

A large, faint, abstract network graph is visible in the background on the left side of the slide. It consists of numerous small, light-blue circular nodes connected by thin, light-blue lines, creating a complex web-like structure.

V2V Migration Tutorial

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.....	1
1 Overview.....	1
2 Preparations.....	3
3 Quick Start.....	4
4 V2V Migration.....	5
4.1 Source Cloud Platform: VMware.....	6
4.2 Source Cloud Platform: KVM.....	14
5 V2V Conversion Host.....	24
6 Typical Practices.....	28
6.1 Source Cloud Platform: VMware.....	28
6.2 Source Cloud Platform: KVM.....	36
Glossary.....	45

1 Overview

ZStack Cloud provides the Migration Service, allowing you to migrate VM systems and data from other virtualization platforms to the current cloud. Currently, with the Migration Service, you can:

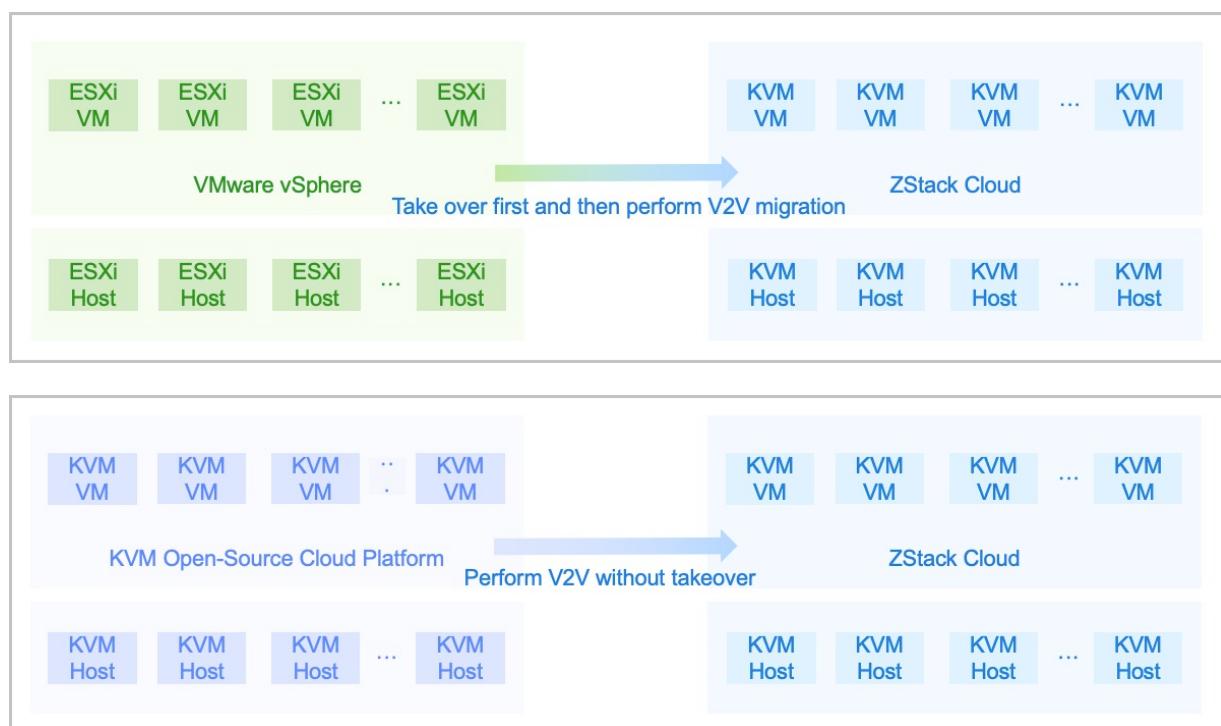
- Migrate VM instances from the vCenter that you took over to the current cloud. The supported vCenter versions include 5.0, 5.1, 5.5, 6.0, 6.5, 6.7, and 7.0. Note that the version of the vCenter server must be consistent with that of the ESXi host.
- Migrate VM instances from a KVM cloud platform to the current cloud.



Note:

If you took over vCenter 7.0, to ensure that the VM console can open properly, we recommend that you download the trusted root CA certificate when you log into vCenter.

Figure 1-1: V2V Migration



The Migration Service is a separate feature module. To use this feature, you need to purchase both the Base License and the Plus License of the Migration Service. The Plus License cannot be used independently.

Advantages of the Migration Service are as follows:

- Allows you to perform one-click V2V migrations for VM instances in bulk.

- Allows you to add a conversion host and create a V2V job and lets the Cloud do the rest.
- Allows you to configure an independent migration network and a network QoS for a conversion host to control transmission bottlenecks and improve migration efficiencies.
- Allows you to customize configurations for destination VM instances when you create a V2V job.
- Monitors and manages the entire migration process in the visualized, well-designed UI.

2 Preparations

- The admin installs the latest version of ZStack Cloud in advance, and deploys necessary resources used for creating VM instances.

For more information, see the [*Installation and Deployment*](#) section in the [*User Guide*](#).

- The admin purchases a Plus License of the Migration Service module in advance, and then installs this module.
- If the source cloud platform is VMware, take over the vCenter to ZStack CloudPrivate Cloud.

3 Quick Start

You can quickly get started with the migration service by following these steps:

1. Add a V2V conversion host. For information about how to add a V2V conversion host, see [*V2V Conversion Host*](#).
2. Create a V2V job to migrate VM instances from other virtualization platforms to the current cloud. For information about how to create a V2V job, see [*V2V Migration*](#).

4 V2V Migration

Currently, you can migrate VM instances from a VMware cloud platform or a KVM cloud platform to the current cloud. Before you use the Migration Service, note the following considerations.

- [VMware Source Platform Considerations](#)
- [KVM Source Platform Considerations](#)

VMware Source Platform Considerations

If the source cloud platform is VMware, note the following:

- Before migrations, perform **data synchronization** to manually synchronize the latest status of resources in the vCenter that you took over.
- You can perform bulk V2V migrations for VM instances, and customize configurations of the migrated VM instances.
- The supported vCenter versions include 5.0, 5.1, 5.5, 6.0, 6.5, 6.7, and 7.0. Note that the version of the vCenter server must be consistent with that of the ESXi host.
- The supported VM systems of the source vCenter include RHEL/CentOS 4.x, 5.x, 6.x, 7.x, SLES 11, 12, 15, Ubuntu 12, 14, 16, 18, Windows 7, and Windows Server 2003 R2, 2008 R2, 2012 R2, 2016, 2019.
- The VM instances will be forced to shut down during the V2V migration. Therefore, pay attention to the business impact.



Note:

The system firstly attempts to shut down the VM instances gently. If the shutdown fails, the system will perform force shutdown.

- The type of the source primary storage is not enforced. The type of the destination primary storage can be LocalStorage, NFS, Ceph, or SharedBlock.
- For Windows VM instances, the Windows VirtIO driver is automatically installed during the migration. This improves the NIC and disk efficiencies.
- You can perform V2V migration for VM instances booted by UEFI. After the migration, these VM instances are also booted by UEFI.

KVM Source Platform Considerations

If the source cloud platform is KVM, note the following:

- You can perform bulk V2V migrations for VM instances, and customize configurations of the migrated VM instances.
- You can migrate the VM instances that are running or paused. Do not power off the VM instances to be migrated
- You can perform V2V migrations for VM instances booted by UEFI. After the migration, these VM instances are also booted by UEFI.
- The type of the source primary storage is not enforced. The type of the destination primary storage can be LocalStorage, NFS, Ceph, or SharedBlock.
- For different types of source primary storages or destination primary storages, the libvirt version and QEMU version must meet the following requirements:
 - If either the source primary storage or destination primary storage is Ceph, use libvirt 1.2.16 and QEMU 1.1 or their later versions.
 - If neither the source primary storage nor destination primary storage is Ceph, use libvirt 1.2.9 and QEMU 1.1 or their later versions.

