamic eth0
         valid_lft 1193sec preferred_lft 1193sec
  ```

- If a link-local address (starting with fe80) is displayed, IPv6 is enabled but dynamic assignment of IPv6 addresses is not enabled.

  Figure 8-24 IPv6 enabled

  ```
  eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
      link/ether fa:16:3e:          brd ff:ff:ff:ff:ff:ff
      inet                   brd                  scope global noprefixroute dynamic eth0
         valid_lft 76391sec preferred_lft 76391sec
      inet6 fe80::f816:                  /64 scope link
         valid_lft forever preferred_lft forever
  ```

- If the following address is displayed, IPv6 is enabled and an IPv6 address has been assigned:

  Figure 8-25 IPv6 enabled and an IPv6 address assigned

  ```
  eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
      link/ether fa:16:3e:75:af:4c brd ff:ff:ff:ff:ff:ff
      inet                  brd              scope global noprefixroute dynamic eth0
         valid_lft 86395sec preferred_lft 86395sec
      inet6 2407:c080:802:                         /128 scope global dynamic
         valid_lft 7496sec preferred_lft 7196sec
      inet6 fe80::f816:3eff:             /64 scope link noprefixroute
         valid_lft forever preferred_lft forever
  ```

📖 **NOTE**

IPv6 is enabled for Linux public images by default, as shown in **Figure 8-24**.

Step 2 Enable IPv6 for the ECS.

1. Run the following command to check whether IPv6 is enabled for the kernel:

    sysctl -a | grep ipv6

    - If a command output is displayed, IPv6 is enabled.
    - If no information is displayed, IPv6 is disabled. Go to **Step 2.2** to load the IPv6 module.

2. Run the following command to load the IPv6 module:

modprobe ipv6

3. Add the following content to the **/etc/sysctl.conf** file:

net.ipv6.conf.all.disable_ipv6=0

4. Save the configuration and exit. Then, run the following command to load the configuration:

sysctl -p

Step 3 Enable dynamic IPv6 address assignment for the ECS.

- Ubuntu 18.04/20.04

    a. Run the following command to access **/etc/netplan/**:

    cd /etc/netplan

    b. Run the following command to list the configuration file:

    ls

    Figure 8-26 Configuration file name

    c. Run the following command to edit the configuration file:

    vi 01-network-manager-all.yaml

    d. Append the following content to the configuration file (pay attention to the yaml syntax and text indentation):

    ```
    ethernets:
     eth0:
      dhcp6: true
    ```

    Figure 8-27 Edited configuration file

    Save the changes and exit.

    e. Run the following command to make the changes take effect:

    sudo netplan apply

- Ubuntu 22.04

    a. Run the following command to access **/etc/netplan/**:

    cd /etc/netplan

    b. Run the following command to list the configuration file:

    ls
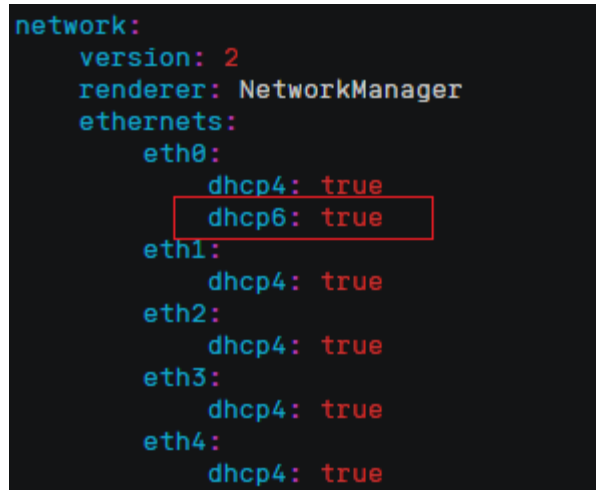
    Figure 8-28 Configuration file name

c. Run the following command to edit the configuration file:

vi 01-netcfg.yaml

d. Append the following content to the configuration file **01-netcfg.yaml** (pay attention to the yaml syntax and text indentation):

```
ethernets:
 eth0:
  dhcp6: true
```

Figure 8-29 Edited configuration file


```
network:
    version: 2
    renderer: NetworkManager
    ethernets:
        eth0:
            dhcp4: true
            dhcp6: true
        eth1:
            dhcp4: true
        eth2:
            dhcp4: true
        eth3:
            dhcp4: true
        eth4:
            dhcp4: true
```

Save the changes and exit.

e. Run the following command to make the changes take effect:

sudo netplan apply

f. Run the following command to edit **/etc/NetworkManager/ NetworkManager.conf**:

vi /etc/NetworkManager/NetworkManager.conf

g. Append the following content to the configuration file **NetworkManager.conf** (pay attention to the file format and indentation):

```
[main]
plugins=ifupdown,keyfile
dhcp=dhclient

[ifupdown]
managed=true

[device]
wifi.scan-rand-mac-address=no
```

Figure 8-30 Modification result


```
[main]
plugins=ifupdown,keyfile
dhcp=dhclient

[ifupdown]
managed=true

[device]
wifi.scan-rand-mac-address=no
```

    h.   Run the following command for the configuration to take effect:

        systemctl restart NetworkManager

- Debian

  a. Add the following content to the **/etc/network/interfaces** file:
     ```
     auto lo
     iface lo inet loopback
     auto eth0
     iface eth0 inet dhcp
     iface eth0 inet6 dhcp
         pre-up sleep 3
     ```

  b. Add configurations for each NIC to the **/etc/network/interfaces** file. The following uses eth1 as an example:
     ```
     auto eth1
     iface eth1 inet dhcp
     iface eth1 inet6 dhcp
         pre-up sleep 3
     ```

  c. Run the following command to restart the network service:

     service networking restart

     ◡ **NOTE**

     If no IPv6 address is assigned after the NICs are brought down and up, you can run this command to restart the network.

  d. Perform **Step 1** to check whether dynamic IPv6 address assignment is enabled.

- CentOS, EulerOS, or Fedora

  a. Open the configuration file **/etc/sysconfig/network-scripts/ifcfg-eth0** of the primary NIC.

     Add the following configuration items to the file:
     ```
     IPV6INIT=yes
     DHCPV6C=yes
     ```

  b. Edit the **/etc/sysconfig/network** file to add or modify the following line:
     ```
     NETWORKING_IPV6=yes
     ```

  c. For an ECS running CentOS 6, you need to edit the configuration files of its extension NICs. For example, if the extension NIC is eth1, you need to edit **/etc/sysconfig/network-scripts/ifcfg-eth1**.

     Add the following configuration items to the file:
     ```
     IPV6INIT=yes
     DHCPV6C=yes
     ```

     In CentOS 6.3, dhcpv6-client requests are filtered by **ip6tables** by default. So, you also need to add a rule allowing the dhcpv6-client request to the **ip6tables** file.

      i.   Run the following command to add the rule to **ip6tables**:

         ip6tables -A INPUT -m state --state NEW -m udp -p udp --dport 546 -d fe80::/64 -j ACCEPT

      ii.   Run the following command to save the rule in **ip6tables**:

         service ip6tables save

Figure 8-31 Example command

```
[root@ecs-cd02 log]# ip6tables -A INPUT -m state --state NEW -m udp -p udp --dport 546 -d fe80::/64 -j ACCEPT
nf_conntrack version 0.5.0 (7964 buckets, 31856 max)
[root@ecs-cd02 log]# service ip6tables save
ip6tables: Saving firewall rules to /etc/sysconfig/ip6table[  OK  ]
```

   d.   (Optional) For CentOS 7/CentOS 8, change the IPv6 link-local address mode of extension NICs to EUI64.

      i.   Run the following command to query the NIC information:

         nmcli con

Figure 8-32 Querying NIC information

```
[root@ecs-166b ~]# nmcli con
NAME                UUID                                    TYPE      DEVICE
System eth0         5fb06bd0-0bb0-7ffb-45f1-d6edd65f3e03    ethernet  eth0
Wired connection 1  9c92fad9-6ecb-3e6c-eb4d-8a47c6f50c04    ethernet  eth1
Wired connection 1  3a73717e-65ab-93e8-b518-24f5af32dc0d    ethernet  eth2
```

      ii.   Run the following command to change the IPv6 link-local address mode of eth1 to EUI64:

         nmcli con modify "*Wired connection 1***" ipv6.addr-gen-mode eui64**

         📖 **NOTE**

           The NIC information varies depending on the CentOS series. In the command, *Wired connection 1* needs to be replaced with the value in the **NAME** column of the queried NIC information.

      iii. Run the following commands to bring eth1 down and up:

         ifdown eth1

         ifup eth1

   e.   Restart the network service.

      i.   For CentOS 6, run the following command to restart the network service:

         service network restart

      ii.   For CentOS 7/EulerOS/Fedora, run the following command to restart the network service:

         systemctl restart NetworkManager

   f.   Perform **Step 1** to check whether dynamic IPv6 address assignment is enabled.

- SUSE, openSUSE, or CoreOS

   SUSE 11 SP4 does not support dynamic IPv6 address assignment.

   No additional configuration is required for SUSE 12 SP1 or SUSE 12 SP2.

   No additional configuration is required for openSUSE 13.2 or openSUSE 42.2.

No additional configuration is required for CoreOS 10.10.5.

----End

Setting the Timeout Duration for IPv6 Address Assignment

After automatic IPv6 address assignment is configured on an ECS running CentOS 6.x or Debian, the ECS will be created as a private image. When this image is used to create an ECS in an environment that IPv6 is unavailable, the ECS may start slow because acquiring an IPv6 address times out. Before creating the private image, you can set the timeout duration for acquiring IPv6 addresses to 30s as follows:

- CentOS 6.x:

    a. Run the following command to edit the **dhclient.conf** file:

       vi /etc/dhcp/dhclient.conf

    b. Press **i** to enter editing mode and add the timeout attribute to the file.
       ```
       timeout  30;
       ```

    c. Enter **:wq** to save the settings and exit.

- Debian 7.5:

    a. Run the following command to edit the **networking** file:

       vi /etc/init.d/networking

    b. Press **i** to enter editing mode and add the timeout attribute.

      Figure 8-33 Modification 1

Figure 8-34 Modification 2

- Debian 8.2.0/8.8.0

  a. Run the following command to edit the **network-pre.conf** file:

     vi /lib/systemd/system/networking.service.d/network-pre.conf

  b. Press *i* to enter editing mode and add the timeout attribute to the file.
     ```
     [Service]
     TimeoutStartSec=30
     ```

- Debian 9.0

  a. Run the following command to edit the **networking.service** file:

     **vi /etc/system/system/network-online.target.wants/
     networking.service**

  b. Press **i** to enter editing mode and change **TimeoutStartSec=5min** to
     TimeoutStartSec=30.

8.11 How Do I Make a System Disk Image Support Fast ECS Creation?

Scenarios

Fast Create greatly reduces the time required for creating ECSs from a system disk image. Currently, this feature is supported by all newly created system disk images by default. Some existing system disk images may not support this feature, you can make them support it through image replication.

For example, if image A does not support fast ECS creation, you can replicate it to generate image copy_A that supports fast ECS creation.

Constraints

Full-ECS images and ISO images cannot be configured using this method.

Check Whether an Image Supports Fast ECS Creation

1. Access the IMS console.

   a. Log in to the management console.

      b. Under **Compute**, click **Image Management Service**.

         The IMS console is displayed.

2. Click the **Private Images** tab to display the image list.

3. Click the name of the target image.

4. On the displayed image details page, check the value of **Fast ECS Creation**.

Figure 8-35 Image details

Name	newCloudinit-Image	ID	e587771f-9920-456f-a987-b00792c4d326
Image Type	System disk image	Disk Capacity (GB)	40
OS	Windows Server 2016 Datacenter 64bit	Status	✅ Normal
Minimum Memory	Unlimited	Image Size	7.21 GB
Maximum Memory	Unlimited	Released ❓	No
Created	2023/01/28 17:30:38 GMT+08:00	Completed	2023/01/28 17:38:58 GMT+08:00
Source	ECS --	Description	--
Encrypted	No	OS Type	Windows
NIC Multi-Queue	Supported	Enterprise Project	default
Fast ECS Creation ❓	Supported		

Configure an Image to Make It Support Fast ECS Creation

1. Locate the target system disk image, click **More** in the **Operation** column, and select **Replicate** from the drop-down list.

   The **Replicate Image** dialog box is displayed.

2. Set **Replication Mode** to **Within Region** and set other parameters based on **Replicating Images Within a Region**.

3. After the image is successfully replicated, the generated image can be used to quickly create ECSs.

8.12 Whey Do I Fail to Install Guest OS Drivers on a Windows ECS?

Possible causes:

- Your image file was exported from a VMware VM, and VMware Tools was not uninstalled or not completely uninstalled.

- You have downloaded Guest OS drivers of an incorrect version for your Windows ECS.

- The disk space available for installing Guest OS drivers is insufficient. Ensure that the disk where Guest OS drivers are installed has at least 300 MB space available.

8.13 How Do I Install Native Xen and KVM Drivers?

Scenarios

When optimizing a Linux private image with Xen virtualization, you need to install native Xen and KVM drivers on the source ECS of the image.

This section describes how to install native Xen and KVM drivers.

⚠️ **CAUTION**

If an ECS has no Xen drivers installed, the network performance of the ECS will be poor, and the security groups and firewall configured for the ECS will not take effect.

If an ECS has no KVM drivers installed, the NICs of the ECS may not be detected and the ECS will be unable to communicate with other resources.

Prerequisites

- The virtualization type of the ECS is Xen. For details, see **Viewing the Virtualization Type of a Linux ECS**.
- The kernel version must be later than 2.6.24.
- Disable your antivirus and intrusion detection software. You can enable them after the driver installation is complete.

Procedure

Modify the configuration file depending on the OS.

- CentOS, EulerOS

  Take CentOS 7.0 as an example. Modify the **/etc/dracut.conf** file. Add the Xen PV and VirtIO drivers to **add_drivers**. Xen PV drivers include xen-blkfront and xen-netfront. VirtIO drivers include virtio_blk, virtio_scsi, virtio_net, virtio_pci, virtio_ring, and virtio. Separate driver names with spaces. Save and exit the **/etc/dracut.conf** file. Run the **dracut -f** command to regenerate initrd.

  For details, see **CentOS and EulerOS**.

- Ubuntu and Debian

  Modify the **/etc/initramfs-tools/modules** file. Add the Xen PV and VirtIO drivers. Xen PV drivers include xen-blkfront and xen-netfront. VirtIO drivers include virtio_blk, virtio_scsi, virtio_net, virtio_pci, virtio_ring, and virtio. Separate driver names with spaces. Save and exit the **/etc/initramfs-tools/modules** file. Run the **update-initramfs -u** command to regenerate initrd.

  For details, see **Ubuntu and Debian**.

- SUSE and openSUSE

  - If the OS version is earlier than SUSE 12 SP1 or openSUSE 13, modify the **/etc/sysconfig/kernel** file and add Xen PV and VirtIO drivers to **INITRD_MODULES=""**. Xen PV drivers include xen_vnif, xen_vbd, and

xen_platform_pci. VirtIO drivers include virtio_blk, virtio_scsi, virtio_net, virtio_pci, virtio_ring, and virtio. Separate driver names with spaces. Run the **mkinitrd** command to regenerate initrd.

– If the OS version is SUSE 12 SP1, modify the **/etc/dracut.conf** file and add Xen PV and VirtIO drivers to **add_drivers**. Xen PV drivers include xen_vnif, xen_vbd, and xen_platform_pci. VirtIO drivers include virtio_blk, virtio_scsi, virtio_net, virtio_pci, virtio_ring, and virtio. Separate driver names with spaces. Run the **dracut -f** command to regenerate initrd.

– If the OS version is later than SUSE 12 SP1 or openSUSE 13, modify the **/etc/dracut.conf** file and add Xen PV and VirtIO drivers to **add_drivers**. Xen PV drivers include xen-blkfront and xen-netfront. VirtIO drivers include virtio_blk, virtio_scsi, virtio_net, virtio_pci, virtio_ring, and virtio. Separate driver names with spaces. Save and exit the **/etc/dracut.conf** file. Run the **dracut -f** command to regenerate initrd.

For details, see **SUSE and openSUSE**.

☐ NOTE

For SUSE, run the following command to check whether xen-kmp (driver package for Xen PV) is installed:

rpm -qa |grep xen-kmp

If information similar to the following is displayed, xen-kmp is installed in the OS:

xen-kmp-default-4.2.2_04_3.0.76_0.11-0.7.5

If xen-kmp is not installed, obtain it from the ISO file and install it.

If you add built-in drivers to the initrd or initramfs file by mistake, the ECS will not be affected.

CentOS and EulerOS

1. Run the following command to open the **/etc/dracut.conf** file:

   vi /etc/dracut.conf

2. Press **i** to enter editing mode and add Xen PV and VirtIO drivers to **add_drivers** (the format varies depending on the OS).

   ```
   [root@CTU10000xxxxx ~]# vi /etc/dracut.conf
   # additional kernel modules to the default
   add_drivers+="xen-blkfront xen-netfront virtio_blk virtio_scsi virtio_net virtio_pci virtio_ring virtio"
   ……
   ```

3. Press **Esc**, enter **:wq**, and press **Enter**. The system saves the change and exits the **/etc/dracut.conf** file.

4. Run the following command to regenerate initrd:

   dracut -f /boot/initramfs-2.6.32-573.8.1.el6.x86_64.img

   If the virtual file system is not the default initramfs, run the **dracut -f** *Name of the initramfs or initrd file actually used* command. The actual initramfs or initrd file name can be obtained from the **grub.cfg** file, which can be **/boot/grub/grub.cfg**, **/boot/grub2/grub.cfg**, or **/boot/grub/grub.conf** depending on the OS.

5. If the virtual file system is initramfs, run the following commands to check whether native Xen and KVM drivers have been installed:

   lsinitrd /boot/initramfs-`uname -r`.img | grep xen

   lsinitrd /boot/initramfs-`uname -r`.img | grep virtio

If the virtual file system is initrd, run the following commands to check whether native Xen and KVM drivers have been installed:

lsinitrd /boot/initrd-`uname -r` | grep xen

lsinitrd /boot/initrd-`uname -r` | grep virtio

Assume that the virtual file system is initramfs. The following command output will be displayed:

