

Windows Server Template Tutorial 2008 R2~ 2019 (GuestTools)

Version: ZStack Cloud 4.3.12

Issue: V4.3.12

Copyright Statement

Copyright © 2022 Shanghai Yunzhou Information and Technology Ltd. All rights reserved.

Without prior written consent of Shanghai Yunzhou Information and Technology Ltd., any organization and any individual do not have the right to extract, copy any part of or all of, and are prohibited to disseminate the contents of this document in any manner.

Trademark

Shanghai Yunzhou Information and Technology Ltd. reserves all rights to its trademarks, including , but not limited to ZStack and other trademarks in connection with Shanghai Yunzhou Information and Technology Ltd.

Other trademarks or registered trademarks presented in this document are owned or controlled solely by its proprietaries.

Notice

The products, services, or features that you purchased are all subject to the commercial contract and terms of Shanghai Yunzhou Information and Technology Ltd., but any part or all of the foregoing displayed in this document may not be in the scope of your purchase or use. Unless there are additional conventions, Shanghai Yunzhou Information and Technology Ltd. will disclaim any statement or warranty, whether implicit or explicit, on the contents of this document.

In an event of product version upgrades or other reasons, the contents of this document will be irregularly updated and released. Unless there are additional conventions, this document, considered solely as a reference guide, will not make any warranty, whether implicit or explicit, on all the statements, information, or suggestions.

Contents

Copyright Statement.....	I
1 Overview.....	1
2 Environment Preparation.....	2
3 Template.....	3
3.1 Windows Template.....	3
3.1.1 Add an Image.....	3
3.1.2 Install an Operating System.....	5
3.1.3 Install GuestTools and other Software.....	10
3.1.4 Prepare the Operating System.....	16
3.1.5 Create a System Template.....	17
3.2 Windows VirtIO Template.....	19
3.2.1 Add an Image.....	19
3.2.2 Install an Operating System.....	23
3.2.3 Install GuestTools and other Software.....	30
3.2.4 Prepare the Operating System.....	36
3.2.5 Create a System Template.....	37
Glossary.....	40

1 Overview

A Windows template is a VM image where a Windows VM instance with installed necessary software such as drives and QGA removes and then regenerates its security identifier (SID, a unique identifier of a user, user group, or computer account). This template can be mainly used to create VM instances in bulk in a custom manner. This Tutorial supports the following versions:

- Windows version: Windows Server 2008 R2, Windows Server 2012 R2, Windows 7, Windows 10, Windows Server 2016, and Windows Server 2019.
- ZStack Cloud version: 3.7.1 or later.

2 Environment Preparation

To encapsulate a template, prepare the following software or tools:

- **ZStack Cloud:**

To obtain 3.7.1 or later versions, go to the [Official Website](#)

- **Windows image:**

Make sure that you obtain a Windows image from the Microsoft official website as needed, and ensure your compliance of relevant authorizations and permissions. This Tutorial references *cn_windows_server_2008_r2_standard_enterprise_datacenter_and_web_with_sp1_x64_dvd_617598.iso*.

- **Optional. USB 3.0 driver:**

USB 2.0 driver is native to Windows Server 2008 R2. Install USB 3.0 driver as needed. The driver path (64-bit) references http://cdn.zstack.io/tools/renesas_usb30_21390.exe .

3 Template

This Tutorial includes two types of encapsulation method: Windows and Windows VirtIO.

Encapsulation procedures for each method are different. Make sure that you perform relevant operations according to the corresponding method as follows:

- **Windows:** Add an image by using Windows platform type. Note that the template with the Windows method has two types of drive: IDE and VirtIO. For more information about how to encapsulate a template with the Windows method, see [Windows Template](#).
- **Windows VirtIO:** Add an image by using Windows VirtIO platform type. Note that the template with the Windows VirtIO method has only one type of drive: VirtIO. For more information about how to encapsulate a template with the Windows VirtIO method, see [Windows VirtIO Template](#).

3.1 Windows Template

To encapsulate a Windows template, follow these steps:

1. Add an image.
2. Install an operating system.
3. Install GuestTools and other software.
4. Prepare the operating system.
5. Create a system template.

The following details the whole process of how to encapsulate a Windows Server 2008 R2 template.

3.1.1 Add an Image

Add a Windows Server 2008 R2 image to ZStack Cloud. This image is used to install the operating system.

On the main menu of ZStack Cloud, choose **Resource Center > Resource Pool > Compute Configuration > Image**. On the **Image** page, click **Add Image**. Then, the **Add Image** page is displayed. On the **Add Image** page, set the following parameters:

- **Name:** Enter a name for the image.
- **Description:** Optional. Enter a description for the image.
- **Image Type:** Select an image type. Here, select system template.
- **Image Format:** Select an image format. Here, select iso.

- **CPU Architecture:** Select a CPU architecture for the image. VM instances created from the image use this CPU architecture.



Note:

If you select aarch64 or mips64, set the BIOS mode to UEFI.

- **Platform:** Select an image platform. Here, select **Windows**.
- **OS:** Select an operating system that is consistent with the image.
- **VirtIO:** Choose whether to enable VirtIO according to your actual operating system and platform.
- **Backup Storage:** Select a backup storage.
- **Image Path:** Specify an image URL or upload a local file.



Note:

- The URL can be either in the **HTTP/HTTPS/FTP/SFTP** format or the **file:///** format. Currently, the *file:///* format supports only ImageStorage backup storages.
- To upload a local file, make sure that this file can be accessed by your browser. ImageStore backup storages are supported.

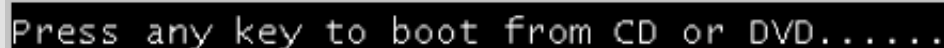
- **BIOS Mode:** Select a BIOS mode, including Legacy or UEFI. Default mode: Legacy.
 - Legacy: This mode supports all operating systems.
 - UEFI: This mode supports Windows 7, Windows Server 2008 R2, Windows 8, and their later versions. Note that the Compatibility Support Module (CSM) must be enabled for Windows 7 and Windows Server 2008 R2.



Note:

- For a Windows-based VM instance (such as Windows Server 2012 R2, Windows Server 2016, and Windows 10) booted by UEFI, the following page will be displayed after the VM instance starts. Press any key to continue the installation of the VM operating system. Otherwise, the VM instance will enter the UEFI Shell.

Figure 3-1: Press Any Key to Continue



If the VM instance already entered the UEFI Shell, you must run the following commands before you boot the operating system.

```
Shell> fs0:  
FS0:\> dir  
FS0:\> cd EFI  
FS0:\EFI\> cd BOOT  
FS0:\EFI\BOOT\> BOOTX64.EFI
```

After you perform the preceding operations, press any key to continue the VM operating system installation. Otherwise, the VM instance will enter the UEFI Shell again.

- **QEMU Guest Agent:** Choose whether the current image has installed QEMU Guest Agent (QGA). Here, leave this option alone.

Figure 3-2: Add Windows Image

< Add Image

Name *

Description

Image Type * System Image Volume Image

Image Format *

CPU Architecture *

Platform *

OS *

VirtIO ☒

Backup Storage * BS-1 x

Image Path * ☒ URL ☐ Local File

BIOS Mode *
⚠ Select the BIOS mode carefully. Mode mismatch may cause VM instances unable to work properly.

QEMU Guest Agent ☐ Installed QEMU Guest Agent

Cancel OK

3.1.2 Install an Operating System

Create a VM instance and install the operating system by using the Windows Server 2008 R2 image you added in the previous step.

Create a VM Instance

On the main menu of ZStack Cloud, choose **Resource Center > Resource Pool > Virtual Resource > VM Instance**. On the **VM Instance** page, click **Create VM Instance**. On the displayed, click on **Standard Creation**. Then, follow these steps to create a VM instance.

1. Complete the basic configurations.

Set the following parameters:

- **Name:** Enter a name for the VM instance.
- **Description:** Optional. Enter a description for the VM instance.
- **Quantity:** Enter the number of VM instances to be created. You can create VM instances in bulk.
- **Tag:** Optional. Bind one or more tags to the VM instance.
- Set the VM offering by using one of the following methods:
 - **Basic Offering:** Set the VM offering by selecting an existing instance offering and disk offering.
 - **Instance Offering:** Select an existing instance offering.
 - **Image:** Select an existing image.
 - **Data Volume:** Optional. Choose whether to create a data volume and attach it to the VM instance. Here, you do not need to create a data volume.
 - **Custom Offering:** Set the VM offering by customizing the following VM configurations:
 - **CPU:** Set the number of CPU cores of the VM instance.
 - **Memory:** Set the memory size of the VM instance.
 - **Image:** Select an existing image.
 - **Data Volume:** Optional. Choose whether to create a data volume and attach it to the VM instance. Here, you do not need to create a data volume.

2. Complete the resource configurations.

Set the following parameters:

- **Network Configurations:** Select an L3 network used by the VM instance and complete the network configurations.
- **Network:** Select an L3 network used by the VM instance. Supported network types: public network, flat network, and VPC network.

- **Make Default:** If you add multiple network configurations, set one of the networks as the default network.
- **Enable SR-IOV:** Optional. Choose whether to use SR-IOV to generate a VF NIC and pass it through to the VM instance.
- **Assign IP:** Optional. Choose whether to assign an IP address to the VM NIC.
- **MAC Address:** Optional. Choose whether to configure a MAC address for the VM instance.
- **Security Group:** Optional. Associate a security group with the VM instance.
- **Cluster:** Optional. Specify a cluster for the host on which the VM instance is to be started.
- **Storage Allocation Policy:** Specify how the Cloud allocates a primary storage.
- **Host:** Optional. Select the host on which the VM instance is to be started. If you specified a cluster, select a host from the cluster.
- **vDrive:** Optional. Add a virtual drive (vDrive) for the VM instance.
- **GPU:** Add a GPU device for the VM instance by specifying a GPU specification or device. The GPU device can be either a physical GPU (pGPU) or a virtual GPU (vGPU).
- **CPU Pinning:** Specify the association between the pCPU of the host and the vCPU of the VM instance. Then, the Cloud allocates a pCPU to the VM instance accordingly. This helps to improve the VM performance.

3. Complete the system configurations.

Set the following parameters:

- **SSH Login Mode:** Optional. Set the SSH login mode.
- **Hostname:** Set a hostname for the VM instance.
- **User Data:** Optional. Inject user-defined parameters or scripts to customize configurations for the VM instance or to accomplish specific tasks.
- **Console Password:** Set a console password for the VM instance.
- **Console Mode:** Set the console mode. Options: VNC, SPICE, and VNC+SPICE. Default: VNC.

4. Confirm the information.

View the information about the VM instance. You can edit the information by clicking the **Edit** icon.

On the **Preview** page, click **OK**. Then, the Windows Server 2008 VM instance is created. The operating system will automatically enter the BIOS mode.

Figure 3-3: Create VM Instance

The screenshot shows the 'Create VM Instance' wizard with the 'Standard Creation' tab selected. On the left, a sidebar lists the steps: 'Basic Configuration' (active), 'Resource Configurations', 'System Configurations', and 'Preview'. The main area contains the following fields and options:

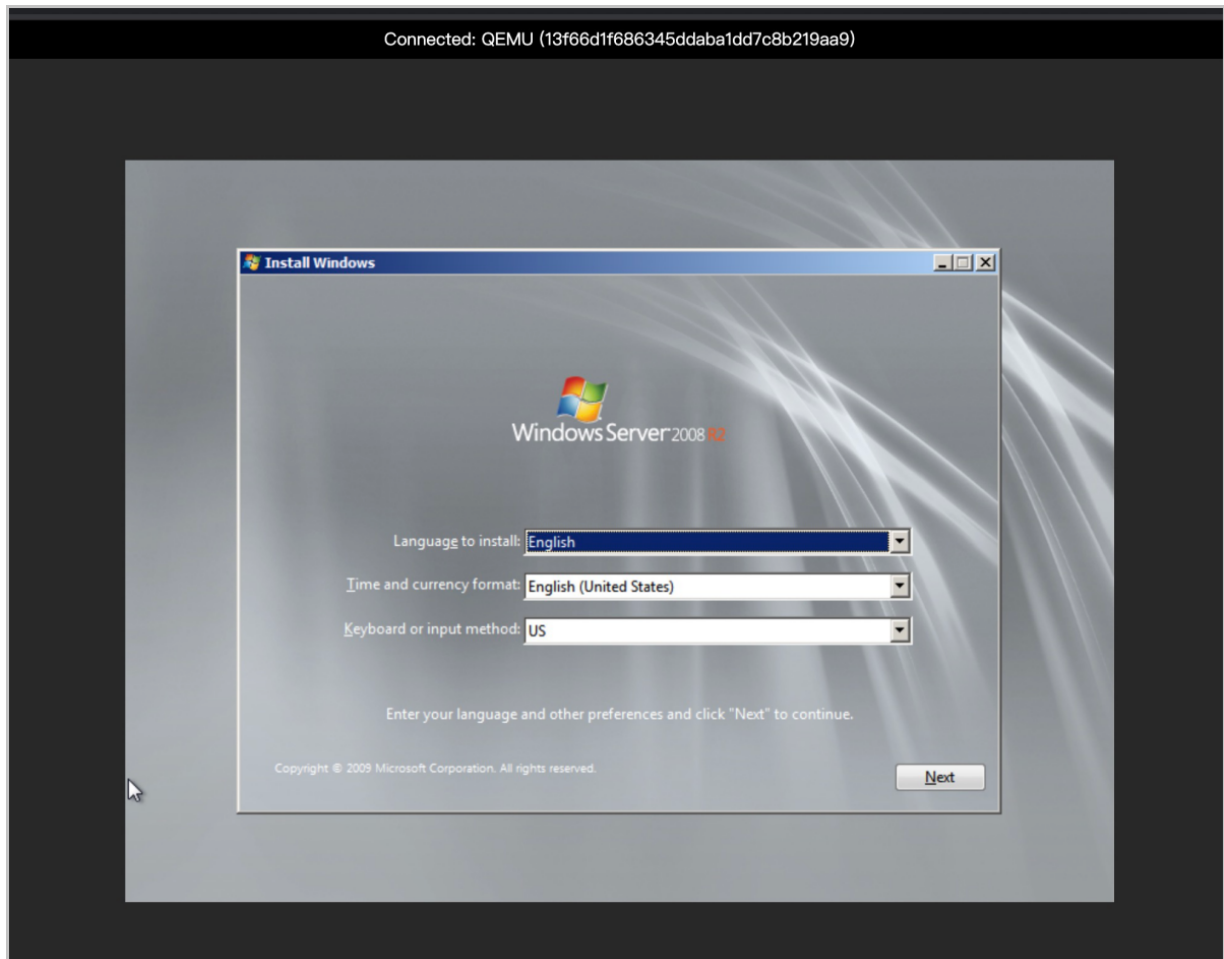
- Name ***: Text input field containing 'WindowsServer2008R2'.
- Description**: Text input field, currently empty, with a character count of '0/256'.
- Quantity ***: A numeric input field set to '1', with minus and plus buttons on either side. Below it, a note states: 'When you create VM instances in bulk, the names of these VM instances will be followed by -1, -2, -3 and so forth to distinguish these VM instances.'
- Tag**: A button labeled 'Attach Tag'.
- Basic Offering** / **Custom Offering**: Two tabs, with 'Basic Offering' selected.
- Instance Offering ***: A selection box showing '1-1 x 1 Core 1 GB Minimum Concurrently Running VMs'.
- Image ***: A selection box showing '08 x Windows Windows'.
- Data Volume**: A checkbox labeled 'Create'.
- > Advanced**: A link to expand advanced settings.