4.1 Source Cloud Platform: VMware

This topic describes VMware-based V2V jobs from the following perspectives:

- [Create a V2V Job](#)
- [Manage a V2V Job](#)
- [V2V Job Details](#)

Create a V2V Job

To create a V2V job based on the VMware platform, follow these five steps:

1. Configure the source resources.

Set the following parameters:

- **Name:** Enter a name for the V2V job.

The V2V job name must be 1 to 128 characters in length and can contain Chinese characters, letters, digits, hyphens (-), underscores (_), periods (.), parenthesis (), colons (:), and plus signs (+).

- **Description:** Optional. Enter a description for the V2V job.
- **Source Platform:** Select the source platform type. Here, select VMware.
- **V2V Conversion Host:** Select a V2V conversion host.

**Note:**

- Before you can create a V2V job, add a V2V conversion host to the Cloud.
- The type of the V2V conversion host must be consistent with that of the source cloud platform.
- The V2V conversion host is a host in the specified destination cluster. Make sure that the hardware resources are sufficient for V2V migration.
- If you select multiple source VM instances, note that the V2V jobs created accordingly will share the same V2V conversion host.

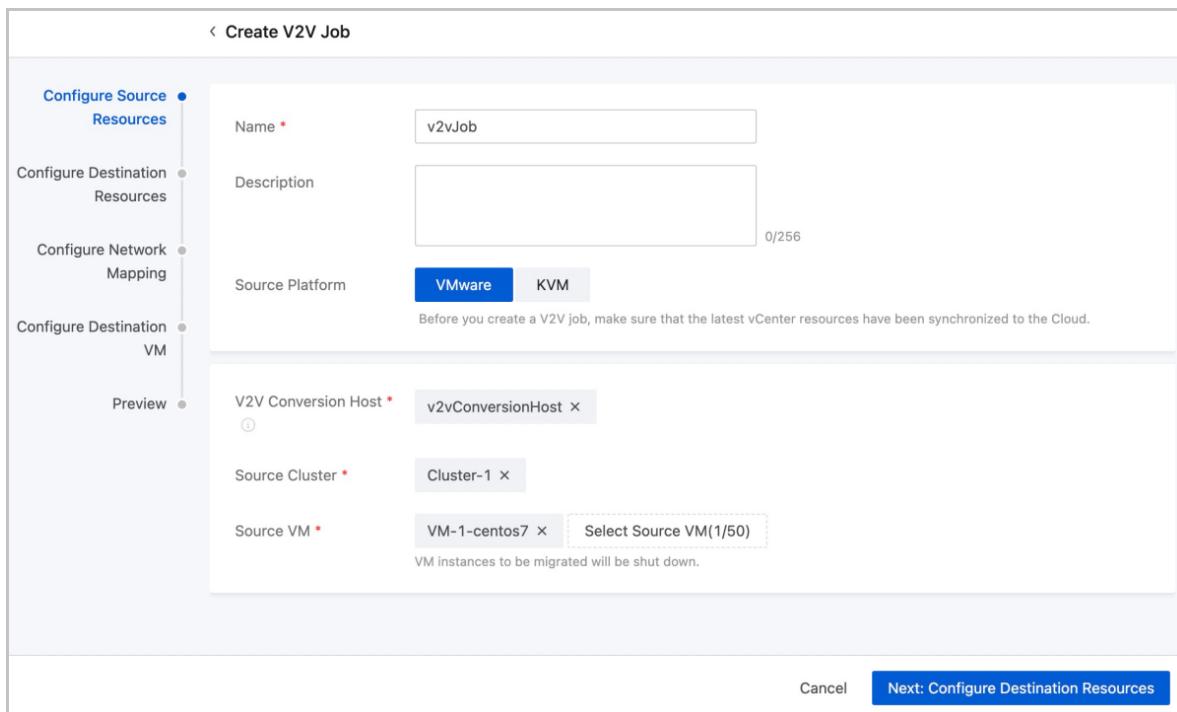
- **Source Cluster:** Select a cluster from the vCenter that you took over as the source cluster.
- **Source VM:** Select one or more vCenter VM instances from the source cluster as the source VM instance or VM instances. You can select up to 50 VM instances at a time.

**Note:**

- If you select more than one VM instance, corresponding V2V jobs will be created in bulk.
 - . Note that one V2V job corresponds to one source VM instance.
- For Windows Server 2012 R2 and Windows Server 2016 VM instances, you need to manually disable the hibernation feature and shut down these VM instances before you create V2V jobs.

To disable or enable the Windows hibernation feature, run the following commands:

- Disable Windows hibernation: cmd-->"powercfg -h off"
- Enable Windows hibernation: cmd-->"powercfg -h on"
- If one of the source VM instances has a data volume, make sure that the disk mode of the data volume is Dependent. Otherwise, the V2V job might fail.

Figure 4-1: Configure Source Resources

2. Configure the destination resources.

Set the following parameters:

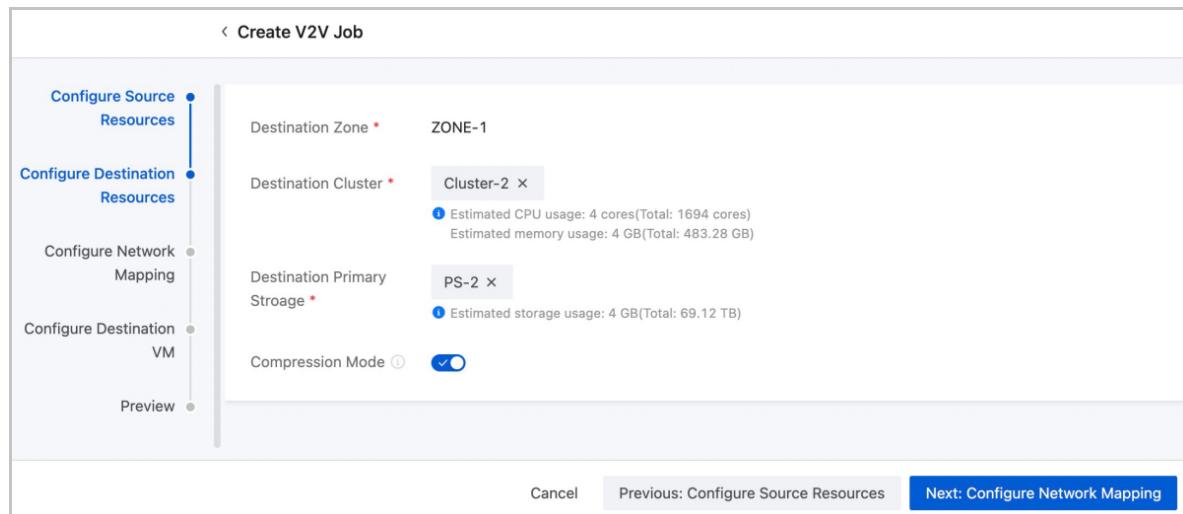
- **Destination Zone:** By default, the current zone is displayed.
- **Destination Cluster:** Select a destination cluster. Then, the estimated CPU usage and memory usage are displayed.
 - Estimated CPU usage: displays the number of the used CPUs of the source VM instance and the total number of available CPUs in the destination cluster.
 - Estimated memory usage: displays the used memory size of the source VM instance and the total available memory size in the destination cluster.
- **Destination Primary Storage:** Select a destination primary storage. Then, the estimated primary storage usage is displayed.
 - Estimated storage usage: displays the used storage of the source VM instance and the total available storage of the destination primary storage.
- **Compression mode:** Choose whether to enable the compression mode. By default, the compression mode is enabled.