```
[root@CTU10000xxxxx home]# lsinitrd /boot/initramfs-`uname -r`.img | grep xen
-rwxr--r-- 1 root     root        54888 Jul 16 17:53 lib/modules/2.6.32-573.8.1.el6.x86_64/kernel/drivers/
block/xen-blkfront.ko
-rwxr--r-- 1 root     root        45664 Jul 16 17:53 lib/modules/2.6.32-573.8.1.el6.x86_64/kernel/
drivers/net/xen-netfront.ko

[root@CTU10000xxxxx home]# lsinitrd /boot/initramfs-`uname -r`.img | grep virtio
-rwxr--r-- 1 root     root        23448 Jul 16 17:53 lib/modules/2.6.32-573.8.1.el6.x86_64/kernel/drivers/
block/virtio_blk.ko
-rwxr--r-- 1 root     root        50704 Jul 16 17:53 lib/modules/2.6.32-573.8.1.el6.x86_64/kernel/
drivers/net/virtio_net.ko
-rwxr--r-- 1 root     root        28424 Jul 16 17:53 lib/modules/2.6.32-573.8.1.el6.x86_64/kernel/drivers/
scsi/virtio_scsi.ko
drwxr-xr-x 2 root     root            0 Jul 16 17:53 lib/modules/2.6.32-573.8.1.el6.x86_64/kernel/drivers/
virtio
-rwxr--r-- 1 root     root        14544 Jul 16 17:53 lib/modules/2.6.32-573.8.1.el6.x86_64/kernel/drivers/
virtio/virtio.ko
-rwxr--r-- 1 root     root        21040 Jul 16 17:53 lib/modules/2.6.32-573.8.1.el6.x86_64/kernel/drivers/
virtio/virtio_pci.ko
-rwxr--r-- 1 root     root        18016 Jul 16 17:53 lib/modules/2.6.32-573.8.1.el6.x86_64/kernel/drivers/
virtio/virtio_ring.ko
```

📖 **NOTE**

If you add built-in drivers to the initrd or initramfs file by mistake, the ECS will not be affected. The drivers cannot be found by running the **lsinitrd** command. You can run the following commands to check whether built-in drivers are in the kernel:

cat /boot/config-`uname -r` | grep CONFIG_VIRTIO | grep y

cat /boot/config-`uname -r` | grep CONFIG_XEN | grep y

Ubuntu and Debian

1. Run the following command to open the **modules** file:

   vi /etc/initramfs-tools/modules

2. Press **i** to enter editing mode and add Xen PV and VirtIO drivers to the **/etc/initramfs-tools/modules** file (the format varies depending on the OS).

   ```
   [root@CTU10000xxxxx ~]#vi /etc/initramfs-tools/modules
   ……
   # Examples:
   #
   # raid1
   # sd_mOd
   xen-blkfront
   xen-netfront
   virtio_blk
   virtio_scsi
   virtio_net
   virtio_pci
   virtio_ring
   virtio
   ```

3. Press **Esc**, enter **:wq**, and press **Enter**. The system saves the change and exits the **/etc/initramfs-tools/modules** file.

4. Run the following command to regenerate initrd:

   update-initramfs -u

5. Run the following commands to check whether native Xen and KVM drivers have been installed:

lsinitramfs /boot/initrd.img-`uname -r` |grep xen

lsinitramfs /boot/initrd.img-`uname -r` |grep virtio

```
[root@ CTU10000xxxxx home]# lsinitramfs /boot/initrd.img-`uname -r` |grep xen
lib/modules/3.5.0-23-generic/kernel/drivers/net/ethernet/qlogic/netxen
lib/modules/3.5.0-23-generic/kernel/drivers/net/ethernet/qlogic/netxen/netxen_nic.ko
lib/modules/3.5.0-23-generic/kernel/drivers/net/xen-netback
lib/modules/3.5.0-23-generic/kernel/drivers/net/xen-netback/xen-netback.ko
lib/modules/3.5.0-23-generic/kernel/drivers/block/xen-blkback
lib/modules/3.5.0-23-generic/kernel/drivers/block/xen-blkback/xen-blkback.ko

[root@ CTU10000xxxxx home]# lsinitramfs /boot/initrd.img-`uname -r` |grep virtio
lib/modules/3.5.0-23-generic/kernel/drivers/scsi/virtio_scsi.ko
```

□ NOTE

If you add built-in drivers to the initrd or initramfs file by mistake, the ECS will not be affected. The drivers cannot be found by running the **lsinitrd** command. You can run the following commands to check whether built-in drivers are in the kernel:

```
[root@ CTU10000xxxxx home]# cat /boot/config-`uname -r` | grep CONFIG_VIRTIO | grep y
CONFIG_VIRTIO_BLK=y
CONFIG_VIRTIO_NET=y
CONFIG_VIRTIO=y
CONFIG_VIRTIO_RING=y
CONFIG_VIRTIO_PCI=y
CONFIG_VIRTIO_MMIO_CMDLINE_DEVICES=y
[root@ CTU10000xxxxx home]# cat /boot/config-`uname -r` | grep CONFIG_XEN | grep y
CONFIG_XEN_BLKDEV_FRONTEND=y
CONFIG_XEN_NETDEV_FRONTEND=y
```

SUSE and openSUSE

If the OS version is earlier than SUSE 12 SP1 or openSUSE 13, modify the **/etc/sysconfig/kernel** file to add drivers. For details, see **scenario 1**.

If the OS version is SUSE 12 SP1, modify the **/etc/dracut.conf** file to add drivers. For details, see **scenario 2**.

If the OS version is later than SUSE 12 SP1 or openSUSE 13, modify the **/etc/dracut.conf** file to add drivers. For details, see **scenario 3**.

- If the OS version is earlier than SUSE 12 SP1 or openSUSE 13, perform the following steps:

  □ NOTE

  For SUSE, run the following command to check whether xen-kmp (driver package for Xen PV) is installed in the OS:

  rpm -qa |grep xen-kmp

  If information similar to the following is displayed, xen-kmp is installed:

  ```
  xen-kmp-default-4.2.2_04_3.0.76_0.11-0.7.5
  ```

  If xen-kmp is not installed, obtain it from the installation ISO and install it first.

  a. Run the following command to open the **/etc/sysconfig/kernel** file:

     vi /etc/sysconfig/kernel

  b. Add Xen PV and VirtIO drivers after **INITRD_MODULES=** (the format varies depending on the OS).

     ```
     SIA10000xxxxx:~ # vi /etc/sysconfig/kernel
     # (like drivers for scsi-controllers, for lvm or reiserfs)
     ```

```
#
INITRD_MODULES="ata_piix ata_generic xen_vnif xen_vbd xen_platform_pci virtio_blk
virtio_scsi virtio_net virtio_pci virtio_ring virtio"
```

c. Run the **mkinitrd** command to regenerate initrd:

📖 NOTE

If the virtual file system is not the default initramfs or initrd, run the **dracut -f** *Name of the initramfs or initrd file actually used* command. The actual initramfs or initrd file name can be obtained from the **menu.lst** or **grub.cfg** file (**/boot/ grub/menu.lst**, **/boot/grub/grub.cfg**, or **/boot/grub2/grub.cfg**).

The following is an example initrd file of SUSE 11 SP4:

```
default 0
timeout 10
gfxmenu (hd0,0)/boot/message
title sles11sp4_001_[_VMX_]
root (hd0,0)
kernel /boot/linux.vmx vga=0x314 splash=silent console=ttyS0,115200n8 console=tty0
net.ifnames=0 NON_PERSISTENT_DEVICE_NAMES=1 showopts
initrd /boot/initrd.vmx
title Failsafe_sles11sp4_001_[_VMX_]
root (hd0,0)
kernel /boot/linux.vmx vga=0x314 splash=silent ide=nodma apm=off noresume edd=off
powersaved=off nohz=off highres=off processsor.max+cstate=1 nomodeset x11failsafe
console=ttyS0,115200n8 console=tty0 net.ifnames=0 NON_PERSISTENT_DEVICE_NAMES=1
showopts
initrd /boot/initrd.vmx
```

/boot/initrd.vmx in the **initrd** line is the initrd file actually used. Run the **dracut -f /boot/initrd.vmx** command. If the initrd file does not contain the **/boot** directory, such as **/initramfs-***xxx*, run the **dracut -f /boot/ initramfs-***xxx* command.

d. Run the following commands to check whether Xen PVOPS and KVM VirtIO have been installed:

lsinitrd /boot/initrd-`uname -r` | grep xen

lsinitrd /boot/initrd-`uname -r` | grep virtio

```
SIA10000xxxxx:~ # lsinitrd /boot/initrd-`uname -r` | grep xen
-rwxr--r-- 1 root root 42400 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/block/
xen-blkfront.ko
-rwxr--r-- 1 root root 44200 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/net/
xen-netfront.ko

SIA10000xxxxx:~ # lsinitrd /boot/initrd-`uname -r` | grep virtio
-rwxr--r-- 1 root root 19248 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/scsi/
virtio_scsi.ko
-rwxr--r-- 1 root root 23856 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/block/
virtio_blk.ko
drwxr-xr-x 2 root root 0 Jul 12 14:53 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/virtio
-rwxr--r-- 1 root root 15848 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/virtio/
virtio_ring.ko
-rwxr--r-- 1 root root 20008 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/virtio/
virtio_pci.ko
-rwxr--r-- 1 root root 12272 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/virtio/
virtio.ko
-rwxr--r-- 1 root root 38208 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/net/
virtio_net.ko
```

e. Restart the ECS.

f. Modify the **/boot/grub/menu.lst** file. Add **xen_platform_pci.dev_unplug=all** and modify the root configuration.

Before the modification:

```
###Don't change this comment -YaST2 identifier: Original name: linux###
title SUSE Linux Enterprise Server 11SP4 - 3.0.76-0.11 (default)
```

```
root (hd0,0)
kernel /boot/vmlinuz-3.0.76-0.11-default root=UUID=4eb40294-4c6f-4384-bbb6-
b8795bbb1130 splash=silentcrashkernel=256M-:128M showopts vga=0x314
initrd /boot/initrd-3.0.76-0.11-default
```

After the modification:

```
###Don't change this comment -YaST2 identifier: Original name: linux###
title SUSE Linux Enterprise Server 11SP4 - 3.0.76-0.11 (default)
root (hd0,0)
kernel /boot/vmlinuz-3.0.76-0.11-default root=UUID=4eb40294-4c6f-4384-bbb6-
b8795bbb1130 splash=silentcrashkernel=256M-:128M showopts vga=0x314
xen_platform_pci.dev_unplug=all
initrd /boot/initrd-3.0.76-0.11-default
```

☐ NOTE

- Ensure that the root partition is in the UUID format.

- **xen_platform_pci.dev_unplug=all** is added to shield QEMU devices.

- For SUSE 11 SP1 64bit to SUSE 11 SP4 64bit, add
  xen_platform_pci.dev_unplug=all to the **menu.lst** file. For SUSE 12 or later,
  QEMU device shield is enabled by default, and you do not need to configure
  it.

g. Run the following commands to check whether Xen drivers exist in initrd:

lsinitrd /boot/initrd-`uname -r` | grep xen

lsinitrd /boot/initrd-`uname -r` | grep virtio

```
SIA10000xxxxx:~ # lsinitrd /boot/initrd-`uname -r` | grep xen
-rwxr--r-- 1 root root 42400 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/block/
xen-blkfront.ko
-rwxr--r-- 1 root root 44200 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/net/
xen-netfront.ko

SIA10000xxxxx:~ # lsinitrd /boot/initrd-`uname -r` | grep virtio
-rwxr--r-- 1 root root 19248 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/scsi/
virtio_scsi.ko
-rwxr--r-- 1 root root 23856 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/block/
virtio_blk.ko
drwxr-xr-x 2 root root 0 Jul 12 14:53 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/virtio
-rwxr--r-- 1 root root 15848 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/virtio/
virtio_ring.ko
-rwxr--r-- 1 root root 20008 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/virtio/
virtio_pci.ko
-rwxr--r-- 1 root root 12272 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/virtio/
virtio.ko
-rwxr--r-- 1 root root 38208 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/net/
virtio_net.ko
```

☐ NOTE

If you add built-in drivers to the initrd or initramfs file, the ECS will not be
affected. This makes it easy to modify the drivers. However, you cannot check the
drivers by running the **lsinitrd** command. You can run the following commands
to check whether built-in drivers are in the kernel:

cat /boot/config-`uname -r` | grep CONFIG_VIRTIO | grep y

cat /boot/config-`uname -r` | grep CONFIG_XEN | grep y

- If the OS version is SUSE 12 SP1, perform the following steps:

a. Run the following command to open the **/etc/dracut.conf** file:

vi /etc/dracut.conf

b. Press **i** to enter editing mode and add Xen PV and VirtIO drivers to **add-
drivers** (the format varies depending on the OS).