At the bottom right, there are two buttons: 'Cancel' and 'Next: Resource Configurations'.

Install the Operating System

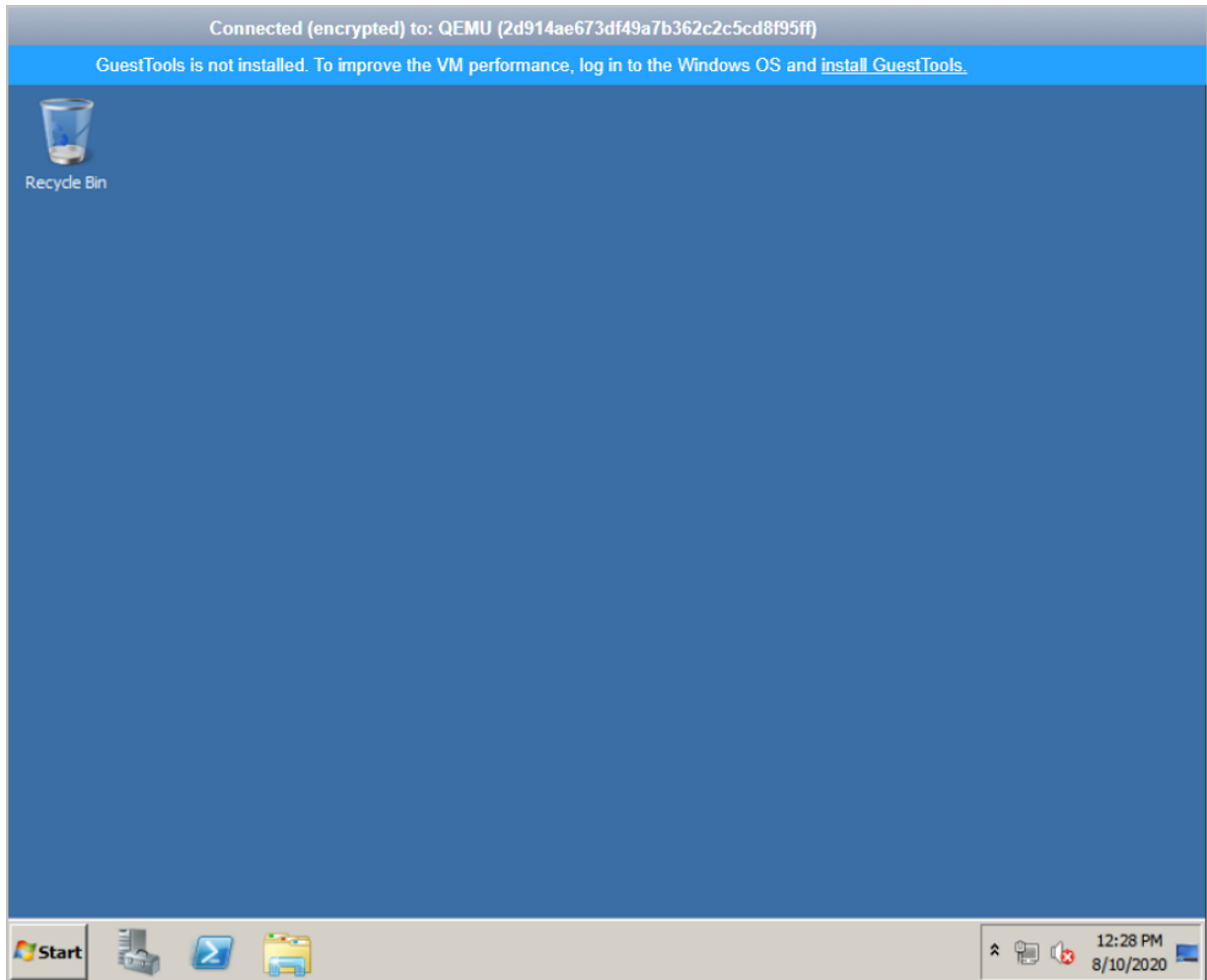
On the **VM Instance** page, select the VM instance you created before, and launch the VM console. Then, the installation page appears.

Figure 3-4: Install Operating System



Complete the configurations by referencing to the common installation process of Windows Server 2008 R2. During the installation, the operating system will be automatically rebooted, due to which the console might be disconnected. In that case, launch the console again. After you complete installing the operating system, set the admin password and log in to the operating system. So far, the Windows operating system is installed.

Figure 3-5: Complete Installing Operating System



Prevent Disk from Being Offline

If the server is abnormally shut down, disks on the VM instance might be offline after the VM instance reboots. To prevent this, after you complete installing the Windows operating system, go to **Command Prompt** as an Administrator, and run the following commands successively.

```
C:\Users\Administrator> diskpart ::Enter diskpart.  
DISKPART> san ::View the SAN policy.  
DISKPART> san policy=onlineall ::Change the SAN policy by using  
diskpart.  
DISKPART> exit
```

3.1.3 Install GuestTools and other Software

GuestTools is a performance optimization tool used by ZStack Cloud to improve the performance of Windows VM instances. The following table lists the tools and drivers contained in GuestTools.

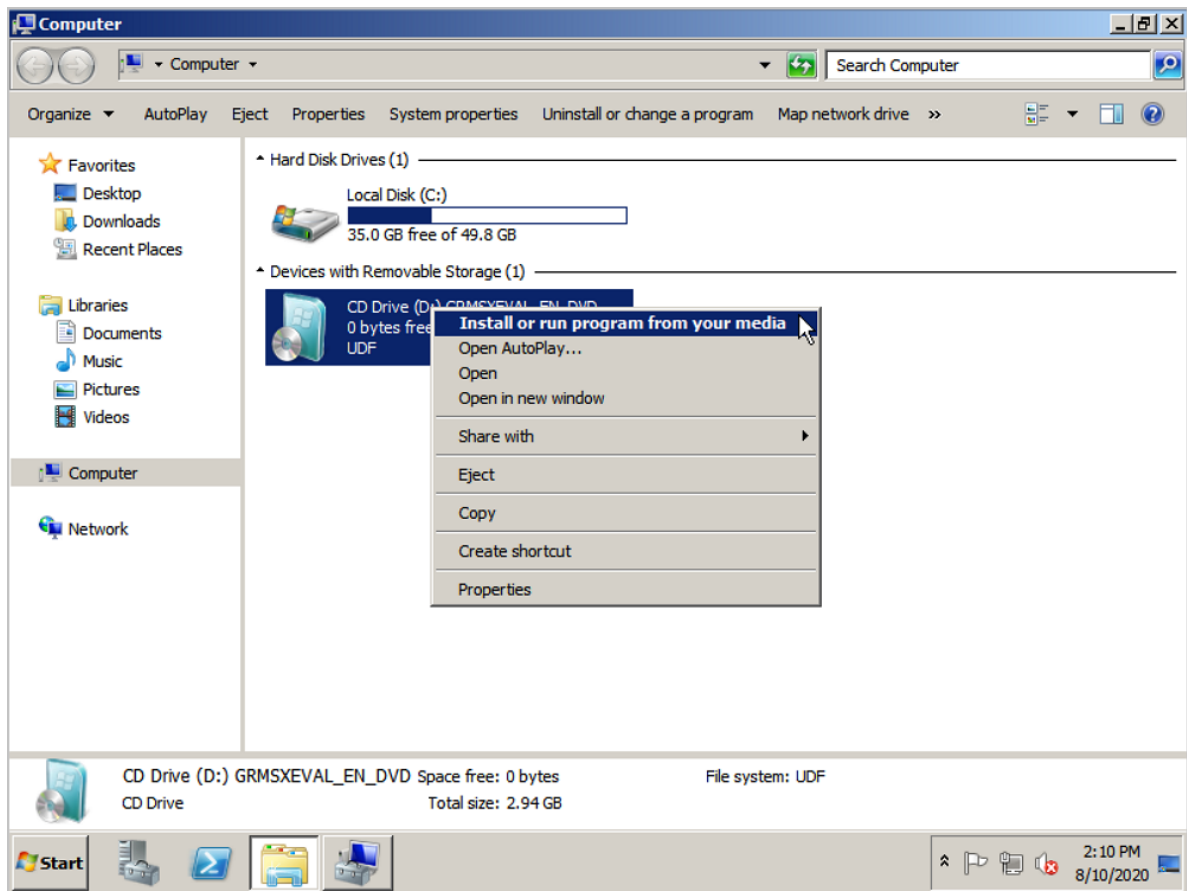
Type	Name	Functionality
VirtIO driver	SCSI controller	Storage controllers of the VirtIO type can effectively improve the disk performance of a VM instance in a virtualization environment.
	PCI simple communications controller	After you install a PCI simple communications controller, a Windows VM instance can communicate with the underlying KVM virtualization.
	PCI device	After you install a PCI device and enable its internal monitoring, Windows will support the balloon memory scaling.
	Ethernet adapter	A VirtIO Ethernet adapter can effectively improve the network performance of a VM instance in a virtualization environment.
Commonly-used tools	QEMU Guest Agent (QGA)	QGA is an application where mutual interactions between a host and a VM instance can be achieved. These interactions do not rely on networks, thereby greatly improving the VM performance and functionality. QGA helps check the state of GuestTools and VirtIO drivers in a VM instance. After QGA is installed, the VM instance enables you to change its password online.
	Cloudbase-Init	The VM instance that has Cloudbase-Init installed enables you to import User Data and achieve other custom functionalities.
	Agent internal monitoring	After an agent is installed, you can check the internal monitoring data of a VM instance.

Install GuestTools

1. Load the GuestTools image.

After you complete installing the operating system, enter the console page of the VM instance, and click **Install GuestTools** in the GuestTools installation prompt. Then, the operating system automatically loads the GuestTools image to the virtual CD Drive. To check this operation, go to the **Computer** page.