Note:

- Enabling the compression mode compresses the caches of the migration data and improves the cache space utilization of the V2V conversion host.
- If the destination primary storage is Ceph, we recommend that you do not use the compression mode.

Figure 4-2: Configure Destination Resources



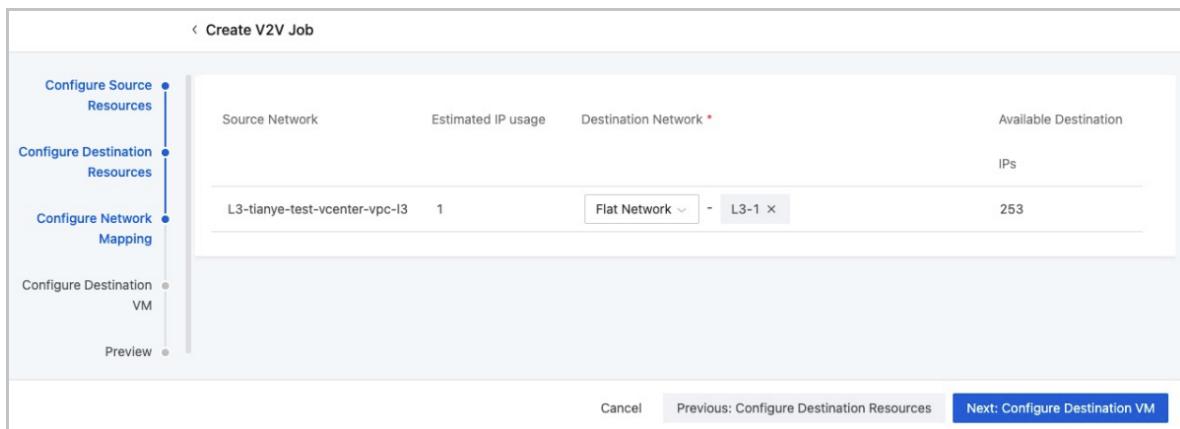
3. Configure the network mapping.

In this step, consider the following:

- The source VM instance has a NIC attached.
 - The source VM instance does not have a NIC attached.
- a. If the source VM instance has a NIC attached,

Set the following parameters:

- Destination Network:** Select a destination network as needed. The destination network is the network attached to the specified destination cluster.
- b. If the source VM instance does not have a NIC attached, go to the next step to manually configure the destination NIC.

Figure 4-3: Configure Network Mapping

4. Configure the destination VM instance.

In this step, consider the following:

- The VM instance has a NIC attached.
- The VM instance does not have a NIC attached.
- a. If the VM instance has a NIC attached,

configure the destination VM instance by setting the following parameters:

- **Start VM After Migration:** Choose whether to automatically start the destination VM instance after the migration.
- **Use Source MAC and IP:** Choose whether to use the source MAC and IP addresses. By default, these addresses are not used.



Note:

- If not used, you can customize the MAC and IP addresses for the destination NIC. If you do configure them, the destination MAC address will be the same as the source MAC address after migration, and the IP address of the destination NIC will be allocated by the system.
- If used, the destination NIC will use the MAC and IP addresses of the source NIC in the next step. If the source NIC does not have an IP address, the IP address of the destination NIC will be allocated by the system.

- **VM Configuration:** Select the VM instance to be configured. You can configure the VM instance by setting the following parameters:

- **Name:** Set the name of the destination VM instance.
- **NIC:** Configure the NIC information.
 - **Network:** Select the network for the destination VM instance.
 - **IP Address:** Optional. Configure the IP address of the destination NIC.

**Note:**

If not configured, the IP address of the destination NIC will be allocated by the system.

- **MAC Address:** Optional. Configure the MAC address of the destination NIC.

**Note:**

If not configured, the MAC address of the destination NIC will be the same as that of the source NIC after migration.

- **Boot Partition:** If the VM instance to be migrated has multiple boot partitions, specify one as the root volume for the VM instance.

**Note:**

- Go to the next step if no further modification is needed.
- Before you migrate a VM instance to the current cloud, make sure that the VM instance has at least one NIC attached.

- b. If the VM instance does not have a NIC attached,

configure the destination VM instance by setting the following parameters:

- **Start VM After Migration:** Choose whether to automatically start the destination VM instance after the migration.
- **VM Configuration:** Select the VM instance to be configured. You can configure the VM instance by setting the following parameters:

- **Name:** Set the name of the destination VM instance.

- **NIC:** Configure the NIC information.

- **Network:** Select the network for the destination VM instance.

- **IP Address:** Optional. Configure the IP address of the destination NIC.

**Note:**

If not configured, the IP address of the destination NIC will be allocated by the system.

- **MAC Address:** Optional. Configure the MAC address of the destination NIC.



Note:

If not configured, the MAC address of the destination NIC will be the same as that of the source NIC after migration.

- **Boot Partition:** If the VM instance to be migrated has multiple boot partitions, specify one as the root volume for the VM instance.

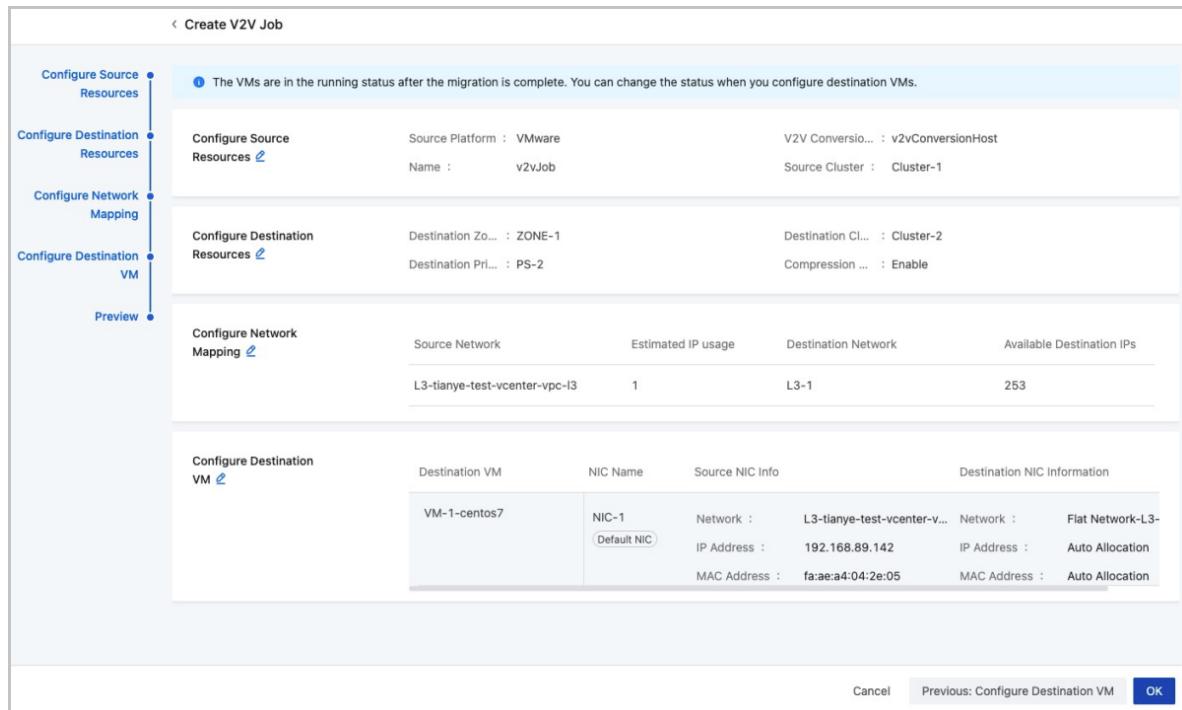


Note:

Before you migrate a VM instance to the current cloud, make sure that the VM instance has at least one NIC attached.