```
[root@CTU10000xxxxx ~]# vi /etc/dracut.conf
# additional kernel modules to the default
```

```
add_drivers+="ata_piix ata_generic xen_vnif xen_vbd xen_platform_pci virtio_blk virtio_scsi
virtio_net virtio_pci virtio_ring virtio"
```

    c.   Press **Esc**, enter **:wq**, and press **Enter**. The system saves the change and exits the **/etc/dracut.conf** file.

    d.   Run the following command to regenerate initrd:

        dracut -f /boot/initramfs-_File name_

        If the virtual file system is not the default initramfs, run the **dracut -f** _Name of the initramfs or initrd file actually used_ command. The actual initramfs or initrd file name can be obtained from the **grub.cfg** file, which can be **/boot/grub/grub.cfg**, **/boot/grub2/grub.cfg**, or **/boot/grub/grub.conf** depending on the OS.

    e.   If the virtual file system is initramfs, run the following commands to check whether native Xen and KVM drivers have been installed:

        lsinitrd /boot/initramfs-`uname -r`.img | grep xen

        lsinitrd /boot/initramfs-`uname -r`.img | grep virtio

        If the virtual file system is initrd, run the following commands to check whether native Xen and KVM drivers have been installed:

        lsinitrd /boot/initrd-`uname -r` | grep xen

        lsinitrd /boot/initrd-`uname -r` | grep virtio

- If the OS version is later than SUSE 12 SP1 or openSUSE 13, perform the following steps:

  Take SUSE Linux Enterprise Server 12 SP2 (x86_64) as an example.

      a.   Run the following command to open the **/etc/dracut.conf** file:

          vi /etc/dracut.conf

      b.   Press **i** to enter editing mode and add Xen PV and VirtIO drivers to **add_drivers** (the format varies depending on the OS).

```
[root@CTU10000xxxxx ~]# vi /etc/dracut.conf
# additional kernel modules to the default
add_drivers+="ata_piix ata_generic xen-blkfront xen-netfront virtio_blk virtio_scsi
virtio_net virtio_pci virtio_ring virtio"
```

      c.   Press **Esc**, enter **:wq**, and press **Enter**. The system saves the change and exits the **/etc/dracut.conf** file.

      d.   Run the following command to regenerate initrd:

          dracut -f /boot/initramfs-_File name_

          If the virtual file system is not the default initramfs, run the **dracut -f** _Name of the initramfs or initrd file actually used_ command. The actual initramfs or initrd file name can be obtained from the **grub.cfg** file, which can be **/boot/grub/grub.cfg**, **/boot/grub2/grub.cfg**, or **/boot/grub/grub.conf** depending on the OS.

      e.   If the virtual file system is initramfs, run the following commands to check whether native Xen and KVM drivers have been installed:

          lsinitrd /boot/initramfs-`uname -r`.img | grep xen

          lsinitrd /boot/initramfs-`uname -r`.img | grep virtio

          If the virtual file system is initrd, run the following commands to check whether the native Xen and KVM drivers have been installed:

          lsinitrd /boot/initrd-`uname -r` | grep xen

          lsinitrd /boot/initrd-`uname -r` | grep virtio

Assume that the virtual file system is initrd. The following command output will be displayed:

```
sluo-ecs-30dc:~ # lsinitrd /boot/initrd-`uname -r` | grep xen
-rw-r--r-- 1 root root 69575 Oct 26 2016 lib/modules/4.4.21-69-default/kernel/drivers/block/xen-blkfront.ko
-rw-r--r-- 1 root root 53415 Oct 26 2016 lib/modules/4.4.21-69-default/kernel/drivers/net/xen-netfront.ko
drwxr-xr-x 2 root root 0 Sep 28 10:21 lib/modules/4.4.21-69-default/updates/pvdriver/xen-hcall
-rwxr-xr-x 1 root root 8320 Sep 28 10:21 lib/modules/4.4.21-69-default/updates/pvdriver/xen-hcall/xen-hcall.ko

