

Administración de imágenes

Guía del usuario

Edición 28
Fecha 2025-11-11



Copyright © Huawei Technologies Co., Ltd. 2025. Todos los derechos reservados.

Quedan terminantemente prohibidas la reproducción y la divulgación del presente documento en todo o en parte, de cualquier forma y por cualquier medio, sin la autorización previa de Huawei Technologies Co., Ltd. otorgada por escrito.

Marcas y permisos



HUAWEI y otras marcas registradas de Huawei pertenecen a Huawei Technologies Co., Ltd.

Todas las demás marcas registradas y los otros nombres comerciales mencionados en este documento son propiedad de sus respectivos titulares.

Aviso

Las funciones, los productos y los servicios adquiridos están estipulados en el contrato celebrado entre Huawei y el cliente. Es posible que la totalidad o parte de los productos, las funciones y los servicios descritos en el presente documento no se encuentren dentro del alcance de compra o de uso. A menos que el contrato especifique lo contrario, ninguna de las afirmaciones, informaciones ni recomendaciones contenidas en este documento constituye garantía alguna, ni expresa ni implícita.

La información contenida en este documento se encuentra sujeta a cambios sin previo aviso. En la preparación de este documento se realizaron todos los esfuerzos para garantizar la precisión de sus contenidos. Sin embargo, ninguna declaración, información ni recomendación contenida en el presente constituye garantía alguna, ni expresa ni implícita.

Índice

1 Gestión de imágenes públicas.....	1
1.1 Descripción.....	1
1.2 Historial de actualizaciones de imagen (x86).....	3
1.3 Historial de actualizaciones de imagen (Arm).....	31
1.4 Problemas conocidos.....	37
2 Crear una imagen privada.....	42
2.1 Introducción.....	42
2.2 Creación de una imagen de disco del sistema desde un ECS de Windows.....	43
2.3 Creación de una imagen de disco del sistema desde un ECS de Linux.....	47
2.4 Creación de una imagen de disco del sistema Windows a partir de un archivo de imagen externo.....	50
2.4.1 Descripción.....	51
2.4.2 Preparación de un archivo de imagen.....	51
2.4.3 Carga de un archivo de imagen externo.....	54
2.4.4 Registro de un archivo de imagen externo como imagen privada.....	55
2.4.5 Creación de un ECS de Windows a partir de una imagen.....	58
2.5 Creación de una imagen de disco de sistema Linux a partir de un archivo de imagen externo.....	59
2.5.1 Descripción.....	59
2.5.2 Preparación de un archivo de imagen.....	60
2.5.3 Carga de un archivo de imagen externo.....	62
2.5.4 Registro de un archivo de imagen externo como imagen privada.....	63
2.5.5 Creación de un ECS de Linux a partir de una imagen.....	66
2.6 Creación de una imagen de disco de datos a partir de un ECS.....	67
2.7 Creación de una imagen de disco de datos a partir de un archivo de imagen externo.....	70
2.8 Creación de una imagen de ECS completo a partir de un ECS.....	73
2.9 Creación de una imagen completa de ECS a partir de una copia de respaldo de CSBS.....	76
2.10 Creación de una imagen completa de ECS a partir de una copia de respaldo de CBR.....	78
2.11 Creación de una imagen de disco de sistema Windows a partir de un archivo ISO.....	80
2.11.1 Descripción.....	80
2.11.2 Integración del controlador VMTools en un archivo ISO.....	82
2.11.3 Registro de un archivo ISO como una imagen ISO.....	87
2.11.4 Creación de un ECS de Windows a partir de una imagen ISO.....	89
2.11.5 Instalación de un sistema operativo Windows y el controlador VMToolsVirtIO.....	90
2.11.6 Configuración del ECS y creación de una imagen de disco del sistema Windows.....	101

2.12 Creación de una imagen de disco de sistema Linux a partir de un archivo ISO.....	102
2.12.1 Descripción.....	102
2.12.2 Registro de un archivo ISO como una imagen ISO.....	104
2.12.3 Creación de un ECS de Linux a partir de una imagen ISO.....	106
2.12.4 Instalación de un sistema operativo Linux.....	107
2.12.5 Configuración del ECS y creación de una imagen de disco del sistema Linux.....	112
2.13 Importación de una imagen.....	114
2.14 Importación rápida de un archivo de imagen.....	115
2.14.1 Descripción.....	115
2.14.2 Importación rápida de un archivo de imagen (Linux).....	118
2.14.3 Importación rápida de un archivo de imagen (Windows).....	124
3 Gestión de imágenes privadas.....	127
3.1 Modificación de una imagen.....	127
3.2 Exportación de lista de imágenes.....	129
3.3 Comprobación de la capacidad del disco de una imagen.....	130
3.4 Creación de un ECS a partir de una imagen.....	132
3.5 Eliminación de imágenes.....	132
3.6 Compartir imágenes.....	133
3.6.1 Descripción.....	133
3.6.2 Obtención del ID de proyecto, ID de cuenta y organización URN.....	135
3.6.3 Compartir imágenes especificadas.....	135
3.6.4 Aceptación o rechazo de imágenes compartidas.....	137
3.6.5 Rechazo de imágenes aceptadas.....	140
3.6.6 Aceptación de imágenes rechazadas.....	141
3.6.7 Dejar de compartir imágenes.....	142
3.6.8 Adición de tenants que pueden usar imágenes compartidas.....	142
3.6.9 Eliminación de destinatarios de imágenes que pueden usar imágenes compartidas.....	143
3.6.10 Replicación de una imagen compartida.....	144
3.7 Exportación de una imagen.....	145
3.8 Optimización de una imagen privada de Windows.....	147
3.8.1 Proceso de optimización.....	147
3.8.2 Visualización del tipo de virtualización de un ECS de Windows.....	147
3.8.3 Obtención de paquetes de software requeridos.....	148
3.8.4 Instalación del PV driver.....	149
3.8.5 Instalación de UVP VMTools.....	152
3.8.6 Borrar registros del sistema.....	155
3.9 Optimización de una imagen privada de Linux.....	155
3.9.1 Proceso de optimización.....	155
3.9.2 Comprobación de si una imagen privada necesita ser optimizada.....	156
3.9.3 Uso de un script para optimizar una imagen privada de Xen.....	158
3.9.4 Desinstalación de PV Drivers de un ECS de Linux.....	158
3.9.5 Cambio del identificador de disco en el archivo de configuración de GRUB a UUID.....	159

3.9.6 Cambio del identificador de disco en el archivo fstab a UUID.....	164
3.9.7 Instalación de controladores KVM nativos.....	165
3.9.8 Borrar registros del sistema.....	171
3.10 Encriptación de imágenes.....	172
3.10.1 Descripción.....	172
3.10.2 Creación de imágenes encriptadas.....	172
3.11 Replicación de imágenes dentro de una región.....	173
3.12 Replicación de imágenes entre regiones.....	175
3.13 Etiquetado de una imagen.....	182
3.14 Auditoría de operaciones clave.....	183
3.14.1 Operaciones de IMS registradas por CTS.....	183
3.14.2 Consulta de trazas.....	185
4 Operaciones de Windows.....	187
4.1 Configuración de la NIC en DHCP.....	187
4.2 Habilitación de la conexión a Escritorio remoto.....	189
4.3 Instalación y configuración de Cloudbase-Init.....	190
4.4 Instalación del complemento de restablecimiento de contraseñas con un solo clic.....	196
4.5 Ejecución de Sysprep.....	199
5 Operaciones Linux.....	202
5.1 Configuración de la NIC en DHCP.....	202
5.2 Eliminación de archivos del directorio de reglas de red.....	204
5.3 Instalación de Cloud-Init.....	206
5.4 Configuración de Cloud-Init.....	216
5.5 Instalación del complemento de restablecimiento de contraseñas con un solo clic.....	220
5.6 Separación de discos de datos de un ECS.....	225
6 Gestión de permisos.....	227
6.1 Creación de un usuario y concesión de permisos.....	227
6.2 Creación de una política personalizada.....	229

1 Gestión de imágenes públicas

1.1 Descripción

Las imágenes públicas proporcionadas por Huawei Cloud se pueden usar con ECS o BMS y vienen con un conjunto de complementos especiales preinstalados. Estas imágenes están disponibles para todos los usuarios y cubren la mayoría de los sistemas operativos convencionales. Esta sección describe los tipos y características de las imágenes públicas.

Tipos de imágenes públicas

Las imágenes públicas proporcionadas por Huawei Cloud incluyen imágenes EulerOS desarrolladas por Huawei e imágenes comerciales de terceros. Elija la imagen pública que mejor satisfaga sus necesidades. Si tiene algún problema con el sistema operativo, puede ponerse en contacto con el proveedor del sistema operativo o ir a la comunidad de código abierto para obtener soporte técnico, pero Huawei Cloud también proporciona asistencia técnica.

Tabla 1-1 Tipos de imágenes públicas

Tipo de imagen	Descripción
Imagen EulerOS desarrollada por Huawei	Huawei EulerOS para ARM64 es un sistema operativo Linux universal (EulerOS) de clase empresarial. Con una fiabilidad excepcional, seguridad mejorada y alta disponibilidad, EulerOS es una plataforma informática de gama alta que aprovecha al máximo la escalabilidad, el rendimiento y la apertura de Linux.
Imagen comercial de terceros	Huawei Cloud prueba, crea y publica rigurosamente imágenes de terceros con licencia que son altamente seguras y estables. Las imágenes públicas de terceros incluyen: <ul style="list-style-type: none">● Windows: Servidor de Windows● Linux: Ubuntu, CentOS, openSUSE, Debian, Fedora, FreeBSD y CoreOS

 **NOTA**

Los sistemas operativos de imagen disponibles varían según las variantes del servidor:

- [Sistemas operativos compatibles con diferentes tipos de ECS](#)
- [Sistemas operativos compatibles con diferentes tipos de BMS](#)

Características de la imagen pública

- Tipos de sistemas operativos: sistemas operativos Linux y Windows que se actualizan y mantienen periódicamente
Para obtener más información sobre el historial de actualizaciones de imágenes públicas, consulte [Historial de actualizaciones de imagen \(x86\)](#).
- Software compatible: Las imágenes públicas contienen algunos complementos de los que dependen las redes de servidores y las funciones básicas.

 **NOTA**

Los complementos que vienen con imágenes públicas son necesarios para que los ECS o BMS funcionen correctamente. No elimine ni modifique ninguno de ellos. De lo contrario, las funciones básicas de sus ECS o BMS se verán afectadas.

Tabla 1-2 Software soportado

Software	Descripción
Cloud-Init o Cloudbase-Init	Cloud-Init o Cloudbase-Init es una herramienta de inicialización de nube de código abierto. Es esencialmente una serie de scripts y componentes de Python. Al crear un servidor en la nube con una imagen que tenga instalado Cloud-Init o Cloudbase-Init, puede inyectar detalles personalizados (como la contraseña de inicio de sesión para el servidor en la nube). También puede consultar y usar metadatos para configurar y gestionar servidores en la nube. De forma predeterminada, Cloud-Init está instalado para las imágenes públicas de Linux y Cloudbase-Init está instalado para las imágenes públicas de Windows.
Complemento de restablecimiento de contraseña con un solo clic	ECS y BMS proporcionan una función de restablecimiento de contraseña con un solo clic. Si olvida la contraseña de su ECS o BMS, o la contraseña caduca, puede establecer una nueva contraseña desde la consola de gestión mediante el complemento de restablecimiento de contraseña con un solo clic. Este complemento se instala para imágenes públicas de forma predeterminada.
Complemento de NIC multi-queue	La cola múltiple de la NIC permite que varias vCPU procesen interrupciones de la NIC, mejorando así el PPS de la red y el rendimiento de E/S. Para obtener más información sobre las imágenes públicas que admiten la cola múltiple de NIC, consulte ¿Cómo Habilito la cola múltiple de NIC para una imagen?

- Compatibilidad: Las imágenes públicas son compatibles con diferentes hardware de servidor.

- Seguridad: Las imágenes públicas son estables y tienen licencia.

1.2 Historial de actualizaciones de imagen (x86)

Esta sección describe el historial de actualizaciones de las imágenes públicas (x86).

2023-09-07

Sistema operativo	Imagen	Detalles
openEuler	Nombre de la imagen: openEuler 22.03 64bit	Imagen publicada.
	Versión del núcleo: 5.10.0-60.109.0.136.oe2203.x86_64	
	Regiones: todas	

2023-08-23

Sistema operativo	Imagen	Detalles
Debian	Nombres de las imágenes: <ul style="list-style-type: none"> ● Debian 11.1.0 64bit ● Debian 10.0.0 64 bit 	<ul style="list-style-type: none"> ● Actualizada la versión del kernel del sistema operativo para corregir vulnerabilidades de seguridad. ● Eliminado el parámetro del kernel kernel.unknown_nmi_panic. ● Actualizada la versión del complemento de contraseña con un solo clic.
	Versiones de kernel: <ul style="list-style-type: none"> ● Debian 11.1.0: 5.10.0-23-amd64 ● Debian 10.0.0: 4.19.0-25-amd64 	
	Regiones: todas	
Rocky Linux	Nombres de las imágenes: <ul style="list-style-type: none"> ● Rocky Linux 9.0 64bit ● Rocky Linux 8.5 64bit ● Rocky Linux 8.4 64bit 	<ul style="list-style-type: none"> ● Actualizada la versión del kernel del sistema operativo para corregir vulnerabilidades de seguridad. ● Eliminado el parámetro del kernel kernel.unknown_nmi_panic. ● Actualizada la versión del complemento de contraseña con un solo clic.

Sistema operativo	Imagen	Detalles
	Versiones de kernel: <ul style="list-style-type: none"> ● Rocky 9.0: 5.14.0-284.25.1.el9_2.x86_64 ● Rocky 8.5: 4.18.0-477.15.1.el8_8.x86_64 ● Rocky 8.4: 4.18.0-477.15.1.el8_8.x86_64 Regiones: todas	
AlmaLinux	Nombres de las imágenes: <ul style="list-style-type: none"> ● AlmaLinux 9.0 64bit ● AlmaLinux 8.4 64bit ● AlmaLinux 8.3 64bit Versiones de kernel: <ul style="list-style-type: none"> ● AlmaLinux 9.0: 5.14.0-284.25.1.el9_2.x86_64 ● AlmaLinux 8.4: 4.18.0-477.21.1.el8_8.x86_64 ● AlmaLinux 8.3: 4.18.0-477.21.1.el8_8.x86_64 Regiones: todas	<ul style="list-style-type: none"> ● Actualizada la versión del kernel del sistema operativo para corregir vulnerabilidades de seguridad. ● Eliminado el parámetro del kernel kernel.unknown_nmi_panic. ● Actualizada la versión del complemento de contraseña con un solo clic.
CentOS	Nombres de las imágenes: <ul style="list-style-type: none"> ● CentOS 8.0 64bit ● CentOS 8.1 64bit ● CentOS 8.2 64bit Versiones de kernel: <ul style="list-style-type: none"> ● CentOS 8.0: 4.18.0-348.7.1.el8_5.x86_64 ● CentOS 8.1: 4.18.0-348.7.1.el8_5.x86_64 ● CentOS 8.2: 4.18.0-348.7.1.el8_5.x86_64 Regiones: todas	<ul style="list-style-type: none"> ● Eliminado el parámetro del kernel kernel.unknown_nmi_panic. ● Actualizada la versión del complemento de contraseña con un solo clic.

2023-08-16

Sistema operativo	Imagen	Detalles
CentOS Stream	Nombres de las imágenes: <ul style="list-style-type: none"> ● CentOS Stream 9 64bit ● CentOS Stream 8 64bit 	Las imágenes publicadas.
	Versiones de kernel: <ul style="list-style-type: none"> ● CentOS Stream 9: 5.14.0-352.el9.x86_64 ● CentOS Stream 8: 4.18.0-500.el8.x86_64 	
	Regiones: todas	

2023-07-29

Sistema operativo	Imagen	Detalles
CentOS	Nombres de las imágenes: <ul style="list-style-type: none"> ● CentOS 7.4 64bit ● CentOS 7.5 64bit ● CentOS 7.6 64bit ● CentOS 7.7 64bit ● CentOS 7.8 64bit ● CentOS 7.9 64bit 	<ul style="list-style-type: none"> ● Actualizada la versión del kernel del sistema operativo para corregir vulnerabilidades de seguridad. ● Eliminado el parámetro del kernel kernel.unknown_nmi_panic. ● Actualizada la versión del complemento de contraseña con un solo clic.
	Versión de kernel: CentOS 7: 3.10.0-1160.92.1.el7.x86_64	
	Regiones: todas	
Ubuntu	Nombres de las imágenes: <ul style="list-style-type: none"> ● Ubuntu 16.04 server 64bit ● Ubuntu 18.04 server 64bit ● Ubuntu 20.04 server 64bit ● Ubuntu 22.04 server 64bit 	<ul style="list-style-type: none"> ● Actualizada la versión del kernel del sistema operativo para corregir vulnerabilidades de seguridad. ● Eliminado el parámetro del kernel kernel.unknown_nmi_panic. ● Actualizada la versión del complemento de contraseña con un solo clic.

Sistema operativo	Imagen	Detalles
	Versiones de kernel: <ul style="list-style-type: none"> ● Ubuntu 16.04: 4.4.0-210-generic ● Ubuntu 18.04: 4.15.0-213-generic ● Ubuntu 20.04: 5.4.0-153-generic ● Ubuntu 22.04: 5.15.0-76-generic Regiones: todas	
EulerOS	Nombre de la imagen: EulerOS 2.5 64bit	<ul style="list-style-type: none"> ● Actualizada la versión del kernel del sistema operativo para corregir vulnerabilidades de seguridad. ● Eliminado el parámetro del kernel kernel.unknown_nmi_panic. ● Actualizada la versión del complemento de contraseña con un solo clic.
	Versión de kernel: EulerOS 2.5: 3.10.0-862.14.1.5.757.eulerosv2r7.x86_64	
	Regiones: todas	
Huawei Cloud EulerOS 1.1	Nombre de la imagen: Huawei Cloud EulerOS 1.1 64bit for CentOS	<ul style="list-style-type: none"> ● Actualizada la versión del kernel del sistema operativo para corregir vulnerabilidades de seguridad. ● Eliminado el parámetro del kernel kernel.unknown_nmi_panic. ● Actualizada la versión del complemento de contraseña con un solo clic.
	Versión de kernel: 5.10.0-60.18.0.50.r865_35.hce2.x86_64	
	Región: AP-Singapore	

2023-06-15

Sistema operativo	Imagen	Detalles
Huawei Cloud EulerOS 2.0	Nombre de la imagen: Huawei Cloud EulerOS 2.0 Standard 64 bit	<ul style="list-style-type: none"> ● Actualizada la versión del kernel del sistema operativo para corregir vulnerabilidades de seguridad. ● Eliminado el parámetro del kernel kernel.unknown_nmi_panic. ● Actualizada la versión del complemento de contraseña con un solo clic.
	Versión de kernel: 5.10.0-60.18.0.50.r865_35.hce2.x86_64	
	Regiones: todas	
Huawei Cloud EulerOS 2.0	Nombre de la imagen: Huawei Cloud EulerOS 2.0 Level 3 of MLPS 2.0 64 bit	<ul style="list-style-type: none"> ● Actualizada la versión del kernel del sistema operativo para corregir vulnerabilidades de seguridad. ● Eliminado el parámetro del kernel kernel.unknown_nmi_panic. ● Actualizada la versión del complemento de contraseña con un solo clic.
	Versión del núcleo: 5.10.0-60.18.0.50.r865_35.hce2.x86_64	
	Regiones: todas	

2022-09-30

Sistema operativo	Imagen	Detalles
Huawei Cloud EulerOS 2.0	Nombre de la imagen: Huawei Cloud EulerOS 2.0 Standard 64 bit for ARM	Imagen publicada.
	Versión de kernel: 5.10.0-60.18.0.50.r509_2.hce2.x86_64	
	Región: AP-Singapore	
Huawei Cloud EulerOS 2.0	Nombre de la imagen: Huawei Cloud EulerOS 2.0 Standard 64 bit	Imagen publicada.

Sistema operativo	Imagen	Detalles
	Versión de kernel: 5.10.0-60.18.0.50.h322_1.hce2.x86_64 Región: AP-Singapore	
Huawei Cloud EulerOS 1.1	Nombre de la imagen: Huawei Cloud EulerOS 1.1 64bit for CentOS Versiones de kernel: 3.10.0-1160.66.1.hce1c.x86_64 5.10.0-60.18.0.50.h322_1.hce2.x86_64 (default) Región: AP-Singapore	Imagen publicada.

2022-03-22

Sistema operativo	Imagen	Detalles
CentOS	Nombres de las imágenes: <ul style="list-style-type: none"> ● CentOS 6.10 64bit ● CentOS 7.2 64bit ● CentOS 7.3 64bit ● CentOS 7.4 64bit ● CentOS 7.5 64bit ● CentOS 7.6 64bit ● CentOS 7.7 64bit ● CentOS 7.8 64bit ● CentOS 7.9 64bit ● CentOS 8.0 64bit ● CentOS 8.1 64bit ● CentOS 8.2 64bit Versiones de kernel: <ul style="list-style-type: none"> ● CentOS 6: 2.6.32-754.35.1.el6.x86_64 ● CentOS 7: 3.10.0-1160.53.1.el7.x86_64 ● CentOS 8: 4.18.0-348.7.1.el8_5.x86_64 	<ul style="list-style-type: none"> ● Actualizada la versión del kernel del sistema operativo para corregir vulnerabilidades de seguridad. ● Actualizado el complemento de restablecimiento de contraseña con un solo clic.

Sistema operativo	Imagen	Detalles
	Regiones: todas	
Ubuntu	Nombres de las imágenes: <ul style="list-style-type: none"> ● Ubuntu 16.04 server 64bit ● Ubuntu 18.04 server 64bit ● Ubuntu 20.04 server 64bit 	<ul style="list-style-type: none"> ● Actualizada la versión del kernel del sistema operativo para corregir vulnerabilidades de seguridad. ● Actualizado el complemento de restablecimiento de contraseña con un solo clic.
	Versiones de kernel: Ubuntu 16.04: 4.4.0-210-generic Ubuntu 18.04: 4.15.0-167-generic Ubuntu 20.04: 5.4.0-99-generic	
	Regiones: todas	
Debian	Nombres de las imágenes: <ul style="list-style-type: none"> ● Debian 9.0.0 64bit ● Debian 10.0.0 64bit 	<ul style="list-style-type: none"> ● Actualizada la versión del kernel del sistema operativo para corregir vulnerabilidades de seguridad. ● Actualizado el complemento de restablecimiento de contraseña con un solo clic.
	Versiones de kernel: <ul style="list-style-type: none"> ● Debian 9: 4.9.0-17-amd64 ● Debian 10: 4.19.0-18-amd64 	
	Regiones: todas	
EulerOS	Nombre de la imagen: EulerOS 2.5 64bit	<ul style="list-style-type: none"> ● Actualizada la versión del kernel del sistema operativo para corregir vulnerabilidades de seguridad. ● Actualizado el complemento de restablecimiento de contraseña con un solo clic.
	Versión de kernel: EulerOS 2.5: 3.10.0-862.14.1.5.h654.eulerosv2r7.x86_64	
	Regiones: todas	

2021-05-21

Sistema operativo	Imagen	Detalles
CentOS	Nombres de las imágenes: <ul style="list-style-type: none"> ● CentOS 7.2 64bit ● CentOS 7.3 64bit ● CentOS 7.4 64bit ● CentOS 7.5 64bit ● CentOS 7.6 64bit ● CentOS 8.0 64bit ● CentOS 8.1 64bit ● CentOS 8.2 64bit 	<ul style="list-style-type: none"> ● Actualizada la versión del kernel del sistema operativo para corregir vulnerabilidades de seguridad. ● Instalado/actualizado el complemento HSS. ● Actualizado el complemento de restablecimiento de contraseña con un solo clic. ● Optimizada la configuración del origen del repositorio. ● Corregidas vulnerabilidades de sudo.
	Versiones de kernel: <ul style="list-style-type: none"> ● CentOS 7: 3.10.0-1160.15.2.el7.x86_64 ● CentOS 8: 4.18.0-240.10.1.el8_3.x86_64 	
	Regiones: todas	
Ubuntu	Nombres de las imágenes: <ul style="list-style-type: none"> ● Ubuntu 16.04 server 64bit ● Ubuntu 18.04 server 64bit 	<ul style="list-style-type: none"> ● Actualizada la versión del kernel del sistema operativo para corregir vulnerabilidades de seguridad. ● Instalado/actualizado el complemento HSS. ● Actualizado el complemento de restablecimiento de contraseña con un solo clic. ● Optimizada la configuración del origen del repositorio. ● Corregidas vulnerabilidades de sudo.
	Versiones de kernel: Ubuntu 16.04: 4.4.0-201-generic Ubuntu 18.04: 4.15.0-136-generic	
	Regiones: todas	

Sistema operativo	Imagen	Detalles
Debian	Nombres de las imágenes: <ul style="list-style-type: none"> ● Debian 9.0.0 64bit ● Debian 10.0.0 64bit 	<ul style="list-style-type: none"> ● Actualizada la versión del kernel del sistema operativo para corregir vulnerabilidades de seguridad. ● Instalado/actualizado el complemento HSS. ● Actualizado el complemento de restablecimiento de contraseña con un solo clic. ● Optimizada la configuración del origen del repositorio. ● Corregidas vulnerabilidades de sudo.
	Versiones de kernel: <ul style="list-style-type: none"> ● Debian 9: 4.9.0-14-amd64 ● Debian 10: 4.19.0-14-amd64 	
	Regiones: todas	
EulerOS	Nombres de las imágenes: <ul style="list-style-type: none"> ● EulerOS 2.5 64bit ● EulerOS 2.2 64bit 	<ul style="list-style-type: none"> ● Actualizada la versión del kernel del sistema operativo para corregir vulnerabilidades de seguridad. ● Instalado/actualizado el complemento HSS. ● Actualizado el complemento de restablecimiento de contraseña con un solo clic. ● Optimizada la configuración del origen del repositorio. ● Corregidas vulnerabilidades de sudo.
	Versiones de kernel: <ul style="list-style-type: none"> ● EulerOS 2.5: 3.10.0-862.14.1.5.h520 ● EulerOS 2.2: 3.10.0-327.62.59.83.h255 	
	Regiones: todas	

2021-04-28

Sistema operativo	Imagen	Detalles
CentOS	Nombres de las imágenes: <ul style="list-style-type: none"> ● CentOS 7.9 64bit ● CentOS 7.8 64bit ● CentOS 7.7 64bit 	Released the images.
	Versión del kernel: 3.10.0-1160.15.2.el7.x86_64	
	Regiones: todas	

2020-12-25

Sistema operativo	Imagen	Detalles
CentOS	Nombres de las imágenes: <ul style="list-style-type: none"> ● CentOS 8.1 64bit ● CentOS 8.2 64bit 	Las imágenes publicadas.
	Versión del kernel: 4.18.0-240.1.1.el8_3.x86_64	
	Regiones: todas	
CentOS	Nombres de las imágenes: <ul style="list-style-type: none"> ● CentOS 7.2 64bit ● CentOS 7.3 64bit ● CentOS 7.4 64bit ● CentOS 7.5 64bit ● CentOS 7.6 64bit ● CentOS 8.0 64bit 	<ul style="list-style-type: none"> ● Actualizada la versión del kernel del sistema operativo para corregir vulnerabilidades de seguridad. ● Instalado/actualizado el complemento UniAgent. ● Actualizado Cloud-Init a 19.1. ● Configuraciones optimizadas en resolv.conf.
	Versiones de kernel: <ul style="list-style-type: none"> ● CentOS 7: 3.10.0-1160.6.1.el7.x86_64 ● CentOS 8: 4.18.0-240.1.1.el8_3.x86_64 	
	Regiones: todas	
Ubuntu	Nombres de las imágenes: <ul style="list-style-type: none"> ● Ubuntu 16.04 server 64bit ● Ubuntu 18.04 server 64bit ● Ubuntu 20.04 server 64bit 	<ul style="list-style-type: none"> ● Actualizada la versión del kernel del sistema operativo para corregir vulnerabilidades de seguridad. ● Instalado/actualizado el complemento UniAgent. ● Actualizado Cloud-Init a 19.1. ● Configuraciones optimizadas en resolv.conf.
	Versiones de kernel: <ul style="list-style-type: none"> ● Ubuntu 16.04: 4.4.0-197-generic ● Ubuntu 18.04: 4.15.0-128-generic ● Ubuntu 20.04: 5.4.0-58-generic 	
	Regiones: todas	

2020-10-09

Sistema operativo	Imagen	Detalles
Ubuntu	Nombre de la imagen: Ubuntu 20.04 64bit	Imagen publicada.
	Versión del núcleo: 5.4.0-47-generic	
	Regiones: todas	

2020-07-23

Sistema operativo	Imagen	Detalles
Windows Server 2012 R2	Nombres de las imágenes: <ul style="list-style-type: none"> ● Windows Server 2012 R2 Standard ● Windows Server 2012 R2 Datacenter 	<ul style="list-style-type: none"> ● Parches del sistema operativo actualizados. ● Actualizado el complemento HSS. ● Actualizado el complemento de restablecimiento de contraseña con un solo clic. ● Eliminado la tarea de script de inicialización automática de discos.
	Regiones: todas	
Windows Server 2016	Nombres de las imágenes: <ul style="list-style-type: none"> ● Windows Server 2016 Standard ● Windows Server 2016 Datacenter 	
	Regiones: todas	
Windows Server 2019	Nombre de la imagen: Windows Server 2019 Datacenter	
	Regiones: todas	

2020-07-15

Sistema operativo	Imagen	Detalles
Windows Server 2008 R2	Nombres de las imágenes: <ul style="list-style-type: none"> ● Windows Server 2008 R2 Standard ● Windows Server 2008 R2 Datacenter ● Windows Server 2008 R2 Enterprise ● Windows Server 2008 R2 Web 	Tomado las imágenes fuera de línea.
	Regiones: todas	

2020-05-18

Sistema operativo	Imagen	Detalles
openEuler	Nombre de la imagen: openEuler 20.03 64bit	Imagen publicada.
	Versión del Kernel: 4.19.90-2003.4.0.0036.oel.x86_64	
	Regiones: todas	

2020-04-30

Sistema operativo	Imagen	Detalles
CentOS	Nombres de las imágenes: <ul style="list-style-type: none"> ● CentOS 6.5 64bit ● CentOS 6.8 64bit ● CentOS 6.9 64bit ● CentOS 6.10 64bit ● CentOS 7.2 64bit ● CentOS 7.3 64bit ● CentOS 7.4 64bit ● CentOS 7.5 64bit ● CentOS 7.6 64bit 	<ul style="list-style-type: none"> ● Actualizada la versión del kernel del sistema operativo para corregir vulnerabilidades de seguridad. ● Actualizado el complemento de restablecimiento de contraseña con un solo clic. ● Actualizado el complemento HSS. ● Parámetros del kernel optimizados relacionados con los puertos seriales. ● NTP deshabilitado y chrony habilitado.
	Versiones de kernel: <ul style="list-style-type: none"> ● CentOS 6: 2.6.32-754.27.1.el6.x86_64 ● CentOS 7: 3.10.0-1062.12.1.el7.x86_64 	
	Regiones: todas	

2020-04-24

Sistema operativo	Imagen	Detalles
Debian	Nombres de las imágenes: <ul style="list-style-type: none"> ● Debian 9.0.0 64bit ● Debian 10.0.0 64bit 	<ul style="list-style-type: none"> ● Actualizada la versión del kernel del sistema operativo para corregir vulnerabilidades de seguridad. ● Actualizado el complemento de restablecimiento de contraseña con un solo clic. ● Actualizado el complemento HSS. ● Parámetros del kernel optimizados relacionados con los puertos seriales. ● NTP deshabilitado y chrony habilitado.
	Versiones de kernel: <ul style="list-style-type: none"> ● Debian 10: 4.19.0-8-amd64 ● Debian 9: 4.9.0-12-amd64 	
	Regiones: todas	

Sistema operativo	Imagen	Detalles
Ubuntu	Nombres de las imágenes: <ul style="list-style-type: none"> ● Ubuntu 18.04 64bit ● Ubuntu 16.04 64bit 	<ul style="list-style-type: none"> ● Actualizada la versión del kernel del sistema operativo para corregir vulnerabilidades de seguridad. ● Actualizado el complemento de restablecimiento de contraseña con un solo clic. ● Actualizado el complemento HSS. ● Parámetros del kernel optimizados relacionados con los puertos seriales. ● NTP deshabilitado y chrony habilitado.
	Versiones de kernel: <ul style="list-style-type: none"> ● Ubuntu 18: 4.15.0-91-generic ● Ubuntu 16: 4.4.0-176-generic 	
	Regiones: todas	
EulerOS	Nombres de las imágenes: <ul style="list-style-type: none"> ● EulerOS 2.5 64bit ● EulerOS 2.3 64bit ● EulerOS 2.2 64bit 	<ul style="list-style-type: none"> ● Actualizada la versión del kernel del sistema operativo para corregir vulnerabilidades de seguridad. ● Actualizado el complemento de restablecimiento de contraseña con un solo clic. ● Actualizado el complemento HSS. ● Parámetros del kernel optimizados relacionados con los puertos seriales. ● NTP deshabilitado y chrony habilitado.
	Versiones de kernel: <ul style="list-style-type: none"> ● EulerOS 2.2: 3.10.0-327.62.59.83.h195.x86_64 ● EulerOS 2.3: 3.10.0-514.44.5.10.h234.x86_64 ● EulerOS 2.5: 3.10.0-862.14.1.5.h428.euleros v2r7.x86_64 	
	Regiones: todas	

Sistema operativo	Imagen	Detalles
openSUSE	Nombre de la imagen: openSUSE 15.0 64bit	<ul style="list-style-type: none"> ● Actualizada la versión del kernel del sistema operativo para corregir vulnerabilidades de seguridad. ● Actualizado el complemento de restablecimiento de contraseña con un solo clic. ● Actualizado el complemento HSS. ● Parámetros del kernel optimizados relacionados con los puertos seriales. ● NTP deshabilitado y chrony habilitado.
	Versión de kernel: 4.12.14-lp150.12.82-default	
	Regiones: todas	
Fedora	Nombre de la imagen: Fedora 30 64bit	<ul style="list-style-type: none"> ● Actualizada la versión del kernel del sistema operativo para corregir vulnerabilidades de seguridad. ● Actualizado el complemento de restablecimiento de contraseña con un solo clic. ● Actualizado el complemento HSS. ● Parámetros del kernel optimizados relacionados con los puertos seriales. ● NTP deshabilitado y chrony habilitado.
	Versión del kernel: 5.5.10-100.fc30.x86_64	
	Regiones: todas	

2020-03-27

Sistema operativo	Imagen	Detalles
CentOS	Nombre de la imagen: CentOS 8.0 64bit	Imagen publicada.
	Versión del kernel: 4.18.0-147.5.1.el8_1.x86_64	
	Regiones: todas	

2020-03-24

Sistema operativo	Imagen	Detalles
Debian	Nombres de las imágenes: <ul style="list-style-type: none"> ● Debian 8.2.0 64bit ● Debian 8.8.0 64bit 	<ul style="list-style-type: none"> ● Actualizado el complemento de restablecimiento de contraseña con un solo clic. ● Actualizado el complemento HSS. ● Parámetros del kernel optimizados relacionados con los puertos seriales. ● NTP deshabilitado y chrony habilitado.
	Versión del kernel: 3.16.0-4-amd64	
	Regiones: todas	

2020-03-19

Sistema operativo	Imagen	Detalles
Windows Server 2016	Nombres de las imágenes: <ul style="list-style-type: none"> ● Windows Server 2016 Standard ● Windows Server 2016 Datacenter 	<ul style="list-style-type: none"> ● Actualizados UVP VMTools y PV driver. ● Actualizado el complemento de restablecimiento de contraseña con un solo clic. ● Actualizado el complemento HSS. ● Rectificado el error de instalación del dominio AD. ● Parches del sistema operativo actualizados.
	Regiones: todas	
Windows Server 2019	Nombre de la imagen: Windows Server 2019 Datacenter	
	Regiones: todas	

2020-03-17

Sistema operativo	Imagen	Detalles
Windows Server 2012 R2	Nombres de las imágenes: <ul style="list-style-type: none"> ● Windows Server 2012 R2 Standard ● Windows Server 2012 R2 Datacenter 	<ul style="list-style-type: none"> ● Actualizado el complemento de restablecimiento de contraseña con un solo clic. ● Actualizado el complemento HSS. ● Rectificado el error de instalación del dominio AD. ● Parches del sistema operativo actualizados.
	Regiones: todas	

2019-12-13

Sistema operativo	Imagen	Detalles
Windows Server 2012 R2	Nombres de las imágenes: <ul style="list-style-type: none"> ● Windows Server 2012 R2 Standard ● Windows Server 2012 R2 Datacenter 	<ul style="list-style-type: none"> ● Parches del sistema operativo actualizados. ● Actualizado el complemento HSS.
	Regiones: todas	
Windows Server 2016	Nombres de las imágenes: <ul style="list-style-type: none"> ● Windows Server 2016 Standard ● Windows Server 2016 Datacenter 	
	Regiones: todas	
Windows Server 2019	Nombre de la imagen: Windows Server 2019 Datacenter	<ul style="list-style-type: none"> ● Parches del sistema operativo actualizados. ● Actualizado el complemento HSS.
	Regiones: todas	
Windows Server 2008 R2	Nombres de las imágenes: <ul style="list-style-type: none"> ● Windows Server 2008 R2 Standard ● Windows Server 2008 R2 Datacenter ● Windows Server 2008 R2 Enterprise ● Windows Server 2008 Web 	<ul style="list-style-type: none"> ● Parches del sistema operativo actualizados. ● Actualizado el complemento HSS.
	Regiones: todas	

2019-11-06

Sistema operativo	Imagen	Detalles
Debian	Nombres de las imágenes: <ul style="list-style-type: none"> ● Debian 10.0.0 64bit ● Debian 8.8.0 64bit ● Debian 8.2.0 64bit 	<ul style="list-style-type: none"> ● Actualizada la versión del kernel del sistema operativo para corregir vulnerabilidades de seguridad. ● Parámetros de kernel de Debian 10.0.0 optimizados.
	Versiones de kernel: <ul style="list-style-type: none"> ● Debian 10: 4.19.0-6-amd64 ● Debian 8: 3.16.0-10-amd64 	
	Regiones: todas	
Fedora	Nombre de la imagen: Fedora 30 64bit	<ul style="list-style-type: none"> ● Actualizada la versión del kernel del sistema operativo para corregir vulnerabilidades de seguridad. ● Parámetros del kernel optimizados.
	Versión del kernel: 5.3.7-200.fc30.x86_64	
	Regiones: todas	
openSUSE	Nombre de la imagen: openSUSE 15.0 64bit	Actualizada la versión del kernel del sistema operativo para corregir vulnerabilidades de seguridad.
	Versión del kernel: 4.12.14-1p150.12.79-default	
	Regiones: todas	

2019-11-05

Sistema operativo	Imagen	Detalles
CentOS	Nombres de las imágenes: <ul style="list-style-type: none"> ● CentOS 6.5 64bit ● CentOS 6.8 64bit ● CentOS 6.9 64bit ● CentOS 6.10 64bit 	Actualizada la versión del kernel del sistema operativo para corregir vulnerabilidades de seguridad.
	Versión del kernel: 2.6.32-754.23.1.el6.x86_64	
	Regiones: todas	

2019-10-15

Sistema operativo	Imagen	Detalles
Debian	Nombres de las imágenes: <ul style="list-style-type: none"> ● Debian 9.0.0 64bit ● Debian 8.8.0 64bit ● Debian 8.2.0 64bit 	<ul style="list-style-type: none"> ● Actualizados los parches del sistema operativo para corregir las vulnerabilidades de seguridad. ● Actualizada la versión del kernel de Debian 9.0.0. ● Actualizado el complemento de NIC de cola múltiple. ● Parámetros del kernel optimizados.
	Versiones de kernel: <ul style="list-style-type: none"> ● Debian 9: 4.9.0-11-amd64 ● Debian 8: 3.16.0-9-amd64 	
	Regiones: todas	
Fedora	Nombre de la imagen: Fedora 29 64bit	<ul style="list-style-type: none"> ● Actualizada la versión del kernel del sistema operativo para corregir vulnerabilidades de seguridad. ● Actualizado el complemento de NIC de cola múltiple. ● Parámetros del kernel optimizados.
	Versión del kernel: 5.1.11-200.fc29.x86_64	
	Regiones: todas	
openSUSE	Nombre de la imagen: openSUSE 15.0 64bit	<ul style="list-style-type: none"> ● Actualizada la versión del kernel del sistema operativo para corregir vulnerabilidades de seguridad. ● Actualizado el complemento de NIC de cola múltiple. ● Parámetros del kernel optimizados.
	Versión del kernel: 4.12.14-1p150.12.64-default	
	Regiones: todas	
Ubuntu	Nombres de las imágenes: <ul style="list-style-type: none"> ● Ubuntu 18.04 64bit ● Ubuntu 16.04 64bit 	<ul style="list-style-type: none"> ● Actualizada la versión del kernel del sistema operativo para corregir vulnerabilidades de seguridad. ● Actualizado el complemento de NIC de cola múltiple. ● Parámetros del kernel optimizados.
	Versiones de kernel: <ul style="list-style-type: none"> ● Ubuntu 18.04: 4.15.0-65-generic ● Ubuntu 16.04: 4.4.0-165-generic 	
	Regiones: todas	

2019-10-10

Sistema operativo	Imagen	Detalles
CentOS	Nombres de las imágenes: <ul style="list-style-type: none"> ● CentOS 6.5 64bit ● CentOS 6.8 64bit ● CentOS 6.9 64bit ● CentOS 6.10 64bit 	<ul style="list-style-type: none"> ● Actualizados los parches del sistema operativo para corregir las vulnerabilidades de seguridad. ● Actualizado el complemento de NIC de cola múltiple. ● Parámetros del kernel optimizados.
	Versión del kernel: 2.6.32-754.15.3.e16.x86_64	
	Regiones: todas	

2019-09-29

Sistema operativo	Imagen	Detalles
CentOS	Nombres de las imágenes: <ul style="list-style-type: none"> ● CentOS 7.2 64bit ● CentOS 7.3 64bit ● CentOS 7.4 64bit ● CentOS 7.5 64bit ● CentOS 7.6 64bit 	<ul style="list-style-type: none"> ● Actualizada la versión del kernel del sistema operativo para corregir vulnerabilidades de seguridad. ● Actualizado el complemento de NIC de cola múltiple. ● Parámetros del kernel optimizados.
	Versión del kernel: 3.10.0-1062.1.1.e17.x86_64	
	Regiones: todas	

2019-08-29

Sistema operativo	Imagen	Detalles
Debian	Nombres de las imágenes: <ul style="list-style-type: none"> ● Debian 9.0.0 64bit ● Debian 8.8.0 64bit ● Debian 8.2.0 64bit 	<ul style="list-style-type: none"> ● Actualizado el complemento de NIC de cola múltiple. ● Rectificada la fuente apt en el Debian OS.
	Versiones de kernel: <ul style="list-style-type: none"> ● Debian 9: 4.9.0-9-amd64 ● Debian 8: 3.16.0-9-amd64 	

Sistema operativo	Imagen	Detalles
	Regiones: todas	

2019-08-26

Sistema operativo	Imagen	Detalles
Windows Server 2008 R2	Nombres de las imágenes: <ul style="list-style-type: none"> ● Windows Server 2008 R2 Standard ● Windows Server 2008 R2 Datacenter ● Windows Server 2008 R2 Enterprise ● Windows Server 2008 Web 	<ul style="list-style-type: none"> ● Actualizados UVP VMTools y PV driver. ● Parches del sistema operativo actualizados. ● Optimizada la duración del tiempo de espera de Cloudbase-Init.
	Regiones: todas	

2019-08-21

Sistema operativo	Imagen	Detalles
Windows Server 2016	Nombres de las imágenes: <ul style="list-style-type: none"> ● Windows Server 2016 Standard ● Windows Server 2016 Datacenter 	<ul style="list-style-type: none"> ● Actualizados UVP VMTools y PV driver. ● Parches del sistema operativo actualizados.
	Regiones: todas	
Windows Server 2019	Nombre de la imagen: Windows Server 2019 Datacenter	
	Regiones: todas	

2019-08-19

Sistema operativo	Imagen	Detalles
Windows Server 2012 R2	Nombres de las imágenes: <ul style="list-style-type: none"> ● Windows Server 2012 R2 Standard ● Windows Server 2012 R2 Datacenter 	<ul style="list-style-type: none"> ● Actualizados UVP VMTools y PV driver. ● Parches del sistema operativo actualizados.
	Regiones: todas	

2019-06-29

Sistema operativo	Imagen	Detalles
EulerOS	Nombres de las imágenes: <ul style="list-style-type: none"> ● EulerOS 2.2 64bit ● EulerOS 2.3 64bit 	Actualizados los parches del sistema operativo para rectificar la vulnerabilidad SACK del kernel de Linux.
	Versiones de kernel: <ul style="list-style-type: none"> ● EulerOS 2.2: 3.10.0-327.62.59.83.h162.x86_64 ● EulerOS 2.3: 3.10.0-514.44.5.10.h198.x86_64 	
	Regiones: todas	

2019-06-27

Sistema operativo	Imagen	Detalles
Fedora	Nombre de la imagen: Fedora 29 64bit	Actualizados los parches del sistema operativo para rectificar la vulnerabilidad SACK del kernel de Linux.
	Versión del kernel: 5.1.11-200.fc29.x86_64	
	Regiones: todas	
openSUSE	Nombre de la imagen: openSUSE 15.0 64bit	Actualizados los parches del sistema operativo para rectificar la vulnerabilidad SACK del kernel de Linux.

Sistema operativo	Imagen	Detalles
	Versión del kernel: 4.12.14-1p150.12.64-default	
	Regiones: todas	

2019-06-26

Sistema operativo	Imagen	Detalles
CentOS	Nombres de las imágenes: <ul style="list-style-type: none"> ● CentOS 6.5 64bit ● CentOS 6.8 64bit ● CentOS 6.9 64bit ● CentOS 6.10 64bit ● CentOS 7.2 64bit ● CentOS 7.3 64bit ● CentOS 7.4 64bit ● CentOS 7.5 64bit ● CentOS 7.6 64bit 	Actualizados los parches del sistema operativo para rectificar la vulnerabilidad SACK del kernel de Linux.
	Versiones de kernel: <ul style="list-style-type: none"> ● CentOS 6: 2.6.32-754.15.3.e16.x86_64 ● CentOS 7: 3.10.0-957.21.3.e17.x86_64 	
	Regiones: todas	
Ubuntu	Nombres de las imágenes: <ul style="list-style-type: none"> ● Ubuntu 18.04 64bit ● Ubuntu 16.04 64bit 	Actualizados los parches del sistema operativo para rectificar la vulnerabilidad SACK del kernel de Linux.
	Versiones de kernel: <ul style="list-style-type: none"> ● Ubuntu 18.04: 4.15.0-52-generic ● Ubuntu 16.04: 4.4.0-151-generic 	
	Regiones: todas	

Sistema operativo	Imagen	Detalles
Debian	Nombres de las imágenes: <ul style="list-style-type: none"> ● Debian 9.0.0 64bit ● Debian 8.8.0 64bit ● Debian 8.2.0 64bit 	Actualizados los parches del sistema operativo para rectificar la vulnerabilidad SACK del kernel de Linux.
	Versiones de kernel: <ul style="list-style-type: none"> ● Debian 9: 4.9.0-9-amd64 ● Debian 8: 3.16.0-9-amd64 	
	Regiones: todas	

2019-06-23

Sistema operativo	Imagen	Detalles
Windows Server 2012 R2	Nombres de las imágenes: <ul style="list-style-type: none"> ● Windows Server 2012 R2 Standard ● Windows Server 2012 R2 Datacenter 	Parches del sistema operativo actualizados.
	Regiones: todas	
Windows Server 2016	Nombres de las imágenes: <ul style="list-style-type: none"> ● Windows Server 2016 Standard ● Windows Server 2016 Datacenter 	Parches del sistema operativo actualizados.
	Regiones: todas	
Windows Server 2019	Nombre de la imagen: Windows Server 2019 Datacenter	Parches del sistema operativo actualizados.
	Regiones: todas	

2019-06-19

Sistema operativo	Imagen	Detalles
Windows Server 2008 R2	Nombres de las imágenes: <ul style="list-style-type: none"> ● Windows Server 2008 R2 Standard ● Windows Server 2008 R2 Datacenter ● Windows Server 2008 R2 Enterprise ● Windows Server 2008 Web 	Parches del sistema operativo actualizados.
	Regiones: todas	

2019-06-05

Sistema operativo	Imagen	Detalles
CentOS	Nombres de las imágenes: <ul style="list-style-type: none"> ● CentOS 6.5 64bit ● CentOS 6.8 64bit ● CentOS 6.9 64bit ● CentOS 6.10 64bit ● CentOS 7.2 64bit ● CentOS 7.3 64bit ● CentOS 7.4 64bit ● CentOS 7.5 64bit ● CentOS 7.6 64bit 	<ul style="list-style-type: none"> ● Configuración de DNS optimizada. ● Actualizado el complemento de restablecimiento de contraseña con un solo clic. ● Rectificado el desorden del nombre NIC de CentOS 6. ● Desinstalado el paquete de software CentOS 7 qemu-guest-agent.
	Versiones de kernel: <ul style="list-style-type: none"> ● CentOS 6: 2.6.32-754.10.1.e16.x86_64 ● CentOS 7: 3.10.0-957.5.1.e17.x86_64 	
	Regiones: todas	

Sistema operativo	Imagen	Detalles
EulerOS	Nombres de las imágenes: <ul style="list-style-type: none"> ● EulerOS 2.2 64bit ● EulerOS 2.3 64bit 	<ul style="list-style-type: none"> ● Configuración de DNS optimizada. ● Actualizado el complemento de restablecimiento de contraseña con un solo clic. ● Rectificado el problema de que el intercambio en caliente de la NIC de imagen de EulerOS no tiene efecto.
	Versiones de kernel: <ul style="list-style-type: none"> ● EulerOS 2.2: 3.10.0-327.62.59.83.h128.x86_64 ● EulerOS 2.3: 3.10.0-514.44.5.10.h142.x86_64 	
	Regiones: todas	

2019-06-03

Sistema operativo	Imagen	Detalles
Ubuntu	Nombres de las imágenes: <ul style="list-style-type: none"> ● Ubuntu 18.04 64bit ● Ubuntu 16.04 64bit ● Ubuntu 14.04 64bit ● Ubuntu 14.04 32bit 	<ul style="list-style-type: none"> ● Configuración de DNS optimizada. ● Actualizado el complemento de restablecimiento de contraseña con un solo clic. ● Parámetros del kernel optimizados de las imágenes de Ubuntu.
	Versiones de kernel: <ul style="list-style-type: none"> ● Ubuntu 18.04: 4.15.0-45-generic ● Ubuntu 16.04: 4.4.0-142-generic ● Ubuntu 14.04: 4.4.0-141-generic 	
	Regiones: todas	
Debian	Nombres de las imágenes: <ul style="list-style-type: none"> ● Debian 9.0.0 64bit ● Debian 8.8.0 64bit ● Debian 8.2.0 64bit 	<ul style="list-style-type: none"> ● Configuración de DNS optimizada. ● Actualizado el complemento de restablecimiento de contraseña con un solo clic. ● Rectificadas algunas configuraciones inválidas de la fuente apt en Debian 8.
	Versiones de kernel: <ul style="list-style-type: none"> ● Debian 9: 4.9.0-8-amd64 ● Debian 8: 3.16.0-7-amd64 	
	Regiones: todas	

2019-05-24

Sistema operativo	Imagen	Detalles
Windows Server 2012 R2	Nombres de las imágenes: <ul style="list-style-type: none"> ● Windows Server 2012 R2 Standard ● Windows Server 2012 R2 Datacenter 	Rectificado el problema de que la primera copia de respaldo de un ECS es demasiado grande en tamaño.
	Regiones: todas	

2019-05-23

Sistema operativo	Imagen	Detalles
Windows Server 2008 R2	Nombres de las imágenes: <ul style="list-style-type: none"> ● Windows Server 2008 R2 Standard ● Windows Server 2008 R2 Datacenter ● Windows Server 2008 R2 Enterprise ● Windows Server 2008 Web 	Rectificado el problema de que la primera copia de respaldo de un ECS es demasiado grande en tamaño.
	Regiones: todas	

2019-05-22

Sistema operativo	Imagen	Detalles
Windows Server 2016	Nombres de las imágenes: <ul style="list-style-type: none"> ● Windows Server 2016 Standard ● Windows Server 2016 Datacenter 	<ul style="list-style-type: none"> ● Rectificado el problema de que la primera copia de respaldo de un ECS es demasiado grande en tamaño. ● Parches del sistema operativo actualizados.
	Regiones: todas	

2019-05-16

Sistema operativo	Imagen	Detalles
Windows Server 2008 R2	Nombres de las imágenes: <ul style="list-style-type: none"> ● Windows Server 2008 R2 Standard ● Windows Server 2008 R2 Datacenter ● Windows Server 2008 R2 Enterprise ● Windows Server 2008 Web 	<ul style="list-style-type: none"> ● Parches del sistema operativo actualizados. ● Rectificada la vulnerabilidad de ejecución remota de código (CVE-2019-0708) del servicio de escritorio remoto de Windows.
	Regiones: todas	

2019-04-25

Sistema operativo	Imagen	Detalles
Windows Server 2019	Nombres de las imágenes: <ul style="list-style-type: none"> ● Windows Server 2019 Standard ● Windows Server 2019 Datacenter 	Las imágenes publicadas.
	Regiones: todas	

2019-04-19

Sistema operativo	Imagen	Detalles
Windows Server 2008 R2	Nombres de las imágenes: <ul style="list-style-type: none"> ● Windows Server 2008 R2 Standard ● Windows Server 2008 R2 Datacenter ● Windows Server 2008 R2 Enterprise ● Windows Server 2008 Web 	<ul style="list-style-type: none"> ● Parches del sistema operativo actualizados. ● Actualizado el controlador UVP VMTools para permitir la expansión de la capacidad en línea.
	Regiones: todas	

Sistema operativo	Imagen	Detalles
Windows Server 2012 R2	Nombres de las imágenes: <ul style="list-style-type: none"> ● Windows Server 2012 R2 Standard ● Windows Server 2012 R2 Datacenter 	<ul style="list-style-type: none"> ● Parches del sistema operativo actualizados. ● Actualizado el controlador UVP VMTools para permitir la expansión de la capacidad en línea.
	Regiones: todas	
Windows Server 2016	Nombres de las imágenes: <ul style="list-style-type: none"> ● Windows Server 2016 Standard ● Windows Server 2016 Datacenter 	<ul style="list-style-type: none"> ● Parches del sistema operativo actualizados. ● Actualizado el controlador UVP VMTools para permitir la expansión de la capacidad en línea.
	Regiones: todas	

1.3 Historial de actualizaciones de imagen (Arm)

En esta sección se describe el historial de actualizaciones de imágenes públicas (Arm).

2023-06-15

Sistema operativo	Imagen	Detalles
Huawei Cloud EulerOS 2.0	Nombre de la imagen: Huawei Cloud EulerOS 2.0 Standard 64 bit	<ul style="list-style-type: none"> ● Actualizada la versión del kernel del sistema operativo para corregir vulnerabilidades de seguridad. ● Actualizada la versión del complemento de contraseña con un solo clic.
	Versión del kernel: 5.10.0-60.18.0.50.r865_35.hce2.aarch64	
	Regiones: todas	
Huawei Cloud EulerOS 2.0	Nombre de la imagen: Huawei Cloud EulerOS 2.0 Level 3 of MLPS 2.0 64 bit	<ul style="list-style-type: none"> ● Actualizada la versión del kernel del sistema operativo para corregir vulnerabilidades de seguridad. ● Actualizada la versión del complemento de contraseña con un solo clic.
	Versión del kernel: 5.10.0-60.18.0.50.r865_35.hce2.aarch64	
	Regiones: todas	

Sistema operativo	Imagen	Detalles
EulerOS	Nombre de la imagen: EulerOS 2.8 64bit with ARM	<ul style="list-style-type: none"> ● Actualizada la versión del kernel del sistema operativo para corregir vulnerabilidades de seguridad. ● Actualizada la versión del complemento de contraseña con un solo clic.
	Versión del kernel: 4.19.36-vhulk1907.1.0.h1393.eulerosv2r8.aarch64	
	Regiones: CN-Hong Kong y AP-Bangkok	

2022-09-30

Sistema operativo	Imagen	Detalles
Huawei Cloud EulerOS 2.0	Nombre de la imagen: Huawei Cloud EulerOS 2.0 Standard 64 bit	Imagen publicada.
	Versión del kernel: 5.10.0-60.18.0.50.h322_1.hce2.aarch64	
	Región: AP-Singapore	

2021-05-24

Sistema operativo	Imagen	Detalles
EulerOS	Nombre de la imagen: EulerOS 2.8 64bit with ARM	<ul style="list-style-type: none"> ● Actualizada la versión del kernel del sistema operativo para corregir vulnerabilidades de seguridad. ● Actualizado el complemento de restablecimiento de contraseña con un solo clic. ● Actualizado el complemento HSS. ● Configurado el origen de repo predeterminado. ● Deshabilitado el dnf-makecache.timer service.
	Versión de kernel: 4.19.36-vhulk1907.1.0.h748.eulerosv2r8.aarch64	
	Regiones: CN-Hong Kong, AP-Singapore, AP-Bangkok, CN South-Guangzhou, CN South-Shenzhen, CN East-Shanghai1, CN East-Shanghai2, CN North-Ulanqab1, CN North-Beijing4, y LA-Sao Paulo1	

2021-04-01

Sistema operativo	Imagen	Detalles
CentOS	Nombres de las imágenes: <ul style="list-style-type: none"> ● CentOS 8.0 64bit with ARM ● CentOS 7.6 64bit with ARM ● CentOS 7.5 64bit with ARM ● CentOS 7.4 64bit with ARM 	<ul style="list-style-type: none"> ● Configuraciones optimizadas en resolv.conf. ● Instalado el complemento HSS. ● Actualizado el complemento de restablecimiento de contraseña con un solo clic. ● Optimizada la configuración del origen del repo. ● Corregidas vulnerabilidades de sudo.
	Versiones de kernel: <ul style="list-style-type: none"> ● CentOS 8: 4.18.0-147.5.1.el8_1.aarch64 ● CentOS 7: 4.18.0-80.7.2.el7.aarch64 	
	Regiones: CN-Hong Kong, AP-Singapore, AP-Bangkok, CN South-Guangzhou, CN South-Shenzhen, CN East-Shanghai1, CN East-Shanghai2, CN North-Ulanqab1, y CN North-Beijing4	
Ubuntu	Nombre de la imagen: Ubuntu 18.04 64bit with ARM	<ul style="list-style-type: none"> ● Configuraciones optimizadas en resolv.conf. ● Instalado el complemento HSS. ● Actualizado el complemento de restablecimiento de contraseña con un solo clic. ● Optimizada la configuración del origen del repo. ● Corregidas vulnerabilidades de sudo.
	Versión del kernel: 4.15.0-70-generic	
	Regiones: CN-Hong Kong, AP-Singapore, AP-Bangkok, CN South-Guangzhou, CN South-Shenzhen, CN East-Shanghai1, CN East-Shanghai2, CN North-Ulanqab1, y CN North-Beijing4	
OpenEuler	Nombre de la imagen: openEuler 20.03 64bit with ARM	<ul style="list-style-type: none"> ● Configuraciones optimizadas en resolv.conf. ● Instalado el complemento HSS. ● Actualizado el complemento de restablecimiento de contraseña con un solo clic. ● Optimizada la configuración del origen del repo. ● Corregidas vulnerabilidades de sudo.
	Versión del kernel: 4.19.90-2003.4.0.0036.oel.aarch64	
	Regiones: CN-Hong Kong, AP-Singapore, AP-Bangkok, CN South-Guangzhou, CN South-Shenzhen, CN East-Shanghai1, CN East-Shanghai2, CN North-Ulanqab1, y CN North-Beijing4	

2020-07-07

Sistema operativo	Imagen	Detalles
EulerOS	Nombre de la imagen: EulerOS 2.8 64bit with ARM	<ul style="list-style-type: none"> ● Actualizada la versión del kernel del sistema operativo para corregir vulnerabilidades de seguridad. ● Actualizado el complemento de restablecimiento de contraseña con un solo clic. ● Actualizado el complemento HSS. ● Configurado el origen de repo predeterminado. ● Deshabilitado el dnf-makecache.timer service.
	Versión de kernel: 4.19.36-vhulk1907.1.0.h748.eulerosv2r8.a arch64	
	Regiones: CN-Hong Kong, AP-Singapore, AP-Bangkok, CN South-Guangzhou, CN South-Shenzhen, CN East-Shanghai1, CN East-Shanghai2, CN North-Ulanqab1, y CN North-Beijing4	

2020-05-18

Sistema operativo	Imagen	Detalles
openEuler	Nombre de la imagen: openEuler 20.03 64bit with ARM	Imagen publicada.
	Versión del kernel: 4.19.90-2003.4.0.0036.oel.aarch64	
	Regiones: CN-Hong Kong, AP-Singapore, AP-Bangkok, CN South-Guangzhou, CN South-Shenzhen, CN East-Shanghai1, CN East-Shanghai2, CN North-Ulanqab1, y CN North-Beijing4	

2020-03-12

Sistema operativo	Imagen	Detalles
CentOS	Nombre de la imagen: CentOS 8.0 64bit with ARM	Imagen publicada.
	Versión de kernel: 4.18.0-147.5.1.el8_1.aarch64	

Sistema operativo	Imagen	Detalles
	Regiones: CN-Hong Kong, AP-Singapore, AP-Bangkok, CN South-Guangzhou, CN South-Shenzhen, CN East-Shanghai1, CN East-Shanghai2, CN North-Ulanqab1, y CN North-Beijing4	
Debian	Nombre de la imagen: Debian 10.2.0 64bit with ARM	Imagen publicada.
	Versión del kernel: 4.19.0-8-arm64	
	Regiones: CN-Hong Kong, AP-Singapore, AP-Bangkok, CN South-Guangzhou, CN South-Shenzhen, CN East-Shanghai1, CN East-Shanghai2, CN North-Ulanqab1, y CN North-Beijing4	

2020-01-03

Sistema operativo	Imagen	Detalles
CentOS	Nombres de las imágenes: <ul style="list-style-type: none"> ● CentOS 7.6 64bit with ARM ● CentOS 7.5 64bit with ARM ● CentOS 7.4 64bit with ARM 	<ul style="list-style-type: none"> ● Actualizada NIC de cola múltiple. ● Parámetros del kernel optimizados. ● Establecida la duración del protector de pantalla en 10 segundos. ● Actualizada la versión del kernel del sistema operativo para corregir vulnerabilidades de seguridad. ● Instalados gdisk, wget y javac. ● Habilitado el servicio chrony y deshabilitado el servicio NTP. ● Configurados cuatro archivos de configuración de NIC para CentOS 7.6 64bit con ARM.
	Versión de kernel: 4.18.0-80.7.2.el7.aarch64	
	Regiones: CN-Hong Kong, AP-Singapore, AP-Bangkok, CN South-Guangzhou, CN South-Shenzhen, CN East-Shanghai1, CN East-Shanghai2, CN North-Ulanqab1, y CN North-Beijing4	

Sistema operativo	Imagen	Detalles
Ubuntu	Nombre de la imagen: Ubuntu 18.04 64bit with ARM	<ul style="list-style-type: none"> ● Actualizada NIC de cola múltiple. ● Parámetros del kernel optimizados. ● Actualizada la versión del kernel del sistema operativo para corregir vulnerabilidades de seguridad. ● Habilitado el servicio chrony y deshabilitado el servicio NTP. ● DNS configurado.
	Versión del kernel: 4.15.0-70-generic	
	Regiones: CN-Hong Kong, AP-Singapore, AP-Bangkok, CN South-Guangzhou, CN South-Shenzhen, CN East-Shanghai1, CN East-Shanghai2, CN North-Ulanqab1, y CN North-Beijing4	
EulerOS	Nombre de la imagen: EulerOS 2.8 64bit with ARM	<ul style="list-style-type: none"> ● Actualizada NIC de cola múltiple. ● Parámetros del kernel optimizados. ● Establecida la duración del protector de pantalla en 10 segundos. ● Agregados parámetros de kernel para que los registros relacionados se puedan ver durante el inicio de ECS. ● Actualizada la versión del kernel del sistema operativo para corregir vulnerabilidades de seguridad. ● Habilitado el servicio chrony y deshabilitado el servicio NTP. ● Establecido el período de validez de la contraseña en 99999.
	Versión de kernel: 4.19.36-vhulk1907.1.0.h475.eulerosv2r8.a arch64	
	Regiones: CN-Hong Kong, AP-Singapore, AP-Bangkok, CN South-Guangzhou, CN South-Shenzhen, CN East-Shanghai1, CN East-Shanghai2, CN North-Ulanqab1, y CN North-Beijing4	

Sistema operativo	Imagen	Detalles
openSUSE	Nombre de la imagen: openSUSE 15.0 64bit with ARM	<ul style="list-style-type: none"> ● Actualizada NIC de cola múltiple. ● Parámetros del kernel optimizados. ● Establecida la duración del protector de pantalla en 10 segundos. ● Actualizada la versión del kernel del sistema operativo para corregir vulnerabilidades de seguridad. ● Habilitado el servicio chrony y deshabilitado el servicio NTP.
	Versión de kernel: 4.12.14-lp150.12.67-predeterminado	
	Regiones: CN-Hong Kong, AP-Singapore, AP-Bangkok, CN South-Guangzhou, CN South-Shenzhen, CN East-Shanghai1, CN East-Shanghai2, CN North-Ulanqab1, y CN North-Beijing4	
Fedora	Nombre de la imagen: Fedora 29 64bit with ARM	<ul style="list-style-type: none"> ● Actualizada NIC de cola múltiple. ● Parámetros del kernel optimizados. ● Establecida la duración del protector de pantalla en 10 segundos. ● Actualizada la versión del kernel del sistema operativo para corregir vulnerabilidades de seguridad. ● Habilitado el servicio chrony y deshabilitado el servicio NTP. ● Configuradas variables de entorno para mostrar el tiempo de ejecución y el nombre del operador de cada comando histórico.
	Versión del kernel: 4.18.16-300.fc29.aarch64	
	Regiones: CN-Hong Kong, AP-Singapore, AP-Bangkok, CN South-Guangzhou, CN South-Shenzhen, CN East-Shanghai1, CN East-Shanghai2, CN North-Ulanqab1, y CN North-Beijing4	

1.4 Problemas conocidos

Esta sección describe problemas conocidos de imágenes públicas en diferentes plataformas. Las imágenes privadas también tienen estos problemas.