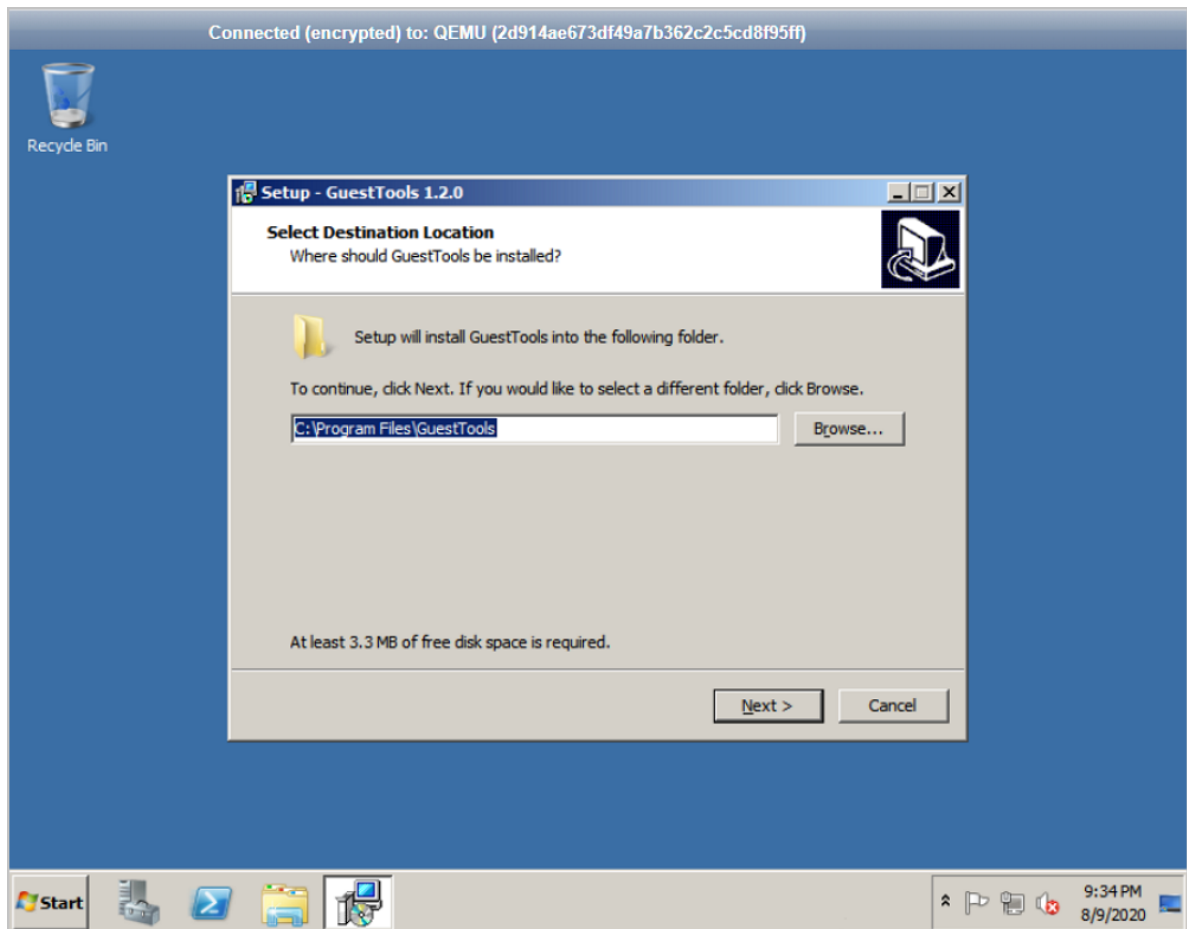
Figure 3-6: Load GuestTools Image

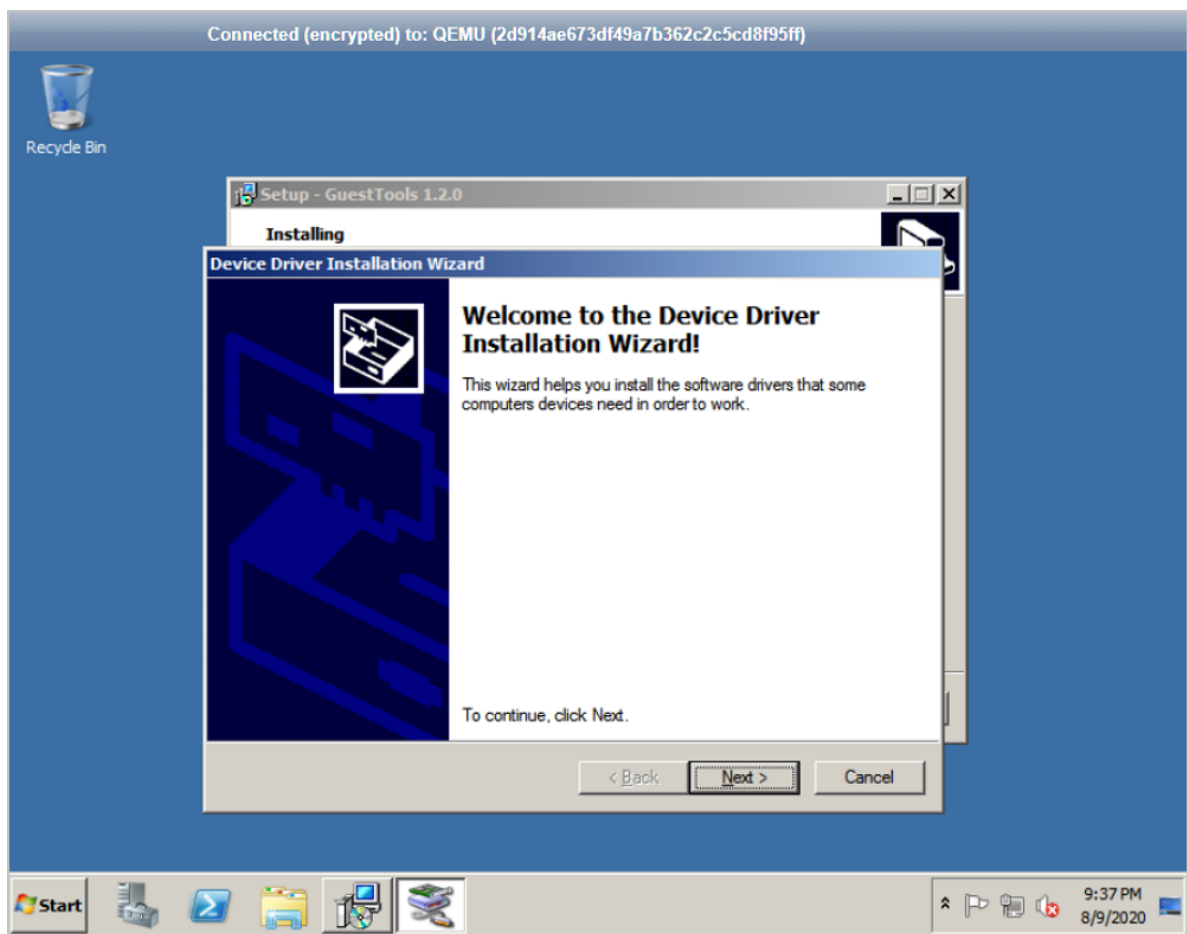


2. Install GuestTools and VirtIO driver.

Right-click the GuestTools CD Drive, select **Install or run program from your media** or double-click the GuestTools installation program. By following the displayed setup installation wizard, install GuestTools, commonly-used tools, and VirtIO drivers, successively.

Figure 3-7: Install GuestTools

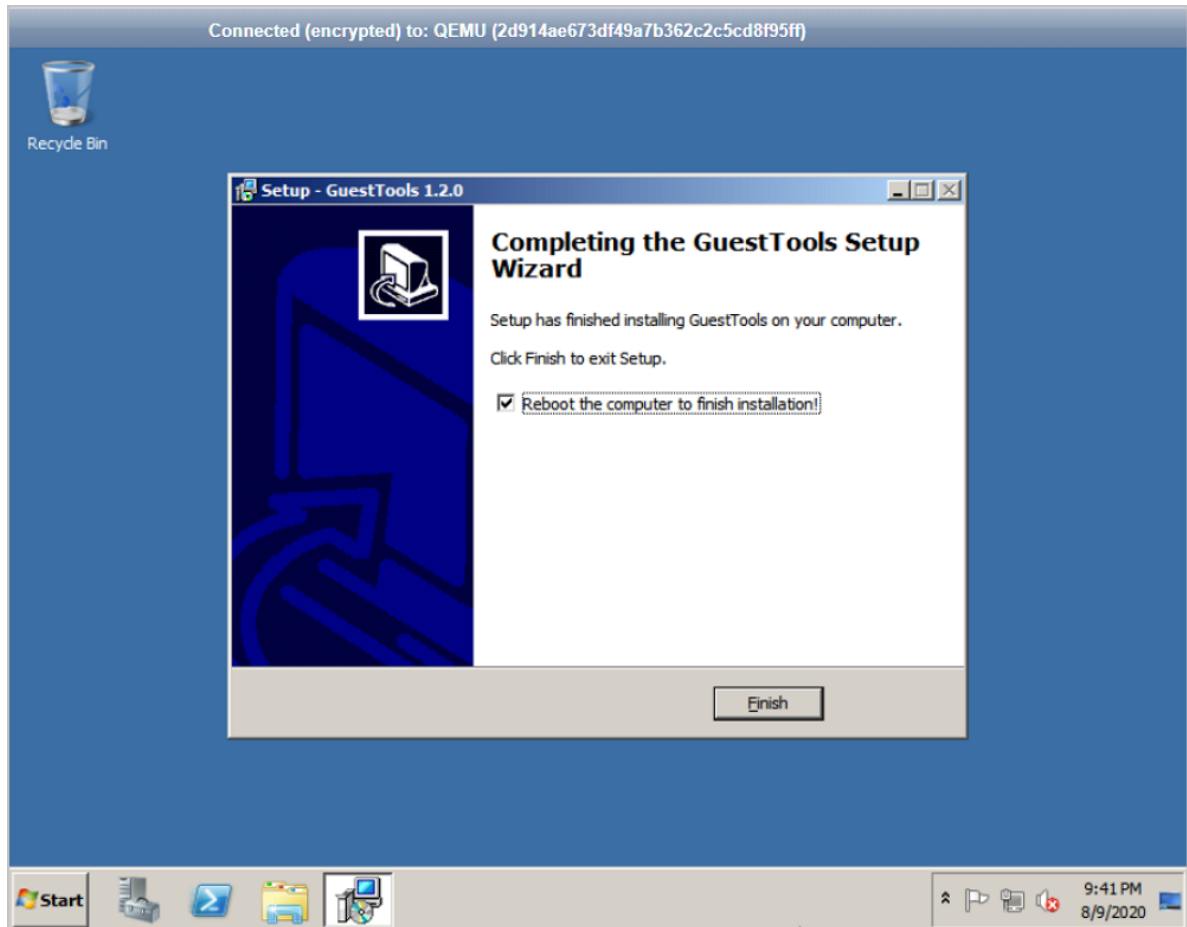




3. Confirm the installation and reboot your computer.

After you complete installing GuestTools, click **Finish** in the displayed dialog box. Make sure that you complete the installation and reboot the computer to make all configurations take effect.

Figure 3-8: Complete the Installation and Reboot Your Computer



After the operating system reboots, the platform of the VM instance is automatically changed to **WindowsVirtio**, and QGA is enabled.

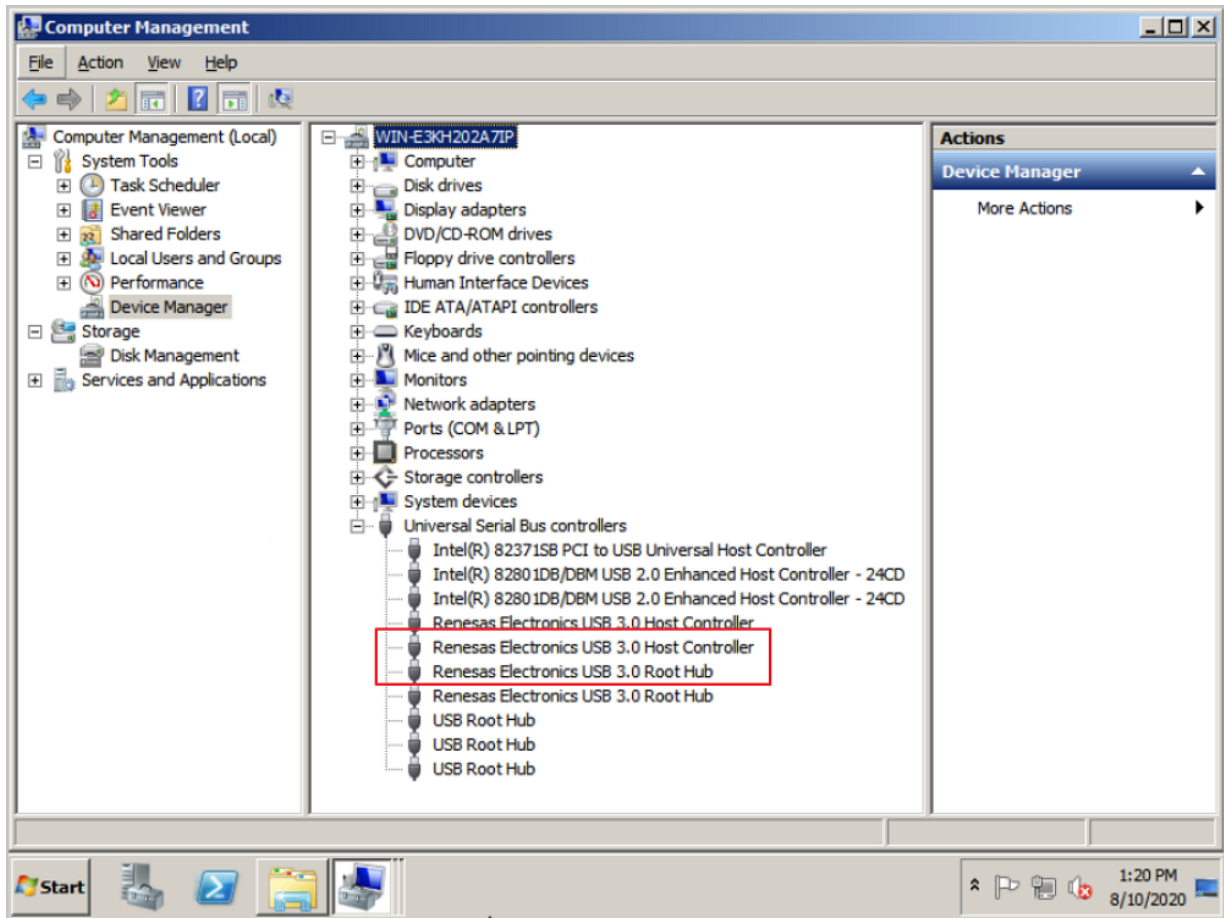
(Optional) Install other Software

You can install other software as needed in addition to the tools or drivers included in GuestTools.

For example, USB 2.0 driver is native to Windows Server 2008 R2. You can install the USB 3.0 driver as needed. Then, you can use the USB passthrough functionality.

You can obtain the driver file from https://cdn.zstack.io/tools/renesas_usb30_21390.exe , and double click the file to install the USB 3.0 driver.

Figure 3-9: Install USB 3.0 Driver



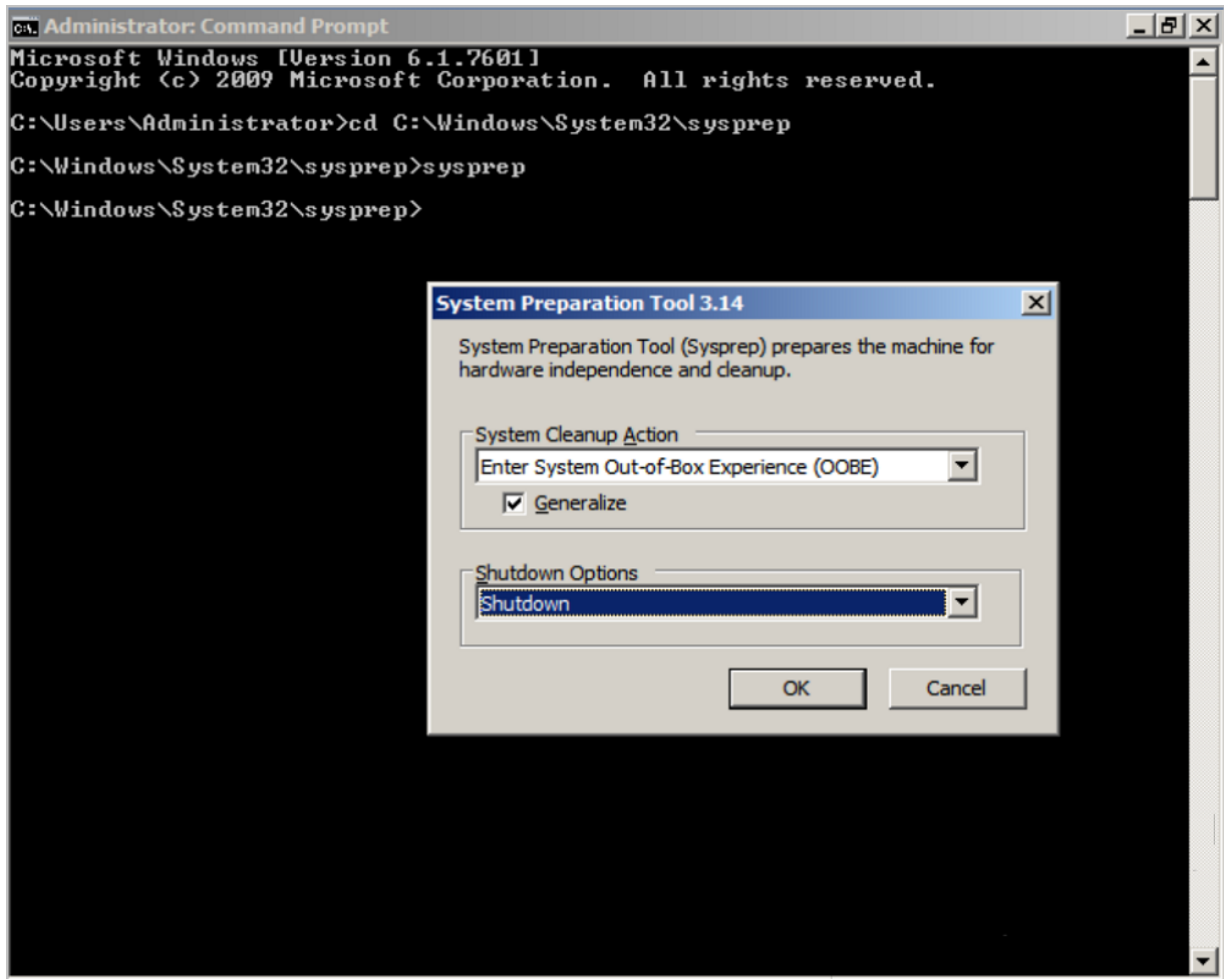
3.1.4 Prepare the Operating System

Operating system preparation is designed for generalizing and removing system-specific information such as hardware of a computer via Windows-native System Preparation Tool (Sysprep). To prepare the operating system, follow these steps:

1. Open the CMD command line by using the administrator permission.
2. Go to the `C:\Windows\System32\sysprep` directory and run the Sysprep tool.
3. Configure preparation policies and perform relevant operations. You can complete this step by setting the following parameters:
 - **System Cleanup Action:** Select **Enter System Out-of-Box Experience (OOBE)**.
 - **Generalize:** Select this checkbox. Then, the VM operating system created from the template has a unique security identity (SID).
 - **Shutdown Options:** Select **Shutdown**.

Click **OK**. Then, the system preparation begins.

Figure 3-10: System Preparation



3.1.5 Create a System Template

After you create the operating system template successfully, you can create VM instances in bulk in a custom manner by using this image. Also, you can export this image to create VM instances in other cloud platforms.