sluo-ecs-30dc:~ # lsinitrd /boot/initrd-`uname -r` | grep virtio
-rw-r--r-- 1 root root 29335 Oct 26 2016 lib/modules/4.4.21-69-default/kernel/drivers/block/virtio_blk.ko
-rw-r--r-- 1 root root 57007 Oct 26 2016 lib/modules/4.4.21-69-default/kernel/drivers/net/virtio_net.ko
-rw-r--r-- 1 root root 32415 Oct 26 2016 lib/modules/4.4.21-69-default/kernel/drivers/scsi/virtio_scsi.ko
drwxr-xr-x 2 root root 0 Sep 28 10:21 lib/modules/4.4.21-69-default/kernel/drivers/virtio
-rw-r--r-- 1 root root 19623 Oct 26 2016 lib/modules/4.4.21-69-default/kernel/drivers/virtio/virtio.ko
-rw-r--r-- 1 root root 38943 Oct 26 2016 lib/modules/4.4.21-69-default/kernel/drivers/virtio/virtio_pci.ko
-rw-r--r-- 1 root root 24431 Oct 26 2016 lib/modules/4.4.21-69-default/kernel/drivers/virtio/virtio_ring.ko
```

📖 **NOTE**

If you add built-in drivers to the initrd or initramfs file, the ECS will not be affected. This makes it easy to modify the drivers. However, you cannot check the drivers by running the **lsinitrd** command. You can run the following commands to check whether built-in drivers are in the kernel:

cat /boot/config-`uname -r` | grep CONFIG_VIRTIO | grep y

cat /boot/config-`uname -r` | grep CONFIG_XEN | grep y

9 Image Replication

When Do I Need to Replicate an Image?

Image replication includes in-region replication and cross-region replication.

- In-region replication

  This is used for conversion between encrypted and unencrypted images or for enabling advanced features (such as fast ECS creation) for images. For details, see **Replicating Images Within a Region**.

- Cross-region replication

  This is used for replicating a private image in the current region to the same account in another region. You can use this private image to deploy the same application environment in the two regions. For details, see **Replicating Images Across Regions**.

What Images Can I Replicate?

Only private images can be replicated. The restrictions on image replication are as follows:

- In-region replication

  Private images created from ISO files and full-ECS images do not support in-region replication.

- Cross-region replication

  Encrypted images do not support cross-region replication.

Can I Replicate Images Across Regions Between the Chinese Mainland, International, and European Websites?

The Chinese Mainland, International, and European websites are accessed by using different accounts. You cannot replicate images between these websites through cross-region replication. However, you can do the replication in the following way:

For example, if you want to replicate a system disk image from the CN-Hong Kong region of the International website to the CN East-Shanghai1 region of the Chinese Mainland website, perform the following operations:

1. Log in to the console of the International website, export the image from the CN-Hong Kong region to an OBS bucket in the region, and download the image to a local directory. Assume that the image file is exported as **Windows Server 2012.qcow2**.

   For details, see **Exporting an Image**.

2. Log in to the console of the Chinese Mainland website, switch to the CN East-Shanghai1 region, and upload the **Windows Server 2012.qcow2** image file to an OBS bucket in the region.

   For details, see **Uploading an External Image File**.

3. Register the image file as a private image

   For details, see **Registering an External Image File as a Private Image**.

How Long Does It Take to Replicate an Image?

The time required for replicating an image depends on the network transmission speed and the number of tasks in the queue. In normal cases, it takes 10 to 20 minutes to replicate data of 1 GB across regions.

What Is the Charge for Image Replication?

- In-region replication

  The replicas of system disk and data disk images are stored in OBS buckets for free.

  📖 **NOTE**

  Full-ECS images cannot be replicated within the same region.

- Cross-region replication

  System disk and data disk images: You are charged for the OBS traffic for replicating images cross regions.

  Full-ECS images: You are charged for the CSBS or CBR traffic for replicating images cross regions and also charged for the space used to store the CSBS or CBR backups associated with the replicas.

  📖 **NOTE**

  The process of cross-region full-ECS image replication is as follows:

  1. The system replicates the backup of a full-ECS image to the destination region.
  2. In the destination region, the system automatically generates a full-ECS image from the backup.

Is There a Limit on the Image Size During Cross-Region Replication?

Yes. An image to be replicated cannot be larger than 128 GB.

If your image file exceeds 128 GB and you want to replicate it between regions, you are advised to export the image to an OBS bucket, import the image to an OBS bucket in the destination region, and register it as a private image.

## What Is the Maximum Number of Concurrent Cross-Region Image Replication Tasks?

Five.

How Do I Replicate an Image Between Projects in a Region?

Cross-region image replication allows you to replicate images between regions. Image sharing allows you to replicate images between projects in the same region.

In the **Share Image** dialog box, enter target project IDs, and click **OK**, as instructed in **Sharing Specified Images**. After the image is shared, switch to the target projects. On the **Image Management Service** > **Images Shared with Me** page, you can view the shared image to be accepted.

Figure 9-1 Accepting or rejecting shared images
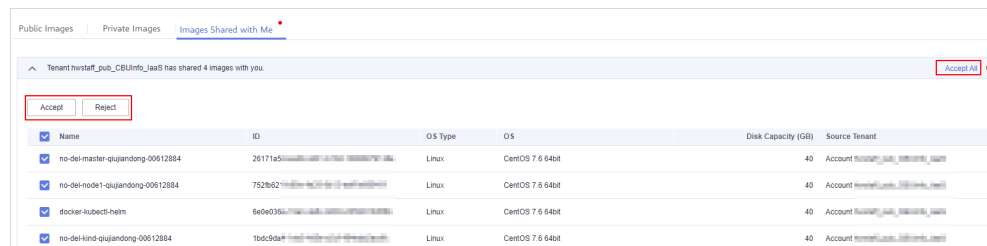
What Are the Regions That Support Cross-Region Replication of System and Data Disk Images?

Figure 9-2 Regions that support cross-region replication of system and data disk images

Source Region \ Destination Region	CN North-Beijing1	CN North-Beijing2	CN North-Beijing4	CN North-Ulanqab1	CN East-Shanghai1	CN East-Shanghai2	CN South-Guangzhou	CN Southwest-Guiyang1	CN-Hong Kong	AP-Bangkok	AP-Singapore	AF-Johannesburg	LA-Mexico City1	LA-Sao Paulo1
CN North-Beijing1	-	√	√	√	√	√	√	√	x	x	x	√	x	x
CN North-Beijing2	√	-	√	√	√	√	√	√	x	x	x	x	x	x
CN North-Beijing4	√	√	-	√	√	√	√	√	x	x	x	x	x	x
CN North-Ulanqab1	√	√	√	-	√	√	√	√	x	x	x	x	x	x
CN East-Shanghai1	√	√	√	√	-	√	√	√	x	x	x	x	x	x
CN East-Shanghai2	√	√	√	√	√	-	√	√	√	x	x	√	x	x
CN South-Guangzhou	√	√	√	√	√	√	-	√	x	x	x	x	x	x
CN Southwest-Guiyang1	√	√	√	√	√	√	√	-	x	x	x	x	x	x
CN-Hong Kong	x	x	x	x	x	√	x	x	-	x	x	√	√	x
AP-Bangkok	x	x	x	x	x	x	x	x	x	-	x	x	x	x
AP-Singapore	x	x	x	x	x	x	x	x	x	x	-	x	x	x
AF-Johannesburg	√	x	x	x	x	√	x	x	√	x	x	-	x	x
LA-Mexico City1	x	x	x	x	x	x	x	x	√	x	x	x	-	x
LA-Sao Paulo1	x	x	x	x	√	x	x	x	x	x	x	x	x	-

📖 **NOTE**

- √ indicates that cross-region replication of system and data disk images is supported.
- × indicates that cross-region replication of system and data disk images is not supported. In this case, export the desired image and then import it to the target region.
- \- indicates that the source and destination regions are the same.
- Region adjustment may affect cross-region image replication of users that are registered after the adjustment. In this case, whether the replication can be performed is subject to the management console display. The users that were registered before the adjustment are not affected.
- Regions not listed in the figure above do not support cross-region replication of system or data disk images.

What Are the Regions That Support Cross-Region Full-ECS Image Replication?

If a full-ECS image cannot be replicated to a different region, you can use it to create an ECS, use the ECS to create a system disk image and a data disk image, and replicate the images to the destination region.

A full-ECS image created using an ECS backup can be replicated from the region where they reside to another region, but the replicated full-ECS image cannot be replicated across regions again.

10 Image Deletion

Will a Private Image Be Automatically Deleted If I Delete or Unsubscribe from the ECS Used to Create the Image?

No. Private images created using ECSs are stored in OBS buckets. Deleting or unsubscribing from the ECS used to create a private image does not affect the image.

Can I Delete an Image I Shared with Others If My Image Quota Becomes Insufficient?

Yes. You can delete a shared image without requiring any operation by image recipients. After you delete the image, the image recipients cannot use it any longer. Inform the image recipients to back up their data before you delete the image.

How Do I Delete a Shared Image? Does the Deletion Affect an ECS or EVS Disk Created from It?

Reject this image on the **Images Shared with Me** tab page. This does not affect an ECS or EVS disk created from it.

11 Image Encryption

How Can I Share an Encrypted Image or Publish It in KooGallery?

You are not allowed to share an encrypted image or publish it in KooGallery directly. If you want to do so, you can replicate the image to generate an unencrypted one, and share or publish the unencrypted image in KooGallery.

How Can I Change an Unencrypted Image to an Encrypted One?

If you want to store an unencrypted image in an encrypted way, you can select an encryption key when you replicate the image. Then, the system will generate an encrypted replica of the unencrypted image.

Constraints

- An encrypted image cannot be shared with other tenants, published in KooGallery, or replicated across regions.
- The key used for encrypting an image cannot be changed.

12 KooGallery Images

What Is a KooGallery Image?

KooGallery is an online store where you can purchase third-party images that have the OS, application environments, and software preinstalled. You can use these images to deploy websites and application development environments in just a few clicks. No additional configuration is required.

KooGallery images have been strictly tested by Huawei Cloud and service providers to ensure the image content security.

How Do I Use a KooGallery Image?

You can use a KooGallery image to:

● Create an ECS

On the ECS creation page, select **KooGallery image** for **Image** and click **Select Image**. Search for the required KooGallery image, select the image, and click **OK**.

Figure 12-1 Selecting a KooGallery image
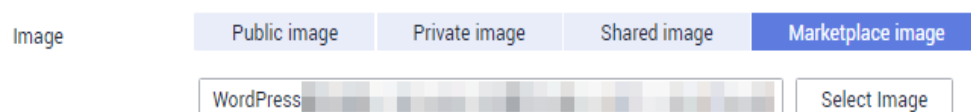
● Change the OS of an ECS

Locate the row that contains the target ECS, choose **More** > **Change OS** in the **Operation** column. Select **KooGallery image**. Search for the required KooGallery image, select the image, and click **OK**.

Figure 12-2 Changing the OS
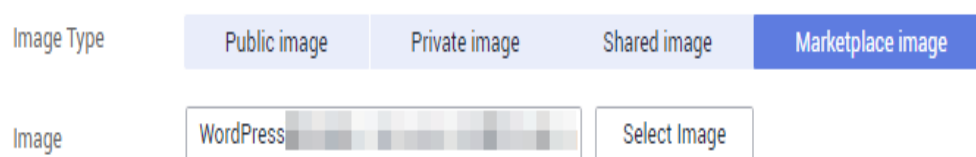
 NOTE

> The ECS must be in the **Stopped** state and its **Billing Mode** cannot be **Yearly/Monthly**.

What Do I Do If No KooGallery Image Is Available When I Change the OS of an ECS?

There are some restrictions on using a KooGallery image to change the OS of an ECS.

For example:

- If an ECS is created from a private image on Marketplace and is billed on a yearly/monthly basis, the OS cannot be changed.

How Do I Publish an Image in KooGallery?

An image can be published in KooGallery based on certain specifications. Huawei Cloud KooGallery is a trusted platform for delivering software and service transactions. It is dedicated to providing users with high-quality and easy-to-use software, services, and solutions based on cloud computing and big data, meeting the requirements of Huawei Cloud users for fast cloud migration and service development.

The prerequisites for publishing an image in KooGallery are as follows:

- A system disk image has been created.

   NOTE

  > Data disk images and full-ECS images cannot be published in KooGallery.

- The account has passed the enterprise real-name authentication.
- Use an account instead of an IAM user to log in to the console.

For details, see **Image Release Guide**.

13 Accounts and Permissions

13.1 How Do I Authorize a Key?

Scenarios

To share an encrypted image, you need to authorize the key used for encrypting the image. This section describes how to authorize a key.

📖 **NOTE**

The key can only be a custom key. The default key cannot be authorized.

Prerequisites

You have confirmed the key to be authorized. (You can view **KMS Key Name** on the image details page).

Procedure

1. Log in to the management console and choose **Security & Compliance** > **Data Encryption Workshop**.
2. On the **Custom Keys** tab, click the alias of the target key to go to the key details page.
3. On the **Grants** tab, click **Create Grant**, and set the following parameters.
   - **User or Account**: Select **Account** and enter the account ID. You can obtain the account ID from **My Credentials**.
   - **Granted Operations**: **Decrypt Data Key** and **Describe Key** are mandatory. Others are optional.
4. Click **OK**.

13.2 How Do I Create an IAM Agency?

Scenarios

During cross-region image replication, an agency is required to verify cloud service permissions in the destination region. Therefore, you need to create a cloud service agency in advance.

Background

An agency is a trust relationship established between you and other Huawei Cloud accounts or cloud services. If you have purchased multiple types of cloud resources on Huawei Cloud, you can create an agency through IAM to establish a trust relationship with a professional company or cloud service for secure and efficient O&M on certain types of your resources.

Procedure

1. Log in to the management console.
2. In the upper right corner of the page, click the username and select **Identity and Access Management**.
3. In the navigation pane, choose **Agencies**.
4. Click **Create Agency**.
5. On the **Create Agency** page, set the following parameters:
   - **Agency Name**: Enter an agency name, such as **ims_admin_agency**.

Figure 13-1 Creating an agency

- **Agency Type**: Select **Cloud service**.
- **Cloud Service**: This parameter is available only if you select **Cloud service** for **Agency Type**. Select **Image Management Service (IMS)** from the drop-down list.
- **Validity Period**: Select **Unlimited**.
- **Description**: This parameter is optional. You can enter **Agency with IMS Administrator privileges**.

6. Click **Next**.
   - Select **Region-specific projects** for **Scope** and select one or more projects from the drop-down list.

     In cross-region image replication, the agency must have the IMS Administrator permissions in the destination region. For example, if you want to replicate an image from CN-Hong Kong to CN East-Shanghai2, the agency must have the IMS Administrator permissions in CN East-Shanghai2.

⚠️ **CAUTION**

Do not select **All projects**. Otherwise, the created agency will be invalid.

   - Select **IMS Administrator** for **Permissions**.

Figure 13-2 Granting permissions to an agency
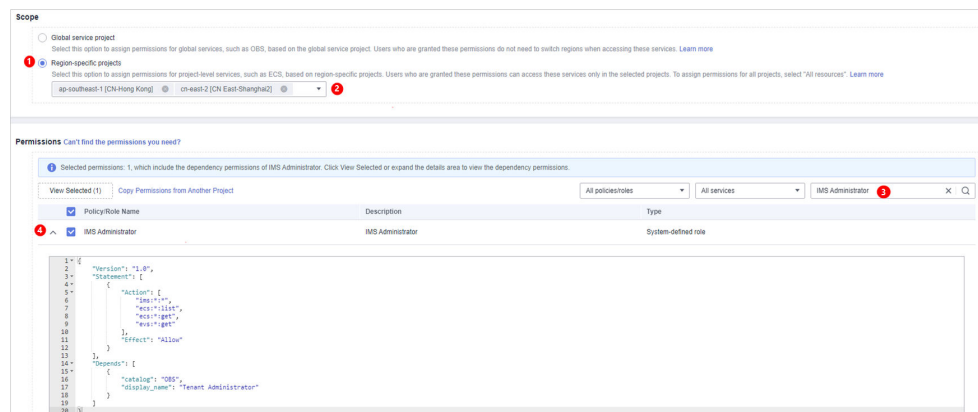
7. Click **OK**.

Figure 13-3 New agency
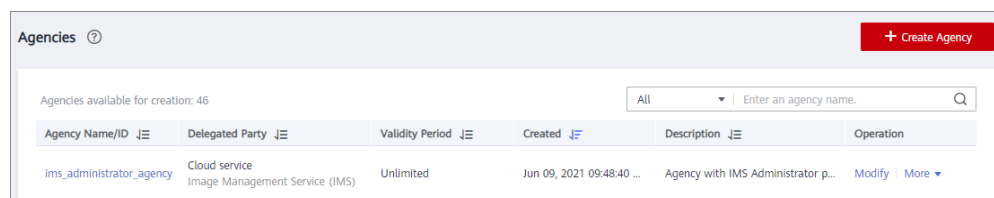
Figure 13-4 Permissions of the new agency
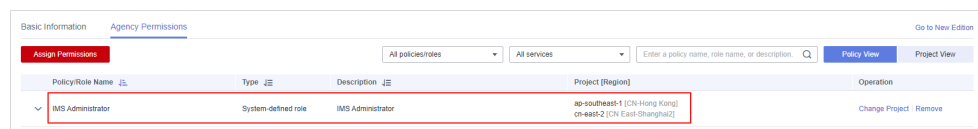
13.3 What Do I Do If Private Images Cannot Be Found on the Enterprise Project Management Service Page After EPS Is Enabled?

Scenarios

If you cannot find the private images on the **Enterprise Project Management Service** page, add the private images to their associated enterprise project.

Procedure

1. Log in to the management console.
2. Under **Compute**, click **Image Management Service**.
3. Click the **Private Images** tab.
4. Locate the row that contains the image, click **More** in the **Operation** column, and select **Allocate to Enterprise Project**.
5. In the displayed dialog box, select the target enterprise project.

13.4 What Do I Do If I Cannot Create an Image from a CSBS Backup or BMS Using a Subaccount with the Allow_all Permission After EPS Is Enabled?

When an enterprise project subaccount is used to create an image, the system displays a message indicating that CSBS or BMS is not supported by EPS. This is because CSBS and BMS are not interconnected with EPS regionally or globally. The global resource viewing permission must be granted to the subaccount in IAM. For example, you can view resources of other cloud services if you have the Tenant Guest permission.

14 Cloud-Init

14.1 Cloud-Init Installation FAQ

You are advised to install Cloud-Init on the ECS that will be used to create a private image so that new ECSs created from the private image support custom configurations (for example, changing the ECS login password).

For details about how to install Cloud-Init, see **Installing Cloud-Init**.

For details about how to configure Cloud-Init, see **Configuring Cloud-Init**.

The following describes common problems you may encounter when installing Cloud-Init and their solutions.

Ubuntu 16.04/CentOS 7: Failed to Set Cloud-Init Automatic Start

● Symptom:

After Cloud-Init is installed, run the following command to set Cloud-Init automatic start:

systemctl enable cloud-init-local.service cloud-init.service cloud-config.service cloud-final.service

Information similar to the following is displayed:

Figure 14-1 Failed to enable Cloud-Init to start automatically

```
root@ecs-wjq-ubuntu14:~# systemctl enable cloud-init-local.service cloud-init.se
rvice cloud-config.service cloud-final.service
Failed to execute operation: Unit file is masked
root@ecs-wjq-ubuntu14:~#
```

● Solution:

a. Run the following command to roll back the configuration:

systemctl unmask cloud-init-local.service cloud-init.service cloud-config.service cloud-final.service

b. Run the following command to set automatic start again:

systemctl enable cloud-init-local.service cloud-init.service cloud-config.service cloud-final.service

c. Run the following command to check the Cloud-Init status:

systemctl status cloud-init-local.service cloud-init.service cloud-config.service cloud-final.service

As shown in the following figures, **failed** is displayed and all services are in the **inactive** state.

Figure 14-2 Checking Cloud-Init status

Figure 14-3 Checking Cloud-Init status

This is because the address that the system uses to access Cloud-Init is redirected to **/usr/bin/**, but the actual installation path is **/usr/local/bin**.

d. Run the following command to copy Cloud-Init to the **usr/bin** directory:

cp /usr/local/cloud-init /usr/bin/

e. Run the following command to restart Cloud-Init:

systemctl restart cloud-init-local.service cloud-init.service cloud-config.service cloud-final.service

Figure 14-4 Restarting Cloud-Init

f. Run the following command to check the Cloud-Init status:

systemctl status cloud-init-local.service cloud-init.service cloud-config.service cloud-final.service

Ubuntu 14.04: chkconfig and systemctl Not Installed

- Symptom:

  chkconfig is not installed.

- Solution:

  Run the following commands to install chkconfig:

  apt-get update

  apt-get install sysv-rc-conf

  cp /usr/sbin/sysv-rc-conf /usr/sbin/chkconfig

  Run the following command to query the Cloud-Init version:

  cloud-init -v

  Information similar to the following is displayed:

  `-bash:/usr/bin/cloud-init:not found this command`

  Solution: Run the following command to copy Cloud-Init to the **usr/bin** directory:

  cp /usr/local/bin/cloud-init /usr/bin/

Debian 9.5: Failed to Query the Cloud-Init Version and Set Automatic Start

1. Run the following command to query the Cloud-Init version:

   cloud-init -v

   Information similar to the following is displayed:

   `-bash:/usr/bin/cloud-init:not found this command`

   Solution: Run the **cp /usr/local/bin/cloud-init /usr/bin/** command to copy Cloud-Init to the **usr/bin** directory.

2. Run the **cloud-init init --local** command.

   Information similar to the following is displayed:

   Figure 14-5 Information returned when Cloud-Init automatic start successfully set

   Cause analysis: The compilation fails because GCC is not installed.

   Solution:

   Run the following command to install GCC. Then, install Cloud-Init again.

   yum -y install gcc

3. After Cloud-Init is installed, run the following command to set Cloud-Init automatic start:

   systemctl enable cloud-init-local.service cloud-init.service cloud-config.service cloud-final.service

   Information similar to the following is displayed.

Figure 14-6 Prompt indicating the failure to set Cloud-Init automatic start

`Failed to enable unit: Unit file /etc/systemd/system/cloud-init-local.service is masked.`

Solution:

a. Run the following command to roll back the configuration:

systemctl unmask cloud-init-local.service cloud-init.service cloud-config.service cloud-final.service

b. Run the following command to set automatic start again:

systemctl enable cloud-init-local.service cloud-init.service cloud-config.service cloud-final.service

c. Run the following command to restart Cloud-Init:

systemctl restart cloud-init-local.service cloud-init.service cloud-config.service cloud-final.service

Run the **systemctl status** command to check the Cloud-Init status. Information similar to the following is displayed:

Figure 14-7 Verifying the service status

CentOS 7/Fedora 28: Required C Compiler Not Installed

- Symptom

  After Cloud-Init is successfully installed, run the following command:

  cloud-init init --local

  The following information is displayed:

  /usr/lib/python2.5/site-packages/Cheetah/Compiler.py:1532: UserWarning:
  You don't have the C version of NameMapper installed! I'm disabling Cheetah's useStackFrames
  option as it is painfully slow with the Python version of NameMapper. You should get a copy of
  Cheetah with the compiled C version of NameMapper.
    "\nYou don't have the C version of NameMapper installed!

- Cause analysis

  This alarm is generated because C version of NameMapper needs to be compiled when Cloud-Init is installed. However, GCC is not installed in the

system, and the compilation cannot be performed. As a result, NameMapper is missing.

- Solution

  Run the following command to install GCC:

  yum -y install gcc

  Reinstall Cloud-Init.

CentOS 7/Fedora: Failed to Use the New Password to Log In to an ECS Created from an Image

- Symptom

  After Cloud-Init is successfully installed on an ECS, an image is created from the ECS. You cannot use a new password to log in to the ECSs created from this image. When you log in to the ECSs using the old password, you find that NICs of these ECSs are not started.

  Figure 14-8 NIC not started