Desconexión de red causada por un arrendamiento DHCP de Windows Server de más de 99 días

Síntoma:

Si la concesión DHCP es superior a 99 días, las direcciones IP de instancia no se pueden renovar automáticamente. Como resultado, la red de instancia se desconectará cuando la concesión llegue a su fin. Es un problema conocido del servicio cliente DHCP de Windows Server 2008.

Imágenes involucradas:

Imágenes públicas y privadas de Windows Server 2008, Windows Server 2012 R2, Windows Server 2016 y Windows Server 2019

Solución:

1. Cambie la concesión DHCP de la subred donde se encuentra la instancia a un día o ilimitada.
2. Ejecute el siguiente comando para hacer que el cambio surta efecto:

NOTA

El siguiente comando le desconectará temporalmente de la red. Hágalo durante las horas no pico.

ipconfig /renew

Errores ocasionales del sistema desencadenados al agregar o eliminar NIC

Síntoma:

Después de iniciar un ECS, agregar o eliminar una NIC u otras acciones equivalentes puede:

- Activa un pánico del kernel y el sistema operativo se reinicia automáticamente.
- Activar interrupciones frecuentes de software, y la red puede no recibir o enviar paquetes.

Enlace de parche: <https://git.kernel.org/pub/scm/linux/kernel/git/stable/linux-stable.git/commit/?id=f00e35e259948b995aa1f3ee7fddb05f34a50157>

Imágenes involucradas:

Imágenes públicas y privadas de CentOS 7

Solución:

Actualice el kernel a una versión que coincida con el kernel 3.10.0-1160.25.1.el7.x86_64 de CentOS 7.

Los núcleos se desconectan ocasionalmente de la red TCP

Síntoma:

Este problema se debe a la vulnerabilidad del kernel CVE-2019-11477 (TCP SACK). Cuando la memoria intermedia de socket está baja, la red puede desconectarse.

Las imágenes involucradas se enumeran en la siguiente tabla.

Tipo de imagen	Versión del núcleo
CentOS 7 imágenes públicas del 26/06/2019 al 29/09/2019	3.10.0-957.21.3.e17.x86_64
Ubuntu 16 y Ubuntu 18 imágenes públicas de 2019-06-26 a 2019-10-15	Ubuntu 16.04: 4.4.0-151-generic Ubuntu 18.04: 4.15.0-52-generic
Imágenes públicas de Debian 9.0 del 26/06/2019 al 15-10/2019	4.9.0-9-amd64
Imágenes públicas de Fedora 29 y openSUSE 15.0 del 27/06/2019 al 15-10/2019	Fedora 29: 5.1.11-200.fc29.x86_64 openSUSE 15.0: 4.12.14-1p150.12.64-predeterminado

Solución:

Actualice el núcleo a la última versión. Ejecute los siguientes comandos para actualizar el núcleo de cada tipo de imagen:

- CentOS/Fedora: **yum update kernel**
- Ubuntu: **apt-get update && apt-get install linux-image-generic**
- openSUSE: **zypper refresh && zypper install kernel-default**
- Debian: **apt-get update && apt search linux-image && apt-get install linux-image-xxx**

NOTA

Puede ejecutar el comando **apt search linux-image** para consultar la última versión del núcleo. El comando **apt-get install linux-image-xxx** se utiliza para actualizar un núcleo a la última versión.

La configuración del parámetro del sistema operativo no tiene efecto

Síntoma:

Después de configurar **net.ipv4.tcp_max_tw_buckets** en el archivo **/etc/sysctl.conf**, el resultado de la comprobación de **sysctl -a** indica que la configuración no tiene efecto. Las configuraciones en **/etc/sysctl.d/huawei.conf** y **/etc/security/limits.d/huawei-nofile.conf** se han construido en imágenes públicas y estas configuraciones tienen prioridades más altas que las de **/etc/sysctl.conf**. Como resultado, las configuraciones en **/etc/sysctl.conf** no tienen efecto.

Los parámetros implicados se enumeran en la siguiente tabla.

Parámetro	Archivo de configuración
vm.swappiness net.core.somaxconn net.ipv4.tcp_max_tw_buckets net.ipv4.tcp_max_syn_backlog	/etc/sysctl.d/huawei.conf

Parámetro	Archivo de configuración
* soft nofile 65535 * hard nofile 65535	/etc/security/limits.d/huawei-nofile.conf

Imágenes involucradas:

- Imágenes públicas de CentOS 7 del 25-09-2018 al 29-09-2019
- Imágenes públicas de CentOS 6 desde 2018-09-25 hasta 2019-10-10
- Imágenes públicas de Ubuntu, openSUSE 15.0, Debian y Fedora 29 del 28-09-2018 al 15-10-2019

Solución:

1. Elimine los archivos de configuración integrados.
rm -rf /etc/sysctl.d/huawei.conf
rm -rf /etc/security/limits.d/huawei-nofile.conf
2. Modifique los archivos de configuración de parámetros del núcleo (**limits.conf** y **sysctl.conf**).

```
cat >>/etc/security/limits.conf <<EOF
```

```
root soft nofile 65535
```

```
root hard nofile 65535
```

```
* soft nofile 65535
```

```
* hard nofile 65535
```

```
EOF
```

```
cat >>/etc/sysctl.conf <<EOF
```

```
vm.swappiness=0
```

```
net.core.somaxconn=1024
```

```
net.ipv4.tcp_max_tw_buckets=5000
```

```
net.ipv4.tcp_max_syn_backlog=1024
```

```
EOF
```

La instancia de descarga basada en NIC 1822 es incompatible con el kernel de Linux 3.16.x

Síntoma:

Los ECS que utilizan la función de descarga de hardware proporcionada por la NIC inteligente de alta velocidad de 25GE desarrollada por Huawei pueden ser incompatibles con los sistemas operativos Linux 3.16.47-3.16.x, lo que puede causar desconexiones ocasionales de red de los ECS. Los ECS que tienen este problema incluyen pero no se limitan a C3ne, M3ne, C6, M6, G5, P2v, G5r, P2vs, P2s, Pi2, FP1cn1, Ai1, e3.26xlarge.14, e3.52xlarge.14, e3.52xlarge.20, KC1 y KM1.

Imágenes involucradas:

Imágenes públicas de Debian 8.2.0 64bit y Debian 8.8.0

Solución:

Elimine las imágenes públicas de Debian 8 de las normas. Migre los servicios de los ECS utilizando esta función de descarga a los ECS S3 y C3 tan pronto como sea posible.

Los datos se pierden durante el restablecimiento del disco debido a la incompatibilidad entre el administrador del servidor de Windows Server 2012 R2 y VMTools

Síntoma:

Un ECS de Windows Server 2012 R2 se configura con dos discos de datos. Cuando Windows Server Manager restablece el segundo disco de datos, se restablece el primer disco de datos. Como resultado, se pierden los datos del primer disco de datos.

Imágenes involucradas:

Imagen pública de Windows Server 2012 R2 antes de 2019-02-19

Solución:

Actualice VMTools de ECS involucrados a 2.5.0.156 o posterior.

Interrupciones de servicio causadas por conexiones persistentes CLOSE_WAIT

Síntoma:

Algunos servicios se interrumpen porque un socket en una conexión TCP creado por el proceso del plug-in de restablecimiento de contraseña de un solo clic permanece en el estado **CLOSE_WAIT**.

Imágenes involucradas:

- Imágenes públicas de CentOS y EulerOS emitidas antes del 5 de junio de 2019
- Imágenes públicas de Ubuntu y Debian publicadas antes del 3 de junio de 2019

Solución:

Actualice los complementos de restablecimiento de contraseña con un solo clic para los ECS.

2 Crear una imagen privada

2.1 Introducción

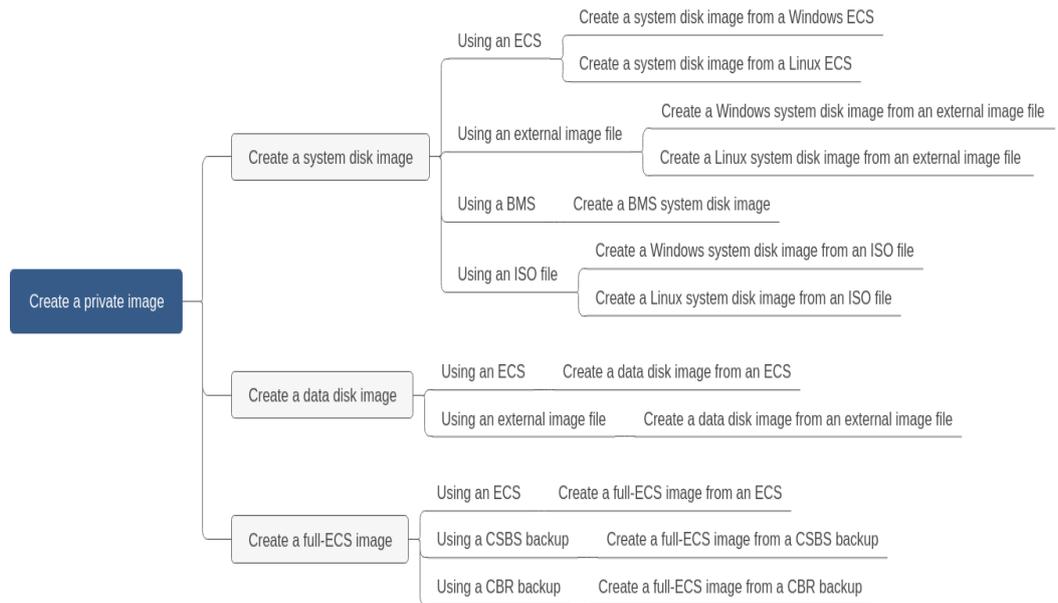
Una imagen privada es una imagen disponible solo para el usuario que la creó. Contiene un sistema operativo, aplicaciones públicas preinstaladas y las aplicaciones personales de un usuario. Una imagen privada puede ser una imagen de disco del sistema, una imagen de disco de datos o una imagen completa de ECS. Se puede crear desde un servidor en la nube o desde un archivo de imagen externo.

La creación de una imagen privada no afecta a la ejecución de los servicios en el servidor en la nube ni provoca la pérdida de datos.

En esta sección se describe cómo crear una imagen privada utilizando cualquiera de los métodos siguientes:

- **Creación de una imagen de disco del sistema desde un ECS de Windows**
- **Creación de una imagen de disco del sistema desde un ECS de Linux**
- **Creación de una imagen de disco del sistema Windows a partir de un archivo de imagen externo**
- **Creación de una imagen de disco de sistema Linux a partir de un archivo de imagen externo**
- **Creación de una imagen de disco de datos a partir de un ECS**
- **Creación de una imagen de disco de datos a partir de un archivo de imagen externo**
- **Creación de una imagen de ECS completo a partir de un ECS**
- **Creación de una imagen completa de ECS a partir de una copia de respaldo de CSBS**
- **Creación de una imagen completa de ECS a partir de una copia de respaldo de CBR**
- **Creación de una imagen de disco de sistema Windows a partir de un archivo ISO**
- **Creación de una imagen de disco de sistema Linux a partir de un archivo ISO**

Figura 2-1 Creación de una imagen privada



Después de crear una imagen de disco del sistema, puede utilizarla para **crear un ECS** o **cambiar el SO** de un ECS.

2.2 Creación de una imagen de disco del sistema desde un ECS de Windows

Escenarios

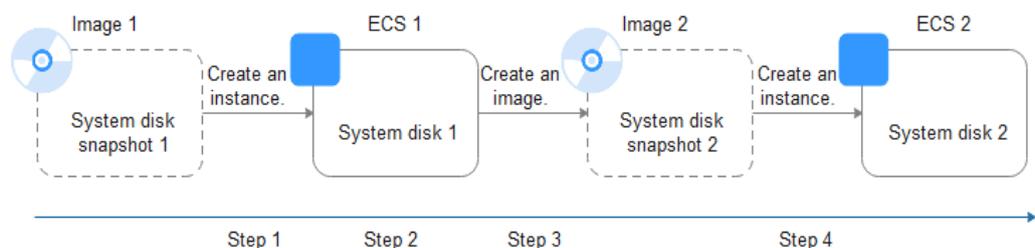
Si ha creado y configurado un Windows ECS basado en sus requisitos de servicio (por ejemplo, instalando software y configurando un entorno de aplicación), puede crear una imagen de disco del sistema basada en esta configurada ECS. Entonces, todos los nuevos ECSs creados a partir de esta imagen tendrán el mismo software y entorno preinstalados.

La creación de una imagen de disco del sistema no afecta a la ejecución de los servicios en el ECS ni provoca la pérdida de datos.

Fondo

La siguiente figura muestra el proceso de crear una imagen de disco de sistema a partir de un ECS.

Figura 2-2 Creación de una imagen de disco del sistema y uso de ella para crear ECS



- Las imágenes de disco del sistema se utilizan a menudo para el escalamiento horizontal de la aplicación. También se pueden utilizar para la implementación de la nube híbrida. Puede crear imágenes de disco del sistema para la sincronización de recursos dentro y fuera de la nube. Siga el siguiente procedimiento:

- a. Cree una imagen de disco del sistema a partir de un ECS.

NOTA

El ECS debe crearse a partir de una imagen privada. Si se crea a partir de una imagen pública, la imagen de disco del sistema no se puede exportar.

- b. Exporte la imagen a un bucket OBS. Para más detalles, consulte [Exportación de una imagen](#).
 - c. Descargue el archivo de imagen desde el bucket OBS.
- Puede crear una imagen a partir de un ECS en ejecución.
La creación de la imagen no afecta al servicio que se ejecuta en el ECS.
En este proceso, no detenga, inicie o reinicie el ECS, o la creación de la imagen puede fallar.
 - El tiempo necesario para crear una imagen depende del tamaño del disco del sistema ECS, la calidad de la red y el número de tareas simultáneas.
 - Se creará una imagen de disco del sistema en la misma región que el ECS que se usó para crearla. Por ejemplo, si un ECS está ubicado en la región CN-Hong Kong, la imagen de disco del sistema creada a partir de ese ECS también estará ubicada en la región CN-Hong Kong. Si desea utilizar la imagen en otra región, primero debe replicarla en esa región. Para más detalles, consulte [Replicación de imágenes entre regiones](#).
 - Si un ECS ha caducado o se ha publicado, puede utilizar la imagen de disco del sistema creada a partir del ECS para restaurarlo.

Prerrequisitos

Antes de crear una imagen privada a partir de un ECS:

- Eliminar cualquier dato sensible ECS que pueda contener.
- Asegúrese de que el ECS está en el estado **Running** o **Stopped**.
- Compruebe la configuración de la red ECS y asegúrese de que DHCP está configurado para las NIC. Habilite la conexión a escritorio remoto si es necesario. Para obtener más información, consulte [Configuración de la NIC en DHCP](#) y [Habilitación de la conexión a Escritorio remoto](#).
- Compruebe si el complemento de restablecimiento de contraseña con un solo clic se ha instalado en el ECS. La función de restablecimiento de contraseña en la consola de gestión solo está disponible para los nuevos ECSs que tienen este plug-in instalado. Para obtener más información, consulte [Instalación del complemento de restablecimiento de contraseñas con un solo clic](#).
- Compruebe si Cloudbase-Init se ha instalado en el ECS. La función de inyección de datos de usuario en la consola de gestión solo está disponible para nuevos ECSs que tienen esta herramienta instalada. Puede utilizar la inyección de datos, por ejemplo, para establecer la contraseña de inicio de sesión para una nueva ECS. For details, see [Instalación y configuración de Cloudbase-Init](#).

- Compruebe e instale el controlador PV y el controlador UVP VMTools para asegurarse de que los nuevos ECSs creados a partir de la imagen admiten la virtualización KVM y XEN y para mejorar el rendimiento de la red.
Para obtener más información, consulte los pasos **2a 5** en **Proceso de optimización**.
- Ejecute Sysprep para asegurarse de que los SID de los nuevos ECSs creados a partir de la imagen sean únicos dentro de su dominio. En un escenario de implementación de clúster, los SID deben ser únicos. Para obtener más información, consulte **Ejecución de Sysprep**.
- Asegúrese de que la capacidad de disco del sistema ECS utilizada para crear una imagen de disco del sistema no debe ser superior a 1 TB.
Si la capacidad es superior a 1 TB, solo puede utilizarla para crear una imagen ECS completa.

 **NOTA**

Si un ECS se crea a partir de una imagen pública, el complemento de restablecimiento de contraseña con un solo clic y Cloudbase-Init se han instalado de forma predeterminada. Puede seguir la guía en los requisitos previos para verificar la instalación.

Procedimiento

Paso 1 Acceda a la consola IMS.

1. Inicie sesión en la consola de gestión.
2. En **Compute**, haga clic en **Image Management Service**.
Se muestra la consola IMS.

Paso 2 Crear una imagen de disco del sistema.

1. Haga clic en **Create Image** en la esquina superior derecha.
2. Establezca parámetros de imagen.

Tabla 2-1 y **Tabla 2-2** enumera los parámetros en las áreas **Image Type and Source** e **Image Information**, respectivamente.

Tabla 2-1 Tipo y fuente de imagen

Parámetro	Descripción
Región	Seleccione una región cercana a donde se proporcionarán sus servicios. Si selecciona una región incorrecta aquí, puede replicar la imagen creada en la región deseada más adelante. Para obtener más información, consulte Replicación de una imagen entre regiones .
Tipo	Seleccione System disk image .
Fuente	Seleccione ECS y seleccione un ECS con las configuraciones requeridas.

Tabla 2-2 Información de imágenes.

Parámetro	Descripción
Cifrado	Este parámetro especifica si la imagen se cifrará. El valor es proporcionado por el sistema y no se puede cambiar. <ul style="list-style-type: none"> – Solo se puede crear una imagen privada no cifrada a partir de una imagen no cifrada ECS. – Solo se puede crear una imagen privada cifrada a partir de una imagen cifrada ECS.
Nombre	Establezca un nombre para la imagen.
Proyecto empresarial	Seleccione un proyecto de empresa en la lista desplegable. Este parámetro sólo está disponible si ha habilitado proyectos de empresa o si su cuenta es una cuenta de empresa. Para habilitar esta función, póngase en contacto con su gestor de clientes. Un proyecto empresarial proporciona una gestión central de los recursos de la nube en función de cada proyecto.
Etiqueta	(Opcional) Establezca una clave de etiqueta y un valor de etiqueta para la imagen para facilitar la identificación y gestión de sus imágenes.
Descripción	(Opcional) Introduzca una descripción de la imagen.

3. Haga clic en **Next**.
4. Confirme los parámetros. Lea el descargo de responsabilidad de la imagen y seleccione **I have read and agree to the Image Disclaimer**, y haga clic en **Submit**.

Paso 3 Vuelva a la página **Private Images** y vea la nueva imagen de disco del sistema.

El tiempo necesario para crear una imagen depende del ECS tamaño del disco del sistema, la calidad de la red y el número de tareas simultáneas. Cuando el estado de la imagen cambia a **Normal**, la creación de la imagen se completa.

 **NOTA**

- No realice ninguna operación en los recursos seleccionados ECS o asociados durante la creación de imágenes.
- Un ECS creado a partir de una imagen encriptada también se cifra. La clave utilizada para cifrar el ECS es la misma que la utilizada para cifrar la imagen.
- También se cifrarán las imágenes creadas a partir de un ECS cifrado. La clave utilizada para cifrar la imagen es la misma que la utilizada para cifrar el ECS.

---Fin

Procedimiento posterior

Después de crear una imagen de disco del sistema, puede utilizar cualquiera de los métodos siguientes para migrar datos entre dos servidores:

- Utilice la imagen para crear nuevos ECS. Para más detalles, consulte [Creación de un ECS a partir de una imagen](#).

- Utilice la imagen para cambiar los sistemas operativos de los ECS existentes. Para obtener más información, consulte [Cambiar el sistema operativo](#).

2.3 Creación de una imagen de disco del sistema desde un ECS de Linux

Escenarios

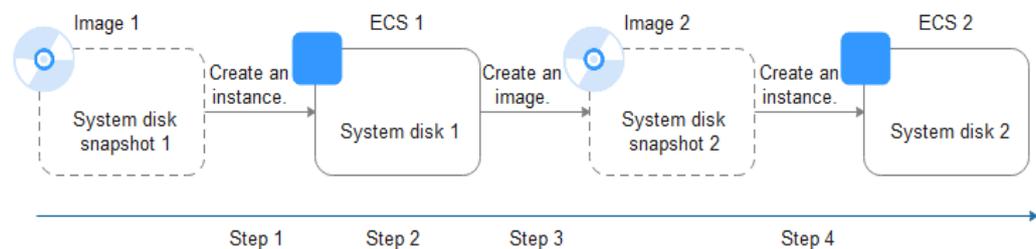
Si ha creado y configurado un ECS de Linux basado en sus requisitos de servicio (por ejemplo, instalación de software y configuración de un entorno de aplicación), puede crear una imagen de disco del sistema basada en ECS configurado. Entonces, todos los nuevos ECSs creados a partir de esta imagen tendrán el mismo software y entorno preinstalados.

La creación de una imagen de disco del sistema no afecta a la ejecución de los servicios en el ECS ni provoca la pérdida de datos.

Antecedentes

La siguiente figura muestra el proceso de crear una imagen de disco de sistema a partir de un ECS.

Figura 2-3 Creación de una imagen de disco del sistema y uso de ella para crear ECS



- Las imágenes de disco del sistema se utilizan a menudo para el escalamiento horizontal de la aplicación. También se pueden utilizar para el despliegue de la nube híbrida. Puede crear imágenes de disco del sistema para la sincronización de recursos dentro y fuera de la nube. El procedimiento es el siguiente:
 - a. Crear una imagen de disco del sistema a partir de un ECS.

NOTA

Si el ECS se crea a partir de cualquiera de las siguientes imágenes, la imagen de disco del sistema no se puede exportar:

- Imagen ISO
 - Imagen privada creada a partir de una imagen pública de SUSE, Red Hat, Ubuntu u Oracle Linux
 - Imagen privada creada a partir de una imagen de Marketplace
- b. Exportar la imagen a un bucket de OBS. Para obtener más información, véase [Exportación de una imagen](#).
 - c. Descargar el archivo de imagen desde el bucket de OBS.
- Puede crear una imagen a partir de un ECS en ejecución.

La creación de la imagen no afecta al servicio que se ejecuta en el ECS.

En este proceso, no detenga, inicie o reinicie el ECS, o la creación de la imagen puede fallar.

- El tiempo necesario para crear una imagen depende del tamaño del disco del sistema ECS, la calidad de la red y el número de tareas simultáneas.
- Se creará una imagen de disco del sistema en la misma región que el ECS que se usó para crearla. Por ejemplo, si un ECS está ubicado en la región CN-Hong Kong, la imagen de disco del sistema creada a partir de ese ECS también estará ubicada en la región CN-Hong Kong. Si desea utilizar la imagen en otra región, primero debe replicarla en esa región. Para más detalles, consulte [Replicación de imágenes entre regiones](#).
- Si un ECS ha caducado o se ha publicado, puede utilizar la imagen de disco del sistema creada a partir del ECS para restaurarlo.

Prerrequisitos

Antes de crear una imagen privada a partir de un ECS:

- Eliminar cualquier dato sensible ECS que pueda contener.
- Asegúrese de que el ECS está en el estado **Running** o **Stopped**.
- Compruebe la configuración de la red ECS y asegúrese de que DHCP está configurado para las NIC. Para más detalles, véase [Configuración de la NIC en DHCP](#).
- Compruebe si el complemento de restablecimiento de contraseña con un solo clic se ha instalado en el ECS. La función de restablecimiento de contraseña en la consola de gestión solo está disponible para los nuevos ECSs que tienen este complemento instalado. Para más detalles, véase [Instalación del complemento de restablecimiento de contraseñas con un solo clic](#).
- Comprobar si se ha instalado Cloud-Init en el ECS. La función de inyección de datos de usuario en la consola de gestión solo está disponible para nuevos ECSs que tienen esta herramienta instalada. Puede utilizar la inyección de datos, por ejemplo, para establecer la contraseña de inicio de sesión para un nuevo ECS. Para más detalles, véase [Instalación de Cloud-Init](#) y [Configuración de Cloud-Init](#).
- Elimine cualquier regla de red para evitar que se desvíe el nombre de la NIC en los ECSs creados a partir de la imagen. Para más detalles, véase [Eliminación de archivos del directorio de reglas de red](#).
- Para garantizar que los ECS creados a partir de la imagen admitan la virtualización Xen y KVM, se debe modificar el Linux ECS utilizado para crear la imagen. Por ejemplo, los ID de disco de los archivos GRUB y fstab deben ser UUID y los controladores nativos de Xen y KVM deben estar instalados.

Para obtener más información, consulte los pasos de **2** a **6** en [Proceso de optimización](#).

- Si se adjuntan varios discos de datos a un ECS usado para crear una imagen privada, es posible que los ECS creados a partir de la imagen no estén disponibles. Es necesario separar todos los discos de datos del ECS antes de usarlo para crear una imagen. Para más detalles, véase [Separación de discos de datos de un ECS](#).
- Si se han conectado discos de datos a la ECS y se ha configurado el montaje automático de la partición en el archivo fstab para la ECS, elimine estas configuraciones del archivo antes de utilizar el ECS para crear una imagen de disco del sistema.
- Asegúrese de que la capacidad de disco del sistema ECS utilizada para crear una imagen de disco del sistema no debe ser superior a 1 TB.

Si la capacidad es superior a 1 TB, solo puede utilizarla para crear una imagen ECS completa.

 **NOTA**

Si ECS se crea a partir de una imagen pública, el complemento de restablecimiento de contraseña con un solo clic y Cloud-Init se han instalado de forma predeterminada. Puede seguir la guía para verificar la instalación.

Procedimiento

Paso 1 Acceda a la consola IMS.

1. Inicie sesión en la consola de gestión.
2. En **Compute**, haga clic en **Image Management Service**.
Se muestra la consola IMS.

Paso 2 Crear una imagen de disco del sistema.

1. Haga clic en **Create Image** en la esquina superior derecha.
2. Establezca parámetros de imagen.

[Tabla 2-3](#) y [Tabla 2-4](#) enumera los parámetros en las áreas **Image Type and Source** e **Image Information**, respectivamente.

Tabla 2-3 Tipo y fuente de imagen

Parámetro	Descripción
Región	<p>Seleccione una región cercana a donde se proporcionarán sus servicios.</p> <p>Si selecciona una región incorrecta aquí, puede replicar la imagen creada en la región deseada más adelante. Para obtener más información, consulte Replicación de una imagen entre regiones.</p>
Tipo	Seleccione System disk image .
Fuente	Seleccione ECS y seleccione un ECS con las configuraciones requeridas.

Tabla 2-4 Información de imágenes.

Parámetro	Descripción
Cifrado	<p>Este parámetro especifica si la imagen se cifrará. El valor es proporcionado por el sistema y no se puede cambiar.</p> <ul style="list-style-type: none"> – Solo se puede crear una imagen privada no cifrada a partir de una imagen no cifrada ECS. – Solo se puede crear una imagen privada cifrada a partir de una imagen cifrada ECS.
Nombre	Establezca un nombre para la imagen.

Parámetro	Descripción
Proyecto empresarial	<p>Seleccione un proyecto de empresa en la lista desplegable. Este parámetro sólo está disponible si ha habilitado proyectos de empresa o si su cuenta es una cuenta de empresa. Para habilitar esta función, póngase en contacto con su gestor de clientes.</p> <p>Un proyecto empresarial proporciona una gestión central de los recursos de la nube en función de cada proyecto.</p>
Etiqueta	(Opcional) Establezca una clave de etiqueta y un valor de etiqueta para la imagen para facilitar la identificación y gestión de sus imágenes.
Descripción	(Opcional) Introduzca una descripción de la imagen.

- Haga clic en **Next**.
- Confirme los parámetros. Lea el descargo de responsabilidad de la imagen y seleccione **I have read and agree to the Image Disclaimer**, y haga clic en **Submit**.

Paso 3 Vuelva a la página **Private Images** y vea la nueva imagen de disco del sistema.

El tiempo necesario para crear una imagen depende del ECS tamaño del disco del sistema, la calidad de la red y el número de tareas simultáneas. Cuando el estado de la imagen cambia a **Normal**, la creación de la imagen se completa.

NOTA

- No realice ninguna operación en los recursos seleccionados ECS o asociados durante la creación de imágenes.
- Un ECS creado a partir de una imagen encriptada también se cifra. La clave utilizada para cifrar el ECS es la misma que la utilizada para cifrar la imagen.
- También se cifrarán las imágenes creadas a partir de un ECS cifrado. La clave utilizada para cifrar la imagen es la misma que la utilizada para cifrar el ECS.

---Fin

Procedimiento posterior

Después de crear una imagen de disco del sistema, puede utilizar cualquiera de los métodos siguientes para migrar datos entre dos servidores:

- Utilice la imagen para crear nuevos ECS. Para más detalles, consulte [Creación de un ECS a partir de una imagen](#).
- Utilice la imagen para cambiar los sistemas operativos de los ECS existentes. Para obtener más información, consulte [Cambiar el sistema operativo](#).

2.4 Creación de una imagen de disco del sistema Windows a partir de un archivo de imagen externo

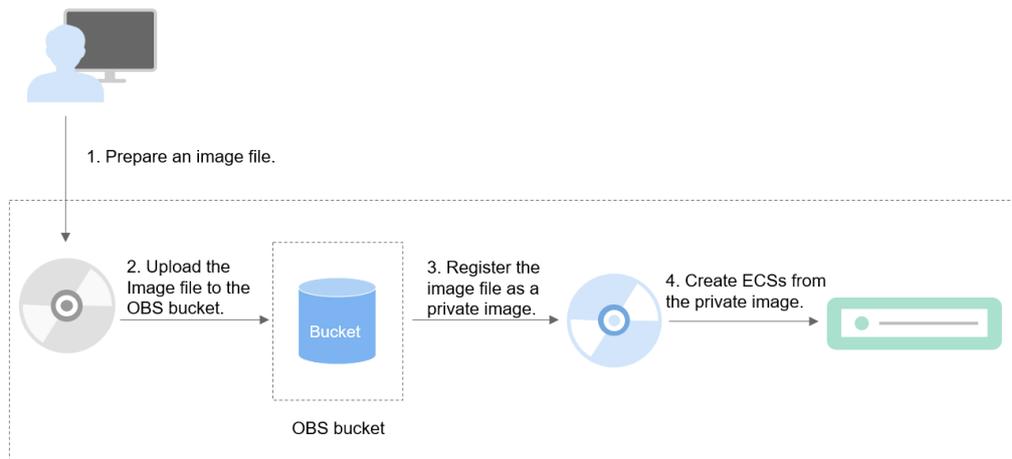
2.4.1 Descripción

Puede importar una imagen local o una imagen de disco del sistema desde otra plataforma en la nube a la nube actual. Después de importar una imagen, puede usarla para crear ECSs o reinstalar los sistemas operativos de ECSs existentes.

Proceso de creación

Figura 2-4 muestra el proceso de creación de una imagen privada.

Figura 2-4 Creación de una imagen de disco del sistema Windows



Como se muestra en la figura, se requieren los siguientes pasos para registrar un archivo de imagen externo como una imagen privada:

1. Prepare un archivo de imagen externo que cumpla con los requisitos de la plataforma. Para obtener más información, véase [Preparación de un archivo de imagen](#).
2. Suba el archivo de imagen externo a tu bucket OBS. Para obtener más información, véase [Carga de un archivo de imagen externo](#).
3. En la consola de gestión, seleccione el archivo de imagen cargado y regístrelo como una imagen privada. Para obtener más información, véase [Registro de un archivo de imagen externo como imagen privada](#).
4. Después de registrar la imagen privada, puede usarla para crear ECS. Para obtener más información, véase [Creación de un ECS de Windows a partir de una imagen](#).

2.4.2 Preparación de un archivo de imagen

Debe preparar un archivo de imagen que cumpla con los requisitos de la plataforma y comprender los problemas conocidos del sistema operativo (consulte [Problemas conocidos](#)).

 **NOTA**

- Se recomienda completar las configuraciones de red, herramientas y controladores de [Tabla 2-5](#) en la máquina virtual de origen y, a continuación, exportar el archivo de imagen. También puede completar las configuraciones en los ECSs creados. Para obtener más información, consulte [¿Qué hago si un archivo de imagen de Windows no está preconfigurado cuando lo uso para registrar una imagen privada?](#)
- Actualmente, un archivo de imagen grande (máximo: 1 TB) solo se puede importar en formato RAW o ZVHD2. Además de los requisitos descritos en [Tabla 2-5](#), es necesario generar un archivo de bitmap para cada archivo de imagen RAW. El archivo de bitmap se carga junto con el archivo de imagen. Para obtener más información, véase [Importación rápida de un archivo de imagen](#).

Tabla 2-5 Requisitos de archivos de imagen de Windows

Propiedad de archivo de imagen	Requerimiento
Sistema operativo	<ul style="list-style-type: none"> ● Windows Server 2008, Windows Server 2012, Windows Server 2016, Windows Server 2019, Windows 10 ● 32 bits o 64 bits ● El sistema operativo no puede vincularse a hardware específico. ● El sistema operativo debe admitir la virtualización completa. <p>Para obtener más información sobre las versiones del sistema operativo compatibles, consulte Formatos de archivos de imágenes externos y sistemas operativos compatibles. Estos sistemas operativos soportan la configuración automática. Para obtener más información, consulte ¿Qué hará el sistema con un archivo de imagen cuando uso el archivo para registrar una imagen privada? Para otros sistemas operativos, compruebe e instale el controlador del sistema operativo invitado. En la página de registro de imágenes, seleccione Other Windows. Después de importar la imagen, si se inicia el sistema depende de la integridad del controlador.</p>
Formato de imagen	VMDK, VHD, QCOW2, RAW, VHDX, QED, VDI, QCOW, ZVHD2, y ZVHD
Tamaño de imagen	<p>Tamaño máximo de archivo: 128 GB</p> <p>Si el tamaño de la imagen está entre 128 GB y 1 TB, convierta el archivo de imagen al formato RAW o ZVHD2 e importe la imagen mediante la importación rápida.</p> <ul style="list-style-type: none"> ● Para obtener más información sobre cómo convertir el formato de archivo de imagen, consulte Conversión del formato de imagen mediante qemu-img-hw. ● Para obtener más información sobre la importación rápida, consulte importación rápida de archivos de imagen.

Propiedad de archivo de imagen	Requerimiento
Network	<p>La NIC debe estar establecida en DHCP. De lo contrario, el inicio de ECS o la capacidad de red será anormal. Para más detalles, consulte: Configuración de la NIC en DHCP</p> <p>Las siguientes operaciones de valor agregado son opcionales:</p> <ul style="list-style-type: none"> ● Activación de la cola múltiple de NIC La cola múltiple de la NIC permite que varias vCPUs procesen interrupciones de la NIC, mejorando así el PPS de la red y el rendimiento de E/S. Para obtener más información, consulte ¿Cómo habilito la cola múltiple de NIC para una imagen? ● Configuración de la asignación dinámica de direcciones IPv6 Las direcciones IPv6 se utilizan para tratar el agotamiento de direcciones IPv4. Si la configuración dinámica está habilitada en un archivo de imagen, los ECSs creados a partir de este archivo se les asignará automáticamente una dirección IPv6. Estos ECS admitirán direcciones IPv4 e IPv6. Configurar la asignación dinámica de direcciones IPv6. Para obtener más información, consulte ¿Cómo configuro un ECS para adquirir dinámicamente direcciones IPv6?
Tool	<p>Se recomienda instalar Cloudbase-Init.</p> <p>Cloudbase-Init es una herramienta de código abierto para la inicialización de instancias en la nube. Al crear ECSs a partir de una imagen con Cloudbase-Init, puede utilizar la inyección de datos de usuario para inyectar detalles de inicialización personalizados (por ejemplo, una ECS contraseña de inicio de sesión) a los ECSs. También puede configurar y gestionar una ejecución ECS consultando y usando metadatos. Si Cloudbase-Init no está instalado, no puede aplicar configuraciones personalizadas a los ECS. Usted tendrá que utilizar la contraseña original en el archivo de imagen para iniciar sesión en los ECS.</p> <p>Para obtener más información, véase Instalación y configuración de Cloudbase-Init.</p>
Controlador	Instalación de UVP VMTtools

Propiedad de archivo de imagen	Requerimiento
Otros requisitos	<ul style="list-style-type: none"> ● Actualmente, no se pueden crear imágenes con discos de datos. El archivo de imagen debe contener solo el disco del sistema, y la capacidad del disco del sistema debe ser de [40 GB, 1024 GB]. ● La contraseña inicial del archivo de imagen debe contener letras mayúsculas, minúsculas, dígitos y caracteres especiales (!@#\$%^_-=+[]{};:./?). ● La partición de arranque y la partición del sistema deben estar en el mismo disco. ● Para un archivo de imagen externo, necesita una combinación de cuenta de administrador de tenant y contraseña. ● Si utiliza un archivo de imagen externo para crear una imagen de disco del sistema Windows y, a continuación, la imagen para crear un ECS, no puede iniciar sesión en el ECS con un par de claves ni obtener la contraseña del par de claves. ● Modos de arranque admitidos: Algunas imágenes de SO x86 son compatibles con el modo de arranque UEFI. (Para obtener más información, consulte Sistemas operativos compatibles con el modo de arranque UEFI.) Las imágenes del sistema operativo Arm solo admiten el modo de arranque UEFI. ● The image file cannot be encrypted, or ECSs created from the registered image may not work properly. ● Se debe generar un archivo de imagen VMDK a partir de una máquina virtual creada en VMware Tools. De lo contrario, es posible que el sistema no se inicie debido a problemas de análisis de imágenes.

2.4.3 Carga de un archivo de imagen externo

Se recomienda utilizar OBS Browser+ para cargar archivos de imagen externos a los buckets de OBS. Para obtener más información, consulte [Prácticas recomendadas de OBS Browser+](#).

Para obtener información sobre cómo descargar el navegador OBS+, consulte https://support.huaweicloud.com/intl/es-us/browsertg-obs/obs_03_1003.html.

 **NOTA**

- El archivo de bucket y la imagen que se va a registrar deben pertenecer a la misma región.
- Solo se pueden cargar en el bucket de OBS archivos de imagen externos no cifrados o aquellos cifrados mediante SSE-KMS.
- La clase de almacenamiento del cucharón OBS debe ser Standard.
- Si desea crear una imagen de disco de datos junto con la imagen de disco del sistema, también debe cargar un archivo de imagen que contenga discos de datos en el bucket de OBS. Puede crear una imagen de disco del sistema y no más de tres imágenes de disco de datos.

2.4.4 Registro de un archivo de imagen externo como imagen privada

Escenarios

Registrar un archivo de imagen cargado en el bucket de OBS como una imagen privada.

Procedimiento

Paso 1 Acceda a la consola IMS.

1. Inicie sesión en la consola de gestión.
2. En **Compute**, haga clic en **Image Management Service**.

Se muestra la consola IMS.

Paso 2 Registrar un archivo de imagen externo como una imagen privada.

1. Haga clic en **Create Image** en la esquina superior derecha.
2. Establezca parámetros de imagen.

Tabla 2-6 y **Tabla 2-7** enumera los parámetros en las áreas **Image Type and Source** e **Image Information**, respectivamente.

Tabla 2-6 Tipo y fuente de imagen

Parámetro	Descripción
Type	Seleccione Import Image .
Region	Seleccione una región cercana a donde se proporcionarán sus servicios. Si selecciona una región incorrecta aquí, puede replicar la imagen creada en la región deseada más adelante. Para obtener más información, consulte Replicación de una imagen entre regiones .
Image Type	Seleccione System disk image .
Source	Seleccione el bucket que almacena el archivo de imagen de la lista y, a continuación, seleccione el archivo de imagen.

Parámetro	Descripción
Enable Fast Create	<p>Este parámetro solo está disponible cuando se selecciona un archivo de imagen ZVHD2 o RAW.</p> <p>Esta función permite la creación rápida de imágenes y admite la importación de archivos grandes (máximo: 1 TB) siempre y cuando los archivos que se van a cargar se conviertan a formato ZVHD2 o RAW y se optimicen. Si tiene un archivo que cumple los requisitos, seleccione Enable Fast Create y seleccione la información de confirmación después de Image File Preparation.</p> <p>NOTA Para obtener información sobre cómo convertir formatos de archivo de imagen y generar archivos de mapa de bits, consulte Importación rápida de un archivo de imagen.</p>

Tabla 2-7 Información de imágenes

Parámetro	Descripción
Enable automatic configuration	Si selecciona esta opción, el sistema comprobará y optimizará automáticamente el archivo de imagen. Para obtener más información, consulte ¿Qué hará el sistema con un archivo de imagen cuando uso el archivo para registrar una imagen privada?
Function	Especifica si la imagen se utiliza para crear ECS o BMS. El valor puede ser ECS system disk image o BMS system disk image . Esta sección utiliza ECS system disk image como ejemplo.
Architecture	<p>Especifique Architecture. Seleccione x86 o ARM.</p> <ul style="list-style-type: none"> – Si el sistema detecta un tipo de arquitectura diferente del establecido, se utilizará el tipo de arquitectura detectado por el sistema. – Si el sistema no detecta el tipo de arquitectura, se utilizará el tipo de arquitectura que establezca.
Boot Mode	<p>Este parámetro es opcional. El valor puede ser BIOS o UEFI. Para obtener más información sobre las diferencias entre los dos, consulte ¿En qué se diferencia el BIOS de UEFI?</p> <p>Para obtener más información sobre los sistemas operativos que admiten el arranque UEFI, consulte sistemas operativos que admiten modo de arranque de UEFI.</p> <p>El modo de arranque debe ser el mismo que en el archivo de imagen. Debe confirmar qué modo de arranque se utiliza en el archivo de imagen. Después de seleccionar el modo de arranque correcto, el modo de arranque se configurará para la imagen en el fondo. Seleccione el modo de arranque correcto, o los ECS creados con la imagen no podrán arrancar.</p>

Parámetro	Descripción
OS	<p>Para asegurarse de que la imagen se puede crear y utilizar correctamente, seleccione un sistema operativo compatible con el del archivo de imagen. Si no selecciona un sistema operativo, el sistema intenta identificar automáticamente el sistema operativo en el archivo de imagen.</p> <p>NOTA</p> <ul style="list-style-type: none"> – Si el sistema detecta que el sistema operativo del archivo de imagen es diferente del que seleccionó, se utilizará el sistema operativo detectado por el sistema. – Si el sistema no puede detectar el sistema operativo en el archivo de imagen, se utilizará el sistema operativo seleccionado. – Si el sistema operativo seleccionado o identificado por el sistema es incorrecto, los ECS creados a partir del archivo de imagen pueden verse afectados.
License Type	Traiga su propia licencia (BYOL) es compatible. Si ha obtenido una licencia de sistema operativo, no necesita solicitar una licencia más.
System Disk (GB)	<p>La capacidad del disco del sistema (rango de valores: 40 GB a 1024 GB). Asegúrese de que este valor es al menos igual a la capacidad del disco del sistema en el archivo de imagen.</p> <p>NOTA</p> <p>Si la imagen VHD cargada se genera usando qemu-img o herramientas similares, comprueba la capacidad del disco del sistema según ¿Qué hago si la capacidad del disco del sistema en un archivo de imagen VHD supera la que he especificado en la consola de gestión cuando uso este archivo para registrar una imagen privada?</p>
Data Disk (GB)	<p>También puede agregar discos de datos a la imagen. Es necesario obtener un archivo de imagen que contenga discos de datos por adelantado. Esta función se utiliza para migrar VMs y discos de datos de otras plataformas a la plataforma actual.</p> <p>Para agregar discos de datos, haga clic en , establezca la capacidad del disco de datos y haga clic en Select Image File. En el cuadro de diálogo que se muestra, seleccione el bucket de destino y, a continuación, el archivo de imagen de destino que contiene el disco de datos.</p> <p>Se puede agregar un máximo de tres discos de datos.</p>
Name	Establezca un nombre para la imagen.
Encryption	<p>(Opcional) Si desea cifrar la imagen, seleccione KMS encryption y seleccione la clave que se utilizará en la lista de claves. Después de seleccionar KMS encryption, el sistema creará una clave predeterminada ims/default para usted. También puede seleccionar una clave de la lista de claves.</p> <p>Para ver cómo cifrar una imagen, consulte Creación de imágenes encriptadas.</p>

Parámetro	Descripción
Enterprise Project	<p>Seleccione un proyecto de empresa en la lista desplegable. Este parámetro solo está disponible si ha habilitado proyectos de empresa o si su cuenta es una cuenta de empresa.</p> <p>Un proyecto empresarial proporciona una gestión central de los recursos de la nube en función de cada proyecto.</p>
Tag	<p>(Opcional) Establezca una clave de etiqueta y un valor de etiqueta para la imagen para facilitar la identificación y gestión de sus imágenes.</p> <p>NOTA</p> <p>Si su organización ha configurado políticas de etiquetas para imágenes, debe agregar etiquetas a las imágenes en función de las políticas. Si no cumple con las políticas de etiquetas, es posible que las imágenes no se creen. Póngase en contacto con el administrador de la organización para obtener más información sobre las políticas de etiquetas.</p> <ul style="list-style-type: none"> – Cada etiqueta consta de una clave y un valor. La clave contiene un máximo de 36 caracteres y el valor contiene un máximo de 43 caracteres. La clave no se puede dejar en blanco ni una cadena de caracteres vacía. El valor no se puede dejar en blanco, sino que puede ser una cadena de caracteres vacía. – Una imagen puede tener un máximo de 10 etiquetas.
Description	(Opcional) Introduzca una descripción de la imagen.

3. Haga clic en **Next** y confirme las especificaciones de la imagen. Seleccione **Statement of Commitment to Image Creation** y **Huawei Image Disclaimer**. Haga clic en **Submit**.

Paso 3 Vuelve a la página de **Private Images**. La imagen se registra correctamente cuando su estado pasa a ser **Normal**.

Si agrega discos de datos durante la creación de imágenes, se generará una imagen de disco del sistema y una imagen de disco de datos. El número de imágenes de disco de datos depende del número de discos de datos que agregue (un máximo de 3).

 **NOTA**

El tiempo necesario para el registro de la imagen viene determinado por el tamaño del archivo de imagen. Es posible que deba esperar un largo período de tiempo para que el archivo de imagen se registre correctamente como una imagen privada.

----Fin

2.4.5 Creación de un ECS de Windows a partir de una imagen

Escenarios

Después de registrar un archivo de imagen externo como una imagen privada en la plataforma en la nube, puede usar la imagen para crear ECS o cambiar los sistemas operativos de ECS existentes.

En esta sección se describe cómo crear un ECS a partir de una imagen.

Procedimiento

Cree un ECS haciendo referencia a [Creación de un ECS a partir de una imagen](#).

Tenga en cuenta lo siguiente al establecer los parámetros:

- **Region:** Seleccione la región donde se encuentra la imagen privada.
- **Specifications:** Seleccione un tipo basado en el tipo de sistema operativo en la imagen y las versiones del sistema operativo descritas en [los sistemas operativos compatibles con diferentes tipos de ECS](#).
- **Imagen:** Seleccione **Private image** y, a continuación, la imagen creada en la lista desplegable.
- (Opcional) **Data Disk:** Agregar discos de datos. Estos discos de datos se crean a partir de una imagen de disco de datos generada junto con una imagen de disco de sistema. De esta manera, puede migrar los datos de los discos de datos junto con los datos del disco del sistema de VM en la plataforma original a la plataforma en la nube actual.

Procedimiento posterior

Después de crear una imagen de disco del sistema, puede utilizarla para cambiar el sistema operativo de un ECS. Para obtener más información, consulte [Cambio del sistema operativo](#).

2.5 Creación de una imagen de disco de sistema Linux a partir de un archivo de imagen externo

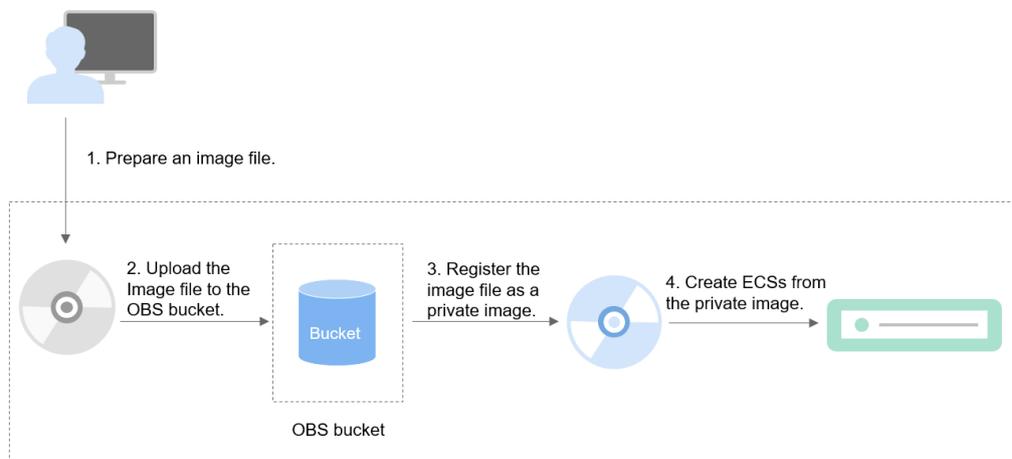
2.5.1 Descripción

Puede importar una imagen local o una imagen de disco del sistema desde otra plataforma en la nube a la nube actual. Después de importar una imagen, puede usarla para crear ECSs o reinstalar los sistemas operativos de ECSs existentes.

Proceso de creación

Figura 2-5 muestra el proceso de creación de una imagen privada.

Figura 2-5 Creación de una imagen de disco del sistema Linux



El procedimiento es el siguiente:

1. Prepare un archivo de imagen externo que cumpla con los requisitos de la plataforma. Para obtener más información, véase [Preparación de un archivo de imagen](#).
2. Suba el archivo de imagen externo a su bucket OBS. Para obtener más información, véase [Carga de un archivo de imagen externo](#).
3. En la consola de gestión, seleccione el archivo de imagen cargado y regístrelo como una imagen privada. Para obtener más información, véase [Registro de un archivo de imagen externo como imagen privada](#).
4. Después de registrar la imagen privada, puede usarla para crear ECS. Para obtener más información, véase [Creación de un ECS de Linux a partir de una imagen](#).

2.5.2 Preparación de un archivo de imagen

Debe preparar un archivo de imagen que cumpla con los requisitos de la plataforma y comprender los problemas conocidos del sistema operativo (consulte [Problemas conocidos](#)).

NOTA

- Se recomienda completar las configuraciones del sistema de archivos, la red y el controlador de [Tabla 2-8](#) en la máquina virtual de origen y, a continuación, exportar el archivo de imagen. También puede completar las configuraciones en los ECSs creados. Para obtener más información, consulte [¿Qué hago si un archivo de imagen de Linux no está preconfigurado cuando lo uso para registrar una imagen privada?](#)
- Currently, a large image file (maximum: 1 TB) can be imported only in RAW or ZVHD2 format. In addition to the requirements described in [Tabla 2-8](#), a bitmap file needs to be generated for each RAW image file. The bitmap file is uploaded together with the image file. For details, see [Importación rápida de un archivo de imagen](#).

Tabla 2-8 Requisitos del archivo de imagen de Linux

Propiedad de archivo de imagen	Requerimiento
Sistema operativo	<ul style="list-style-type: none"> ● SUSE, Oracle Linux, Red Hat, Ubuntu, openSUSE, CentOS, Debian, Fedora, EulerOS, y NeoKylin ● 32 bits o 64 bits ● El sistema operativo no puede vincularse a hardware específico. ● El sistema operativo debe admitir la virtualización completa. <p>Para obtener más información sobre las versiones del sistema operativo compatibles, consulte Formatos de archivos de imágenes externos y sistemas operativos compatibles. Estos sistemas operativos soportan la configuración automática. Para obtener más información, consulte ¿Qué hará el sistema con un archivo de imagen cuando uso el archivo para registrar una imagen privada? Para otros sistemas operativos, compruebe e instale los controladores VirtIO (consulte Instalación de controladores KVM nativos). En la página de registro de imágenes, seleccione Other Linux. Después de importar la imagen, si se inicia el sistema depende de la integridad del controlador.</p>

Propiedad de archivo de imagen	Requerimiento
Formato de imagen	VMDK, VHD, QCOW2, RAW, VHDX, QED, VDI, QCOW, ZVHD2 y ZVHD
Tamaño de imagen	<p>Tamaño máximo de archivo: 128 GB</p> <p>Si el tamaño de la imagen está entre 128 GB y 1 TB, convierta el archivo de imagen al formato RAW o ZVHD2 e importe la imagen mediante la importación rápida.</p> <ul style="list-style-type: none"> ● Para obtener más información sobre cómo convertir el formato de archivo de imagen, consulte Conversión del formato de imagen mediante qemu-img-hw. ● Para obtener más información sobre la importación rápida, consulte importación rápida de archivos de imagen.
Red	<p>La NIC debe estar establecida en DHCP y los archivos deben eliminarse del directorio de rol de red. De lo contrario, el inicio de ECS o la capacidad de red será anormal. Para más detalles, consulte:</p> <ul style="list-style-type: none"> ● Eliminación de archivos del directorio de reglas de red ● Configuración de la NIC en DHCP <p>Las siguientes operaciones de valor agregado son opcionales:</p> <ul style="list-style-type: none"> ● Activación de la cola múltiple de NIC La cola múltiple de la NIC permite que varias vCPUs procesen interrupciones de la NIC, mejorando así el PPS de la red y el rendimiento de E/S. Para obtener más información, consulte ¿Cómo habilito la cola múltiple de NIC para una imagen? ● Configuración de la asignación dinámica de direcciones IPv6 Las direcciones IPv6 se utilizan para tratar el agotamiento de direcciones IPv4. Si la configuración dinámica está habilitada en un archivo de imagen, los ECS creados a partir de este archivo se les asignará automáticamente una dirección IPv6. Estos ECS admitirán direcciones IPv4 e IPv6. Configurar la asignación dinámica de direcciones IPv6. Para obtener más información, consulte ¿Cómo configuro un ECS para adquirir dinámicamente direcciones IPv6?
Herramienta	<p>Se recomienda instalar Cloud-Init.</p> <p>Cloud-Init es una herramienta de código abierto para la inicialización de instancias en la nube. Al crear ECS a partir de una imagen con Cloud-Init, puede usar la inyección de datos de usuario para inyectar detalles de inicialización personalizados (por ejemplo, una ECS contraseña de inicio de sesión) a los ECS. También puede configurar y gestionar una ejecución ECS consultando y usando metadatos. Si Cloud-Init no está instalado, no puede aplicar configuraciones personalizadas a los ECS. Usted tendrá que utilizar la contraseña original en el archivo de imagen para iniciar sesión en los ECS.</p> <p>Para obtener más información, véase Instalación de Cloud-Init.</p>

Propiedad de archivo de imagen	Requerimiento
Controlador	Instalación de controladores KVM nativos
Sistema de archivos	<ul style="list-style-type: none"> ● Cambio del identificador de disco en el archivo de configuración de GRUB a UUID ● Cambio del identificador de disco en el archivo fstab a UUID
Otros requerimientos	<ul style="list-style-type: none"> ● Actualmente, no se pueden crear imágenes con discos de datos. El archivo de imagen debe contener solo el disco del sistema, y la capacidad del disco del sistema debe ser de [40 GB, 1024 GB]. ● La contraseña inicial del archivo de imagen debe contener letras mayúsculas, minúsculas, dígitos y caracteres especiales (!@%\$%^_-=+[{ }],./?). ● La partición de arranque y la partición del sistema deben estar en el mismo disco. ● Modos de arranque admitidos: Algunas imágenes de SO x86 son compatibles con el modo de arranque UEFI. (Para obtener más información, consulte Sistemas operativos compatibles con el modo de arranque UEFI.) Las imágenes del sistema operativo Arm solo admiten el modo de arranque UEFI. ● El archivo de imagen no se puede cifrar, o es posible que los ECS creados a partir de la imagen registrada no funcionen correctamente. ● El archivo <code>/etc/fstab</code> no puede contener información de montaje automático de discos que no sean del sistema. De lo contrario, el inicio de sesión en ECS creado puede fallar. ● Si el archivo de imagen externa utiliza LVM como disco del sistema, los ECS creados a partir de la imagen privada no admiten la inyección de archivos. ● Si la VM donde se encuentra el archivo de imagen externo se ha apagado, debe ser un apagado correcto. De lo contrario, puede producirse una pantalla azul cuando se inicia los ECS creados a partir de la imagen privada. ● Se debe crear un archivo de imagen VMDK a partir de una máquina virtual generada por VMware Tools. De lo contrario, es posible que el sistema no se inicie debido a problemas de análisis de imágenes.

2.5.3 Carga de un archivo de imagen externo

Se recomienda utilizar OBS Browser+ para cargar archivos de imagen externos a los buckets de OBS. Para obtener más información, consulte [Prácticas recomendadas de OBS Browser+](#).

Para obtener información sobre cómo descargar el navegador OBS+, consulte https://support.huaweicloud.com/intl/es-us/browsertg-obs/obs_03_1003.html.

 **NOTA**

- El archivo de bucket y la imagen que se va a registrar deben pertenecer a la misma región.
- Solo se pueden cargar en el bucket de OBS archivos de imagen externos no cifrados o aquellos cifrados mediante SSE-KMS.
- La clase de almacenamiento del cucharón OBS debe ser Standard.
- Si desea crear una imagen de disco de datos junto con la imagen de disco del sistema, también debe cargar un archivo de imagen que contenga discos de datos en el bucket de OBS. Puede crear una imagen de disco del sistema y no más de tres imágenes de disco de datos.

2.5.4 Registro de un archivo de imagen externo como imagen privada

Escenarios

Registrar un archivo de imagen cargado en el bucket de OBS como una imagen privada.

Procedimiento

Paso 1 Acceda a la consola IMS.

1. Inicie sesión en la consola de gestión.
2. En **Compute**, haga clic en **Image Management Service**.
Se muestra la consola IMS.

Paso 2 Registrar un archivo de imagen externo como una imagen privada.

1. Haga clic en **Create Image** en la esquina superior derecha.
2. Establezca parámetros de imagen.

Tabla 2-9 y **Tabla 2-10** enumera los parámetros en las áreas **Image Type and Source** e **Image Information**, respectivamente.

Tabla 2-9 Tipo y fuente de imagen

Parámetro	Descripción
Type	Seleccione Import Image .
Region	Seleccione una región cercana a donde se proporcionarán sus servicios. Si selecciona una región incorrecta aquí, puede replicar la imagen creada en la región deseada más adelante. Para obtener más información, consulte Replicación de una imagen entre regiones .
Image Type	Seleccione System disk image .
Source	Seleccione el bucket que almacena el archivo de imagen de la lista y, a continuación, seleccione el archivo de imagen.

Parámetro	Descripción
Enable Fast Create	<p>Este parámetro solo está disponible cuando se selecciona un archivo de imagen ZVHD2 o RAW.</p> <p>Esta función permite la creación rápida de imágenes y admite la importación de archivos grandes (máximo: 1 TB) siempre y cuando los archivos que se van a cargar se conviertan a formato ZVHD2 o RAW y se optimicen. Si tiene un archivo que cumple los requisitos, seleccione Enable Fast Create y seleccione la información de confirmación después de Image File Preparation.</p> <p>NOTA Para obtener información sobre cómo convertir formatos de archivo de imagen y generar archivos de mapa de bits, consulte Importación rápida de un archivo de imagen.</p>

Tabla 2-10 Información de imágenes

Parámetro	Descripción
Enable automatic configuration	Si selecciona esta opción, el sistema comprobará y optimizará automáticamente el archivo de imagen. Para obtener más información, consulte ¿Qué hará el sistema con un archivo de imagen cuando uso el archivo para registrar una imagen privada?
Function	Especifica si la imagen se utiliza para crear ECS o BMS. El valor puede ser ECS system disk image o BMS system disk image . Esta sección utiliza ECS system disk image como ejemplo.
Architecture	<p>Especifique Architecture. Seleccione x86 o ARM.</p> <ul style="list-style-type: none"> – Si el sistema detecta un tipo de arquitectura diferente del establecido, se utilizará el tipo de arquitectura detectado por el sistema. – Si el sistema no detecta el tipo de arquitectura, se utilizará el tipo de arquitectura que establezca.
Boot Mode	<p>Este parámetro es opcional. El valor puede ser BIOS o UEFI. Para obtener más información sobre las diferencias entre los dos, consulte ¿En qué se diferencia el BIOS de UEFI?</p> <p>Para obtener más información sobre los sistemas operativos que admiten el arranque UEFI, consulte sistemas operativos que admiten modo de arranque de UEFI.</p> <p>El modo de arranque debe ser el mismo que en el archivo de imagen. Debe confirmar qué modo de arranque se utiliza en el archivo de imagen. Después de seleccionar el modo de arranque correcto, el modo de arranque se configurará para la imagen en el fondo. Seleccione el modo de arranque correcto, o los ECS creados con la imagen no podrán arrancar.</p>

Parámetro	Descripción
OS	<p>Para asegurarse de que la imagen se puede crear y utilizar correctamente, seleccione un sistema operativo compatible con el del archivo de imagen. Si no selecciona un sistema operativo, el sistema intenta identificar automáticamente el sistema operativo en el archivo de imagen.</p> <p>NOTA</p> <ul style="list-style-type: none"> – Si el sistema detecta que el sistema operativo del archivo de imagen es diferente del que seleccionó, se utilizará el sistema operativo detectado por el sistema. – Si el sistema no puede detectar el sistema operativo en el archivo de imagen, se utilizará el sistema operativo seleccionado. – Si el sistema operativo seleccionado o identificado por el sistema es incorrecto, los ECS creados a partir del archivo de imagen pueden verse afectados.
License Type	Traiga su propia licencia (BYOL) es compatible. Si ha obtenido una licencia de sistema operativo, no necesita solicitar una licencia más.
System Disk (GB)	<p>La capacidad del disco del sistema (rango de valores: 40 GB a 1024 GB). Asegúrese de que este valor es al menos igual a la capacidad del disco del sistema en el archivo de imagen.</p> <p>NOTA</p> <p>Si la imagen VHD cargada se genera usando qemu-img o herramientas similares, comprueba la capacidad del disco del sistema según ¿Qué hago si la capacidad del disco del sistema en un archivo de imagen VHD supera la que he especificado en la consola de gestión cuando uso este archivo para registrar una imagen privada?</p>
Data Disk (GB)	<p>También puede agregar discos de datos a la imagen. Es necesario obtener un archivo de imagen que contenga discos de datos por adelantado. Esta función se utiliza para migrar VMs y discos de datos de otras plataformas a la plataforma actual.</p> <p>Para agregar discos de datos, haga clic en , establezca la capacidad del disco de datos y haga clic en Select Image File. En el cuadro de diálogo que se muestra, seleccione el bucket de destino y, a continuación, el archivo de imagen de destino que contiene el disco de datos.</p> <p>Se puede agregar un máximo de tres discos de datos.</p>
Name	Establezca un nombre para la imagen.
Encryption	<p>(Opcional) Si desea cifrar la imagen, seleccione KMS encryption y seleccione la clave que se utilizará en la lista de claves. Después de seleccionar KMS encryption, el sistema creará una clave predeterminada ims/default para usted. También puede seleccionar una clave de la lista de claves.</p> <p>Para ver cómo cifrar una imagen, consulte Creación de imágenes encriptadas.</p>

Parámetro	Descripción
Enterprise Project	<p>Seleccione un proyecto de empresa en la lista desplegable. Este parámetro solo está disponible si ha habilitado proyectos de empresa o si su cuenta es una cuenta de empresa.</p> <p>Un proyecto empresarial proporciona una gestión central de los recursos de la nube en función de cada proyecto.</p>
Tag	<p>(Opcional) Establezca una clave de etiqueta y un valor de etiqueta para la imagen para facilitar la identificación y gestión de sus imágenes.</p> <p>NOTA</p> <p>Si su organización ha configurado políticas de etiquetas para imágenes, debe agregar etiquetas a las imágenes en función de las políticas. Si no cumple con las políticas de etiquetas, es posible que las imágenes no se creen. Póngase en contacto con el administrador de la organización para obtener más información sobre las políticas de etiquetas.</p> <ul style="list-style-type: none"> – Cada etiqueta consta de una clave y un valor. La clave contiene un máximo de 36 caracteres y el valor contiene un máximo de 43 caracteres. La clave no se puede dejar en blanco ni una cadena de caracteres vacía. El valor no se puede dejar en blanco, sino que puede ser una cadena de caracteres vacía. – Una imagen puede tener un máximo de 10 etiquetas.
Description	(Opcional) Introduzca una descripción de la imagen.

- Haga clic en **Next** y confirme las especificaciones de la imagen. Seleccione **Statement of Commitment to Image Creation** y **Huawei Image Disclaimer**. Haga clic en **Submit**.

Paso 3 Vuelve a la página de **Private Images**. La imagen se registra correctamente cuando su estado pasa a ser **Normal**.

Si agrega discos de datos durante la creación de imágenes, se generará una imagen de disco del sistema y una imagen de disco de datos. El número de imágenes de disco de datos depende del número de discos de datos que agregue (un máximo de 3).

 **NOTA**

El tiempo necesario para el registro de la imagen viene determinado por el tamaño del archivo de imagen. Es posible que deba esperar un largo periodo de tiempo para que el archivo de imagen se registre correctamente como una imagen privada.

----Fin

2.5.5 Creación de un ECS de Linux a partir de una imagen

Escenarios

Después de registrar un archivo de imagen externo como una imagen privada en la plataforma en la nube, puede usar la imagen para crear ECS o cambiar los sistemas operativos de ECS existentes.