Create a VM Image

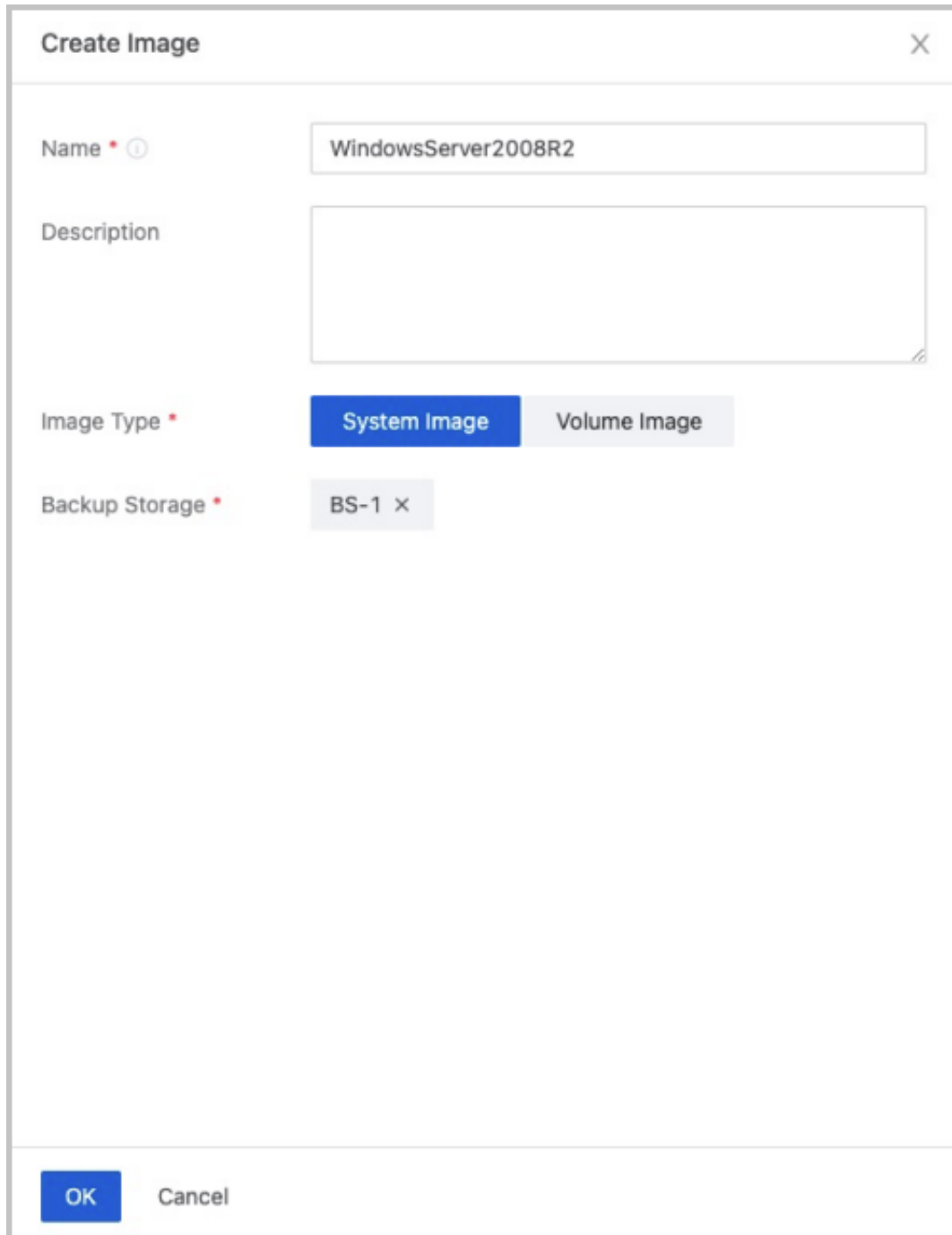
On the **VM Instance** page, select the target VM instance and create an image for the VM instance.

On the **Create Image** page, set the following parameters:

- **Name:** Enter a name for the image.
- **Description:** Optional. Enter a description for the image.
- **Image Type:** Select system image.
- **Backup Storage:** Select an existing backup storage.

Click **OK**. Then, the image is created.

Figure 3-11: Create Image



Create Image [X]

Name * ⓘ WindowsServer2008R2

Description

Image Type * **System Image** Volume Image

Backup Storage * BS-1 ×

OK Cancel



Note:

If your backup storage is ImageStore or Ceph, you can create an image for a VM instance when it is in the running state. For other types of backup storage, you need to stop the VM instance before you can create an image.

Export the Image

Exported images can be used directly by other cloud platforms to create VM instances. The export method varies based on the backup storage type.

- **ImageStore backup storages**

On the **Image** page, click **Actions > Export Image**. Then, an image is exported.

After the image is generated, you can download the exported image by copying the image URL on the **Overview** tab page of the image details page.

- **Ceph backup storages**

On the **Overview** tab page of the created image, copying **Backup Storage Path** will prompt you for the corresponding information such as pool and image in the Ceph backup storage.

After you copy this image path, you can export the Ceph image by running **rbd** on the Ceph backup storage. Assume that the storage path of the Ceph backup storage is *ceph#//bak-t-c9923f982/61ece0adc72*, run the following command:

```
[root@ceph-node1 ~]#rbd export bak-t-c9923f982/61ece0adc72 /root/
export-test.image
#bak-t-c9923f982 is the pool name where the image belongs.
#61ece0adc72 is the image name.
#/root/export-test.image is the name of the exported target file .
```

3.2 Windows VirtIO Template

To encapsulate a Windows VirtIO template, follow these steps:

1. Add an image.
2. Install an operating system.
3. Install GuestTools and other software.
4. Prepare the operating system.
5. Create a system template.

The following details the whole process of how to encapsulate a Windows Server 2008 R2 template.

3.2.1 Add an Image

Add a Windows Server 2008 R2 image and a VirtIO drive image to ZStack Cloud. These two images are used to install the operating system.

Add a Windows Image

On the main menu of ZStack Cloud, choose **Resource Center > Resource Pool > Compute Configuration > Image**. On the **Image** page, click **Add Image**. Then, the **Add Image** page is displayed.

On the **Add Image** page, set the following parameters:

- **Name:** Enter a name for the image.
- **Description:** Optional. Enter a description for the image.
- **Image Type:** Select an image type. Here, select system template.
- **Image Format:** Select an image format. Here, select iso.
- **CPU Architecture:** Select a CPU architecture. Here, select x86_64.
- **Platform:** Select the platform for the image. Here, select **Windows**.
- **OS:** Select Windows.
- **VirtIO:** Enable VirtIO.
- **Backup Storage:** Select an existing backup storage.
- **Image Path:** Specify an image URL or upload a local file.



Note:


- The URL can be either in the **HTTP/HTTPS/FTP/SFTP** format or the **file:///** format. Currently, the *file:///* format supports only ImageStorage backup storages.
 - To upload a local file, make sure that this file can be accessed by your browser. ImageStore backup storages are supported.
- **BIOS Mode:** Select a BIOS mode, including Legacy or UEFI. Default mode: Legacy.
 - Legacy: This mode supports all operating systems.
 - UEFI: This mode supports Windows 7, Windows Server 2008 R2, Windows 8, and their later versions. Note that the Compatibility Support Module (CSM) must be enabled for Windows 7 and Windows Server 2008 R2.



Note:

- For a Windows-based VM instance (such as Windows Server 2012 R2, Windows Server 2016, and Windows 10) booted by UEFI, the following page will be displayed after the VM instance starts. Press any key to continue the installation of the VM operating system. Otherwise, the VM instance will enter the UEFI Shell.

Figure 3-12: Press Any Key to Continue



Press any key to boot from CD or DVD.....

If the VM instance already entered the UEFI Shell, you must run the following commands before you boot the operating system.

```
Shell> fs0:
FS0:\> dir
FS0:\> cd EFI
FS0:\EFI\> cd BOOT
FS0:\EFI\BOOT\> BOOTX64.EFI
```

After you perform the preceding operations, press any key to continue the VM operating system installation. Otherwise, the VM instance will enter the UEFI Shell again.

- **QEMU Guest Agent:** Choose whether the current image has installed QEMU Guest Agent (QGA). Here, leave this option alone.
- **Support Elastic Baremetal Instance:** Choose whether to support elastic baremetal instance. Here, leave this option alone.

Figure 3-13: Add Windows Image

The 'Add Image' dialog box is shown with the following configuration:

- Name:** WindowsServer2008R2
- Description:** (Empty text box, 0/256 characters)
- Image Type:** System Image (selected), Volume Image
- Image Format:** iso
- CPU Architecture:** x86_64
- Platform:** Windows
- OS:** Windows (selected in both dropdowns)
- VirtIO:** ☒ (checked)
- Backup Storage:** BS-1
- Image Path:** ☒ URL, ☐ Local File. URL: http://www.microsoft.com/en-us/windows-ser
- BIOS Mode:** Legacy. A warning message states: 'Select the BIOS mode carefully. Mode mismatch may cause VM instances unable to work properly.'
- QEMU Guest Agent:** ☐ Installed QEMU Guest Agent

Buttons at the bottom right: Cancel, OK.

Add a VirtIO Image

On the **Image** page, click **Add Image**. On the displayed **Add Image** page, set the following parameters:

- **Name:** Enter a name for the image.
- **Description:** Optional. Enter a description for the image.
- **Image Type:** Select an image type. Here, select system template.
- **Image Format:** Select an image format. Here, select iso.
- **Platform:** Select the platform for the image. Here, select **Other**.
- **Backup Storage:** Select an existing backup storage.
- **Image Path:** Specify an image URL or upload a local file.



Note:

ZStack Cloud provides built-in VirtIO drive images. You can obtain different versions of images from the following paths:

- C74: `file:///opt/zstack-dvd/x86_64/c74/zstack-windows-virtio-driver.iso`
 - C76: `file:///opt/zstack-dvd/x86_64/c76/zstack-windows-virtio-driver.iso`
- **BIOS Mode:** Select a BIOS mode. The BIOS mode does not affect the image.
 - **QEMU Guest Agent:** Choose whether the current image has installed QEMU Guest Agent (QGA). Here, leave this option alone.
 - **Support Elastic Baremetal Instance:** Choose whether to support elastic baremetal instance. Here, leave this option alone.

Figure 3-14: Add VirtIO Image

The screenshot shows the 'Add Image' dialog box with the following configuration:

- Name:** VirtIO
- Description:** (empty)
- Image Type:** System Image (selected), Volume Image
- Image Format:** iso
- CPU Architecture:** x86_64
- Platform:** Other
- OS:** Other
- VirtIO:** ☒
- Backup Storage:** BS-1
- Image Path:** ☒ URL, ☐ Local File
file:///opt/zstack-dvd/x86_64/c74/zstack-winc
- BIOS Mode:** Legacy
⚠ Select the BIOS mode carefully. Mode mismatch may cause VM instances unable to work properly.
- QEMU Guest Agent:** ☐ Installed QEMU Guest Agent

Buttons: Cancel, OK

3.2.2 Install an Operating System

Create a VM instance and install an operating system by using the Windows Server 2008 R2 image you added before.

Create a VM Instance

On the main menu of ZStack Cloud, choose **Resource Center > Resource Pool > Virtual Resource > VM Instance**. On the **VM Instance** page, click **Create VM Instance**. On the displayed, click on **Standard Creation**. Then, follow these steps to create a VM instance.

On the main menu of ZStack Cloud, choose **Resource Center > Resource Pool > Virtual Resource > VM Instance**. On the **VM Instance** page, click **Create VM Instance**. On the displayed, click on **Standard Creation**. Then, follow these steps to create a VM instance.

1. Complete the basic configurations.

Set the following parameters:

- **Name:** Enter a name for the VM instance.
- **Description:** Optional. Enter a description for the VM instance.
- **Quantity:** Enter the number of VM instances to be created. You can create VM instances in bulk.
- **Tag:** Optional. Bind one or more tags to the VM instance.
- Set the VM offering by using one of the following methods:
 - **Basic Offering:** Set the VM offering by selecting an existing instance offering and disk offering.
 - **Instance Offering:** Select an existing instance offering.
 - **Image:** Select the **WindowsVirtio** image you added before.
 - **Data Volume:** Optional. Choose whether to create a data volume and attach it to the VM instance. Here, you do not need to create a data volume.
 - **Custom Offering:** Set the VM offering by customizing the following VM configurations:
 - **CPU:** Set the number of CPU cores of the VM instance.
 - **Memory:** Set the memory size of the VM instance.
 - **Image:** Select an existing image.
 - **Data Volume:** Optional. Choose whether to create a data volume and attach it to the VM instance. Here, you do not need to create a data volume.

2. Complete the resource configurations.

Set the following parameters:

- **Network Configurations:** Select an L3 network used by the VM instance and complete the network configurations.

- **Network:** Select an L3 network used by the VM instance. Supported network types: public network, flat network, and VPC network.
- **Make Default:** If you add multiple network configurations, set one of the networks as the default network.
- **Enable SR-IOV:** Optional. Choose whether to use SR-IOV to generate a VF NIC and pass it through to the VM instance.
- **Assign IP:** Optional. Choose whether to assign an IP address to the VM NIC.
- **MAC Address:** Optional. Choose whether to configure a MAC address for the VM instance.
- **Security Group:** Optional. Associate a security group with the VM instance.
- **Cluster:** Optional. Specify a cluster for the host on which the VM instance is to be started.
- **Storage Allocation Policy:** Specify how the Cloud allocates a primary storage.
- **Host:** Optional. Select the host on which the VM instance is to be started. If you specified a cluster, select a host from the cluster.
- **vDrive:** Optional. Add a virtual drive (vDrive) for the VM instance.
- **GPU:** Add a GPU device for the VM instance by specifying a GPU specification or device. The GPU device can be either a physical GPU (pGPU) or a virtual GPU (vGPU).
- **CPU Pinning:** Specify the association between the pCPU of the host and the vCPU of the VM instance. Then, the Cloud allocates a pCPU to the VM instance accordingly. This helps to improve the VM performance.

3. Complete the system configurations.

Set the following parameters:

- **SSH Login Mode:** Optional. Set the SSH login mode.
- **Hostname:** Set a hostname for the VM instance.
- **User Data:** Optional. Inject user-defined parameters or scripts to customize configurations for the VM instance or to accomplish specific tasks.
- **Console Password:** Set a console password for the VM instance.
- **Console Mode:** Set the console mode. Options: VNC, SPICE, and VNC+SPICE. Default: VNC.

4. Confirm the information.

View the information about the VM instance. You can edit the information by clicking the **Edit** icon.

On the **Preview** page, click **OK**. Then, the Windows Server 2008 VM instance is created. The operating system will automatically enter the BIOS mode.

Figure 3-15: Create VM Instance

The screenshot shows the 'Create VM Instance' dialog box with the 'Standard Creation' tab selected. On the left, a sidebar lists 'Basic Configuration', 'Resource Configurations', 'System Configurations', and 'Preview'. The 'Basic Configuration' section is active and contains the following fields:

- Name ***: WindowsServer2008R2
- Description**: (empty text box, 0/256 characters)
- Quantity ***: 1 (with minus and plus buttons)
- Tag**: Attach Tag

Below these fields, a note states: 'When you create VM instances in bulk, the names of these VM instances will be followed by -1, -2, -3 and so forth to distinguish these VM instances.'