  ```
  [root@ecs-fedora28-wjq-test ~]# ifconfig
  lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
          inet 127.0.0.1  netmask 255.0.0.0
          inet6 ::1  prefixlen 128  scopeid 0x10<host>
          loop  txqueuelen 1000  (Local Loopback)
          RX packets 0  bytes 0 (0.0 B)
          RX errors 0  dropped 0  overruns 0  frame 0
          TX packets 0  bytes 0 (0.0 B)
          TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
  ```

- Solution:

  Log in to the ECS used to create the image, open the DHCP configuration file **/etc/sysconfig/network-scripts/ifcfg-eth***X*, and comment out **HWADDR**.

14.2 What Can I Do with a Cloud-Init ECS?

Introduction to Cloud-Init

Cloud-Init is an open-source tool for cloud instance initialization. When creating ECSs from an image with Cloud-Init, you can use user data injection to inject customized initialization details (for example, an ECS login password) to the ECSs. You can also configure and manage a running ECS by querying and using metadata. If Cloud-Init is not installed, you cannot apply custom configurations to the ECSs. You will have to use the original password in the image file to log in to the ECSs.

Installation Methods

You are advised to install Cloud-Init or Cloudbase-Init on the ECS to be used to create a private image so that new ECSs created from the private image support custom configurations.

- For Windows OSs, download and install Cloudbase-Init.

  For how to install Cloudbase-Init, see **Installing and Configuring Cloudbase-Init**.

- For Linux OSs, download and install Cloud-Init.

  For how to install Cloud-Init, see **Installing Cloud-Init**.

  For how to configure Cloud-Init, see **Configuring Cloud-Init**.

14.3 What Do I Do If Injecting the Key or Password Using Cloud-Init Failed After NetworkManager Is Installed?

Symptom

A major cause is that the version of Cloud-Init is incompatible with that of NetworkManager. In Debian 9.0 and later versions, NetworkManager is incompatible with Cloud-Init 0.7.9.

Solution

Uninstall the current Cloud-Init and install Cloud-Init 0.7.6 or an earlier version.

For details about how to install Cloud-Init, see **Installing Cloud-Init**.

14.4 How Do I Install growpart for SUSE 11 SP4?

Scenarios

growpart for SUSE and openSUSE is an independent toolkit that does not start with **cloud-***. Perform operations in this section to install growpart.

Procedure

1. Run the following commands to check whether Cloud-Init and growpart have been installed:

   rpm -qa | grep cloud-init

   The command output is as follows:

   ```
   cloud-init-0.7.8-39.2
   ```

   rpm -qa | grep growpart

   The command output is as follows:

   ```
   growpart-0.29-8.1
   ```

2. Run the following command to uninstall Cloud-Init and growpart:

   zypper remove cloud-init growpart

3. Run the following commands to delete residual files:

   rm -fr /etc/cloud/*

   rm -fr /var/lib/cloud/*

4. Run the following command to install growpart:

   zypper install http://download.opensuse.org/repositories/home:/garloff:/ OTC:/cloudinit/SLE_11_SP4/noarch/growpart-0.27-1.1.noarch.rpm

5. Run the following command to install python-oauth:

   **zypper install http://download.opensuse.org/repositories/home:/garloff:/
   OTC:/cloudinit/SLE_11_SP4/x86_64/python-oauth-1.0.1-35.1.x86_64.rpm**

6. Run the following command to install Cloud-Init:

   **zypper install http://download.opensuse.org/repositories/home:/garloff:/
   OTC:/cloudinit/SLE_11_SP4/x86_64/cloud-init-0.7.6-27.23.1.x86_64.rpm**

7. Run the following commands to check whether growpart, python-oauth, and
   Cloud-Init have been installed successfully:

   rpm -qa | grep growpart

   The command output is as follows:

   ```
   growpart-0.27-1.1
   ```

   rpm -qa | grep python-oauth

   The command output is as follows:

   ```
   python-oauthlib-0.6.0-1.5
   python-oauth-1.0.1-35.1
   ```

   rpm -qa | grep cloud-init

   The command output is as follows:

   ```
   cloud-init-0.7.6-27.19.1
   ```

8. Run the following command to check the configuration:

   **chkconfig cloud-init-local on;chkconfig cloud-init on;chkconfig cloud-
   config on;chkconfig cloud-final on**

15 ECS Creation

15.1 Can I Change the Image of a Purchased ECS?

Yes.

If you have selected an incorrect image or your service requirements have changed, you can change the image of your ECS.

You can change the image type (public, private, KooGallery, and shared images) and OS. For details, see **Changing the OS**.

15.2 Can I Use a Private Image to Create ECSs with Different Hardware Specifications from the ECS Used to Create the Private Image?

Yes. You can specify the CPU, memory, bandwidth, data disks of the new ECSs if necessary. You can also specify their system disk capacity. The value must be smaller than 1024 GB but no less than the system disk capacity in the image.

15.3 Can I Specify the System Disk Capacity When I Create an ECS Using an Image?

Yes. However, the value must be smaller than 1024 GB but no less than the system disk capacity in the image.

15.4 What Do I Do If No Partition Is Found During the Startup of an ECS Created from an Imported Private Image?

Symptom

This may be caused by a disk partition ID change after the cross-platform image import. As a result, no partition can be found based on the original disk partition ID in the image. In this case, you need to change the disk partition in the image (**UUID=***UUID of the disk partition*).

Solution

The following uses openSUSE 13.2 as an example to describe how to change the partition name.

1. Run the following command to query the disk partition ID:

   ls -l /dev/disk/by-id/

   The example command output is as follows.

   ```
   total 0
   lrwxrwxrwx 1 root root 10 Jul 22 01:35 ata-QEMU_HARDDISK_QM00001 -> ../../xvda
   lrwxrwxrwx 1 root root 11 Jul 22 01:35 ata-QEMU_HARDDISK_QM00001-part1 -> ../../xvda1
   lrwxrwxrwx 1 root root 12 Jul 22 01:35 ata-QEMU_HARDDISK_QM00001-part10 -> ../../xvda10
   lrwxrwxrwx 1 root root 11 Jul 22 01:35 ata-QEMU_HARDDISK_QM00001-part2 -> ../../xvda2
   lrwxrwxrwx 1 root root 11 Jul 22 01:35 ata-QEMU_HARDDISK_QM00001-part5 -> ../../xvda5
   lrwxrwxrwx 1 root root 11 Jul 22 01:35 ata-QEMU_HARDDISK_QM00001-part6 -> ../../xvda6
   lrwxrwxrwx 1 root root 11 Jul 22 01:35 ata-QEMU_HARDDISK_QM00001-part7 -> ../../xvda7
   lrwxrwxrwx 1 root root 11 Jul 22 01:35 ata-QEMU_HARDDISK_QM00001-part8 -> ../../xvda8
   lrwxrwxrwx 1 root root 11 Jul 22 01:35 ata-QEMU_HARDDISK_QM00001-part9 -> ../../xvda9
   lrwxrwxrwx 1 root root 10 Jul 22 01:35 ata-QEMU_HARDDISK_QM00005 -> ../../xvde
   lrwxrwxrwx 1 root root 10 Jul 22 01:35 scsi-SATA_QEMU_HARDDISK_QM00001 -> ../../xvda
   lrwxrwxrwx 1 root root 11 Jul 22 01:35 scsi-SATA_QEMU_HARDDISK_QM00001-part1 -> ../../xvda1
   lrwxrwxrwx 1 root root 12 Jul 22 01:35 scsi-SATA_QEMU_HARDDISK_QM00001-part10 -> ../../xvda10
   lrwxrwxrwx 1 root root 11 Jul 22 01:35 scsi-SATA_QEMU_HARDDISK_QM00001-part2 -> ../../xvda2
   lrwxrwxrwx 1 root root 11 Jul 22 01:35 scsi-SATA_QEMU_HARDDISK_QM00001-part5 -> ../../xvda5
   lrwxrwxrwx 1 root root 11 Jul 22 01:35 scsi-SATA_QEMU_HARDDISK_QM00001-part6 -> ../../xvda6
   lrwxrwxrwx 1 root root 11 Jul 22 01:35 scsi-SATA_QEMU_HARDDISK_QM00001-part7 -> ../../xvda7
   lrwxrwxrwx 1 root root 11 Jul 22 01:35 scsi-SATA_QEMU_HARDDISK_QM00001-part8 -> ../../xvda8
   lrwxrwxrwx 1 root root 11 Jul 22 01:35 scsi-SATA_QEMU_HARDDISK_QM00001-part9 -> ../../xvda9
   lrwxrwxrwx 1 root root 10 Jul 22 01:35 scsi-SATA_QEMU_HARDDISK_QM00005 -> ../../xvde
   ```

   ata-QEMU_HARDDISK_xxx and **scsi-SATA_QEMU_HARDDISK_xxx** indicate that the disk of the ECS is simulated using Quick EMUlator (QEMU). The content on the left of **->** is the disk partition ID, and that on the right of **->** is the partition name.

2. Run the following command to query the disk partition UUID:

   ls -l /dev/disk/by-uuid/

   The example command output is as follows.

   ```
   total 0
   lrwxrwxrwx 1 root root 11 Jul 22 01:35 45ecd7a0-29da-4402-a017-4564a62308b8 -> ../../xvda5
   lrwxrwxrwx 1 root root 11 Jul 22 01:35 55386c6a-9e32-41d4-af7a-e79596221f51 -> ../../xvda9
   lrwxrwxrwx 1 root root 11 Jul 22 01:35 55f36660-9bac-478c-a701-7ecc5347f789 -> ../../xvda8
   lrwxrwxrwx 1 root root 11 Jul 22 01:35 780f36bc-0ada-4c98-9a8d-44570d65333d -> ../../xvda1
   lrwxrwxrwx 1 root root 11 Jul 22 01:35 b3b7c47f-6a91-45ef-80d6-275b1cc16e19 -> ../../xvda6
   ```

```
lrwxrwxrwx 1 root root 11 Jul 22 01:35 ea63b55d-3b6e-4dcd-8986-956b72bac3e9 -> ../../xvda7
lrwxrwxrwx 1 root root 12 Jul 22 01:35 eb3cc645-925e-4bc5-bedf-c2a6f3b65809 -> ../../xvda10
```

The content on the left of **->** is the disk partition UUID, and that on the right of **->** is the partition name. Obtain the relationship between the disk partition name, partition ID, and partition UUID.

3. Run the following command to check the partition names in the **/etc/fstab** file:

    vi /etc/fstab

    The example command output is as follows.

    ```
    /dev/disk/by-id/scsi-SATA_QEMU_HARDDISK_QM00001-part5 / ext3 defaults,errors=panic 1 1
    /dev/disk/by-id/scsi-SATA_QEMU_HARDDISK_QM00001-part1 /boot ext3 defaults,errors=panic 1 2
    /dev/disk/by-id/scsi-SATA_QEMU_HARDDISK_QM00001-part6 /home ext3 nosuid,errors=panic 1 2
    /dev/disk/by-id/scsi-SATA_QEMU_HARDDISK_QM00001-part10 /opt ext3 defaults,errors=panic 1 2
    /dev/disk/by-id/scsi-SATA_QEMU_HARDDISK_QM00001-part7 /tmp ext3 nodev,nosuid,errors=panic 1 2
    /dev/disk/by-id/scsi-SATA_QEMU_HARDDISK_QM00001-part9 /usr ext3 defaults,errors=panic 1 2
    /dev/disk/by-id/scsi-SATA_QEMU_HARDDISK_QM00001-part8 /var ext3 nodev,nosuid,errors=panic 1 2
    sysfs /sys sysfs noauto 0 0
    proc /proc proc defaults 0 0
    usbfs /proc/bus/usb usbfs noauto 0 0
    devpts /dev/pts devpts mode=0620,gid=5 0 0
    /dev/cdrom /media/ udf,iso9660 noexec,noauto,nouser,nodev,nosuid 1 2
    tmpfs /dev/shm tmpfs noexec,nodev,nosuid 0 0
    ```

    The values in the first column are the disk partition IDs.

4. Press **i** to enter editing mode. Change the disk partition ID in the row that contains **/dev/disk/xxx** in the **/etc/fstab** file in step **3** to **UUID=**_UUID of the disk partition_ based on the query results in step **1** and step **2**.

    The modified content is as follows.
    ```
    UUID=45ecd7a0-29da-4402-a017-4564a62308b8 / ext3 defaults,errors=panic 1 1
    UUID=780f36bc-0ada-4c98-9a8d-44570d65333d /boot ext3 defaults,errors=panic 1 2
    UUID=b3b7c47f-6a91-45ef-80d6-275b1cc16e19 /home ext3 nosuid,errors=panic 1 2
    UUID=eb3cc645-925e-4bc5-bedf-c2a6f3b65809 /opt ext3 defaults,errors=panic 1 2
    UUID=ea63b55d-3b6e-4dcd-8986-956b72bac3e9 /tmp ext3 nodev,nosuid,errors=panic 1 2
    UUID=55386c6a-9e32-41d4-af7a-e79596221f51 /usr ext3 defaults,errors=panic 1 2
    UUID=55f36660-9bac-478c-a701-7ecc5347f789 /var ext3 nodev,nosuid,errors=panic 1 2
    sysfs /sys sysfs noauto 0 0
    proc /proc proc defaults 0 0
    usbfs /proc/bus/usb usbfs noauto 0 0
    devpts /dev/pts devpts mode=0620,gid=5 0 0
    /dev/cdrom /media/ udf,iso9660 noexec,noauto,nouser,nodev,nosuid 1 2
    tmpfs /dev/shm tmpfs noexec,nodev,nosuid 0 0
    ```

    ◻ **NOTE**

    Ensure that the UUIDs are correct. Otherwise, the ECS cannot start properly.

5. Press **Esc**, enter **:wq**, and press **Enter**. The system saves the configuration and exits the vi editor.

6. Check the partition names in the system boot configuration file.

    The system boot configuration files vary depending on the OS. Confirm the boot configuration file of the current OS.

    –   Grand Unified Boot Loader (GRUB) configuration file

        ▪   /boot/grub/grub.conf

        ▪   /boot/grub/menu.lst

        ▪   /boot/grub/grub.cfg

- /boot/grub2/grub.cfg

  – Syslinux configuration file

    - /extlinux.conf

    - /boot/syslinux/extlinux.conf

    - /boot/extlinux/extlinux.conf

    - /boot/syslinux/syslinux.cfg

    - /syslinux/syslinux.cfg

    - /syslinux.cfg

The boot file in this example is **/boot/grub/menu.lst**. Run the following command to check it:

vi /boot/grub/menu.lst

```
default 0
timeout 3
title xxx Server OS - xxxxxx
kernel /boot/vmlinuz-3.0.101-0.47.52-default root=/dev/disk/by-id/scsi-
SATA_QEMU_HARDDISK_QM00001-part5 resume= memmap=0x2000000$0x3E000000
nmi_watchdog=2 crashkernel=512M-:256M console=ttyS0,115200 console=tty0 xen_emul_unplug=all
initrd /boot/initrd-3.0.101-0.47.52-default
```

7. Press **i** to enter editing mode and change the partition names in the system boot configuration file.

   Change the disk partition name in the **/boot/grub/menu.lst** file in **6** to **UUID=**_UUID of the disk partition_ based on the query results in **1** and **2**.