En esta sección se describe cómo crear un ECS a partir de una imagen.

Procedimiento

Cree un ECS haciendo referencia a [Creación de un ECS a partir de una imagen](#).

Tenga en cuenta lo siguiente al establecer los parámetros:

- **Region:** Seleccione la región donde se encuentra la imagen privada.
- **Specifications:** Seleccione un tipo basado en el tipo de sistema operativo en la imagen y las versiones del sistema operativo descritas en [los sistemas operativos compatibles con diferentes tipos de ECS](#).
- **Imagen:** Seleccione **Private image** y, a continuación, la imagen creada en la lista desplegable.
- (Opcional) **Data Disk:** Agregar discos de datos. Estos discos de datos se crean a partir de una imagen de disco de datos generada junto con una imagen de disco de sistema. De esta manera, puede migrar los datos de los discos de datos junto con los datos del disco del sistema de VM en la plataforma original a la plataforma en la nube actual.

Procedimiento posterior

Después de crear una imagen de disco del sistema, puede utilizarla para cambiar el sistema operativo de un ECS. Para obtener más información, consulte [Cambio del sistema operativo](#).

2.6 Creación de una imagen de disco de datos a partir de un ECS

Escenarios

Una imagen de disco de datos contiene solo datos de servicio. Puede crear una imagen de disco de datos desde un ECS y luego usar la imagen para crear nuevos discos de EVS. Esta es una forma conveniente de migrar datos de un ECS a discos de EVS.

Se recomienda utilizar imágenes de disco de datos en los siguientes escenarios:

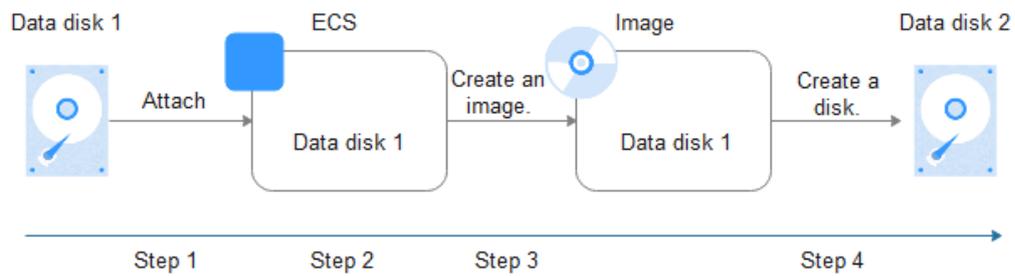
- Migrar datos de servicio en un ECS a otra cuenta.
Crear una imagen de disco de datos desde el disco de datos y [compartir](#) la imagen con la cuenta de destino. A continuación, puede utilizar la imagen de disco de datos de la cuenta para crear discos de datos, completando la migración de datos de servicio.
- Migrar datos de servicio en un ECS a otra región.
Crear una imagen de disco de datos a partir del disco de datos en la región actual y replique la imagen en la región de destino (para obtener más información, consulte [Replicación de imágenes entre regiones](#)). A continuación, puede utilizar la imagen de disco de datos en la región de destino para crear discos de datos, completando la migración de datos de servicio.

Por ejemplo, puede crear una imagen de disco de datos para clonar los datos de un ECS cuyo disco está a punto de caducar.

Antecedentes

La siguiente figura muestra el proceso de crear una imagen de disco de datos a partir de un ECS.

Figura 2-6 Creación de una imagen de disco de datos y uso de ella para crear discos de datos



Prerrequisitos

- Se ha conectado un disco de datos al ECS y el ECS se está ejecutando o parando. Para obtener más información sobre cómo adjuntar un disco de datos, consulte *Guía de usuario de Elastic Cloud Server*.
- La capacidad del disco de datos del ECS no debe ser superior a 1 TB.
Si la capacidad es superior a 1 TB, solo puede utilizar el ECS para crear una imagen de ECS completo.

Procedimiento

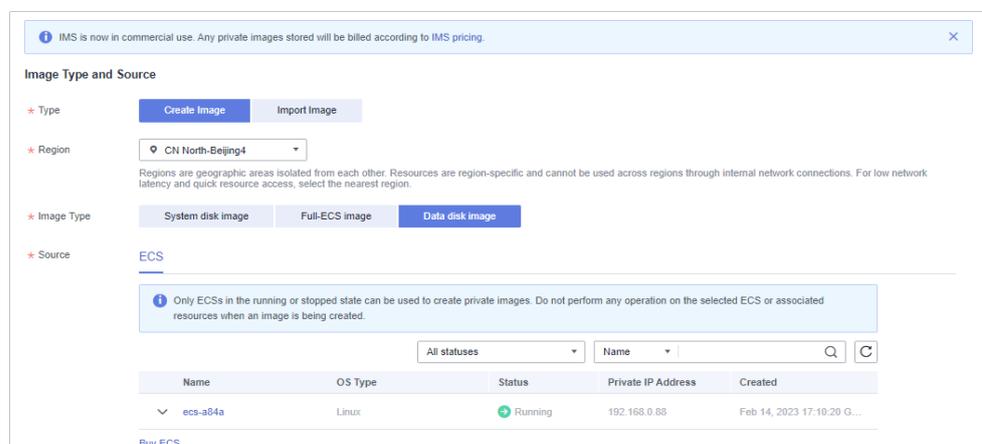
Paso 1 Acceda a la consola IMS.

1. Inicie sesión en la consola de gestión.
2. En **Compute**, haga clic en **Image Management Service**.
Se muestra la consola IMS.

Paso 2 Cree una imagen de disco de datos.

1. Haga clic en **Create Image** en la esquina superior derecha.
2. En el área **Image Type and Source**, seleccione **Create Image** para **Type** y, a continuación, seleccione **Data disk image** para **Image Type**.
3. Seleccione **ECS** para **Source** y, a continuación, seleccione un disco de datos del ECS.

Figura 2-7 Creación de una imagen de disco de datos



4. En el área **Image Information**, establezca **Name**, **Tag**, y **Description** y seleccione un proyecto de empresa.

Si el disco de datos no está encriptado, la imagen privada creada a partir de él tampoco está encriptado. El atributo de encriptación no se puede cambiar durante la creación de la imagen. Después de crear la imagen, puede cambiar su atributo de cifrado basado en la [Replicación de imágenes dentro de una región](#).

NOTA

Si su organización ha configurado políticas de etiquetas para imágenes, debe agregar etiquetas a las imágenes en función de las políticas. Si no cumple con las políticas de etiquetas, es posible que las imágenes no se creen. Póngase en contacto con el administrador de la organización para obtener más información sobre las políticas de etiquetas.

- Cada etiqueta consiste en una clave y un valor. La clave contiene un máximo de 36 caracteres y el valor contiene un máximo de 43 caracteres. La clave no se puede dejar en blanco ni una cadena de caracteres vacía. El valor no se puede dejar en blanco, sino que puede ser una cadena de caracteres vacía.
- Una imagen puede tener un máximo de 10 etiquetas.

5. Haga clic en **Next**.
6. Confirme la configuración. Lea el descargo de responsabilidad de la imagen y seleccione **I have read and agree to the Image Disclaimer**, y haga clic en **Submit**.

Se muestra la lista de imágenes privadas. Espere hasta que la imagen del disco de datos se cree correctamente.

Paso 3 Vuelva a la página **Private Images** y vea la nueva imagen de disco de datos.

----Fin

Procedimiento posterior

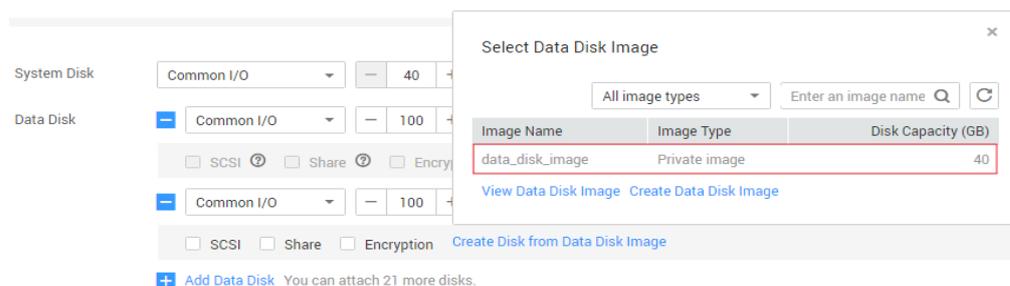
Si desea utilizar la imagen de disco de datos creada para crear un disco EVS y adjuntarlo a un ECS puede realizar cualquiera de las siguientes operaciones:

- Busque la fila que contiene la imagen de disco de datos creada y haga clic en **Create Data Disk** para crear uno o varios discos de datos. A continuación, conecte los discos de datos a un ECS.
- En la página de creación de ECS, haga clic en **Create Disk from Data Disk Image** y seleccione la imagen de disco de datos.

NOTA

De esta manera, se puede usar una imagen de disco de datos para crear un disco de datos para un ECS solo una vez. Por ejemplo, un disco de datos creado a partir de la imagen de disco de datos **data_disk_image** se ha añadido al ECS. No se puede añadir ningún otro disco de datos creado a partir de esta imagen al ECS.

Figura 2-8 Adición de discos de datos



2.7 Creación de una imagen de disco de datos a partir de un archivo de imagen externo

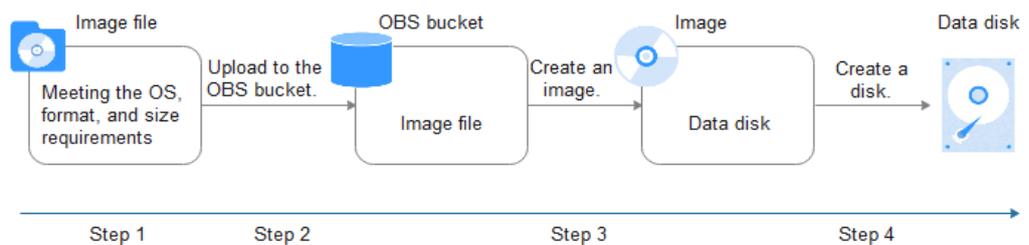
Escenarios

Una imagen de disco de datos contiene solo datos de servicio. Puede crear una imagen de disco de datos utilizando un archivo de imagen local o un archivo de imagen externo (archivo de imagen en otra plataforma en la nube). A continuación, puede utilizar la imagen de disco de datos para crear discos EVS y migrar sus datos de servicio a la nube.

Antecedentes

La siguiente figura muestra el proceso de creación de una imagen de disco de datos a partir de un archivo de imagen externo.

Figura 2-9 Creación de una imagen de disco de datos a partir de un archivo de imagen externo



1. Prepare un archivo de imagen externo. El archivo debe estar en formato VHD, VMDK, QCOW2, RAW, VHDX, QCOW, VDI, QED, ZVHD o ZVHD2. Si desea utilizar un archivo de imagen en otros formatos, convierta el archivo en cualquiera de los formatos enumerados antes de importarlo a la plataforma en la nube.
Para obtener más información sobre la conversión de formato de archivo de imagen, consulte [Convertir el formato de imagen usando qemu-img](#) o [Convertir el formato de imagen usando qemu-img-hw](#).
2. Al cargar el archivo de imagen externa, debe seleccionar un bucket de OBS con almacenamiento estándar. Para obtener más información, véase [Carga de un archivo de imagen externo](#).
3. Cree una imagen de disco de datos. Para obtener más información, véase [Procedimiento](#).
4. Utilice la imagen de disco de datos para crear discos de datos. Para obtener más información, véase [Procedimiento posterior](#).

Procedimiento

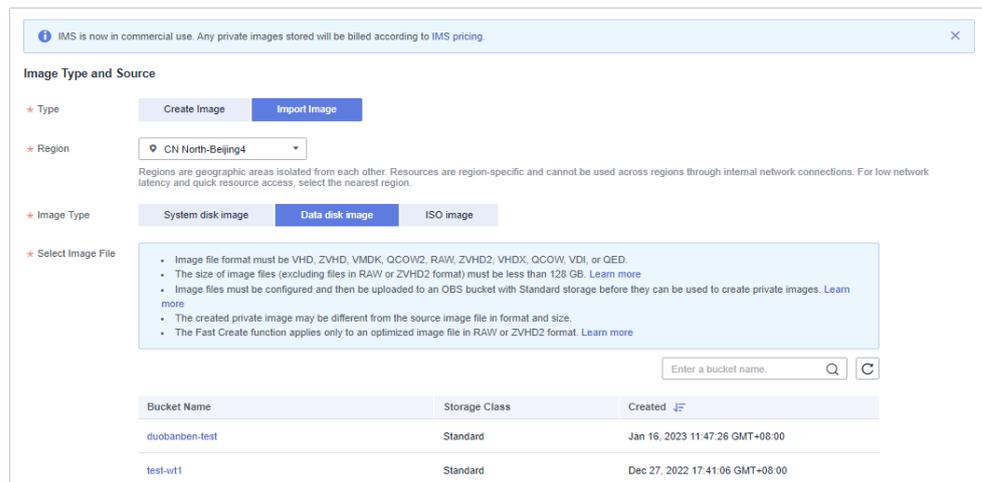
Paso 1 Acceda a la consola IMS.

1. Inicie sesión en la consola de gestión.
2. En **Compute**, haga clic en **Image Management Service**.
Se muestra la consola IMS.

Paso 2 Cree una imagen de disco de datos.

1. Haga clic en **Create Image** en la esquina superior derecha.
2. En el área **Image Type and Source**, seleccione **Import Image** para **Type** y, a continuación, seleccione **Data disk image** para **Image Type**.
3. Select the bucket storing the image file from the list and then select the image file.

Figura 2-10 Creación de una imagen de disco de datos a partir de un archivo de imagen externo



4. Para registrar el archivo de imagen mediante la función de creación rápida, seleccione **Enable Fast Create**.

NOTA

- Actualmente, esta función solo admite archivos de imagen en formato ZVHD2 o RAW.
- Para ver cómo convertir formatos de archivo de imagen y generar archivos de mapa de bits, consulte [Importación rápida de un archivo de imagen](#).

Después de seleccionar **Enable Fast Create**, seleccione la información de confirmación **Image File Preparation** si ha preparado los archivos necesarios.

5. En el área **Image Information**, establezca los siguientes parámetros.
 - **OS Type:** El valor es de **Windows** o **Linux**.
 - **Data Disk:** El valor oscila entre 0 GB y 2048 GB y no debe ser menor que la capacidad del disco de datos en el archivo de imagen.
 - **Name:** Introduzca un nombre para la imagen.
 - (Opcional) **Encryption:** Si desea cifrar la imagen, seleccione **KMS encryption** y, a continuación, seleccione la clave que se utilizará en la lista de claves.
 - **Enterprise Project:** seleccione un proyecto de empresa para la imagen en la lista desplegable. predeterminado es el proyecto de empresa predeterminado.
 - (Optional) **Tag:** Set a tag key and a tag value for the image to easily identify and manage it.

NOTA

Si su organización ha configurado políticas de etiquetas para imágenes, debe agregar etiquetas a las imágenes en función de las políticas. Si agrega una etiqueta que no cumple con las políticas de etiquetas, es posible que las imágenes no se creen. Póngase en contacto con el administrador de la organización para obtener más información sobre las políticas de etiquetas.

- Cada etiqueta consiste en una clave y un valor. La clave contiene un máximo de 36 caracteres y el valor contiene un máximo de 43 caracteres. La clave no se puede dejar en blanco ni una cadena de caracteres vacía. El valor no se puede dejar en blanco, sino que puede ser una cadena de caracteres vacía.
 - Una imagen puede tener un máximo de 10 etiquetas.
- (Opcional) **Description**: Introduzca la descripción de la imagen.
6. Haga clic en **Next**.
 7. Confirme la configuración. Lea el descargo de responsabilidad de la imagen y seleccione **I have read and agree to the Image Disclaimer**, y haga clic en **Submit**.

Paso 3 Vuelva a la página **Private Images** y vea la nueva imagen de disco de datos.

Cuando el estado de la imagen cambia a **Normal**, la creación de la imagen se completa.

----Fin

Procedimiento posterior

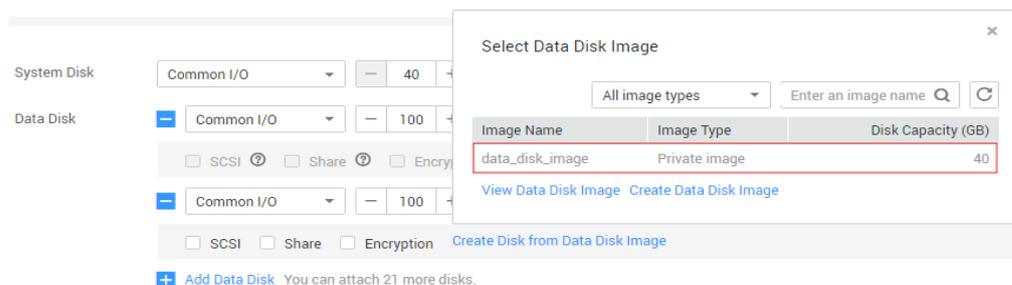
Si desea utilizar la imagen de disco de datos creada para crear un disco EVS y adjuntarlo a un ECS puede realizar cualquiera de las siguientes operaciones:

- Busque la fila que contiene la imagen de disco de datos creada y haga clic en **Create Data Disk** para crear uno o varios discos de datos. A continuación, conecte los discos de datos a un ECS.
- En la página de creación de ECS, haga clic en **Create Disk from Data Disk Image** y seleccione la imagen de disco de datos.

NOTA

De esta manera, se puede usar una imagen de disco de datos para crear un disco de datos para un ECS solo una vez. Por ejemplo, un disco de datos creado a partir de la imagen de disco de datos **data_disk_image** se ha añadido al ECS. No se puede añadir ningún otro disco de datos creado a partir de esta imagen al ECS.

Figura 2-11 Adición de discos de datos



2.8 Creación de una imagen de ECS completo a partir de un ECS

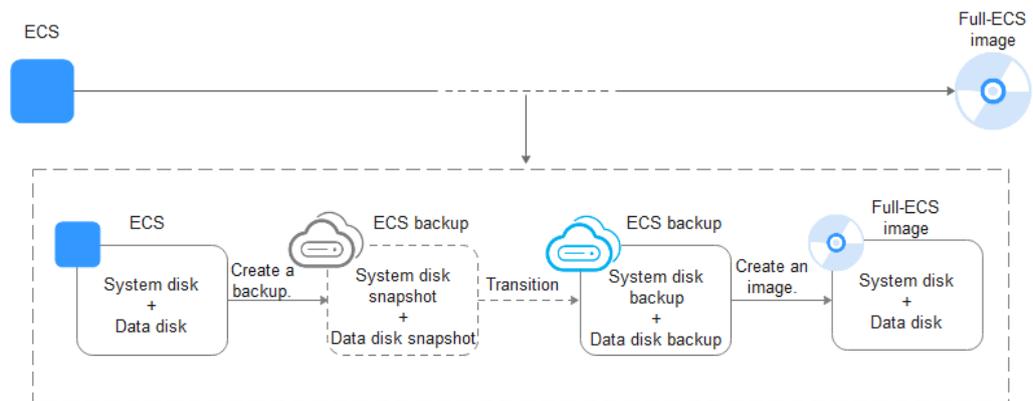
Escenarios

Puede crear una imagen de un ECS completo, que incluye no solo el sistema operativo, sino también el software y todos los datos del servicio. A continuación, puede utilizar esta imagen para migrar datos aprovisionando rápidamente clones exactos del ECS original.

Antecedentes

La siguiente figura muestra el proceso de creación de una imagen a partir de un ECS completo, con el sistema y los discos de datos incluidos.

Figura 2-12 Creación de una imagen completa de ECS a partir de un ECS



- El tiempo necesario para crear una imagen completa del ECS depende del tamaño del disco, la calidad de la red y el número de tareas simultáneas.
- El ECS utilizado para crear una imagen completa del ECS debe estar en estado **Running** o **Stopped**. Para crear una imagen ECS completa que contenga una base de datos, utilice un ECS detenido.
- Si un ECS está en estado **Stopped**, no lo inicie cuando lo esté usando para crear una imagen completa del ECS.
- Cuando se crea una imagen completa del ECS a partir de un ECS, no realice ninguna operación en el ECS o la creación de la imagen puede fallar.
- En el caso de **Figura 2-12**, si hay instantáneas del disco del sistema y discos de datos, pero la creación de copia de respaldo de ECS no está completa, la imagen completa del ECS que cree solo estará disponible en la zona de disponibilidad donde está el ECS de origen y solo se puede utilizar para aprovisionar ECS en esta zona de disponibilidad. No puede aprovisionar ECS en otras zonas de disponibilidad de la región hasta que el ECS original esté completamente respaldado y la imagen completa de ECS esté en el estado **Normal**.
- Si utiliza una imagen completa del ECS para cambiar un sistema operativo de ECS, solo los datos del disco del sistema pueden ser escritos en el ECS. Por lo tanto, si desea restaurar o migrar los datos del disco de datos de un ECS usando una imagen completa

del ECS, solo puede usar la imagen para crear un nuevo ECS en lugar de usarla para cambiar el sistema operativo de ECS.

Restricciones

- Al crear una imagen de ECS completo a partir de un ECS, asegúrese de que ECS se ha configurado correctamente, o la creación de la imagen puede fallar.
 Para obtener más información, consulte [¿Cómo configuro un ECS, BMS o archivo de imagen antes de usarlo para crear una imagen?](#)
- Un ECS de Windows utilizado para crear una imagen completa del ECS no puede tener un volumen extendido, o los datos se pueden perder cuando se crean ECS a partir de esa imagen.
- Un ECS de Linux utilizado para crear una imagen completa del ECS no puede tener un grupo de discos o disco lógico que contenga varios discos físicos, o los datos pueden perderse cuando se crean ECS a partir de esa imagen.
- Un ECS utilizado para crear una imagen completa del ECS no puede contener un disco de Dedicated Distributed Storage Service (DSS).
- Una imagen completa del ECS no se puede exportar, publicar en Marketplace o replicar dentro de una región.
- Al crear una imagen completa del ECS desde un ECS de Windows, debe cambiar la política SAN del ECS a OnlineAll. De lo contrario, los discos EVS conectados a los ECS creados a partir de la imagen pueden estar fuera de línea.

Windows tiene tres tipos de políticas SAN: **OnlineAll**, **OfflineShared** y **OfflineInternal**.

Tabla 2-11 Políticas de SAN en Windows

Tipo	Descripción
OnlineAll	Todos los discos recién detectados se ponen en línea automáticamente.
OfflineShared	Todos los discos en buses compartibles, como iSCSI y FC, se dejan sin conexión de forma predeterminada, mientras que los discos en buses no compartibles se mantienen en línea.
OfflineInternal	Todos los discos recién detectados se dejan sin conexión.

- a. Ejecute **cmd.exe** y ejecute el siguiente comando para consultar la política SAN actual del ECS:
diskpart
- b. Ejecute el siguiente comando para ver la política SAN del ECS:
san
 - Si la política de SAN es **OnlineAll**, ejecute el comando **exit** para salir de DiskPart.
 - Si la política de SAN no es **OnlineAll**, vaya a **c**.
- c. Ejecute el siguiente comando para cambiar la política SAN de ECS a **OnlineAll**:
san policy=onlineall

Procedimiento

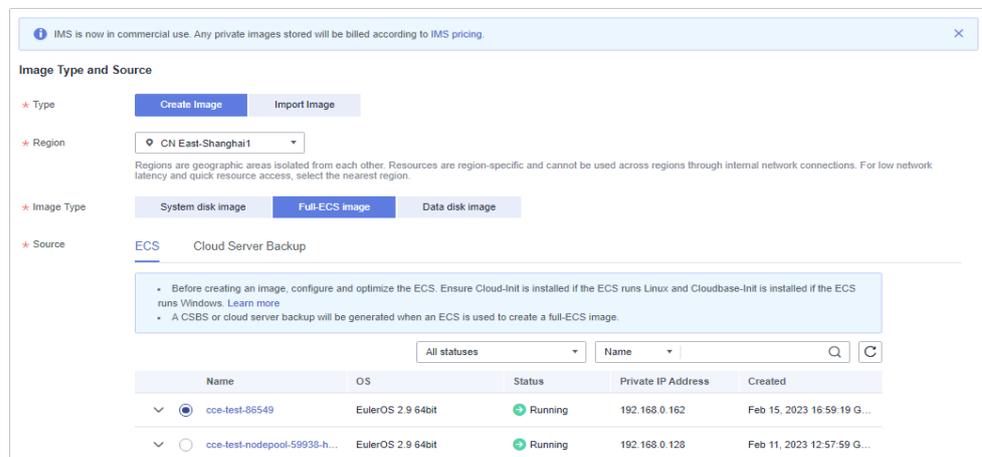
Paso 1 Acceda a la consola IMS.

1. Inicie sesión en la consola de gestión.
2. En **Compute**, haga clic en **Image Management Service**.
Se muestra la consola IMS.

Paso 2 Crear una imagen completa de ECS.

1. Haga clic en **Create Image** en la esquina superior derecha.
2. En el área **Image Type and Source**, seleccione **Create Image** para **Type** y, a continuación, seleccione **Full-ECS image** para **Image Type**.
3. Seleccione **ECS** para **Source** y, a continuación, seleccione un ECS de la lista.

Figura 2-13 Creación de una imagen ECS completa con un ECS



4. Especifique **Server Backup Vault** para almacenar las copias de respaldo.
La imagen de ECS completa creada y la copia de respaldo se almacenan en el almacén de copia de respaldo del servidor.
Si no hay ningún almacén de copia de respaldo del servidor disponible, haga clic en **Create Server Backup Vault** para crear uno. Asegúrese de seleccionar **Backup** para **Protection Type**. Para obtener más información acerca de las copias de respaldo y los almacenes de CBR, vea [¿Qué es el CBR?](#)
5. En el área **Image Information**, configure los detalles básicos de la imagen, como el nombre y la descripción de la imagen.
6. Haga clic en **Next**.
7. Confirme la configuración. Lea el descargo de responsabilidad de la imagen y seleccione **I have read and agree to the Image Disclaimer**, y haga clic en **Submit**.

Paso 3 Vuelva a la página de **Private Images** y vea la nueva imagen completa de ECS.

- Cuando el estado de la imagen cambia a **Normal**, la creación de la imagen se completa.
- Si **Available in AZX** aparece en **Normal** en la columna **Status** para una imagen completa del ECS, no se ha creado la copia de respaldo de este ECS y solo se crea una instantánea de disco. (**AZX** indica la zona de disponibilidad donde reside el ECS de origen de la imagen.)

En este caso, la imagen completa del ECS se puede utilizar para aprovisionar ECS solo en la zona de disponibilidad especificada. Si desea utilizar esta imagen para aprovisionar

ECS en otras zonas de disponibilidad de la región, debe esperar hasta que **Available in AZX** desaparezca de debajo de **Normal**, lo que indica que la copia de respaldo ECS se ha creado correctamente. Este proceso dura aproximadamente 10 minutos, dependiendo del volumen de datos del ECS de origen.

Figura 2-14 Estado de la imagen completa de ECS

<input type="checkbox"/> Name	Status	OS Type	OS	Image Type
<input type="checkbox"/> full-image-ecs-00	Normal Available in AZ1	Linux	Ubuntu 16.04 server 64bit	Full-ECS image(x86)

----Fin

Procedimiento posterior

- Si desea utilizar la imagen completa del ECS para crear ECS, haga clic en **Apply for Server** en la columna **Operation**. En la página mostrada, cree ECS siguiendo las instrucciones de *Guía de usuario de Elastic Cloud Server*.

NOTA

Cuando se utiliza una imagen completa del ECS para crear un ECS:

- La información del sistema y del disco de datos predeterminada por la imagen se mostrará automáticamente.
- Si la imagen completa del ECS contiene varios discos de datos, se necesita algún tiempo para cargar y mostrar la información del disco.
- Si utiliza una imagen completa del ECS para cambiar un sistema operativo de ECS, solo los datos del disco del sistema pueden ser escritos en el ECS. Por lo tanto, si desea restaurar o migrar los datos del disco de datos de un ECS usando una imagen completa del ECS, solo puede usar la imagen para crear un nuevo ECS en lugar de usarla para cambiar el sistema operativo de ECS.
- Si desea compartir la imagen completa de ECS con otros tenants, puede utilizar cualquiera de los siguientes métodos:
 - Si el ECS desde el que se creó la imagen completa del ECS tiene una copia de respaldo de CSBS, primero debe migrar la copia de respaldo a ECS antes de compartir la imagen porque CSBS está siendo obsoleta. Para obtener más información, consulte [Migración de recursos desde CSBS/VBS](#).
 - Si el ECS no tiene una copia de respaldo de este tipo, puede compartir la imagen completa de ECS directamente.

2.9 Creación de una imagen completa de ECS a partir de una copia de respaldo de CSBS

Escenarios

Crear una imagen completa del ECS a partir de una copia de respaldo CSBS. Esta imagen se puede utilizar para crear ECS.

NOTA

CSBS está siendo reemplazado gradualmente por CBR. Si **CSBS Backup** no está disponible para **Source**, seleccione otro origen de imagen.

Antecedentes

- Si utiliza una copia de respaldo CSBS para crear una imagen completa de ECS, solo se le cobrará por la copia de respaldo CSBS. Para obtener precios detallados del servicio, consulte **Cloud Server Backup Service** en [Detalles de precio de producto](#).
- Al eliminar una imagen de ECS completa, puede elegir si desea eliminar la copia de respaldo de CSBS asociada. Si decide no eliminar la copia de respaldo de CSBS, se le seguirá cobrando por ella.
- Si utiliza una imagen completa del ECS para cambiar un sistema operativo de ECS, solo los datos del disco del sistema pueden ser escritos en el ECS. Por lo tanto, si desea restaurar o migrar los datos del disco de datos de un ECS usando una imagen completa del ECS, solo puede usar la imagen para crear un nuevo ECS en lugar de usarla para cambiar el sistema operativo de ECS.

Restricciones

- Al crear una imagen de ECS completo a partir de una copia de respaldo de CSBS, asegúrese de que el ECS de origen de la copia de respaldo de CSBS se haya configurado correctamente, o la creación de la imagen puede fallar.
Para obtener más información, consulte [¿Cómo configuro un ECS, BMS o archivo de imagen antes de usarlo para crear una imagen?](#)
- Si un ECS está en estado **Stopped**, no lo inicie cuando lo esté usando para crear una imagen completa del ECS.
- Una copia de respaldo CSBS utilizada para crear una imagen ECS completa no puede tener discos compartidos.
- Solo se puede usar una copia de respaldo CSBS disponible para crear una imagen completa de ECS. Una copia de respaldo de CSBS se puede utilizar para crear solo una imagen completa de ECS.
- Una imagen completa del ECS no se puede exportar, publicar en Marketplace o replicar dentro de una región.

Procedimiento

Paso 1 Acceda a la consola IMS.

1. Inicie sesión en la consola de gestión.
2. En **Compute**, haga clic en **Image Management Service**.
Se muestra la consola IMS.

Paso 2 Crear una imagen completa de ECS.

1. Haga clic en **Create Image** en la esquina superior derecha.
2. En el área **Image Type and Source**, seleccione **Create Image** para **Type** y, a continuación, seleccione **Full-ECS image** para **Image Type**.
3. Seleccione **CSBS Backup** para **Source** y, a continuación, seleccione una copia de respaldo de la lista.

4. En el área **Image Information**, configure los detalles básicos de la imagen, como el nombre y la descripción de la imagen.
5. Haga clic en **Next**.
6. Confirme la configuración. Lea el descargo de responsabilidad de la imagen y seleccione **I have read and agree to the Image Disclaimer**, y haga clic en **Submit**.

Paso 3 Vuelva a la página **Image Management Service** para monitorear el estado de la imagen.

Cuando el estado de la imagen cambia a **Normal**, la creación de la imagen se completa.

----Fin

Procedimiento posterior

- Si desea utilizar la imagen completa del ECS para crear ECS, haga clic en **Apply for Server** en la columna **Operation**. En la página mostrada, cree ECS siguiendo las instrucciones de *Guía de usuario de Elastic Cloud Server*.

NOTA

Cuando se utiliza una imagen completa del ECS para crear un ECS:

- La información del sistema y del disco de datos predeterminada por la imagen se mostrará automáticamente.
- Si la imagen completa del ECS contiene varios discos de datos, se necesita algún tiempo para cargar y mostrar la información del disco.
- Si utiliza una imagen completa del ECS para cambiar un sistema operativo de ECS, solo los datos del disco del sistema pueden ser escritos en el ECS. Por lo tanto, si desea restaurar o migrar los datos del disco de datos de un ECS usando una imagen completa del ECS, solo puede usar la imagen para crear un nuevo ECS en lugar de usarla para cambiar el sistema operativo de ECS.
- Si desea compartir una imagen completa del ECS con otros tenants, primero debe migrar la copia de respaldo asociada a ECS porque solo se pueden compartir las imágenes completas de ECS creadas a partir de copias de respaldo de ECS. Para obtener más información, consulte [Migración de recursos desde CSBS/VBS](#).

2.10 Creación de una imagen completa de ECS a partir de una copia de respaldo de CBR

Escenarios

Puede utilizar una copia de respaldo de Cloud Backup and Recovery (CBR) para crear una imagen completa del ECS, que puede utilizarse para crear ECSs.

Antecedentes

- El servicio CBR brinda servicios de copia de respaldo para discos de EVS, BMS, y ECS y admite restauración de datos de servidores y discos mediante copias de respaldo. Si ha creado una copia de respaldo para un ECS mediante CBR, puede utilizarla para crear una imagen completa del ECS.
- Si utiliza una copia de respaldo de CBR para crear una imagen de ECS completa, solo se le cobrará por la copia de respaldo de CBR. Para obtener detalles sobre precios, consulte "Cloud Backup and Recovery" en [Detalles de precio de producto](#).

- Al eliminar una imagen completa de ECS, puede elegir si desea eliminar la copia de respaldo de CBR asociada. Si decide no eliminar la copia de respaldo de CBR, se le seguirá cobrando por ella.
- Si utiliza una imagen completa del ECS para cambiar un sistema operativo de ECS, solo los datos del disco del sistema pueden ser escritos en el ECS. Por lo tanto, si desea restaurar o migrar los datos del disco de datos de un ECS usando una imagen completa del ECS, solo puede usar la imagen para crear un nuevo ECS en lugar de usarla para cambiar el sistema operativo de ECS.

Restricciones

- Al crear una imagen completa del ECS a partir de una copia de respaldo de CBR, asegúrese de que el ECS de origen de la copia de respaldo de CBR se haya configurado correctamente, o la creación de la imagen podría fallar.
Para obtener más información, consulte [¿Cómo configuro un ECS, BMS o archivo de imagen antes de usarlo para crear una imagen?](#)
- Se puede utilizar una copia de respaldo de CBR para crear una sola imagen completa del ECS.
- Si un ECS está en estado **Stopped**, no lo inicie cuando lo esté usando para crear una imagen completa del ECS.
- Una imagen de ECS completa creada a partir de una copia de respaldo de CBR se puede compartir con otros tenants. Sin embargo, si se trata de una copia de respaldo de CBR compartida, la imagen de ECS completa creada a partir de ella no se puede compartir.
- Una imagen completa del ECS no se puede exportar, publicar en Marketplace o replicar dentro de una región.

Procedimiento

Paso 1 Acceda a la consola IMS.

1. Inicie sesión en la consola de gestión.
2. En **Compute**, haga clic en **Image Management Service**.
Se muestra la consola IMS.

Paso 2 Crear una imagen completa de ECS.

1. Haga clic en **Create Image** en la esquina superior derecha.
2. En el área **Image Type and Source**, seleccione **Create Image** para **Type** y, a continuación, seleccione **Full-ECS image** para **Image Type**.
3. Seleccione **Cloud Server Backup** para **Source** y, a continuación, seleccione un ECS de la lista.
4. En el área **Image Information**, configure los detalles básicos de la imagen, como el nombre y la descripción de la imagen.
5. Haga clic en **Next**.
6. Confirme las configuraciones. Lea el descargo de responsabilidad de la imagen y seleccione **I have read and agree to the Image Disclaimer**, y haga clic en **Submit**.

Paso 3 Vuelva a la página **Image Management Service** para monitorear el estado de la imagen.

Cuando el estado de la imagen cambia a **Normal**, la creación de la imagen se completa.

----Fin

Procedimiento posterior

Una vez completada la creación de la imagen completa de ECS, puede realizar las siguientes operaciones:

- Si desea utilizar la imagen para crear ECS, haga clic en **Apply for Server** en la columna **Operation**. En la página mostrada, seleccione **Private image** y, a continuación, seleccione la imagen completa de ECS creada. Para obtener más información, consulte [Compra de un ECS](#).

NOTA

Cuando se utiliza una imagen completa del ECS para crear un ECS:

- La información del sistema y del disco de datos predeterminada por la imagen se mostrará automáticamente.
- Si la imagen completa del ECS contiene varios discos de datos, se necesita algún tiempo para cargar y mostrar la información del disco.
- Si desea compartir la imagen con otros tenants, haga clic en **More** en la columna **Operation** y seleccione **Share** en la lista desplegable. En el cuadro de diálogo que se muestra, introduzca los ID de proyecto de los destinatarios de la imagen. Para obtener más información, consulte [Compartir imágenes especificadas](#).
- Si utiliza una imagen completa del ECS para cambiar un sistema operativo de ECS, solo los datos del disco del sistema pueden ser escritos en el ECS. Por lo tanto, si desea restaurar o migrar los datos del disco de datos de un ECS usando una imagen completa del ECS, solo puede usar la imagen para crear un nuevo ECS en lugar de usarla para cambiar el sistema operativo de ECS.
- Si desea replicar la imagen en otra región, haga clic en **More** en la columna **Operation** y seleccione **Replicate** en el cuadro de lista desplegable. En el cuadro de diálogo que se muestra, mantenga **Across Regions** y establezca otros parámetros, como **Name** y **Destination Region**. Para obtener más información, véase [Replicación de imágenes entre regiones](#).

2.11 Creación de una imagen de disco de sistema Windows a partir de un archivo ISO

2.11.1 Descripción

Un archivo ISO es una imagen de disco de un disco óptico. Un gran número de archivos de datos se pueden comprimir en un solo archivo ISO. Del mismo modo, para acceder a los archivos almacenados en una ISO, el archivo ISO debe descomprimirse. Por ejemplo, puede utilizar un CD-ROM virtual para abrir un archivo ISO o grabar el archivo ISO en un CD o DVD y, a continuación, utilizar el CD-ROM para leer la imagen.

En esta sección se describe cómo crear una imagen de disco del sistema Windows a partir de un archivo ISO.

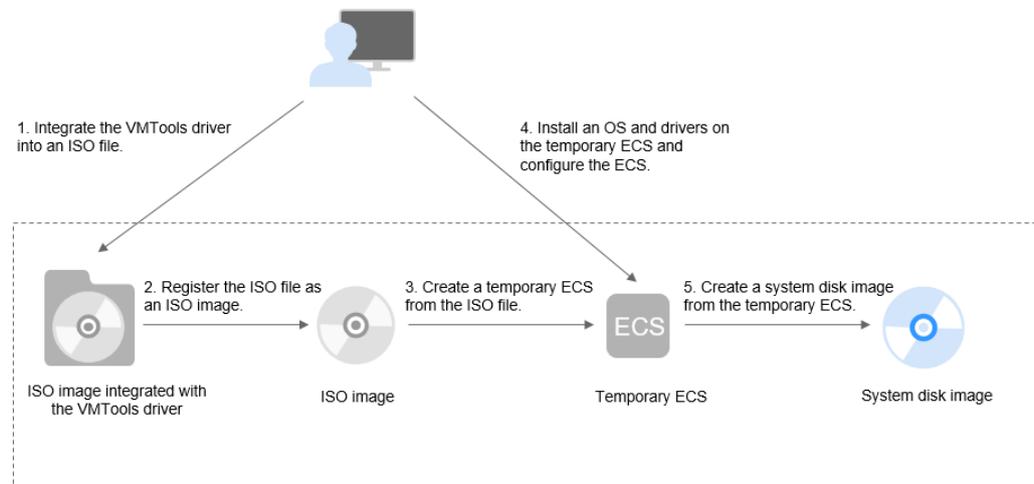
NOTA

Esta sección solo es aplicable a la consola de gestión. Si es usuario de API, consulte [Creación de una imagen a partir de un archivo de ISO](#).

Proceso de creación

Figura 2-15 muestra el proceso de creación de una imagen de disco del sistema Windows a partir de un archivo ISO.

Figura 2-15 Creación de una imagen de disco del sistema Windows



El procedimiento es el siguiente:

1. Integre el controlador VMTools en el archivo ISO.
Windows utiliza el disco IDE y NIC de VirtIO. Antes de registrar una imagen en la plataforma en la nube, integre el controlador VMTools en el archivo ISO de Windows. Para obtener más información, véase [Integración del controlador VMTools en un archivo ISO](#).
2. Registre el archivo ISO como una imagen ISO.
En la consola de gestión, registre el archivo ISO que tiene integrado el controlador VMTools como una imagen. La imagen es una imagen ISO y no se puede utilizar para aprovisionar ECS. Para obtener más información, véase [Registro de un archivo ISO como una imagen ISO](#).
3. Cree un ECS temporal a partir de la imagen ISO.
Utilice la imagen ISO registrada para crear un ECS temporal. El ECS no tiene ningún sistema operativo o controlador instalado. Para obtener más información, véase [Creación de un ECS de Windows a partir de una imagen ISO](#).
4. Instale un sistema operativo y los controladores necesarios para el ECS temporal y configure los parámetros relacionados.
Las operaciones incluyen la instalación de un sistema operativo, controlador PV, y un controlador VMTools, así como la configuración de atributos. Para obtener más detalles, consulte [Instalación de un sistema operativo Windows y el controlador VMToolsVirtIO](#) y [Paso 1 en Configuración del ECS y creación de una imagen de disco del sistema Windows](#).
5. Cree una imagen de disco del sistema a partir del ECS temporal.
En la consola de gestión, cree una imagen de disco del sistema a partir del ECS temporal en el que se han completado la instalación y la configuración. Una vez creada la imagen, elimine el ECS temporal para evitar que se generen cargos adicionales. Para obtener más

información, véase [Creación de una imagen de disco del sistema desde un ECS de Windows](#).

Restricciones

- Una imagen ISO creada a partir de un archivo ISO solo se utiliza para crear un ECS temporal. No estará disponible en la consola de ECS. No se puede utilizar para crear ECS o cambiar el sistema operativo de ECS. Es necesario instalar un sistema operativo en el ECS temporal y utilizar ese ECS para crear una imagen de disco del sistema que se puede utilizar para crear ECS o cambiar SO de ECS.
- Un ECS temporal tiene una funcionalidad limitada. Por ejemplo, no puede conectar discos a él. No se recomienda usarlo como un ECS normal.

2.11.2 Integración del controlador VMTtools en un archivo ISO

Escenarios

En la nube se utiliza un sistema de Windows con el disco duro de Electrónica integrada de unidades (IDE) y Virtio NIC. Por lo tanto, debe integrar el controlador VMTtools en el archivo ISO de Windows antes de registrar una imagen en la plataforma en la nube. Normalmente, un archivo ISO contiene todos los archivos que se incluirían en un disco óptico. Algunos softwares solo se pueden instalar desde una unidad de CD-ROM. Por lo tanto, se requiere una unidad de CD-ROM virtual.

Esta sección utiliza AnyBurn y UltraISO como ejemplos para describir cómo integrar el controlador VMTtools en un archivo ISO.

NOTA

- AnyBurn es un software ligero de grabación de CD/DVD/Blu-ray con una versión gratuita.
- UltraISO es una herramienta de manejo de archivos de imagen ISO CD/DVD. Una versión de prueba gratuita está limitada a archivos ISO de 300 MB o menos. Se recomienda comprar una versión estándar.

Prerrequisitos

Usted ha obtenido un archivo ISO.

NOTA

El nombre del archivo ISO solo puede contener letras, dígitos, guiones (-) y guiones bajos (_). Si el nombre no cumple con los requisitos, cámbielo.

AnyBurn

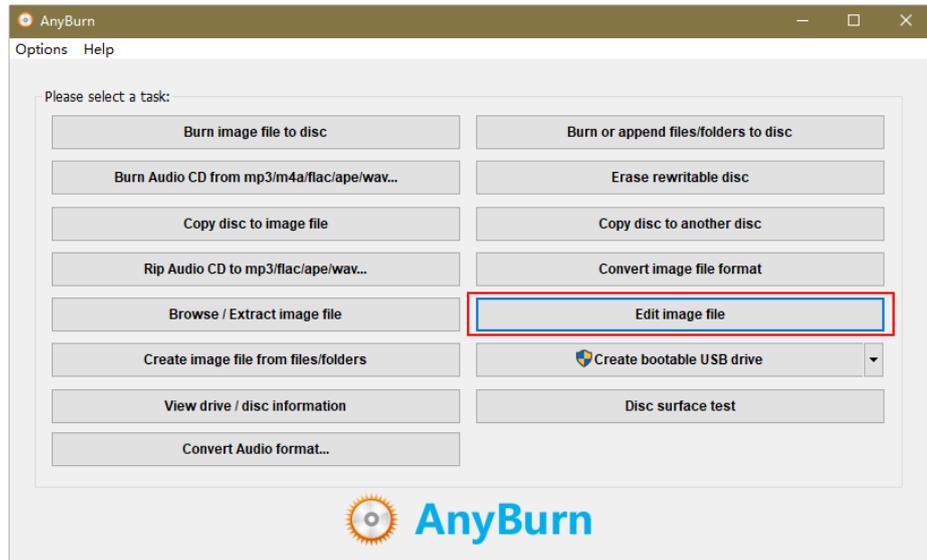
1. Descargue [AnyBurn](#) e instálelo en su PC local.
2. Descargue el paquete de controladores de VMTtools y descomprima en su PC local.

Descargue el paquete desde <https://ecs-instance-driver.obs.cn-north-1.myhuaweicloud.com/vmttools-windows.zip>.

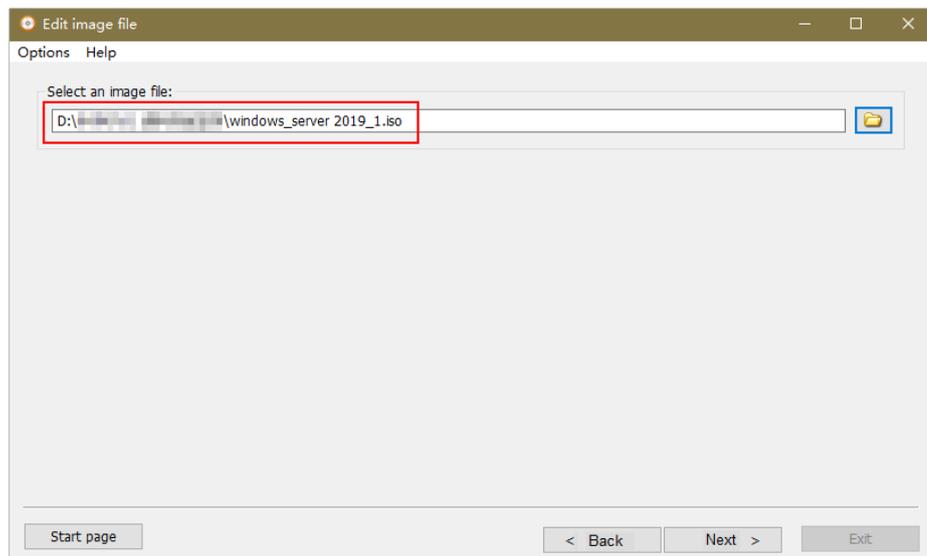
Para la asignación entre las versiones de Windows y los paquetes de VMTtools, consulte [Obtención de paquetes de software requeridos](#).

3. Utilice AnyBurn para abrir el archivo ISO.

- a. Abra AnyBurn y seleccione **Edit Image File**.

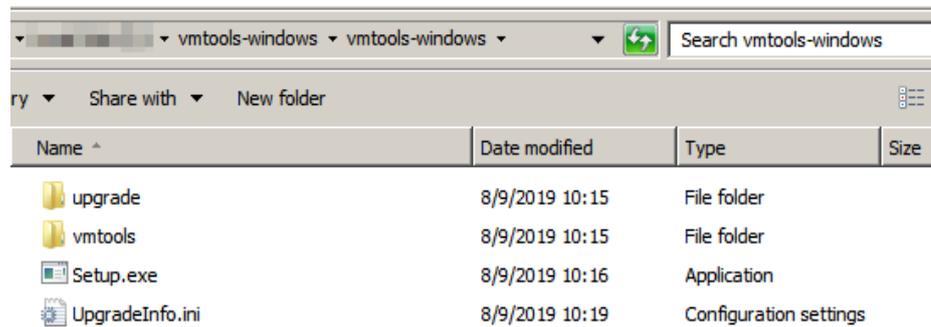


- b. Seleccione el archivo ISO y haga clic en **Next**.

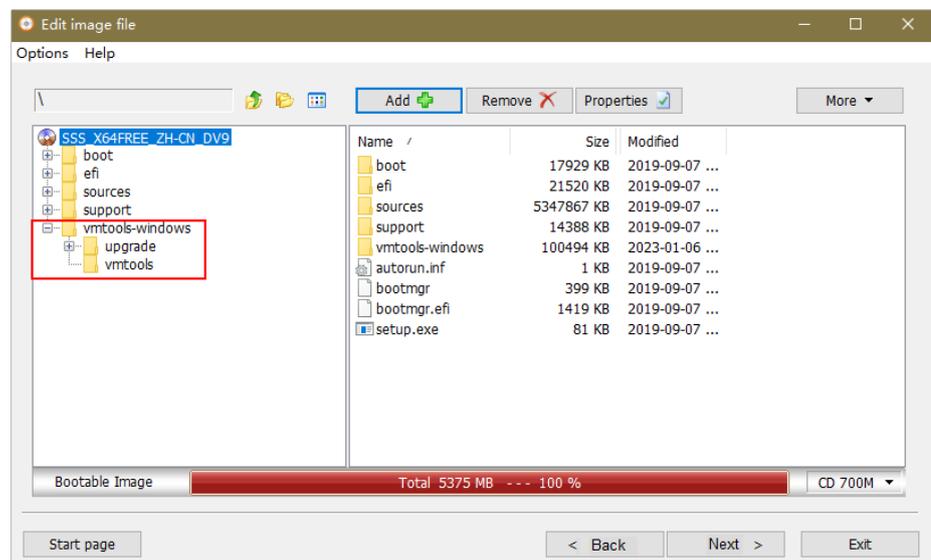


4. Edite el archivo ISO para integrar el controlador VMTools en él.
- a. Descomprima el archivo **vmtools-windows.zip** descargado a 2 para obtener **vmtools-windows.iso** y, a continuación, descomprima **vmtools-windows.iso** para obtener la carpeta **vmtools-windows**.

Figura 2-16 carpeta **vmtools-windows**

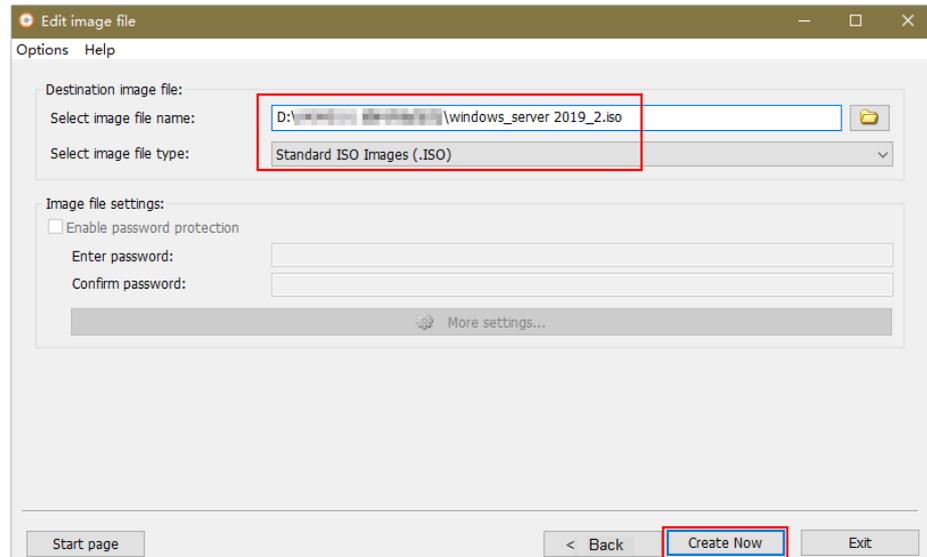


- b. Arrastre y suelte la carpeta **vmtools-windows** al nodo principal del archivo ISO (o haga clic en **Add** y seleccione la carpeta para agregarla al nodo principal) y haga clic en **Next**.



- c. Seleccione una ruta para guardar el nuevo archivo ISO y especifique un nombre para el nuevo archivo. Seleccione **ISO** como tipo de archivo. Haga clic en **Create Now**.

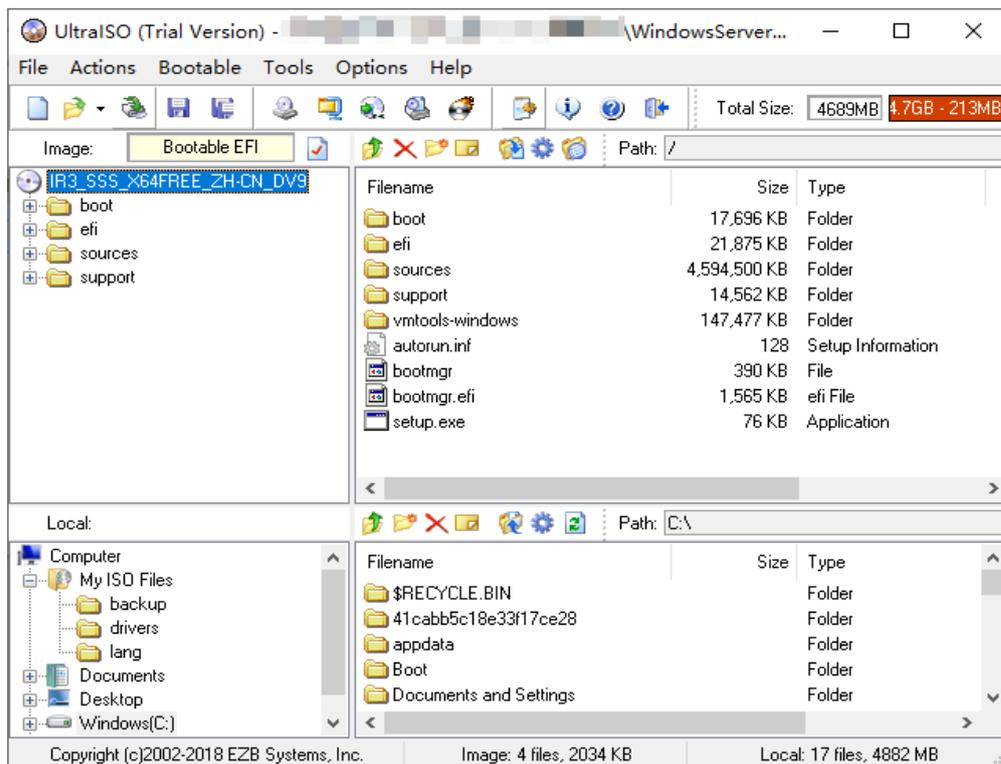
Después de generar el nuevo archivo ISO, vea el controlador VMTools en él.



UltraISO

1. Descargue UltraISO e instálelo en su PC local.
Dirección de descarga: <https://www.ultraiso.com/>
2. Descargue el paquete de controladores de VMTools y descomprima en su PC local.
Descargue el paquete desde <https://ecs-instance-driver.obs.cn-north-1.myhuaweicloud.com/vmtools-windows.zip>.
Para la asignación entre las versiones de Windows y los paquetes de VMTools, consulte [Obtención de paquetes de software requeridos](#).
3. Utilice UltraISO para abrir el archivo ISO.

Figura 2-17 Apertura del archivo ISO

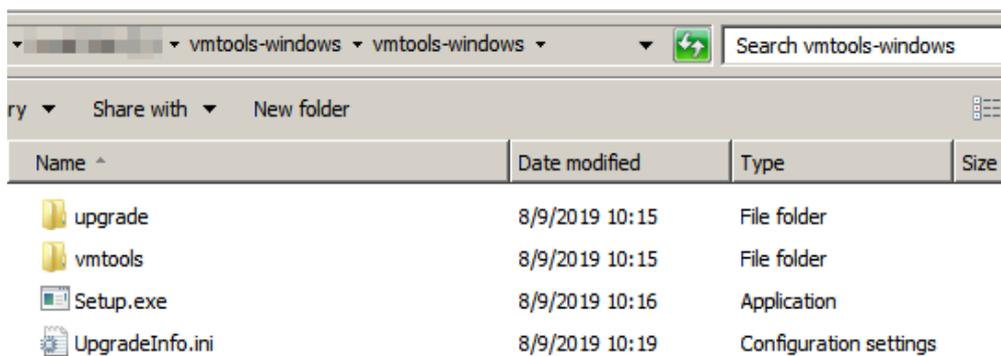


⚠ ATENCIÓN

No extraiga el archivo ISO ni lo abra con alguna herramienta que no sea UltraISO, o los datos de arranque se perderán.

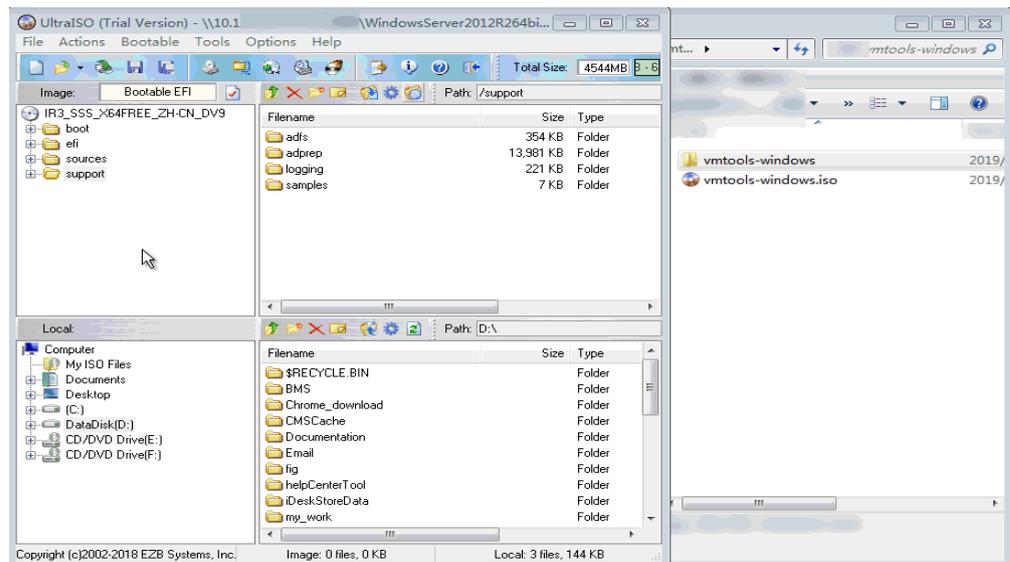
- Descomprima el archivo **vmtools-windows.zip** descargado a **2** para obtener **vmtools-windows.iso** y, a continuación, descomprima **vmtools-windows.iso** para obtener la carpeta **vmtools-windows**.

Figura 2-18 carpeta **vmtools-windows**



- Arrastre y suelte la carpeta **vmtools-windows** obtenida en **4** al nodo principal del archivo ISO.

Figura 2-19 Adición de la carpeta vmtools-windows al archivo ISO



6. Utilice UltraISO para exportar el archivo ISO con el controlador VMTools a un archivo .iso en su PC local.

2.11.3 Registro de un archivo ISO como una imagen ISO

Escenarios

Registre un archivo ISO externo en la plataforma en la nube como una imagen privada (imagen ISO). Antes de registrar una imagen, cargue el archivo ISO exportado en [Integración del controlador VMTools en un archivo ISO](#) al bucket OBS.

La imagen ISO no se puede replicar, exportar o cifrar.

Prerrequisitos

- El archivo que se va a registrar debe estar en formato ISO.
- El archivo de imagen ISO se ha subido al bucket OBS. Para obtener más información, véase [Carga de un archivo de imagen externo](#).

Procedimiento

Paso 1 Acceda a la consola IMS.

1. Inicie sesión en la consola de gestión.
2. En **Compute**, haga clic en **Image Management Service**.
Se muestra la consola IMS.

Paso 2 Registre un archivo ISO como una imagen ISO.

1. Haga clic en **Create Image** en la esquina superior derecha.
2. En el área **Image Type and Source**, seleccione **Import Image** para **Type** y, a continuación, seleccione **ISO image** para **Image Type**.
3. En la lista de archivos de imagen, seleccione el bucket y, a continuación, el archivo de imagen.

Figura 2-20 Creación de una imagen privada a partir de un archivo ISO

Image Type and Source

* Type

* Region
Regions are geographic areas isolated from each other. Resources are region-specific and cannot be used across regions through internal network connections. For low network latency and quick resource access, select the nearest region.

* Image Type

* Select Image File

- The image file must be no greater than 128 GB. [Learn more](#)
- The private image created using an ISO file is unavailable on the ECS console. [Learn how to use an ISO image.](#)
- The created private image may be different from the source image file in format and size.
- Ensure that UVP VMTools has been integrated into the ISO file before using it to create an image.

Bucket Name	Storage Class	Created
ccc-charts-cn-east-3	Standard	Sep 01, 2022 15:37:57 GMT+08:00
bucket-	Standard	Jul 19, 2022 11:40:23 GMT+08:00

[Create Bucket](#)

4. En el área **Image Information**, establezca los siguientes parámetros.

Figura 2-21 Configuración de la información de la imagen

Image Information

Architecture

Boot Mode

The boot mode must be the same as that of the OS contained in the image file. Otherwise, ECSs created from this system disk image will fail to start.

OS

* System Disk (GB) Ensure that the system disk size is greater than the image file size.

* Name

* Enterprise Project

Tag It is recommended that you use TMS's predefined tag function to add the same tag to different cloud resources. [View predefined tags](#)

You can add 10 more tags.

Description

0/1,024

- **Architecture.** Seleccione **x86** o **ARM**.

NOTA

Este parámetro solo se requiere en regiones que admiten tanto x86 como Arm.

- **Boot Mode:** Seleccione **BIOS** o **UEFI**. Asegúrese de que el modo de arranque seleccionado es el mismo que en el archivo de imagen, o los ECS creados a partir de esta imagen no podrán arrancar. La arquitectura Arm no admite el modo de arranque del BIOS.

NOTA

Si el modo de arranque en el archivo de imagen es **BIOS**, pero selecciona aquí **UEFI** para **Boot Mode**, no podrá ajustar la resolución.

- **OS:** Seleccione el sistema operativo especificado en el archivo ISO. Para asegurarse de que la imagen se puede crear y utilizar correctamente, seleccione un sistema operativo compatible con el del archivo de imagen.
- **License Type:** Traiga su propia licencia (BYOL) es compatible. Si ha obtenido una licencia de sistema operativo, no necesita solicitar una licencia más.
- **System Disk:** Establezca la capacidad del disco del sistema (rango de valores: 40 GB a 1024 GB), que no debe ser menor que la capacidad del disco del sistema en el archivo de imagen.
- **Name:** Ingrese un nombre para la imagen que se va a crear.
- **Enterprise Project:** Seleccione el proyecto de empresa al que pertenecen las imágenes.
- **Tag:** (Optional) Add a tag to the image to be created.

NOTA

Si su organización ha configurado políticas de etiquetas para imágenes, debe agregar etiquetas a las imágenes en función de las políticas. Si agrega una etiqueta que no cumple con las políticas de etiquetas, es posible que las imágenes no se creen. Póngase en contacto con el administrador de la organización para obtener más información sobre las políticas de etiquetas.

- Cada etiqueta consiste en una clave y un valor. La clave contiene un máximo de 36 caracteres y el valor contiene un máximo de 43 caracteres. La clave no se puede dejar en blanco ni una cadena de caracteres vacía. El valor no se puede dejar en blanco, sino que puede ser una cadena de caracteres vacía.
 - Una imagen puede tener un máximo de 10 etiquetas.
- **Description:** (Opcional) Introduzca la descripción de la imagen según sea necesario.
5. Haga clic en **Next**.
 6. Confirme la configuración. Seleccione **Statement of Commitment to Image Creation** y **Huawei Image Disclaimer**. Haga clic en **Submit**.

Paso 3 Vuelva a la página **Image Management Service** para monitorear el estado de la imagen.

Cuando el estado de la imagen cambia a **Normal**, la imagen se registra correctamente.

----Fin

2.11.4 Creación de un ECS de Windows a partir de una imagen ISO

Escenarios

Esta sección describe cómo crear un ECS a partir de una imagen ISO registrada.

Restricciones

Los usuarios de Dedicated Cloud (DeC) no pueden crear ECS a partir de imágenes ISO.

Si el servicio **DeC** está habilitado para un usuario en una región especificada, el usuario será un usuario DeC. Para obtener más información, vea [¿Qué es DeC?](#)

Procedimiento

Paso 1 Acceda a la consola IMS.

1. Inicie sesión en la consola de gestión.
2. En **Compute**, haga clic en **Image Management Service**.
Se muestra la consola IMS.

Paso 2 Utilice una imagen ISO para crear un ECS de Windows.

1. Haga clic en la pestaña **Private Images**. Busque la fila que contiene la imagen ISO y haga clic en **Create ECS** en la columna **Operation**.

El ECS creado es solo para uso temporal y debe eliminarse cuando haya terminado con él. El sistema crea un ECS de pago por uso con especificaciones fijas. Cuando utilice la imagen privada creada a partir de este ECS para crear nuevos ECS, puede personalizar las especificaciones y el modo de facturación.

NOTA

Si es usuario de **DeC**, el botón **Create ECS** de la columna **Operation** no estará disponible para usted porque un usuario de DeC no puede utilizar una imagen ISO para crear un ECS.

2. Configure el ECS como se le solicite y haga clic en **OK**.

----Fin

Procedimiento posterior

Después de crear el ECS, puede iniciar sesión de forma remota para continuar con la instalación del sistema operativo y los controladores.