Figure 4-4: Configure Destination VM

5. Confirm and submit.

Figure 4-5: Confirm and Submit

Manage a V2V Job

On the main menu of ZStack Cloud, choose **Platform O&M > Migration Service > V2V Migration**. Then, the **V2V Migration** page is displayed.

The following table lists the actions that you can perform on a V2V job.

Action	Description
Reboot V2V Job	<p>Reboot a V2V job if the job failed.</p> <p>Note:</p> <ul style="list-style-type: none"> If migration data caches exist, rebooting the V2V job can improve the migration efficiency. <ul style="list-style-type: none"> You can set the period for retaining the migration data caches in the global setting.
Edit V2V Job	Modify the name and description of a V2V job.
Delete V2V Job	Delete a V2V job after migration.

V2V Job Details

On the **V2V Migration** page, click on the name of a V2V job. Then, the details page of the V2V job is displayed. On the details page, you can view the V2V job status and the basic information about the source VM instance and destination VM instance.

Figure 4-6: V2V Job Details

The screenshot shows the 'v2vJob' details page. At the top, there's a navigation bar with 'Actions' and tabs for 'Overview' (selected) and 'Audit'. The 'Basic Info' section contains fields like Job Status (Succeeded), Source VM (VM-1-centos7), Destination VM (VM-1-centos7), Duration (1 minutes53 seconds), UUID (c9c8b7127f054fab91b78d939664285c), Creation Time (2021-11-11 11:44:04), and Last Operation (2021-11-11 11:45:57). The 'Resource Configurations' section shows mappings between Source and Destination VMs, including Platform (VMware), Zone (ZONE-1), Primary Storage (datastore1), Cluster (Cluster-1) for the source, and Zone (ZONE-1), Primary Storage (PS-2), Cluster (Cluster-2) for the destination.

4.2 Source Cloud Platform: KVM

This topic describes KVM-based V2V jobs from the following perspectives:

- [Create a V2V Job](#)
- [Manage a V2V Job](#)
- [V2V Job Details](#)

Create a V2V Job

To create a V2V job based on the KVM platform, follow these five steps:

1. Configure the source resources.

Set the following parameters;

- **Name:** Enter a name for the V2V job.
- **Description:** Optional. Enter a description for the V2V job.
- **Source Platform:** Select KVM.
- **V2V Conversion Host:** Specify a V2V conversion host.



Note:

- Before you can create a V2V job, add a V2V conversion host to the Cloud.
 - The type of the V2V conversion host must be consistent with that of the source cloud platform.
 - The V2V conversion host is a host in the specified destination cluster. Make sure that the hardware resources are sufficient for V2V migration.
 - If you select multiple source VM instances, note that the V2V jobs created accordingly will share the same V2V conversion host.
- **Source Host IP:** Enter the IP address of the source host.
 - **Source Host SSH Port:** Set the SSH port of the source host. Default: 22.
 - **SSH Username:** Enter the username. Default: root.
 - **SSH Password:**
 - If you select **Password**, enter the SSH password. You can log in to the source host through the SSH password authentication.
 - If you select **PrivateKey**, enter the corresponding SSH private key. You can log in to the source host through the SSH private key authentication.



Note:

Before you select this option, create an SSH private key for the source host in advance.

- **Virsh Info:**
 - By default, this checkbox is not selected, indicating that the virtual resources of the source host are not remotely accessed through virsh.
 - If selected, you need to enter the **SASL Username** and **SASL Password** when the remote libvirtd requires Simple Authentication and Security Layer (SASL) authentication. You can securely connect to the remote libvirtd only after passing the verification.
 - **SASL Username:** Enter the corresponding SASL username.
 - **SASL Password:** Enter the corresponding SASL password.
- **Get Source VM Info:** Obtain information about the running or paused VM instances that are available for migration.
- **Source VM:** Select one or more KVM VM instances from the source host.



Note:

- You can select up to 50 VM instances at a time.

- Do not power off the VM instances to be migrated.
- If you select more than one VM instance, corresponding V2V jobs will be created in bulk
 - . Note that one V2V job corresponds to one source VM instance.

• **Pause Running VM:**

- By default, this checkbox is not selected, indicating that the VM instances continue to run during the migration. This ensures the business continuity of the source VM instances.
- If selected, the source VM instances will be paused when the migration starts, and the data written to the disk at that time will be migrated. After the migration is completed, you need to manually start the paused source VM instances.



Note:

For VM instances with high I/O, we recommend that you pause them before migration to ensure the data integrity.

Figure 4-7: Configure Source Resources

The screenshot shows the 'Create V2V Job' interface with the 'Configure Source Resources' tab selected. The 'Name' field is set to 'KVM-V2V'. The 'Source Platform' is set to 'KVM'. The 'V2V Conversion Host' is listed as 'v2vConversionHost-KVM'. In the 'Source Host' section, the IP is '172.20.1.51', port is '22', and the username is 'root'. The 'SSH Password' option is selected. The 'Virsh Info' section has a 'Configure Virsh' checkbox. The 'Source VM Info' section shows a note about 15 running or paused VM instances and a 'Try Again' button. The 'Source VM' dropdown contains '52361ea66e3947e985ec5...' and a 'Select Source VM(1/50)' button. A 'Pause VM' checkbox is available. Navigation buttons 'Cancel' and 'Next: Configure Destination Resources' are at the bottom.

2. Configure the destination resources.

Set the following parameters:

- **Destination Zone:** By default, the current zone is displayed.
- **Destination Cluster:** Select a destination cluster. Then, the estimated CPU usage and memory usage are displayed.
 - Estimated CPU usage: displays the number of the used CPUs of the source VM instance and the total number of available CPUs in the destination cluster.
 - Estimated memory usage: displays the used memory size of the source VM instance and the total available memory size in the destination cluster.
- **Destination Primary Storage:** Select a destination primary storage. Then, the estimated primary storage usage is displayed.
 - Estimated storage usage: displays the used storage of the source VM instance and the total available storage of the destination primary storage.
- **Compression mode:** Choose whether to enable the compression mode. By default, the compression mode is enabled.



Note:

- Enabling the compression mode compresses the caches of the migration data and improves the cache space utilization of the V2V conversion host.
- If the destination primary storage is Ceph, we recommend that you do not use the compression mode.

Figure 4-8: Configure Destination Resources

The screenshot shows the 'Create V2V Job' interface with the 'Configure Destination Resources' step selected. The left sidebar lists steps: 'Configure Source Resources' (selected), 'Configure Destination Resources' (highlighted), 'Configure Network Mapping', 'Configure Destination VM', and 'Preview'. The main panel displays configuration options for the destination cluster and storage, along with a note about compression mode.

Configuration Option	Value	Notes
Destination Zone	ZONE-1	
Destination Cluster	Cluster-2	Estimated CPU usage: 8 cores(Total: 1653 cores) Estimated memory usage: 16 GB(Total: 414.28 GB)
Destination Primary Storage	PS-2	Estimated storage usage: 300 GB(Total: 261.83 TB)
Compression Mode	Enabled	

3. Configure the network mapping.

In this step, consider the following:

- The source VM instance has a NIC attached.
- The source VM instance does not have a NIC attached.

- a. If the source VM instance has a NIC attached,

Set the following parameters:

- **Destination Network:** Select a destination network as needed. The destination network is the network attached to the specified destination cluster.
- b. If the source VM instance does not have a NIC attached, go to the next step to manually configure the destination NIC.

Figure 4-9: Configure Network Mapping

Source NIC	Estimated IP usage	Destination Network *	Available Destination IPs
NIC-1	1	VPC Network - L3-VPC	64804

4. Configure the destination VM instance.

In this step, consider the following:

- The VM instance has a NIC attached.
- The VM instance does not have a NIC attached.