```
default 0
timeout 3
title xxx Server OS - xxxxxx
kernel /boot/vmlinuz-3.0.101-0.47.52-default root=UUID=45ecd7a0-29da-4402-a017-4564a62308b8
resume= memmap=0x2000000$0x3E000000 nmi_watchdog=2 crashkernel=512M-:256M
console=ttyS0,115200 console=tty0 xen_emul_unplug=all
initrd /boot/initrd-3.0.101-0.47.52-default
```

8. Press **Esc**, enter **:wq**, and press **Enter**. The system saves the configuration and exits the vi editor.

15.5 What Do I Do If the Disks of an ECS Created from a CentOS Image Cannot Be Found?

Symptom

Generally, this is because the xen-blkfront.ko module is not loaded during the startup. You need to modify OS kernel startup parameters. **Figure 15-1** shows the startup screen after the login to the ECS.

Figure 15-1 Startup screen

Solution

Perform the following operations to modify OS kernel boot parameters:

📖 **NOTE**

These operations must be performed after the OS starts. You are advised to modify kernel boot parameters in the ECS used for creating the image.

1. Run the following command to log in to the OS:

   lsinitrd /boot/initramfs- `uname` **-r** `.img |grep -i xen`

   – If the command output contains **xen-blkfront.ko**, contact the customer service.

   – If no command output is displayed, go to **2**.

2. Back up the GRUB configuration file.

   – If the ECS runs CentOS 6, run the following command:

     cp /boot/grub/grub.conf /boot/grub/grub.conf.bak

   – If the ECS runs CentOS 7, run the following command:

     cp /boot/grub2/grub.cfg /boot/grub2/grub.cfg.bak

3. Use the **vi** editor to open the GRUB configuration file. Run the following command (using CentOS 7 as an example):

   vi /boot/grub2/grub.cfg

4. Add **xen_emul_unplug=all** to the default boot kernel.

   📖 **NOTE**

   Search for the line that contains **root=UUID=** and add **xen_emul_unplug=all** to the end of the line.

   menuentry 'CentOS Linux (3.10.0-229.el7.x86_64) 7 (Core) with debugging' --class centos --class gnu-linux --class gnu --class os --unrestricted $menuentry_id_option 'gnulinux-3.10.0-229.el7.x86_64-advanced-bf3cc825-7638-48d8-8222-cd2f412dd0de' {
   load_video
   set gfxpayload=keep
   insmod gzio
   insmod part_msdos
   insmod ext2
   set root='hd0,msdos1'
   if [x$feature_platform_search_hint = xy]; then
     search --no-floppy --fs-uuid --set=root --hint='hd0,msdos1' bf3cc825-7638-48d8-8222-

```
cd2f412dd0de
    else
      search --no-floppy --fs-uuid --set=root bf3cc825-7638-48d8-8222-cd2f412dd0de
    fi
    linux16 /boot/vmlinuz-3.10.0-229.el7.x86_64 root=UUID=bf3cc825-7638-48d8-8222-
cd2f412dd0de xen_emul_unplug=all ro crashkernel=auto rhgb quiet  systemd.log_level=debug
systemd.log_target=kmsg
      initrd16 /boot/initramfs-3.10.0-229.el7.x86_64.img
}
```

5. Press **Esc**, enter **:wq**, and press **Enter** to exit the vi editor.

6. Create an image using the ECS, upload and register the image on the cloud platform.

15.6 What Do I Do If an ECS Created from a Windows Image Failed to Start When I Have Enabled Automatic Configuration During Image Registration?

Symptom

This issue is probably caused by the failure of offline VirtIO driver injection.

Solution

When you inject VirtIO drivers for a Windows ECS offline, there are some restrictions:

- If the boot mode in the image file is UEFI, the VirtIO drivers cannot be injected offline.

- It is recommended that you disable Group Policy Object (GPO). Some policies may cause the failure of VirtIO driver injection offline.

- It is recommended that you stop antivirus software. Otherwise, the VirtIO drivers may fail to be injected offline.

To update VirtIO drivers, see **Optimizing a Windows Private Image**.

15.7 What Do I Do If an Exception Occurs When I Start an ECS Created from an Image Using the UEFI Boot Mode?

Symptom

An ECS created from a private image using the UEFI boot mode cannot start.

Possible Causes

The image OS uses the UEFI boot mode, but the uefi attribute is not added to the image.

Solution

1. Delete the ECS that failed to start.

2. Call the API to update the image attributes and change the value of **hw_firmware_type** to **uefi**.

   API URI: PATCH /v2/cloudimages/{*image_id*}

   For details about how to call the API, see **Updating Image Information**.

3. Use the updated image to create an ECS.

16 Driver Installation

16.1 Must I Install Guest OS Drivers on an ECS?

Installing Guest OS drivers on an ECS improves your experience in using the ECS. In addition, it also ensures high reliability and stability of ECSs.

- Windows ECSs: Install PV and VirtIO drivers on ECSs.
- Linux ECSs: Install Xen PV and VirtIO drivers and add them to initrd.

16.2 Why Do I Need to Install and Update VirtIO Drivers for Windows?

Why Do I Need to Install VirtIO Drivers?

VirtIO drivers are paravirtualized drivers that provide high-performance disks and NICs for ECSs.

- A standard Windows OS does not have VirtIO drivers.
- Public images have VirtIO drivers by default.
- You need to install VirtIO drivers for private images. For details, see **Installing VirtIO Drivers**.

Why Do I Need to Update VirtIO Drivers?

This ensures that known issues identified in the community or R&D tests can be avoided on the latest drivers.

When Do I Need to Update VirtIO Drivers?

After a major error is fixed, you are advised to update VirtIO drivers immediately. (This has not happened by now.)

After other issues are fixed, decide whether to update VirtIO drivers based on your needs.

What Do I Need to Do?

- Upgrade VirtIO drivers in Windows private images or running Windows ECSs.
- If you have any technical issue or question, contact the customer service.

16.3 Whey Do I Fail to Install Guest OS Drivers on a Windows ECS?

Possible causes:

- Your image file was exported from a VMware VM, and VMware Tools was not uninstalled or not completely uninstalled.
- You have downloaded Guest OS drivers of an incorrect version for your Windows ECS.
- The disk space available for installing Guest OS drivers is insufficient. Ensure that the disk where Guest OS drivers are installed has at least 300 MB space available.

16.4 How Do I Install PV Drivers in Windows?

This only applies to Xen ECSs, which have been discontinued and no longer been available for new users. For details, see **Discontinued ECS Specifications**. If you are a new user or you are an existing user that will use this image to create a non-Xen ECS, this answer does not apply to you.

For details, see **Installing PV Drivers**.

16.5 How Do I Install VirtIO Drivers in Windows?

The installation only applies to KVM ECSs. Before using an ECS or external image file to create a private image, ensure that VirtIO drivers have been installed in the OS so that ECSs created from this image can support KVM virtualization and the network performance can be improved.

For details, see **Installing VirtIO Drivers**.

16.6 How Do I Install Native KVM Drivers in Linux?

When optimizing a Linux private image, you need to install native KVM drivers on the ECS from which the image will be created. If you ECS already has native KVM drivers installed, you do not need to install the drivers again.

For details, see **Installing Native KVM Drivers**.

16.7 How Do I Install Native Xen and KVM Drivers?

Scenarios

When optimizing a Linux private image with Xen virtualization, you need to install native Xen and KVM drivers on the source ECS of the image.

This section describes how to install native Xen and KVM drivers.

⚠ **CAUTION**

If an ECS has no Xen drivers installed, the network performance of the ECS will be poor, and the security groups and firewall configured for the ECS will not take effect.

If an ECS has no KVM drivers installed, the NICs of the ECS may not be detected and the ECS will be unable to communicate with other resources.

Prerequisites

- The virtualization type of the ECS is Xen. For details, see **Viewing the Virtualization Type of a Linux ECS**.
- The kernel version must be later than 2.6.24.
- Disable your antivirus and intrusion detection software. You can enable them after the driver installation is complete.

Procedure

Modify the configuration file depending on the OS.

- CentOS, EulerOS

  Take CentOS 7.0 as an example. Modify the **/etc/dracut.conf** file. Add the Xen PV and VirtIO drivers to **add_drivers**. Xen PV drivers include xen-blkfront and xen-netfront. VirtIO drivers include virtio_blk, virtio_scsi, virtio_net, virtio_pci, virtio_ring, and virtio. Separate driver names with spaces. Save and exit the **/etc/dracut.conf** file. Run the **dracut -f** command to regenerate initrd.

  For details, see **CentOS and EulerOS**.

- Ubuntu and Debian

  Modify the **/etc/initramfs-tools/modules** file. Add the Xen PV and VirtIO drivers. Xen PV drivers include xen-blkfront and xen-netfront. VirtIO drivers include virtio_blk, virtio_scsi, virtio_net, virtio_pci, virtio_ring, and virtio. Separate driver names with spaces. Save and exit the **/etc/initramfs-tools/ modules** file. Run the **update-initramfs -u** command to regenerate initrd.

  For details, see **Ubuntu and Debian**.

- SUSE and openSUSE

  - If the OS version is earlier than SUSE 12 SP1 or openSUSE 13, modify the **/etc/sysconfig/kernel** file and add Xen PV and VirtIO drivers to **INITRD_MODULES=""**. Xen PV drivers include xen_vnif, xen_vbd, and

xen_platform_pci. VirtIO drivers include virtio_blk, virtio_scsi, virtio_net, virtio_pci, virtio_ring, and virtio. Separate driver names with spaces. Run the **mkinitrd** command to regenerate initrd.

– If the OS version is SUSE 12 SP1, modify the **/etc/dracut.conf** file and add Xen PV and VirtIO drivers to **add_drivers**. Xen PV drivers include xen_vnif, xen_vbd, and xen_platform_pci. VirtIO drivers include virtio_blk, virtio_scsi, virtio_net, virtio_pci, virtio_ring, and virtio. Separate driver names with spaces. Run the **dracut -f** command to regenerate initrd.

– If the OS version is later than SUSE 12 SP1 or openSUSE 13, modify the **/etc/dracut.conf** file and add Xen PV and VirtIO drivers to **add_drivers**. Xen PV drivers include xen-blkfront and xen-netfront. VirtIO drivers include virtio_blk, virtio_scsi, virtio_net, virtio_pci, virtio_ring, and virtio. Separate driver names with spaces. Save and exit the **/etc/dracut.conf** file. Run the **dracut -f** command to regenerate initrd.

For details, see **SUSE and openSUSE**.

📖 **NOTE**

For SUSE, run the following command to check whether xen-kmp (driver package for Xen PV) is installed:

rpm -qa |grep xen-kmp

If information similar to the following is displayed, xen-kmp is installed in the OS:

xen-kmp-default-4.2.2_04_3.0.76_0.11-0.7.5

If xen-kmp is not installed, obtain it from the ISO file and install it.

If you add built-in drivers to the initrd or initramfs file by mistake, the ECS will not be affected.

CentOS and EulerOS

1. Run the following command to open the **/etc/dracut.conf** file:

   vi /etc/dracut.conf

2. Press **i** to enter editing mode and add Xen PV and VirtIO drivers to **add_drivers** (the format varies depending on the OS).

   ```
   [root@CTU10000xxxxx ~]# vi /etc/dracut.conf
   # additional kernel modules to the default
   add_drivers+="xen-blkfront xen-netfront virtio_blk virtio_scsi virtio_net virtio_pci virtio_ring virtio"
   ……
   ```

3. Press **Esc**, enter **:wq**, and press **Enter**. The system saves the change and exits the **/etc/dracut.conf** file.

4. Run the following command to regenerate initrd:

   dracut -f /boot/initramfs-2.6.32-573.8.1.el6.x86_64.img

   If the virtual file system is not the default initramfs, run the **dracut -f** *Name of the initramfs or initrd file actually used* command. The actual initramfs or initrd file name can be obtained from the **grub.cfg** file, which can be **/boot/grub/grub.cfg**, **/boot/grub2/grub.cfg**, or **/boot/grub/grub.conf** depending on the OS.

5. If the virtual file system is initramfs, run the following commands to check whether native Xen and KVM drivers have been installed:

   lsinitrd /boot/initramfs-`uname -r`.img | grep xen

   lsinitrd /boot/initramfs-`uname -r`.img | grep virtio

If the virtual file system is initrd, run the following commands to check whether native Xen and KVM drivers have been installed:

lsinitrd /boot/initrd-`uname -r` | grep xen

lsinitrd /boot/initrd-`uname -r` | grep virtio

Assume that the virtual file system is initramfs. The following command output will be displayed:

```
[root@CTU10000xxxxx home]# lsinitrd /boot/initramfs-`uname -r`.img | grep xen
-rwxr--r--  1 root    root        54888 Jul 16 17:53 lib/modules/2.6.32-573.8.1.el6.x86_64/kernel/drivers/
block/xen-blkfront.ko
-rwxr--r--  1 root    root        45664 Jul 16 17:53 lib/modules/2.6.32-573.8.1.el6.x86_64/kernel/
drivers/net/xen-netfront.ko