2.11.5 Instalación de un sistema operativo Windows y el controlador VMToolsVirtIO

Escenarios

Esta sección utiliza Windows Server 2008 R2 64-bit como ejemplo para describir cómo instalar Windows en un ECS.

El procedimiento de instalación varía en función del archivo de imagen que utilice. Realice las operaciones según se indique en la pantalla.

NOTA

Establezca la zona horaria, la dirección KMS, el servidor de parches, el método de entrada y el idioma según los requisitos del servicio.

Prerrequisitos

Ha iniciado sesión remotamente en el ECS y ha ingresado a la página de instalación.

Procedimiento

ATENCIÓN

No detenga ni reinicie el ECS durante la instalación del sistema operativo. De lo contrario, la instalación del sistema operativo fallará.

Paso 1 Instale el sistema operativo de Windows.

1. Especifique los parámetros en la página de **Install Windows**.

Figura 2-22 Instalar Windows



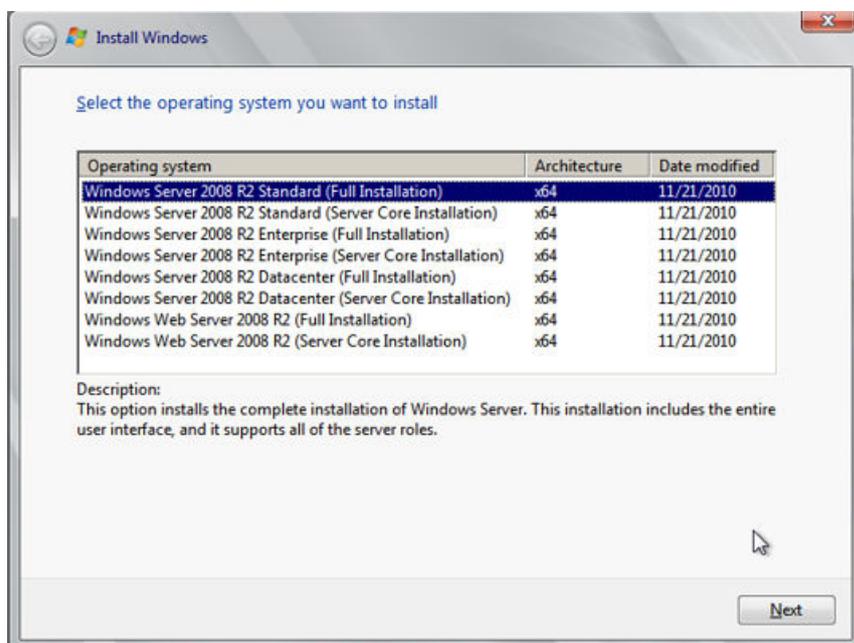
2. Haga clic en **Next**.
Aparece la ventana de confirmación de la instalación.

Figura 2-23 Ventana de confirmación de instalación



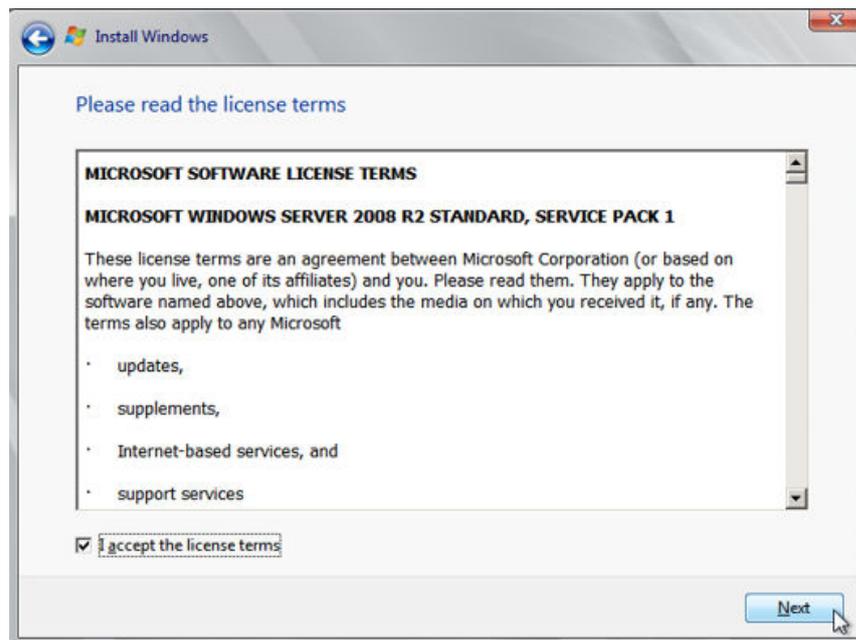
3. Haga clic en **Install now**.
Aparece la ventana **Select the operating system you want to install**.

Figura 2-24 Selección de la versión del sistema operativo



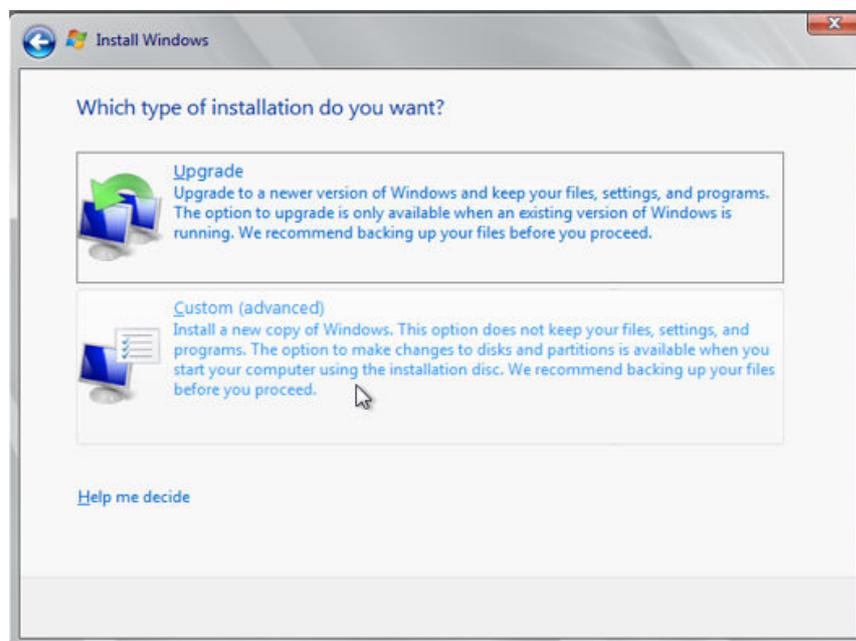
4. Seleccione la versión del sistema operativo que se va a instalar y haga clic en **Next**.
Se muestra la ventana **Please read the license terms**.

Figura 2-25 Ventana de términos de licencia



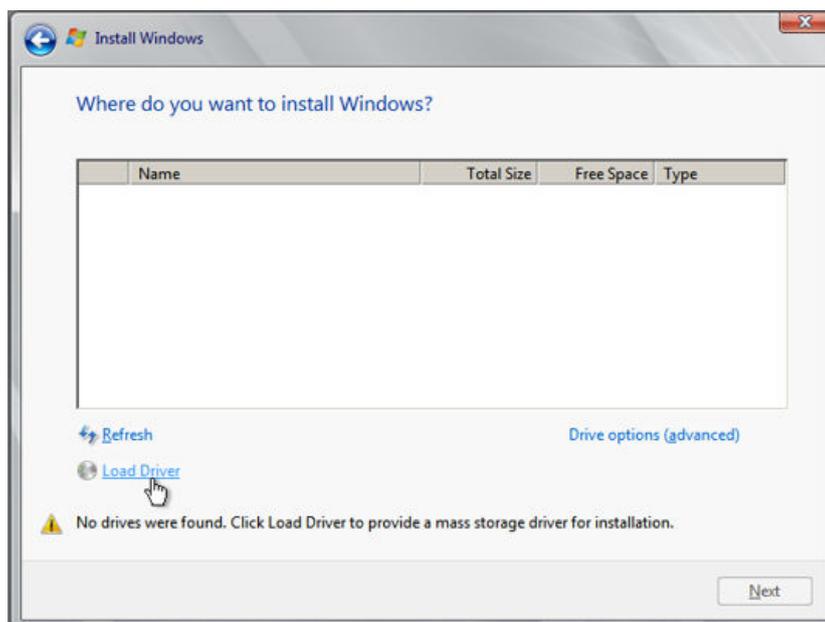
5. Seleccione **I accept the license terms** y haga clic en **Next**.
La ventana **Which type of installation do you want?** se muestra.

Figura 2-26 Tipo de instalación



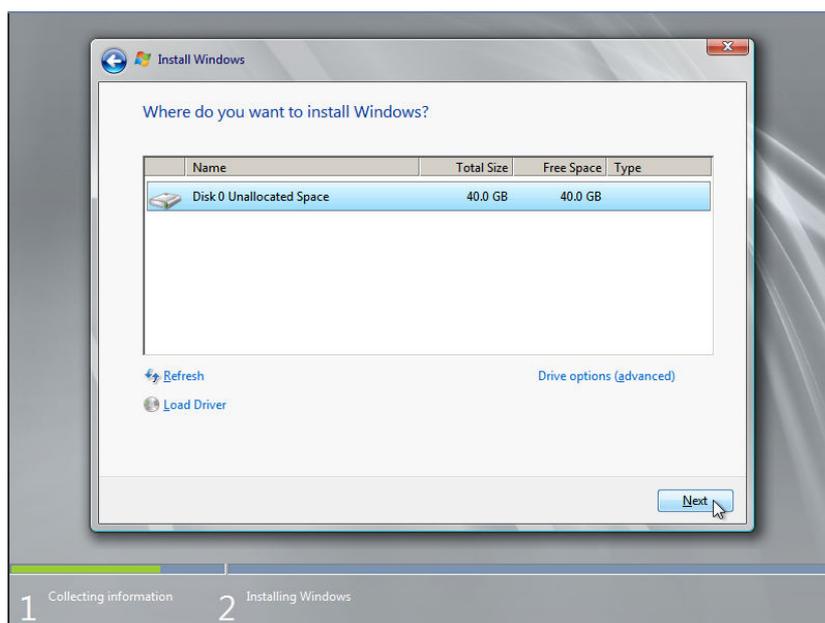
6. Seleccione **Custom (advanced)**.
La ventana **Where do you want to install Windows?** se muestra.
 - Si el sistema muestra un mensaje que indica que no se ha encontrado ningún controlador, vaya a **Paso 1.7**.

Figura 2-27 Ruta de instalación



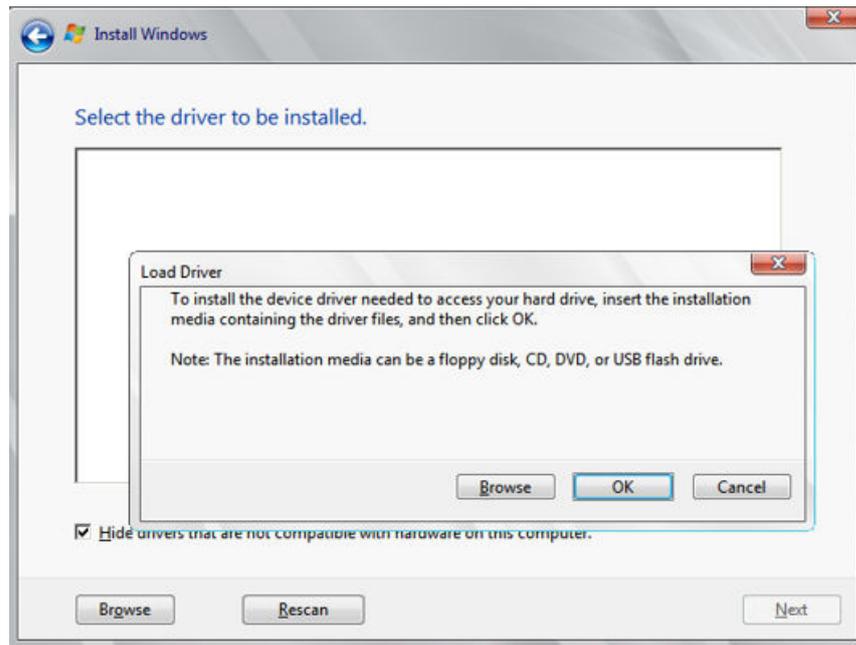
- Si se muestra un disco, vaya a **Paso 1.10**.

Figura 2-28 Ruta de instalación



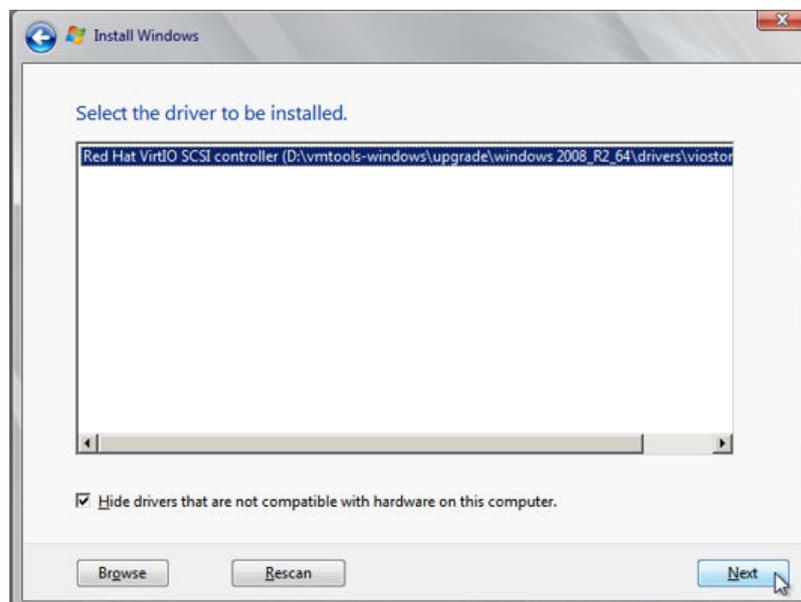
7. Haga clic en **Load Driver** y, a continuación, **Browse**.

Figura 2-29 Carga de controladores



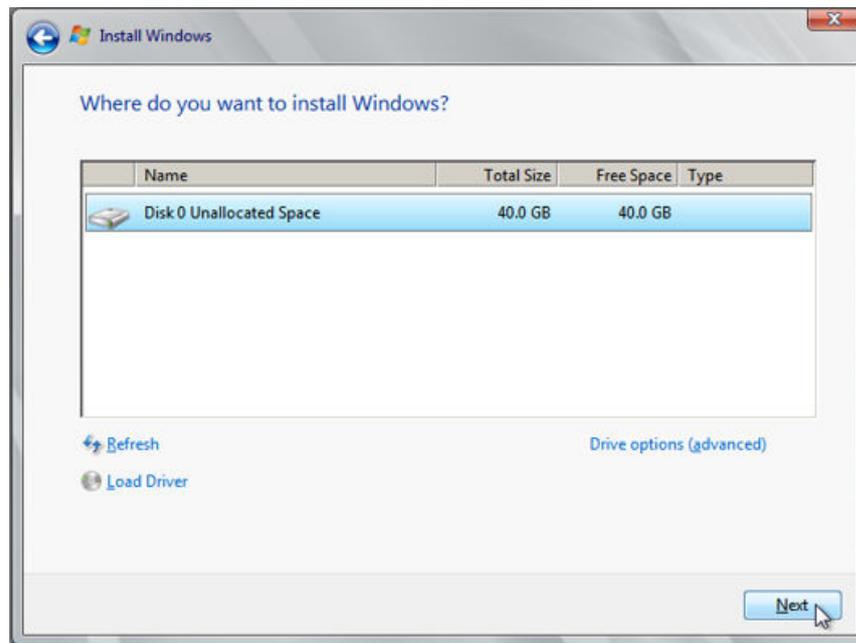
8. Elija la siguiente ruta y haga clic en **OK**.
vmtools-windows/upgrade/\$OS_Version/drivers/viostor
9. Seleccione el controlador que coincida con el sistema operativo y haga clic en **Next**.
El sistema puede proporcionar múltiples controladores. Seleccione **VISOTOR.INF** que se muestra en la siguiente figura.

Figura 2-30 Selección del controlador que se va a instalar



10. Seleccione el disco y haga clic en **Next**.

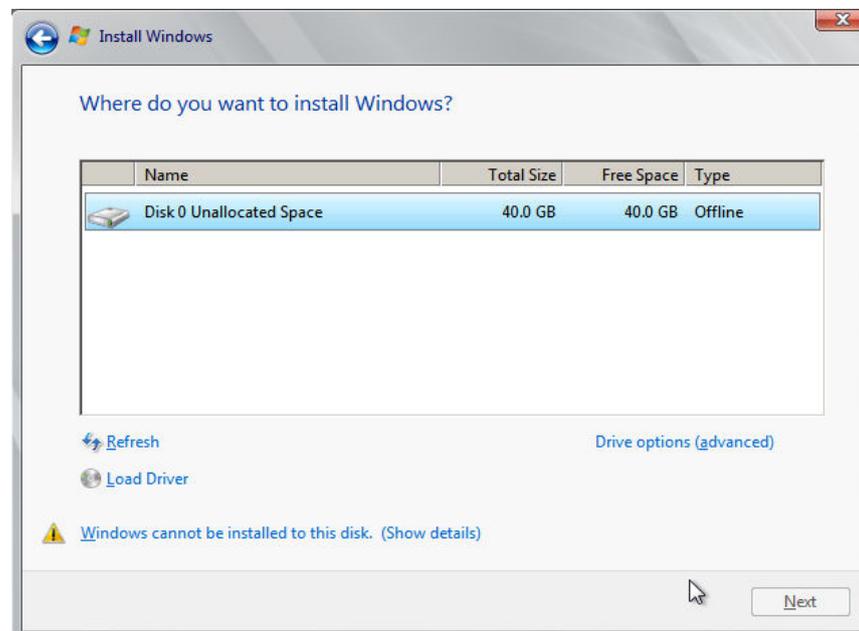
Figura 2-31 Ruta de instalación



NOTA

Si el tipo de disco es de **Offline**, puede detener y, a continuación, iniciar el ECS y reiniciar el proceso de instalación del sistema operativo.

Figura 2-32 Disco sin conexión



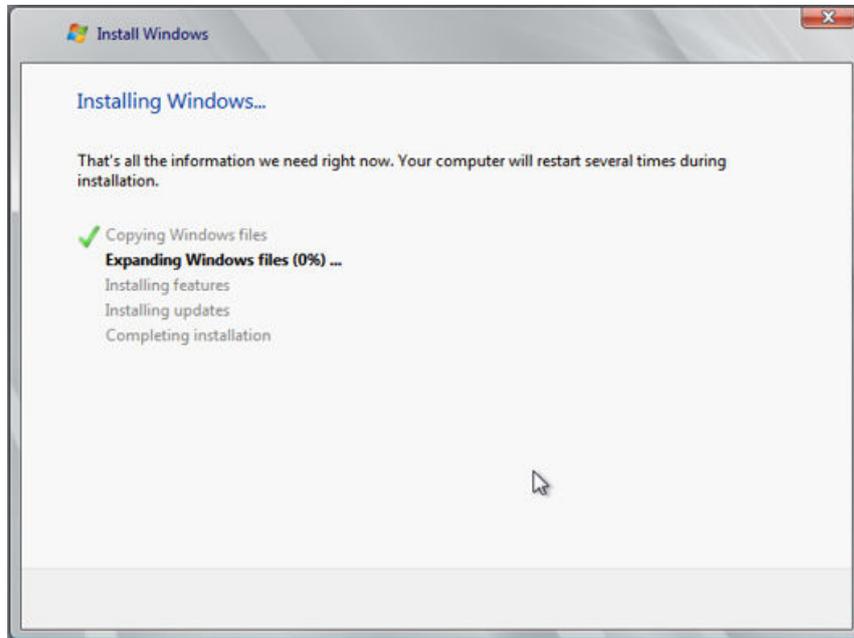
11. Se muestra la ventana **Installing Windows** y se inicia la instalación del sistema operativo.

La instalación dura unos 50 minutos. El ECS se reinicia durante la instalación. Después de que el ECS se reinicie correctamente, inicie sesión de nuevo y configure el sistema operativo como se le solicite.

 **NOTA**

Debe establecer una contraseña para el usuario del sistema operativo.
Caracteres especiales compatibles incluyen !@\$%^_-=+[{ }],;/?/

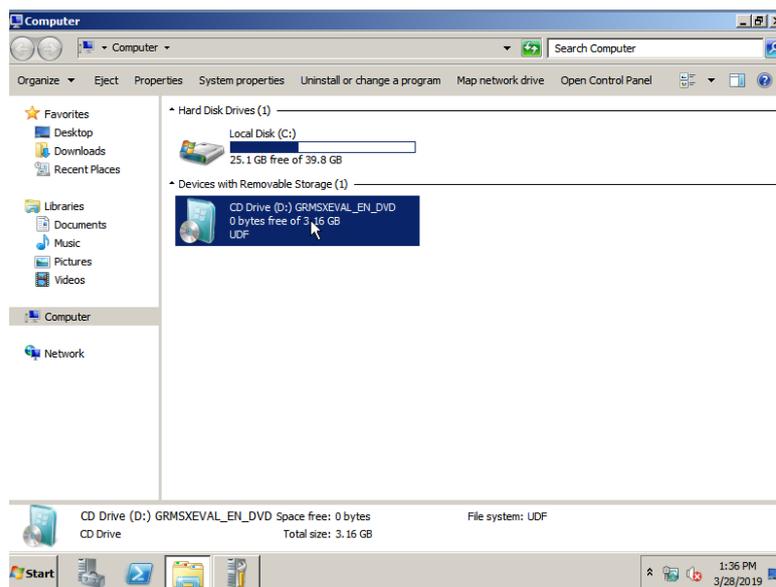
Figura 2-33 Progreso de instalación



Paso 2 Instale controladores relacionados.

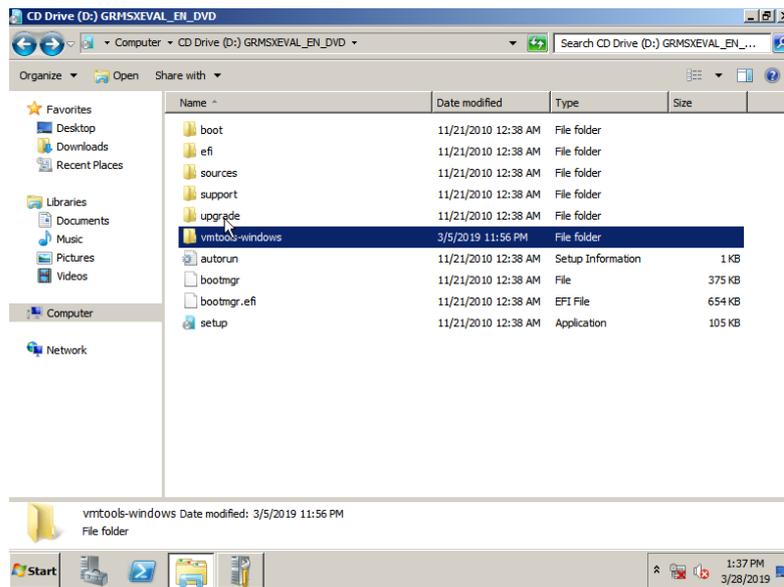
1. Abra **Computer** y haga doble clic en la unidad de CD.

Figura 2-34 Inicio de la unidad de CD



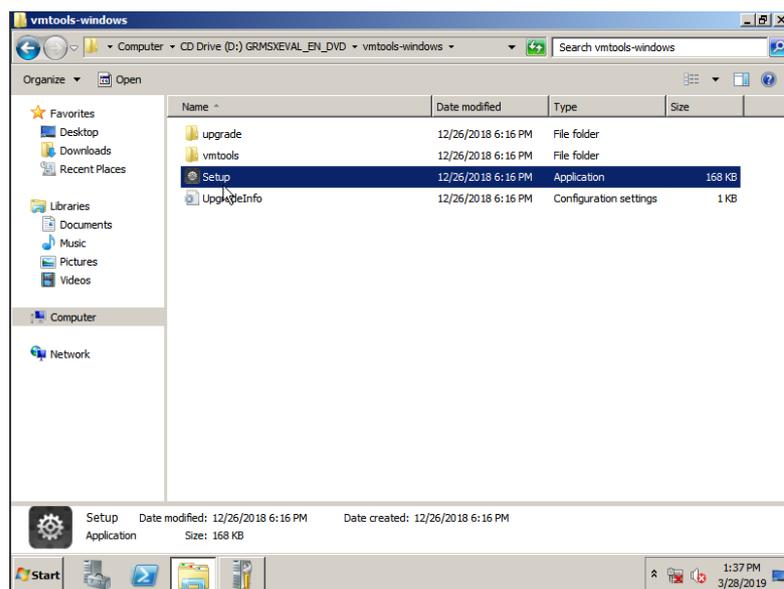
2. Haga doble clic en la carpeta **vmtools-windows**.

Figura 2-35 Abrir la carpeta **vmtools-windows**



3. Haga doble clic en el archivo de **Setup**.

Figura 2-36 Ejecución del archivo de instalación



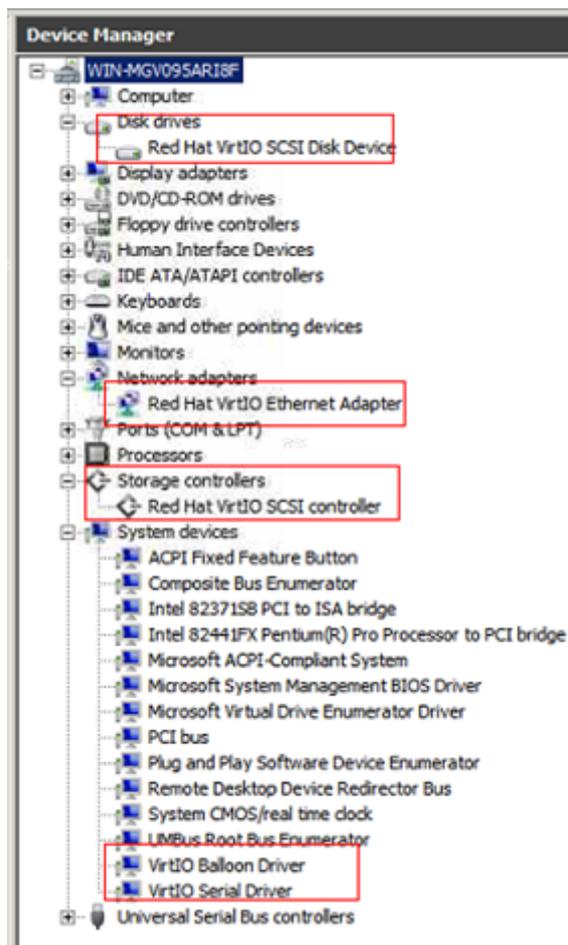
4. Instale el controlador como se le indique.

Figura 2-37 Instalación de UVP VMTools para Windows



5. Después de instalar el controlador, inicie el **Device Manager** y compruebe que los controladores que se muestran en el cuadro rojo de la siguiente figura se han instalado correctamente.

Figura 2-38 Device Manager

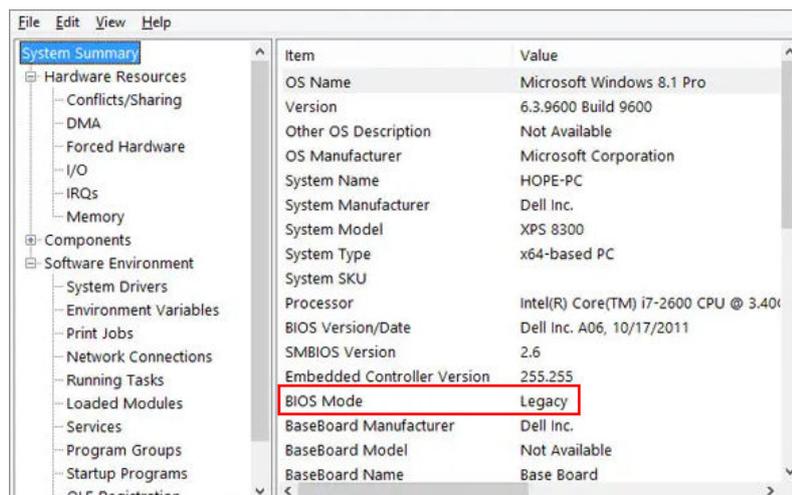


----Fin

Procedimiento posterior

Compruebe si se puede cambiar la resolución. Si no puede, diríjase en función de los modos de arranque del sistema.

Mantenga pulsada la tecla **Windows** y presione **R** en el teclado, escriba **msinfo32** en el cuadro **Run** y presione **Enter**. En el panel derecho del cuadro de diálogo **System Information**, busque **BIOS Mode**.



- Si el valor de **BIOS Mode** es de **Legacy**, el modo de arranque del sistema es BIOS. Vaya al paso para [configurar la información de la imagen](#), seleccione **BIOS** para **Boot Mode**.
- Si el valor de **BIOS Mode** es **UEFI**, solucione la falla de cambio consultando [¿Qué debo hacer si no puedo cambiar la resolución de un sistema operativo Windows iniciado en modo UEFI?](#)

2.11.6 Configuración del ECS y creación de una imagen de disco del sistema Windows

Escenarios

Después de instalar un sistema operativo para el ECS temporal, configure el ECS e instale los controladores del sistema operativo proporcionados por la plataforma en la nube para garantizar que los ECS creados posteriormente estén disponibles.

NOTA

Los controladores del Guest OS incluyen el UVP VMTools y el controlador PV. El UVP VMTools se instaló en el ECS en la sección anterior, por lo que esta sección solo describe cómo instalar el controlador PV.

Esta sección describe cómo configurar un ECS de Windows, instalar los controladores del sistema operativo y crear una imagen de disco del sistema Windows.

Procedimiento

Paso 1 Configurar el ECS.

1. Compruebe si las NIC están establecidas en DHCP. Si el ECS está configurado con una dirección IP estática, cambie el modo de asignación de direcciones IP a DHCP como se indica en [Configuración de NIC al DHCP](#).
2. Habilite la conexión de escritorio remoto para el ECS según sea necesario. Para obtener más información acerca de cómo habilitar esta función, consulte [Habilitación de la conexión a escritorio remoto](#).
3. Instale el PV driver. Para obtener más información, consulte [Instalación del controlador PV](#).

Después de instalar el controlador, debe borrar los registros del sistema. Para obtener más detalles, consulte [Borrar registros del sistema](#).

4. Instale y configure Cloudbase-Init. La inyección de datos de usuario en la consola de gestión solo estará disponible para los nuevos ECS creados a partir de la imagen después de instalar esta herramienta. Por ejemplo, puede utilizar la inyección de datos para definir la contraseña de inicio de sesión de un ECS nuevo. Para obtener más información, consulte [Instalación y configuración de Cloudbase-Init](#).
5. (Opcional) Configurar funciones de valor agregado.
 - Habilite múltiples colas de NIC. Para obtener más detalles, consulte [¿Cómo puedo hacer múltiples colas de NIC para una imagen?](#)
 - Configurar la asignación dinámica de direcciones IPv6. Para obtener más detalles, consulte [¿Cómo configuro un ECS para obtener direcciones IPv6 dinámicamente?](#)

Paso 2 Detenga el ECS para que las configuraciones surtan efecto.

Paso 3 Utilice el ECS para crear una imagen de disco del sistema Windows.

Para obtener más información, véase [Creación de una imagen de disco del sistema desde un ECS de Windows](#).

----Fin

Procedimiento posterior

Después de crear la imagen de disco del sistema, elimine el ECS temporal de manera oportuna para evitar generar cargos adicionales.

2.12 Creación de una imagen de disco de sistema Linux a partir de un archivo ISO

2.12.1 Descripción

Un archivo ISO es una imagen de disco de un disco óptico. Un gran número de archivos de datos se pueden comprimir en un solo archivo ISO. Del mismo modo, para acceder a los archivos almacenados en una ISO, el archivo ISO debe descomprimirse. Por ejemplo, puede utilizar un CD-ROM virtual para abrir un archivo ISO o grabar el archivo ISO en un CD o DVD y, a continuación, utilizar el CD-ROM para leer la imagen.

Esta sección describe cómo crear una imagen de disco de sistema Linux usando un archivo ISO.

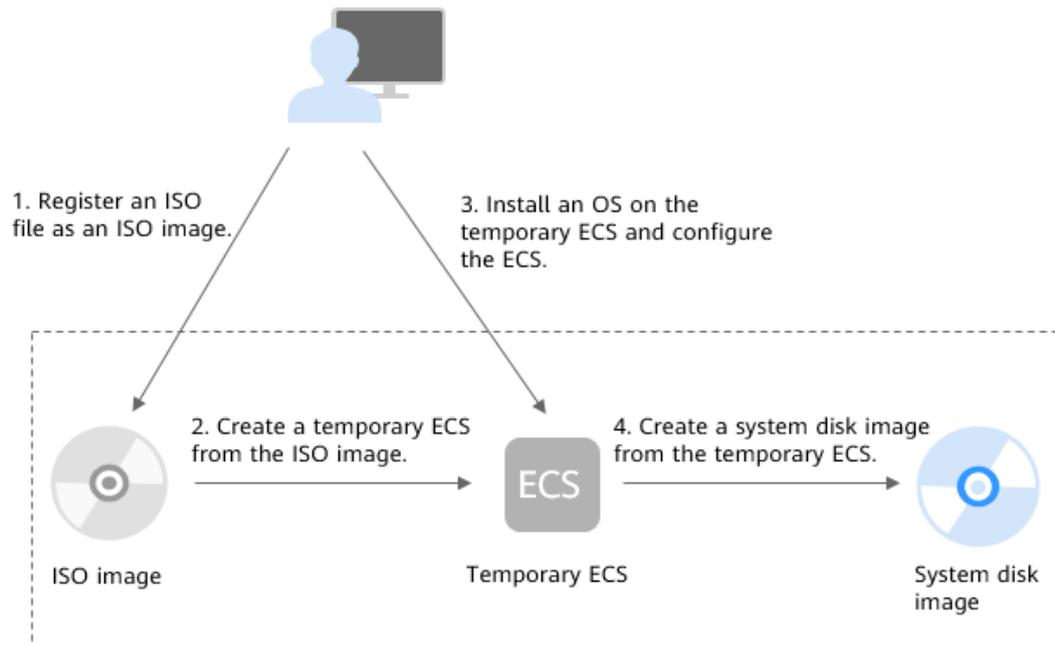
NOTA

Esta sección solo es aplicable a la consola de gestión. Si es usuario de API, consulte [Creación de una imagen a partir de un archivo de ISO](#).

Proceso de creación

Figura 2-39 muestra el proceso de crear una imagen de disco del sistema Linux a partir de un archivo ISO.

Figura 2-39 Creación de una imagen de disco del sistema Linux



El procedimiento es el siguiente:

1. Registre un archivo ISO como una imagen ISO.
En la consola de gestión, registre el archivo ISO preparado como una imagen. La imagen es una imagen ISO y no se puede utilizar para aprovisionar ECS. Para obtener más información, véase [Registro de un archivo ISO como una imagen ISO](#).
2. Cree un ECS temporal a partir de la imagen ISO.
Utilice la imagen ISO registrada para crear un ECS temporal. El ECS no tiene ningún sistema operativo o controlador instalado. Para obtener más información, véase [Creación de un ECS de Linux a partir de una imagen ISO](#).
3. Instale un sistema operativo y los controladores necesarios para el ECS temporal y configure los parámetros relacionados.
Las operaciones incluyen la instalación de un sistema operativo, la instalación de controladores nativos de Xen y KVM, la configuración de atributos de NIC y la eliminación de archivos del directorio de reglas de red. Para obtener más detalles, consulte [Instalación de un sistema operativo Linux](#) y [Paso 1 en Configuración del ECS y creación de una imagen de disco del sistema Linux](#).
4. Cree una imagen de disco del sistema a partir del ECS temporal.
En la consola de gestión, cree una imagen de disco del sistema a partir del ECS temporal en el que se han completado la instalación y la configuración. Una vez creada la imagen, elimine el ECS temporal para evitar que se generen cargos adicionales. Para obtener más información, véase [Creación de una imagen de disco del sistema desde un ECS de Linux](#).

Restricciones

- Una imagen ISO creada a partir de un archivo ISO solo se utiliza para crear un ECS temporal. No estará disponible en la consola de ECS. No se puede utilizar para crear ECS o cambiar el sistema operativo de ECS. Es necesario instalar un sistema operativo

en el ECS temporal y utilizar ese ECS para crear una imagen de disco del sistema que se puede utilizar para crear ECS o cambiar SO de ECS.

- Un ECS temporal tiene una funcionalidad limitada. Por ejemplo, no puede conectar discos a él. No se recomienda usarlo como un ECS normal.

2.12.2 Registro de un archivo ISO como una imagen ISO

Escenarios

Registre un archivo ISO externo en la plataforma en la nube como una imagen privada (imagen ISO). Antes de registrar una imagen, suba el archivo ISO al bucket OBS.

La imagen ISO no se puede replicar, exportar o cifrar.

Prerrequisitos

- El archivo que se va a registrar debe estar en formato ISO.
- El archivo de imagen ISO se ha subido al bucket OBS. Para más detalles, consulte [Carga de un archivo de imagen externo](#).

NOTA

El nombre del archivo de imagen ISO solo puede contener letras, dígitos, guiones (-) y guiones bajos (_). Si el nombre del archivo de imagen no cumple con los requisitos, cambie el nombre antes de cargar el archivo de imagen en el bucket OBS.

Procedimiento

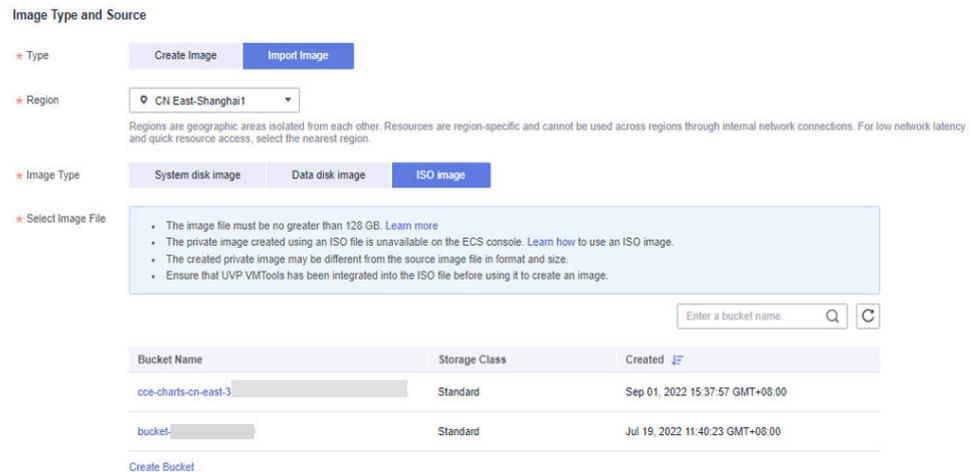
Paso 1 Acceda a la consola IMS.

1. Inicie sesión en la consola de gestión.
2. En **Compute**, haga clic en **Image Management Service**.
Se muestra la consola IMS.

Paso 2 Registre un archivo ISO como una imagen ISO.

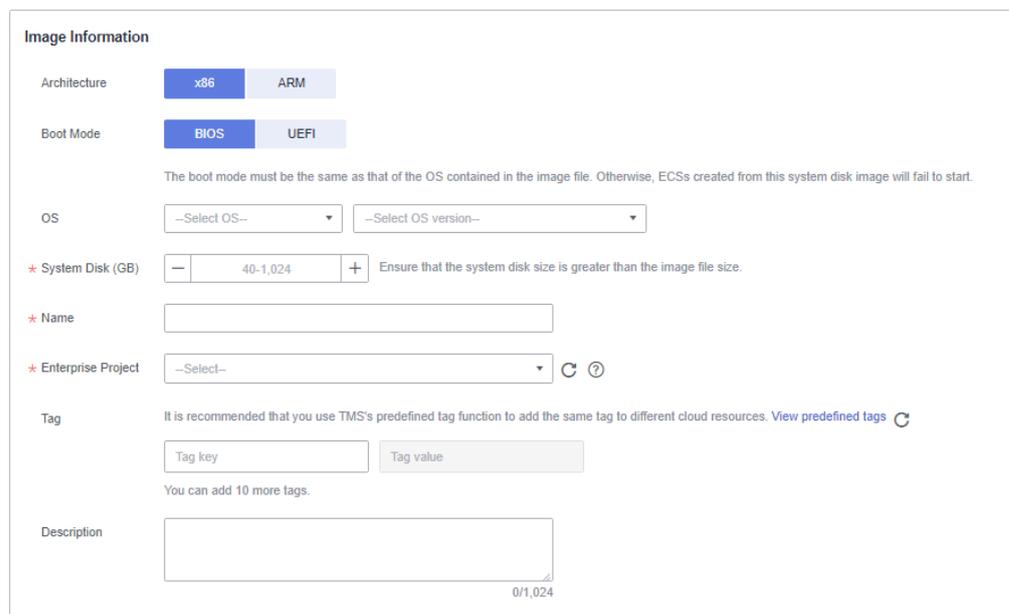
1. Haga clic en **Create Image** en la esquina superior derecha.
2. En el área **Image Type and Source**, seleccione **Import Image** para **Type** y, a continuación, seleccione **ISO image** para **Image Type**.
3. En la lista de archivos de imagen, seleccione el bucket y, a continuación, el archivo de imagen.

Figura 2-40 Creación de una imagen privada a partir de un archivo ISO



4. En el área **Image Information**, establezca los siguientes parámetros.

Figura 2-41 Configuración de la información de la imagen



- **Architecture.** Seleccione **x86** o **ARM**.

NOTA

Este parámetro solo se requiere en regiones que admiten tanto x86 como Arm.

- **Boot Mode:** Seleccione **BIOS** o **UEFI**. Asegúrese de que el modo de arranque seleccionado es el mismo que en el archivo de imagen, o los ECS creados a partir de esta imagen no podrán arrancar. La arquitectura Arm no admite el modo de arranque del BIOS.

NOTA

Si el modo de arranque en el archivo de imagen es **BIOS**, pero selecciona aquí **UEFI** para **Boot Mode**, no podrá ajustar la resolución.

- **OS:** Seleccione el sistema operativo especificado en el archivo ISO. Para asegurarse de que la imagen se puede crear y utilizar correctamente, seleccione un sistema operativo compatible con el del archivo de imagen.
- **License Type:** Traiga su propia licencia (BYOL) es compatible. Si ha obtenido una licencia de sistema operativo, no necesita solicitar una licencia más.
- **System Disk:** Establezca la capacidad del disco del sistema (rango de valores: 40 GB a 1024 GB), que no debe ser menor que la capacidad del disco del sistema en el archivo de imagen.
- **Name:** Ingrese un nombre para la imagen que se va a crear.
- **Enterprise Project:** Seleccione el proyecto de empresa al que pertenecen las imágenes.
- **Tag:** (Optional) Add a tag to the image to be created.

NOTA

Si su organización ha configurado políticas de etiquetas para imágenes, debe agregar etiquetas a las imágenes en función de las políticas. Si agrega una etiqueta que no cumple con las políticas de etiquetas, es posible que las imágenes no se creen. Póngase en contacto con el administrador de la organización para obtener más información sobre las políticas de etiquetas.

- Cada etiqueta consiste en una clave y un valor. La clave contiene un máximo de 36 caracteres y el valor contiene un máximo de 43 caracteres. La clave no se puede dejar en blanco ni una cadena de caracteres vacía. El valor no se puede dejar en blanco, sino que puede ser una cadena de caracteres vacía.
 - Una imagen puede tener un máximo de 10 etiquetas.
- **Description:** (Opcional) Introduzca la descripción de la imagen según sea necesario.
5. Haga clic en **Next**.
 6. Confirme la configuración. Seleccione **Statement of Commitment to Image Creation** y **Huawei Image Disclaimer**. Haga clic en **Submit**.

Paso 3 Vuelva a la página **Image Management Service** para monitorear el estado de la imagen.

Cuando el estado de la imagen cambia a **Normal**, la imagen se registra correctamente.

---Fin

2.12.3 Creación de un ECS de Linux a partir de una imagen ISO

Escenarios

Esta sección describe cómo crear un ECS a partir de una imagen ISO registrada.

Restricciones

Los usuarios de Dedicated Cloud (DeC) no pueden crear ECS a partir de imágenes ISO.

Si el servicio **DeC** está habilitado para un usuario en una región especificada, el usuario será un usuario DeC. Para obtener más información, vea [¿Qué es DeC?](#)

Procedimiento

Paso 1 Acceda a la consola de IMS.

1. Inicie sesión en la consola de gestión.
2. En **Compute**, haga clic en **Image Management Service**.
Se muestra la consola de IMS.

Paso 2 Utilizar una imagen ISO para crear un ECS de Linux.

1. Haga clic en la pestaña **Private Images**. Busque la fila que contiene la imagen ISO y haga clic en **Create ECS** en la columna **Operation**.

El ECS creado es solo para uso temporal y debe eliminarse cuando haya terminado con él. El sistema crea un ECS de pago por uso con especificaciones fijas. Cuando utilice la imagen privada creada a partir de este ECS para crear nuevos ECS, puede personalizar las especificaciones y el modo de facturación.

NOTA

Si es usuario de **DeC**, el botón **Create ECS** de la columna **Operation** no estará disponible para usted porque un usuario de DeC no puede utilizar una imagen ISO para crear un ECS.

2. Configure el ECS según se le solicite y haga clic en **OK**.

----Fin

Procedimiento posterior

Después de crear el ECS, puede iniciar sesión de forma remota para continuar con la instalación del sistema operativo y los controladores.

2.12.4 Instalación de un sistema operativo Linux

Escenarios

Esta sección utiliza CentOS 7 64-bit como ejemplo para describir cómo instalar Linux en un ECS.

El procedimiento de instalación varía en función del archivo de imagen que utilice. Realice las operaciones según se indique en la pantalla.

NOTA

Configure la zona horaria, la dirección de actualización del origen del repositorio, el método de entrada, el idioma y otros elementos según los requisitos del servicio.

Prerrequisitos

Ha iniciado sesión remotamente en el ECS y ha ingresado a la página de instalación.

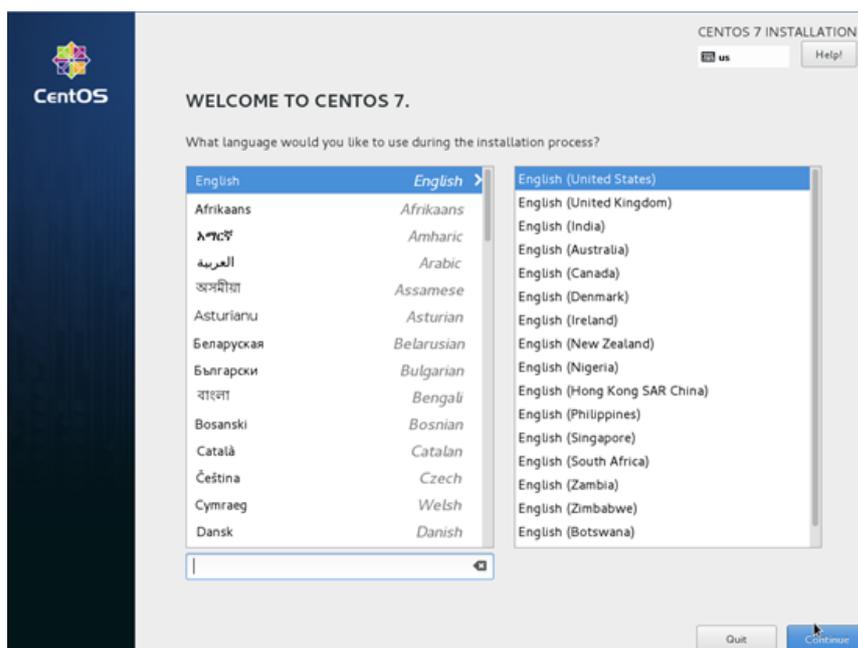
Procedimiento

⚠ ATENCIÓN

No detenga ni reinicie el ECS durante la instalación del sistema operativo. De lo contrario, la instalación del sistema operativo fallará.

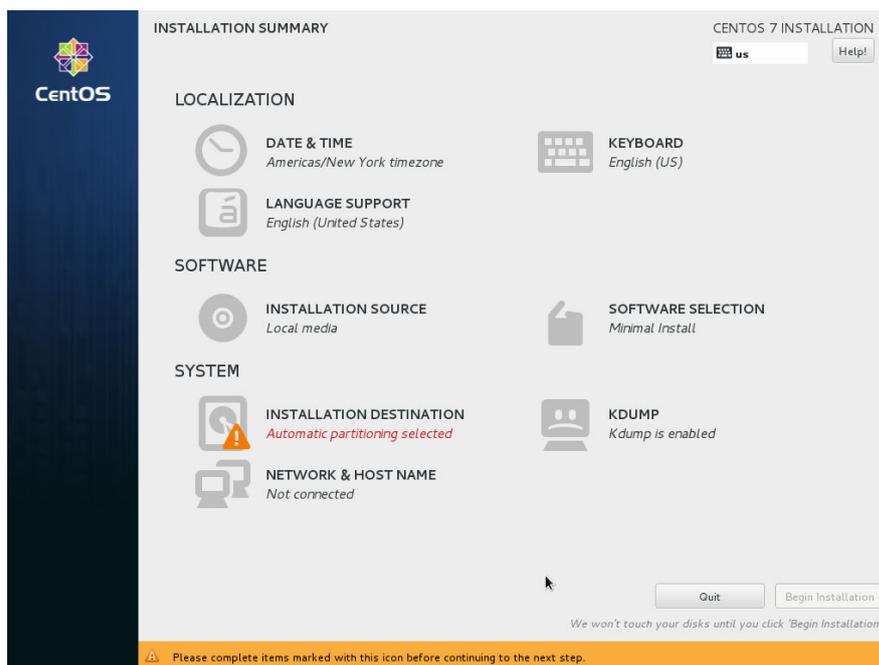
1. En la página de instalación, seleccione el idioma y haga clic en **Continue**.

Figura 2-42 Página de instalación



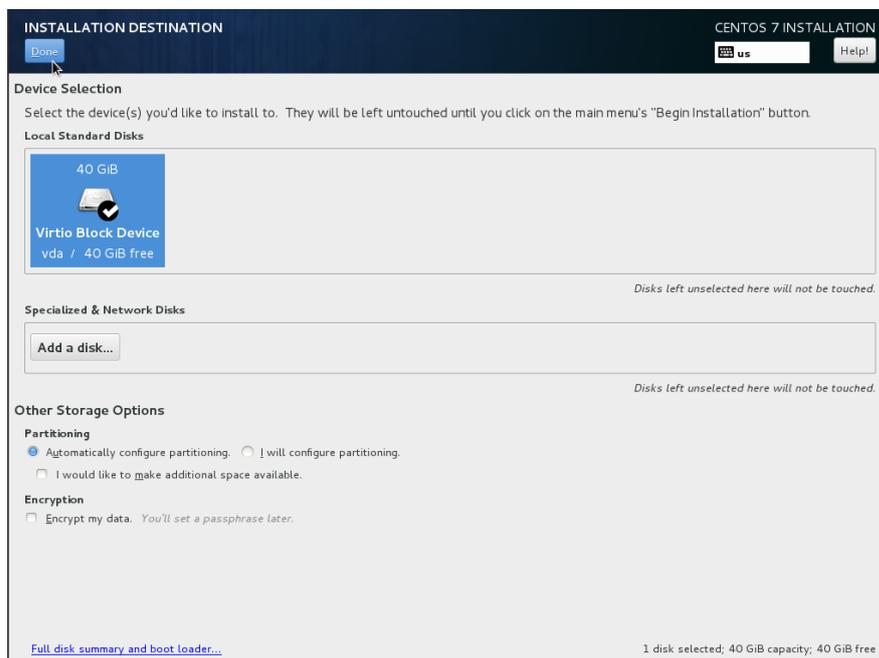
2. En la página **INSTALLATION SUMMARY**, seleccione **SYSTEM > INSTALLATION DESTINATION**.

Figura 2-43 Página de INSTALLATION SUMMARY



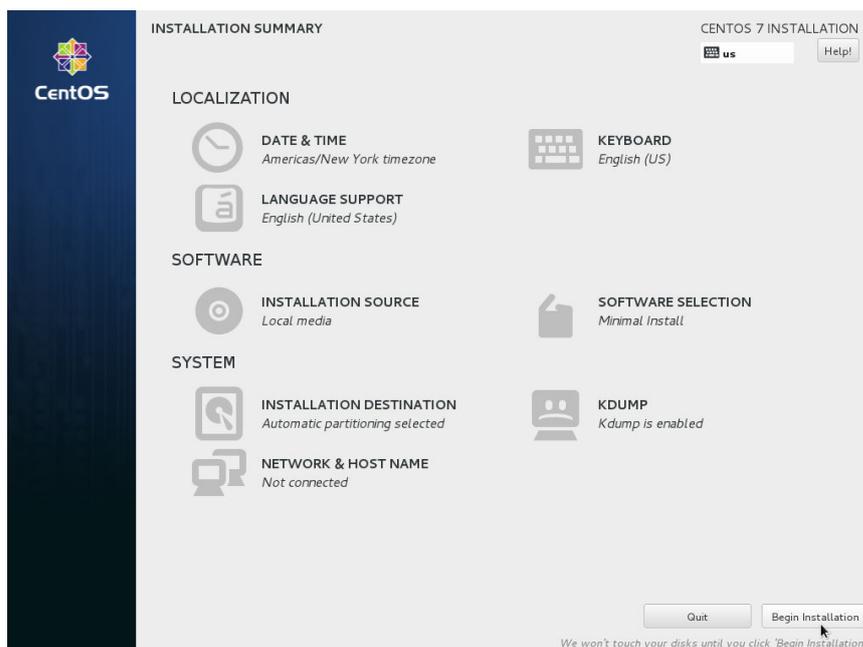
3. Seleccione el disco de destino y haga clic en **Done**.

Figura 2-44 Ubicación de instalación



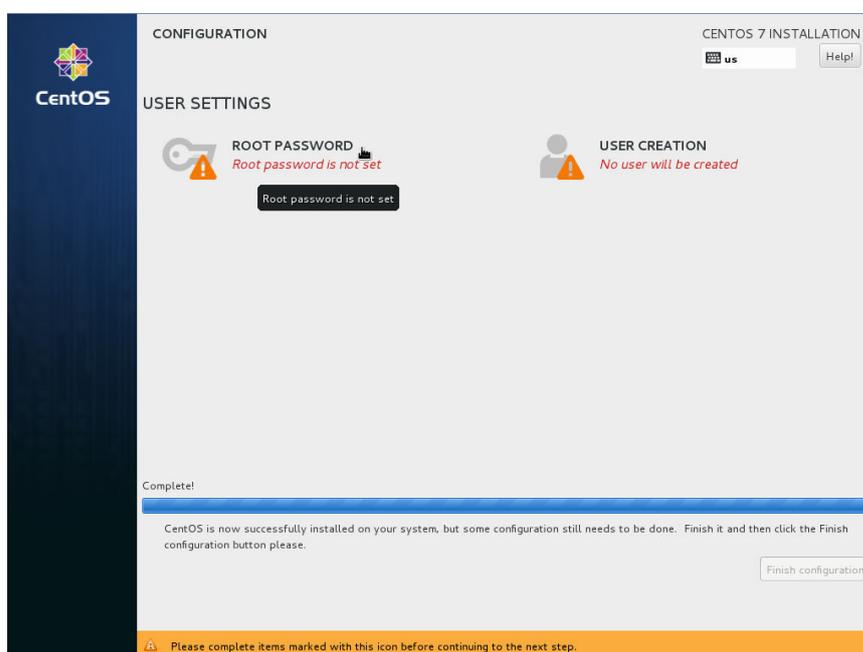
4. Haga clic en **Begin Installation**.

Figura 2-45 Inicio de la instalación



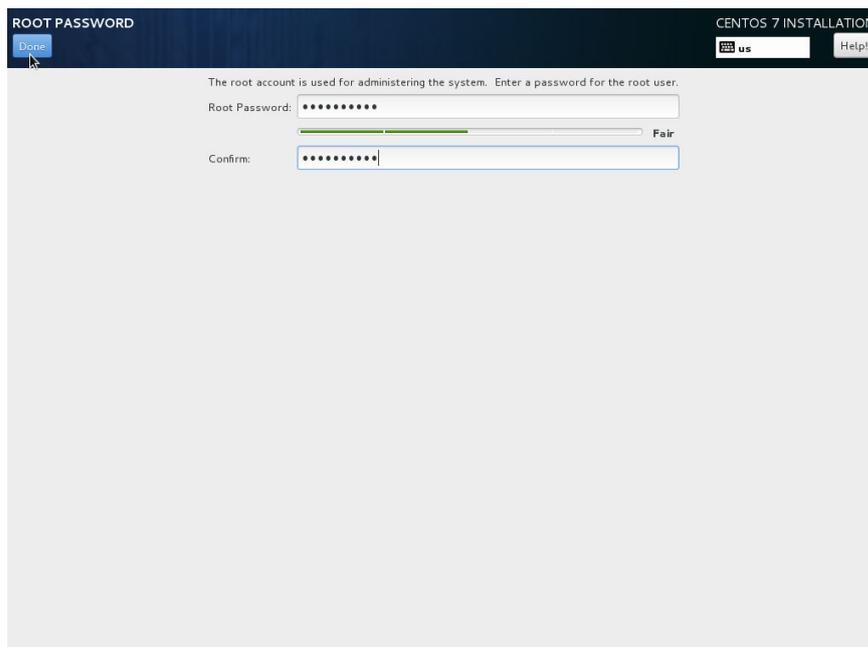
5. Espere a que se complete la instalación automática del sistema operativo. Cuando el progreso alcanza el 100%, CentOS se instala correctamente.

Figura 2-46 Instalación exitosa



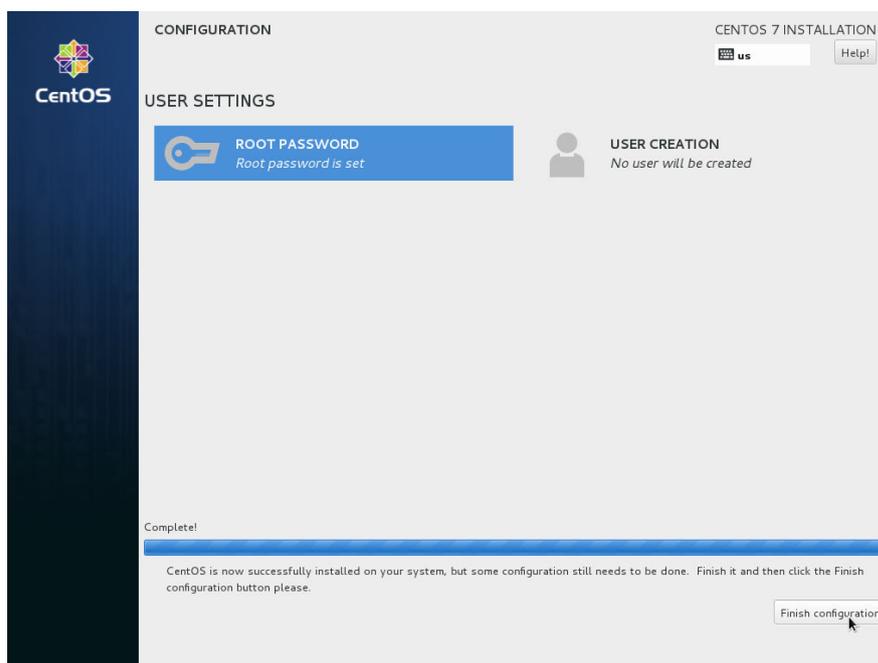
6. En el área **USER SETTINGS**, haga clic en **ROOT PASSWORD**. Se muestra la página **ROOT PASSWORD**.
7. Establezca una contraseña para el usuario **root** como se le solicite y haga clic en **Done**.

Figura 2-47 Configuración de una contraseña para el usuario root



8. Haga clic en **Finish configuration**.

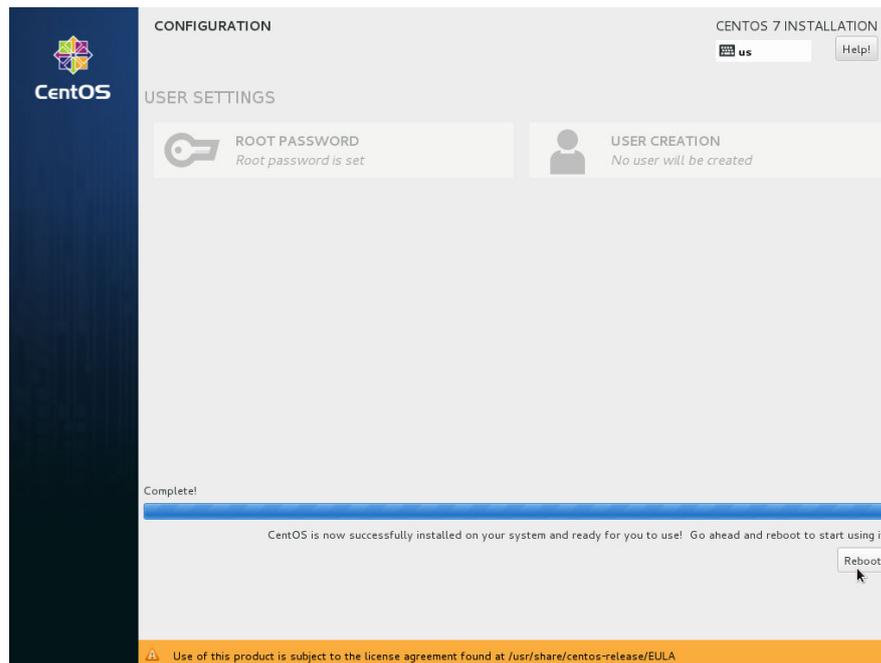
Figura 2-48 Finalización de la configuración



9. Haga clic en **Reboot**.

Si se le pide que instale el sistema operativo de nuevo después de reiniciar el ECS, salga de la página de inicio de sesión de VNC y reinicie el ECS en la consola.

Figura 2-49 Reiniciar el ECS



2.12.5 Configuración del ECS y creación de una imagen de disco del sistema Linux

Escenarios

Después de instalar un sistema operativo para el ECS temporal, configure el ECS e instale los controladores Xen y KVM nativos para asegurarse de que los ECS creados posteriormente estén disponibles.

Esta sección describe cómo configurar un ECS de Linux, instalar controladores y crear una imagen de disco del sistema Linux.

Procedimiento

Paso 1 Configurar el ECS.

1. Configurar la red.
 - Ejecute el comando **ifconfig** para comprobar si la dirección IP privada del ECS es la misma que se muestra en la consola. Si no son coherentes, elimine los archivos del directorio de reglas de red según se indica en [Eliminación de archivos desde el directorio de regla de red](#).
 - Compruebe si las NIC están establecidas en DHCP. Si el ECS está configurado con una dirección IP estática, cambie el modo de asignación de direcciones IP a DHCP como se indica en [Configuración de NIC al DHCP](#).
 - Ejecute el comando de **service sshd status** para verificar si SSH está habilitado. Si está deshabilitado, ejecute el comando **service sshd start** para habilitarlo. Asegúrese de que su firewall ECS, por ejemplo, Linux iptables, permita el acceso a SSH.
2. Instale los controladores.

Para garantizar que el rendimiento de la red y las funciones básicas de los ECS creados a partir de la imagen privada son normales, instale los controladores virtuales nativos de Xen y KVM en el ECS utilizado para crear la imagen. Antes de instalar los controladores virtuales nativos de Xen y KVM, desinstale el PV driver.

NOTA

Deshabilite su antivirus y software de detección de intrusión. Puede habilitarlos después de instalar los controladores Xen y KVM.

- Desinstale el PV driver. Para obtener más detalles, consulte [Desinstalación del controlador PV desde un Linux](#).
 - Instalar controladores Xen y KVM nativos. Para obtener más información, consulte [¿Cómo instalo los controladores nativos de Xen y KVM?](#)
 - Después de instalar los controladores, debe borrar los archivos de registro y los registros históricos. Para obtener más detalles, consulte [Borrar registros del sistema](#).
3. Configurar un sistema de archivos.
- Cambie el identificador de disco en el archivo de configuración de GRUB a UUID. Para obtener más información, consulte [Cambio del identificador de disco en el archivo de configuración de GRUB a UUID](#).
 - Cambie el identificador de disco en el archivo fstab a UUID. Para obtener más información, consulte [Cambio del identificador de disco en el archivo fstab a UUID](#).
 - Borre la información de adjuntos automáticos de discos que no son del sistema en el archivo `/etc/fstab` para evitar impactos en los adjuntos de disco de datos posteriores. Para obtener más información, consulte [Separación de discos de datos de un ECS](#).
4. (Opcional) Configurar funciones de valor agregado.
- Instale y configure Cloud-Init. Para obtener más información, consulte [Instalación de Cloud-Init](#) y [Configuración de Cloud-Init](#).
 - Habilite múltiples colas de NIC. Para obtener más detalles, consulte [¿Cómo puedo hacer múltiples colas para una imagen?](#)
 - Configurar la asignación dinámica de direcciones IPv6. Para obtener más detalles, consulte [¿Cómo configuro un ECS para obtener direcciones IPv6 dinámicamente?](#)

Paso 2 Cree una imagen de disco del sistema Linux.

Para obtener más información, véase [Creación de una imagen de disco del sistema desde un ECS de Linux](#).

----Fin

Procedimiento posterior

Después de crear la imagen de disco del sistema, elimine el ECS temporal de manera oportuna para evitar generar cargos adicionales.

2.13 Importación de una imagen

Debe preparar un archivo de imagen que cumpla con los requisitos de la plataforma y comprender los problemas conocidos del sistema operativo (consulte [Problemas conocidos](#)).

Restricciones

- Para obtener detalles sobre las restricciones de los archivos de imagen de Windows, consulte [Preparación de un archivo de imagen \(Windows\)](#).
- Para obtener detalles sobre las restricciones de los archivos de imagen de Linux, consulte [Preparación de un archivo de imagen \(Linux\)](#).