- a. If the source VM instance does not have a NIC attached,

configure the destination VM instance by setting the following parameters:

- **Start VM After Migration:** Choose whether to automatically start the destination VM instance after the migration.
- **VM Configuration:** Select the VM instance to be configured. You can configure the VM instance by setting the following parameters.

- **Name:** Set the name of the destination VM instance.

— **NIC:** Configure the NIC information.

- **Network:** Select the network for the destination VM instance.
- **IP Address:** Optional. Configure the IP address of the destination NIC.



Note:

If not configured, the IP address of the destination NIC will be allocated by the system.

- **MAC Address:** Optional. Configure the MAC address of the destination NIC.



Note:

If not configured, the MAC address of the destination NIC will be the same as that of the source NIC after migration.



Note:

- Go to the next step if no further modification is needed.
- Before you migrate a VM instance to the current cloud, make sure that the VM instance has at least one NIC attached.

b. If the VM instance has a NIC attached,

configure the destination VM instance by setting the following parameters:

- **Start VM After Migration:** Choose whether to automatically start the destination VM instance after the migration.
- **VM Configuration:** Select the VM instance to be configured. You can configure the VM instance by setting the following parameters:
 - **Name:** Set the name of the destination VM instance.
 - **CPU:** Set the number of CPU cores for the destination VM instance. The number must be an integer ranging from 1 to 1024.
 - **Memory:** 16MB~100TB。 : Set the memory size for the destination VM instance. The memory must be an integer ranging from 16 MB to 100 TB.
 - **Platform:** Select the image platform type.

The image platform determines the platform used for creating VM instances. You can set whether to use KVM VirtIO drivers (including disk drivers and NIC drivers).

- Linux: If VirtIO is enabled, the image operating system (OS) will have a VirtIO driver attached. If VirtIO is disabled, the OS, such as RHEL 5.8, will use a QEMU device instead.
 - Windows: If VirtIO is enabled, the image OS will have a VirtIO driver attached. If VirtIO is disabled, the OS will use a QEMU device instead.
 - Other: If VirtIO is enabled, the image OS will have a VirtIO driver attached. If VirtIO is disabled, the OS will use a QEMU device instead. This type of platform is compatible with some operating systems of earlier versions that do not support VirtIO drivers.
- **VirtIO:** Choose whether to enable VirtIO based on your operating system and platform.
- **Volume:** Select the volume to be migrated and set a name for the volume.
- **NIC:** Configure the destination NIC information by setting the following parameters:
- **Network:** Select the network for the destination VM instance.
 - **Specify IP:** Optional. Configure the IP address for the destination NIC.

**Note:**

If not configured, the IP address of the destination NIC will be allocated by the system.

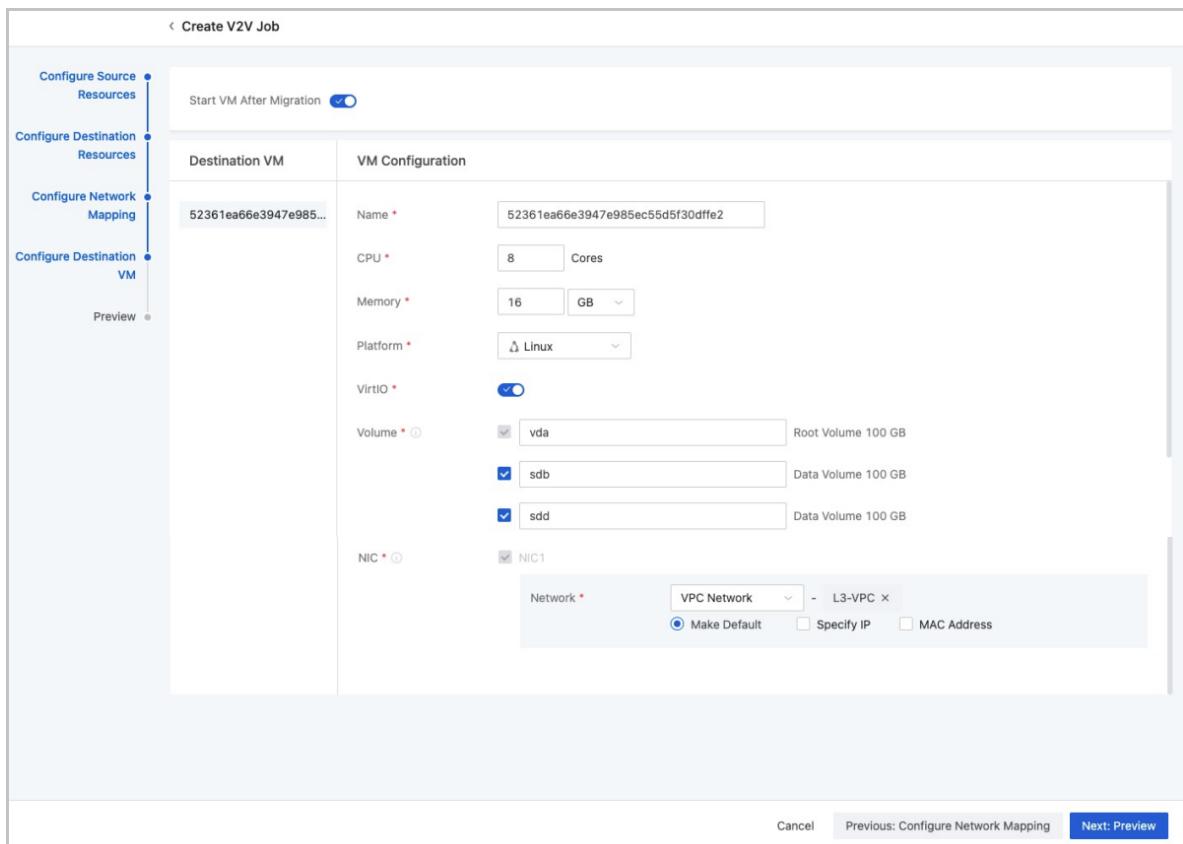
- **MAC Address:** Optional. Configure the MAC address for the destination NIC.

**Note:**

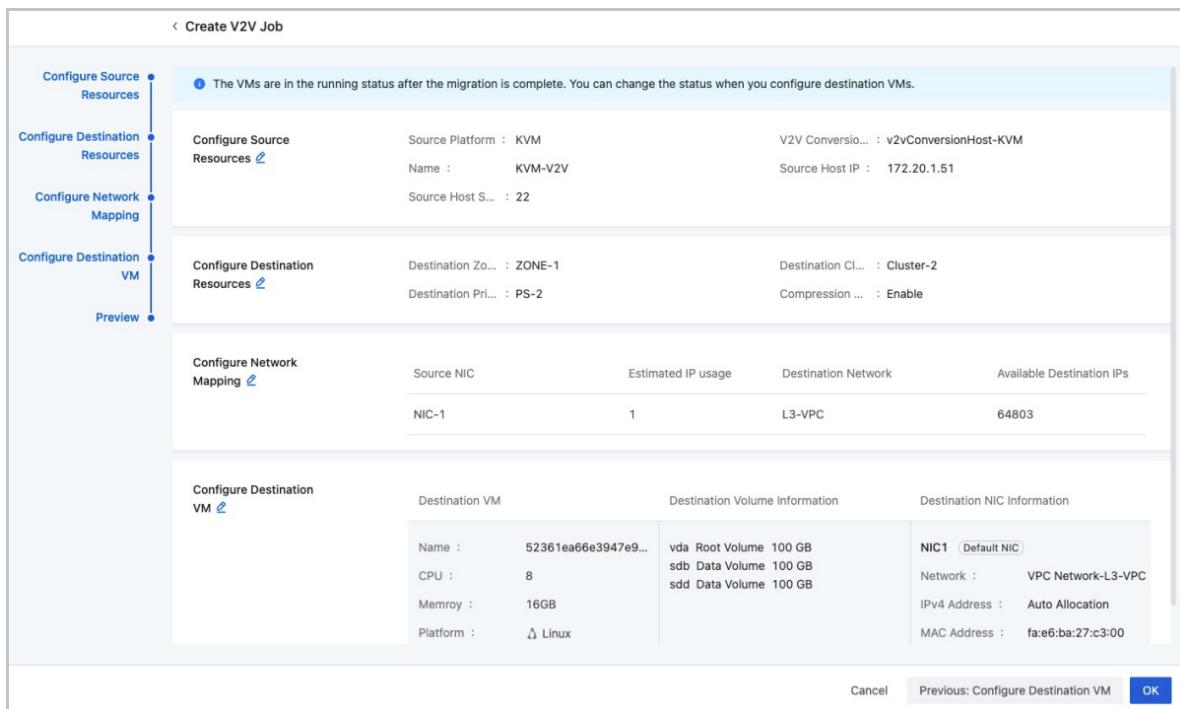
If not configured, the MAC address of the destination NIC will be the same as that of the source NIC.