[root@CTU10000xxxxx home]# lsinitrd /boot/initramfs-`uname -r`.img | grep virtio
-rwxr--r--  1 root    root        23448 Jul 16 17:53 lib/modules/2.6.32-573.8.1.el6.x86_64/kernel/drivers/
block/virtio_blk.ko
-rwxr--r--  1 root    root        50704 Jul 16 17:53 lib/modules/2.6.32-573.8.1.el6.x86_64/kernel/
drivers/net/virtio_net.ko
-rwxr--r--  1 root    root        28424 Jul 16 17:53 lib/modules/2.6.32-573.8.1.el6.x86_64/kernel/drivers/
scsi/virtio_scsi.ko
drwxr-xr-x  2 root    root            0 Jul 16 17:53 lib/modules/2.6.32-573.8.1.el6.x86_64/kernel/drivers/
virtio
-rwxr--r--  1 root    root        14544 Jul 16 17:53 lib/modules/2.6.32-573.8.1.el6.x86_64/kernel/drivers/
virtio/virtio.ko
-rwxr--r--  1 root    root        21040 Jul 16 17:53 lib/modules/2.6.32-573.8.1.el6.x86_64/kernel/drivers/
virtio/virtio_pci.ko
-rwxr--r--  1 root    root        18016 Jul 16 17:53 lib/modules/2.6.32-573.8.1.el6.x86_64/kernel/drivers/
virtio/virtio_ring.ko
```

📖 **NOTE**

If you add built-in drivers to the initrd or initramfs file by mistake, the ECS will not be affected. The drivers cannot be found by running the **lsinitrd** command. You can run the following commands to check whether built-in drivers are in the kernel:

cat /boot/config-`uname -r` | grep CONFIG_VIRTIO | grep y

cat /boot/config-`uname -r` | grep CONFIG_XEN | grep y

Ubuntu and Debian

1. Run the following command to open the **modules** file:

   vi /etc/initramfs-tools/modules

2. Press **i** to enter editing mode and add Xen PV and VirtIO drivers to the **/etc/initramfs-tools/modules** file (the format varies depending on the OS).
   ```
   [root@CTU10000xxxxx ~]#vi /etc/initramfs-tools/modules
   ……
   # Examples:
   #
   # raid1
   # sd_mOd
   xen-blkfront
   xen-netfront
   virtio_blk
   virtio_scsi
   virtio_net
   virtio_pci
   virtio_ring
   virtio
   ```

3. Press **Esc**, enter **:wq**, and press **Enter**. The system saves the change and exits the **/etc/initramfs-tools/modules** file.

4. Run the following command to regenerate initrd:

   update-initramfs -u

5. Run the following commands to check whether native Xen and KVM drivers have been installed:

lsinitramfs /boot/initrd.img-`uname -r` |grep xen

lsinitramfs /boot/initrd.img-`uname -r` |grep virtio

```
[root@ CTU10000xxxxx home]# lsinitramfs /boot/initrd.img-`uname -r` |grep xen
lib/modules/3.5.0-23-generic/kernel/drivers/net/ethernet/qlogic/netxen
lib/modules/3.5.0-23-generic/kernel/drivers/net/ethernet/qlogic/netxen/netxen_nic.ko
lib/modules/3.5.0-23-generic/kernel/drivers/net/xen-netback
lib/modules/3.5.0-23-generic/kernel/drivers/net/xen-netback/xen-netback.ko
lib/modules/3.5.0-23-generic/kernel/drivers/block/xen-blkback
lib/modules/3.5.0-23-generic/kernel/drivers/block/xen-blkback/xen-blkback.ko

[root@ CTU10000xxxxx home]# lsinitramfs /boot/initrd.img-`uname -r` |grep virtio
lib/modules/3.5.0-23-generic/kernel/drivers/scsi/virtio_scsi.ko
```

◯ NOTE

> If you add built-in drivers to the initrd or initramfs file by mistake, the ECS will not be affected. The drivers cannot be found by running the **lsinitrd** command. You can run the following commands to check whether built-in drivers are in the kernel:
>
> ```
> [root@ CTU10000xxxxx home]# cat /boot/config-`uname -r` | grep CONFIG_VIRTIO | grep y
> CONFIG_VIRTIO_BLK=y
> CONFIG_VIRTIO_NET=y
> CONFIG_VIRTIO=y
> CONFIG_VIRTIO_RING=y
> CONFIG_VIRTIO_PCI=y
> CONFIG_VIRTIO_MMIO_CMDLINE_DEVICES=y
> [root@ CTU10000xxxxx home]# cat /boot/config-`uname -r` | grep CONFIG_XEN | grep y
> CONFIG_XEN_BLKDEV_FRONTEND=y
> CONFIG_XEN_NETDEV_FRONTEND=y
> ```

SUSE and openSUSE

If the OS version is earlier than SUSE 12 SP1 or openSUSE 13, modify the **/etc/sysconfig/kernel** file to add drivers. For details, see **scenario 1**.

If the OS version is SUSE 12 SP1, modify the **/etc/dracut.conf** file to add drivers. For details, see **scenario 2**.

If the OS version is later than SUSE 12 SP1 or openSUSE 13, modify the **/etc/dracut.conf** file to add drivers. For details, see **scenario 3**.

- If the OS version is earlier than SUSE 12 SP1 or openSUSE 13, perform the following steps:

  ◯ NOTE

  > For SUSE, run the following command to check whether xen-kmp (driver package for Xen PV) is installed in the OS:
  >
  > **rpm -qa |grep xen-kmp**
  >
  > If information similar to the following is displayed, xen-kmp is installed:
  >
  > ```
  > xen-kmp-default-4.2.2_04_3.0.76_0.11-0.7.5
  > ```
  >
  > If xen-kmp is not installed, obtain it from the installation ISO and install it first.

  a. Run the following command to open the **/etc/sysconfig/kernel** file:

  vi /etc/sysconfig/kernel

  b. Add Xen PV and VirtIO drivers after **INITRD_MODULES=** (the format varies depending on the OS).
  ```
  SIA10000xxxxx:~ # vi /etc/sysconfig/kernel
  # (like drivers for scsi-controllers, for lvm or reiserfs)
  ```

```
#
INITRD_MODULES="ata_piix ata_generic xen_vnif xen_vbd xen_platform_pci virtio_blk
virtio_scsi virtio_net virtio_pci virtio_ring virtio"
```

c.   Run the **mkinitrd** command to regenerate initrd:

📖 NOTE

> If the virtual file system is not the default initramfs or initrd, run the **dracut -f**
> *Name of the initramfs or initrd file actually used* command. The actual initramfs
> or initrd file name can be obtained from the **menu.lst** or **grub.cfg** file (**/boot/**
> **grub/menu.lst**, **/boot/grub/grub.cfg**, or **/boot/grub2/grub.cfg**).

The following is an example initrd file of SUSE 11 SP4:

```
default 0
timeout 10
gfxmenu (hd0,0)/boot/message
title sles11sp4_001_[_VMX_]
root (hd0,0)
kernel /boot/linux.vmx vga=0x314 splash=silent console=ttyS0,115200n8 console=tty0
net.ifnames=0 NON_PERSISTENT_DEVICE_NAMES=1 showopts
initrd /boot/initrd.vmx
title Failsafe_sles11sp4_001_[_VMX_]
root (hd0,0)
kernel /boot/linux.vmx vga=0x314 splash=silent ide=nodma apm=off noresume edd=off
powersaved=off nohz=off highres=off processsor.max+cstate=1 nomodeset x11failsafe
console=ttyS0,115200n8 console=tty0 net.ifnames=0 NON_PERSISTENT_DEVICE_NAMES=1
showopts
initrd /boot/initrd.vmx
```

/boot/initrd.vmx in the **initrd** line is the initrd file actually used. Run the
dracut -f /boot/initrd.vmx command. If the initrd file does not contain
the **/boot** directory, such as **/initramfs-**xxx, run the **dracut -f /boot/**
initramfs-xxx command.

d.   Run the following commands to check whether Xen PVOPS and KVM
VirtIO have been installed:

lsinitrd /boot/initrd-`uname -r` | grep xen

lsinitrd /boot/initrd-`uname -r` | grep virtio

```
SIA10000xxxxx:~ # lsinitrd /boot/initrd-`uname -r` | grep xen
-rwxr--r-- 1 root root 42400 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/block/
xen-blkfront.ko
-rwxr--r-- 1 root root 44200 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/net/
xen-netfront.ko

SIA10000xxxxx:~ # lsinitrd /boot/initrd-`uname -r` | grep virtio
-rwxr--r-- 1 root root 19248 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/scsi/
virtio_scsi.ko
-rwxr--r-- 1 root root 23856 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/block/
virtio_blk.ko
drwxr-xr-x 2 root root 0 Jul 12 14:53 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/virtio
-rwxr--r-- 1 root root 15848 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/virtio/
virtio_ring.ko
-rwxr--r-- 1 root root 20008 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/virtio/
virtio_pci.ko
-rwxr--r-- 1 root root 12272 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/virtio/
virtio.ko
-rwxr--r-- 1 root root 38208 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/net/
virtio_net.ko
```

e.   Restart the ECS.

f.   Modify the **/boot/grub/menu.lst** file. Add
xen_platform_pci.dev_unplug=all and modify the root configuration.

Before the modification:

```
###Don't change this comment -YaST2 identifier: Original name: linux###
title SUSE Linux Enterprise Server 11SP4 - 3.0.76-0.11 (default)
```

```
root (hd0,0)
kernel /boot/vmlinuz-3.0.76-0.11-default root=UUID=4eb40294-4c6f-4384-bbb6-
b8795bbb1130 splash=silentcrashkernel=256M-:128M showopts vga=0x314
initrd /boot/initrd-3.0.76-0.11-default
```

After the modification:

```
###Don't change this comment -YaST2 identifier: Original name: linux###
title SUSE Linux Enterprise Server 11SP4 - 3.0.76-0.11 (default)
root (hd0,0)
kernel /boot/vmlinuz-3.0.76-0.11-default root=UUID=4eb40294-4c6f-4384-bbb6-
b8795bbb1130 splash=silentcrashkernel=256M-:128M showopts vga=0x314
xen_platform_pci.dev_unplug=all
initrd /boot/initrd-3.0.76-0.11-default
```

📖 NOTE

- Ensure that the root partition is in the UUID format.
- **xen_platform_pci.dev_unplug=all** is added to shield QEMU devices.
- For SUSE 11 SP1 64bit to SUSE 11 SP4 64bit, add **xen_platform_pci.dev_unplug=all** to the **menu.lst** file. For SUSE 12 or later, QEMU device shield is enabled by default, and you do not need to configure it.

g. Run the following commands to check whether Xen drivers exist in initrd:

lsinitrd /boot/initrd-`uname -r` | grep xen

lsinitrd /boot/initrd-`uname -r` | grep virtio

```
SIA10000xxxxx:~ # lsinitrd /boot/initrd-`uname -r` | grep xen
-rwxr--r-- 1 root root 42400 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/block/
xen-blkfront.ko
-rwxr--r-- 1 root root 44200 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/net/
xen-netfront.ko

SIA10000xxxxx:~ # lsinitrd /boot/initrd-`uname -r` | grep virtio
-rwxr--r-- 1 root root 19248 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/scsi/
virtio_scsi.ko
-rwxr--r-- 1 root root 23856 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/block/
virtio_blk.ko
drwxr-xr-x 2 root root 0 Jul 12 14:53 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/virtio
-rwxr--r-- 1 root root 15848 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/virtio/
virtio_ring.ko
-rwxr--r-- 1 root root 20008 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/virtio/
virtio_pci.ko
-rwxr--r-- 1 root root 12272 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/virtio/
virtio.ko
-rwxr--r-- 1 root root 38208 Jun 22 2012 lib/modules/2.6.32-279.el6.x86_64/kernel/drivers/net/
virtio_net.ko
```

📖 NOTE

If you add built-in drivers to the initrd or initramfs file, the ECS will not be affected. This makes it easy to modify the drivers. However, you cannot check the drivers by running the **lsinitrd** command. You can run the following commands to check whether built-in drivers are in the kernel:

cat /boot/config-`uname -r` | grep CONFIG_VIRTIO | grep y

cat /boot/config-`uname -r` | grep CONFIG_XEN | grep y

- If the OS version is SUSE 12 SP1, perform the following steps:

a. Run the following command to open the **/etc/dracut.conf** file:

vi /etc/dracut.conf

b. Press **i** to enter editing mode and add Xen PV and VirtIO drivers to **add-drivers** (the format varies depending on the OS).

```
[root@CTU10000xxxxx ~]# vi /etc/dracut.conf
# additional kernel modules to the default
```

```
add_drivers+="ata_piix ata_generic xen_vnif xen_vbd xen_platform_pci virtio_blk virtio_scsi
virtio_net virtio_pci virtio_ring virtio"
```

c. Press **Esc**, enter **:wq**, and press **Enter**. The system saves the change and exits the **/etc/dracut.conf** file.

d. Run the following command to regenerate initrd:

dracut -f /boot/initramfs-*File name*

If the virtual file system is not the default initramfs, run the **dracut -f** *Name of the initramfs or initrd file actually used* command. The actual initramfs or initrd file name can be obtained from the **grub.cfg** file, which can be **/boot/grub/grub.cfg**, **/boot/grub2/grub.cfg**, or **/boot/grub/grub.conf** depending on the OS.

e. If the virtual file system is initramfs, run the following commands to check whether native Xen and KVM drivers have been installed:

lsinitrd /boot/initramfs-`uname -r`.img | grep xen

lsinitrd /boot/initramfs-`uname -r`.img | grep virtio

If the virtual file system is initrd, run the following commands to check whether native Xen and KVM drivers have been installed:

lsinitrd /boot/initrd-`uname -r` | grep xen

lsinitrd /boot/initrd-`uname -r` | grep virtio

- If the OS version is later than SUSE 12 SP1 or openSUSE 13, perform the following steps:

Take SUSE Linux Enterprise Server 12 SP2 (x86_64) as an example.

a. Run the following command to open the **/etc/dracut.conf** file:

vi /etc/dracut.conf

b. Press **i** to enter editing mode and add Xen PV and VirtIO drivers to **add_drivers** (the format varies depending on the OS).