NOTA

- Se recomienda completar las configuraciones de red, herramientas y controladores en el VM de origen y, a continuación, exportar el archivo de imagen. También puede completar las configuraciones en los ECSs creados. Para obtener más información, consulte [¿Qué hago si un archivo de imagen de Windows no está preconfigurado cuando lo uso para registrar una imagen privada?](#) y [¿Qué debo hacer si un archivo de imagen de Linux no está preconfigurado cuando lo uso para registrar una imagen privada?](#)
- Actualmente, un archivo de imagen grande (máximo: 1 TB) solo se puede importar en formato RAW o ZVHD2. Además de cumplir con los requisitos para los archivos de imagen comunes, es necesario generar un archivo de bitmap para cada archivo de imagen RAW. El archivo de bitmap se cargará junto con el archivo de imagen. Para obtener más información, véase [Importación rápida de un archivo de imagen](#).

Importar

IMS proporciona varios métodos para importar imágenes. Puede seleccionar un método basado en el tipo de archivo de imagen, el formato o el tamaño.

Tabla 2-12 Importación de una imagen

Formato	Tamaño del archivo	Referencia
VMDK, VHD, QCOW2, VHDX, QED, VDI, QCOW, or ZVHD	No más de 128 GB	<ul style="list-style-type: none"> ● Creación de una imagen de disco del sistema Windows a partir de un archivo de imagen externo ● Creación de una imagen de disco de sistema Linux a partir de un archivo de imagen externo ● Creación de una imagen de disco de datos a partir de un archivo de imagen externo
RAW o ZVHD2	No más de 1 TB	<ul style="list-style-type: none"> ● Creación de una imagen de disco de datos a partir de un archivo de imagen externo

Formato	Tamaño del archivo	Referencia
ISO	No más de 128 GB	<ul style="list-style-type: none">● Creación de una imagen de disco de sistema Windows a partir de un archivo ISO● Creación de una imagen de disco de sistema Linux a partir de un archivo ISO

2.14 Importación rápida de un archivo de imagen

2.14.1 Descripción

Si un archivo de imagen tiene más de 128 GB, puede importarlo utilizando la importación rápida. Solo los formatos RAW y ZVHD2 admiten la importación rápida. El archivo de imagen que se va a importar no puede exceder 1 TB.

Métodos

Puede importar un archivo de imagen con cualquiera de los métodos siguientes dependiendo del formato de archivo:

- ZVHD2
 - Optimizar el archivo de imagen.
 - Subir el archivo de imagen a un bucket OBS.
 - Registrar el archivo de imagen en la plataforma en la nube.
- RAW
 - Optimizar el archivo de imagen.
 - Generar un archivo de mapa de bits para el archivo de imagen.
 - Subir el archivo de imagen y el archivo de mapa de bits a un bucket OBS.
 - Registrar el archivo de imagen en la plataforma en la nube.
- Otros
 - Si el formato de archivo se convierte a ZVHD2:
 - Optimizar el archivo de imagen.
 - Convertir el formato de archivo de imagen a ZVHD2.
 - Subir el archivo de imagen a un bucket OBS.
 - Registrar el archivo de imagen en la plataforma en la nube.
 - Si el formato de archivo se convierte a RAW:
 - Optimizar el archivo de imagen.
 - Convertir el formato de archivo de imagen a RAW y generar un archivo de mapa de bits para el archivo de imagen.
 - Subir el archivo de imagen y el archivo de mapa de bits a un bucket OBS.

- iv. Registrar el archivo de imagen en la plataforma en la nube.

NOTA

- La importación de archivos grandes depende de la carga perezosa que aplaza la carga de los datos del archivo hasta que sea necesario. Esto reduce el tiempo de carga inicial. Sin embargo, los archivos RAW no admiten esta característica. Cuando sube un archivo RAW, necesita subir su bitmap juntos.
- Para obtener más información sobre cómo optimizar un archivo de imagen, consulte [Proceso de optimización](#) (Windows) o [Proceso de optimización](#) (Linux) dependiendo del tipo de sistema operativo especificado en el archivo de imagen.

Proceso de importación

A continuación se describe cómo importar un archivo de imagen externo. Supongamos que necesita convertir el formato de archivo a ZVHD2 o RAW.

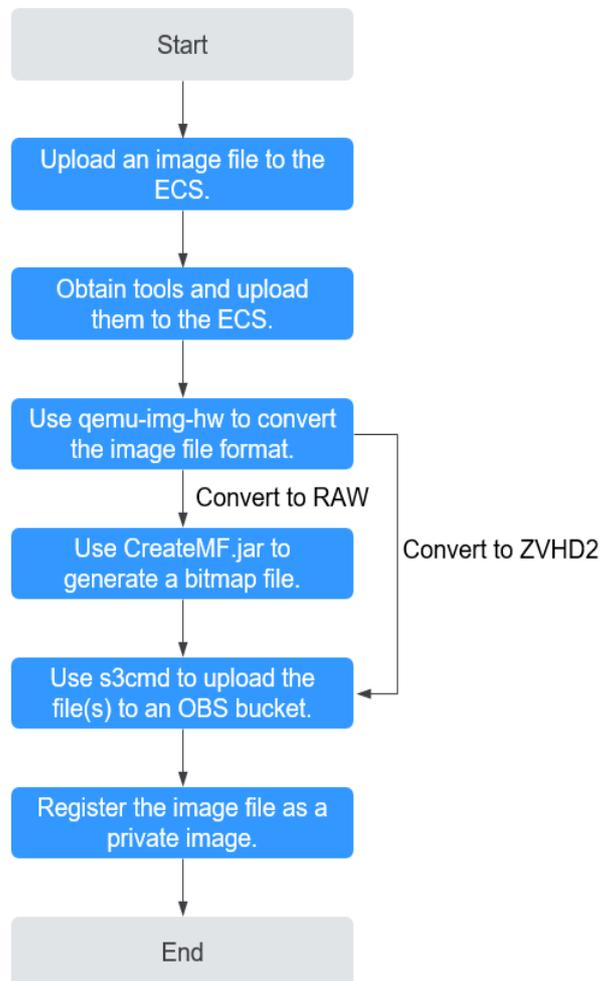
Puede usar **qemu-img-hw** o la herramienta de código abierto **qemu-img** para convertir el formato de imagen. **qemu-img-hw** solo se puede usar en Linux.

NOTA

El paquete de herramientas contiene **qemu-img-hw** (para convertir formatos de imagen) y **CreateMF.jar** (para generar archivos de bitmap).

- Linux
Se recomienda utilizar un ECS de EulerOS para convertir el formato de archivo.

Figura 2-50 Proceso de importación



Para obtener más información, véase [Importación rápida de un archivo de imagen \(Linux\)](#).

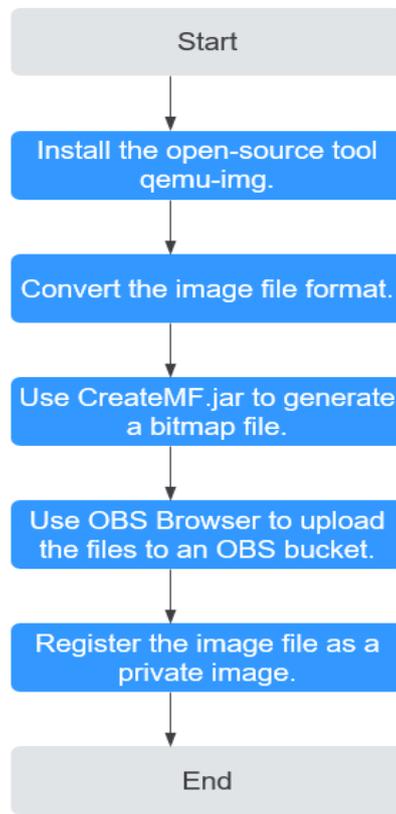
- Windows

Se recomienda utilizar un PC local que ejecute Windows para convertir el formato de archivo.

NOTA

qemu-img no puede convertir archivos de imagen al formato ZVHD2. Necesita convertir un archivo de imagen al formato RAW y luego usar **CreateMF.jar** para generar un archivo de mapa de bits.

Figura 2-51 Proceso de importación (Windows)



Para obtener más información, véase [Importación rápida de un archivo de imagen \(Windows\)](#).

2.14.2 Importación rápida de un archivo de imagen (Linux)

Escenarios

Esta sección describe cómo convertir el formato de un archivo de imagen en un servidor Linux y luego importarlo rápidamente a la plataforma en la nube. Se recomienda utilizar un ECS de EulerOS para convertir formatos de archivo de imagen y generar archivos de bitmap.

En Linux, se recomienda usar **qemu-img-hw** para convertir formatos de imagen.

Prerrequisitos

- El archivo de imagen ha sido optimizado. Para obtener más información, consulte [Proceso de optimización](#) (Windows) o [Proceso de optimización](#) (Linux). Asegúrese de que el archivo de imagen cumple los requisitos en [Tabla 2-5](#)(Windows) o [Tabla 2-8](#)(Linux).

NOTA

Seleccione el contenido de referencia basado en el tipo de sistema operativo en el archivo de imagen.

- Ha creado un ECS que ejecuta EulerOS en la consola de gestión y ha vinculado una EIP al ECS.
- Se ha creado un bucket OBS en la consola de gestión.

Procedimiento

Paso 1 Sube un archivo de imagen.

- Si el archivo de imagen se carga desde un PC con Linux, ejecute el comando **scp**. Por ejemplo, para cargar **image01.qcow2** en el directorio **/usr/** del ECS, ejecute el siguiente comando:

```
scp /var/image01.qcow2 root@xxx.xxx.xx.xxx:/usr/  
xxx.xxx.xxx.xxx indica la EIP vinculada con el ECS.
```

- Si el archivo de imagen se carga desde un PC con Windows, utilice una herramienta de transferencia de archivos, como WinSCP, para cargar el archivo de imagen.

Paso 2 Obtenga la herramienta de conversión de imágenes (**qemu-img-hw.zip**) y la herramienta de generación de archivos de bitmap (**createMF.zip**), súbalos al ECS y descomprima los paquetes.

Tabla 2-13 Paquetes de herramientas

Paquete de herramientas	Dónde obtenerlos
qemu-img-hw.zip	https://cn-south-1-cloud-reset-pwd.obs.cn-south-1.myhuaweicloud.com/imageImportTools/qemu-img-hw.zip
createMF.zip	https://cn-south-1-cloud-reset-pwd.obs.cn-south-1.myhuaweicloud.com/imageImportTools/createMF.zip

Paso 3 Utilice **qemu-img-hw** para convertir el formato de imagen.

1. Vaya al directorio donde se almacena **qemu-img-hw**, por ejemplo, **/usr/qemu-img-hw**.

```
cd /usr/qemu-img-hw
```

2. Ejecute el siguiente comando para hacer **qemu-img-hw** ejecutable:

```
chmod +x qemu-img-hw
```

3. Ejecute **qemu-img-hw** para convertir el formato de archivo de imagen a ZVHD2 (recomendado) o RAW.

Formato de comando:

```
./qemu-img-hw convert -p -O Target_image_format Source_image_file  
Target_image_file
```

Por ejemplo, ejecute el siguiente comando para convertir un archivo **image01.qcow2** en un archivo **image01.zvhd2**:

```
./qemu-img-hw convert -p -O zvhd2 image01.qcow2 image01.zvhd2
```

- Si el archivo de imagen se convierte al formato ZVHD2, vaya a **Paso 5**.
- Si el archivo de imagen se convierte al formato RAW, vaya a **Paso 4**.

Paso 4 Utilice **CreateMF.jar** para generar un archivo de bitmap.

1. Asegúrese de que se ha instalado JDK en el ECS.
Ejecute los siguientes comandos para comprobar si JDK está instalado:
source /etc/profile
java -version
Si se muestra una versión de Java, se ha instalado JDK.
2. Ejecute el siguiente comando para ingresar el directorio donde se almacena **CreateMF.jar**:
cd /usr/createMF
3. Ejecute el siguiente comando para generar un archivo de bitmap:
java -jar CreateMF.jar /Original RAW file path/Generated .mf file path
Ejemplo:
java -jar CreateMF.jar image01.raw image01.mf

 **ATENCIÓN**

- El archivo de bitmap generado .mf debe tener el mismo nombre que el archivo de imagen RAW. Por ejemplo, si el nombre del archivo de imagen es **image01.raw**, el nombre de mapa de bits generado es **image01.mf**.
-

Paso 5 Usar **s3cmd** para subir el archivo (s) a un bucket OBS.

1. Instale **s3cmd** en el ECS.
Si se ha instalado **s3cmd**, omita este paso.
 - a. Ejecute el siguiente comando para instalar **setuptools**:
yum install python-setuptools
 - b. Ejecute el siguiente comando para instalar **wget**:
yum install wget
 - c. Ejecute los siguientes comandos para obtener el paquete de software **s3cmd**:
wget https://github.com/s3tools/s3cmd/archive/master.zip
mv master.zip s3cmd-master.zip
 - d. Ejecute los siguientes comandos para instalar **s3cmd**:
unzip s3cmd-master.zip
cd s3cmd-master
python setup.py install

2. Configurar **s3cmd**.

Ejecute el siguiente comando para configurar **s3cmd**:

```
s3cmd --configure  
Access Key: Enter an AK.  
Secret Key: Enter an SK.  
Default Region: Enter the region where the bucket is located.  
S3 Endpoint: Refer to the OBS endpoint.  
DNS-style bucket+hostname:port template for accessing a bucket: Enter a  
server address with a bucket name, for example, mybucket.obs.myclouds.com.  
Encryption password: Press Enter.  
Path to GPG program: Press Enter.  
Use HTTPS protocol: Specifies whether to use HTTPS. The value can be Yes or  
No.
```

```
HTTP Proxy server name: Specifies the proxy address used to connect the cloud
from an external network. (If you do not need it, press Enter.)
HTTP Proxy server port: Specifies the proxy port used to connect to the cloud
from an external network (If you do not need it, press Enter.)
Test access with supplied credentials? y
(If "Success. Your access key and secret key worked fine :-)" is displayed,
the connection is successful.)
Save settings? y (Specifies whether to save the configurations. If you enter
y, the configuration will be saved.)
```

 **NOTA**

Las configuraciones se almacenarán en `/root/.s3cfg`. Si desea modificar estas configuraciones, ejecute el comando `s3cmd --configure` para configurar los parámetros o ejecute el comando `vi.s3cfg` para editar el archivo `.s3cfg`.

3. Ejecute el siguiente comando para cargar el archivo de imagen ZVHD2 (o el archivo de imagen RAW y su archivo de mapa de bits) en un bucket OBS.

```
s3cmd put image01.zvhd2 s3://mybucket/
```

 **ATENCIÓN**

El archivo de `.mf` bitmap debe estar en el mismo bucket de OBS que el archivo de imagen RAW.

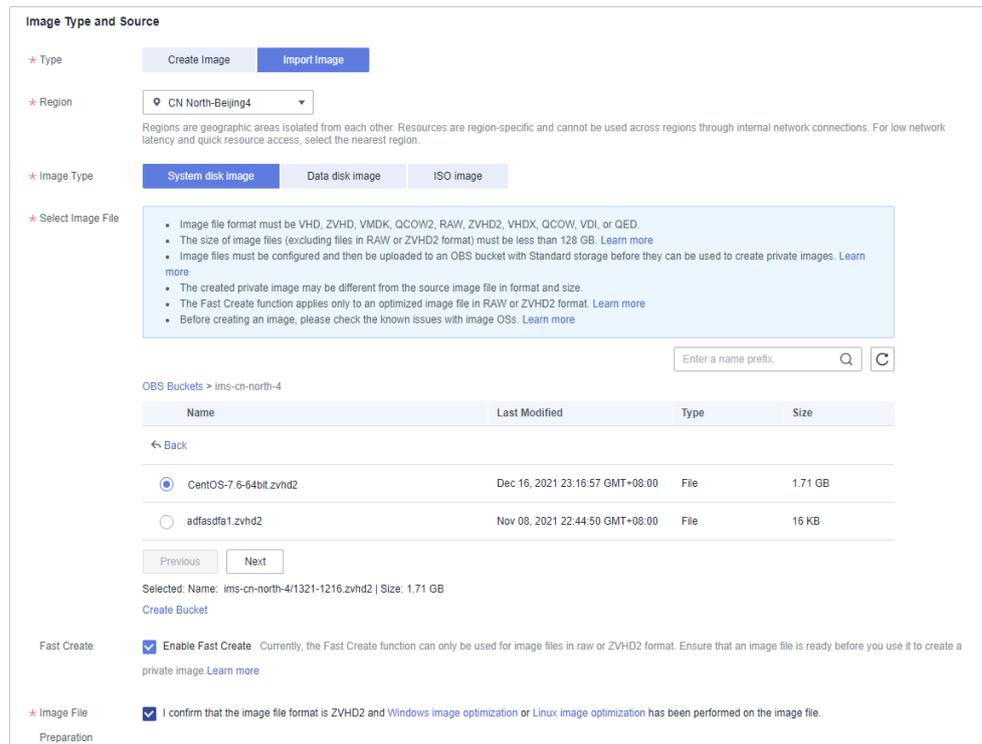
Paso 6 Registre una imagen privada.

Puede registrar una imagen privada usando el archivo convertido ZVHD2 o RAW en la consola o usando una API.

Método 1: Registrar una imagen privada en la consola.

1. Acceda a la consola IMS.
 - a. Inicie sesión en la consola de gestión.
 - b. En **Compute**, haga clic en **Image Management Service**.
Se muestra la consola IMS.
2. En la esquina superior derecha, haga clic en **Create Image**.
3. En el área **Image Type and Source**, seleccione **Import Image** para **Type** y, a continuación, seleccione **System disk image** o **Data disk image** para **Image Type**.
4. Seleccione el bucket que almacena el archivo de imagen ZVHD2 o RAW y, a continuación, seleccione el archivo de imagen. Si el archivo de imagen está en formato RAW, también debe seleccionar su archivo de bitmap.
5. Seleccione **Enable Fast Create** y seleccione la frase siguiente **Image File Preparation**.

Figura 2-52 Importación rápida de un archivo de imagen



6. Configure los parámetros según se indique.

Para obtener más información sobre los parámetros, consulte [Registro de un archivo de imagen externo como imagen privada](#).

⚠ ATENCIÓN

- El sistema operativo debe ser el mismo que en el archivo de imagen.
- La capacidad del disco del sistema debe ser mayor que la especificada en el archivo de imagen.

Ejecute el siguiente comando para comprobar la capacidad del disco del sistema en el archivo de imagen:

```
qemu-img-hw info test.zvh2
```

Método 2: Registrar una imagen privada usando una API.

Puede utilizar la API POST `/v2/cloudimages/quickimport/action` para importar rápidamente un archivo de imagen.

Para obtener más información sobre cómo invocar a esta API, consulte [Importación de un archivo de imagen rápidamente](#).

----Fin

Apéndice 1: Comandos comunes de `qemu-img-hw`

- Conversión de formatos de archivo de imagen: `qemu-img-hw convert -p -O Target_image_format Source_image_file Target_image_file`

Los parámetros se describen de la siguiente manera:

-p: indica el progreso de la conversión.

La parte siguiente **-O** (que debe estar en mayúsculas) consiste en el formato de imagen de destino, el archivo de imagen de origen y el archivo de imagen de destino.

Por ejemplo, ejecute el siguiente comando para convertir un archivo de imagen QCOW2 en un archivo ZVHD2:

```
qemu-img-hw convert -p -O zvhd2 test.qcow2 test.zvhd2
```

- Consultar información del archivo de imagen: **qemu-img-hw info** *Source image file*
Un comando de ejemplo es **qemu-img-hw info test.zvhd2**.
- Consultar información de ayuda: **qemu-img-hw -help**

Apéndice 2: Errores comunes durante la ejecución de qemu-img-hw

- Síntoma:

La siguiente información se muestra cuando ejecuta el comando **qemu-img-hw**:

```
./qemu-img-hw: /lib64/libc.so.6: version `GLIBC_2.14' not found (required by ./qemu-img-hw)
```

Solución:

Ejecute el comando **strings /lib64/libc.so.6 | grep glibc** para comprobar la versión de glibc. Si la versión es demasiado temprana, instale la versión más reciente. Ejecute los siguientes comandos en secuencia:

```
wget http://ftp.gnu.org/gnu/glibc/glibc-2.15.tar.gz
```

```
wget http://ftp.gnu.org/gnu/glibc/glibc-ports-2.15.tar.gz
```

```
tar -xvf glibc-2.15.tar.gz
```

```
tar -xvf glibc-ports-2.15.tar.gz
```

```
mv glibc-ports-2.15 glibc-2.15/ports
```

```
mkdir glibc-build-2.15
```

```
cd glibc-build-2.15
```

```
../glibc-2.15/configure --prefix=/usr --disable-profile --enable-add-ons --with-headers=/usr/include --with-binutils=/usr/bin
```

NOTA

Si se muestra **configure: error: no acceptable C compiler found in \$PATH**, ejecute el comando **yum -y install gcc**.

```
make
```

```
make install
```

- Síntoma:

La siguiente información se muestra cuando ejecuta el comando **qemu-img-hw**:

```
./qemu-img-hw: error while loading shared libraries: libaio.so.1: cannot open shared object file: No such file or directory
```

Solución: Ejecute primero el comando **yum install libaio**.

2.14.3 Importación rápida de un archivo de imagen (Windows)

Escenarios

Esta sección describe cómo convertir el formato de un archivo de imagen en un servidor Windows y luego importarlo rápidamente a la plataforma en la nube. Se recomienda utilizar un PC con Windows local para convertir formatos de imagen y generar archivos de bitmap.

En Windows, utilice la herramienta de código abierto **qemu-img** para convertir formatos de imagen. **qemu-img** admite la conversión entre archivos de imagen de los formatos VHD, VMDK, QCOW2, RAW, VHDX, QCOW, VDI y QED. Convierta una imagen al formato RAW y, a continuación, utilice la herramienta **CreateMF.jar** para generar un archivo de bitmap.

Prerrequisitos

- El archivo de imagen ha sido optimizado. Para obtener más información, consulte [Proceso de optimización](#) (Windows) o [Proceso de optimización](#) (Linux). Asegúrese de que el archivo de imagen cumple los requisitos en [Tabla 2-5](#)(Windows) o [Tabla 2-8](#)(Linux).

NOTA

Seleccione el contenido de referencia basado en el tipo de sistema operativo en el archivo de imagen.

- Se ha creado un bucket OBS en la consola de gestión, y OBS Browser+ ya está listo.

Procedimiento

Paso 1 Instale la herramienta de conversión de imágenes de código abierto **qemu-img**. Para obtener más detalles, consulte [Conversión del formato de imagen mediante qemu-img](#).

Paso 2 Ejecute el comando **cmd** para ir al directorio de instalación **qemu-img** y ejecute el comando **qemu-img** para convertir el archivo de imagen al formato RAW.

Por ejemplo, ejecute el siguiente comando para convertir un archivo **image.qcow2** en un archivo **image.raw**:

```
qemu-img convert -p -O raw image.qcow2 image.raw
```

Paso 3 Utilice **CreateMF.jar** para generar un archivo de bitmap.

1. Obtenga el paquete **CreateMF.jar** y descomprímalo.

Tabla 2-14 CreateMF.jar package

Paquete de herramientas	Cómo obtenerlo
createMF.zip	https://cn-south-1-cloud-reset-pwd.obs.cn-south-1.myhuaweicloud.com/imageImportTools/createMF.zip

2. Asegúrese de que JDK se ha instalado en el entorno actual.

Puede verificar la instalación ejecutando **cmd.exe** y, a continuación, **java -version**. Si se muestra la información de la versión de Java, se ha instalado JDK.

3. Vaya al directorio donde está almacenado **CreateMF.jar**.

Por ejemplo, si ha descargado **CreateMF.jar** a **D:/test**, ejecute los siguientes comandos para acceder al directorio:

D:

cd test

4. Ejecute el siguiente comando para generar un archivo de bitmap para el archivo de imagen RAW:

java -jar CreateMF.jar D:/image01.raw D:/image01.mf

 **ATENCIÓN**

- El archivo de bitmap generado **.mf** debe tener el mismo nombre que el archivo de imagen RAW. Por ejemplo, si el nombre del archivo de imagen es **image01.raw**, el nombre de mapa de bits generado es **image01.mf**.

Paso 4 Utilice OBS Browser+ para cargar el archivo de imagen convertido y su archivo de bitmap en un bucket de OBS.

Debe cargar el archivo de imagen RAW y su archivo de bitmap en el mismo bucket de OBS.

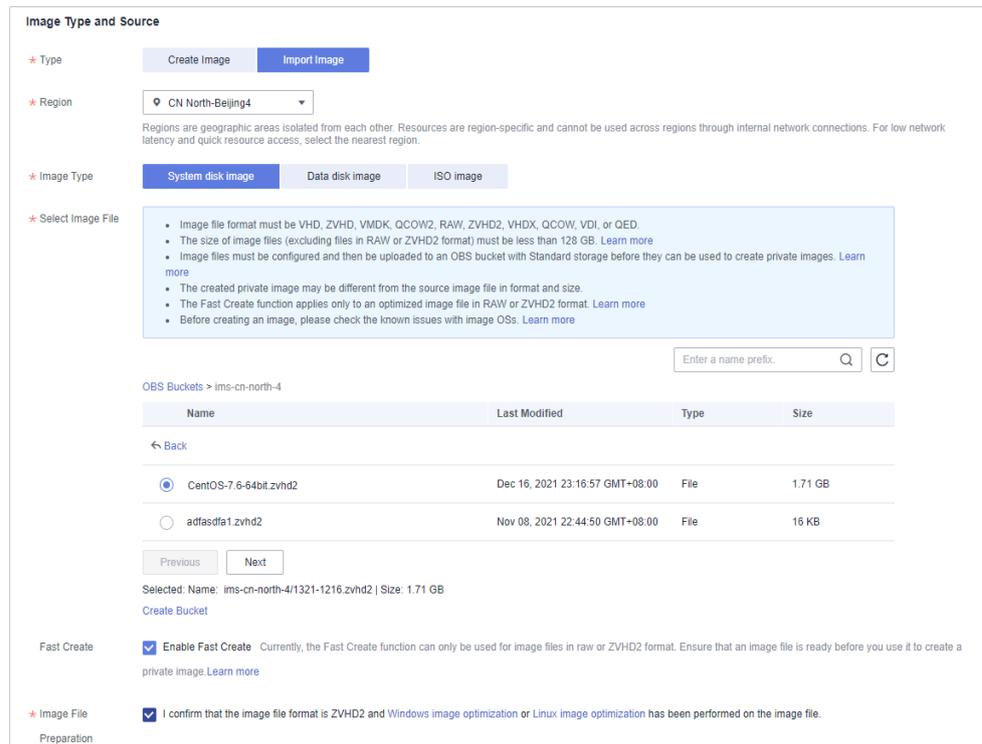
Paso 5 Registre una imagen privada.

Puede registrar una imagen privada usando el archivo convertido ZVHD2 o RAW en la consola o usando una API.

Método 1: Registrar una imagen privada en la consola.

1. Acceda a la consola IMS.
 - a. Inicie sesión en la consola de gestión.
 - b. En **Compute**, haga clic en **Image Management Service**.
Se muestra la consola IMS.
2. En la esquina superior derecha, haga clic en **Create Image**.
3. En el área **Image Type and Source**, seleccione **Import Image** para **Type** y, a continuación, seleccione **System disk image** o **Data disk image** para **Image Type**.
4. Seleccione el bucket que almacena el archivo de imagen ZVHD2 o RAW y, a continuación, seleccione el archivo de imagen. Si el archivo de imagen está en formato RAW, también debe seleccionar su archivo de bitmap.
5. Seleccione **Enable Fast Create** y seleccione la frase siguiente **Image File Preparation**.

Figura 2-53 Importación rápida de un archivo de imagen



6. Configure los parámetros según se indique.

Para obtener más información sobre los parámetros, consulte [Registro de un archivo de imagen externo como imagen privada](#).

ATENCIÓN

- El sistema operativo debe ser el mismo que en el archivo de imagen.
- La capacidad del disco del sistema debe ser mayor que la especificada en el archivo de imagen.

Ejecute el siguiente comando para comprobar la capacidad del disco del sistema en el archivo de imagen:

```
qemu-img-hw info test.zvhd2
```

Método 2: Registrar una imagen privada usando una API.

Puede utilizar la API POST `/v2/cloudimages/quickimport/action` para importar rápidamente un archivo de imagen.

Para obtener más información sobre cómo invocar a esta API, consulte [Importación de un archivo de imagen rápidamente](#).

----Fin

3 Gestión de imágenes privadas

3.1 Modificación de una imagen

Escenarios

Puede modificar los siguientes atributos de una imagen privada:

- Nombre
- Descripción
- Memoria mínima
- Memoria máxima
- NIC de cola múltiple

NIC de cola múltiple permite que varias CPU procesen interrupciones de NIC para equilibrar la carga. Para obtener más información, consulte [¿Cómo habilito la cola múltiple de NIC para una imagen?](#)

- Modo de arranque

Restricciones

- Solo se puede modificar una imagen privada en el estado **Normal**.

Procedimiento

Utilice cualquiera de los métodos siguientes para modificar una imagen:

Método 1:

1. Acceda a la consola IMS.
 - a. Inicie sesión en la consola de gestión.
 - b. En **Compute**, haga clic en **Image Management Service**.
Se muestra la consola IMS.
2. Haga clic en la pestaña **Private Images** para mostrar la lista de imágenes.
3. Busque la fila que contiene la imagen y haga clic en **Modify** en la columna **Operation**.

4. En el cuadro de diálogo **Modify Image**, modifique la imagen.

Figura 3-1 Modificación de una imagen

Modify Image ×

* Name

Description

Minimum Memory Ensure that the minimum memory size of an image is set to its original size before you reinstall OSs of the ECSs that were created using the image.

Unlimited	1 GiB	2 GiB	4 GiB	8 GiB	16 GiB	32 GiB
64 GiB	128 GiB					

Maximum Memory

Unlimited	4 GiB	32 GiB	64 GiB	128 GiB
-----------	-------	--------	--------	---------

NIC Multi-Queue

Supported	Not supported
-----------	---------------

Boot Mode

BIOS	UEFI
------	------

The boot mode must be the same as that of the OS contained in the image file. Otherwise, ECSs created from this system disk image will fail to start.

OK Cancel

Método 2:

1. Acceda a la consola IMS.
 - a. Inicie sesión en la consola de gestión.
 - b. En **Compute**, haga clic en **Image Management Service**.
Se muestra la consola IMS.
2. Haga clic en la pestaña **Private Images** para mostrar la lista de imágenes.
3. En la lista de imágenes, haga clic en el nombre de la imagen deseada.
4. En la página de detalles de la imagen, haga clic en **Modify** en la esquina superior derecha. En el cuadro de diálogo **Modify Image**, modifique los atributos de imagen.

Método 3:

El sistema le permite cambiar rápidamente el nombre de una imagen privada.

1. Acceda a la consola IMS.
 - a. Inicie sesión en la consola de gestión.
 - b. En **Compute**, haga clic en **Image Management Service**.
Se muestra la consola IMS.
2. Haga clic en la pestaña **Private Images**.
3. En la lista de imágenes privadas, localice la imagen de destino y mueva el cursor a la columna **Name**.
4. Haga clic en  para cambiar el nombre de la imagen.
5. Haga clic en **OK**.

3.2 Exportación de lista de imágenes

Escenarios

Puede exportar la lista de imágenes pública o privada en la región actual como un archivo CSV a su PC local.

- Para las imágenes públicas, el archivo describe el nombre de la imagen, el estado de la imagen, el sistema operativo, el tipo de imagen, el tiempo de creación de la imagen, el disco del sistema y la memoria mínima.
- Para las imágenes privadas, el archivo describe el nombre de la imagen, el ID de la imagen, el estado de la imagen, el sistema operativo, el tipo de imagen, el tiempo de creación de la imagen, las capacidades del disco, los discos compartidos, el tamaño de la imagen, la memoria mínima y la encriptación.

Exportación de información de imagen privada

1. Acceda a la consola IMS.
 - a. Inicie sesión en la consola de gestión.
 - b. En **Compute**, haga clic en **Image Management Service**.
Se muestra la consola IMS.

2. Haga clic en la pestaña **Private Images** y haga clic en .

El sistema exportará automáticamente la lista de imágenes privadas en la región actual bajo su cuenta a un directorio local.

NOTA

El nombre del archivo tiene el formato de **private-images-Region ID-Export time**.

Exportación de información de imagen pública

1. Acceda a la consola IMS.
 - a. Inicie sesión en la consola de gestión.
 - b. En **Compute**, haga clic en **Image Management Service**.
Se muestra la consola IMS.

2. Haga clic en la pestaña **Public Images** y haga clic en .

El sistema exportará automáticamente todas las imágenes públicas de la región actual a un directorio local.

NOTA

El nombre del archivo tiene el formato de **public-images-Region ID-Export time**.

3.3 Comprobación de la capacidad del disco de una imagen

Escenarios

Puede comprobar la capacidad del disco de una imagen privada.

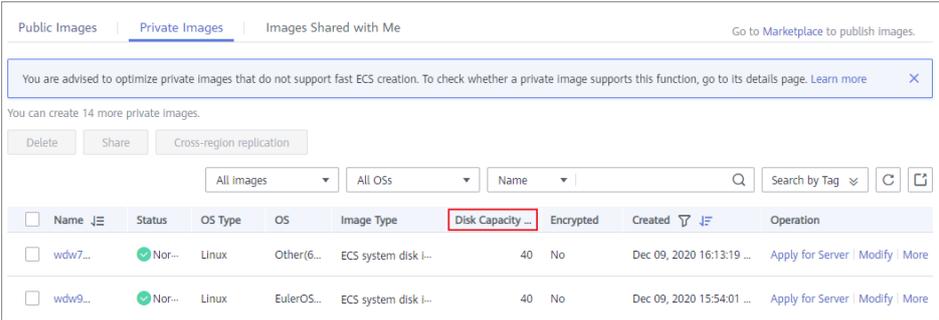
- Para comprobar la capacidad del disco de una imagen de disco del sistema, una imagen de disco de datos o una imagen ISO, consulte [Comprobar la capacidad del disco de una imagen de disco del sistema, una imagen de disco de datos o una imagen ISO](#).
- Para comprobar la capacidad del disco de una imagen completa de ECS, consulte [Comprobar la capacidad del disco de una imagen completa del ECS](#).

Comprobar la capacidad del disco de una imagen de disco del sistema, una imagen de disco de datos o una imagen ISO

Compruebe la capacidad del disco en la columna **Disk Capacity** de la lista de imágenes privadas.

1. Acceda a la consola IMS.
 - a. Inicie sesión en la consola de gestión.
 - b. En **Compute**, haga clic en **Image Management Service**.
Se muestra la consola IMS.
2. Haga clic en la pestaña **Private Images** para mostrar la lista de imágenes.
3. Compruebe el valor en la columna **Disk Capacity**. La unidad es **GB**.

Figura 3-2 Comprobación de la capacidad del disco de una imagen de disco del sistema, una imagen de disco de datos o una imagen ISO



<input type="checkbox"/>	Name	Status	OS Type	OS	Image Type	Disk Capacity	Encrypted	Created	Operation
<input type="checkbox"/>	wdw7...	✔ Nor...	Linux	Other(6...	ECS system disk i...	40	No	Dec 09, 2020 16:13:19 ...	Apply for Server Modify More
<input type="checkbox"/>	wdw9...	✔ Nor...	Linux	EulerOS...	ECS system disk i...	40	No	Dec 09, 2020 15:54:01 ...	Apply for Server Modify More

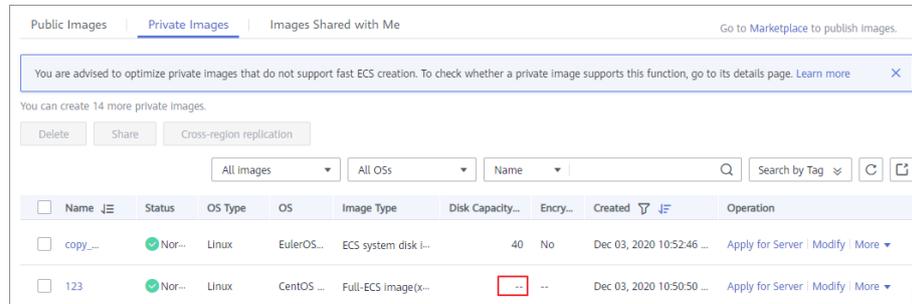
Comprobar la capacidad del disco de una imagen completa del ECS

La capacidad de disco de una imagen completa del ECS es la suma de la capacidad de disco del sistema y la capacidad de disco de datos en la copia de respaldo a partir de la cual se crea la imagen completa del ECS.

1. Acceda a la consola IMS.
 - a. Inicie sesión en la consola de gestión.

- b. En **Compute**, haga clic en **Image Management Service**.
 Se muestra la consola IMS.
2. Haga clic en la pestaña **Private Images** para mostrar la lista de imágenes.
 El valor de la columna **Disk Capacity** es --.

Figura 3-3 Comprobación de la capacidad del disco de una imagen completa del ECS



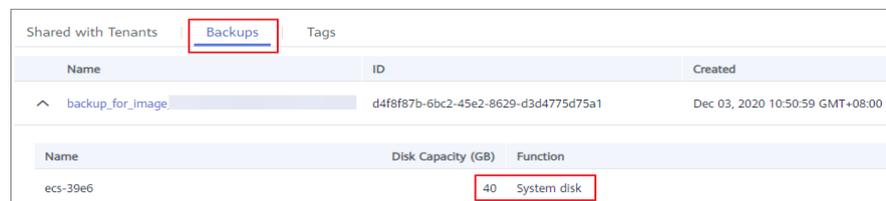
3. Haga clic en el nombre de la imagen completa del ECS.
4. Haga clic en la pestaña **Backups** y vea las capacidades del disco del sistema y los discos de datos en la copia de respaldo.

Capacidad del disco de una imagen completa del ECS = Capacidad del disco del sistema en la copia de respaldo + Capacidad de los discos de datos en la copia de respaldo

Por ejemplo:

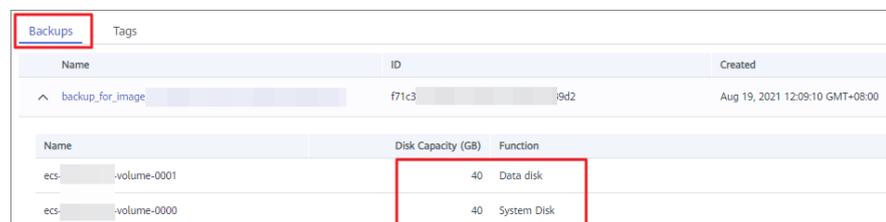
- Si la capacidad del disco del sistema es de 40 GB y no hay ningún disco de datos conectado, la capacidad del disco de imagen de ECS completo es de 40 GB.

Figura 3-4 Comprobación de los detalles de la copia de respaldo



- Si la capacidad del disco del sistema es de 40 GB y la capacidad del disco de datos es de 40 GB, la capacidad del disco de imagen ECS completa es de 80 GB.

Figura 3-5 Comprobación de los detalles de la copia de respaldo



3.4 Creación de un ECS a partir de una imagen

Escenarios

Puede utilizar una imagen pública, privada o compartida para crear un ECS.

- Si utiliza una imagen pública, el ECS creado contiene un sistema operativo y aplicaciones públicas preinstaladas. Es necesario instalar aplicaciones según sea necesario.
- Si utiliza una imagen privada o compartida, el ECS creado contiene un sistema operativo, aplicaciones públicas preinstaladas y aplicaciones personales de un usuario.

Procedimiento

1. Acceda a la consola IMS.
 - a. Inicie sesión en la consola de gestión.
 - b. En **Compute**, haga clic en **Image Management Service**.
Se muestra la consola IMS.
2. Haga clic en la ficha **Public Images**, **Private Images**, o **Images Shared with Me** para mostrar la lista de imágenes.
3. Busque la fila que contiene la imagen deseada y haga clic en **Apply for Server** en la columna **Operation**.
4. Para obtener más información sobre cómo crear un ECS, consulte [Compra de un ECS](#).
Cuando se utiliza una imagen de disco del sistema para crear un ECS puede establecer las especificaciones de ECS y el tipo de disco del sistema sin tener en cuenta las de la imagen, pero la capacidad del disco del sistema solo puede ser mayor que la de la imagen.
Cuando se utiliza una imagen de ECS completo para crear un ECS, la información del sistema y del disco de datos predeterminada por la imagen se mostrará automáticamente. Puede aumentar la capacidad de un disco del sistema o discos de datos, pero no puede reducirla.

NOTA

Si una imagen completa de ECS contiene varios discos de datos, se tarda algún tiempo en cargar y mostrar la información del disco.

3.5 Eliminación de imágenes

Escenarios

Puede eliminar imágenes privadas que ya no se utilizarán.

- Las imágenes privadas eliminadas no se pueden recuperar. Realice esta operación solo cuando sea absolutamente necesario.
- Después de eliminar una imagen privada, no se puede utilizar para crear discos ECS o EVS.

- Después de eliminar una imagen privada, los ECS creados a partir de la imagen pueden seguir utilizándose y todavía se facturan. Sin embargo, el sistema operativo no se puede volver a instalar para los ECS y no se pueden crear los ECS con la misma configuración.
- La eliminación de la imagen de origen de una imagen replicada no tiene ningún efecto en la imagen replicada. Del mismo modo, la eliminación de una imagen replicada no tiene ningún efecto en su origen.

Restricciones

- Las imágenes privadas que se han publicado en Marketplace no se pueden eliminar.
- Si una imagen se comparte con una cuenta u organización, primero debe eliminar la cuenta u organización de los destinatarios de la imagen antes de eliminarla.

Procedimiento

1. Acceda a la consola IMS.
 - a. Inicie sesión en la consola de gestión.
 - b. En **Compute**, haga clic en **Image Management Service**.
Se muestra la consola IMS.
2. Haga clic en la pestaña **Private Images** para mostrar la lista de imágenes.
3. Busque la fila que contiene la imagen, elija **More > Delete** en la columna **Operation**.

NOTA

Para eliminar varias imágenes:

1. Seleccione las imágenes que desea eliminar en la lista de imágenes.
 2. Haga clic en **Delete** encima de la lista de imágenes.
4. (Opcional) Seleccione **Delete CSBS backups or cloud server backups of the full-ECS images**.

Este parámetro solo está disponible cuando se han seleccionado imágenes ECS completas de la lista de imágenes.

Si selecciona esta opción, el sistema eliminará Copias de respaldo de CSBS o CBR. Después de eliminar las copias de respaldo de CSBS o CBR, ya no se cobran.

NOTA

Si las copias de respaldo de CSBS o CBR no se eliminan, la causa puede ser que estas copias de respaldo se están creando y no se pueden eliminar. En este caso, elimínelos manualmente como se le indique.

5. Haga clic en **Yes**.

3.6 Compartir imágenes

3.6.1 Descripción

Puede compartir sus imágenes privadas con otros tenants. Los tenants que acepten las imágenes compartidas pueden usar las imágenes para crear los ECS de las mismas especificaciones.

 **ATENCIÓN**

La plataforma en la nube no es responsable de la integridad o seguridad de las imágenes compartidas. Cuando utilice una imagen compartida, asegúrese de que la imagen proviene de un usuario compartido de confianza.

Restricciones

- No puede compartir imágenes privadas que se hayan publicado en Marketplace.
- Solo puede compartir imágenes dentro de la región en la que residen. Para compartir una imagen entre regiones, primero debe replicar la imagen en la región de destino.
- Una imagen de disco del sistema o una imagen de disco de datos se puede compartir con hasta 128 tenants, proyectos u organizaciones, y una imagen completa de ECS se puede compartir con hasta 10 tenants, proyectos u organizaciones.

 **NOTA**

Actualmente, el uso compartido de imágenes con una cuenta u organización solo está disponible en ciertas regiones.

- Una imagen completa de ECS solo se puede compartir cuando se crea a partir de una copia de respaldo de CBR o de un ECS que nunca ha tenido una copia de respaldo de CSBS.

Procedimiento

Si desea compartir una imagen privada con otro tenant, el procedimiento es el siguiente:

1. Usted obtiene el ID de proyecto, ID de cuenta u organización URN de tenant.

 **NOTA**

Para obtener más información sobre cómo obtener un ID de proyecto o un ID de cuenta, consulte [Obtención de información de cuenta, usuario de IAM, grupo, proyecto, región y delegación](#). Para obtener detalles sobre cómo obtener un URN de organización, consulte [Ver detalles sobre una organización](#).

2. Comparte una imagen con el tenant.
3. El tenant acepta la imagen compartida.

Después de aceptar la imagen, el tenant puede usarla para crear ECS.

 **NOTA**

Si la imagen se comparte con una cuenta u organización, el tenant puede omitir este paso.

Preguntas frecuentes relacionadas

Si tiene alguna pregunta, consulte [Preguntas frecuentes sobre el uso compartido de imágenes](#).

3.6.2 Obtención del ID de proyecto, ID de cuenta y organización URN

Escenarios

Antes de que un tenant comparta una imagen con usted, debe proporcionar su ID de proyecto, ID de cuenta u organización URN. Para obtener más información sobre cómo obtener un ID de proyecto o un ID de cuenta, consulte [Procedimiento](#). Para obtener detalles sobre cómo obtener una organización URN, consulte [Ver detalles sobre una organización](#).

NOTA

Actualmente, el uso compartido de imágenes con una cuenta u organización solo está disponible en ciertas regiones.

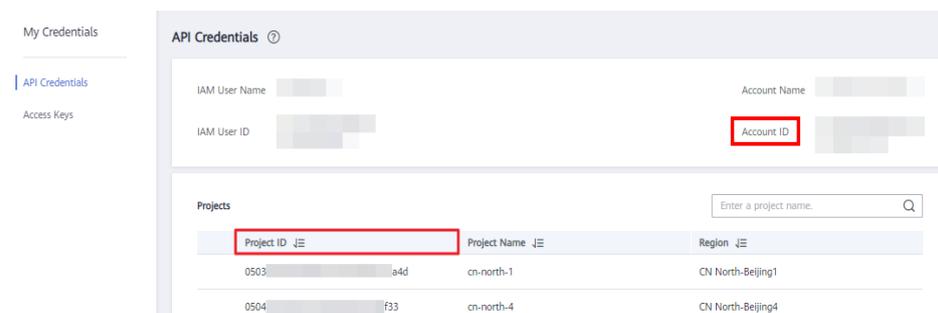
Procedimiento

1. Acceda a la consola de IMS.
 - a. Inicie sesión en la consola de gestión.
 - b. En **Compute**, haga clic en **Image Management Service**.
Se muestra la consola de IMS.
2. Haga clic en el nombre de usuario en la esquina superior derecha y seleccione **My Credentials** en la lista desplegable.

En la página **My Credentials**, vea el ID de proyecto o el ID de cuenta.

Las imágenes solo se pueden compartir dentro de la región donde residen. Por lo tanto, obtenga el ID del proyecto, el ID de cuenta u organización URN en la misma región.

Figura 3-6 Consulta del ID del proyecto o el ID de la cuenta



3.6.3 Compartir imágenes especificadas

Escenarios

Después de obtener el ID del proyecto de un tenant, puede compartir las imágenes privadas especificadas con el tenant. Puede compartir una sola imagen o varias imágenes según sea necesario.

Prerrequisitos

- Ha obtenido el ID del proyecto del tenant objetivo.

- Antes de compartir una imagen, asegúrese de que se hayan eliminado los datos confidenciales de la imagen.

Procedimiento

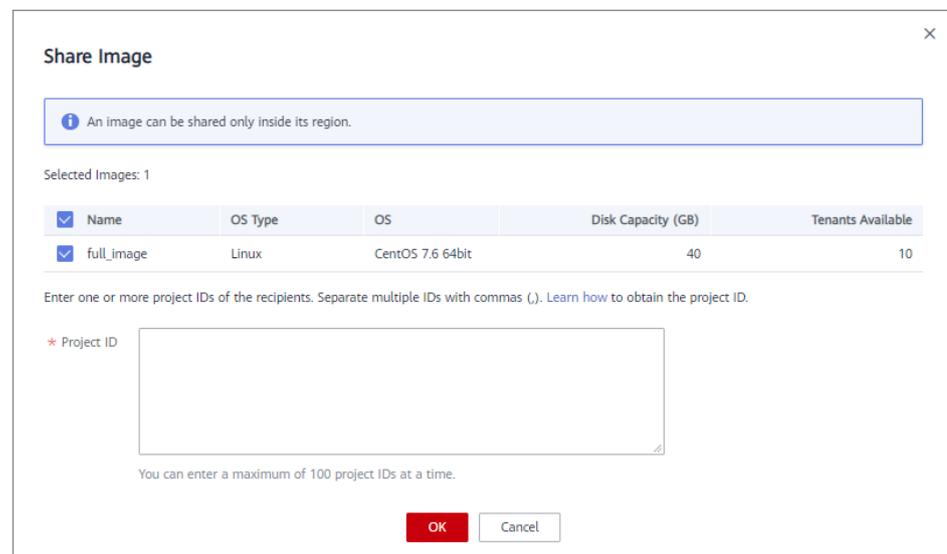
- Compartir varias imágenes.
 - a. Acceda a la consola de IMS.
 - i. Inicie sesión en la consola de gestión.
 - ii. En **Compute**, haga clic en **Image Management Service**.
Se muestra la consola de IMS.
 - b. Haga clic en la pestaña **Private Images**.
 - c. Seleccione las imágenes privadas que desea compartir y haga clic en **Share** encima de la lista de imágenes.
 - d. En el cuadro de diálogo **Share Image**, introduzca el ID del proyecto del tenant objetivo.

Para compartir imágenes con más de un tenant, separe sus ID de proyecto con comas (,).

📖 NOTA

- Se pueden ingresar 100 ID de proyecto al mismo tiempo, como máximo.
- Puede compartir imágenes solo dentro de la región en la que residen. Para compartir una imagen entre regiones, primero debe replicar la imagen en la región de destino.
- Si el tenant de destino es un usuario de varios proyectos, puede compartir imágenes con cualquier proyecto del tenant.

Figura 3-7 Compartir imágenes



- e. Haga clic en **OK**.
- Compartir una sola imagen.
 - a. Acceda a la consola de IMS.
 - i. Inicie sesión en la consola de gestión.
 - ii. En **Compute**, haga clic en **Image Management Service**.

Se muestra la consola de IMS.

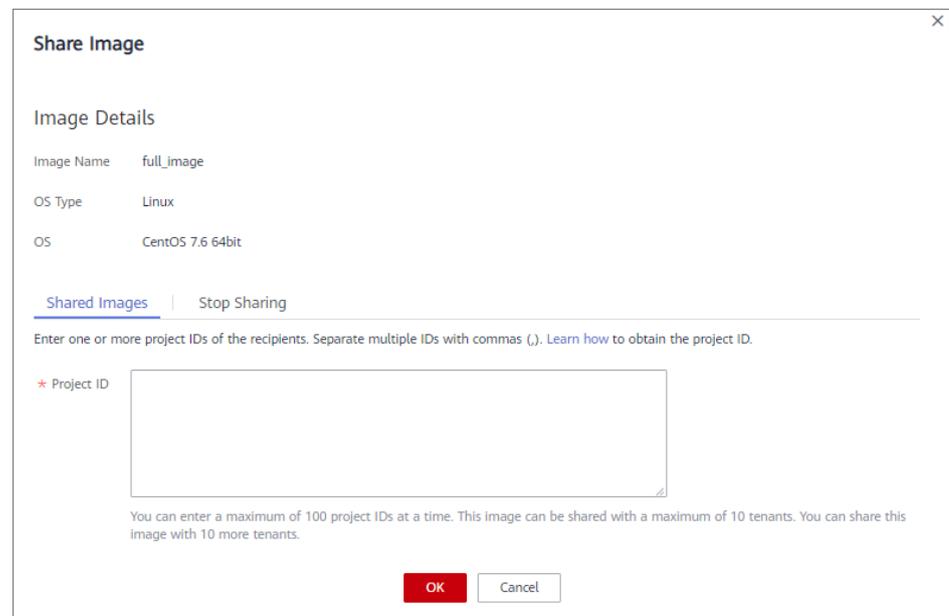
- b. Haga clic en la pestaña **Private Images**.
- c. Busque la fila que contiene la imagen privada que desea compartir, haga clic en **More** en la columna **Operation** y seleccione **Share** en la lista desplegable.
- d. En el cuadro de diálogo **Share Image**, introduzca el ID del proyecto del tenant objetivo.

Para compartir una imagen con más de un tenant, separe sus ID de proyecto con comas (,).

 **NOTA**

- Se pueden ingresar 100 ID de proyecto al mismo tiempo, como máximo.
- Puede compartir imágenes solo dentro de la región en la que residen. Para compartir una imagen entre regiones, primero debe replicar la imagen en la región de destino.
- Si el tenant de destino es un usuario de varios proyectos, puede compartir imágenes con cualquier proyecto del tenant.

Figura 3-8 Compartir una imagen



- e. Click **OK**.

Operaciones relacionadas

Después de compartir imágenes con un tenant, este puede aceptar las imágenes compartidas en la página **Images Shared with Me** de la consola IMS. Para obtener información detallada sobre las operaciones, consulte [Aceptación o rechazo de imágenes compartidas](#).

3.6.4 Aceptación o rechazo de imágenes compartidas

Escenarios

Después de que otro tenant comparta imágenes con usted, recibirá un mensaje. Puede optar por aceptar o rechazar todas o algunas de las imágenes compartidas.

NOTA

- Si no se encuentra en la misma región que el tenant que comparte las imágenes con usted, no recibirá el mensaje.
- Si las imágenes se comparten con su cuenta u organización, omita esta sección.
Actualmente, el uso compartido de imágenes con una cuenta u organización solo está disponible en ciertas regiones.

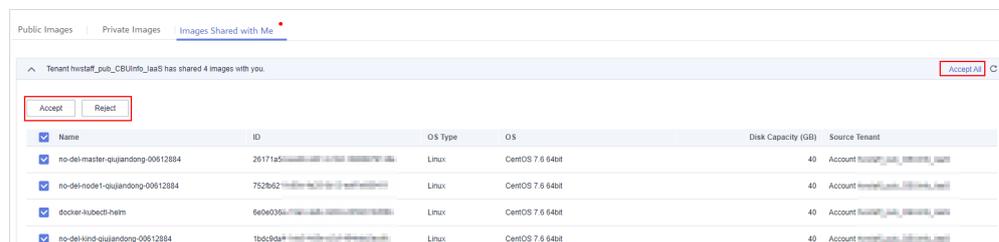
Prerrequisitos

- Otro tenant ha compartido imágenes con usted.
- Si la imagen compartida es una imagen de ECS completo, debe crear un almacén de copia de respaldo del servidor para almacenar la imagen completa de ECS y las copias de respaldo de la imagen de ECS completo antes de aceptar la imagen compartida. Cuando cree un almacén de copia de respaldo del servidor, establezca **Protection Type** en **Backup**.

Procedimiento

1. Acceda a la consola de IMS.
 - a. Inicie sesión en la consola de gestión.
 - b. En **Compute**, haga clic en **Image Management Service**.
Se muestra la consola de IMS.
2. En la esquina superior izquierda, cambie a la región donde reside el proyecto de destino y, a continuación, seleccione el proyecto.
3. Haga clic en la ficha **Images Shared with Me**.
Aparece un mensaje encima de la lista de imágenes que le pregunta si desea aceptar las imágenes compartidas.
 - Para aceptar todas las imágenes compartidas, haga clic en **Accept All** en la esquina superior derecha.
 - Para aceptar algunas imágenes, seleccione las imágenes y haga clic en **Accept**.
 - Para rechazar algunas imágenes, seleccione las imágenes y haga clic en **Reject**.

Figura 3-9 Aceptación o rechazo de imágenes compartidas



NOTA

- Si no se muestra ningún mensaje, compruebe si ha seleccionado una región correcta.
4. (Opcional) En el cuadro de diálogo **Accept Full-ECS Image**, seleccione un almacén de copia de seguridad del servidor con el tipo de protección de **Backup** y haga clic en **OK**. Este cuadro de diálogo se muestra cuando la imagen compartida es una imagen ECS completa.

Al aceptar una imagen completa del ECS, debe especificar un almacén para almacenar las copias de respaldo de CBR asociadas a la imagen completa del ECS. La capacidad del almacén no debe ser inferior a la capacidad total de las copias de seguridad del disco del sistema y del disco de datos.

 **NOTA**

Para obtener más información acerca de los almacenes de copia de respaldo del servidor, vea [¿Qué es el CBR?](#)

Resultados

- **Pending:** Si no acepta o rechaza inmediatamente una imagen compartida, la imagen se encuentra en el estado **pendiente**.

Una imagen compartida pendiente no se muestra en la lista de imágenes compartidas.

- **Accepted:** Después de aceptar una imagen, se muestra en la lista de imágenes compartidas. Puede utilizar la imagen para crear ECS.
- **Rejected:** Después de rechazar una imagen, no se muestra en la lista de imágenes compartidas. Puede hacer clic en **Rejected Images** para ver las imágenes que ha rechazado y aun así puede elegir aceptarlas.

 **NOTA**

- Si una imagen se comparte tanto con tu proyecto como con tu cuenta, la imagen se puede mostrar en la lista de imágenes compartidas y puedes usarla incluso si no se acepta ni se rechaza el uso compartido con tu proyecto.
- Si una imagen se comparte tanto con tu proyecto como con tu organización, la imagen se puede mostrar en la lista de imágenes compartidas y puedes usarla incluso si no se acepta ni se rechaza el uso compartido con tu proyecto.

Procedimiento posterior

Después de aceptar una imagen de disco del sistema compartida por otro tenant, puede:

- Utilice la imagen para crear uno o más ECS (seleccione **Shared Image** durante la creación de ECS). Para obtener más información, consulte [Compra de un ECS](#).
- Utilice la imagen para cambiar el sistema operativo de los ECS existentes. Para obtener más información, consulte [Cambio del SO](#).

Figura 3-10 Cambio del SO

Change OS ×

Selected specifications s3.small.1 | 1 vCPUs | 1 GB

Current Image EulerOS 2.2 64bit
System Disk Capacity: 40 GB OS Bit: 64-bit

Select an image

Image Type Public image Private image Shared image Marketplace image

Image discuz_centos6.5 ↕ ↻

Login Mode Password Key pair

Password Keep the password secure. If you forget the password, you can log in to the ECS console and reset the password.

OK Cancel

Después de aceptar una imagen de disco de datos compartida por otro tenant, puede usar la imagen para crear discos de EVS (localice la fila que contiene la imagen y haga clic en **Create Data Disk** en la columna **Operation**).

3.6.5 Rechazo de imágenes aceptadas

Escenarios

Puede rechazar las imágenes aceptadas si ya no las necesita.

Después de rechazar una imagen, no se mostrará en la página **Images Shared with Me**.

Prerrequisitos

Ha aceptado imágenes compartidas por otros usuarios.

Procedimiento

1. Acceda a la consola IMS.
 - a. Inicie sesión en la consola de gestión.
 - b. En **Compute**, haga clic en **Image Management Service**.
Se muestra la consola IMS.
2. Haga clic en la ficha **Images Shared with Me**.
3. Determine el siguiente paso en función de cuántas imágenes debe rechazar.
 - Para rechazar varias imágenes: seleccione las imágenes que desea rechazar y haga clic en **Reject** encima de la lista de imágenes. En el cuadro de diálogo que se muestra, haga clic en **Yes**.

- Para rechazar una imagen específica: localice la imagen que se va a rechazar y elija **More > Reject** en la columna **Operation**. En el cuadro de diálogo que se muestra, haga clic en **Yes**.

3.6.6 Aceptación de imágenes rechazadas

Escenarios

Si desea utilizar las imágenes compartidas que ha rechazado, puede aceptarlas de la lista de imágenes rechazadas.

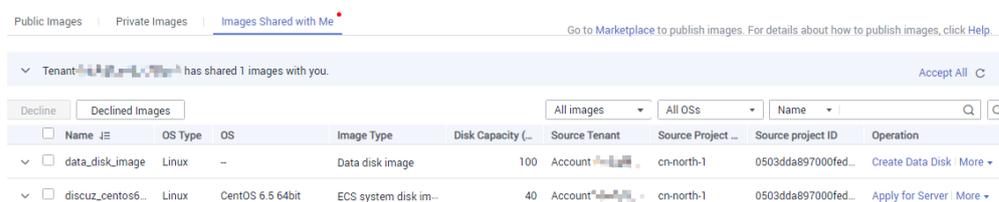
Prerrequisitos

- Ha rechazado las imágenes compartidas por otros.
- Los propietarios de la imagen no han dejado de compartir las imágenes.

Procedimiento

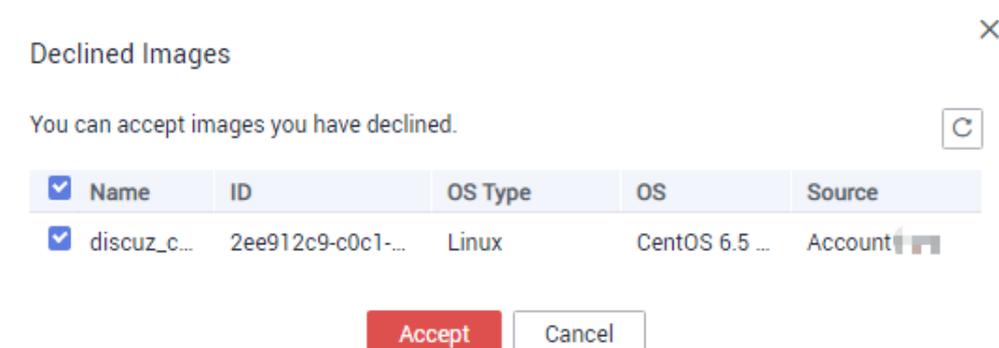
1. Acceda a la consola IMS.
 - a. Inicie sesión en la consola de gestión.
 - b. En **Compute**, haga clic en **Image Management Service**.
Se muestra la consola IMS.
2. Haga clic en la ficha **Images Shared with Me**.

Figura 3-11 Images Shared with Me



3. Haga clic en **Rejected Images**. Se muestran todas las imágenes rechazadas.

Figura 3-12 Imágenes rechazadas



4. Seleccione las imágenes que desea aceptar y haga clic en **Accept**.
5. Verifique las imágenes aceptadas en la lista de imágenes compartidas.

3.6.7 Dejar de compartir imágenes

Escenarios

Puedes dejar de compartir imágenes. Después de dejar de compartir una imagen:

- La imagen será invisible para el destinatario en la consola de gestión y no se devolverán datos cuando el destinatario consulte la imagen a través de una API.
- El destinatario no puede usar la imagen para crear un disco de ECS o EVS, ni cambiar el sistema operativo de un ECS.
- El destinatario no puede reinstalar el sistema operativo de los ECS creados a partir de la imagen compartida ni crear instancias idénticas a estos ECS.

NOTA

Si una imagen se comparte con un proyecto, una cuenta y también con una organización que se puede incluir entre sí, debe dejar de compartir la imagen con todos ellos para detener por completo el uso compartido.

Prerrequisitos

Ha compartido imágenes privadas con otros.

Procedimiento

1. Acceda a la consola IMS.
 - a. Inicie sesión en la consola de gestión.
 - b. En **Compute**, haga clic en **Image Management Service**.
Se muestra la consola IMS.
2. Haga clic en la pestaña **Private Images**.
3. Busque la fila que contiene la imagen privada que ya no desea compartir y elija **More > Share** en la columna **Operation**.
4. En el cuadro de diálogo **Share Image**, haga clic en la pestaña **Stop Sharing**.
5. Seleccione , cuenta, u organización del proyecto para el que desea detener el uso compartido de imágenes y haga clic en **OK**.

3.6.8 Adición de tenants que pueden usar imágenes compartidas

Escenarios

Además de los tenants con los que ha compartido imágenes, puede agregar más tenants que pueden usar las imágenes compartidas.

Prerrequisitos

- Debe compartir imágenes privadas.
- Usted ha obtenido los ID del proyecto, ID de cuenta, u organización URN de los tenants a agregar.

Procedimiento

1. Acceda a la consola IMS.
 - a. Inicie sesión en la consola de gestión.
 - b. En **Compute**, haga clic en **Image Management Service**.
Se muestra la consola IMS.
2. Haga clic en la pestaña **Private Images**.
3. Haga clic en el nombre de la imagen para ver los detalles.
4. Haga clic en **Add Tenant**.
5. En el cuadro de diálogo **Add Tenant**, escriba el ID del proyecto, el ID de cuenta u organización URN del tenant que se va a agregar y haga clic en **OK**.
Para agregar varios tenants, ingrese sus ID de proyecto, ID de cuenta u organización URN y sepárelos con comas (.). Haga clic en **OK**.

NOTA

- Puede compartir imágenes solo dentro de la región en la que residen. Para compartir una imagen entre regiones, primero debe replicar la imagen en la región de destino.
- Un ID de proyecto identifica de forma única a un tenant en una región específica. Si introduce un ID de proyecto que pertenece a una región diferente a la de las imágenes, se mostrará un mensaje indicando que no se puede encontrar el tenant.

3.6.9 Eliminación de destinatarios de imágenes que pueden usar imágenes compartidas

Escenarios

En esta sección se describe cómo eliminar destinatarios de imágenes que pueden usar imágenes compartidas.

Prerrequisitos

- Debe compartir imágenes privadas.
- Ha obtenido el ID de proyecto, ID de cuenta u organización URN de los destinatarios de la imagen.

Procedimiento

1. Acceda a la consola IMS.
 - a. Inicie sesión en la consola de gestión.
 - b. En **Compute**, haga clic en **Image Management Service**.
Se muestra la consola IMS.
2. Haga clic en la pestaña **Private Images**.
3. Haga clic en el nombre de la imagen para ver los detalles.
4. Vea los tenants que pueden usar la imagen compartida.
5. Eliminar uno o todos los destinatarios:
 - Para eliminar un único destinatario de imagen, localice el destinatario de destino y haga clic en **Delete**.

- Para eliminar todos los destinatarios de imágenes, haga clic en **Delete All** todo encima de la lista de destinatarios de imágenes.

6. Haga clic en **Yes**.

3.6.10 Replicación de una imagen compartida

Escenarios

Replicar una imagen privada que se compartió con usted. La imagen se muestra en la lista de imágenes privadas. Puede exportar, compartir y replicar esta imagen, o utilizarla para crear ECS.