**Note:**

Before you migrate a VM instance to the current cloud, make sure that the VM instance has at least one NIC attached.

Figure 4-10: Configure Destination VM

5. Confirm and Submit.

Figure 4-11: Confirm and Submit

Manage a V2V Job

On the main menu of ZStack Cloud, choose **Platform O&M > Migration Service > V2V Migration**. Then, the **V2V Migration** page is displayed.

The following table lists the actions that you can perform on a V2V job.

Action	Description
Reboot V2V Job	<p>Reboot a V2V job if the job failed.</p> <p>Note:</p> <p>If migration data caches exist, rebooting the V2V job can improve the migration efficiency.</p> <ul style="list-style-type: none"> You can set the period for retaining the migration data caches in the global setting.
Edit V2V Job	Modify the name and description of a V2V job.
Delete V2V Job	Delete a V2V job after migration.

V2V Job Details

On the **V2V Migration** page, click on the name of a V2V job. Then, the details page of the V2V job is displayed. On the details page, you can view the V2V job status and the basic information about the source VM instance and destination VM instance.

Figure 4-12: V2V Job Details

The screenshot shows the 'V2V Migration' interface for a job named 'KVM-V2V'. The 'Overview' tab is selected. The 'Basic Info' section displays the following details:

- Job Status : Succeeded
- Source VM : 52361ea66e3947e985ec55d5f30dff2
- Destination VM : 52361ea66e3947e985ec55d5f30dff2
- V2V Conversio... : v2vConversionHost-KVM
- Duration : 10 minutes31 seconds
- UUID : 300ff23344eb42e58c5e2e9044d08a56
- Creation Time : 2021-11-12 09:57:11
- Last Operation... : 2021-11-12 10:07:42

The 'Resource Configurations' section shows the following settings:

Source VM	Host IP	172.20.1.51
	Platform	KVM
Destination VM	CPU	8 Cores
	Memory	16 GB
	Total Volume C...	300 GB
	Zone	ZONE-1
	Primary Storage	PS-2
	Cluster	Cluster-2

The 'Configuration Info' section indicates that Compression is set to Enable.

5 V2V Conversion Host

Before you can perform V2V migration, specify a host in the destination cluster as the V2V conversion host.

- [Add a V2V Conversion Host](#)
- [V2V Conversion Host Details](#)
- [Manage a V2V Conversion Host](#)
- [Considerations](#)

Add a V2V Conversion Host

On the main menu of ZStack Cloud, choose **Platform O&M > Migration Service > V2V Conversion Host**. On the **V2V Conversion Host** page, click **Add V2V Conversion Host**. Then, the **Add V2V Conversion Host** page is displayed.

On the displayed page, set the following parameters:

- **Name:** Enter a name for the V2V conversion host.
Note that the name must be 1 to 128 characters in length and can contain Chinese characters, letters, digits, hyphens (-), underscores (_), periods (.), parenthesis (), colons (:), and plus signs (+).
- **Description:** Optional. Enter a description for the V2V conversion host.
- **Type:** Select a V2V conversion host type, including VMware and KVM.



Note:

The type of the V2V conversion host must be consistent with that of the source cloud platform.

- **Host:** Select a host from the destination cluster as the V2V conversion host.



Note:

A host cannot be used as a V2V conversion host for both the VMware platform type and the KVM platform type at the same time.

- **Cache Path:** Enter a local path on the V2V conversion host as the storage path.



Note:

During the V2V migration, the VM system and data are first cached in the V2V conversion host and then imported into the target primary storage.

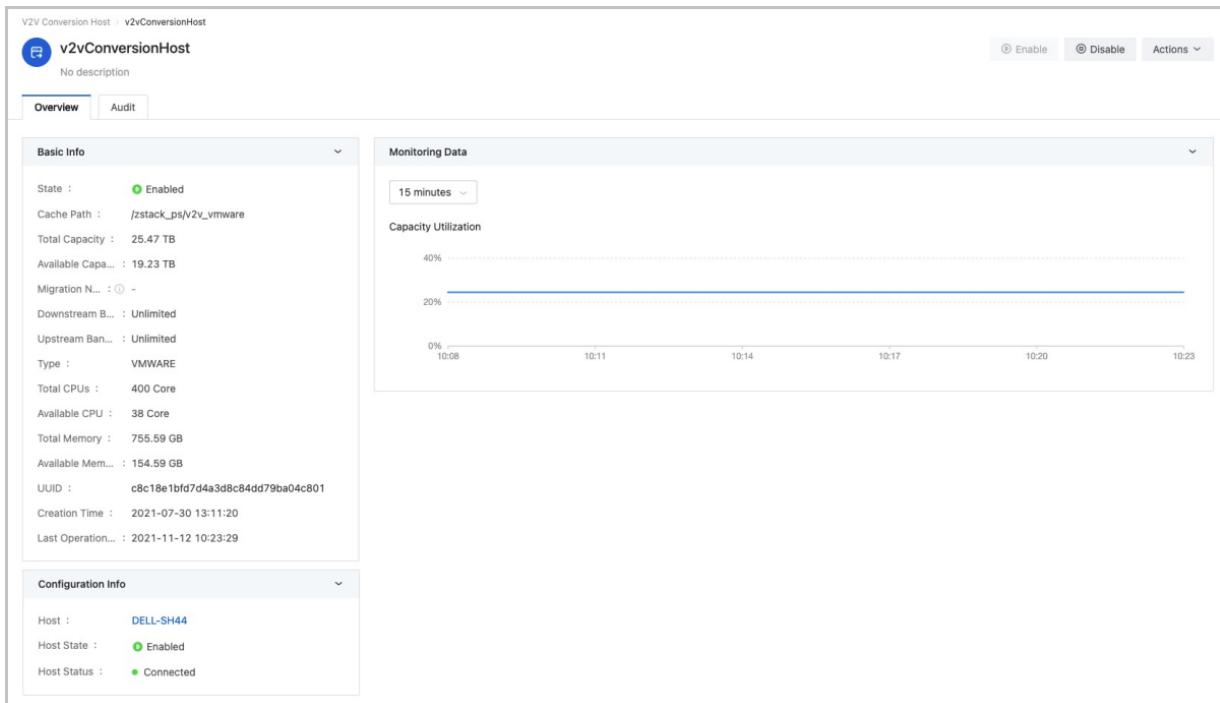
- **Migration Network:** Optional. If you deployed an independent network for V2V migration, enter the CIDR of the network.