```
[root@CTU10000xxxxx ~]# vi /etc/dracut.conf
# additional kernel modules to the default
add_drivers+="ata_piix ata_generic xen-blkfront xen-netfront virtio_blk virtio_scsi
virtio_net virtio_pci virtio_ring virtio"
```

c. Press **Esc**, enter **:wq**, and press **Enter**. The system saves the change and exits the **/etc/dracut.conf** file.

d. Run the following command to regenerate initrd:

dracut -f /boot/initramfs-*File name*

If the virtual file system is not the default initramfs, run the **dracut -f** *Name of the initramfs or initrd file actually used* command. The actual initramfs or initrd file name can be obtained from the **grub.cfg** file, which can be **/boot/grub/grub.cfg**, **/boot/grub2/grub.cfg**, or **/boot/grub/grub.conf** depending on the OS.

e. If the virtual file system is initramfs, run the following commands to check whether native Xen and KVM drivers have been installed:

lsinitrd /boot/initramfs-`uname -r`.img | grep xen

lsinitrd /boot/initramfs-`uname -r`.img | grep virtio

If the virtual file system is initrd, run the following commands to check whether the native Xen and KVM drivers have been installed:

lsinitrd /boot/initrd-`uname -r` | grep xen

lsinitrd /boot/initrd-`uname -r` | grep virtio

Assume that the virtual file system is initrd. The following command output will be displayed:

```
sluo-ecs-30dc:~ # lsinitrd /boot/initrd-`uname -r` | grep xen
-rw-r--r-- 1 root root 69575 Oct 26 2016 lib/modules/4.4.21-69-default/kernel/drivers/block/xen-blkfront.ko
-rw-r--r-- 1 root root 53415 Oct 26 2016 lib/modules/4.4.21-69-default/kernel/drivers/net/xen-netfront.ko
drwxr-xr-x 2 root root 0 Sep 28 10:21 lib/modules/4.4.21-69-default/updates/pvdriver/xen-hcall
-rwxr-xr-x 1 root root 8320 Sep 28 10:21 lib/modules/4.4.21-69-default/updates/pvdriver/xen-hcall/xen-hcall.ko

sluo-ecs-30dc:~ # lsinitrd /boot/initrd-`uname -r` | grep virtio
-rw-r--r-- 1 root root 29335 Oct 26 2016 lib/modules/4.4.21-69-default/kernel/drivers/block/virtio_blk.ko
-rw-r--r-- 1 root root 57007 Oct 26 2016 lib/modules/4.4.21-69-default/kernel/drivers/net/virtio_net.ko
-rw-r--r-- 1 root root 32415 Oct 26 2016 lib/modules/4.4.21-69-default/kernel/drivers/scsi/virtio_scsi.ko
drwxr-xr-x 2 root root 0 Sep 28 10:21 lib/modules/4.4.21-69-default/kernel/drivers/virtio
-rw-r--r-- 1 root root 19623 Oct 26 2016 lib/modules/4.4.21-69-default/kernel/drivers/virtio/virtio.ko
-rw-r--r-- 1 root root 38943 Oct 26 2016 lib/modules/4.4.21-69-default/kernel/drivers/virtio/virtio_pci.ko
-rw-r--r-- 1 root root 24431 Oct 26 2016 lib/modules/4.4.21-69-default/kernel/drivers/virtio/virtio_ring.ko
```

📖 NOTE

If you add built-in drivers to the initrd or initramfs file, the ECS will not be affected. This makes it easy to modify the drivers. However, you cannot check the drivers by running the **lsinitrd** command. You can run the following commands to check whether built-in drivers are in the kernel:

cat /boot/config-`uname -r` | grep CONFIG_VIRTIO | grep y

cat /boot/config-`uname -r` | grep CONFIG_XEN | grep y

17 Image Tags

17.1 How Many Tags Can I Add to an Image?

An image can have a maximum of 10 tags.

17.2 How Do I Add, Delete, and Modify Image Tags?

 NOTE

- When adding predefined tags to an image or searching for an image using predefined tags, you must have permission to access the Tag Management Service (TMS).
- If your organization has pre-configured tag policies for images, you need to add tags to your images based on the policies. If you do not comply with the tag policies, images may fail to be created. Contact the organization administrator to learn more about the tag policies.
  - Each tag consists of a key and a value. The key contains a maximum of 36 characters, and the value contains a maximum of 43 characters. The key cannot be left blank or be an empty character string. The value cannot be left blank but can be an empty character string.
  - An image can have a maximum of 10 tags.

1. Access the IMS console.

   a. Log in to the management console.

   b. Under **Compute**, click **Image Management Service**.

      The IMS console is displayed.

2. Click the **Private Images** tab and click the image name to display the image details.

   – To modify an image tag, go to **3**.

   – To delete an image tag, go to **4**.

   – To add an image tag, go to **5**.

3. Click the **Tags** tab, locate the target tag, and click **Edit** in the **Operation** column. In the displayed dialog box, modify the tag.

4. Click the **Tags** tab, locate the target tag, and click **Delete** in the **Operation** column. In the displayed dialog box, click **Yes**.

5. Click the **Tags** tab and then **Add Tag**. In the displayed dialog box, add a tag.

17.3 How Do I Search for Private Images by Tag?

> **NOTE**
>
> - When adding predefined tags to an image or searching for an image using predefined tags, you must have permission to access the Tag Management Service (TMS).
> - If your organization has pre-configured tag policies for images, you need to add tags to your images based on the policies. If you do not comply with the tag policies, images may fail to be created. Contact the organization administrator to learn more about the tag policies.
>   - Each tag consists of a key and a value. The key contains a maximum of 36 characters, and the value contains a maximum of 43 characters. The key cannot be left blank or be an empty character string. The value cannot be left blank but can be an empty character string.
>   - An image can have a maximum of 10 tags.

Search for Private Images by Tag

1. Access the IMS console.

    a. Log in to the management console.

    b. Under **Compute**, click **Image Management Service**.

    The IMS console is displayed.

2. Click the **Private Images** tab and click the search box above the private image list. Under **Resource Tag**, specify the tag key and value to search for images.

    Figure 17-1 Searching for images by tag
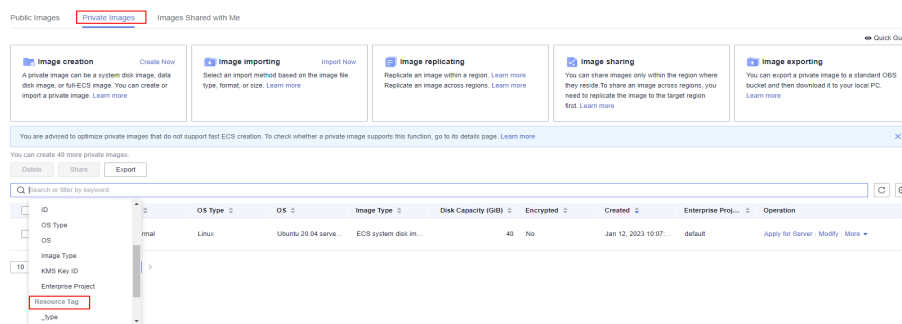
    > **NOTE**
    >
    > - Neither the tag key nor tag value can be empty. When the tag key and tag value are matched, the system automatically shows your desired private images.
    > - You can add multiple tags to search for shared images. The system will display private images that match all tags.

18 Billing

18.1 What Are the Billing Standards of IMS?

Billing of Different Image Types

Image Type	Billing
Public	Free
Private	• System disk image, ISO image, or data disk image: free OBS buckets invisible to users are provided for free to store the images. • Full-ECS image: charged for the storage on CSBS or CBR If the image is created from a CSBS or CBR backup, you will be billed for the space used to store the CSBS or CBR backup.
Shared	• If it is a system or data disk image, the OBS storage is free. • If it is a full-ECS image, you will be billed for the space used to store the CBR backup. **NOTE** Full-ECS images created from a CBR backup can be shared but those created from a CSBS backup cannot.
KooGallery	Determined by the image provider.

Billing of Private Image Operations

Operation	Billing Item
Uploading an external image file to an OBS bucket	OBS storage (You are advised to delete unneeded image files.)

Operation	Billing Item
Creating an ECS from a system disk image or full-ECS image	EVS disks attached to the created ECS (The system disk image and full-ECS image are free of charge.) For example, when you use a full-ECS image (with a 40 GB system disk and 100 GB data disk) to create an ECS, you will be charged based on the total capacity of the system disk and data disk. **NOTE** If a private image is created using an ECS created from a KooGallery image, you will be billed for the private image based on the KooGallery price.
Replication of a system or data disk image within a region	None. OBS buckets are available for free to store the image copies.
Cross-region replication of a system or data disk image	Traffic generated by OBS cross-region replication
Cross-region replication of a full-ECS image	● Traffic of CSBS or CBR cross-region replication ● Space used for storing the CSBS or CBR backup associated with the newly replicated image
Exporting images	OBS space for storing the exported images

Reference

- For OBS pricing details, see **OBS Pricing Details**.
- For CSBS pricing details, see **CSBS Pricing Details**.
- For CBR pricing details, see **CBR Pricing Details**.
- For EVS pricing details, see **EVS Pricing Details**.

18.2 How Will I Be Billed for Full-ECS Images?

- For a full-ECS image created from a CSBS or CBR backup, you will be charged for the space used to store the CSBS or CBR backup.

- For a full-ECS image shared by others, you will be charged for the space used to store the CBR backup.

- When you use a full-ECS image to create an ECS, the full-ECS image is free of charge, but you will be billed for EVS disks attached to the ECS.

  For example, when you use a full-ECS image (with a 40 GB system disk and 100 GB data disk) to create an ECS, you will be charged based on the total capacity of the system disk and data disk.

- When you replicate a full-ECS image across regions, you will be billed for:
  - Traffic of CSBS or CBR cross-region replication

- Space for storing the CSBS or CBR backup associated with the newly replicated image

19 Change History

Released On	Description
2023-10-31	This issue is the twenty-ninth official release. Added the following content: **How Do I Authorize a Key?**
2023-08-08	This issue is the twenty-eighth official release. Modified the following content: Deleted cloudResetPwdUpdateAgent in **What Do I Do If the One-Click Password Resetting Plug-In Failed to Start?**.
2023-07-14	This issue is the twenty-seventh official release. Added the following content: ● **How Do I Use a Private Image Created from a First-Generation ECS to Create a Second-Generation ECS?** ● **KooGallery Images**
2023-05-11	This issue is the twenty-sixth official release. Modified the following content: Deleted a note for enabling self-assigned IPv6 addresses in **How Do I Configure an ECS to Dynamically Acquire IPv6 Addresses?**.
2023-02-24	This issue is the twenty-fifth official release. Added the following content: **What Do I Do If I Cannot Change the Resolution of a Windows OS Booted in UEFI Mode?**
2023-01-06	This issue is the twenty-fourth official release. Modified the following content: Added Debian, Ubuntu, Red Hat, FreeBSD, and other OS types in **EOS Plan**.

Released On	Description
2022-12-07	This issue is the twenty-third official release. Added the following content: ● **End-of-Support for OSs** ● **What Do I Do If CentOS Linux Is No Longer Maintained?** ● **EOS Plan**
2022-11-09	This issue is the twenty-second official release. Added the following content: ● **Driver Installation** ● **Image Tags**
2022-08-23	This issue is the twenty-first official release. Added the following content: **Basic Concepts** **How Will I Be Billed for Sharing an Image?** **What Are the Differences Between Sharing Images and Replicating Images?** **How Will I Be Billed for Full-ECS Images?** Modified the following content: ● Modified the caution in **How Do I Install Native Xen and KVM Drivers?**. ● Provided a method for replicating images across regions in the NOTE in **What Are the Regions That Support Cross-Region Replication of System and Data Disk Images?** when they cannot be migrated by using cross-region replication of IMS.
2022-08-12	This issue is the twentieth official release. Added the following content: ● **How Do I Optimize an Image?**
2022-04-14	This issue is the nineteenth official release. Modified the following content: Regions that support cross-region replication of system and data disk images are listed in **Image Replication**.
2021-07-15	This issue is the eighteenth official release. Deleted the following content: ● How Do I Share a Full-ECS Image Created from a CSBS Backup with Other Tenants?

Released On	Description
2021-05-28	This issue is the seventeenth official release. Modified the following content: ● Added the operation for enabling IPv6 on Windows Server 2012 in **How Do I Configure an ECS to Dynamically Acquire IPv6 Addresses?** ● Updated the ECSs that support NIC multi-queue in **How Do I Enable NIC Multi-Queue for an Image?**
2021-03-03	This issue is the sixteenth official release. Modified the following content: ● **How Do I Configure an ECS to Dynamically Acquire IPv6 Addresses?**
2020-11-28	This issue is the eleventh official release. Added the following content: ● **Is There Any Difference Between the Image Created from a CSBS/CBR Backup and That Created from an ECS?** ● **Why Can't I Find My Private Image When I Want to Use It to Create an ECS or Change the OS of an ECS?**
2020-05-28	This issue is the tenth official release. Added the following content: ● **Why Can't I Find an ISO Image When I Want to Use It to Create an ECS or Change the OS of an ECS?** ● **What Do I Do If I Cannot Share My Images?** ● **Can I Download My Private Images to a Local PC?** ● **What Do I Do If the Export Option Is Unavailable for My Image?** ● **How Do I Configure an ECS to Dynamically Acquire IPv6 Addresses?** ● **Image Deletion** Modified the following content: Adjusted the structure of the document.
2020-01-30	This issue is the ninth official release. Added the following content: ● **How Can I Use a Backup to Create an EVS Disk or ECS?** ● **Can I Use the System Disk Image of an ECS on a BMS After I Export It from the Cloud Platform?** ● **Can I Download a Public Image to My Local PC?**

Released On	Description
2019-12-30	This issue is the eighth official release. Added the following content: ● **What Do I Do If I Want to Set Up an OpenVPN or PyTorch Environment But No Public Images Containing OpenVPN or PyTorch Are Available?** ● **How Can I Back Up the Current Status of an ECS for Restoration in the Case of a System Fault?**
2019-11-30	This issue is the seventh official release. Added the following content: ● **What Are the Differences Between Images and Backups?** ● **Full-ECS Image FAQs** Modified the following content: Adjusted the structure of the document.
2019-09-30	This issue is the sixth official release. Added the following content: ● **What Do I Do If I Cannot Find a Desired Image?** ● **Image Creation FAQs** ● **Image Sharing FAQs** ● **Image Encryption** ● **How Do I Make a System Disk Image Support Fast ECS Creation?**
2019-04-30	This issue is the fifth official release. Added the following content: **Why Do I Need to Install and Update VirtIO Drivers for Windows?** Deleted the following content: What Do I Do If I Cannot Create an Image in ZVHD2 Format Using an API?
2019-04-09	This issue is the fourth official release. Deleted the following content: What Do I Do If the Provided OS Images Cannot Meet My Requirement?
2019-03-30	This issue is the third official release. Added the following content: **What Do I Do If an Exception Occurs When I Start an ECS Created from an Image Using the UEFI Boot Mode?** Modified the following content: **What Will the System Do to an Image File When I Use the File to Register a Private Image?**

Released On	Description
2019-02-15	This issue is the second official release. Added the following content: • **How Do I Increase the Image Quota?** • **What Can I Do with a Cloud-Init ECS?**
2019-01-10	This issue is the first official release.