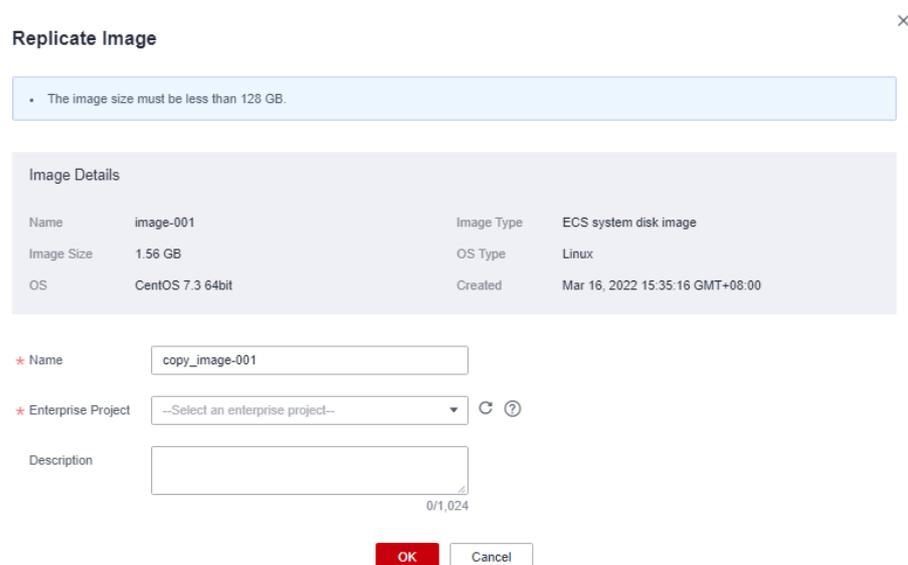
Restricciones

- Actualmente, solo se pueden replicar imágenes de disco de datos y de sistema. Las imágenes de ECS completas no son compatibles.
- Actualmente, las imágenes solo se pueden replicar dentro de una región.
- Una imagen que se va a replicar no puede tener más de 128 GB.
- No se puede replicar una imagen para generar una imagen cifrada.

Procedimiento

1. Acceda a la consola IMS.
 - a. Inicie sesión en la consola de gestión.
 - b. En **Compute**, haga clic en **Image Management Service**.
Se muestra la consola IMS.
2. En la consola IMS mostrada, haga clic en la pestaña **Images Shared with Me**.
Se muestran las imágenes compartidas que se aceptan.
3. Busque una imagen compartida, haga clic en **More** en la columna **Operation** y seleccione **Replicate** en la lista desplegable.

Figura 3-13 Replicación de una imagen



4. En el cuadro de diálogo **Replicate Image**, especifique **Name**, **Enterprise Project** y **Description**.
5. Haga clic en **OK**.

Puede hacer clic en la pestaña **Private Images** y ver el progreso de creación de la imagen en la lista de imágenes privadas. Cuando el estado de la imagen cambia a **Normal**, la creación de la imagen se completa.

3.7 Exportación de una imagen

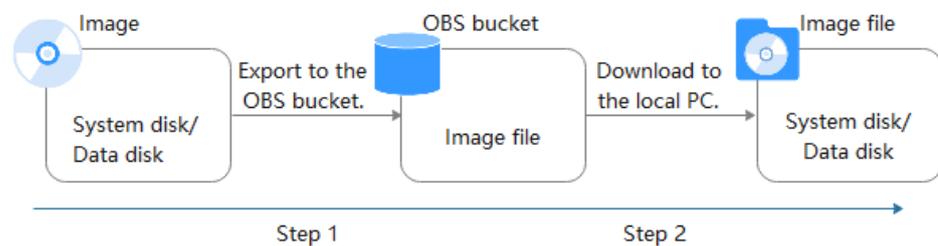
Escenarios

Puede exportar una imagen privada a un bucket de OBS estándar y luego descargarla a su PC local.

Antecedentes

- Puede reproducir servidores en la nube y sus entornos en ejecución en clústeres o nubes privadas mediante la exportación de sus imágenes desde la plataforma en la nube. En la siguiente figura se muestra el proceso de exportación de una imagen.

Figura 3-14 Exportación de una imagen



- El tiempo necesario para exportar una imagen depende del tamaño de la imagen y del número de tareas de exportación simultáneas.
- Puede exportar imágenes en formato ZVHD2, QCOW2, VMDK, VHD o ZVHD. El formato predeterminado de una imagen privada es ZVHD2. Las imágenes exportadas en diferentes formatos pueden variar en tamaño.
- Si una imagen tiene más de 128 GB, puede seleccionar **Enable** para **Fast Export** al exportar la imagen a un bucket de OBS. En este caso, no puede especificar el formato de la imagen exportada. Puede convertir el formato de imagen después de que se exporte.

📖 NOTA

Exportación rápida no está disponible para imágenes encriptadas. Para exportar una imagen cifrada, descifrela primero.

Restricciones

- Una imagen solo se puede exportar a un bucket estándar que esté en la misma región que la imagen.
- No se pueden exportar las siguientes imágenes privadas:
 - Imágenes completas de ECS

- Imágenes de ISO
- Imágenes privadas creadas a partir de una imagen pública de Windows, SUSE, Red Hat, Ubuntu u Oracle Linux
- Imágenes privadas creadas a partir de una imagen de Marketplace
- El tamaño de la imagen debe ser inferior a 1 TB. Las imágenes de más de 128 GB solo admiten exportación rápida.

 **NOTA**

En algunas regiones, una imagen de más de 128 GB se puede exportar normalmente (no es una exportación rápida).

Prerrequisitos

- Tiene permisos de administrador para OBS.
- Un bucket de OBS está disponible en la región donde se encuentra la imagen privada.
Si no hay ningún bucket de OBS disponible, cree uno consultando [Creación de un bucket](#). Seleccione **Standard** para **Storage Class**.

 **NOTA**

Se le cobrará por almacenar imágenes exportadas en el bucket de OBS. Para obtener más información, consulte [Detalles de precios de OBS](#).

Procedimiento

1. Acceda a la consola IMS.
 - a. Inicie sesión en la consola de gestión.
 - b. En **Compute**, haga clic en **Image Management Service**.
Se muestra la consola IMS.
2. Busque la fila que contiene la imagen que se va a exportar, haga clic en **More** en la columna **Operation** y seleccione **Export**.
3. En el cuadro de diálogo **Export Image** que se muestra, establezca los parámetros siguientes:
 - **Exportación rápida:** Para exportar una imagen de más de 128 GB, debe habilitar la exportación rápida y no puede especificar el formato de la imagen exportada (que solo puede ser ZVHD2). Después de exportar la imagen, puede usar **qemu-img-hw** para convertirla al formato deseado. Para obtener más información, consulte [Conversión del formato de imagen mediante qemu-img-hw](#).

 **NOTA**

Para obtener más información sobre las diferencias entre exportación y exportación rápida, consulte [Comparación entre importación e importación rápida y entre exportación y exportación rápida](#).

- **Format:** Seleccione uno de **qcow2**, **vmdk**, **vhd**, y **zvhd** como lo necesite.
- **Name:** Introduzca un nombre que sea fácil de identificar.
- **Storage Path:** Haga clic en  para expandir la lista de bucket y seleccione un bucket de OBS para almacenar la imagen exportada.

NOTA

Una imagen solo se puede exportar a un bucket estándar que esté en la misma región que la imagen. Por lo tanto, solo tales buckets están disponibles en la lista.

4. Haga clic en **OK**.
Puede ver el progreso de la exportación de imágenes encima de la lista de imágenes privadas.

Procedimiento posterior

Después de exportar la imagen con éxito, puede descargarla desde el bucket OBS a través de la consola de gestión u OBS Browser+. Para obtener más información, consulte [Descarga de un archivo](#).

3.8 Optimización de una imagen privada de Windows

3.8.1 Proceso de optimización

El correcto funcionamiento de los ECS depende del controlador Xen Guest OS (controlador PV) y el controlador KVM Guest OS (UVP VMTools). Para garantizar que los ECS admitan tanto Xen como KVM y para mejorar el rendimiento de la red, se debe instalar el controlador PV y UVP VMTools para la imagen.

1. Cree un ECS utilizando la imagen privada de Windows que se va a optimizar e inicie sesión en el ECS.
2. Instale la versión más reciente de PV driver en el ECS.
Para obtener más información, véase [Instalación del PV driver](#).
3. Instale el UVP VMTools que se requieren para crear los ECS utilizando recursos virtuales de KVM.
Para obtener más información, véase [Instalación de UVP VMTools](#).
4. En el ECS, seleccione **Control Panel > Power Options**. Haga clic en **Choose when to turn off the display**, seleccione **Never** para **Turn off the display** y guarde los cambios.
5. Borre los registros del sistema y, a continuación, detenga el ECS.
Para obtener más información, véase [Borrar registros del sistema](#).
6. Cree una imagen privada de Windows desde el ECS.

3.8.2 Visualización del tipo de virtualización de un ECS de Windows

Abra la ventana cmd y ejecute el siguiente comando para consultar el tipo de virtualización del ECS:

```
systeminfo
```

Si los valores del **System Manufacturer** y **BIOS Version** son **Xen**, el ECS utiliza Xen. Para que la imagen privada de Windows admita KVM al mismo tiempo, realice las operaciones en las siguientes secciones del ECS.

NOTA

Si el ECS utiliza KVM, también se recomienda optimizar la imagen privada para evitar excepciones con los ECS creados a partir de la imagen.

Figura 3-15 Visualización del tipo de virtualización de un ECS de Windows

```

systeminfo
Host Name: ECS-E5AF
OS Name: Microsoft Windows Server 2012 R2 Datacenter
OS Version: 6.3.9600 N/A Build 9600
OS Manufacturer: Microsoft Corporation
OS Configuration: Standalone Server
OS Build Type: Multiprocessor Free
Registered Owner: Windows User
Registered Organization:
Product ID: 00253-50000-00000-AA442
Original Install Date: 11/2/2015, 21:05:21
System Boot Time: 8/2/2018, 10:31:04
System Manufacturer: Ken
System Model: HUN HUN
System Type: x64-based PC
Processor(s): 1 Processor(s) Installed.
               [01]: Intel64 Family 6 Model 62 Stepping 4 GenuineIn
               tel 3200 MHz
BIOS Version: Ken 4.1.2.115-908.762., 3/21/2018
Windows Directory: C:\Windows
System Directory: C:\Windows\system32
Boot Device: \Device\HarddiskVolume1
System Locale: en-us;English (United States)
Input Locale: en-us;English (United States)
Time Zone: (UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi
Total Physical Memory: 1.016 MB
Available Physical Memory: 226 MB
Virtual Memory: Max Size: 1.336 MB
Virtual Memory: Available: 476 MB
Virtual Memory: In Use: 860 MB
    
```

3.8.3 Obtención de paquetes de software requeridos

PV Driver

Tabla 3-1 enumera los paquetes de software de controlador PV necesarios para optimizar las imágenes privadas de Windows.

Tabla 3-1 Paquetes de software de PV driver

Paquete de software	OS	Cómo obtenerlo
pvdriver-win2008R2-64bit.zip	Windows Server 2008 R2 64bit	https://ecs-instance-driver.obs.cn-north-1.myhuaweicloud.com/pvdriver-win2008R2-64bit.zip
pvdriver-win2012-64bit.zip	Windows Server 2012 64bit	https://ecs-instance-driver.obs.cn-north-1.myhuaweicloud.com/pvdriver-win2012-64bit.zip
pvdriver-win2012R2-64bit.zip	Windows Server 2012 R2 64bit	https://ecs-instance-driver.obs.cn-north-1.myhuaweicloud.com/pvdriver-win2012R2-64bit.zip
pvdriver-win2016-64bit.zip	Windows Server 2016 64bit	https://ecs-instance-driver.obs.cn-north-1.myhuaweicloud.com/pvdriver-win2016-64bit.zip
pvdriver-win2019-64bit.zip	Windows Server 2019 64bit	https://ecs-instance-driver.obs.cn-north-1.myhuaweicloud.com/pvdriver-win2019-64bit.zip

UVP VMTools

Tabla 3-2 lista los paquetes de software UVP VMTools necesarios para optimizar las imágenes privadas de Windows.

Tabla 3-2 Paquetes de software de UVP VMTools

Paquete de software	OS	Cómo obtenerlo
vmtools-WIN2008-x86.zip	Windows Server 2008-x86	https://ecs-instance-driver.obs.cn-north-1.myhuaweicloud.com/vmtools-WIN2008-x86.zip
vmtools-WIN2008-x64.zip	Windows Server 2008-x64	https://ecs-instance-driver.obs.cn-north-1.myhuaweicloud.com/vmtools-WIN2008-x64.zip
vmtools-WIN2008R2-x64.zip	Windows Server 2008 R2-x64	https://ecs-instance-driver.obs.cn-north-1.myhuaweicloud.com/vmtools-WIN2008R2-x64.zip
vmtools-WIN2012-x64.zip	Windows Server 2012-x64	https://ecs-instance-driver.obs.cn-north-1.myhuaweicloud.com/vmtools-WIN2012-x64.zip
vmtools-WIN2012R2-x64.zip	Windows Server 2012 R2-x64	https://ecs-instance-driver.obs.cn-north-1.myhuaweicloud.com/vmtools-WIN2012R2-x64.zip
vmtools-WIN2016-x64.zip	<ul style="list-style-type: none"> ● Windows Server 2016-x64 ● Windows Server 2019-x64 	https://ecs-instance-driver.obs.cn-north-1.myhuaweicloud.com/vmtools-WIN2016-x64.zip

3.8.4 Instalación del PV driver

Esta sección solo se aplica a los ECS de Xen, que han sido descontinuados y ya no están disponibles para nuevos usuarios. Para obtener más información, consulte [Especificaciones de ECS descontinuadas](#). Si es un usuario nuevo o ya es un usuario que utilizará esta imagen para crear un ECS que no sea Xen, omita esta sección.

Escenarios

Cuando utilice un ECS o archivo de imagen externo para crear una imagen privada, asegúrese de que el PV driver se haya instalado en el sistema operativo para habilitar la virtualización de Xen para ECS creado posteriormente, mejore el rendimiento de procesamiento de E/S de ECS e implemente funciones avanzadas como monitorizar el hardware de los ECS.

 **ATENCIÓN**

Si no instala el PV driver, el rendimiento de la red ECS será deficiente y los grupos de seguridad y el firewall configurados para ECS no tendrán efecto.

El PV driver se ha instalado de forma predeterminada cuando se utiliza una imagen pública para crear ECS. Puede realizar las siguientes operaciones para verificar la instalación:

Abra el archivo de configuración de **version** para comprobar si el PV driver es el más reciente:

C:\Program Files (x86)\Xen PV Drivers\bin\version

- Si la versión del PV driver es posterior a 2.5, no es necesario instalar el PV driver.
- Si la versión del PV driver no se muestra o la versión es 2.5 o anterior, realice operaciones en [Instalación del PV driver](#) o [Instalación del paquete de actualización del PV driver](#).

Prerrequisitos

- Se ha instalado un sistema operativo para el ECS y se ha vinculado una EIP al ECS.
- La capacidad restante del disco del sistema ECS debe ser superior a 32 MB.
- Si ECS utiliza Windows 2008, debe instalar el PV driver con la cuenta de administrador.
- El paquete de software del PV driver se ha descargado en el ECS. Para obtener el paquete de software, consulte [Obtención de paquetes de software requeridos](#).
- Para evitar un error de instalación, realice las siguientes operaciones antes de iniciar la instalación:
 - Desinstale herramientas de plataforma de virtualización de terceros, como Citrix Xen Tools y VMware Tools. Para ver cómo desinstalar las herramientas, consulte los documentos oficiales correspondientes de las herramientas.
 - Deshabilite el software antivirus y de detección de intrusión. Puede activar el software después de instalar el PV driver.

Instalación del PV driver

1. Inicie sesión en el ECS de Windows mediante VNC.
Para obtener más información sobre cómo iniciar sesión en un ECS, consulte [Descripción del inicio de sesión](#).

 **NOTA**

Debe iniciar sesión en el ECS con VNC. No se permite la conexión a escritorio remoto porque el controlador de NIC necesita actualizarse durante la instalación, pero la NIC está en uso para la conexión a escritorio remoto. Como resultado, la instalación fallará.

2. En el ECS, elija **Start > Control Panel**.
3. Haga clic en **Uninstall a program**.
4. Desinstale **GPL PV drivers for Windows x.x.x.xx** según se indique.
5. Descargue el controlador PV requerido basado en el sistema operativo de ECS y [Obtención de paquetes de software requeridos](#).
6. Descomprima el paquete de software del PV driver.

7. Haga clic con el botón derecho del ratón en **GPL PV Drivers for Windows x.x.x.xx**, seleccione **Run as administrator** y complete la instalación según se le solicite.
8. Reinicie el ECS según se le solicite para que el PV driver surta efecto.
Los ECS que ejecutan Windows Server 2008 deben reiniciarse dos veces.

 **NOTA**

Después de instalar el PV driver, se perderá la configuración de la NIC de ECS. Si ha configurado las NIC antes, debe volver a configurarlas.

Instalación del paquete de actualización del PV driver

1. Inicie sesión en el ECS de Windows mediante VNC.
Para obtener más información sobre cómo iniciar sesión en un ECS, consulte [Descripción del inicio de sesión](#).

 **NOTA**

Debe iniciar sesión en el ECS con VNC. No se permite la conexión a escritorio remoto porque el controlador de NIC necesita actualizarse durante la instalación, pero la NIC está en uso para la conexión a escritorio remoto. Como resultado, la instalación fallará.

2. En el ECS, elija **Start > Control Panel**.
3. Elija **Programs > Uninstall a program**, encuentre el programa de PV driver y desinstálelo.
4. Una vez completada la desinstalación, reinicie el ECS para borrar el entorno.
5. Descarga **pvdriver-windows.zip** desde el siguiente enlace:
<https://ecs-instance-driver.obs.cn-north-1.myhuaweicloud.com/pvdriver-windows.zip>
6. Descarga **pvdriver-windows.zip** desde el siguiente enlace:
7. Haga clic en **Setup.exe** para instalar el PV driver. El paquete se adaptará automáticamente a la versión del sistema operativo.
8. Reinicie el ECS según se le solicite para que el PV driver surta efecto.
Los ECS que ejecutan Windows Server 2008 deben reiniciarse dos veces.

 **NOTA**

Después de instalar el PV driver, se perderá la configuración de la NIC de ECS. Si ha configurado las NIC antes, debe volver a configurarlas.

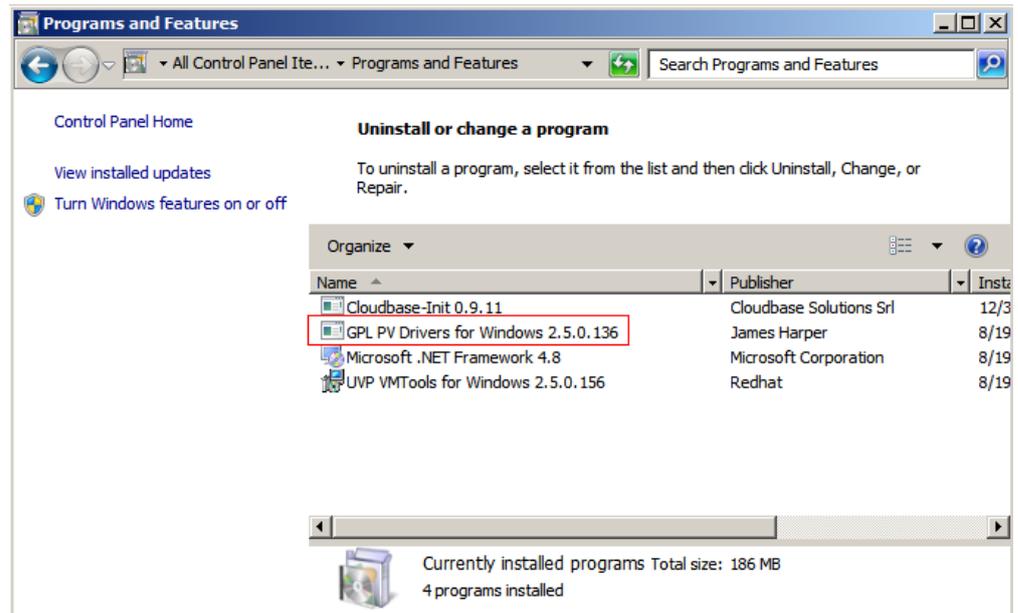
Verificación de la instalación

Realice los siguientes pasos para verificar la instalación del PV driver:

1. Haga clic en **Start**. Seleccione **Control Panel > Programs and Features**.
2. Localice el PV driver para Windows.

Si UVP VMTTools para Windows existe, la instalación se realiza correctamente, como se muestra en [Figura 3-16](#).

Figura 3-16 Verificación de la instalación



3.8.5 Instalación de UVP VMTools

Escenarios

Esta sección solo se aplica a los ECS de KVM, que reemplazarán gradualmente a los ECS de Xen. Antes de utilizar un ECS o un archivo de imagen externo para crear una imagen privada, asegúrese de que UVP VMTools se haya instalado en el sistema operativo para permitir que los correos electrónicos creados ECSs posteriormente admitan la virtualización de KVM y mejoren el rendimiento de la red.

ATENCIÓN

Si no instala UVP VMTools, es posible que no se detecten las NIC del ECS y el ECS no se pueda comunicar con otros recursos.

UVP VMTools se ha instalado de forma predeterminada cuando se utiliza una imagen pública para crear ECSs. Puede realizar las siguientes operaciones para verificar la instalación:

Abra el archivo de configuración de **version** para comprobar si UVP VMTools es el último:

C:\Program Files (x86)\virtio\bin\version

- Si no se muestra la versión de UVP VMTools, realice operaciones en [Instalación de UVP VMTools](#) o [Instalación del paquete de actualización de UVP VMTools](#) para instalar UVP VMTools.
- Si la versión es anterior a 2.5.0, instale UVP VMTools siguiendo las instrucciones en [Instalación del paquete de actualización de UVP VMTools](#).
- Si la versión es 2.5.0 o posterior, se pueden utilizar UVP VMTools actuales.

Prerrequisitos

- Una EIP ha sido vinculada al ECS.
- El paquete de instalación de UVP VMTools se ha descargado en el ECS. Para obtener el paquete de instalación, consulte [Obtención de paquetes de software requeridos](#).
- Asegúrese de que el ECS tenga al menos 50 MB de espacio en disco.
- Para evitar un error de instalación, realice las siguientes operaciones antes de iniciar la instalación:
 - Desinstale herramientas de plataforma de virtualización de terceros, como Citrix Xen Tools y VMware Tools. Para ver cómo desinstalar las herramientas, consulte los documentos oficiales correspondientes de las herramientas.
 - Deshabilite su antivirus y software de detección de intrusión. Puede activar el software después de que UVP VMTools esté instalado.

Instalación de UVP VMTools

Las siguientes operaciones describen cómo instalar UVP VMTools. **vmtools-WIN2016-x64.exe** extraído de **vmtools-WIN2016-x64.zip** se usa como ejemplo.

1. Inicie sesión en el ECS de Windows mediante VNC.

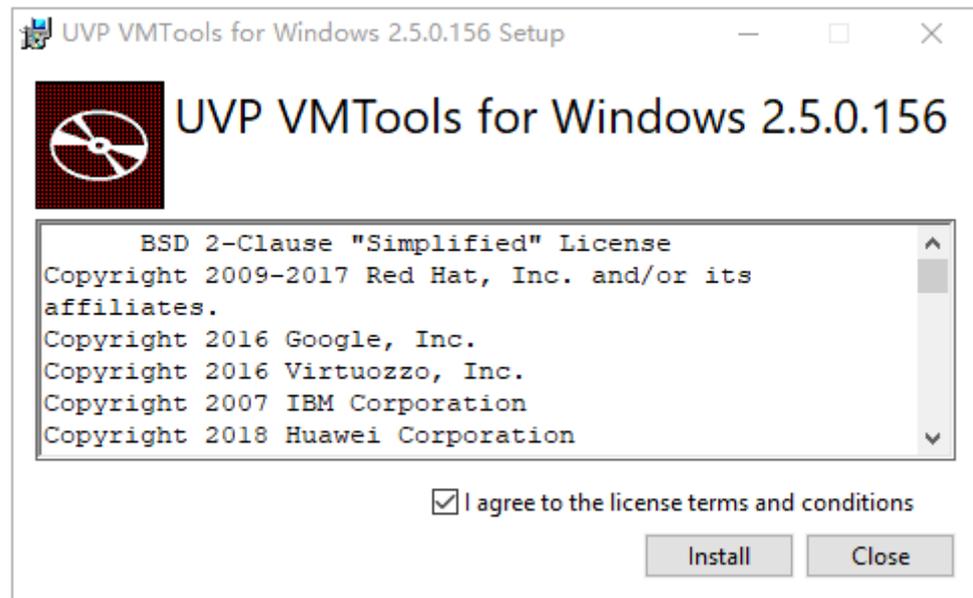
Para obtener más información sobre cómo iniciar sesión en un ECS, consulte [Descripción del inicio de sesión](#).

NOTA

Debe iniciar sesión en el ECS con VNC. No se permite la conexión a escritorio remoto porque el controlador de NIC necesita actualizarse durante la instalación, pero la NIC está en uso para la conexión a escritorio remoto. Como resultado, la instalación fallará.

2. Descargue los UVP VMTools requeridos basados en el sistema operativo ECS y [Obtención de paquetes de software requeridos](#).
3. Descomprima el paquete de software de UVP Tools **vmtools-WIN2016-x64.zip**.
4. Haga clic con el botón derecho en **vmtools-WIN2016-x64.exe** y seleccione **Run as administrator** en el menú contextual.
5. En el cuadro de diálogo que se muestra, seleccione **I agree to the license terms and conditions** y haga clic en **Install**.

Figura 3-17 Instalación de UVP VMTools



6. Reinicie el sistema operativo para que surta efecto UVP VMTools.
7. Realice las operaciones en [Verificación de la instalación](#) para comprobar si UVP VMTools se ha instalado correctamente.

Instalación del paquete de actualización de UVP VMTools

1. Inicie sesión en el ECS de Windows mediante VNC.
Para obtener más información sobre cómo iniciar sesión en un ECS, consulte [Descripción del inicio de sesión](#).

NOTA

Debe iniciar sesión en el ECS con VNC. No se permite la conexión a escritorio remoto porque el controlador de NIC necesita actualizarse durante la instalación, pero la NIC está en uso para la conexión a escritorio remoto. Como resultado, la instalación fallará.

2. Descargue **vmtools-windows.zip** desde el siguiente enlace:
<https://ecs-instance-driver.obs.cn-north-1.myhuaweicloud.com/vmtools-windows.zip>
3. Extraiga **vmtools-windows.iso** de **vmtools-windows.zip**.
4. Descomprima **vmtools-windows.iso** y haga clic en **Setup.exe** para actualizar UVP VMTools. El paquete de actualización se adaptará automáticamente a la versión del sistema operativo.
5. Realice las operaciones en [Verificación de la instalación](#) para comprobar si UVP VMTools se ha instalado correctamente.

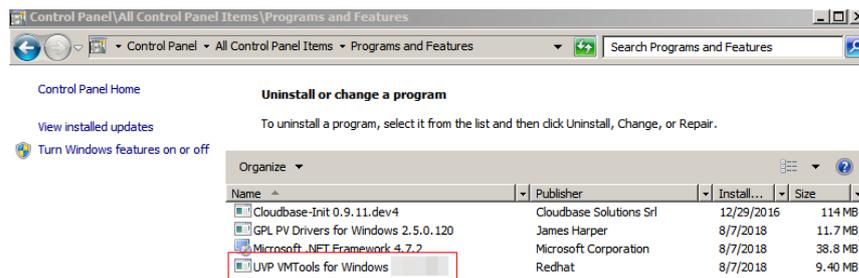
Verificación de la instalación

Realice los siguientes pasos para verificar la instalación de UVP VMTools:

1. Haga clic en **Start**. Seleccione **Control Panel > Programs and Features**.
2. Ubique UVP VMTools para Windows.

Si UVP VMTools para Windows existe, la instalación se realiza correctamente, como se muestra en [Figura 3-18](#).

Figura 3-18 Verificación de la instalación



3.8.6 Borrar registros del sistema

Después de instalar el PV driver y VMTools UVP, realice las siguientes operaciones para borrar los registros del sistema:

1. Para Windows Server 2008 y Windows Server 2012, haga clic con el botón derecho en **Computer** y seleccione **Manage**.
2. En el cuadro de diálogo que se muestra, elija **System Tools > Event Viewer > Windows Logs** y elimine los registros de cinco elementos.
3. Detengan el ECS.

3.9 Optimización de una imagen privada de Linux

3.9.1 Proceso de optimización

La virtualización de ECS está cambiando gradualmente de Xen a KVM. Por lo tanto, las imágenes privadas deben ser compatibles con Xen y KVM. Para asegurarse de que los ECS creados a partir de una imagen privada pueden ejecutarse correctamente, se recomienda optimizarlas sin importar que utilicen Xen o KVM.

Un ECS de Linux solo puede ejecutarse correctamente cuando se han instalado controladores nativos de KVM (VirtIO) en él y el ID de disco en su archivo de configuración de GRUB y archivo fstab se ha cambiado a UUID.

Preparaciones

1. Utilice la imagen de Linux para ser optimizada para **crear** un ECS, y comience e inicie sesión en el ECS.
2. Compruebe si la imagen privada necesita ser optimizada.

Para obtener más información, véase [Comprobación de si una imagen privada necesita ser optimizada](#).

El tipo de virtualización puede causar diferencias de segmento en un proceso de optimización.

Proceso

1. Desinstale PV drivers del ECS.
Para obtener más información, véase [Desinstalación de PV Drivers de un ECS de Linux](#).

 **NOTA**

Si el ECS está utilizando la virtualización de KVM, omita este paso.

2. Cambie el ID de disco en el archivo de configuración de GRUB a UUID.
Para obtener más información, véase [Cambio del identificador de disco en el archivo de configuración de GRUB a UUID](#).
3. Cambie el ID de disco en el archivo fstab a UUID.
Para obtener más información, véase [Cambio del identificador de disco en el archivo fstab a UUID](#).
4. Instale controladores de virtualización nativos.
Para KVM, instale controladores de KVM nativos. Para obtener más información, véase [Instalación de controladores KVM nativos](#).
5. Elimine los archivos de registro y los registros históricos, y detenga el ECS.
Para obtener más información, véase [Borrar registros del sistema](#).
6. Cree una imagen privada de Linux desde el ECS.

 **NOTA**

Alternativamente, puede utilizar un script para completar el proceso automáticamente. Para obtener más información, véase [Uso de un script para optimizar una imagen privada de Xen](#).

3.9.2 Comprobación de si una imagen privada necesita ser optimizada

- Si el tipo de virtualización es Xen, se requiere optimización.
- Si el tipo de virtualización es KVM y los controladores VirtIO no están instalados, se requiere optimización.
- Si el tipo de virtualización es KVM y los controladores VirtIO están instalados, no se requiere optimización.

Procedimiento

1. Ejecute el siguiente comando para comprobar el tipo de virtualización de un ECS:
lscpu
 - Si el valor de **Hypervisor vendor** es de **Xen**, optimice la imagen privada como se indica en [Proceso](#).
 - Si el valor de **Hypervisor vendor** es de **KVM**, vaya al siguiente paso para una comprobación adicional.

Figura 3-19 Comprobación del tipo de virtualización de un ECS de Linux

```
# lscpu
Architecture:          x86_64
CPU op-mode(s):      32-bit, 64-bit
Byte Order:          Little Endian
CPU(s):              4
On-line CPU(s) list: 0-3
Thread(s) per core:  1
Core(s) per socket:  4
Socket(s):           1
NUMA node(s):       1
Vendor ID:           GenuineIntel
CPU family:          6
Model:               62
Model name:          Intel(R) Xeon(R) CPU E5-2690 v2 @ 3.00GHz
Stepping:            4
CPU MHz:             3000.079
BogoMIPS:            6000.15
Hypervisor vendor:   Xen
Virtualization type: full
L1d cache:           32K
L1i cache:           32K
L2 cache:            256K
L3 cache:            25600K
NUMA node0 CPU(s):  0-3
You have new mail in /var/spool/mail/root
root@SZV-hemal#
```

2. Compruebe si se han instalado los controladores VirtIO.

– CentOS/EulerOS

Para `initramfs`, ejecute el siguiente comando:

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

Para `initrd`, ejecute el siguiente comando:

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

– Ubuntu/Debian

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

– SUSE/openSUSE

■ SUSE 12 SP1/openSUSE 13 o anterior:

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

■ SUSE 12 SP1 o posterior a SUSE 12 SP1/openSUSE 13:

Para `initramfs`, ejecute el siguiente comando:

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

Para `initrd`, ejecute el siguiente comando:

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

Si se muestra **virtio**, se han instalado los controladores VirtIO. Para obtener más información, consulte [Creación de una imagen de disco de sistema Linux a partir de un archivo de imagen externo](#).

```
root@SZV-hemal# lsinitrd /boot/initramfs-$(uname -r).img | grep virtio
-rw-r--r-- 1 root root 8984 Sep 30 2021 usr/lib/modules/4.18.0-348.7.1.el8_5.x86_64/kernel/drivers/block/virtio_b
lk.ko.xz
-rw-r--r-- 1 root root 14836 Sep 30 2021 usr/lib/modules/4.18.0-348.7.1.el8_5.x86_64/kernel/drivers/char/virtio_co
nsole.ko.xz
-rw-r--r-- 1 root root 25748 Sep 30 2021 usr/lib/modules/4.18.0-348.7.1.el8_5.x86_64/kernel/drivers/net/virtio_net
.ko.xz
-rw-r--r-- 1 root root 8684 Sep 30 2021 usr/lib/modules/4.18.0-348.7.1.el8_5.x86_64/kernel/drivers/scsi/virtio_sc
si.ko.xz
```

De lo contrario, los controladores VirtIO no se han instalado. Optimice la imagen privada según las instrucciones de [Proceso](#).

3.9.3 Uso de un script para optimizar una imagen privada de Xen

1. Utilice la imagen de Linux que se va a optimizar para crear un ECS, y comience e inicie sesión en el ECS.
2. Ejecute el siguiente comando para descargar el script de instalación del controlador en el directorio **root**:

```
curl URL > ~/resize_ecs_modify_linux.sh
```

URL indica la dirección de descarga del script.

https://latin-server-resize.obs.na-mexico-1.myhuaweicloud.com/resize_ecs_modify_linux.sh

3. Ejecute el siguiente comando para ejecutar el script:

```
bash resize_ecs_modify_linux.sh
```

Figura 3-20 Ejecución del script

```
suse11sp3:/home # bash resize_ecs_modify_linux.sh
2018-08-21 11:04:23 Info:*****BEGIN Modify*****
2018-08-21 11:04:23 Info:get linux system type and version...
2018-08-21 11:04:23 Info:system type: suse11
2018-08-21 11:04:23 Info:search grub file...
2018-08-21 11:04:23 Info:find grub file: /boot/grub/menu.lst
2018-08-21 11:04:23 Info:search initrd file list...
2018-08-21 11:04:23 Info:find initrd file: /boot/initrd-3.0.76-0.11-default
2018-08-21 11:04:23 Info:begin to modify grub file...
2018-08-21 11:04:23 Info:modify grub file: /boot/grub/menu.lst
2018-08-21 11:04:23 Info:backup file: /boot/grub/menu.lst
2018-08-21 11:04:23 Info:modify grub file success!
2018-08-21 11:04:23 Info:backup file: /boot/grub/menu.lst
2018-08-21 11:04:23 Info:add xen_platform_pci.dev_unplug=all in /boot/grub/menu.lst
2018-08-21 11:04:23 Info:begin to modify fstab file...
2018-08-21 11:04:23 Info:modify fstab file: /etc/fstab
2018-08-21 11:04:23 Info:backup file: /etc/fstab
2018-08-21 11:04:23 Info:modify fstab file success!
2018-08-21 11:04:23 Info:check xen/ide driver is already exist in initrd** or not
```

4. Espere hasta que se complete la ejecución del script. Si aparece el mensaje "*{Image name}* already contain xen and virtio driver", significa que los controladores se han instalado.

Figura 3-21 Ejecución exitosa del script

```
2018-08-21 11:04:23 Info:check xen/ide driver is already exist in initrd** or not
35604 blocks
35604 blocks
35604 blocks
35604 blocks
2018-08-21 11:04:24 Info:xen driver:yes
2018-08-21 11:04:24 Info:ide driver:yes
2018-08-21 11:04:24 Info:check virtio driver is already exist in initrd** or not
35604 blocks
35604 blocks
35604 blocks
35604 blocks
2018-08-21 11:04:25 Info:virtio driver:yes
2018-08-21 11:04:25 Info:suse11 already contain xen and virtio driver
```

3.9.4 Desinstalación de PV Drivers de un ECS de Linux

Escenarios

Al optimizar una imagen privada de Linux con la virtualización de Xen, debe instalar controladores nativos de Xen y KVM en el ECS de origen de la imagen.

Para asegurarse de que puede instalar correctamente los controladores Xen nativos y KVM, primero debe desinstalar los controladores PV del ECS.

Procedimiento

1. Inicie sesión en el ECS como usuario **root** con VNC.
2. Ejecute el siguiente comando para comprobar si PV drivers están instalados en el sistema operativo:

```
ps -ef | grep uvp-monitor
```

- Si se muestra la siguiente información, se han instalado PV drivers.
- De lo contrario, PV drivers no están instalados. No se requerirá ninguna otra acción.

```
root      4561          1      0   Jun29 ?        00:00:00  /usr/bin/uvp-  
monitor  
root      4567      4561      0   Jun29 ?        00:00:00  /usr/bin/uvp-  
monitor  
root      6185      6085      0   03:04 pts/2        00:00:00  grep uvp-monitor
```

3. En la ventana de inicio de sesión de VNC, abra la CLI.

Para ver cómo abrir la CLI, consulte el manual del sistema operativo.

4. Ejecute el siguiente comando para desinstalar PV drivers:

```
/etc/.uvp-monitor/uninstall
```

- PV drivers se desinstalan correctamente si se muestra el siguiente resultado del comando:

```
The PV driver is uninstalled successfully. Reboot the system for the  
uninstallation to take effect.
```

- Si la salida del comando indica que **.uvp-monitor** no se encuentra, vaya a [5](#).

```
-bash: /etc/.uvp-monitor/uninstall: No such file or directory
```

5. Realice las siguientes operaciones para eliminar uvp-monitor que no surtieron efecto, evitando el desbordamiento de registros:

- a. Ejecute el siguiente comando para comprobar si los programas de UVP en modo usuario están instalados en el sistema operativo:

```
rpm -qa | grep uvp
```

La información que aparecerá en pantalla será similar a la información siguiente:

```
libxenstore_uvp3_0-3.00-36.1.x86_64  
uvp-monitor-2.2.0.315-3.1.x86_64  
kmod-uvpmod-2.2.0.315-3.1.x86_64
```

- b. Ejecute los siguientes comandos para eliminar los paquetes de instalación:

```
rpm -e kmod-uvpmod
```

```
rpm -e uvp-monitor
```

```
rpm -e libxenstore_uvp
```

3.9.5 Cambio del identificador de disco en el archivo de configuración de GRUB a UUID

Escenarios

Al optimizar una imagen privada de Linux, debe cambiar el identificador de disco a UUID en el archivo de configuración de GRUB del ECS.

Modifique el archivo de configuración **menu.lst** o **grub.cfg** (**/boot/grub/menu.lst**, **/boot/grub/grub.cfg**, **/boot/grub2/grub.cfg**, **/boot/grub/grub.conf**, o **/boot/efi/EFI/euleros/grub.cfg**), y configure la partición de arranque usando el UUID.

📖 NOTA

La partición raíz identificada en el archivo de configuración varía según el sistema operativo. Puede ser **root=/dev/xvda** o **root=/dev/disk**.

Procedimiento

- Ubuntu 14.04: Ejecutar **blkid** para obtener el UUID de la partición raíz. Modifique el archivo **/boot/grub/grub.cfg** y use el UUID de la partición root para configurar el elemento de arranque. Si la partición raíz ya utiliza UUID, no se requiere ninguna modificación. El procedimiento es el siguiente:
 - a. Inicie sesión en el ECS como usuario **root**.
 - b. Ejecute el siguiente comando para consultar todos los tipos de sistemas de archivos montados y los UUID de dispositivos:

blkid

Se muestra la siguiente información:

```
/dev/xvda1: UUID="ec51d860-34bf-4374-ad46-a0c3e337fd34" TYPE="ext3"  
/dev/xvda5: UUID="7a44a9ce-9281-4740-b95f-c8de33ae5c11" TYPE="swap"
```

- c. Ejecute el siguiente comando para consultar el archivo **grub.cfg**:

cat /boot/grub/grub.cfg

Se muestra la siguiente información:

```
.....menuentry 'Ubuntu Linux, with Linux 3.13.0-24-generic' --class  
ubuntu --class gnu-linux --class gnu --class os --unrestricted  
$menuentry_id_option 'gnulinux-3.13.0-24-generic-advanced-  
ec51d860-34bf-4374-ad46-a0c3e337fd34' {  
  recordfail  
  load_video  
  gfxmode $linux_gfx_mode  
  insmod gzio  
  insmod part_msdos  
  insmod ext2  
  if [ x${feature_platform_search_hint} = xy ]; then  
  search --no-floppy --fs-uuid --set=root ec51d860-34bf-4374-ad46-  
a0c3e337fd34  
  else  
  search --no-floppy --fs-uuid --set=root ec51d860-34bf-4374-ad46-  
a0c3e337fd34  
  fi  
  echo 'Loading Linux 3.13.0-24-generic ...'  
  linux /boot/vmlinuz-3.13.0-24-generic root=/dev/xvda1 ro  
  echo 'Loading initial ramdisk ...'  
  initrd /boot/initrd.img-3.13.0-24-generic  
}
```

- d. Compruebe si la partición raíz en el archivo de configuración **/boot/grub/grub.cfg** contiene **root=/dev/xvda1** o **root=UUID=ec51d860-34bf-4374-ad46-a0c3e337fd34**.
 - Si **root=UUID=ec51d860-34bf-4374-ad46-a0c3e337fd34** está contenida, la partición raíz está en el formato UUID y no requiere ningún cambio.
 - Si está contenido **root=/dev/xvda1**, la partición raíz está en el formato de nombre de dispositivo. Vaya a [5](#).

- e. Identifique el UUID del dispositivo de partición raíz basado en **root=/dev/xvda1** (nombre del dispositivo de la partición raíz) y la información de partición obtenida ejecutando el comando **blkid**.
- f. Ejecute el siguiente comando para abrir el archivo **grub.cfg**:

```
vi /boot/grub/grub.cfg
```

- g. Pulse **i** para entrar en el modo de edición y cambiar la partición raíz al formato UUID, por ejemplo, de **root=/dev/xvda1** a **root=UUID=ec51d860-34bf-4374-ad46-a0c3e337fd34**.
- h. Pulse **Esc**, ingrese **:wq** y pulse **Enter**. El sistema guarda la configuración y sale del editor vi.
- i. Ejecute el siguiente comando para verificar el cambio:

```
cat /boot/grub/grub.cfg
```

El cambio se realiza correctamente si se muestra información similar a la siguiente:

```
.....menuentry 'Ubuntu Linux, with Linux 3.13.0-24-generic' --class
ubuntu --class gnu-linux --class gnu --class os --unrestricted
$menuentry_id_option 'gnulinux-3.13.0-24-generic-advanced-
ec51d860-34bf-4374-ad46-a0c3e337fd34' {
recordfail
load_video
gfxmode $linux_gfx_mode
insmod gzio
insmod part_msdos
insmod ext2
if [ x$feature_platform_search_hint = xy ]; then
search --no-floppy --fs-uuid --set=root ec51d860-34bf-4374-ad46-
a0c3e337fd34
else
search --no-floppy --fs-uuid --set=root ec51d860-34bf-4374-ad46-
a0c3e337fd34
fi
echo 'Loading Linux 3.13.0-24-generic ...'
linux /boot/vmlinuz-3.13.0-24-generic root=UUID=ec51d860-34bf-4374-ad46-
a0c3e337fd34 ro
echo 'Loading initial ramdisk ...'
initrd /boot/initrd.img-3.13.0-24-generic
}
```

- CentOS 6.5: Ejecutar **blkid** para obtener el UUID de la partición raíz. Modifique el archivo **/boot/grub/grub.conf** y use el UUID de la partición raíz para configurar el elemento de arranque. Si la partición raíz ya utiliza UUID, no se requiere ninguna modificación. El procedimiento es el siguiente:

- a. Inicie sesión en el ECS como usuario **root**.
- b. Ejecute el siguiente comando para consultar todos los tipos de sistemas de archivos montados y los UUID de dispositivos:

```
blkid
```

Se muestra la siguiente información:

```
/dev/xvda1: UUID="749d6c0c-990a-4661-bed1-46769388365a" TYPE="swap"  

/dev/xvda2: UUID="f382872b-eda6-43df-9516-5a687fecdc6e" TYPE="ext4"
```

- c. Ejecute el siguiente comando para consultar el archivo **grub.conf**:

```
cat /boot/grub/grub.conf
```

Se muestra la siguiente información:

```
default=0
timeout=5
splashimage=(hd0,1)/boot/grub/splash.xpm.gz
hiddenmenu
```

```
title CentOS (2.6.32-573.8.1.el6.x86_64)
root (hd0,1)
kernel /boot/vmlinuz-2.6.32-573.8.1.el6.x86_64 ro root=/dev/xvda2
rd_NO_LUKS rd_NO_LVM LANG=en_US.UTF-8 rd_NO_MD SYSFONT=latacyrheb-sun16
crashkernel=autoKEYBOARDTYPE=pc KEYTABLE=us rd_NO_DM rhgb quiet
initrd /boot/initramfs-2.6.32-573.8.1.el6.x86_64.img
```

- d. Compruebe si la partición raíz en el archivo de configuración **/boot/grub/grub.conf** contiene **root=/dev/xvda2** o **root=UUID=f382872b-eda6-43df-9516-5a687fecdc6**.

- Si **root=UUID=f382872b-eda6-43df-9516-5a687fecdc6** está contenida, la partición raíz está en el formato UUID y no requiere ningún cambio.
- Si **root=/dev/xvda2** está contenido, la partición raíz está en el formato de nombre de dispositivo. Vaya a **5**.

- e. Identifique el UUID del dispositivo de partición raíz basado en **root=/dev/xvda2** (nombre del dispositivo de la partición raíz) y la información de partición obtenida al ejecutar el comando **blkid**.
- f. Ejecute el siguiente comando para abrir el archivo **grub.conf**:
- vi /boot/grub/grub.conf**
- g. Pulse **i** para entrar en el modo de edición y cambiar la partición raíz al formato UUID, por ejemplo, de **root=/dev/xvda2** a **root=UUID=f382872b-eda6-43df-9516-5a687fecdc6**.
- h. Pulse **Esc**, escriba **:wq** y pulse **Enter**. El sistema guarda la configuración y sale del editor vi.
- i. Ejecute el siguiente comando para verificar el cambio:

cat /boot/grub/grub.conf

El cambio se realiza correctamente si se muestra información similar a la siguiente:

```
default=0
timeout=5
splashimage=(hd0,1)/boot/grub/splash.xpm.gz
hiddenmenu
title CentOS (2.6.32-573.8.1.el6.x86_64)
root (hd0,1)
kernel /boot/vmlinuz-2.6.32-573.8.1.el6.x86_64 ro root=UUID=f382872b-eda6-43df-9516-5a687fecdc6 rd_NO_LUKS rd_NO_LVM LANG=en_US.UTF-8
rd_NO_MD SYSFONT=latacyrheb-sun16 crashkernel=autoKEYBOARDTYPE=pc
KEYTABLE=us rd_NO_DM rhgb quiet
initrd /boot/initramfs-2.6.32-573.8.1.el6.x86_64.img
```

- CentOS 7.0: Ejecute **blkid** para obtener el UUID de la partición raíz. Modifique el archivo **/boot/grub2/grub.cfg** y use el UUID de la partición raíz para configurar el elemento de arranque. Si la partición raíz ya utiliza UUID, no se requiere ninguna modificación.
- a. Inicie sesión en el ECS como usuario **root**.
- b. Ejecute el siguiente comando para consultar todos los tipos de sistemas de archivos montados y los UUID de dispositivos:

blkid

Se muestra la siguiente información:

```
/dev/xvda2: UUID="4eb40294-4c6f-4384-bbb6-b8795bbb1130" TYPE="xfs"
/dev/xvda1: UUID="2de37c6b-2648-43b4-a4f5-40162154e135" TYPE="swap"
```

- c. Ejecute el siguiente comando para consultar el archivo **grub.cfg**:

cat /boot/grub2/grub.cfg

Se muestra la siguiente información:

```

.....
menuentry 'CentOS Linux (3.10.0-229.el7.x86_64) 7 (Core)' --class fedora
--class gnu-linux --class gnu --class os --unrestricted
$menuentry_id_option 'gnulinux-3.10.0-229.el7.x86_64-
advanced-4eb40294-4c6f-4384-bbb6-b8795bbb1130' {
load_video
set gfxpayload=keep
insmod gzio
insmod part_msdos
insmod xfs
set root='hd0,msdos2'
if [ x$feature_platform_search_hint = xy ]; then
search --no-floppy --fs-uuid --set=root --
hint='hd0,msdos2'4eb40294-4c6f-4384-bbb6-b8795bbb1130
else
search --no-floppy --fs-uuid --set=root 4eb40294-4c6f-4384-bbb6-
b8795bbb1130
fi
linux16 /boot/vmlinuz-3.10.0-229.el7.x86_64 root=/dev/xvda2 ro
crashkernel=auto rhgb quiet LANG=en_US.UTF-8
initrd16 /boot/initramfs-3.10.0-229.el7.x86_64.img
}

```

- d. Compruebe si la partición root en el archivo de configuración **/boot/grub2/grub.cfg** contiene **root=/dev/xvda2** o **root=UUID=4eb40294-4c6f-4384-bbb6-b8795bbb1130**.
 - Si **root=UUID=4eb40294-4c6f-4384-bbb6-b8795bbb1130** está contenida, la partición raíz está en el formato UUID y no requiere ningún cambio.
 - Si **root=/dev/xvda2** está contenido, la partición raíz está en el formato de nombre de dispositivo. Vaya a [5](#).
- e. Identifique el UUID del dispositivo de partición raíz basado en **root=/dev/xvda2** (nombre del dispositivo de la partición raíz) y la información de partición obtenida al ejecutar el comando **blkid**.
- f. Ejecute el siguiente comando para abrir el archivo **grub.cfg**:
vi /boot/grub2/grub.cfg
- g. Pulse **i** para entrar en el modo de edición y cambiar la partición raíz al formato UUID, por ejemplo, de **root=/dev/xvda2** a **root=UUID=4eb40294-4c6f-4384-bbb6-b8795bbb1130**.
- h. Pulse **Esc**, escriba **:wq** y pulse **Enter**. El sistema guarda la configuración y sale del editor vi.
- i. Ejecute el siguiente comando para verificar el cambio:
cat /boot/grub2/grub.cfg

El cambio se realiza correctamente si se muestra información similar a la siguiente:

```

.....
menuentry 'CentOS Linux (3.10.0-229.el7.x86_64) 7 (Core)' --class fedora
--class gnu-linux --class gnu --class os --unrestricted
$menuentry_id_option 'gnulinux-3.10.0-229.el7.x86_64-
advanced-4eb40294-4c6f-4384-bbb6-b8795bbb1130' {
load_video
set gfxpayload=keep
insmod gzio
insmod part_msdos
insmod xfs
set root='hd0,msdos2'
if [ x$feature_platform_search_hint = xy ]; then
search --no-floppy --fs-uuid --set=root --
hint='hd0,msdos2'4eb40294-4c6f-4384-bbb6-b8795bbb1130
else
search --no-floppy --fs-uuid --set=root 4eb40294-4c6f-4384-bbb6-

```

```
b8795bbb1130
fi
linux16 /boot/vmlinuz-3.10.0-229.el7.x86_64 root=UUID=4eb40294-4c6f-4384-
bbb6-b8795bbb1130 ro crashkernel=auto rhgb quiet LANG=en_US.UTF-8
initrd16 /boot/initramfs-3.10.0-229.el7.x86_64.img
}
```

3.9.6 Cambio del identificador de disco en el archivo `fstab` a UUID

Escenarios

Al optimizar una imagen privada de Linux, debe cambiar el identificador de disco a UUID en el archivo de configuración `fstab` del ECS.

Procedimiento

- Tome CentOS 7.0 como ejemplo. Ejecute `blkid` para obtener los UUID de todas las particiones. Modifique el archivo `/etc/fstab` y use los UUIDs de partición para configurar el montaje automático de partición.

1. Inicie sesión en el ECS como usuario `root`.
2. Ejecute el siguiente comando para consultar todos los tipos de sistemas de archivos montados y UUIDs de dispositivos:

blkid

Se muestra la siguiente información:

```
/dev/xvda2: UUID="4eb40294-4c6f-4384-bbb6-b8795bbb1130" TYPE="xfs"
/dev/xvda1: UUID="2de37c6b-2648-43b4-a4f5-40162154e135" TYPE="swap"
```

3. Ejecute el siguiente comando para consultar el archivo `fstab`:

cat /etc/fstab

Se muestra la siguiente información:

```
[root@CTU1000028010 ~]# cat /etc/fstab
/dev/xvda2 / xfs defaults 0 0
/dev/xvda1 swap swap defaults 0 0
```

4. Compruebe si el identificador de disco en el archivo `fstab` es el nombre del dispositivo.
 - Si el disco está representado por UUID, no se requiere ninguna operación adicional.
 - Si el disco está representado por el nombre del dispositivo, vaya a [5](#).
5. Ejecute el siguiente comando para abrir el archivo `fstab`:

vi /etc/fstab

6. Presione `i` para entrar en el modo de edición y cambie el identificador de disco en el archivo `fstab` a UUID.

- Tome CentOS 7.1 como ejemplo. Ejecute `blkid` para obtener los UUID de todas las particiones. Modifique el archivo `/etc/fstab` y use los UUID de partición para configurar el montaje automático de partición.

1. Inicie sesión en el ECS como usuario `root`.
2. Ejecute el siguiente comando para consultar todos los tipos de sistemas de archivos montados y UUIDs de dispositivos:

blkid

```
/dev/xvda2: UUID="4eb40294-4c6f-4384-bbb6-b8795bbb1130" TYPE="xfs"
/dev/xvda1: UUID="2de37c6b-2648-43b4-a4f5-40162154e135" TYPE="swap"
```

Antes del cambio:

```
[root@CTU1000028010 ~]# cat /etc/fstab
/dev/xvda2 / xfs defaults 0 0
/dev/xvda1 swap swap defaults 0 0
```

Después del cambio:

```
[root@CTU1000028010 ~]# cat /etc/fstab
UUID=4eb40294-4c6f-4384-bbb6-b8795bbb1130 / xfs defaults 0 0
UUID=2de37c6b-2648-43b4-a4f5-40162154e135 swap swap defaults 0 0
```

3. Pulse **Esc**, escriba **:wq** y pulse **Enter**. El sistema guarda la configuración y sale del editor vi.
4. Ejecute el siguiente comando para verificar el cambio:

cat /etc/fstab

El cambio se realiza correctamente si se muestra información similar a la siguiente:

```
[root@CTU1000028010 ~]# cat /etc/fstab
UUID=4eb40294-4c6f-4384-bbb6-b8795bbb1130 / xfs defaults 0 0
UUID=2de37c6b-2648-43b4-a4f5-40162154e135 swap swap defaults 0 0
```

3.9.7 Instalación de controladores KVM nativos

Escenarios

Al optimizar una imagen privada de Linux, debe instalar controladores KVM nativos en el ECS. Si se instalaron los controladores, consulte esta sección.

 **ATENCIÓN**

Si no instala controladores KVM, es posible que no se detecten las NIC de ECS y que ECS no pueda comunicarse con otros recursos.

Prerrequisitos

- Se debe optimizar el ECS. Para obtener más información, véase [Comprobación de si una imagen privada necesita ser optimizada](#).
- El kernel de ECS debe ser posterior a 2.6.24.
- Deshabilite su antivirus y software de detección de intrusión. Puede activar el software después de instalar los controladores KVM.

Procedimiento

Modifique el archivo de configuración basado en la versión del sistema operativo.

Tabla 3-3 Modificación de archivos de configuración para diferentes sistemas operativos

Sistema operativo	Configuración	Referencia
CentOS/EulerOS	<p>Tome CentOS 7.0 como ejemplo.</p> <ol style="list-style-type: none"> En el archivo /etc/dracut.conf, agregue controladores VirtIO a add_drivers, incluidos virtio_blk, virtio_scsi, virtio_net, virtio_pci, virtio_ring y virtio. Separe los nombres de los controladores con espacios. Guarde y salga del archivo /etc/dracut.conf y ejecute el comando dracut -f para generar initrd de nuevo. 	CentOS y EulerOS
Ubuntu/Debian	<ol style="list-style-type: none"> En el archivo /etc/initramfs-tools/modules, agregue controladores VirtIO, incluidos virtio_blk, virtio_scsi, virtio_net, virtio_pci, virtio_ring, y virtio. Separe los nombres de los controladores con espacios. Guarde y salga del archivo /etc/initramfs-tools/modules y ejecute el comando update-initramfs -u para generar initrd de nuevo. 	Ubuntu y Debian
SUSE y openSUSE	<p>Si la versión del sistema operativo es anterior a SUSE 12 SP1 u openSUSE 13:</p> <ol style="list-style-type: none"> En el archivo /etc/sysconfig/kernel, agregue los controladores VirtIO a INITRD_MODULES="". Los controladores de VirtIO incluyen virtio_blk, virtio_scsi, virtio_net, virtio_pci, virtio_ring y virtio. Separe los nombres de los controladores con espacios. Ejecute el comando mkinitrd para generar initrd de nuevo. 	SUSE y openSUSE (anteriores a SUSE 12 SP1 u openSUSE 13)
	<p>Si la versión del sistema operativo es SUSE 12 SP1:</p> <ol style="list-style-type: none"> En el archivo /etc/dracut.conf, agregue los controladores VirtIO a add_drivers. Los controladores de VirtIO incluyen virtio_blk, virtio_scsi, virtio_net, virtio_pci, virtio_ring y virtio. Separe los nombres de los controladores con espacios. Ejecute el comando dracut -f para generar initrd de nuevo. 	SUSE y openSUSE (SUSE 12 SP1)

Sistema operativo	Configuración	Referencia
	<p>Si la versión del sistema operativo es posterior a SUSE 12 SP1 u openSUSE 13:</p> <ol style="list-style-type: none"> En el archivo <code>/etc/dracut.conf</code>, agregue controladores VirtIO a <code>add_drivers</code>, incluidos <code>virtio_blk</code>, <code>virtio_scsi</code>, <code>virtio_net</code>, <code>virtio_pci</code>, <code>virtio_ring</code> y <code>virtio</code>. Separe los nombres de los controladores con espacios. Guarde y salga del archivo <code>/etc/dracut.conf</code> y ejecute el comando <code>dracut -f</code> para generar <code>initrd</code> de nuevo. 	<p>SUSE y openSUSE (posteriores a SUSE 12 SP1 u openSUSE 13)</p>

CentOS y EulerOS

- Ejecute el siguiente comando para abrir el archivo `/etc/dracut.conf`:
vi /etc/dracut.conf
- Pulse **i** para acceder al modo de edición y agregar controladores VirtIO a `add_drivers` (el formato varía según el sistema operativo).

```
[root@CTU10000xxxxx ~]# vi /etc/dracut.conf
# additional kernel modules to the default
add_drivers+="virtio_blk virtio_scsi virtio_net virtio_pci virtio_ring
virtio"
....
```
- Pulse **Esc**, escriba `:wq` y pulse **Enter**. El sistema guarda el cambio y sale del archivo `/etc/dracut.conf`.
- Ejecute el siguiente comando para regenerar `initrd`:
dracut -f /boot/initramfs-2.6.32-573.8.1.el6.x86_64.img

Si el sistema de archivos virtual no es el `initramfs` predeterminado, ejecute el comando `dracut -f Name of the initramfs or initrd file actually used`. El nombre real del archivo `initramfs` o `initrd` se puede obtener del archivo `grub.cfg`, que puede ser `/boot/grub/grub.cfg`, `/boot/grub2/grub.cfg`, o `/boot/grub/grub.conf` dependiendo del sistema operativo.
- Si el sistema de archivos virtual es `initramfs`, ejecute el siguiente comando para verificar si se han instalado controladores KVM nativos:
lsinitrd /boot/initramfs-`uname -r`.img | grep virtio

Si el sistema de archivos virtual es `initrd`, ejecute el siguiente comando para verificar si se han instalado controladores KVM nativos:
lsinitrd /boot/initrd-`uname -r` | grep virtio

Supongamos que el sistema de archivos virtual es `initramfs`. Se mostrará el siguiente resultado del comando:

```
[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
```

NOTA

Si agrega controladores integrados al archivo `initrd` o `initramfs`, ECS no se verá afectado. Esto facilita la modificación de los controladores. Sin embargo, no puede comprobar los controladores ejecutando el comando `lsinitrd`. Puede ejecutar el siguiente comando para comprobar si los controladores son integrados en el kernel:

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

Ubuntu y Debian

1. Ejecute el siguiente comando para abrir el archivo **modules**:
vi /etc/initramfs-tools/modules
2. Pulse **i** para acceder al modo de edición y agregar controladores VirtIO al archivo **/etc/initramfs-tools/modules** (el formato varía según el sistema operativo).

```
[root@CTU10000xxxxx ~]#vi /etc/initramfs-tools/modules
...
# Examples:
#
# raid1
# sd_m0d
virtio_blk
virtio_scsi
virtio_net
virtio_pci
virtio_ring
virtio
```
3. Pulse **Esc**, escriba **:wq** y pulse **Enter**. El sistema guarda el cambio y sale del archivo **/etc/initramfs-tools/modules**.
4. Ejecute el siguiente comando para regenerar `initrd`:
update-initramfs -u
5. Ejecute el siguiente comando para comprobar si se han instalado los controladores KVM nativos:

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

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

NOTA

Si agrega controladores integrados al archivo `initrd` o `initramfs`, ECS no se verá afectado. Esto facilita la modificación de los controladores. Sin embargo, no puede comprobar los controladores ejecutando el comando `lsinitrd`. Puede ejecutar el siguiente comando para comprobar si los controladores son integrados en el 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
```

SUSE y openSUSE (anteriores a SUSE 12 SP1 u openSUSE 13)

Modifique el archivo `/etc/sysconfig/kernel`.

1. Ejecute el siguiente comando para modificar el archivo `/etc/sysconfig/kernel`:

vi /etc/sysconfig/kernel

2. Agregue controladores VirtIO a `INITRD_MODULES=""` (el formato de los controladores depende del sistema operativo).