The 'Basic Offering' section is also visible, showing:

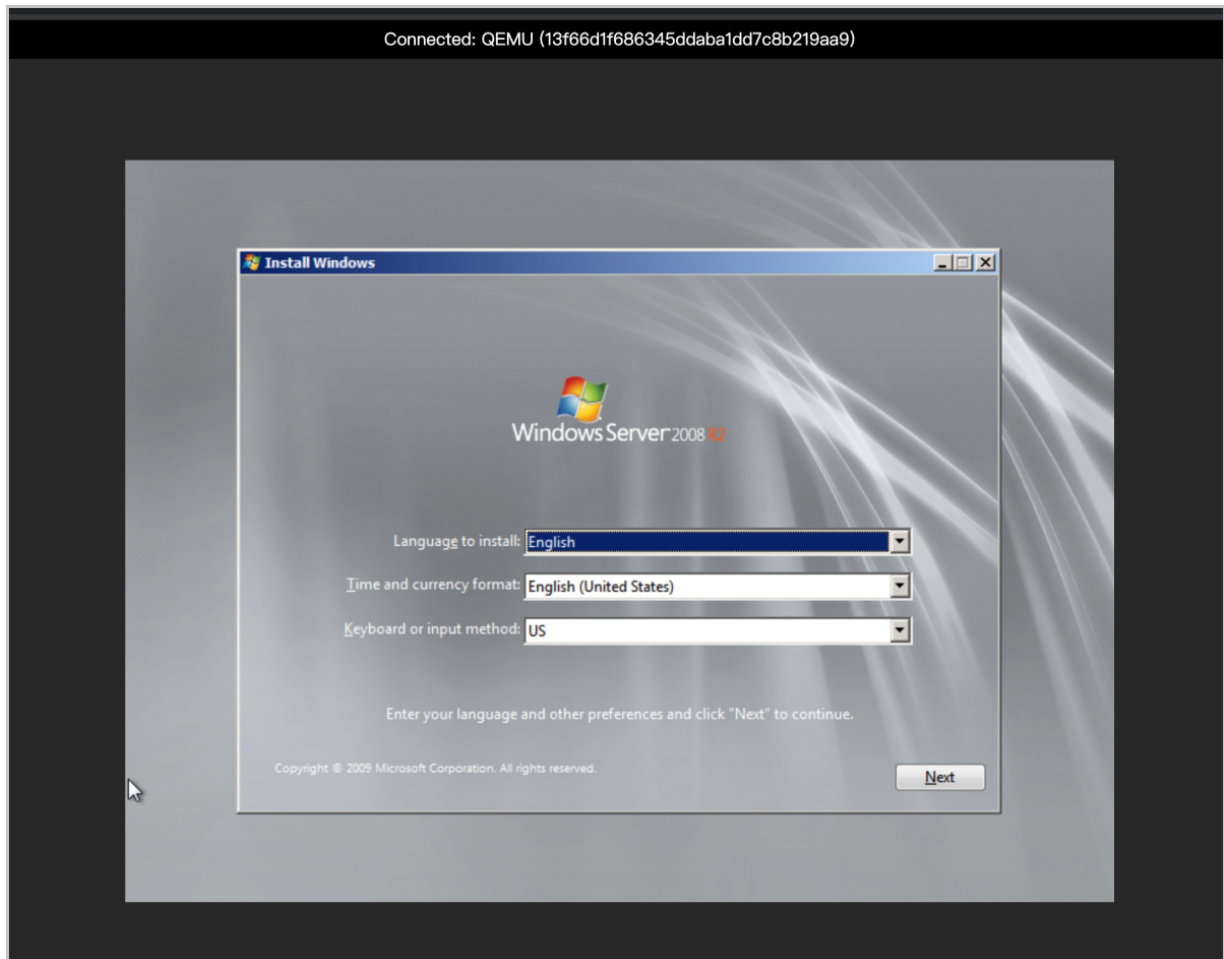
- Instance Offering ***: 1-1 x 1 Core | 1 GB | Minimum Concurrently Running VMs
- Image ***: 08 x Windows | Windows
- Data Volume**: ☐ Create

A '> Advanced' link is located at the bottom of the configuration section. At the bottom right of the dialog, there are 'Cancel' and 'Next: Resource Configurations' buttons.

Install the Operating System

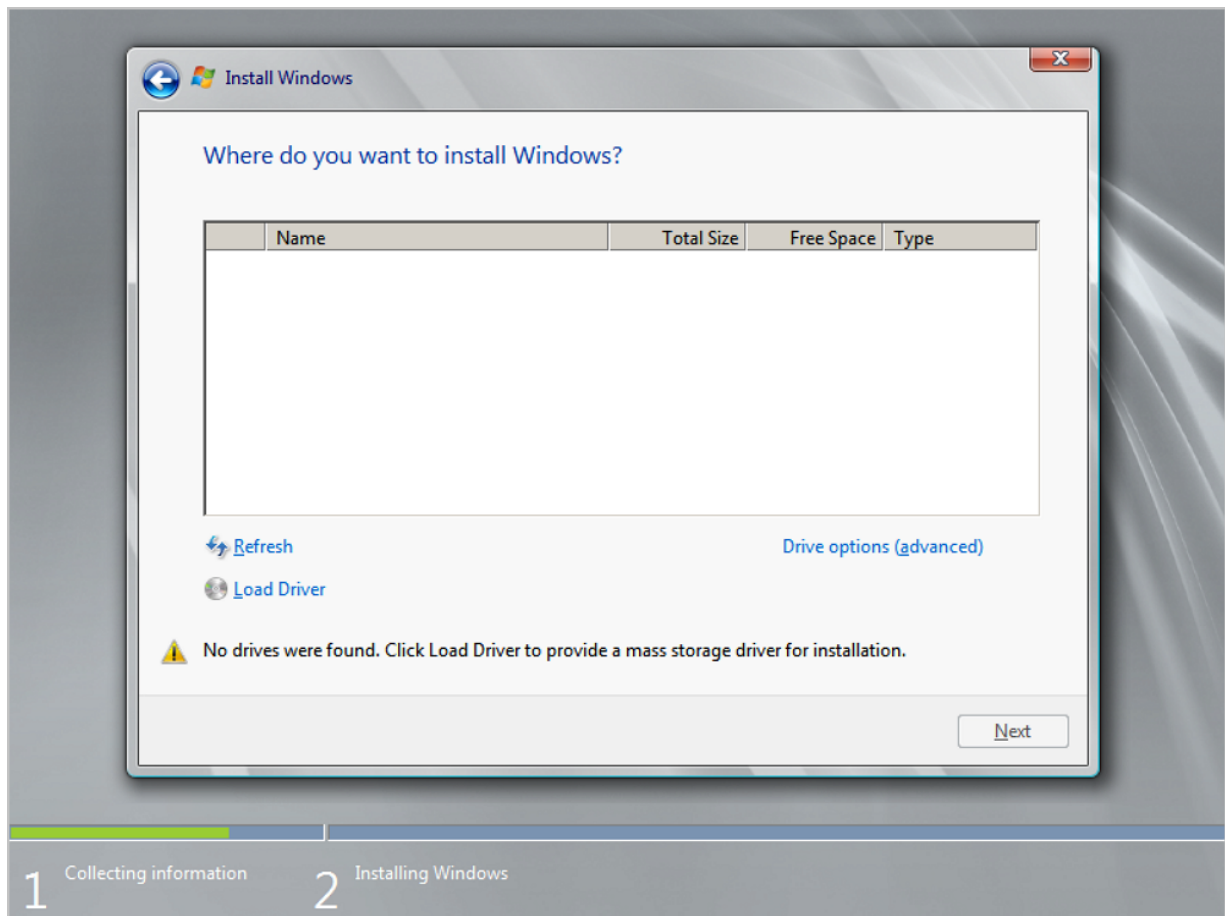
On the **VM Instance** page, select the VM instance you created before, and launch the VM console. Then, the installation page appears.

Figure 3-16: Install Operating System



To configure your own operating system, reference to the normal Windows Server 2008 R2. When you select the installation path during installation, you will prompt for **No drives were found.**, as shown in [No Drives Were Found](#).

Figure 3-17: No Drives Were Found

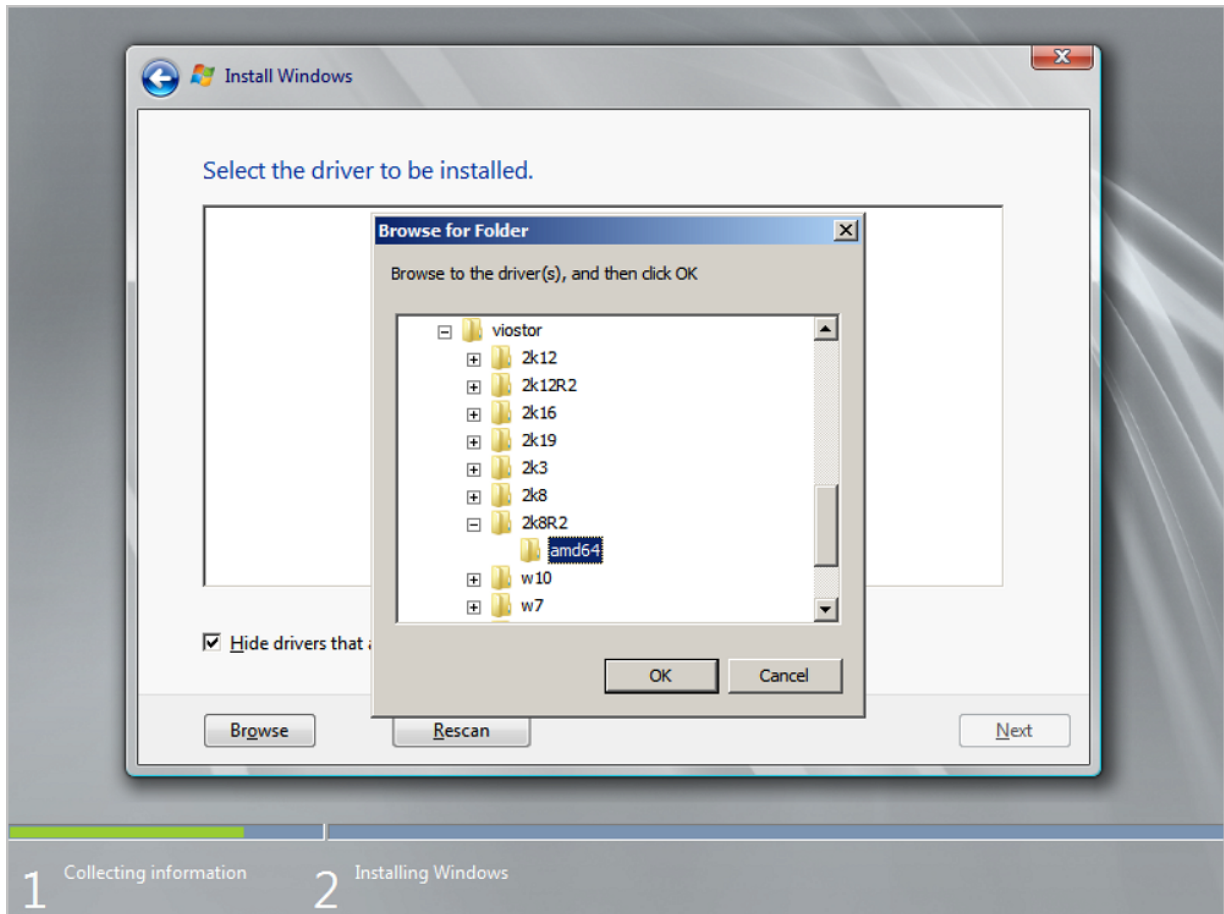


At this time, to continue the installation, install a disk drive. Choose **Load Driver** > **Browse**.

According to the operating system, select the disk drive in the VirtIO driver image, and click **OK** > **Next** to complete loading the disk drive.

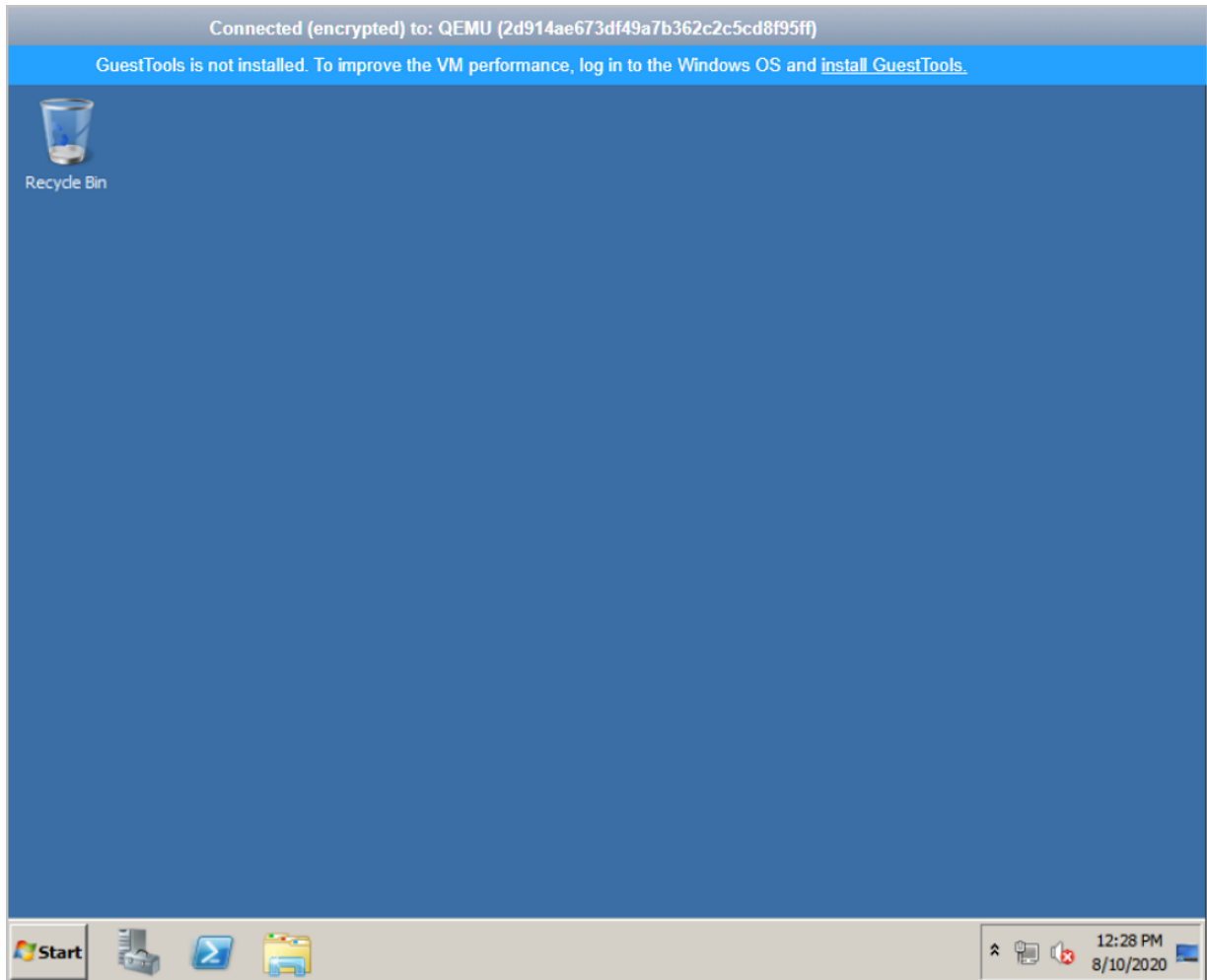
- For the 64-bit operating system, the path of the disk drive is `viostor*\amd64`.
- For the 32-bit operating system, the path of the disk drive is `viostor*\x86`.