**Note:**

- If you deployed an independent network for V2V migration, you could add the network to the Cloud directly.
 - In a V2V migration scenario, the migration network is used to convert data migrated from the destination primary storage to the V2V conversion host.
 - Using an independent migration network can avoid network congestion and improve transmission efficiencies.
 - If not set, the management network will be used by default for V2V migration.
- **Upstream Bandwidth:** Optional. Set the upstream bandwidth of the V2V conversion host. This parameter limits the speed of uploading data from the V2V conversion host to the destination primary storage. The upstream bandwidth must be an integer ranging from 1 Mbps to 32 Gbps. Unit: Mbps and Gbps.
 - **Downstream Bandwidth:** Optional. Set the downstream bandwidth for the V2V conversion host. This parameter limits the speed of downloading data from the source primary storage to the V2V conversion host. The downstream bandwidth must be an integer ranging from 1 Mbps to 32 Gbps. Unit: Mbps and Gbps.

V2V Conversion Host Details

On the main menu of ZStack Cloud, choose **Platform O&M > Migration Service > V2V Conversion Host**. On the **V2V Conversion Host** page, click on the name of a V2V conversion to go to the details page. The details page displays the basic information, monitoring data, and configurations of the V2V conversion host.

Figure 5-1: V2V Conversion Host Details

Manage a V2V Conversion Host

On the main menu of ZStack Cloud, choose **Platform O&M > Migration Service > V2V Conversion Host**. Then, the **V2V Conversion Host** page is displayed.

The following table lists the actions that you can perform on a V2V conversion host.

Action	Description
Edit V2V Conversion Host	Modify the name and description of the V2V conversion host.
Enable V2V Conversion Host	Enable a V2V conversion host.
Disable V2V Conversion Host	Disable a V2V Conversion host. Note: If you disable a V2V conversion host when you perform a V2V job, the job is not affected.
Set Network Bandwidth	Set the upstream or downstream bandwidth of the V2V conversion host.
Delete V2V Conversion Host	Delete a V2V conversion host.

Action	Description
	<p>Note:</p> <ul style="list-style-type: none"> Deleting a V2V conversion host automatically cancels the ongoing V2V job. Deleting a V2V conversion host also deletes the local records of the backup data on the conversion host, but the actual data is not affected. If you add this conversion host again, the local records are not recovered automatically.

Considerations

- A V2V conversion host must have sufficient hardware resources, such as network bandwidth and disk space. The following table lists the minimum configuration requirements.

Table 5-1: Minimum Configuration Requirements for V2V Conversion Host

Hardware	Configuration Requirements
CPU	Minimum 8 cores
Memory	Minimum 16 GB
Network	Minimum 1 Gigabyte NIC
Storage	<p>Minimum 50 GB for the rest of storage spaces</p> <p>Note: You can modify the storage configuration according to the number of VM instances to be migrated.</p>

- The type of the V2V conversion host must be consistent with that of the source cloud platform.
- You can set an independent migration network and a network QoS for a V2V conversion host to control transmission bottlenecks and to improve migration efficiencies.

6 Typical Practices

6.1 Source Cloud Platform: VMware

Context

Scenario: Due to business needs, you need to migrate VM instances from your vCenter to the current cloud. Assume that:

- You deployed a vCenter environment and the latest ZStack Cloud Private Cloud and took over vCenter on ZStack Cloud Private Cloud.
- You prepared a storage server and added it to the destination cluster as a compute node. You use this compute node as the V2V conversion host.
- You purchased and installed the Migration Service module.

The following table lists the information about the source and the destination cloud platform.

Source Cloud Platform	Destination Cloud Platform
vCenter <ul style="list-style-type: none"> • Version: 6.0 • Primary storage type: LocalStorage • Network: public network, flat network, and VPC network • Number of VM instances: 4 <ul style="list-style-type: none"> — VM-1-centos7 (with 1 data volume) — VM-2-win2008 (with 2 data volumes) — VM-3-win2016 (with 1 data volume) — VM-4-win2012 (with 2 data volumes) 	ZStack Cloud Private Cloud <ul style="list-style-type: none"> • Version: the latest version • Primary storage type: SharedBlock • Network: public network, flat network, and VPC network

The workflow is as follows:

1. Add a V2V conversion host.
2. Create a V2V job to migrate the 4 VM instances from the vCenter that you took over to the current cloud.

Procedure

1. Add a V2V conversion host.

In this scenario, you will add a compute node prepared in the destination cluster as the V2V conversion host.

On the main menu of ZStack Cloud, choose **Platform O&M > Migration Service > V2V Conversion Host**. On the **V2V Conversion Host** page, click **Add V2V Conversion Host**. Then, the **Add V2V Conversion Host** page is displayed.

On the displayed page, set the following parameters:

- **Name:** Enter a name for the V2V conversion host.
- **Description:** Optional. Enter a description for the V2V conversion host.
- **Type:** Select VMware Platform.



Note:

The type of the V2V conversion host must be consistent with that of the source platform you selected when you create a V2V job.

- **Host:** Select a host from the destination cluster as the V2V conversion host.



Note:

A host cannot be used as a V2V conversion host for both the VMware platform type and the KVM platform type at the same time.

- **Cache Path:** Enter a local path on the V2V conversion host as the storage path.



Note:

During the V2V migration, the VM system and data are first cached in the V2V conversion host and then imported into the target primary storage.

- **Migration Network:** Optional. If you deployed an independent network for V2V migration, enter the CIDR of the network.



Note:

- If you deployed an independent network for V2V migration, you could add the network to the Cloud directly.
- In a V2V migration scenario, the migration network is used to convert data migrated from the destination primary storage to the V2V conversion host.
- Using an independent migration network can avoid network congestion and improve transmission efficiencies.
- If not set, the management network will be used by default for V2V migration.

- **Upstream Bandwidth:** Optional. Set the upstream bandwidth of the V2V conversion host. This parameter limits the speed of uploading data from the V2V conversion host to the destination primary storage. The upstream bandwidth must be an integer ranging from 1 Mbps to 32 Gbps. Unit: Mbps and Gbps.
- **Downstream Bandwidth:** Optional. Set the downstream bandwidth for the V2V conversion host. This parameter limits the speed of downloading data from the source primary storage to the V2V conversion host. The downstream bandwidth must be an integer ranging from 1 Mbps to 32 Gbps. Unit: Mbps and Gbps.

Figure 6-1: Add V2V Conversion Host

2. Create a V2V job to migrate these 4 VM instances from the vCenter that you took over to the current cloud.

On the main menu of ZStack Cloud, choose **Platform O&M > Migration Service > V2V Migration**. On the **V2V Migration** page, click **Create V2V Job**. Then, the **Create V2V Job** page is displayed

- a) Configure the source resources.

Set the following parameters:

- **Name:** Enter a name for the V2V job.

The V2V job name must be 1 to 128 characters in length and can contain Chinese characters, letters, digits, hyphens (-), underscores (_), periods (.), parenthesis (), colons (:), and plus signs (+).

- **Description:** Optional. Enter a description for the V2V job.
- **Source Platform:** Select the source platform type. Here, select VMware.
- **V2V Conversion Host:** Select a V2V conversion host.



Note:

- Before you can create a V2V job, add a V2V conversion host to the Cloud.
- The type of the V2V conversion host must be consistent with that of the source cloud platform.
- The V2V conversion host is a host in the specified destination cluster. Make sure that the hardware resources are sufficient for V2V migration.
- If you select multiple source VM instances, note that the V2V jobs created accordingly will share the same V2V conversion host.

- **Source Cluster:** Select a cluster from the vCenter that you took over as the source cluster.
- **Source VM:** Select one or more vCenter VM instances from the source cluster as the source VM instance or VM instances. You can select up to 50 VM instances at a time.