```
SIA10000xxxxx:~ # vi /etc/sysconfig/kernel
# (like drivers for scsi-controllers, for lvm or reiserfs)
#
INITRD_MODULES="ata_piix ata_generic virtio_blk virtio_scsi virtio_net
virtio_pci virtio_ring virtio"
```

3. Ejecute el comando `mkinitrd` para generar `initrd` de nuevo.

NOTA

Si el sistema de archivos virtual no es el `initramfs` o `initrd` predeterminado, ejecute el comando **`dracut -f Name of the initramfs or initrd file actually used`**. El nombre real del archivo `initramfs` o `initrd` se puede obtener del archivo `menu.lst` o `grub.cfg` (`/boot/grub/menu.lst`, `/boot/grub/grub.cfg`, o `/boot/grub2/grub.cfg`).

A continuación se muestra un archivo `initrd` de ejemplo de 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 processor.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` en la línea `initrd` es el archivo `initrd` que realmente se usa. Ejecute el comando **`dracut -f /boot/initrd.vmx`**. Si el archivo `initrd` no contiene el directorio `/boot`, como `/initramfs-xxx`, ejecute el comando **`dracut -f /boot/initramfs-xxx`**.

4. Ejecute el siguiente comando para verificar si se han instalado los controladores KVM VirtIO:

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

```
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
```

5. Reinicie el ECS.
6. Ejecute el siguiente comando para comprobar si existen controladores KVM en `initrd`:

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

```
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
```

📖 NOTA

Si agrega controladores integrados al archivo `initrd` o `initramfs`, ECS no se verá afectado. Esto facilita la modificación de los controladores. Sin embargo, no puede comprobar los controladores ejecutando el comando `lsinitrd`. Puede ejecutar el siguiente comando para comprobar si los controladores son integrados en el kernel:

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

SUSE y openSUSE (SUSE 12 SP1)

Modifique el archivo `/etc/dracut.conf`.

1. Ejecute el siguiente comando para abrir el archivo `/etc/dracut.conf`:

```
vi /etc/dracut.conf
```

2. Pulse **i** para acceder al modo de edición y agregar controladores VirtIO a `add-drivers` (el formato varía según el sistema operativo).

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

3. Pulse **Esc**, escriba `:wq` y pulse **Enter**. El sistema guarda el cambio y sale del archivo `/etc/dracut.conf`.

4. Ejecute el siguiente comando para regenerar `initrd`:

```
dracut -f /boot/initramfs-File name
```

Si el sistema de archivos virtual no es el `initramfs` predeterminado, ejecute el comando `dracut -f Name of the initramfs or initrd file actually used`. El nombre real del archivo `initramfs` o `initrd` se puede obtener del archivo `grub.cfg`, que puede ser `/boot/grub/grub.cfg`, `/boot/grub2/grub.cfg`, o `/boot/grub/grub.conf` dependiendo del sistema operativo.

5. Si el sistema de archivos virtual es `initramfs`, ejecute el siguiente comando para verificar si se han instalado controladores KVM nativos:

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

Si el sistema de archivos virtual es `initrd`, ejecute el siguiente comando para verificar si se han instalado controladores KVM nativos:

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

SUSE y openSUSE (posteriores a SUSE 12 SP1 u openSUSE 13)

Modifique el archivo `/etc/dracut.conf`.

Tome SUSE Linux Enterprise Server 12 SP2 (x86_64) como ejemplo.

1. Ejecute el siguiente comando para abrir el archivo `/etc/dracut.conf`:

vi /etc/dracut.conf

2. Pulse **i** para acceder al modo de edición y agregar controladores VirtIO a `add_drivers` (el formato varía según el sistema operativo).

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

3. Pulse **Esc**, escriba `:wq` y pulse **Enter**. El sistema guarda el cambio y sale del archivo `/etc/dracut.conf`.

4. Ejecute el siguiente comando para regenerar `initrd`:

dracut -f /boot/initramfs-File name

Si el sistema de archivos virtual no es el `initramfs` predeterminado, ejecute el comando **dracut -f Name of the initramfs or initrd file actually used**. El nombre real del archivo `initramfs` o `initrd` se puede obtener del archivo `grub.cfg`, que puede ser `/boot/grub/grub.cfg`, `/boot/grub2/grub.cfg`, o `/boot/grub/grub.conf` dependiendo del sistema operativo.

5. Si el sistema de archivos virtual es `initramfs`, ejecute el siguiente comando para verificar si se han instalado controladores KVM nativos:

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

Si el sistema de archivos virtual es `initrd`, ejecute el siguiente comando para verificar si se han instalado controladores KVM nativos:

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

Supongamos que el sistema de archivos virtual es `initrd`. Se mostrará el siguiente resultado del comando:

```
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
```

NOTA

Si agrega controladores integrados al archivo `initrd` o `initramfs`, ECS no se verá afectado. Esto facilita la modificación de los controladores. Sin embargo, no puede comprobar los controladores ejecutando el comando `lsinitrd`. Puede ejecutar el siguiente comando para comprobar si los controladores son integrados en el kernel:

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

3.9.8 Borrar registros del sistema

Eliminar los archivos de registro y los registros históricos y detener el ECS.

1. Ejecute los siguientes comandos para eliminar archivos de clave redundantes:
echo > /\$path/\$to/\$root/.ssh/authorized_keys
Un comando de ejemplo es **echo > /root/.ssh/authorized_keys**.
echo > /\$path/\$to/\$none-root/.ssh/authorized_keys
Un comando de ejemplo es **echo > /home/linux/.ssh/authorized_keys**.
2. Ejecute el siguiente comando para borrar los archivos de registro en el directorio **/var/log**:
rm -rf /var/log/*

 **NOTA**

Antes de eliminar los archivos de registro, haga una copia de respaldo de los directorios de registro y los archivos de registro requeridos por el inicio de la aplicación. Por ejemplo, si se elimina el directorio de registro Nginx predeterminado **/var/log/nginx**, es posible que Nginx no se inicie.
3. Ejecute los siguientes comandos para eliminar registros históricos:
echo > /root/.bash_history
history -c

3.10 Encriptación de imágenes

3.10.1 Descripción

IMS le permite crear imágenes cifradas para garantizar la seguridad de los datos.

 **NOTA**

Para utilizar la función de encriptación de imágenes, debe solicitar permisos de administrador de KMS.

Restricciones

- DEW debe estar habilitado.
- Imágenes encriptadas no se pueden compartir con otras personas.
- Las imágenes encriptadas no se pueden publicar en el Marketplace.
- El disco del sistema de un ECS creado a partir de una imagen encriptada también se cifra, y su clave es la misma que la clave de imagen.
- Si un ECS tiene un disco de sistema cifrado, las imágenes privadas creadas a partir del ECS también se cifran.
- La clave utilizada para cifrar una imagen no se puede cambiar.
- Si la clave utilizada para cifrar una imagen está desactivada o eliminada, la imagen no estará disponible.

3.10.2 Creación de imágenes encriptadas

Puede crear una imagen cifrada utilizando un archivo de imagen externo o un ECS cifrado.

- Cree una imagen cifrada utilizando un archivo de imagen externo.
Cuando registre el archivo de imagen externa como una imagen privada, seleccione **KMS encryption** y seleccione una clave. Para más detalles, véase [Creación de una](#)

[imagen de disco del sistema Windows a partir de un archivo de imagen externo](#) y [Creación de una imagen de disco de sistema Linux a partir de un archivo de imagen externo](#).

- Cree una imagen encriptada usando un ECS encriptado.

Cuando se utiliza un ECS para crear una imagen privada, si el disco del sistema del ECS está cifrado, la imagen privada creada con el ECS también se cifra. La clave utilizada para cifrar la imagen debe ser la misma que la utilizada para cifrar el disco del sistema. Para más detalles, véase [Creación de una imagen de disco del sistema desde un ECS de Windows](#) y [Creación de una imagen de disco del sistema desde un ECS de Linux](#).

3.11 Replicación de imágenes dentro de una región

Escenarios

Puede convertir imágenes cifradas y no cifradas entre sí o habilitar algunas funciones avanzadas (como la creación rápida de ECS a partir de una imagen) mediante la función de replicación de imágenes in-region. Es posible que necesite replicar una imagen para:

- Replicar una imagen cifrada en una imagen no cifrada.

Las imágenes cifradas no se pueden compartir con otros tenants ni publicarlas como imágenes de Marketplace. Si desea publicar o compartir una imagen cifrada, puede replicarla en una imagen no cifrada.

- Replica una imagen encriptada en una encriptada.

No se pueden cambiar las claves para cifrar imágenes. Si desea cambiar la clave de una imagen cifrada, puede replicarla en una imagen nueva y cifrarla con una clave de cifrado.

- Replica una imagen no cifrada en una cifrada.

Si desea almacenar una imagen sin cifrar de forma cifrada, puede replicar esta imagen como una nueva y cifrar la nueva imagen con una clave.

- Optimice una imagen privada de disco de sistema para que pueda usarse para crear rápidamente los ECS.

La creación rápida reduce considerablemente el tiempo necesario para crear ECS a partir de una imagen de disco del sistema. Actualmente, esta característica es compatible con todas las imágenes de disco de sistema recién creadas de forma predeterminada. Es posible que las imágenes de disco del sistema existentes no admitan esta función. Puede optimizar las imágenes mediante la función de replicación de imagen in-region. Por ejemplo, si la imagen A no admite la creación rápida de ECS, puede replicarla para generar la imagen copy_A que admita la creación rápida de ECS.

Restricciones

- Las imágenes completas de ECS no se pueden replicar dentro de la misma región.
- Las imágenes privadas creadas con archivos ISO no admiten replicación dentro de la región.

Prerrequisitos

Las imágenes que se van a replicar están en el estado **Normal**.

Procedimiento

1. Acceda a la consola IMS.
 - a. Inicie sesión en la consola de gestión.
 - b. En **Compute**, haga clic en **Image Management Service**.
Se muestra la consola IMS.
2. Busque la fila que contiene la imagen que se va a replicar, haga clic en **More** en la columna **Operation** y seleccione **Replicate**.
3. En el cuadro de diálogo **Replicate Image** que se muestra, establezca los siguientes parámetros:

Figura 3-22 Replicación de imágenes en una región

Replicate Image ×

• The image size must be less than 128 GiB.

Image Details

Name	copy_cn-...	Image Type	ECS system disk image
Image Size	16 KiB	OS Type	Linux
OS	CentOS 8.5 64bit	Created	Apr 01, 2024 16:48:26 GMT+08:00

Replication Mode: **Within Region** | Across Regions

* Name: copy_copy_cr...

* Enterprise Project: --Select an enterprise project--

Description: [Empty text box]

Encryption: KMS encryption

OK Cancel

- **Replication Mode:** Seleccione **Within Region**.

📖 NOTA

Este parámetro solo está disponible cuando la región actual también admite la replicación entre regiones.

- **Name:** Introduzca un nombre que sea fácil de identificar.
- **Enterprise Project:** Seleccione un proyecto de empresa en la lista desplegable. Este parámetro solo está disponible si ha habilitado proyectos de empresa o si su cuenta es una cuenta de empresa. Para habilitar esta función, póngase en contacto con su gestor de clientes.
- **Description:** Este parámetro es opcional. Introduzca la descripción de la replicación.
- **Encryption:** Si desea cifrar la imagen o cambiar una clave, seleccione **KMS encryption** y seleccione la clave que desea utilizar en la lista desplegable.

4. Haga clic en **OK**.

En la página **Private Images**, consulte el progreso de la replicación. Si el estado de la nueva imagen se convierte en **Normal**, la replicación de la imagen se realiza correctamente.

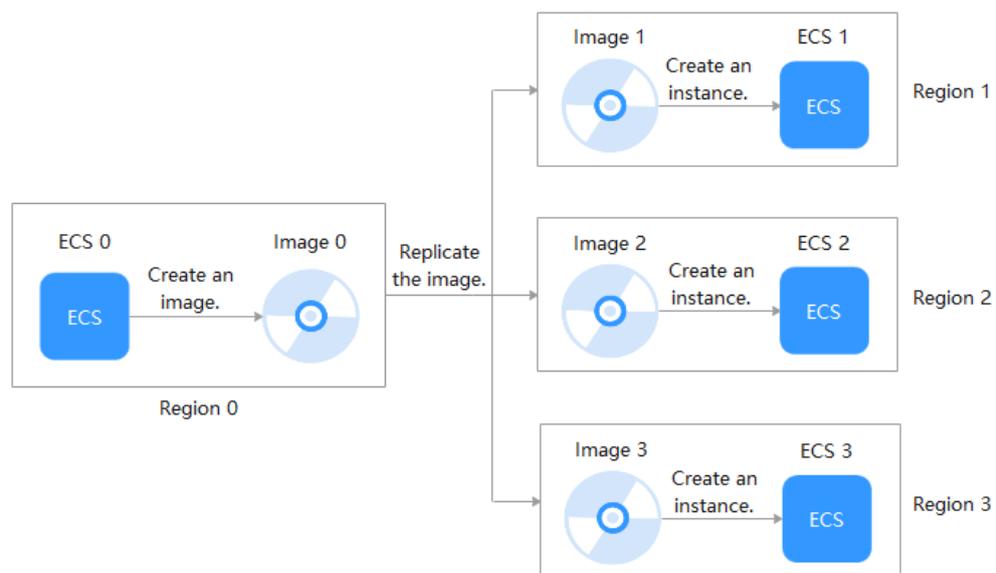
3.12 Replicación de imágenes entre regiones

Escenarios

Una imagen es un recurso regional. Si desea utilizar una imagen privada en otra región, puede replicarla en la región objetivo.

La replicación de imágenes entre regiones es necesaria para la HA del sistema normalmente cuando el sistema se despliega en varias regiones. En la mayoría de los casos, los ECS se despliegan en varias regiones (incluidas regiones fuera de China). Si desea clonar un ECS entre regiones, puede replicar su imagen entre las regiones y, a continuación, usar la imagen para crear los ECS idénticos en la región de destino.

Figura 3-23 Replicación típica entre regiones



Antecedentes

- La replicación entre regiones se aplica al despliegue de servidores entre regiones o a la copia de respaldo de datos. A menudo se utiliza junto con el uso compartido de imágenes para la replicación de imágenes entre regiones y cuentas. En la siguiente tabla se describe la replicación de imágenes en diferentes escenarios.

Escenario	Descripción	Procedimiento
Replicación entre regiones bajo la misma cuenta	Una vez completada la replicación, se genera una nueva imagen en la región de destino. La nueva imagen tiene un ID que es diferente del ID de la imagen de origen.	Consulte esta sección.
Replicación entre regiones y cuentas	Replica la imagen en la región de destino y la comparte con otras cuentas.	Vea esta sección y Compartir imágenes especificadas .
Replicación entre cuentas en la misma región	Una vez completada la replicación, la imagen se comparte con el tenant de destino. El tenant objetivo puede usar la imagen (con el mismo ID que la imagen de origen), pero el propietario de la imagen sigue siendo el tenant que la compartió.	Véase Compartir imágenes especificadas .

- Cuando se replica una imagen completa del ECS entre regiones, también se replicarán las copias de respaldo de CSBS o CBR asociados. Por lo tanto, se le cobrará por estas copias de respaldo en la región de destino.
- El tiempo necesario para replicar una imagen entre regiones depende de la velocidad de la red, el tamaño de la imagen y el número de tareas simultáneas.
- Puede seleccionar varias imágenes para la replicación entre regiones a la vez. Sin embargo, no se le permite seleccionar una imagen ISO, una imagen cifrada, una imagen de ECS completa, una imagen congelada o la imagen que se está creando.
- Se requiere una delegación para la replicación de imágenes entre regiones. Esta delegación cuenta con los permisos de administrador de IMS, lo que le permite realizar operaciones en los proyectos en la región de destino.

Por ejemplo, si desea replicar una imagen de la región A a la región B, la delegación debe tener los permisos de administrador de IMS en la región B. Para saber cómo crear una agencia, consulte [Crear una delegación](#).

Restricciones

- Para obtener más información, consulte [¿Cuáles son las regiones que admiten la replicación entre regiones de imágenes de disco de datos y sistemas?](#)

Figura 3-24 Regiones que admiten la replicación entre regiones de imágenes de disco de datos y de sistemas

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	-

NOTA

- √ indica que se admite la replicación entre regiones de imágenes de disco de datos y de sistema.
- × indica que no se admite la replicación entre regiones de imágenes de disco de datos y de sistemas. En este caso, exporte la imagen deseada y luego impórtelo a la región de destino.
- - indica que las regiones de origen y de destino son las mismas.
- El ajuste de región puede afectar la replicación de imágenes entre regiones de los usuarios que se registran después del ajuste. En este caso, la posibilidad de realizar la replicación está sujeta a la visualización de la consola de gestión. Los usuarios registrados antes del ajuste no se ven afectados.
- Para las regiones de Latinoamérica, solo se pueden reproducir imágenes desde LA-Santiago hasta LA-Mexico City1 or LA-Sao Paulo1.
- Las regiones no enumeradas en la figura anterior no soportan la replicación entre regiones de imágenes del sistema o del disco de datos.

- La replicación entre regiones de imágenes ECS completas también está disponible en ciertas regiones.

Si una imagen completa del ECS no se puede replicar en una región diferente, puede usarla para crear un ECS, usar el ECS para crear una imagen de disco del sistema y una imagen de disco de datos, y replicar las imágenes en la región de destino.

Una imagen completa del ECS creada usando una copia de respaldo de ECS se puede replicar desde la región donde residen a otra región, pero la imagen completa replicada del ECS no se puede replicar entre regiones de nuevo.

- Solo puede replicar imágenes privadas entre regiones. Si desea replicar una imagen de otro tipo (por ejemplo, una imagen pública) entre regiones, puede utilizar la imagen para crear un ECS, utilizar el ECS para crear una imagen privada y, a continuación, replicar la imagen privada entre regiones.

NOTA

Una imagen privada no se puede replicar entre regiones después de que se publique en el Marketplace.

- Para realizar la replicación entre regiones, los usuarios de IAM deben tener el permiso `ReadOnlyAccess` de IAM y el permiso `FullAccess` de IMS tanto en las regiones de origen como de destino.
- El tamaño de cada imagen que se va a replicar entre regiones no puede ser superior a 128 GB.
- Puede replicar solo cinco imágenes entre regiones a la vez.
- Las imágenes ISO y las imágenes cifradas no se pueden replicar entre regiones.

Procedimiento

1. Inicie sesión en la consola de gestión.
2. En **Compute**, haga clic en **Image Management Service**.
Se muestra la consola de IMS.
3. Busque la fila que contiene la imagen que se va a replicar, haga clic en **More** en la columna **Operation** y seleccione **Replicate**.
4. En el cuadro de diálogo **Replicate Image** que se muestra, establezca los siguientes parámetros:

NOTA

Si la región actual no admite la replicación entre regiones, establezca los parámetros haciendo referencia a [Replicación de imágenes dentro de una región](#).

Figura 3-25 Replicación de una imagen entre regiones

Replicate Image

Image Size 9.7 GB

OS Type Windows

OS Windows-Server-2012-R2-Datacenter-64bit

Created Dec 02, 2020 11:22:41 GMT+08:00

Replication Mode Within Region Across Regions

* Name

* Destination Region

* Destination Project

* IAM Agency [View Agency](#)

- **Modo de replicación:** Seleccione **Across Regions**.
- **Name:** Introduzca un nombre que sea fácil de identificar. El nombre de la imagen tiene el siguiente formato: **copy_Name of the source region where the image is located_Source image name**.
- **Destination Region:** Seleccione la región en la que desea utilizar la imagen.
- **Destination Project:** Seleccione un proyecto en la región de destino. Después de seleccionar la región de destino, el sistema muestra automáticamente los proyectos disponibles.
- **Target Server Backup Vault:** Este parámetro solo está disponible para imágenes de ECS completas creadas con copias de respaldo de CBR. Seleccione un almacén para almacenar copias de respaldo.
Si no hay ningún almacén de copia de respaldo de CBR disponible en la región de destino, haga clic en **Create Server Backup Vault** para crear uno. Asegúrese de seleccionar **Replication** para **Protection Type**. Para otros parámetros, consulte [Compra de un almacén de copia de respaldo de servidor](#). Una vez creado el almacén, haga clic en para actualizar la página y seleccione el almacén en el cuadro de lista desplegable.
- **IAM Agency:** Seleccione una delegación IAM.
- **Description:** Este parámetro es opcional. Introduzca la descripción de la replicación.

- Haga clic en **OK**.
Cambie a la región de destino. Si el estado de la imagen se convierte en **Normal**, la replicación de la imagen se realiza correctamente.

NOTA

El tiempo necesario para replicar una imagen entre regiones depende de la velocidad de la red, el tamaño de la imagen y el número de tareas simultáneas.

Crear una delegación

- Inicie sesión en la consola de gestión.
- En la esquina superior derecha de la página, haga clic en el nombre de usuario y seleccione **Identity and Access Management**.
- En el panel de navegación, elija **Agencies**.
- Haga clic en **Create Agency**.
- En la página **Create Agency**, establezca los siguientes parámetros:
 - Agency Name**: Ingrese un nombre de la agencia, como **ims_admin_agency**.

Figura 3-26 Creación de una delegación

The screenshot shows the 'Create Agency' form with the following fields and values:

- Agency Name**: ims_admin_agency
- Agency Type**: Cloud service (selected), Account (unselected)
- Cloud Service**: Image Management Service (IMS)
- Validity Period**: Unlimited
- Description**: Agency with IMS Administrator privileges

At the bottom of the form, there are two buttons: **Next** (red) and **Cancel** (white).

- Agency Type**: Seleccione **Cloud service**.
- Cloud Service**: Este parámetro solo está disponible si selecciona **Cloud service** para **Agency Type**. Seleccione **Image Management Service (IMS)** en la lista desplegable.
- Validity Period**: Seleccione **Unlimited**.

- **Description:** Este parámetro es opcional. Puede ingresar **Agency with IMS Administrator privileges**.
6. Haga clic en **Next**.
- Seleccione **Region-specific projects** para **Scope** y seleccione uno o más proyectos de la lista desplegable.

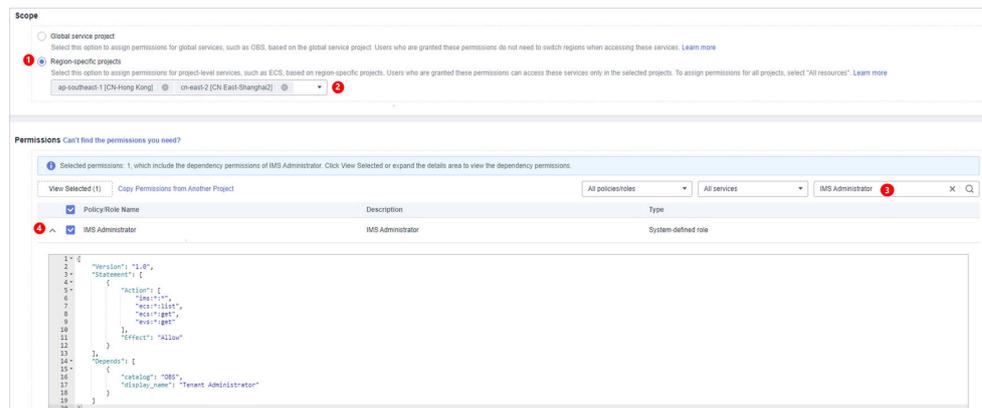
En la replicación de imágenes entre regiones, la delegación debe tener los permisos de administrador de IMS en la región de destino. Por ejemplo, si desea replicar una imagen de CN-Hong Kong, la delegación debe tener los permisos de administrador de IMS en CN East-Shanghai2.



No seleccione **All projects**. De lo contrario, la delegación creada será inválida.

- Seleccione **IMS Administrator** para **Permissions**.

Figura 3-27 Concesión de permisos a una delegación

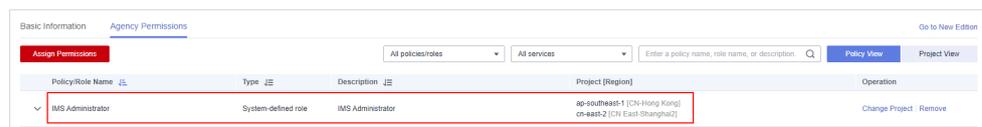


7. Haga clic en **OK**.

Figura 3-28 Nueva delegación



Figura 3-29 Permisos de la nueva delegación



3.13 Etiquetado de una imagen

Escenarios

Puede utilizar etiquetas para clasificar imágenes. Puede agregar, modificar o eliminar etiquetas de imagen, o buscar las imágenes requeridas por etiqueta en la lista de imágenes.

NOTA

- Al agregar etiquetas predefinidas a una imagen o buscar una imagen con etiquetas predefinidas, debe tener permiso para acceder al Tag Management Service (TMS).
- Si su organización tiene políticas de etiquetas preconfiguradas para imágenes, debe agregar etiquetas a las imágenes en función de las políticas. Si no cumple con las políticas de etiquetas, es posible que las imágenes no se creen. Póngase en contacto con el administrador de la organización para obtener más información sobre las políticas de etiquetas.
 - Cada etiqueta consiste en una clave y un valor. La clave contiene un máximo de 36 caracteres y el valor contiene un máximo de 43 caracteres. La clave no puede dejarse en blanco ni ser una cadena de caracteres vacía. El valor no se puede dejar en blanco, sino que puede ser una cadena de caracteres vacía.
 - Una imagen puede tener un máximo de 10 etiquetas.

Restricciones

Una imagen puede tener un máximo de 10 etiquetas.

Agregar, eliminar y modificar etiquetas de imagen

1. Acceda a la consola IMS.
 - a. Inicie sesión en la consola de gestión.
 - b. En **Compute**, haga clic en **Image Management Service**.
Se muestra la consola IMS.
2. Haga clic en la pestaña **Private Images** y haga clic en el nombre de la imagen para mostrar los detalles de la imagen.
 - Para modificar una etiqueta de imagen, vaya a **3**.
 - Para eliminar una etiqueta de imagen, vaya a **4**.
 - Para agregar una etiqueta de imagen, vaya a **5**.
3. Haga clic en la pestaña **Tags**, busque la pestaña de destino y haga clic en **Edit** en la columna **Operation**. En el cuadro de diálogo que se muestra, modifique la etiqueta.
4. Haga clic en la pestaña **Tags**, busque la pestaña de destino y haga clic en **Delete** en la columna **Operation**. En el cuadro de diálogo que se muestra, haga clic en **Yes**.
5. Haga clic en la ficha **Tags** y, a continuación, en **Add Tag**. En el cuadro de diálogo que se muestra, agregue una etiqueta.

Buscar imágenes privadas por etiqueta

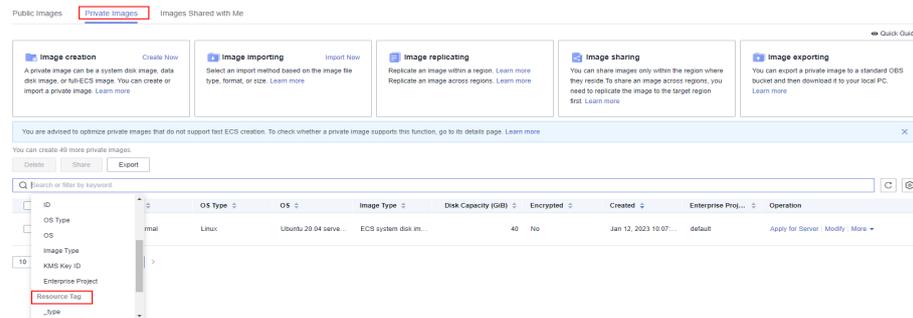
1. Acceda a la consola IMS.
 - a. Inicie sesión en la consola de gestión.

- b. En **Compute**, haga clic en **Image Management Service**.

Se muestra la consola IMS.

2. Haga clic en la pestaña **Private Images** y haga clic en el cuadro de búsqueda encima de la lista de imágenes privadas. Especifique las claves de etiqueta y los valores en **Resource Tag** para buscar imágenes privadas.

Figura 3-30 Búsqueda de imágenes por etiqueta



NOTA

- Ni la clave de la etiqueta ni el valor de la etiqueta pueden estar vacíos. Cuando la clave de la etiqueta y el valor de la etiqueta coinciden, el sistema muestra automáticamente las imágenes privadas deseadas.
- Puede agregar varias etiquetas para buscar imágenes compartidas. El sistema mostrará imágenes privadas que coincidan con todas las etiquetas.

3.14 Auditoría de operaciones clave

3.14.1 Operaciones de IMS registradas por CTS

Escenarios

Cloud Trace Service (CTS) es un servicio de auditoría de registros proporcionado por Huawei Cloud y destinado a la seguridad en la nube. Le permite recopilar, almacenar y consultar registros de operaciones de recursos en la nube y utilizar estos registros para análisis de seguridad, auditoría de cumplimiento, seguimiento de recursos y localización de fallas.

Puede usar CTS para grabar operaciones de IMS para realizar consultas, auditorías y seguimiento posterior.

Prerrequisitos

Necesita habilitar CTS antes de usarlo. Si no está habilitado, las operaciones de IMS no se pueden registrar. Después de estar habilitado, CTS crea automáticamente un rastreador para registrar todas sus operaciones. El rastreador almacena solo las operaciones de los últimos siete días. Para almacenar las operaciones durante más tiempo, almacene archivos de seguimiento en buckets de OBS.

Operaciones de IMS registradas por CTS

Tabla 3-4 Operaciones de IMS que pueden ser registradas por CTS

Operación	Tipo de recurso	Nombre de seguimiento
Creación de una imagen	ims	createImage
Modificación de una imagen	ims	updateImage
Eliminación de imágenes en un lote	ims	deleteImage
Replicación de una imagen	ims	copyImage
Exportación de una imagen	ims	exportImage
Adición de un tenant que puede usar una imagen compartida	ims	addMember
Modificación de tenants que pueden usar una imagen compartida	ims	updateMember
Eliminación de tenants del grupo donde los miembros pueden usar una imagen compartida	ims	deleteMemeber

Tabla 3-5 Relación entre las operaciones de IMS y las API nativas de OpenStack

Operación	Nombre de seguimiento	Tipo de servicio	Tipo de recurso	Componente de OpenStack
Creación de una imagen	createImage	IMS	image	glance
Modificar/Subir una imagen	updateImage	IMS	image	glance
Eliminación de una imagen	deleteImage	IMS	image	glance
Etiquetado de una imagen	addTag	IMS	image	glance
Eliminación de una etiqueta de imagen	deleteTag	IMS	image	glance

Operación	Nombre de seguimiento	Tipo de servicio	Tipo de recurso	Componente de OpenStack
Adición de un tenant que puede usar una imagen compartida	addMember	IMS	image	glance
Modificación de la información sobre un tenant que puede usar una imagen compartida	updateMember	IMS	image	glance
Eliminación de un tenant del grupo donde los miembros pueden usar una imagen compartida	deleteMember	IMS	image	glance

3.14.2 Consulta de trazas

Escenarios

Una vez que CTS está habilitado, comienza a registrar las operaciones de IMS. Puede ver las operaciones registradas en los últimos siete días en la consola de gestión de CTS.

En esta sección se describe cómo ver los registros.

Procedimiento

1. Acceda a la consola CTS.
 - a. Inicie sesión en la consola de gestión.
 - b. Haga clic en **Cloud Trace Service** en **Management & Governance**.
2. En el panel de navegación de la izquierda, elija **Trace List**.
3. Establezca los criterios de filtro y haga clic en **Query**.

Los siguientes filtros están disponibles:

- **Trace Type**, **Trace Source**, **Resource Type**, y **Search By**.

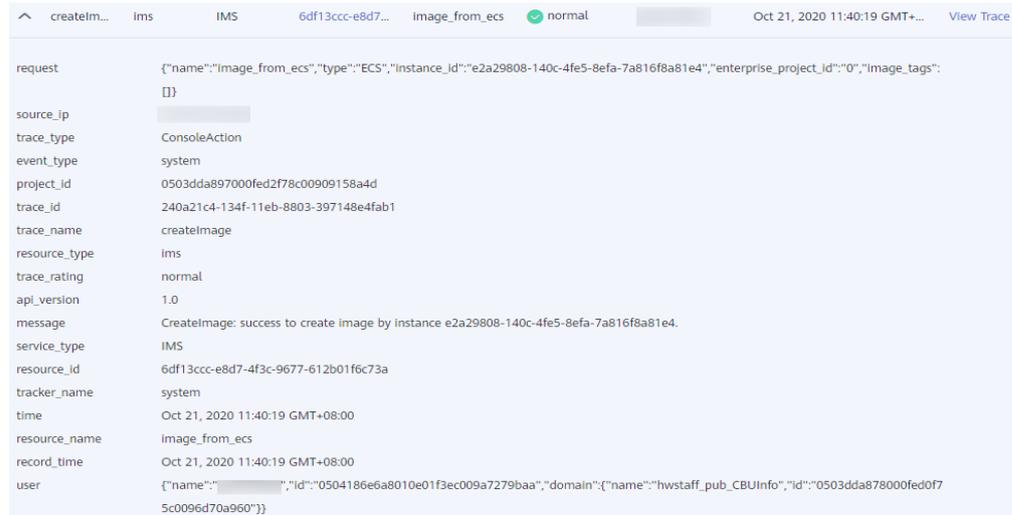
Seleccione **Management** para **Trace Type** e **IMS** para **Trace Source**.

Tenga en cuenta que:

- Si selecciona **Resource ID** para **Search By**, debe introducir un ID de recurso. Solo se admite la concordancia de palabras completas.
- Si selecciona **Resource name** para **Search By**, debe seleccionar o introducir un nombre de recurso específico.

- **Operator:** Seleccione un operador específico de la lista desplegable.
 - **Trace Status:** Los valores disponibles son **All trace statuses**, **Normal**, **Warning**, e **Incident**.
 - **Time Range:** Puede seleccionar **Last 1 hour**, **Last 1 day**, **Last 1 week** o **Customize**.
4. Localice el rastro de destino y haga clic en  para ampliar los detalles del rastro.

Figura 3-31 Ampliación de un rastro



5. Haga clic en **View Trace** en la esquina superior derecha del área de detalles de traza.

4 Operaciones de Windows

4.1 Configuración de la NIC en DHCP

Escenarios

Si se crea una imagen privada a partir de un ECS o archivo de imagen externo y la VM donde se encuentra el archivo de imagen externo o ECS está configurada con una dirección IP estática, debe cambiar el atributo NIC a DHCP para que los nuevos ECSs creados a partir de la imagen privada puedan obtener dinámicamente una dirección IP.

Esta sección utiliza Windows Server 2008 R2 como ejemplo para describir cómo configurar DHCP. Para obtener más información acerca de cómo configurar DHCP en ECS que ejecuten otros sistemas operativos, consulte la documentación pertinente del sistema operativo.

NOTA

Al registrar un archivo de imagen externo como una imagen privada, configure DHCP en la VM donde se encuentra el archivo de imagen externo. Se recomienda configurar DHCP en la VM y, a continuación, exportar el archivo de imagen.

Prerrequisitos

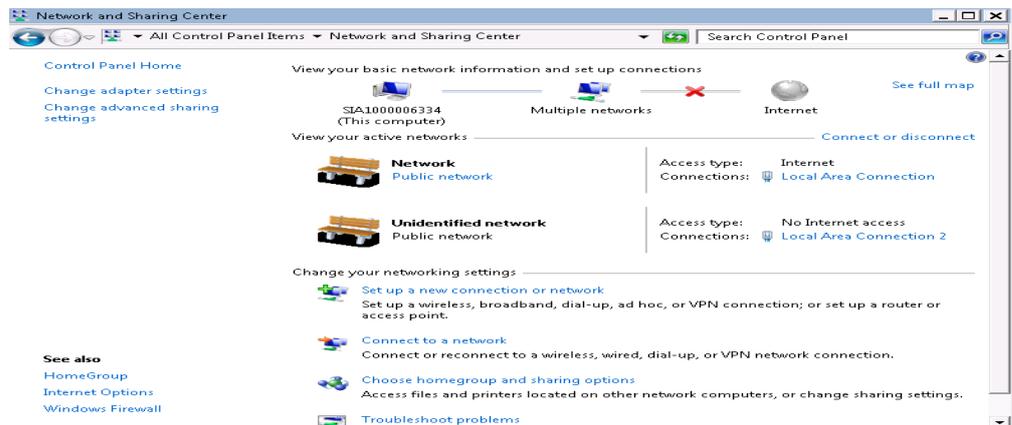
Ha iniciado sesión en el ECS utilizado para crear una imagen privada de Windows.

Para obtener más información sobre cómo iniciar sesión en un ECS, consulte [Descripción del inicio de sesión](#).

Procedimiento

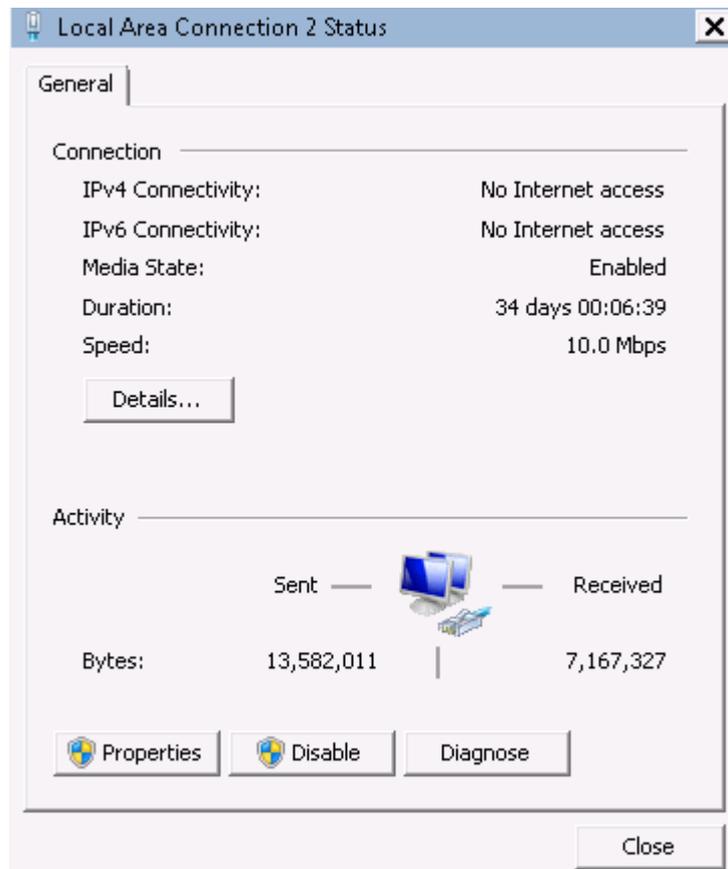
1. En el ECS, seleccione **Start > Control Panel**.
2. Haga clic en **Network and Internet Connections**.
3. Haga clic en **Network and Sharing Center**.

Figura 4-1 Centro de redes y recursos compartidos



4. Seleccione la conexión configurada con la dirección IP estática. Por ejemplo, haga clic en **Local Area Connection 2**.

Figura 4-2 Local Area Connection 2 Status

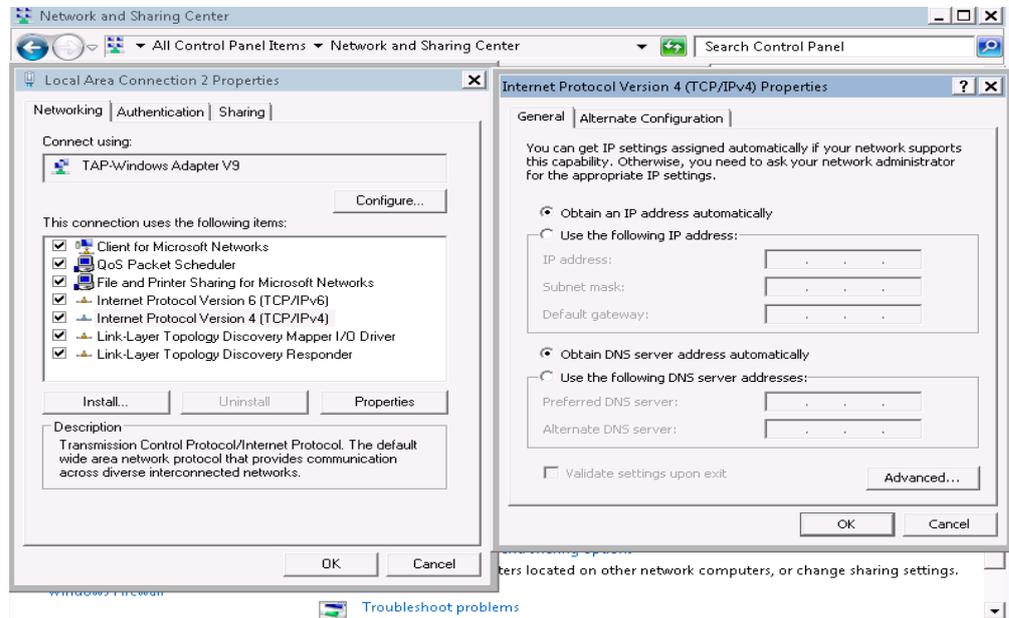


5. Haga clic en **Properties** y seleccione la versión configurada del protocolo de Internet.
6. En la pestaña **General**, seleccione **Obtain an IP address automatically** y **Obtain DNS server address automatically** y haga clic en **OK**. **Figura 4-3** muestra el cuadro de diálogo para configurar el modo de obtención de direcciones IP.

NOTA

Le recomendamos guardar la información de red original para que pueda restaurar la red si es necesario.

Figura 4-3 Configuración del modo de obtención de direcciones IP



4.2 Habilitación de la conexión a Escritorio remoto

Escenarios

Si desea acceder de forma remota a un ECS, habilite la conexión de escritorio remoto para el ECS de origen al crear una imagen privada. Esta función debe estar habilitada para los ECS acelerados por GPU.

NOTA

Al registrar un archivo de imagen externo como una imagen privada, habilite la conexión de escritorio remoto en la VM donde se encuentra el archivo de imagen externo. Se recomienda activar esta función en VM y, a continuación, exportar el archivo de imagen.

Prerrequisitos

Ha iniciado sesión en el ECS utilizado para crear una imagen privada de Windows.

Para obtener más información sobre cómo iniciar sesión en un ECS, consulte [Descripción del inicio de sesión](#).

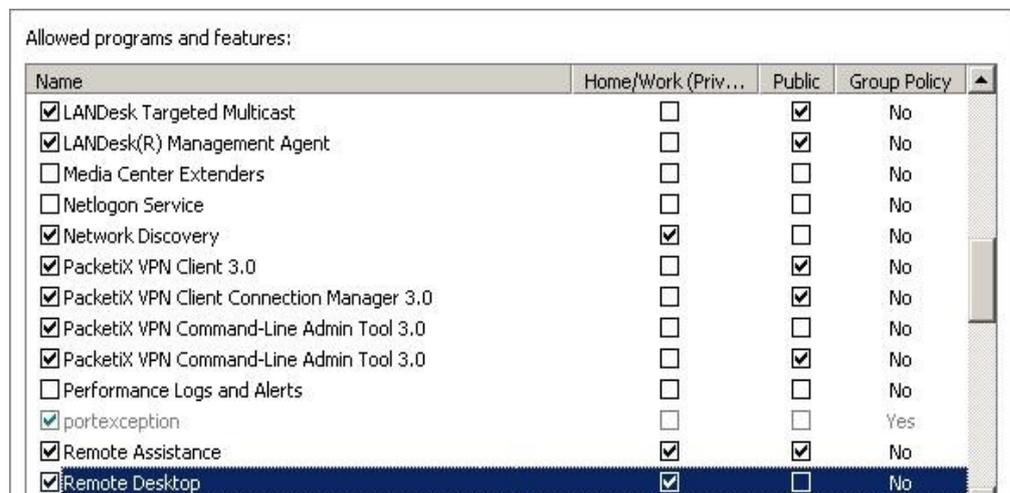
Procedimiento

1. Antes de activar esta función, se recomienda establecer la resolución del ECS a 1920×1080.

En el ECS, seleccione **Start > Control Panel**. En **Appearance and Personalization**, haga clic en **Adjust screen resolution**. A continuación, seleccione un valor adecuado en el cuadro de lista desplegable **Resolution**.

2. Elija **Start**, haga clic con el botón derecho en **Computer** y elija **Properties** en el menú contextual.
3. Haga clic en **Remote settings**.
4. En la ficha **Remote**, seleccione **Allow connections from computers running any version of Remote Desktop (less secure)**.
5. Haga clic en **OK**.
6. Seleccione **Start > Control Panel** y vaya a **Windows Firewall**.
7. Elija **Allow a program or feature through Windows Firewall** en el panel izquierdo.
8. Seleccione los programas y características que permite el firewall de Windows para **Remote Desktop** según los requisitos de red y haga clic en **OK** en la parte inferior.

Figura 4-4 Configuración de escritorio remoto



4.3 Instalación y configuración de Cloudbase-Init

Escenarios

Para asegurarse de que puede usar la función de inyección de datos de usuario para inyectar información personalizada inicial en los ECS creados a partir de una imagen privada (como configurar la contraseña de inicio de sesión de ECS), instale Cloudbase-Init en el ECS utilizado para crear la imagen.

- Si Cloudbase-Init no está instalado, no puede configurar un ECS. Como resultado, solo puede usar la contraseña en el archivo de imagen para iniciar sesión en el ECS.
- De forma predeterminada, los ECS creados a partir de una imagen pública tienen Cloudbase-Init instalado. No es necesario instalar o configurar Cloudbase-Init en dichos ECS.
- Para los ECS creados a partir de archivos de imagen externos, instale y configure Cloudbase-Init realizando las operaciones de esta sección.

NOTA

Cloudbase-Init es un software de código abierto. Si la versión instalada tiene vulnerabilidades de seguridad, se recomienda actualizarla a la versión más reciente.

Prerrequisitos

- Una EIP ha sido vinculada al ECS.
- Ha iniciado sesión en el ECS.
- El modo de obtención de la dirección IP del ECS es DHCP.
- El complemento de restablecimiento de contraseña con un solo clic se ha instalado en el ECS.

Si reinicia el ECS al instalar Cloudbase-Init en él, la contraseña puede cambiarse a una aleatoria. Por lo tanto, debe instalar el complemento de restablecimiento de contraseña con un solo clic en el ECS. Para obtener más información, véase [Instalación del complemento de restablecimiento de contraseñas con un solo clic](#).

Instalar Cloudbase-Init

1. En el menú **Start** de Windows, seleccione **Control Panel > Programs > Programs and Features** y compruebe si Cloudbase-Init 1.1.2 está instalado.
 - Si está instalado Cloudbase-Init 1.1.2, omita los pasos siguientes y vaya a [Configurar Cloudbase-Init](#).
 - Si Cloudbase-Init está instalado, pero la versión no es 1.1.2, desinstale Cloudbase-Init y vaya al siguiente paso.
 - Si Cloudbase-Init no está instalado, vaya al siguiente paso.
2. Compruebe si la versión del sistema operativo es de escritorio de Windows.
 - En caso afirmativo, vaya a [3](#).
 - Si el sistema operativo es Windows Server, vaya a [4](#).
3. Habilitar la cuenta de administrador (Windows 7 se utiliza como ejemplo).
 - a. Haga clic en **Start** y seleccione **Control Panel > System and Security > Administrative Tools**.
 - b. Haga doble clic en **Computer Management**.
 - c. Seleccione **System Tools > Local Users and Groups > Users**.
 - d. Haga clic con el botón derecho en **Administrator** y seleccione **Properties**.
 - e. Deseleccione **Account is disabled**.
4. Descargue el paquete de instalación de Cloudbase-Init.

Descargue el paquete de instalación de Cloudbase-Init de la versión adecuada basada en la arquitectura del sistema operativo desde el sitio web oficial de Cloudbase-Init (<http://www.cloudbase.it/cloud-init-for-windows-instances/>).

Para obtener la versión estable, visite las siguientes rutas:

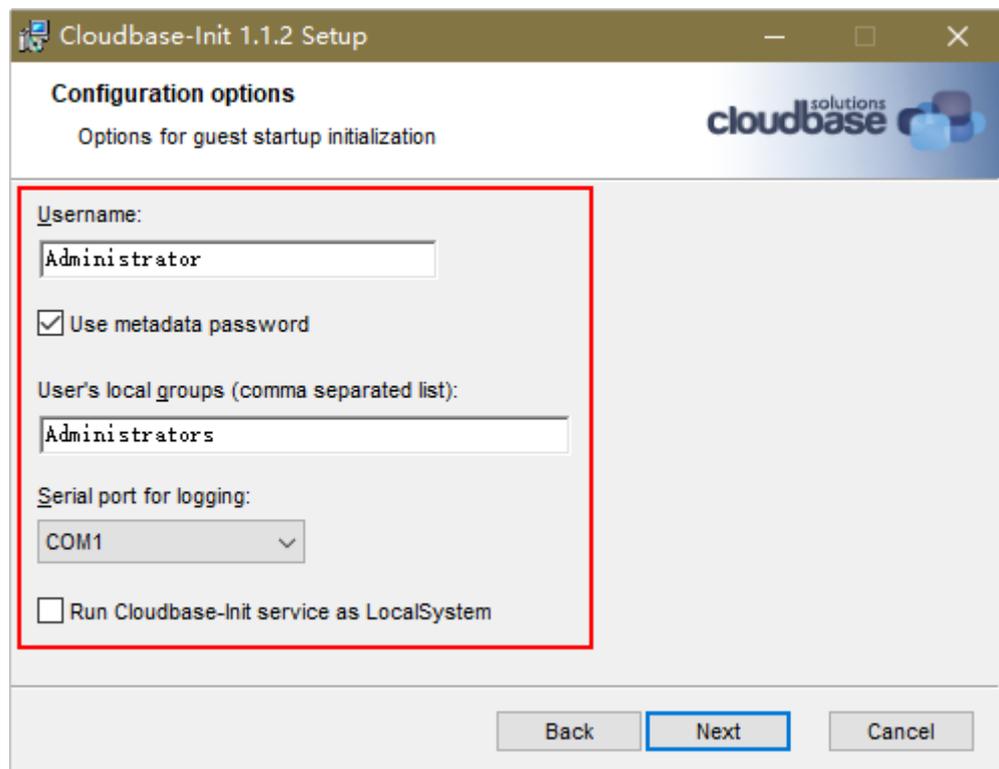
 - 64-bit: https://www.cloudbase.it/downloads/CloudbaseInitSetup_Stable_x64.msi
 - 32-bit: https://www.cloudbase.it/downloads/CloudbaseInitSetup_Stable_x86.msi
5. Haga doble clic en el paquete de instalación de Cloudbase-Init.

6. Haga clic en **Next**.
7. Seleccione **I accept the terms in the License Agreement** y haga clic en **Next**.
8. Mantenga la ruta de acceso predeterminada y haga clic en **Next**.
9. En la ventana **Configuration options**, escriba **Administrator** para **Username**, seleccione **COM1** para **Serial port for logging** y asegúrese de que no está seleccionado **Run Cloudbase-Init service as LocalSystem**.

 **NOTA**

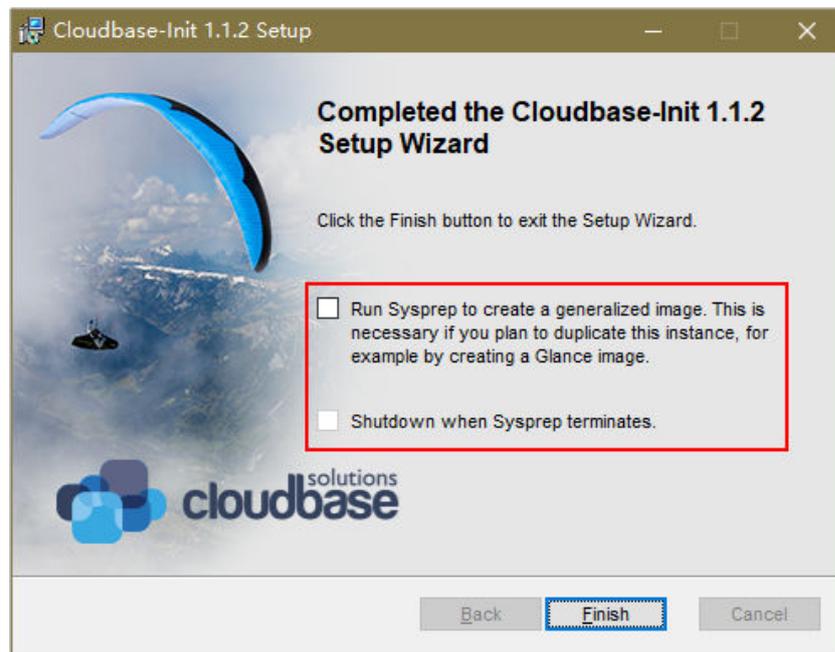
El número de versión que se muestra en la figura es solo para referencia.

Figura 4-5 Configuración de parámetros



10. Haga clic en **Next**.
11. Haga clic en **Install**.
12. En el cuadro de diálogo **Files in Use**, seleccione **Close the application and attempt to restart them** y haga clic en **OK**.
13. Compruebe si la versión del sistema operativo es de escritorio de Windows.
 - En caso afirmativo, vaya a **15**.
 - Si no, vaya a **14**.
14. En la ventana **Completed the Cloudbase-Init Setup Wizard**, asegúrese de que ninguna de las opciones esté seleccionada.

Figura 4-6 Completar la instalación de Cloudbase-Init



NOTA

El número de versión que se muestra en la figura es solo para referencia.

15. Haga clic en **Finish**.

Configurar Cloudbase-Init

1. Edite el archivo de configuración **C:\Program Files\Cloudbase Solutions\Cloudbase-Init\conf\cloudbase-init.conf** en la ruta de instalación de Cloudbase-Init.
 - a. Agregue **netbios_host_name_compatibility=false** a la última línea del archivo para que el nombre de host admita un máximo de 63 caracteres.

NOTA

Debido a las restricciones de sistema de Windows, NetBIOS no contiene más de 15 caracteres.

- b. Agregue **metadatos_services=cloudbaseinit.metadata.services.httpservice.HttpService** para permitir que el agente acceda al origen de datos OpenStack de IaaS.
- c. Agrega **plugins** para configurar los complementos que se cargarán. Separe los diferentes complementos con comas (.). La información en negrita es la palabra clave de cada complemento.

- Los siguientes complementos se cargan por defecto. Puede conservar todos o algunos de ellos según sea necesario.

```
plugins=cloudbaseinit.plugins.common.localscripts.LocalScriptsPlugin,  
cloudbaseinit.plugins.common.mtu.MTUPlugin, cloudbaseinit.plugins.windows.createuser.CreateUserPlugin, cloudbaseinit.plugins.common.setuserpassword.SetUserPasswordPlugin, cloudbaseinit.plugins.common.sshpublickeys.SetUserSSHPublicKeysPlugin, cloudbaseinit.plugins.common.sethostname.SetHostNamePlugin, cloudbaseinit.plugins.windows.extendvolumes.ExtendVolumesPlugin, cloudbaseinit.plugins.common.userdata.UserDataPlugin,  
cloudbaseinit.plugins.windows.licensing.WindowsLicensingPlugin
```

Funciones de complemento:

- **LocalScriptsPlugin** configura los scripts.
- **MTUPlugin** configura las interfaces de red MTU.
- **CreateUserPlugin** crea un usuario.
- **SetUserPasswordPlugin** configura una contraseña.
- **SetUserSSHPublicKeysPlugin** configura una clave.
- **SetHostNamePlugin** configura un nombre de host.
- **ExtendVolumesPlugin** expande espacio de disco.
- **UserDataPlugin** inyecta datos de usuario.
- **WindowsLicensingPlugin** activa instancias de Windows.

 **NOTA**

Si puede cambiar el nombre de host de los ECS después de que se hayan creado a partir de esta imagen y los servicios de los ECS son sensibles a los cambios en el nombre de host, no se recomienda configurar el **SetHostNamePlugin** aquí.

■ **Complementos opcionales:**

```
plugins=cloudbaseinit.plugins.windows.winrmlistener.ConfigWinRMListen  
erPlugin,cloudbaseinit.plugins.windows.winrmcertificateauth.ConfigWin  
RMCertificateAuthPlugin
```

Funciones de complemento:

- **ConfigWinRMListenerPlugin** configura la escucha de inicios de sesión remotos.
- **ConfigWinRMCertificateAuthPlugin** configura los inicios de sesión remotos sin autenticación de contraseña.

 **ATENCIÓN**

Los complementos WinRM utilizan un algoritmo criptográfico débil, que puede causar riesgos de seguridad. Por lo tanto, se recomienda no cargar los complementos.

- d. (Opcional) Agregue los siguientes elementos de configuración para configurar el número de tiempos de reintento y el intervalo para obtener metadatos:

```
retry_count=40  
retry_count_interval=5
```

- e. (Opcional) Agregue el siguiente elemento de configuración para evitar desconexiones de red de metadatos causadas por la ruta predeterminada agregada por Windows:

```
[openstack]  
add_metadata_private_ip_route=False
```

- f. (Opcional) Si la versión de Cloudbase-Init es 0.9.12 o posterior, puede personalizar la longitud de la contraseña.

Cambie el valor de **user_password_length** para personalizar la longitud de la contraseña.

- g. (Opcional) Agregue el siguiente elemento de configuración para deshabilitar el cambio de contraseña en el primer inicio de sesión:

```
first_logon_behaviour=no
```

- h. (Opcional) Agregue el siguiente elemento de configuración para asegurarse de que la sincronización de tiempo desde el BIOS persiste durante los reinicios del sistema:

real_time_clock_utc=true

 **NOTA**

La entrada de registro **RealTimeIsUniversal=1** permite al sistema sincronizar el tiempo desde el BIOS. Si **real_time_clock_utc=true** no está configurado, Cloudbase-Init revertirá **RealTimeIsUniversal** a **0**. Como resultado, el sistema no puede sincronizar el tiempo desde el BIOS después de un reinicio.

2. Libere la dirección DHCP actual para que los ECS creado pueda obtener direcciones correctas.

En la línea de comandos de Windows, ejecute el siguiente comando para liberar la dirección DHCP actual:

ipconfig /release

 **NOTA**

Esta operación interrumpirá la conexión de red y afectará negativamente al uso de ECS. La red se recuperará automáticamente después de que los ECS se inicien de nuevo.

3. Al crear una imagen con un ECS de Windows, debe cambiar la política SAN del ECS a **OnlineAll**. De lo contrario, los discos EVS conectados a los ECS creados a partir de la imagen pueden estar fuera de línea.

Windows tiene tres tipos de políticas SAN: **OnlineAll**, **OfflineShared** y **OfflineInternal**.

Tabla 4-1 Políticas de SAN

Tipo	Descripción
OnlineAll	Todos los discos recién detectados se ponen en línea automáticamente.
OfflineShared	Todos los discos en buses compartibles, como iSCSI y FC, se dejan sin conexión de forma predeterminada, mientras que los discos en buses no compartibles se mantienen en línea.
OfflineInternal	Todos los discos recién detectados se dejan sin conexión.

- a. Ejecute **cmd.exe** y ejecute el siguiente comando para consultar la política SAN actual de ECS con DiskPart:

diskpart

- b. Ejecute el siguiente comando para ver la política SAN del ECS:

san

- Si la política de SAN es **OnlineAll**, ejecute el comando **exit** para salir de DiskPart.
 - Si la política de SAN no es **OnlineAll**, vaya a **3.c**.
- c. Ejecute el siguiente comando para cambiar la política SAN de ECS a **OnlineAll**:
- san policy=onlineall**

4.4 Instalación del complemento de restablecimiento de contraseñas con un solo clic

Escenarios

Se recomienda instalar el complemento de restablecimiento de contraseña CloudResetPwdAgent antes de crear una imagen privada. De esta manera, puede restablecer la contraseña de los ECS creados a partir de la imagen con unos pocos clics.

- Los ECS creados a partir de una imagen pública tienen este plug-in instalado de forma predeterminada.
- Para los ECS creados a partir de un archivo de imagen externo, instale el complemento realizando las operaciones de esta sección.

Precauciones

- Puede decidir si desea instalar el complemento CloudResetPwdAgent.
- El complemento ha sido de código abierto en la plataforma de código abierto GitHub según *GNU General Public License v2.0*.
- [Tabla 4-2](#) enumera los sistemas operativos que admiten este complemento.

Tabla 4-2 Sistemas operativos compatibles con el complemento de restablecimiento de contraseña con un solo clic

Tipo de sistema operativo	Versión del sistema operativo
Windows	Windows Server 2016 Datacenter 64bit Windows Server 2012 R2 Standard 64bit Windows Server 2012 R2 Datacenter 64bit Windows Server 2008 R2 Enterprise 64bit Windows Server 2008 SP2 Enterprise 64bit Windows Server 2008 R2 Datacenter 64bit Windows Server 2008 R2 Standard 64bit Windows Server 2008 R2 WEB 64bit

Prerrequisitos

- El estado del ECS es de **Running**.
- El ECS debe tener un espacio restante de más de 300 MB, y los datos se pueden escribir en su unidad C.
- DHCP debe estar habilitado para la VPC utilizada por el ECS.
- Las redes del ECS son normales.
- La regla de grupo de seguridad saliente del ECS debe cumplir los siguientes requisitos:
 - **Protocolo: TCP**

- **Rango de puerto: 80**
- **Extremo remoto: 169.254.0.0/16**

Si utiliza la regla de grupo de seguridad saliente predeterminada, se pueden cumplir los requisitos anteriores y se puede inicializar el ECS. La regla predeterminada del grupo de seguridad saliente es la siguiente:

- **Protocolo: Todos**
- **Rango de puerto: Todos**
- **Extremo remoto: 0.0.0.0/16**

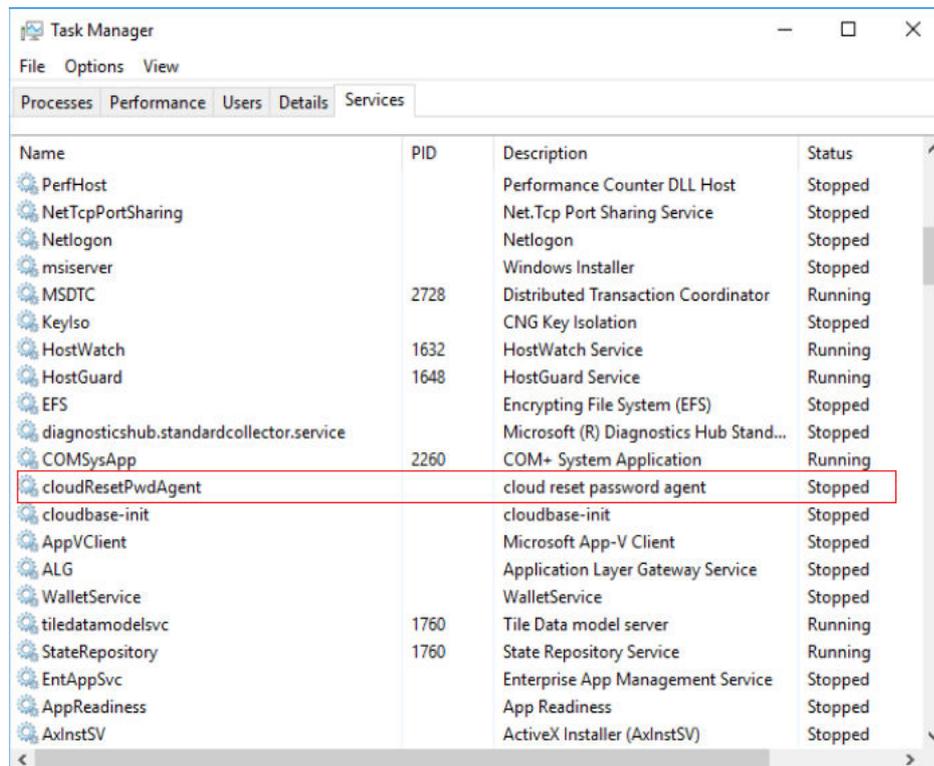
Procedimiento

Paso 1 Inicie sesión en el ECS.

Paso 2 Compruebe si el complemento de restablecimiento de contraseña CloudResetPwdAgent está instalado en el ECS.

Inicie el **Task Manager** y compruebe si se muestra **cloudResetPwdAgent** en la pestaña **Services**. Como se muestra en **Figura 4-7**, se ha instalado el complemento de restablecimiento de contraseña en el ECS.

Figura 4-7 Instalación exitosa de complemento



- Si la instalación se realiza correctamente, no se requiere ninguna otra acción.
- De lo contrario, vaya a **3**.

Paso 3 Descargue **CloudResetPwdAgent.zip** y verifique su integridad haciendo referencia a **Obtención del complemento de restablecimiento de contraseñas de un solo clic**.

No hay ningún requisito especial para el directorio que almacena **CloudResetPwdAgent.zip**.

Paso 4 Descomprima **CloudResetPwdAgent.zip**.

No hay ningún requisito especial para el directorio que almacena el **CloudResetPwdAgent.zip** descomprimido.

Paso 5 Instale los plug-in.

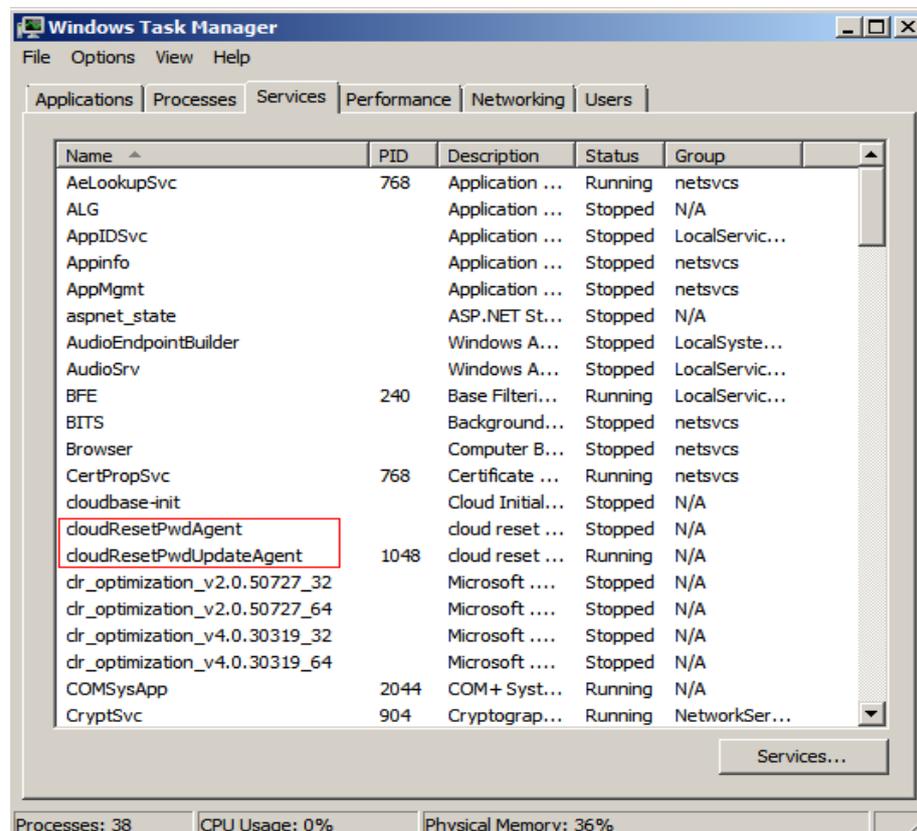
1. Haga doble clic en **setup.bat** tanto en **CloudResetPwdAgent.Windows** como en **CloudResetPwdUpdateAgent.Windows**.

Los complementos de restablecimiento de contraseña comienzan a instalarse.

2. Vea el **Task Manager** y compruebe si la instalación se ha realizado correctamente.

Si **cloudResetPwdAgent** y **cloudResetPwdUpdateAgent** se muestran en el **Task Manager**, como se muestra en **Figura 4-8**, la instalación se realiza correctamente. De lo contrario, la instalación falló.

Figura 4-8 Administrador de tareas de Windows



NOTA

Si la instalación falló, compruebe si el entorno de instalación cumple con los requisitos e instale de nuevo los complementos.

----Fin

4.5 Ejecución de Sysprep

Escenarios

La ejecución de Sysprep garantiza que un ECS tiene un SID único después de agregarlo a un dominio.

Después de instalar Cloudbase-Init en un ECS, debe decidir si los ECS necesidades se deben agregar a un dominio o si debe tener un SID único. En caso afirmativo, ejecute Sysprep como se indica en esta sección.

Prerrequisitos

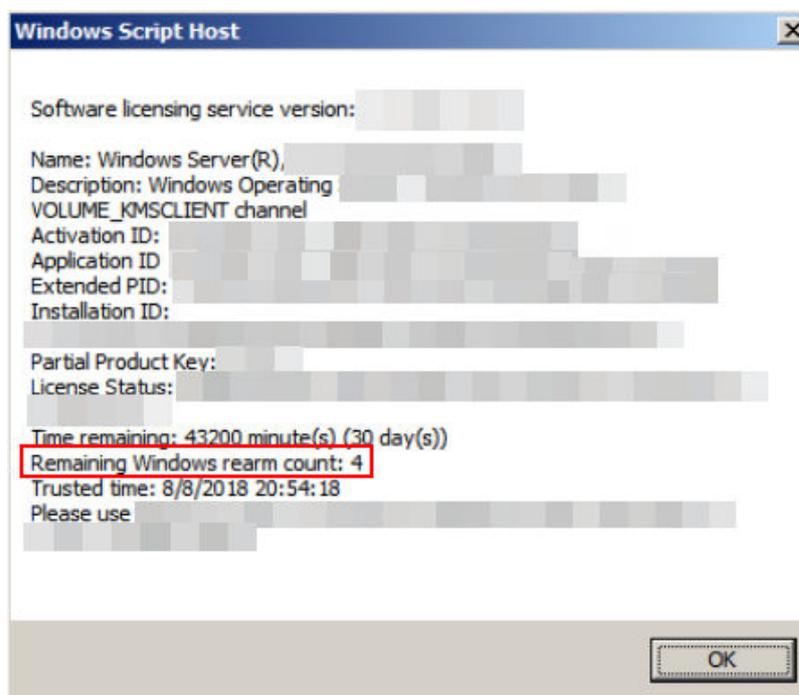
- Ejecute Sysprep como administrador.
- Para Windows recién activado ECS, solo puede ejecutar Sysprep una vez a la vez.
- Si un ECS se crea a partir de un archivo de imagen, solo se puede utilizar Sysprep proporcionado por el archivo de imagen. Además, Sysprep debe residir siempre en el directorio `%WINDIR%\system32\sysprep`.
- Windows debe estar en el estado activado, y el recuento de rearme restante de Windows debe ser mayor o igual a 1. De lo contrario, no se puede ejecutar la encapsulación Sysprep.

Ejecute el siguiente comando en la línea de comandos de Windows y compruebe cuántas veces puede ejecutar Sysprep en el cuadro de diálogo **Windows Script Host** mostrado:

```
slmgr.vbs /dlv
```

Si el valor de **Remaining Windows rearm count** es **0**, no se puede ejecutar Sysprep.

Figura 4-9 Windows Script Host



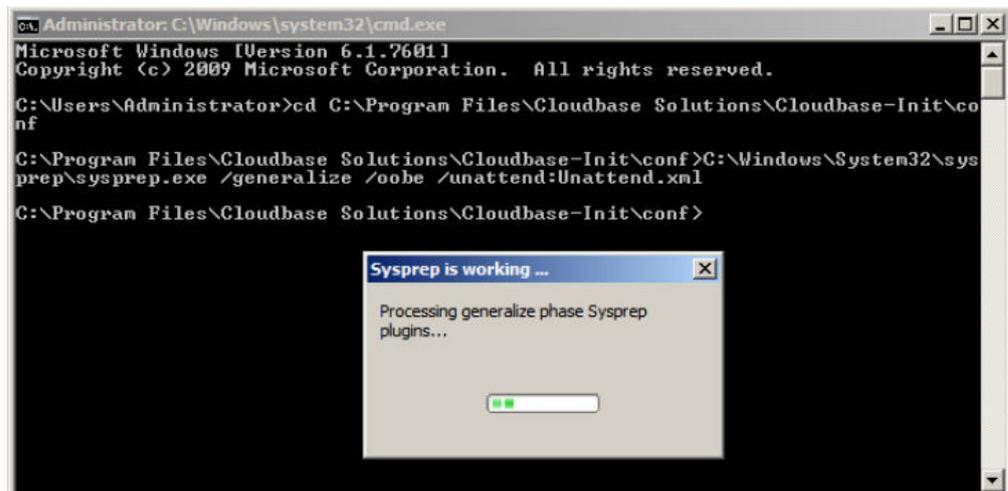
Procedimiento

1. Ingrese al directorio de instalación de Cloudbase-Init.
C:\Program Files\Cloudbase Solutions se utiliza como ejemplo del directorio de instalación de Cloudbase-Init. Cambie al directorio raíz de la unidad C y ejecute el siguiente comando para ingresar al directorio de instalación:
cd C:\Program Files\Cloudbase Solutions\Cloudbase-Init\conf
2. Ejecute el siguiente comando para encapsular Windows:
C:\Windows\System32\sysprep\sysprep.exe /generalize /oobe /unattend:Unattend.xml

ATENCIÓN

- Asegúrese de que **/unattend:Unattend.xml** esté contenido en el comando anterior. De lo contrario, se restablecerá el nombre de usuario, la contraseña y otra información de la configuración importante del ECS, y deberá configurar el sistema operativo manualmente cuando utilice los ECS creados a partir de la imagen privada de Windows.
 - Después de ejecutar este comando, se detendrá ECS automáticamente. Una vez que se detenga el ECS, utilice el ECS para crear una imagen. Los ECS creados con la imagen tienen SID único. Si reinicia un ECS de Windows en el que se ha ejecutado Sysprep, Sysprep solo tiene efecto para el ECS actual. Antes de crear una imagen con el ECS, debe ejecutar Sysprep de nuevo.
 - Para Windows Server 2012 y Windows Server 2012 R2, la contraseña de administrador del ECS se eliminará después de que Sysprep se ejecute en el ECS. Debe iniciar sesión en ECS y restablecer la contraseña del administrador. En este caso, la contraseña de administrador establecida en la consola de gestión no será válida. Mantenga segura la contraseña que configuró.
 - Si se requiere una cuenta de dominio para los inicios de sesión, ejecute Sysprep en ECS antes de usarlo para crear una imagen privada. Para obtener más información sobre el impacto de ejecutar Sysprep, consulte [¿Por qué se requiere Sysprep para crear imágenes privadas con un ECS de Windows?](#)
 - La cuenta Cloudbase-Init de un Windows ECS es una cuenta interna del agente Cloudbase-Init. Esta cuenta se utiliza para obtener metadatos y completar la configuración relevante cuando se inicia Windows ECS. Si modifica o elimina esta cuenta, o desinstala el agente de Cloudbase-Init, no podrá inyectar información personalizada inicial en ECS creado desde una imagen privada de Windows. Por lo tanto, no se recomienda modificar o eliminar la cuenta de Cloudbase-Init.
-

Figura 4-10 Ejecución de Sysprep



Procedimiento posterior

1. Cree una imagen privada desde el ECS en el que se ejecuta Sysprep. Para más detalles, véase [Creación de una imagen de disco del sistema desde un ECS de Windows](#).
2. Puede utilizar la imagen para crear ECS. Cada uno ECS tiene un SID único.

Ejecute el siguiente comando para consultar el SID de ECS:

```
whoami /user
```

Figura 4-11 ECS SID antes de ejecutar Sysprep

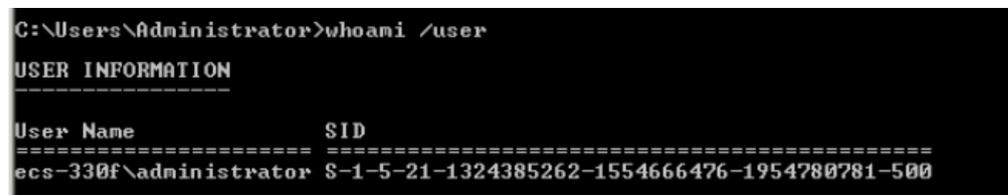
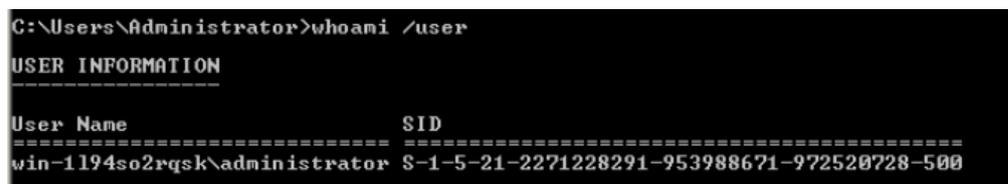


Figura 4-12 ECS SID después de ejecutar Sysprep



5 Operaciones Linux

5.1 Configuración de la NIC en DHCP

Escenarios

Si se crea una imagen privada a partir de un ECS o archivo de imagen externo y la VM donde se encuentra el archivo de imagen externo o ECS está configurada con una dirección IP estática, debe cambiar el atributo NIC a DHCP para que los nuevos ECSs creados a partir de la imagen privada puedan obtener dinámicamente una dirección IP.

El método de configuración varía en función de los sistemas operativos.

NOTA

Al registrar un archivo de imagen externo como una imagen privada, configure DHCP en la VM donde se encuentra el archivo de imagen externo. Se recomienda configurar DHCP en la VM y, a continuación, exportar el archivo de imagen.

Prerrequisitos

Ha iniciado sesión en el ECS utilizado para crear una imagen privada de Windows.

Para obtener más información acerca de cómo iniciar sesión en un ECS, consulte [Descripción de inicio de sesión](#).

Ubuntu 18 o posterior

1. Ejecute `vi /etc/netplan/01-netcfg.yaml` en el ECS para abrir el archivo `/etc/netplan/01-netcfg.yaml` y compruebe si el valor de `dhcp4` es `true`.

- Si `dhcp4` está establecido en `true`, escriba `:q` para salir del editor. No se requerirá ninguna otra acción.