Figure 3-18: Load Disk Drive



After you load the disk drive, select a system installation path and click **Next** to continue the preceding installation process. During installation, the operating system will automatically reboot, which may lead to disconnection of the console. In that case, re-enter the operating system. After you complete installing the operating system, customize the admin password and log in to the operating system. So far, the Windows operating system is installed.

Figure 3-19: Complete Installing Operating System



Prevent Disk from Being Offline

If the server is abnormally shut down, disks on the VM instance might be offline after the VM instance reboots. To prevent this, after you complete installing the Windows operating system, go to **Command Prompt** as an Administrator, and run the following commands successively.

```
C:\Users\Administrator> diskpart ::Enter diskpart.  
DISKPART> san ::View the SAN policy.  
DISKPART> san policy=onlineall ::Change the SAN policy by using  
diskpart.  
DISKPART> exit
```

3.2.3 Install GuestTools and other Software

GuestTools is a performance optimization tool used by ZStack Cloud to improve the performance of Windows VM instances. The following table lists the tools and drivers contained in GuestTools.

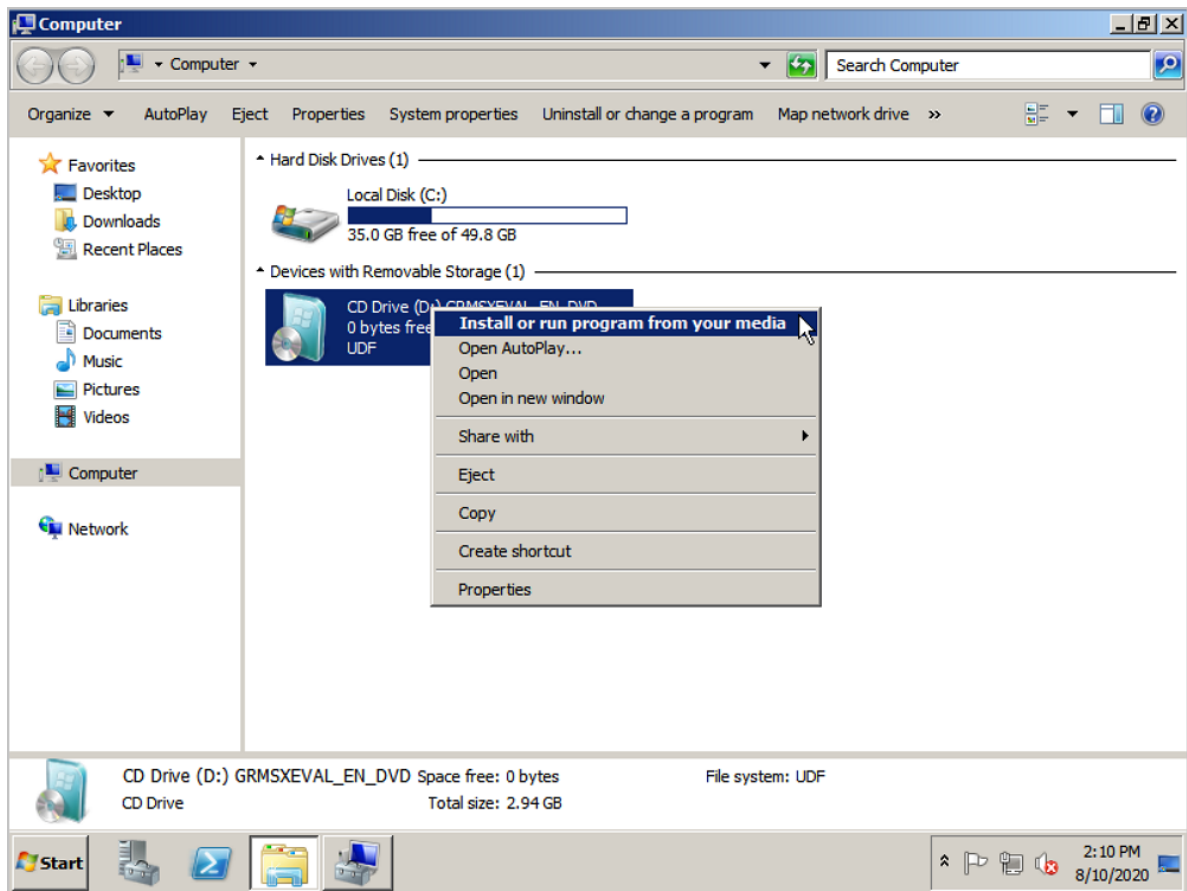
Type	Name	Functionality
VirtIO driver	SCSI controller	Storage controllers of the VirtIO type can effectively improve the disk performance of a VM instance in a virtualization environment.
	PCI simple communications controller	After you install a PCI simple communications controller, a Windows VM instance can communicate with the underlying KVM virtualization.
	PCI device	After you install a PCI device and enable its internal monitoring, Windows will support the balloon memory scaling.
	Ethernet adapter	A VirtIO Ethernet adapter can effectively improve the network performance of a VM instance in a virtualization environment.
Commonly-used tools	QEMU Guest Agent (QGA)	QGA is an application where mutual interactions between a host and a VM instance can be achieved. These interactions do not rely on networks, thereby greatly improving the VM performance and functionality. QGA helps check the state of GuestTools and VirtIO drivers in a VM instance. After QGA is installed, the VM instance enables you to change its password online.
	Cloudbase-Init	The VM instance that has Cloudbase-Init installed enables you to import User Data and achieve other custom functionalities.
	Agent internal monitoring	After an agent is installed, you can check the internal monitoring data of a VM instance.

Install GuestTools

1. Load the GuestTools image.

After you complete installing the operating system, enter the console page of the VM instance, and click **Install GuestTools** in the GuestTools installation prompt. Then, the operating system automatically loads the GuestTools image to the virtual CD Drive. To check this operation, go to the **Computer** page.

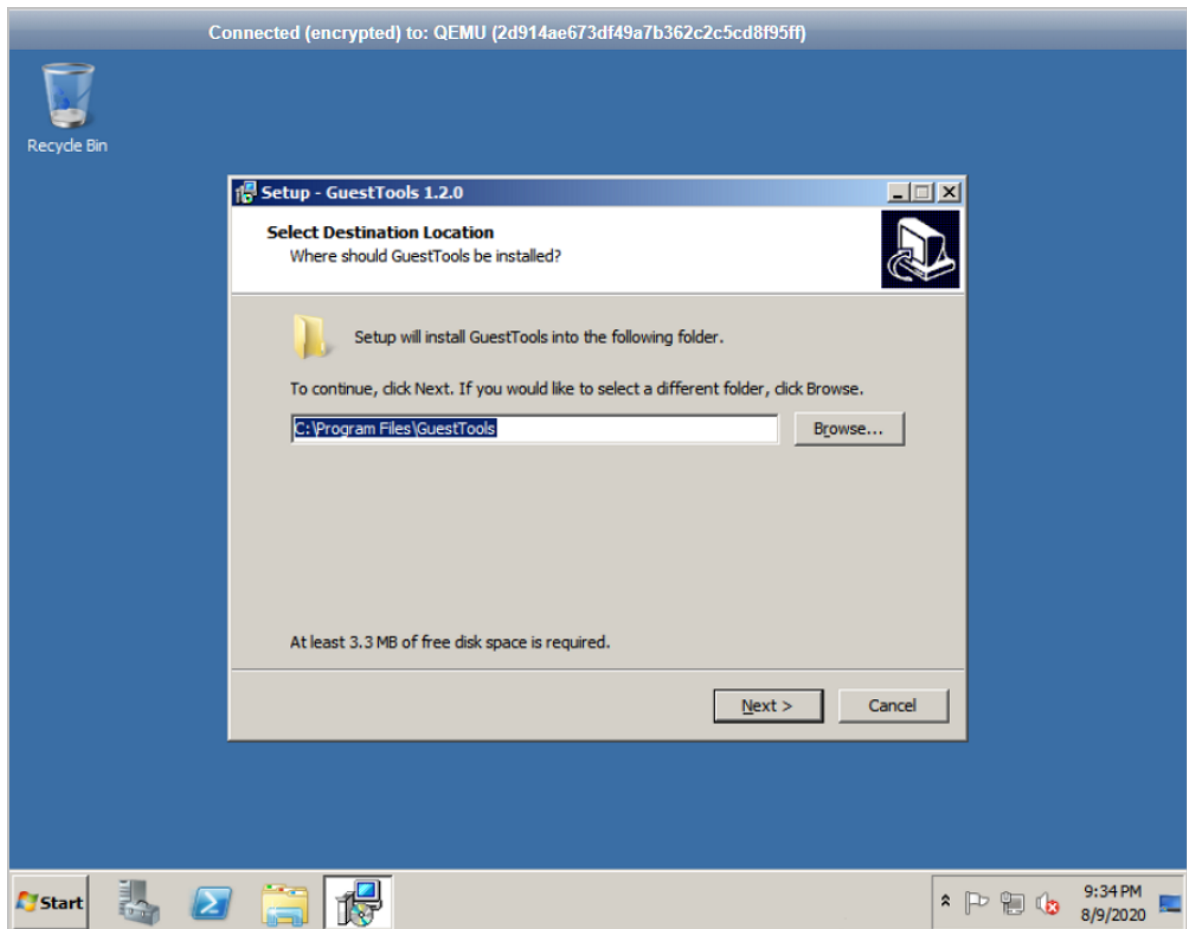
Figure 3-20: Load GuestTools Image

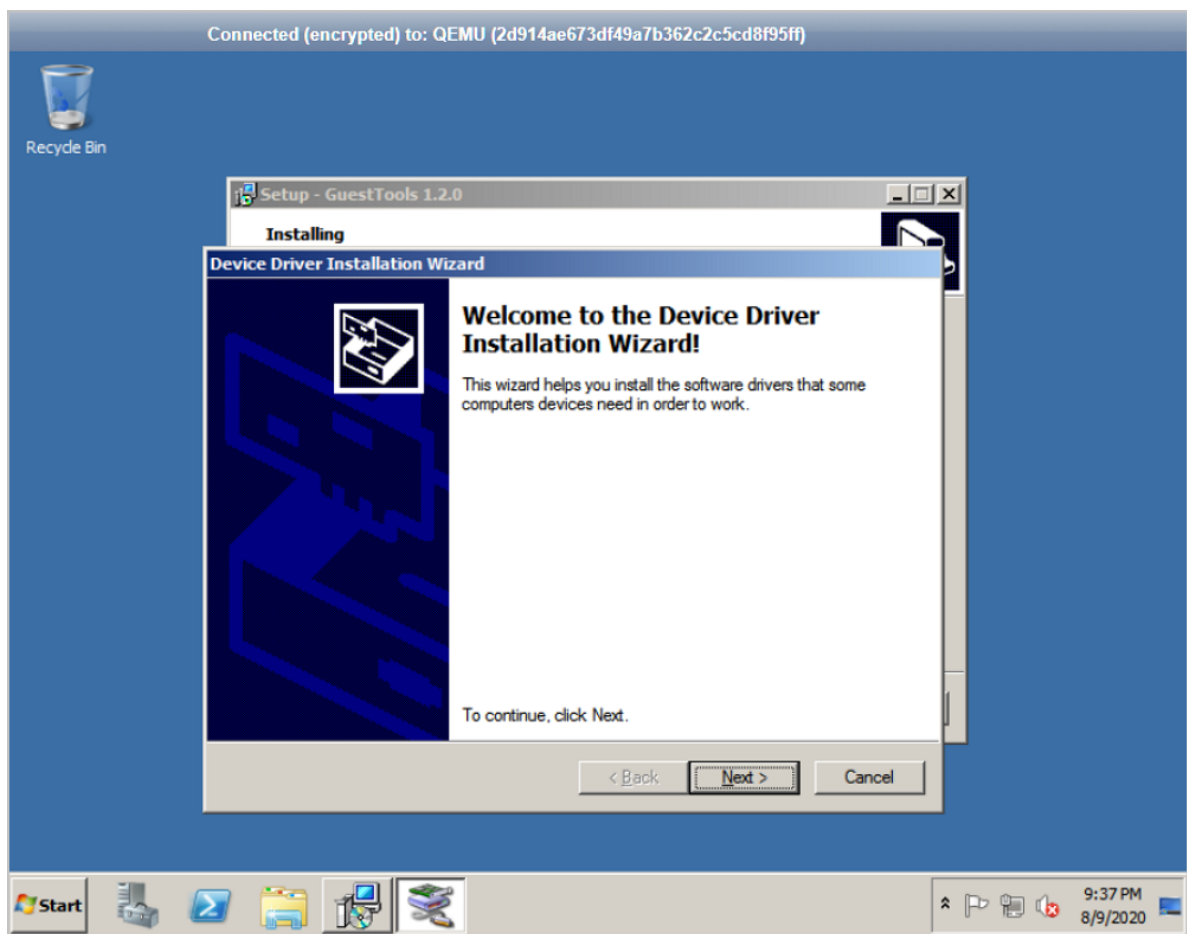


2. Install GuestTools and VirtIO driver.

Right-click the GuestTools CD Drive, select **Install or run program from your media** or double-click the GuestTools installation program. By following the displayed setup installation wizard, install GuestTools, commonly-used tools, and VirtIO drivers, successively.

Figure 3-21: Install GuestTools

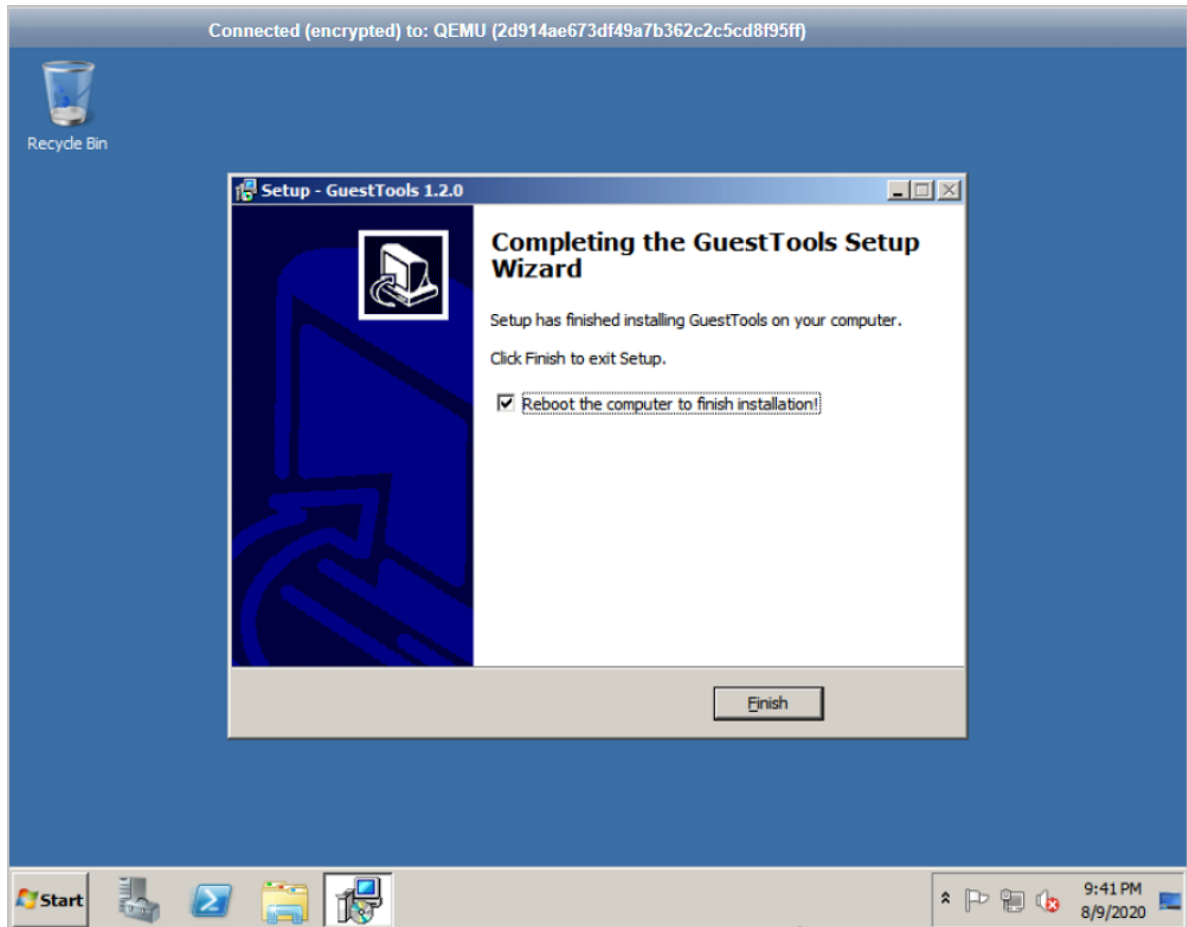




3. Confirm the installation and reboot your computer.

After you complete installing GuestTools, click **Finish** in the displayed dialog box. Make sure that you complete the installation and reboot the computer to make all configurations take effect.

Figure 3-22: Complete the Installation and Reboot Your Computer



After the operating system reboots, the platform of the VM instance is automatically changed to **WindowsVirtio**, and QGA is enabled.

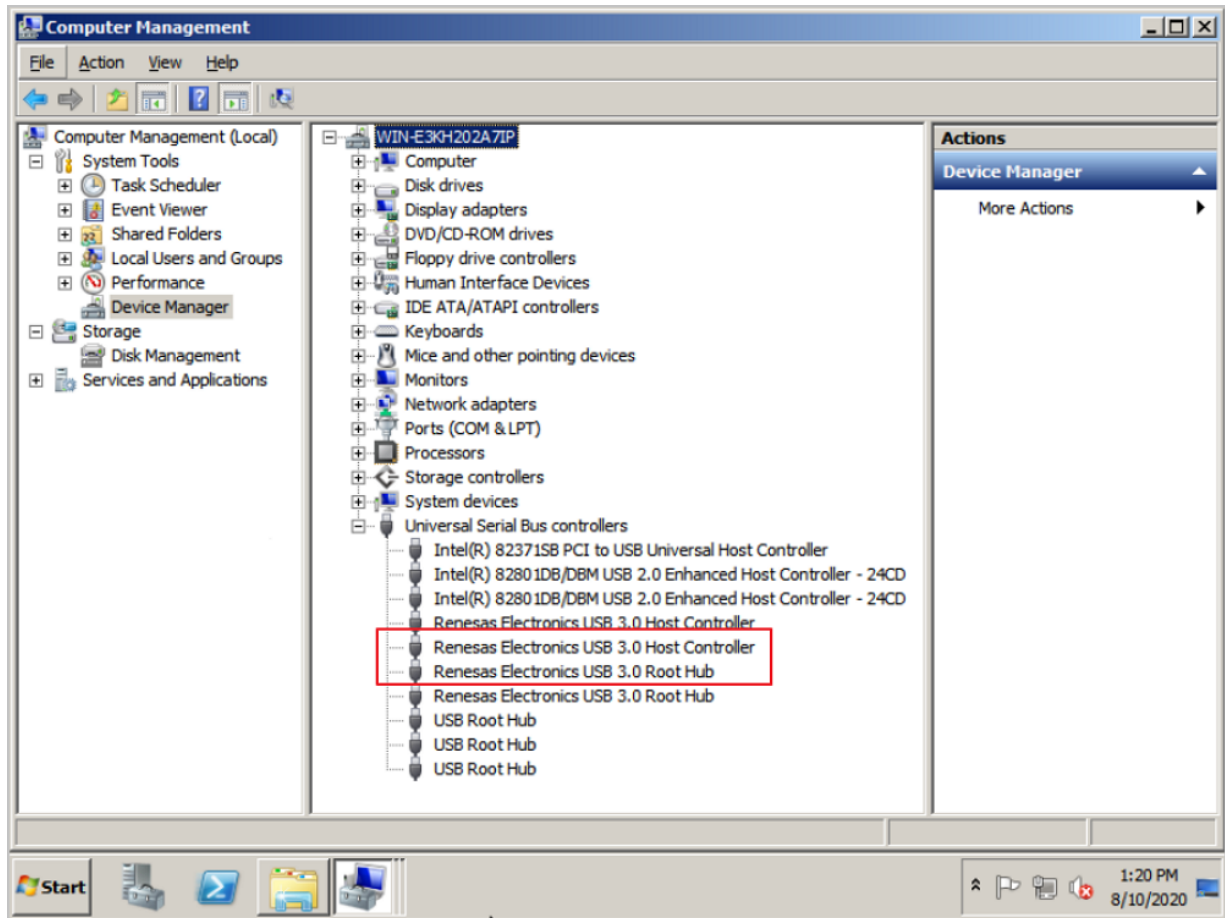
(Optional) Install other Software

You can install other software as needed in addition to the tools or drivers included in GuestTools.

For example, USB 2.0 driver is native to Windows Server 2008 R2. You can install the USB 3.0 driver as needed. Then, you can use the USB passthrough functionality.

You can obtain the driver file from https://cdn.zstack.io/tools/renesas_usb30_21390.exe , and double click the file to install the USB 3.0 driver.

Figure 3-23: Install USB 3.0 Driver



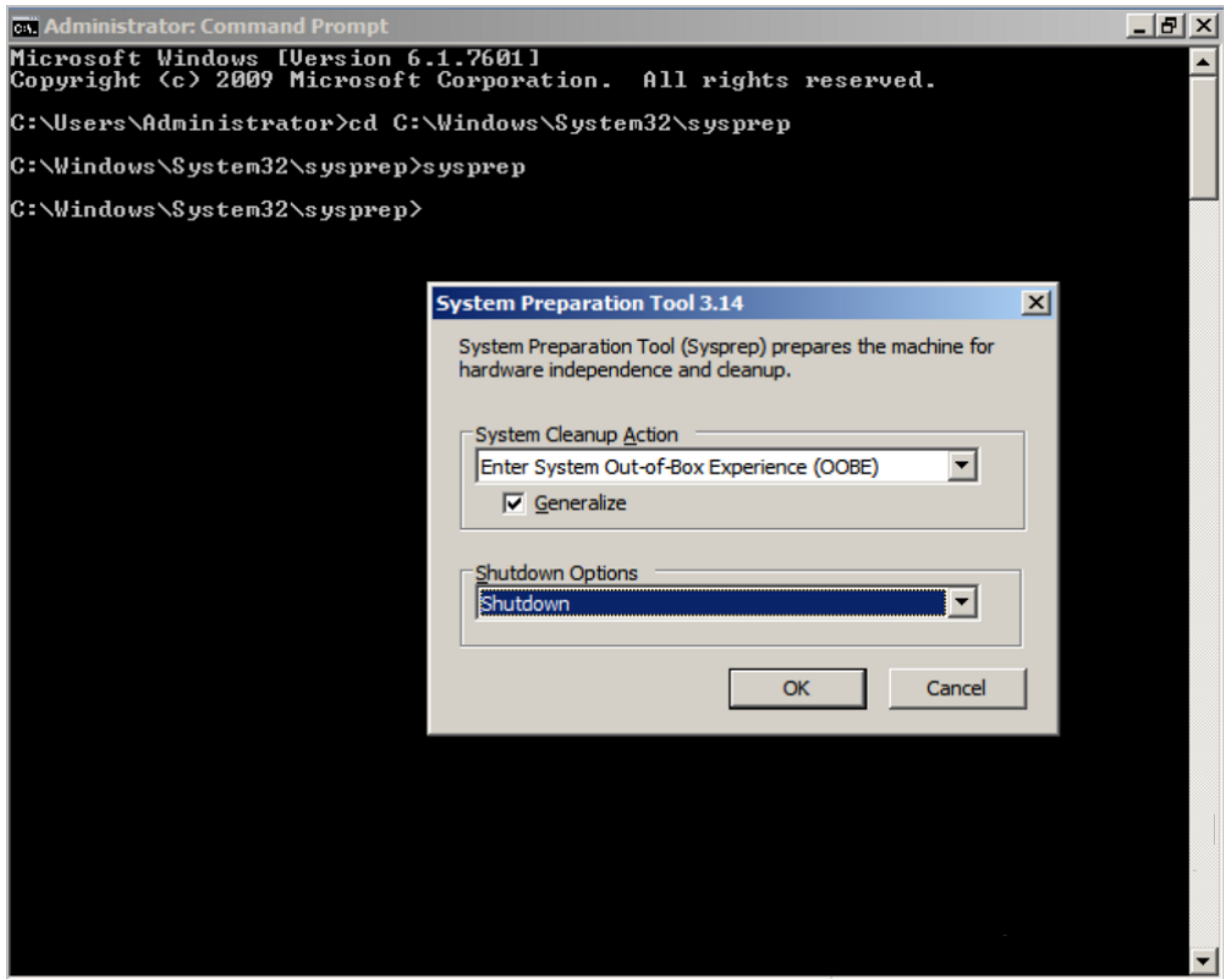
3.2.4 Prepare the Operating System

Operating system preparation is designed for generalizing and removing system-specific information such as hardware of a computer via Windows-native System Preparation Tool (Sysprep). To prepare the operating system, follow these steps:

1. Open the CMD command line by using the administrator permission.
2. Go to the `C:\Windows\System32\sysprep` directory and run the Sysprep tool.
3. Configure preparation policies and perform relevant operations. You can complete this step by setting the following parameters:
 - **System Cleanup Action:** Select **Enter System Out-of-Box Experience (OOBE)**.
 - **Generalize:** Select this checkbox. Then, the VM operating system created from the template has a unique security identity (SID).
 - **Shutdown Options:** Select **Shutdown**.

Click **OK**. Then, the system preparation begins.

Figure 3-24: System Preparation



3.2.5 Create a System Template

After you create the operating system template successfully, you can create VM instances in bulk in a custom manner by using this image. Also, you can export this image to create VM instances in other cloud platforms.

Create a VM Image

On the **VM Instance** page, select the target VM instance and create an image for the VM instance.

On the **Create Image** page, set the following parameters:

- **Name:** Enter a name for the image.
- **Description:** Optional. Enter a description for the image.
- **Image Type:** Select system image.
- **Backup Storage:** Select an existing backup storage.

Click **OK**. Then, the image is created.

Figure 3-25: Create Image

Create Image [X]

Name * ⓘ WindowsServer2008R2

Description

Image Type * System Image Volume Image

Backup Storage * BS-1 ×

OK Cancel



Note:

If your backup storage is ImageStore or Ceph, you can create an image for a VM instance when it is in the running state. For other types of backup storage, you need to stop the VM instance before you can create an image.

Export the Image

Exported images can be used directly by other cloud platforms to create VM instances. The export method varies based on the backup storage type.

- **ImageStore backup storages**

On the **Image** page, click **Actions > Export Image**. Then, an image is exported.

After the image is generated, you can download the exported image by copying the image URL on the **Overview** tab page of the image details page.

- **Ceph backup storages**

On the **Overview** tab page of the created image, copying **Backup Storage Path** will prompt you for the corresponding information such as pool and image in the Ceph backup storage.

After you copy this image path, you can export the Ceph image by running **rbd** on the Ceph backup storage. Assume that the storage path of the Ceph backup storage is *ceph#//bak-t-c9923f982/61ece0adc72*, run the following command:

```
[root@ceph-node1 ~]#rbd export bak-t-c9923f982/61ece0adc72 /root/  
export-test.image  
#bak-t-c9923f982 is the pool name where the image belongs.  
#61ece0adc72 is the image name.  
#/root/export-test.image is the name of the exported target file .
```

Glossary

VM Instance

A VM instance is a virtual machine instance running on a host. A VM instance has its own IP address and can access public networks and run application services.

Volume

A volume provides storage space for a VM instance. Volumes are categorized into root volumes and data volumes.

Root Volume

A root volume provides support for the system operations of a VM instance.

Data Volume

A data volume provides extended storage space for a VM instance.

Image

An image is a template file used to create a VM instance or volume. Images are categorized into system images and volume images.

Instance Offering

An instance offering defines the number of vCPU cores, memory size, network bandwidth, and other configuration settings of VM instances.

Disk Offering

A disk offering defines the capacity and other configuration settings of volumes.

GPU Specification

A GPU specification defines the frame per second (FPS), video memory, resolution, and other configuration settings of a physical or virtual GPU. GPU specifications are categorized into physical GPU specifications and virtual GPU specifications.

Auto-Scaling Group

An auto-scaling group is a group of VM instances that are used for the same scenarios. An auto-scaling group can automatically scale out or in based on application workloads or health status of VM instances in the group.

Snapshot

A snapshot is a point-in-time capture of data status in a volume.

Affinity Group

An affinity group is an orchestration policy for IaaS resources to ensure the high performance and high availability of businesses...

Zone

A zone is a logical group of resources such as clusters, L2 networks, and primary storages. Zone is the largest resource scope defined in the Cloud.

Cluster

A cluster is a logical group of hosts (compute nodes).

Host

A host provides compute, network, and storage resources for VM instances.

Primary Storage

A primary storage is one or more servers that store volume files of VM instances. These files include root volume snapshots, data volume snapshots, image caches, root volumes, and data volumes.

Backup Storage

A backup storage is one or more servers that store VM image templates, including ISO image files.

iSCSI Storage

iSCSI storage is a SAN storage that uses the iSCSI protocol for data transmission. You can add an iSCSI SAN block as a Shared Block primary storage or pass through the block to a VM instance.

FC Storage

FC storage is an SAN storage that uses the FC technology for data transmission. You can add an FC SAN block as a Shared Block primary storage or pass through the block to a VM instance.