```
network:
  version:2
  renderer:NetworkManager
  ethernets:
    eth0:
      dhcp4: true
```

- Si `dhcp4` se establece en `no` y se configura una dirección IP estática, vaya al siguiente paso.

```
network:
  version:2
  renderer:NetworkManager
  ethernets:
    eth0:
      dhcp4: no
      addresses: [192.168.1.109/24]
      gateway4: 192.168.1.1
      nameservers:
        addresses: [8.8.8.8,114.114.114.114]
```

2. Presione **i** para entrar en el modo de edición.

Elimine la configuración de la dirección IP estática y establezca **dhcp4** en **true**. También puede usar un signo numérico (#) para comentar la configuración de la dirección IP estática.

```
network:
  version:2
  renderer:NetworkManager
  ethernets:
    eth0:
      dhcp4: true # Set dhcp4 to true.
      #dhcp4: no # Delete or comment out the static IP address
settings.
  #addresses: [192.168.1.109]
  #gateway4: 192.168.1.1
  #nameservers:
  # addresses: [8.8.8.8,114.114.114.114]
```

3. Si su ECS tiene más de una NIC, configure DHCP para todos ellos.

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

4. Presione **Esc**, introduzca **:wq** y presione **Enter** para guardar la configuración y salir del editor de vi.
5. Ejecute el comando **netplan apply** para que los ajustes surtan efecto.

Ubuntu 16.04

1. Ejecute el siguiente comando en ECS para abrir el archivo **/etc/network/interfaces**:

vi /etc/network/interfaces

- Si DHCP se ha configurado para todas las NIC, escriba **:q** para salir del editor vi.

```
auto lo
iface lo inet loopback
auto eth0
iface eth0 inet dhcp

auto eth1
iface eth1 inet dhcp
```

- Si las direcciones IP estáticas están configuradas en las NIC, vaya a **2**.

```
auto lo
iface lo inet loopback
auto eth0
#iface eth0 inet dhcp
iface eth0 inet static
address 192.168.1.109
```

```
netmask 255.255.255.0  
gateway 192.168.1.1
```

2. Presione **i** para entrar en el modo de edición.
3. Elimine la configuración de la dirección IP estática y configure DHCP para las NIC.

También puede usar un signo numérico (#) para comentar la configuración de la dirección IP estática.

```
auto lo  
iface lo inet loopback  
auto eth0  
iface eth0 inet dhcp
```

Si el ECS tiene varias NICs, debe configurar DHCP para todas las NIC.

```
auto lo  
iface lo inet loopback  
auto eth0  
iface eth0 inet dhcp  
auto eth1  
iface eth1 inet dhcp
```

4. Pulse **Esc**, escriba **:wq** y pulse **Enter**.
El sistema guarda la configuración y sale del editor vi.

Operaciones relacionadas

Configure DHCP para habilitar el ECS para obtener direcciones IP continuamente.

- Para CentOS y EulerOS, utilice el editor vi para agregar **PERSISTENT_DHCLIENT=""** al archivo de configuración **/etc/sysconfig/network-scripts/ifcfg-ethX**.
- Para SUSE Linux Enterprise, utilice el editor vi para establecer **DHCLIENT_USE_LAST_LEASE** en **no** en el archivo de configuración **/etc/sysconfig/network/dhcp**.
- Para Ubuntu 12.04 o posterior, actualice dhclient a ISC dhclient 4.2.4 para que la NIC pueda obtener direcciones IP del servidor DHCP consistentemente. Para realizar la actualización, primero debe instalar isc-dhcp-server.

5.2 Eliminación de archivos del directorio de reglas de red

Escenarios

Para evitar que el nombre de la NIC se derive cuando se utiliza una imagen privada para crear ECS, debe eliminar los archivos del directorio de reglas de red de la VM donde se encuentra el ECS o archivo de imagen durante la creación de la imagen privada.

NOTA

Al registrar un archivo de imagen externo como una imagen privada, elimine archivos del directorio de reglas de red en la VM donde se encuentra el archivo de imagen externo. Se recomienda eliminar los archivos de la VM y, a continuación, exportar el archivo de imagen.

Prerrequisitos

Se han instalado un sistema operativo y controladores VirtIO en el ECS.

Procedimiento

1. Ejecute el siguiente comando para consultar archivos en el directorio de reglas de red:

```
ls -l /etc/udev/rules.d
```

2. Ejecute los siguientes comandos para eliminar los archivos cuyos nombres contienen **persistente** y **net** del directorio de reglas de red:

Ejemplo:

```
rm /etc/udev/rules.d/30-net_persistent-names.rules
```

```
rm /etc/udev/rules.d/70-persistent-net.rules
```

El contenido en cursiva de los comandos varía según el entorno.

NOTA

Para las imágenes de CentOS 6, para evitar la deriva de nombres de NIC, debe crear un archivo de configuración de reglas vacío.

Ejemplo:

```
touch /etc/udev/rules.d/75-persistent-net-generator.rules //Reemplazar 75 por el valor real en el entorno.
```

3. Eliminar reglas de red.

- Si el sistema operativo utiliza la imagen del sistema initrd, realice las siguientes operaciones:

- i. Ejecute el siguiente comando para comprobar si el archivo de imagen initrd cuyo nombre comienza por **initrd** y termina por **default** contiene los archivos de reglas de dispositivo de red **persistent** y de **net** (reemplazar el contenido en cursiva en el siguiente comando con la versión real del sistema operativo):

```
lsinitrd /boot/initrd-2.6.32.12-0.7-default |grep persistent|grep net
```

- En caso negativo, no se requiere ninguna otra acción.
- En caso afirmativo, vaya a [3.ii](#).

- ii. Ejecute el siguiente comando para realizar una copia de seguridad de los archivos de imagen initrd (reemplazar la parte cursiva en el siguiente comando con la versión real del sistema operativo):

```
cp /boot/initrd-2.6.32.12-0.7-default /boot/initrd-2.6.32.12-0.7-default_bak
```

- iii. Ejecute el siguiente comando para generar el archivo initrd de nuevo:

```
mkinitrd
```

- Si el sistema operativo utiliza la imagen del sistema initramfs (como Ubuntu), realice las siguientes operaciones:

- i. Ejecute el siguiente comando para comprobar si el archivo de imagen initramfs cuyo nombre comienza con **initrd** y termina con **generic** contiene archivos de reglas persistentes y de red.

```
lsinitramfs /boot/initrd.img-3.19.0-25-generic|grep persistent|grep net
```

- En caso negativo, no se requiere ninguna otra acción.
- En caso afirmativo, vaya a [3.ii](#).

- ii. Ejecute el siguiente comando para hacer una copia de seguridad de los archivos de imagen initrd:

```
cp /boot/initrd.img-3.19.0-25-generic /boot/initrd.img-3.19.0-25-generic_bak
```

- iii. Ejecute el siguiente comando para generar los archivos de imagen `initramfs` de nuevo:

```
update-initramfs -u
```

5.3 Instalación de Cloud-Init

Escenarios

Para asegurarse de que puede usar la función de inyección de datos de usuario para inyectar información personalizada inicial en los ECS creados a partir de una imagen privada (como configurar la ECS contraseña de inicio de sesión), instale Cloud-Init en el ECS utilizado para crear la imagen.

- Es necesario descargar Cloud-Init desde su sitio web oficial. Por lo tanto, debe vincular una EIP al ECS.
- Si Cloud-Init no está instalado, no puede configurar un ECS. Como resultado, solo puede usar la contraseña del archivo de imagen para iniciar sesión en los ECS creados.
- De forma predeterminada, los ECS creados a partir de una imagen pública tienen Cloud-Init instalado. No es necesario instalar o configurar Cloud-Init en dichos ECS.
- Para los ECS creados con un archivo de imagen externo, instale y configure Cloud-Init realizando las operaciones de esta sección. Para ver cómo configurar Cloud-Init, consulte [Configuración de Cloud-Init](#).

NOTA

Cloud-Init es un software de código abierto. Si la versión instalada tiene vulnerabilidades de seguridad, se recomienda actualizarla a la versión más reciente.

Prerrequisitos

- Una EIP ha sido vinculada al ECS.
- Ha iniciado sesión en el ECS.
- El modo de obtención de la dirección IP del ECS es DHCP.

Procedimiento

1. Comprueba si se ha instalado Cloud-Init.
Para obtener más información, véase [Comprobar si se ha instalado Cloud-Init](#).

2. Instale Cloud-Init.

Puede instalar Cloud-Init de cualquiera de las siguientes maneras: **(Recomendado) Instalar Cloud-Init usando el paquete de instalación oficial**, **Instalar Cloud-Init usando el paquete oficial de código fuente y pip** y **Instalar Cloud-Init usando el código fuente oficial de GitHub**.

Comprobar si se ha instalado Cloud-Init

Realice las operaciones proporcionadas aquí para comprobar si se ha instalado Cloud-Init. Los métodos para comprobar si Cloud-Init está instalado varían en función de los sistemas operativos.

- Si se encuentra en un entorno de Python 3, ejecute el siguiente comando para comprobar si Cloud-Init está instalado (Ubuntu22.0.4 se usa como ejemplo):

which cloud-init

- Si se muestra información similar a la siguiente, se ha instalado Cloud-Init:

```
/usr/bin/cloud-init
```

- Si se muestra información similar a la siguiente, Cloud-Init no está instalado:

```
/usr/bin/which: no cloud-init in (/usr/local/bin:/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin)
```

- Si estás en un entorno de Python 2, ejecuta el siguiente comando para comprobar si Cloud-Init está instalado (CentOS 6 se usa como ejemplo):

which cloud-init

- Si se muestra información similar a la siguiente, se ha instalado Cloud-Init:

```
cloud-init-0.7.5-10.el6.centos.2.x86_64
```

- Si no se devuelve ninguna información, Cloud-Init no está instalado.

 **NOTA**

Para confirmar que Cloud-Init realmente no está instalado, se recomienda ejecutar **rpm -qa | grep cloud-init** para comprobar de nuevo. Si cualquiera de **which cloud-init** y **rpm -qa | grep cloud-init** muestra que Cloud-Init se ha instalado, Cloud-Init está instalado.

Si se ha instalado Cloud-Init, realice las siguientes operaciones:

- Compruebe si se utiliza el certificado SSH en el sistema operativo ECS. Si el certificado ya no se utiliza, elimínelo.

- Si el certificado se almacena en un directorio de usuario **root**, por ejemplo, `$path/$to/$root/.ssh/authorized_keys`, ejecute los siguientes comandos:

```
cd /root/.ssh
```

```
rm authorized_keys
```

- Si el certificado no está almacenado en un directorio de usuario **root**, por ejemplo, `$path/$to/$none-root/.ssh/authorized_keys`, ejecute los siguientes comandos:

```
cd /home/centos/.ssh
```

```
rm authorized_keys
```

- Ejecute el siguiente comando para eliminar la caché generada por Cloud-Init y asegúrese de que la ECS creada a partir de la imagen privada se puede iniciar con el certificado:

```
sudo rm -rf /var/lib/cloud/*
```

 **NOTA**

No reinicie el ECS después de realizar la configuración. De lo contrario, necesita configurarlo de nuevo.

(Recomendado) Instalar Cloud-Init usando el paquete de instalación oficial

El método de instalación de Cloud-Init en un ECS varía dependiendo del sistema operativo. Realice las operaciones de instalación como usuario **root**.

A continuación se describe cómo instalar Cloud-Init en un ECS que ejecute SUSE Linux, CentOS, Fedora, Debian y Ubuntu. Para otros tipos de sistemas operativos, instale el tipo requerido de Cloud-Init. Por ejemplo, necesita instalar coreos-cloudinit en los ECS que ejecutan CoreOS.

- SUSE Linux

Rutas de acceso para obtener el paquete de instalación de Cloud-Init para SUSE Linux

<https://ftp5.gwdg.de/pub/opensuse/repositories/Cloud:/Tools/>
<http://download.opensuse.org/repositories/Cloud:/Tools/>

 **NOTA**

Seleccione el paquete de instalación de repositorio necesario en las rutas proporcionadas. Tome SUSE Enterprise Linux Server 12 como ejemplo. Realice los siguientes pasos para instalar Cloud-Init:

- a. Inicie sesión en el ECS utilizado para crear una imagen privada de Linux.
- b. Ejecute el siguiente comando para instalar el origen de instalación de red para SUSE Enterprise Linux Server 12:

```
zypper ar https://ftp5.gwdg.de/pub/opensuse/repositories/Cloud:/Tools/  
SLE_12_SP3/Cloud:Tools.repo
```

- c. Ejecute el siguiente comando para actualizar el origen de instalación de red:

```
zypper refresh
```

- d. Ejecute el siguiente comando para instalar Cloud-Init:

```
zypper install cloud-init
```

- e. Ejecute los siguientes comandos para habilitar Cloud-Init para que se inicie automáticamente al iniciar el sistema:

- SUSE 11

```
chkconfig cloud-init-local on; chkconfig cloud-init on; chkconfig cloud-  
config on; chkconfig cloud-final on
```

```
service cloud-init-local status; service cloud-init status; service cloud-  
config status; service cloud-final status
```

- SUSE 12 y openSUSE 12/13/42

```
systemctl enable cloud-init-local.service cloud-init.service cloud-  
config.service cloud-final.service
```

```
systemctl status cloud-init-local.service cloud-init.service cloud-  
config.service cloud-final.service
```

 **ATENCIÓN**

Para SUSE y openSUSE, realice los siguientes pasos para deshabilitar el cambio dinámico del nombre de ECS:

1. Ejecute el siguiente comando para abrir el archivo **dhcp** usando el editor vi:

```
vi etc/sysconfig/network/dhcp
```
2. Cambie el valor de **DHCLIENT_SET_HOSTNAME** en el archivo **dhcp** a **no**.

● **CentOS**

Tabla 5-1 enumera las rutas de instalación de Cloud-Init para CentOS. Seleccione el paquete de instalación requerido en las siguientes direcciones.

Tabla 5-1 Direcciones del paquete de instalación de Cloud-Init

Tipo de sistema operativo	Versión	Cómo obtenerlo
CentOS	6 32-bit	https://archives.fedoraproject.org/pub/archive/epel/6/i386/
	6 64-bit	https://archives.fedoraproject.org/pub/archive/epel/6/x86_64/
	7 64-bit	https://archives.fedoraproject.org/pub/archive/epel/7/x86_64/Packages/e/

- a. Ejecute los siguientes comandos para instalar Cloud-Init:

```
yum install Cloud-Init installation package address/epel-release-x-y.noarch.rpm  

yum install cloud-init
```

 **NOTA**

La dirección del paquete de instalación de Cloud-Init indica la dirección del paquete de instalación de Cloud-Init epel-release, y x-y indica la versión de Cloud-Init epel-release requerida por el sistema operativo actual. Reemplácelos con los valores reales según [Tabla 5-1](#).

- Tome CentOS 6 de 64 bits como ejemplo. Si la versión es 6.8, el comando es el siguiente:

```
yum install https://archives.fedoraproject.org/pub/archive/epel/6/x86_64/epel-release-6-8.noarch.rpm
```

- Tome CentOS 7 de 64 bits como ejemplo. Si la versión es 7.14, el comando es el siguiente:

```
yum install https://archives.fedoraproject.org/pub/epel/7/x86_64/Packages/e/epel-release-7-14.noarch.rpm
```

- b. Ejecute los siguientes comandos para habilitar Cloud-Init para que se inicie automáticamente al iniciar el sistema:

```
systemctl enable cloud-init-local.service cloud-init.service cloud-config.service cloud-final.service
```

```
systemctl status cloud-init-local.service cloud-init.service cloud-config.service cloud-final.service
```

- Fedora

Antes de instalar Cloud-Init, asegúrese de que la dirección de origen de instalación de red se ha configurado para el sistema operativo comprobando si el archivo `/etc/yum.repo.d/fedora.repo` contiene la dirección de origen de instalación del paquete de software. Si el archivo no contiene la dirección, configure la dirección siguiendo las instrucciones en el sitio web oficial de Fedora.

- a. Ejecute el siguiente comando para instalar Cloud-Init:

```
yum install cloud-init
```

- b. Ejecute los siguientes comandos para habilitar Cloud-Init para que se inicie automáticamente al iniciar el sistema:

```
systemctl enable cloud-init-local.service cloud-init.service cloud-config.service  
cloud-final.service
```

```
systemctl status cloud-init-local.service cloud-init.service cloud-config.service  
cloud-final.service
```

- Debian y Ubuntu

Antes de instalar Cloud-Init, asegúrese de que la dirección de origen de instalación de red se ha configurado para el sistema operativo comprobando si el archivo `/etc/apt/sources.list` contiene la dirección de origen de instalación del paquete de software. Si el archivo no contiene la dirección, configure la dirección siguiendo las instrucciones en el sitio web oficial de Debian o Ubuntu.

- a. Ejecute los siguientes comandos para instalar Cloud-Init:

```
apt-get update
```

```
apt-get install cloud-init
```

- b. Ejecute los siguientes comandos para habilitar Cloud-Init para que se inicie automáticamente al iniciar el sistema:

```
systemctl enable cloud-init-local.service cloud-init.service cloud-config.service  
cloud-final.service
```

```
systemctl status cloud-init-local.service cloud-init.service cloud-config.service  
cloud-final.service
```

Cloud-Init-23.2.2 se utiliza como ejemplo para describir cómo instalar Cloud-Init en CentOS, Fedora, Ubuntu, Debian y SUSE.

Descargue el paquete de código fuente `cloud-init-23.2.2.tar.gz` desde <https://launchpad.net/cloud-init/trunk/23.2.2/+download/cloud-init-23.2.2.tar.gz>.

- Centos 7/Fedora Server 36

AVISO

Asegúrese de que Python 3 se ha instalado.

- a. Comprueba si se ha instalado Cloud-Init. Si se muestra algún resultado de comando, se ha instalado Cloud-Init.

```
cloud-init -v
```

- b. Elimine el directorio de caché de Cloud-Init.

```
rm -rf /var/lib/cloud/*
```

- c. Instale paquetes de dependencias de Cloud-Init.

```
yum install python3-pip -y  
yum install python3-devel
```

- d. Descargue el paquete Cloud-Init.

```
wget https://launchpad.net/cloud-init/trunk/23.2.2/+download/cloud-  
init-23.2.2.tar.gz
```

- e. Descomprima el paquete Cloud-Init.

```
tar -zxvf cloud-init 23.2.2.tar.gz
```

- f. Vaya al directorio `cloud-init-23.2.2` e instale bibliotecas dependientes:

```
cd cloud-init23.2.2  
pip3 install -r requirements.txt
```

- g. Instale Cloud-Init.

```
python3 setup.py build  
python3 setup.py install --init-system system
```

- h. (Opcional) Deshabilite la capacidad de configuración de red de Cloud-Init modificando el archivo `/etc/cloud/cloud.cfg`.

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

Agregue el siguiente contenido al archivo:

```
network:
  config: disabled
```

- i. Reinicie Cloud-Init y compruebe su estado.

```
systemctl restart cloud-init-local.service cloud-init.service cloud-
config.service cloud-final.service
systemctl status cloud-init-local.service cloud-init.service cloud-
config.service cloud-final.service
```

```
Searching for six==1.16.0
Best match: six 1.16.0
Adding six 1.16.0 to easy-install.pth file

Using /usr/local/lib/python3.6/site-packages
Searching for typing-extensions==4.1.1
Best match: typing-extensions 4.1.1
Adding typing-extensions 4.1.1 to easy-install.pth file

Using /usr/local/lib/python3.6/site-packages
Searching for zipp==3.6.0
Best match: zipp 3.6.0
Adding zipp 3.6.0 to easy-install.pth file

Using /usr/local/lib/python3.6/site-packages
Finished processing dependencies for cloud-init==23.2.2
[root@localhost cloud-init-23.2.2]#
[root@localhost cloud-init-23.2.2]#
[root@localhost cloud-init-23.2.2]# cloud-init -v
/usr/local/bin/cloud-init 23.2.2
[root@localhost cloud-init-23.2.2]# _
```

- j. Habilite los servicios relacionados con Cloud-Init para que se inicien automáticamente al iniciar el sistema.

```
systemctl enable cloud-init-local.service cloud-init.service cloud-
config.service cloud-final.service
```

- k. Comprueba si Cloud-Init se está ejecutando correctamente.

```
cloud-init -v
cloud-init init --local
```

```
Using /usr/local/lib/python3.6/site-packages
Finished processing dependencies for cloud-init==23.2.2
[root@localhost cloud-init-23.2.2]#
[root@localhost cloud-init-23.2.2]#
[root@localhost cloud-init-23.2.2]# cloud-init -v
/usr/local/bin/cloud-init 23.2.2
[root@localhost cloud-init-23.2.2]# _
```

● **Ubuntu22.04/Debian 11**

AVISO

Asegúrese de que Python 3 se ha instalado.

- a. Compruebe y elimine los archivos de configuración redundantes de Cloud-Init.

```
rm -rf /var/lib/cloud/*
rm -f /var/log/cloud-init*
```

Elimine todos los archivos excepto los archivos de configuración relacionados con el registro del directorio `/etc/cloud/cloud.cfg.d/`.

- b. Actualice su lista de paquetes y compruebe si Wget está instalado. Si no lo es, instálelo.

```
sudo apt update
sudo apt install wget
```

- c. Instale paquetes de dependencias.

```
apt-get install cloud-guest-utils -y
apt-get install python3-pip -y
apt-get install python3-devel
```

- d. Descargue el paquete Cloud-Init.

```
wget https://launchpad.net/cloud-init/trunk/23.2.2/+download/cloud-
init-23.2.2.tar.gz
```

- e. Descomprima el paquete Cloud-Init.
`tar -zxvf cloud-init 23.2.2.tar.gz`
- f. Vaya al directorio **cloud-init**.
`cd cloud-init`
- g. Instalar bibliotecas dependientes.
`pip3 install -r requirements.txt`
- h. Instale Cloud-Init.
`python3 setup.py install`
- i. (Opcional) Desactive la capacidad de configuración de red de Cloud-Init.
Debe hacerlo cuando la versión de Cloud-Init sea 0.7.9 o posterior y desee configurar la red.

 **NOTA**

1. Abra el archivo `/etc/cloud/cloud.cfg`.
`vi /etc/cloud/cloud.cfg`
2. Ingrese `i` y configure **network**. (Si no hay tal elemento de configuración, agréguelo.)
`network:`
`config: disabled`
- j. Reinicie Cloud-Init y compruebe su estado.
`systemctl restart cloud-init-local.service cloud-init.service cloud-config.service cloud-final.service`
`systemctl status cloud-init-local.service cloud-init.service cloud-config.service cloud-final.service`
- k. Habilite los servicios relacionados con Cloud-Init para que se inicien automáticamente al iniciar el sistema.
`systemctl enable cloud-init-local.service cloud-init.service cloud-config.service cloud-final.service`
- l. Comprueba si Cloud-Init se está ejecutando correctamente.
`cloud-init -v`
`cloud-init init --local`

● **SUSE Enterprise Linux Server 15**

AVISO

Asegúrese de que Python 3 se ha instalado.

- a. Vea repositorios de SUSE existentes.
`zypper lr`
- b. Elimine los repositorios de SUSE.
`zypper rr No. of repositories listed in 1`
- c. Configure un repositorio de SUSE.
`zypper ar https://ftp5.gwdg.de/pub/opensuse/repositories/Cloud:/Tools/SLE_15_SP4/Cloud:Tools.repo`
- d. Actualice el repositorio de SUSE.
`zypper refresh`
- e. Instale Cloud-Init.
`zypper install cloud-init`
- f. Ejecuta **cloud-init -v**. Si se muestran mensajes de error similares a los siguientes, instale los paquetes de dependencias.

Instalar Cloud-Init usando el paquete oficial de código fuente y pip

Las siguientes operaciones usan Cloud-Init 0.7.9 como ejemplo para describir cómo instalar Cloud-Init.

1. Descargue el paquete de código fuente **cloud-init-0.7.9.tar.gz** (se recomienda la versión 0.7.9) y súbalo al directorio **/home/** del ECS.

Descargue **cloud-init-0.7.9.tar.gz** desde la siguiente ruta:

<https://launchpad.net/cloud-init/trunk/0.7.9/+download/cloud-init-0.7.9.tar.gz>

2. Cree un archivo **pip.conf** en el directorio **~/pip/** y edite el siguiente contenido:

NOTA

Si el directorio **~/pip/** no existe, ejecute el comando **mkdir ~/pip** para crearlo.

```
[global]
index-url = https://<$mirror>/simple/
trusted-host = <$mirror>
```

NOTA

Reemplace **<\$mirror>** con un origen PyPI de red pública.

Fuente de PyPI de la red pública <https://pypi.python.org/>

3. Ejecute el siguiente comando para instalar el paquete de código fuente de Cloud-Init descargado (seleccione **--upgrade** según sea necesario durante la instalación):

```
pip install [--upgrade] /home/cloud-init-0.7.9.tar.gz
```

NOTA

Para obtener más información sobre cómo instalar un paquete de código fuente de Cloud-Init, consulte [Documentación de Cloud-Init](#).

4. Ejecute el comando **cloud-init -v**. Cloud-Init se instala correctamente si se muestra la siguiente información:

```
cloud-init 0.7.9
```

5. Habilite Cloud-Init para que se inicie automáticamente al iniciar el sistema.

- Si el sistema operativo utiliza SysVinit para gestionar el inicio automático de los servicios, ejecute los siguientes comandos:

```
chkconfig --add cloud-init-local; chkconfig --add cloud-init; chkconfig --add cloud-config; chkconfig --add cloud-final
```

```
chkconfig cloud-init-local on; chkconfig cloud-init on; chkconfig cloud-config on; chkconfig cloud-final on
```

```
service cloud-init-local status; service cloud-init status; service cloud-config status; service cloud-final status
```

- Si el sistema operativo utiliza Systemd para gestionar el inicio automático de servicios, ejecute los siguientes comandos:

```
systemctl enable cloud-init-local.service cloud-init.service cloud-config.service cloud-final.service
```

```
systemctl status cloud-init-local.service cloud-init.service cloud-config.service cloud-final.service
```

 **ATENCIÓN**

Si instalas Cloud-Init usando el paquete de código fuente oficial y pip, presta atención a lo siguiente:

1. Agregar usuario **syslog** al grupo **adm** durante la instalación. Si existe usuario **syslog**, agréguelo al grupo **adm**. Para algunos sistemas operativos (como CentOS y SUSE), es posible que el usuario **syslog** no exista. Ejecute los siguientes comandos para crear usuario de **syslog** y agregarlo al grupo **adm**:

```
useradd syslog
groupadd adm
usermod -g adm syslog
```

2. Cambie el valor de **distro** en **system_info** en el archivo `/etc/cloud/cloud.cfg` basado en la versión de lanzamiento del sistema operativo, como **distro: ubuntu**, **distro: sles**, **distro: debian**, y **distro: fedora**.

Instalar Cloud-Init usando el código fuente oficial de GitHub

Puede obtener el código fuente de Cloud-Init de GitHub en <https://github.com/canonical/cloud-init/>

1. Ejecute los siguientes comandos para descargar el paquete de código fuente y copiarlo a la carpeta `/tmp/CLOUD-INIT` :

 **NOTA**

Cloud-Init 0.7.6: <https://github.com/canonical/cloud-init/archive/refs/tags/0.7.6.zip>

Cloud-Init 0.7.9: <https://github.com/canonical/cloud-init/archive/refs/tags/0.7.9.zip>

Todas las versiones: <https://github.com/canonical/cloud-init/releases>

```
wget https://github.com/canonical/cloud-init/archive/refs/tags/0.7.6.zip
```

```
mkdir /tmp/CLOUD-INIT
```

```
cp cloud-init-0.7.6.zip /tmp/CLOUD-INIT
```

```
cd /tmp/CLOUD-INIT
```

2. Ejecute el siguiente comando para descomprimir el paquete:

```
unzip cloud-init-0.7.6.zip
```

3. Ejecute el siguiente comando para ingresar a la carpeta **cloud-init-0.7.6**:

```
cd cloud-init-0.7.6
```

4. (Opcional) Si la versión de Cloud-Init es 18.3 a 22.3, ejecute los siguientes comandos:

```
sed -i '/VALID_DMI_ASSET_TAGS =/a\VALID_DMI_ASSET_TAGS += ["HUAWAICLOUD"]' cloudinit/sources/DataSourceOpenStack.py
```

```
cat cloudinit/sources/DataSourceOpenStack.py | grep VALID_DMI_ASSET_TAGS
```

Si se muestra la siguiente información, la ejecución se realiza correctamente.

```
root@ecs-cc9e cloud-init# cat cloudinit/sources/DataSourceOpenStack.py | grep VALID_DMI_ASSET_TAGS
VALID_DMI_ASSET_TAGS = VALID_DMI_PRODUCT_NAMES
VALID_DMI_ASSET_TAGS += ["HUAWAICLOUD"]
VALID_DMI_ASSET_TAGS += [DMI_ASSET_TAG_OPENTELEKOM, DMI_ASSET_TAG_SAPCCLOUD]
elif dmi.read_dmi_data("chassis-asset-tag") in VALID_DMI_ASSET_TAGS:
root@ecs-cc9e cloud-init#
```

5. Instale Cloud-Init. Los comandos varían según el tipo de sistema operativo.

- Para CentOS 6.x o SUSE 11.x, ejecute los siguientes comandos:
python setup.py build
python setup.py install --init-system sysvinit
- Para CentOS 7.x o SUSE 12.x, ejecute los siguientes comandos:
python setup.py build
python setup.py install --init-system systemd

NOTA

Agregar usuario **syslog** al grupo **adm** durante la instalación. Si existe usuario **syslog**, agréguelo al grupo **adm**. Para algunos sistemas operativos (como CentOS y SUSE), es posible que el usuario **syslog** no exista. Ejecute los siguientes comandos para crear usuario de **syslog** y agregarlo al grupo **adm**:

```
useradd syslog
groupadd adm
usermod -g adm syslog
```

6. Habilite Cloud-Init para que se inicie automáticamente al iniciar el sistema.

- Si el sistema operativo utiliza SysVinit para gestionar el inicio automático de los servicios, ejecute los siguientes comandos:

```
chkconfig --add cloud-init-local; chkconfig --add cloud-init; chkconfig --add
cloud-config; chkconfig --add cloud-final
```

```
chkconfig cloud-init-local on; chkconfig cloud-init on; chkconfig cloud-config
on; chkconfig cloud-final on
```

```
service cloud-init-local status; service cloud-init status; service cloud-config
status; service cloud-final status
```

- Si el sistema operativo utiliza Systemd para gestionar el inicio automático de servicios, ejecute los siguientes comandos:

```
systemctl enable cloud-init-local.service cloud-init.service cloud-config.service
cloud-final.service
```

```
systemctl status cloud-init-local.service cloud-init.service cloud-config.service
cloud-final.service
```

7. Ejecute los siguientes comandos para comprobar si se ha instalado Cloud-Init:

```
cloud-init -v
cloud-init init --local
```

Cloud-Init se instala correctamente si se muestra la siguiente información:

```
cloud-init 0.7.6
```

5.4 Configuración de Cloud-Init

Escenarios

Es necesario configurar Cloud-Init después de que esté instalado.

Prerrequisitos

- Se ha instalado Cloud-Init.
- Una EIP ha sido vinculada al ECS.

- Ha iniciado sesión en ECS.
- El modo de obtención de la dirección IP del ECS es DHCP.

Procedimiento

Se requieren las siguientes operaciones:

1. Configurar Cloud-Init.
Para obtener más información, véase [Configurar Cloud-Init](#).
2. Revise si se configuró correctamente Cloud-Init.
Para obtener más información, véase [Comprobar la configuración de Cloud-Init](#).

Configurar Cloud-Init

1. Configurar los permisos de usuario para iniciar sesión en ECS. Si selecciona usuario **root**, habilite los permisos SSH del usuario **root** y habilite el inicio de sesión remoto en el ECS mediante una contraseña.
 - Si introduce una contraseña, utilícela para iniciar sesión en el ECS de forma remota mediante SSH o noVNC.
 - Si inyecta una clave, utilícela para iniciar sesión en el ECS de forma remota mediante SSH.

2. Habilite el inicio de sesión remoto usando la contraseña del usuario **root** y habilite los permisos SSH del usuario **root**.

Tome CentOS 6.7 como ejemplo. Si el valor de **disable_root** en el archivo `/etc/cloud/cloud.cfg` es de **0**, los permisos están habilitados. (En algunos sistemas operativos, el valor **true** indica que los permisos están deshabilitados y **false** indica que los permisos están habilitados). Establezca **ssh_pwauth** en **1** y **lock_passwd** en **False** (indicando que las contraseñas de usuario no están bloqueadas).

```
users:  
- name: root  
  lock_passwd: False  
  
disable_root: 0  
ssh_pwauth: 1
```

3. Evite que Cloud-Init se haga cargo de la red en `/etc/cloud/cloud.cfg`.

Si la versión de Cloud-Init es 0.7.9 o posterior, agregue el siguiente contenido a `/etc/cloud/cloud.cfg`:

Figura 5-1 Evitar que Cloud-Init se apodere de la red

```
users:  
- name: root  
  lock_passwd: False  
  
disable_root: 0  
ssh_pwauth: 1  
  
datasource_list: ['OpenStack']  
  
network:  
  config: disabled
```

NOTA

El contenido agregado debe estar en formato YAML.

- Habilite al agente para acceder al origen de datos de OpenStack de IaaS.

Añada la siguiente información a la última línea de `/etc/cloud/cloud.cfg`:

```
datasource_list: [ OpenStack ]
datasource:
  OpenStack:
    metadata_urls: ['http://169.254.169.254']
    max_wait: 120
    timeout: 5
    apply_network_config: false
```

NOTA

- Puede decidir si desea establecer `max_wait` y `timeout`. Los valores de `max_wait` y `timeout` en la salida del comando anterior son solo de referencia.
- Si la versión del sistema operativo es anterior a Debian 8 o CentOS 5, no puede habilitar al agente para acceder a la fuente de datos de OpenStack de IaaS.
- La ruta `zeroconf` predeterminada debe estar deshabilitada para los ECS de CentOS y EulerOS para un acceso preciso al origen de datos OpenStack de IaaS.
`echo "NOZEROCONF=yes" >> /etc/sysconfig/network`
- `apply_network_config: false` solo es requerido por los usuarios que usan Cloud-Init 18.3 o posterior.

- Añada el siguiente contenido a `/etc/cloud/cloud.cfg`:

manage_etc_hosts: localhost

Esto evita que el sistema permanezca en el estado **Waiting for cloudResetPwdAgent** durante mucho tiempo durante el inicio de ECS.

Figura 5-2 Adición de `manage_etc_hosts: localhost`

```
datasource_list: ['OpenStack']
manage_etc_hosts: localhost

datasource:
  OpenStack:
    # timeout: the timeout value for a request at metadata service
    timeout : 50
    # The length in seconds to wait before giving up on the metadata
    # service. The actual total wait could be up to
    # len(resolvable_metadata_urls)*timeout
    max_wait : 120
```

- Ejecute el comando `vi /etc/ssh/sshd_config` para abrir el archivo `/etc/ssh/sshd_config` usando el editor `vi`.

Cambie el valor de `PasswordAuthentication` en el archivo `sshd_config` a `yes`.

NOTA

Para SUSE y openSUSE, cambie los valores de los siguientes parámetros en el archivo `sshd_config` a `yes`:

- `PasswordAuthentication`
- `ChallengeResponseAuthentication`

- Modifique `cloud_init_modules` en el archivo de configuración `cloud.cfg`.

– Mueva `ssh` de abajo a arriba para acelerar el inicio de sesión de SSH.

- Habilite la actualización del nombre de host. No comente ni elimine la sentencia - **update_hostname**.

```
cloud_init_modules:
- ssh
- migrator
- bootcmd
- write-files
- growpart
- resizefs
- set_hostname
- update_hostname
- update_etc_hosts
- rsyslog
- users-groups
```

8. Modifique la configuración para que el nombre de host del ECS creado a partir de la imagen no contenga el sufijo **.novalocal** y pueda contener un punto (.

- a. Ejecute el siguiente comando para modificar el archivo **__init__.py**:
vi /usr/lib/python*/site-packages/cloudinit/sources/__init__.py

La versión de Python varía según el sistema operativo.

Pulse **i** para entrar en el modo de edición. Modifique el contenido del archivo de la siguiente manera en función de la palabra clave **toks**:

```
if toks:
    toks = str(toks).split('.')
else:
    #toks = ["ip-%s" % lhost.replace(".", "-")] # Comment out this line.
    toks = lhost.split(".novalocal") # Add this line.

if len(toks) > 1:
    hostname = toks[0]
    #domain = '.'.join(toks[1:]) # Comment out this line.
else:
    hostname = toks[0]

if fqdn and domain != defdomain:
    #return hostname # Comment out this line.
    return "%s.%s" % (hostname, domain) # Add this line.
else:
    return hostname
```

Una vez completada la modificación, pulse **Esc** para salir del modo de edición y entrar en **:wq!** para guardar la configuración y salir.

- b. Ejecute el siguiente comando para cambiar a la carpeta **cloudinit/sources**:

cd /usr/lib/python*/site-packages/cloudinit/sources/

La versión de Python varía según el sistema operativo.

- c. Ejecute los siguientes comandos para eliminar el archivo **__init__.pyc** y el archivo **__init__.pyo** optimizado:

rm -rf __init__.pyc

rm -rf __init__.pyo

- d. Ejecute los siguientes comandos para borrar los registros:

rm -rf /var/lib/cloud/*

rm -rf /var/log/cloud-init*

9. Ejecute el siguiente comando para editar el archivo **/etc/cloud/cloud.cfg.d/05_logging.cfg** para usar **cloudLogHandler** para procesar registros:

vim /etc/cloud/cloud.cfg.d/05_logging.cfg

```
[logger_cloudinit]
level=DEBUG
```

```
qualname=cloudinit  
handlers=cloudLogHandler  
propagate=1
```

10. Elimine el usuario **linux** y el directorio **/home/linux** de la plantilla de imagen.

```
userdel linux
```

```
rm -fr /home/linux
```

Comprobar la configuración de Cloud-Init

Ejecute el siguiente comando para comprobar si Cloud-Init se ha configurado correctamente:

```
cloud-init init --local
```

Si Cloud-Init se ha instalado correctamente, se muestra la información de la versión y no se produce ningún error. Por ejemplo, no se mostrarán mensajes que indiquen la falta de archivos.

NOTA

(Opcional) Ejecute el siguiente comando para establecer el período de validez de la contraseña al máximo:

```
chage -M 99999 $user_name
```

user_name es un usuario del sistema, como usuario **root**.

Se recomienda establecer el período de validez de la contraseña en **99999**.

5.5 Instalación del complemento de restablecimiento de contraseñas con un solo clic

Escenarios

Se recomienda instalar el complemento de restablecimiento de contraseña CloudResetPwdAgent antes de crear una imagen privada. De esta manera, puede restablecer la contraseña de los ECS creados a partir de la imagen con unos pocos clics.

- Los ECS creados a partir de una imagen pública tienen este plug-in instalado de forma predeterminada.
- Para los ECS creados a partir de un archivo de imagen externo, instale el complemento realizando las operaciones de esta sección.

Precauciones

- Puede decidir si desea instalar el complemento CloudResetPwdAgent.
- El complemento ha sido de código abierto en la plataforma de código abierto GitHub según *GNU General Public License v2.0*.
- No todos los sistemas operativos admiten el complemento de restablecimiento de contraseña con un solo clic. [Tabla 5-2](#) enumera los sistemas operativos que admiten este complemento.

Tabla 5-2 Sistemas operativos compatibles con el complemento de restablecimiento de contraseña con un solo clic

Tipo de sistema operativo	Versión del sistema operativo
CentOS	CentOS 8.3 64bit CentOS 8.2 64bit CentOS 8.1 64bit CentOS 8.0 64bit CentOS 7.3 64bit CentOS 7.2 64bit CentOS 7.0 64bit CentOS 7.1 64bit CentOS 6.9 64bit CentOS 6.8 64bit CentOS 6.8 32bit CentOS 6.6 32bit CentOS 6.6 64bit CentOS 6.5 64bit CentOS 6.4 64bit CentOS 6.3 64bit NOTA Para CentOS 8, deshabilite SELinux antes de instalar el complemento de restablecimiento de contraseña con un solo clic. Después de instalar el complemento, puede determinar si habilitar SELinux según sea necesario.
Debian	Debian 9.0 64bit Debian 8.8 64bit Debian 8.2 64bit Debian 7.5 64bit Debian 7.5 32bit
openSUSE	openSUSE 42.2 64bit openSUSE 13.2 64bit openSUSE Leap 42.2 64bit openSUSE Leap 42.1 64bit
SUSE	SUSE 12 SP2 64bit SUSE 12 SP1 64bit SUSE 11 SP4 64bit

Tipo de sistema operativo	Versión del sistema operativo
Ubuntu	Ubuntu 16.10 32bit Ubuntu 16.04 32bit Ubuntu Server 16.04 64bit Ubuntu Server 14.04 64bit Ubuntu Server 14.04 32bit
EulerOS	EulerOS 2.2 64bit
Fedora	Fedora 25 64bit Fedora 24 64bit
Oracle Linux	Oracle Linux 7.3 64bit Oracle Linux 6.9 64bit Oracle Linux 6.5 64bit

Prerrequisitos

- El estado del ECS es de **Running**.
- El ECS debe tener un espacio restante de más de 300 MB, y los datos se pueden escribir en su directorio raíz.
- SELinux afecta al complemento de restablecimiento de contraseña de los ECS de Linux. Puede deshabilitarlo haciendo referencia a [Deshabilitación de SELinux](#).
- Los ECS creados con una imagen de SUSE 11 SP4 deben tener 4 GB o una memoria mayor.
- DHCP debe estar habilitado para la VPC utilizada por el ECS.
- Las redes del ECS son normales.
- La regla de grupo de seguridad saliente del ECS debe cumplir los siguientes requisitos:
 - **Protocolo: TCP**
 - **Rango de puerto: 80**
 - **Extremo remoto: 169.254.0.0/16**

Si utiliza la regla de grupo de seguridad saliente predeterminada, se pueden cumplir los requisitos anteriores y se puede inicializar el ECS. La regla predeterminada del grupo de seguridad saliente es la siguiente:

- **Protocolo: Todos**
- **Rango de puerto: Todos**
- **Extremo remoto: 0.0.0.0/16**

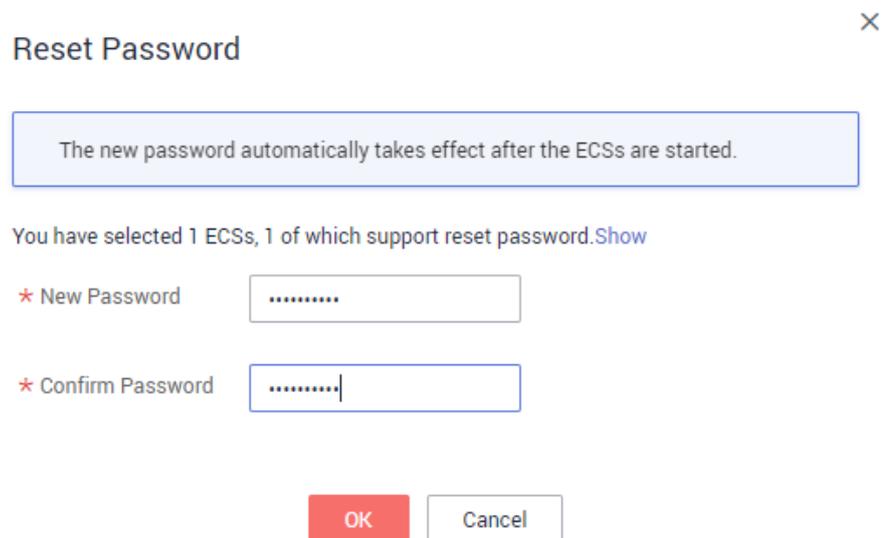
Procedimiento

Paso 1 Utilice cualquiera de los siguientes métodos para comprobar si los complementos de restablecimiento de contraseña se han instalado en el ECS:

Método 1: Utilice la consola de gestión para la consulta.

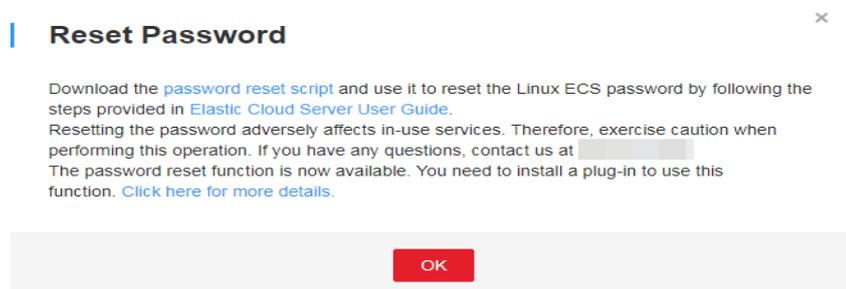
1. Inicie sesión en la consola de gestión.
2. Haga clic en . En **Compute**, haga clic en **Elastic Cloud Server**.
3. Busque la fila que contiene el ECS de destino, haga clic en **More** en la columna **Operation** y seleccione **Reset Password** en la lista desplegable.
 - Si aparece un cuadro de diálogo en el que se le pide que introduzca la nueva contraseña, se instalarán los complementos de restablecimiento de contraseña. No se requiere ninguna otra acción.

Figura 5-3 Información mostrada si se han instalado los complementos de restablecimiento de contraseña



- Si aparece un cuadro de diálogo que le pide que descargue un script de restablecimiento de contraseña, los complementos de restablecimiento de contraseña no se han instalado. Luego, instálelos.

Figura 5-4 Información mostrada si los plug-ins de restablecimiento de contraseña no se han instalado



Método 2: Utilice ECS para consultar.

1. Inicie sesión en ECS como usuario root.
2. Ejecute el siguiente comando para comprobar si CloudResetPwdAgent y CloudResetPwdUpdateAgent están instalados:

ls -lh /Cloud*

Figura 5-5 Comprobación de si se han instalado los complementos

```
[root@test-... home]# ls -lh /Cloud*
/CloudResetPwdUpdateAgent:
total 20K
drwxr-xr-x 2 root root 4.0K Feb 14 09:20 bin
drwxr-xr-x 2 root root 4.0K Dec 6 17:09 conf
drwxr-xr-x 3 root root 4.0K Dec 6 17:09 depend
drwxr-xr-x 2 root root 4.0K Dec 6 17:09 lib
drwxr-xr-x 2 root root 4.0K Feb 14 09:20 logs

/CloudrResetPwdAgent:
total 20K
drwxr-xr-x 2 root root 4.0K Feb 14 09:20 bin
drwxr-xr-x 2 root root 4.0K Dec 6 17:09 conf
drwxr-xr-x 2 root root 4.0K Dec 6 17:09 depend
drwxr-xr-x 2 root root 4.0K Dec 6 17:09 lib
drwxr-xr-x 2 root root 4.0K Feb 14 09:20 logs
```

Compruebe si la información obtenida es similar a la mostrada en [Figura 5-5](#).

- En caso afirmativo, se han instalado los plug-in.
- En caso negativo, los plug-in no se han instalado. Luego, instálelos.

Paso 2 Descargue **CloudResetPwdAgent.zip** y verifique su integridad haciendo referencia a [Obtención del complemento de restablecimiento de contraseña de un solo clic \(Linux\)](#).

No hay ningún requisito especial para el directorio que almacena **CloudResetPwdAgent.zip**.

Paso 3 Ejecute el siguiente comando para descomprimir **CloudResetPwdAgent.zip**:

No hay ningún requisito especial para el directorio que almacena el **CloudResetPwdAgent.zip** descomprimido. Utilice cualquier directorio.

unzip -o -d Decompressed directory CloudResetPwdAgent.zip

Un ejemplo es el siguiente:

Si el plug-in se descomprime en **/home/linux/test**, ejecute el siguiente comando:

unzip -o -d /home/linux/test CloudResetPwdAgent.zip

Paso 4 Instale el complemento de restablecimiento de contraseña con un solo clic.

1. Ejecute el siguiente comando para abrir el archivo **CloudResetPwdAgent.Linux**:

cd CloudResetPwdAgent/CloudResetPwdAgent.Linux

2. Ejecute el siguiente comando para agregar el permiso de ejecución para el archivo **setup.sh**:

chmod +x setup.sh

3. Ejecute el siguiente comando para instalar el complemento:

sudo sh setup.sh

Si se muestra "cloudResetPwdAgent install successfully." y no se muestra "Failed to start service cloudResetPwdAgent", la instalación se realiza correctamente.

 **NOTA**

- También puede comprobar si el complemento se ha instalado utilizando los métodos proporcionados en [Paso 1](#).
- Si la instalación falla, compruebe si el entorno de instalación cumple con los requisitos e instale de nuevo el complemento.

Paso 5 Modifique el permiso de archivo del complemento de restablecimiento de contraseña.

```
chmod 640 /CloudrResetPwdAgent/logs/resetPwdAgent.log
chmod 640 /CloudrResetPwdAgent/logs/wrapper.log
chmod 700 /CloudrResetPwdAgent/bin/cloudResetPwdAgent.script
chmod 700 /CloudrResetPwdAgent/bin/wrapper
chmod 600 /CloudrResetPwdAgent/lib/commons-codec-1.14.jar
chmod 600 /CloudrResetPwdAgent/lib/libwrapper.so
chmod 600 /CloudrResetPwdAgent/lib/resetpwdagent.jar
chmod 600 /CloudrResetPwdAgent/lib/wrapper.jar
chmod 640 /CloudrResetPwdAgent/lib/json-20160810.jar
----Fin
```

5.6 Separación de discos de datos de un ECS

Escenarios

Si se conectan varios discos de datos al ECS utilizado para crear una imagen privada, es posible que los ECS creados a partir de la imagen no estén disponibles. Por lo tanto, debe separar todos los discos de datos del ECS antes de usarlo para crear una imagen privada.

Esta sección describe cómo separar todos los discos de datos de un ECS.

Prerrequisitos

Ha iniciado sesión en el ECS utilizado para crear una imagen privada de Linux.

Procedimiento

1. Compruebe si el ECS tiene discos de datos.
Ejecute el siguiente comando para comprobar el número de discos adjuntos al ECS:
fdisk -l
 - Si el número es mayor que 1, el ECS tiene discos de datos. Vaya a [2](#).
 - Si el número es igual a 1, no hay ningún disco de datos conectado al ECS. Vaya a [3](#).
2. Ejecute el siguiente comando para revisar los discos de datos conectados al ECS:
mount
 - Si la salida del comando no contiene ninguna información del disco EVS, no es necesario separar ningún disco de datos EVS.

```
/dev/vda1 on / type ext4 (rw,relatime,data=ordered)
```

- Si se muestra información similar a la siguiente, vaya a **3**:

```
/dev/vda1 on / type ext4 (rw,relatime,data=ordered)
```

```
/dev/vdb1 on /mnt/test type ext4 (rw,relatime,data=ordered)
```

3. Elimine la información de configuración en el archivo **fstab**.

- a. Ejecute el siguiente comando para editar el archivo **fstab**:

vi /etc/fstab

- b. Elimine la configuración del disco del archivo **fstab**.

El archivo **/etc/fstab** contiene información sobre los sistemas de archivos y los dispositivos de almacenamiento conectados automáticamente al ECS cuando se inicia el ECS. La configuración acerca de los discos de datos conectados automáticamente al ECS debe eliminarse, por ejemplo, la última línea que se muestra en la siguiente figura.

Figura 5-6 Configuración del disco EVS en el archivo **fstab**

```
[root@ecs-bf78 ~]# cat /etc/fstab
#
# /etc/fstab
# Created by anaconda on Wed Feb 27 06:58:16 2019
#
# Accessible filesystems, by reference, are maintained under '/dev/disk'
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info
#
UUID=4c2c090d-4228-49fc-9cbe-3920b3bf287c / ext4 defaults 1 1
UUID=9c29104b-31b8-4421-a207-102f86ec7ae5 /mnt/test ext4 defaults 1 1
```

4. Ejecute el siguiente comando para separar los discos de datos del ECS:

Ejecute el siguiente comando para separar los discos:

umount /dev/vdb1

5. Ejecute el siguiente comando para revisar los discos de datos conectados al ECS:

mount

Si la salida del comando no contiene información sobre los discos de datos, se han desconectado del ECS.

6 Gestión de permisos

6.1 Creación de un usuario y concesión de permisos

Escenarios

En esta sección se describe cómo utilizar **Identity and Access Management** (IAM) para implementar un control detallado a sus imágenes. Con IAM, usted puede:

- Crear los usuarios de IAM para empleados en base a la estructura organizativa de su empresa. Cada usuario de IAM tiene sus propias credenciales de identidad para acceder a las imágenes.
- Conceder solo los permisos necesarios para que los usuarios realicen una tarea específica.
- Confiar una cuenta o un servicio en la nube para realizar operaciones de mantenimiento eficientes y profesionales en sus imágenes.

Si su cuenta no necesita usuarios individuales de IAM para la gestión de permisos, puede omitir esta sección.

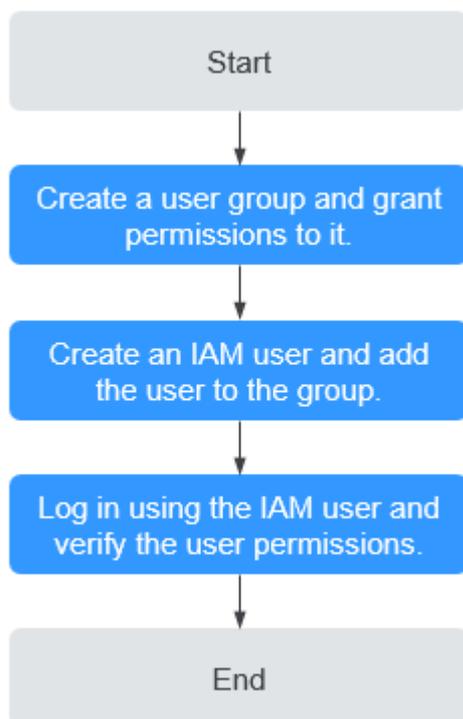
En esta sección se utiliza el permiso **IMS ReadOnlyAccess** como ejemplo para describir cómo conceder permisos a un usuario. **Figura 6-1** muestra el proceso.

Prerrequisitos

Obtenga información sobre los permisos (consulte **Permisos de IMS**) admitidos por IMS. Para ver los permisos del sistema de otros servicios, consulte **Permisos del sistema**.

Flujo de proceso

Figura 6-1 Proceso para la concesión de permisos IMS



1. **Crear un grupo de usuario y concederle permisos.**
Cree un grupo de usuarios en la consola de IAM y conceda el permiso de solo lectura al grupo asignando el permiso **IMS ReadOnlyAccess**.
2. **Crear un usuario de IAM y agregarlo al grupo de usuario.**
Cree un usuario en la consola de IAM y agregue el usuario al grupo creado en **1**.
3. **Iniciar sesión** y verificar permisos.
Inicie sesión en la consola de gestión con el usuario de IAM, cambie a una región en la que surtan efecto los permisos, y verifique los permisos (asumir que el usuario solo tiene el permiso **IMS ReadOnlyAccess**).
 - En **Service List**, elija **Image Management Service**. En la consola IMS, realice operaciones excepto consultar imágenes, como crear, modificar y eliminar una imagen.
Por ejemplo, haga clic en **Create Private Image** en la esquina superior derecha. Si se le solicitan permisos insuficientes, el permiso **IMS ReadOnlyAccess** tiene efecto.
 - Elija cualquier otro servicio de la **Service List**, como **Virtual Private Cloud**. Si aparece un mensaje que indica permisos insuficientes para acceder al servicio, el permiso **IMS ReadOnlyAccess** de IMS tiene efecto.

6.2 Creación de una política personalizada

Escenarios

Las políticas personalizadas se pueden crear como un suplemento a los permisos del sistema de IMS. Para ver las acciones admitidas por políticas personalizadas, consulte [Políticas de permisos y acciones admitidas](#).

Puede crear políticas personalizadas de cualquiera de las dos formas siguientes:

- Editor visual: Seleccione los servicios en la nube, acciones, recursos y condiciones de solicitud sin la necesidad de conocer la sintaxis de la política.
- JSON: Edite las políticas de JSON desde cero o basándose en una política existente.

Para obtener más información, consulte [Creación de una política personalizada](#). Esta sección proporciona ejemplos de políticas personalizadas de IMS comunes.

Políticas de ejemplo

- Ejemplo 1: Permitir a los usuarios crear imágenes

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ims:serverImages:create"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "KMS:*:*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "ecs:cloudServers:get",
        "ecs:servers:get",
        "ecs:serverVolumes:use",
        "ecs:cloudServers:list",
        "ecs:serverVolumeAttachments:list",
        "ecs:servers:list"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "bms:servers:list",
        "bms:servers:get",
        "bms:serverFlavors:get"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "evs:volumes:*"
      ]
    }
  ]
}
```

```
}
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "OBS:*:*"
      ]
    }
  ]
}
```

NOTA

La acción necesaria para crear una imagen es **ims:serverImages:create**. Otras son acciones dependientes para crear una imagen.

- **Ejemplo 2: Denegación de la eliminación de imágenes**

Una política de denegación debe usarse junto con otras políticas para que surtan efecto. Si las políticas asignadas a un usuario contienen acciones Allow y Deny, las acciones Deny tienen prioridad sobre las acciones Allow.

El siguiente método se puede utilizar si necesita asignar la política **FullAccess** de IMS a un usuario, pero también prohibir que el usuario elimine imágenes. Cree una política personalizada para denegar la eliminación de imágenes y asigne ambas políticas al grupo al que pertenece el usuario. Entonces, el usuario puede realizar todas las operaciones en IMS excepto la eliminación de imágenes. El siguiente se muestra un ejemplo de política de denegación:

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ims:images:delete"
      ]
    }
  ]
}
```