L2 Network

An L2 network is a layer 2 broadcast domain used for layer 2 isolation. Generally, L2 networks are identified by names of devices on the physical network.

VXLAN Pool

A VXLAN pool is a collection of VXLAN networks established based on VXLAN Tunnel Endpoints (VTEPs). The VNI of each VXLAN network in a VXLAN pool must be unique.

L3 Network

An L3 network includes IP ranges, gateway, DNS, and other network configurations that are used by VM instances.

Public Network

Generally, a public network is a logical network that is connected to the Internet. However, in an environment that has no access to the Internet, you can also create a public network.

Flat Network

A flat network is connected to the network where the host is located and has direct access to the Internet. VM instances in a flat network can access public networks by using elastic IP addresses.

VPC Network

A VPC network is a private network where VM instances can be created. A VM instance in a VPC network can access the Internet through a VPC vRouter.

Management Network

A management network is used to manage physical resources in the Cloud. For example, you can create a management network to manage access to hosts, primary storages, backup storages, and VPC vRouters.

Flow Network

A flow network is a dedicated network for port mirror transmission. You can use a flow network to transmit the mirrors of data packets of NIC ports to the target ports.

VPC vRouter

A VPC vRouter is a dedicated VM instance that provides multiple network services.

VPC vRouter HA Group

A VPC vRouter HA group consists of two VPC vRouters. Either VPC vRouter can be a primary or secondary VPC vRouter for the group. If the primary VPC vRouter does not work as expected, the VPC vRouter becomes the secondary VPC vRouter in the group to ensure high availability of business.

vRouter Image

A vRouter image encapsulates network services and can be used to create VPC vRouters and load balancers. vRouter images can be categorized into VPC vRouter images and load balancer (LB) images.

Dedicated-Performance LB Image

A dedicated-performance load balancer (LB) image encapsulates dedicated-performance load-balancing services and can be used to create load balancer instances. However, a dedicated-performance load balancer image cannot be used to create VM instances.

vRouter Offering

A vRouter offering defines the number of vCPU cores, memory size, image, management network, and public network configuration settings of VPC vRouters. You can use a vRouter offering to create VPC vRouters that can provide network services for public networks and VPC networks.

LB Instance Offering

A load balancer (LB) instance offering defines the CPU, memory, image, and management network configuration settings used to create LB instances. LB instances provide load balancing services for the public network, flat network, and VPC network.

SDN Controller

An SDN controller is used to control network devices such as switches. You can add an external SDN controller to the Cloud and use the controller to control external switches and other network devices.

Security Group

A security group provides security control services for VM instances on the L3 network. It filters the ingress or egress TCP, UDP, and ICMP packets of specified VM instances in specified networks based on the specified security rules.

VIP

In bridged network environments, a virtual IP address (VIP) provides network services such as serving as an elastic IP address (EIP), port forwarding, load balancing, IPsec tunneling. When a VIP provides the preceding network services, packets are sent to the VIP and then routed to the destination network where VM instances are located.

EIP

An elastic IP address (EIP) functions based on the NAT technology. IP addresses in a private network are translated into an EIP that is in another network. This way, private networks can be accessed from other networks by using EIPs.

Port Forwarding

Port forwarding functions based on the layer-3 forwarding service of VPC vRouters. This service forwards traffic flows of the specified IP addresses and ports in a public network to specified ports of VM instances by using the specified protocol. If your public IP addresses are insufficient, you can configure port forwarding for multiple VM instances by using one public IP address and port.

Load Balancer

A load balancer distributes traffic flows of a virtual IP address to backend servers. It automatically inspects the availability of backend servers and isolates unavailable servers during traffic distribution. This way, the load balancer improves the availability and service capability of your business.

Listener

A listener monitors the frontend requests of a load balancer and distributes the requests to a backend server based on the specified policy. In addition, the listener performs health checks on backend servers.

Forwarding Rule

A forwarding rule forwards the requests from different domain names or URLs to different backend server groups.

Backend Server Group

A backend server group is a group of backend servers that handles requests distributed by load balancers. It is the basic unit for traffic distribution by load balancer instances.

Backend Server

A backend server handles requests distributed by a load balancer. You can add a VM instance on the Cloud or a server on a third-party cloud as a backend server.

Frontend Network

A frontend network is a type of network that is associated with a load balancer. Requests from the network are distributed by the load balancer to backend servers based on a specified policy.

Backend Network

A backend network is a type of network that is associated with a load balancer. Requests from frontend networks are distributed by the load balancer to servers in the backend network.

Load Balancer Instance

A load balancer instance is a custom VM instance used to provide load balancing services.

Certificate

If you select HTTPS for a listener, associate it with a certificate to make the listener take effect. You can upload either a certificate or certificate chain.

Firewall

A firewall is an access control policy that monitors ingress and egress traffic of VPC vRouters and decides whether to allow or block specific traffic based on a defined set of security rules.

IPsec Tunnel

An IPsec tunnel encrypts and verifies IP packets that transmit over a virtual private network (VPN) from one site to another.

OSPF Area

An OSPF area is split from an autonomous system based on the OSPF protocol. This splitting simplifies the management of vRouters.

NetFlow

An NetFlow monitors the ingress and egress traffic of the NICs of VPC vRouters. The supported versions of data flows are V5 and V9.

Port Mirroring

Port mirroring mirrors the traffic data of VM NICs and sends the traffic data to the target ports. This allows for the analysis of data packets of ports and simplifies the monitoring and management of data traffic and makes it easier to locate network errors and exceptions.

Route Table

A route table contains information about various routes that you configure. Route entries in a route table must include the destination network, next hop, and route priority.

CloudFormation

CloudFormation is a service that simplifies the management of cloud resources and automates deployment and O&S. You can create a stack template to configure cloud resources and their dependencies. This way, resources can be automatically configured and deployed in batches. CloudFormation provides easy management of the lifecycle of cloud resources and integrates automatic O&S into API and SDK.

Resource Stack

A resource stack is a stack of resources that are configured by using a stack template. The resources in the stack have dependencies with each other. You can manage resources in the stack by managing the resource stack.

Stack Template

A stack template is a UTF8-encoded file based on which you can create resource stacks. The stack template defines the resources that you want, the dependencies between the resources , and the configuration settings of the resources. When you use a stack template to create a resource stack, CloudFormation parses the template and the resources are automatically created and configured.

Sample Template

A sample template is a commonly used resource stack. You can use a sample template provide by the Cloud to create resource stacks.

Designer

A designer is a CloudFormation tool that allows you to orchestrate cloud resources. You can drag and drop resources on a canvas and use lines to establish dependencies between the resources.

Baremetal Cluster

A baremetal cluster consists of baremetal chassis. You can manage baremetal chassis by managing a baremetal cluster where the chassis reside.

Deployment Server

A deployment server is a server that provides PXE service and console proxy service for baremetal chassis.

Baremetal Chassis

A baremetal chassis is used to create a baremetal instance and is identified based on the BMC interface and IPMI configuration setting.

Preconfigured Template

A preconfigured template is used to create a preconfigured file that allows for unattended batch installation of an operating system for baremetal instances.

Baremetal Instance

A baremetal instance is an instantiated baremetal chassis.

Elastic Baremetal Management

Elastic Baremetal Management provides dedicated physical servers for your applications to ensure high performance and stability. In addition, this feature allows elastic scaling. You can apply for and scale resources based on your needs.

Provision Network

A provision network is a dedicated network for PXE boot and image downloads while creating elastic baremetal instances.

Elastic Baremetal Cluster

An elastic baremetal cluster consists of elastic baremetal instances. You can manage elastic baremetal instances by managing an elastic baremetal cluster where the instances reside.

Gateway Node

A gateway node is a node where the ingress and egress traffic of the Cloud and elastic baremetal instances is forwarded.

Baremetal Node

A baremetal node is used to create a baremetal instance and is identified based on the BMC interface and IPMI configuration setting.

Elastic Baremetal Instance

An elastic baremetal instance has the same performance as physical servers and allows elastic scaling. You can apply for and scale resources based on your needs.

Elastic Baremetal Offering

An elastic baremetal offering defines the number of vCPU cores, memory size, CPU architecture, CPU model, and other configuration settings of elastic baremetal instances.

vCenter

The Cloud allows you to take over vCenter and manage resources on the vCenter.

VM Instance

A VM instance is an ESXi virtual machine instance running on a host. A VM instance has its own IP address to access public networks and can run application services.

Network

A vCenter network defines the network settings of VM instances on vCenter, such as IP range, gateway, DNS, and network services.

Volume

A volume provides storage space for a VM instance on vCenter. A volume attached to a VM instance can be used as a root volume or data volume. A root volume provides support for the system operations of a VM instance. A data volume provides extended storage space for a VM instance.

Image

An image is a template file used to create a VM instance or volume on vCenter. Images are categorized into system images and volume images.

Event Message

Event Message displays event alarm messages of vCenter that is took over by the Cloud. This feature allows you to locate errors and exceptions efficiently.

Network Topology

A network topology visualizes the network architecture of the Cloud. It allows for efficient planning , management, and improvement of network architecture. Network topologies can be categorized into global topologies and custom topologies.

Performance Analysis

Performance Analysis displays the performance metrics of key resources under monitoring in the Cloud. Cloud resources can be externally or internally monitored. You can use either method to monitor the performance of resources in the Cloud and improve O&S efficiency.

Capacity Management

Capacity Management visualizes the capacities and usages of key resources in the Cloud. You can use this feature to improve O&S efficiency.

MN Monitoring

MN monitoring allows you to view the health status of each management node when you use multiple management nodes to achieve high availability.

Alarm

An alarm is used to monitor the status of time-series data and events and respond to the status change. Alarms can be categorized into resource alarm, event alarm, and extended alarm.

One-Click Alarm

A one-click alarm integrates multiple metrics of a resource. You can create one-click alarms for multiple resources to monitor these resources.

Alarm Template

An alarm template is a template of alarm rules. If you associate an alarm template with a resource group, an alarm is created to monitor the resources in the group.

Resource Group

A resource group consists of resources grouped based on your business needs. If you associate an alarm template with a resource group, the alarm rules specified by the template take effect on all the resources in the group.

Message Template

A message template specifies the text template of a resource alarm message or event alarm message sent to an SNS system.

Message Source

A message source is used to take over extended alarm messages. If you configure alarms for message sources, extended alarm messages can be sent to various endpoints.

Endpoint

An endpoint is a method that users obtain subscribed messages. Endpoints are categorized into system endpoints, email, DingTalk, HTTP application, short message service, and Microsoft Teams.

Alarm Message

An alarm message is a message sent the time when an alarm is triggered.

Operation Log

An operation log is a chronological record of operations on the specified objects and their operation results.

Audit

Audit monitors and records all activities on the Cloud. You can use this feature to implement operation tracking, cybersecurity classified protection compliance, security analysis, troubleshooting, and automatic O&M.

Backup Management

Backup management integrates multiple disaster recovery technologies such as incremental backup and full backup that are suitable for multiple business scenarios. You can implement local backup and remote backup based on your business needs.

Backup Job

You can create a backup job to back up local VM instances, volumes, or databases to a specified storage server on a regular basis.

Local Backup Data

Local backup data of VM instances, volumes, and databases is stored in the local backup storage.

Local Backup Storage

A local backup storage is located at the local data center and is used to store local backup data.

Remote Backup Storage

A remote backup storage is located at a remote data center or a public cloud and is used to store remote backup data.

Continuous Data Protection (CDP)

Continuous Data Protection (CDP) provides second-level and fine-grained continuous backups for important business systems in VM instances, allowing users to restore VM data to any time state and retrieve files without restoring the system.

CDP Task

You can create a CDP task to continuously back up your VM data to a specified backup storage to achieve continuous data protection and restoration.

CDP Data

The backup data generated from continuous data protection on VM instances is stored in local backup storages.

Scheduled Job

A scheduled job defines that a specific action be implemented at a specified time based on a scheduler.

Scheduler

A scheduler is used to schedule jobs. It is suitable for business scenarios that last for a long time.

Tag

A tag is used to mark resources. You can use a tag to search for and aggregate resources.

Migration Service

The Cloud provides V2V migration service that allows you to migrate VM instances and data from other virtualized platform to the current cloud platform.

V2V Migration

V2V Migration allows you to migrate VM instances from the VMware or KVM platform to the current cloud platform.

V2V Conversion Host

A V2V conversion host is a host in the destination cluster that you need to specify during V2V migration to cache VM instances and data when you implement V2V migration. After the VM instances and data are cached in the V2Vconversion host, they are migrated to the destination primary storage.

User

A user is a natural person that constructs the most basic unit in business management.

Member Group

A member group is a collection of natural persons or a collection of project members. You can use a member group to grant permissions.

Role

A role is a collection of permissions that can be granted to users. A user that assumes a role can call API operations based on the permissions specified by the role. Roles are categorized into system roles and custom roles.

3rd Party Authentication

The 3rd party authentication feature allows you to integrate third-party authentication systems to the Cloud. Then you can use a third-party account to log in to the Cloud and use the resources in the Cloud. You can add an AD or LDAP server to the Cloud.

Project

A project is a task that needs to be accomplished by specific personnel at a specified time.

Resources and budgets are also specified for projects. In business management, you can plan resources at the project granularity and allocate an independent resource pool for a project.

Project Member

A project member is a member in a project who is granted permissions on specific project resources and can use the resources to accomplish tasks. Project members include the project admin, project managers, and normal project members.

Process Management

Process management is part of ticket management that manages the processes related to the resources of projects. Processes can be categorized into default processes and custom processes.

My Approvals

In the Cloud, only the administrator and project administrators are granted approval permissions. the administrator and project administrators can approve or reject a ticket. If a ticket is approved, resources are automatically deployed and allocated to the specified project.

Bills

A bill is the expense of resources totaled at a specified time period. Billing is accurate to the second. Bills can be categorized into project bills, department bills, and account bills.

Pricing List

A pricing list is a list of unit prices of different resources. The unit price of a resource is set based on the specification and usage time of the resource.

Console Proxy

Console proxy allows you to log in to a VM instance by using the IP address of a proxy.

AccessKey Management

An AccessKey pair is a security credential that one party authorizes another party to call API operations and access its resources in the Cloud. AccessKey pairs shall be kept confidential.

IP Blocklist/Allowlist

An IP blocklist or allowlist identifies and filters IP addresses that access the Cloud. You can create an IP allowlist or blocklist to improve access control of the Cloud.

Application Center

Application Center allows you to add third-party applications to the Cloud and then access the applications by using the Cloud. It extends the functionality of the Cloud.

Sub-Account Management

A sub-account is created and managed by the admin. Resources created under a sub-account is managed by the sub-account.

Theme and Appearance

You can customize the theme and appearance of the Cloud.

Email Server

If you select Email as the endpoint of an alarm, you need to set an email server. Then alarm messages are sent to the email server.

Log Server

A log server is used to collect logs of the management node. You can add a log server to the cloud and use the collected logs to locate errors and exceptions. This makes your O&M more efficient.

Global Setting

Global Setting allows you to configure settings that take effect on the whole platform.

Scenario Template

Scenario Template provides multiple templates that encapsulate scenario-based global settings . You can apply a template globally with one click based on your business needs. This improves your O&M efficiency.