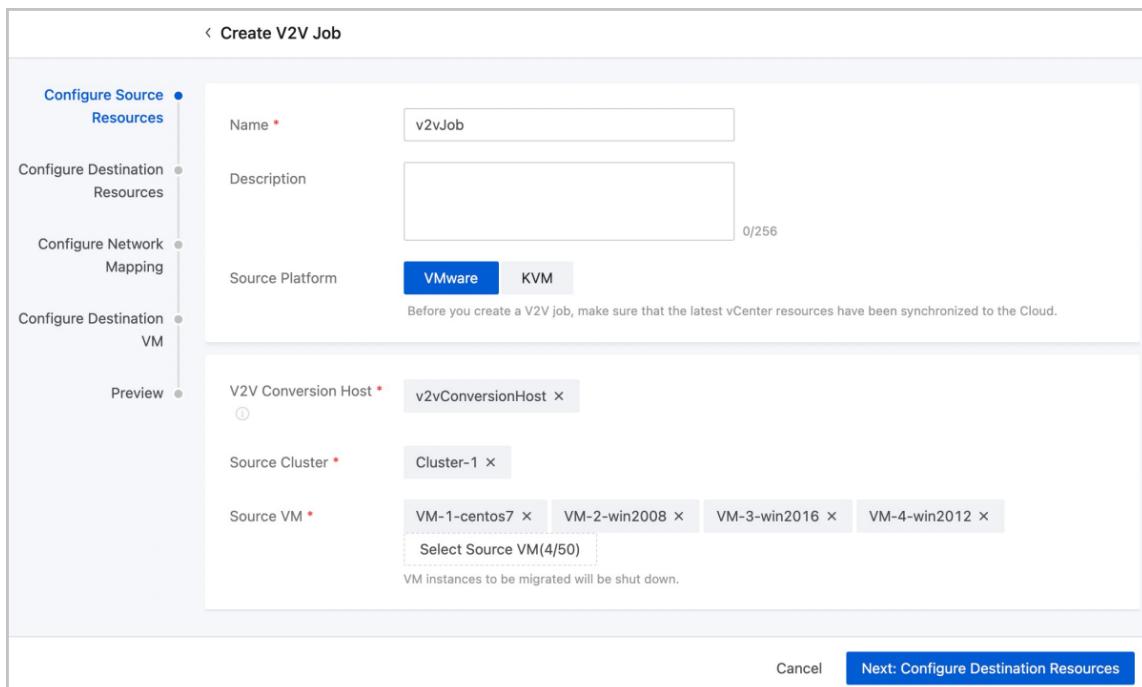


Note:

- If you select more than one VM instance, corresponding V2V jobs will be created in bulk. Note that one V2V job corresponds to one source VM instance.
- For Windows Server 2012 R2 and Windows Server 2016 VM instances, you need to manually disable the hibernation feature and shut down these VM instances before you create V2V jobs.

To disable or enable the Windows hibernation feature, run the following commands:

- Disable Windows hibernation: cmd--> "powercfg -h off"
- Enable Windows hibernation: cmd--> "powercfg -h on"
- If one of the source VM instances has a data volume, make sure that the disk mode of the data volume is Dependent. Otherwise, the V2V job might fail.

Figure 6-2: Configure Source Resources

b) Configure destination resources.

Set the following parameters:

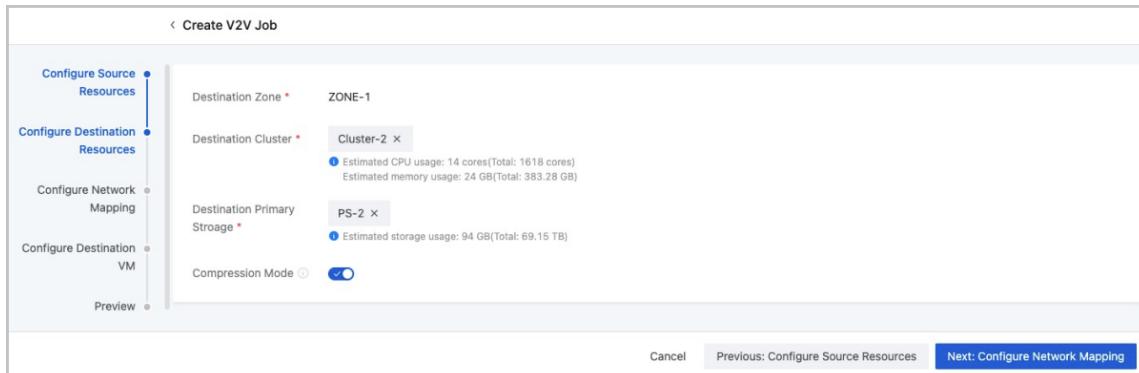
- **Destination Zone:** By default, the current zone is displayed.
- **Destination Cluster:** Select a destination cluster. Then, the estimated CPU usage and memory usage are displayed.
 - Estimated CPU usage: displays the number of the used CPUs of the source VM instance and the total number of available CPUs in the destination cluster.
 - Estimated memory usage: displays the used memory size of the source VM instance and the total available memory size in the destination cluster.
- **Destination Primary Storage:** Select a destination primary storage. Then, the estimated primary storage usage is displayed.
 - Estimated storage usage: displays the used storage of the source VM instance and the total available storage of the destination primary storage.
- **Compression mode:** Choose whether to enable the compression mode. By default, the compression mode is enabled.



Note:

- Enabling the compression mode compresses the caches of the migration data and improves the cache space utilization of the V2V conversion host.
- If the destination primary storage is Ceph, we recommend that you do not use the compression mode.

Figure 6-3: Configure Destination Resources



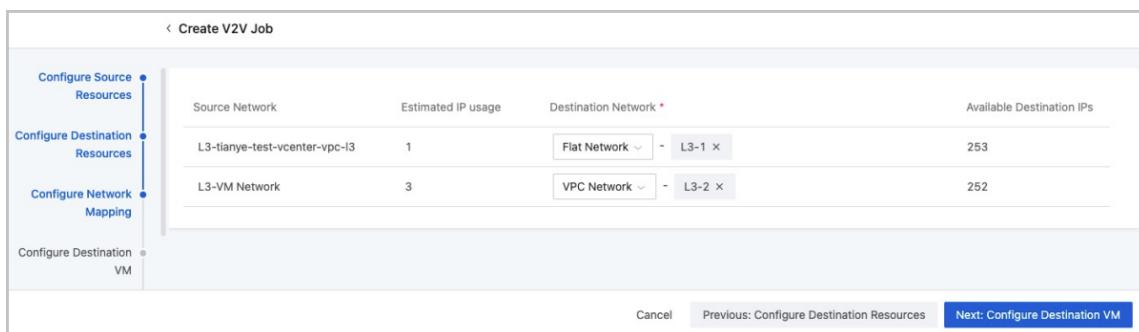
c) Configure network mapping.

In this scenario, all the chosen VM instances have a NIC attached.

Set the following parameters:

- Destination Network:** Select a destination network as needed. The destination network is the network attached to the specified destination cluster.

Figure 6-4: Configure Network Mapping | Source VMs Have NIC Attached



d) Configure destination VM instances.

Parameters of the destination VM instances are configured by the system by default.

Therefore, go to the next step if no further modification is needed.

You can also configure the destination VM instances by setting the following parameters:

- **Start VM After Migration:** Choose whether to automatically start the destination VM instance after the migration.
- **Use Source MAC and IP:** Choose whether to use the source MAC and IP addresses. By default, these addresses are not used.

**Note:**

- If not used, you can customize the MAC and IP addresses for the destination NIC. If you do configure them, the destination MAC address will be the same as the source MAC address after migration, and the IP address of the destination NIC will be allocated by the system.
- If used, the destination NIC will use the MAC and IP addresses of the source NIC in the next step. If the source NIC does not have an IP address, the IP address of the destination NIC will be allocated by the system.

- **VM Configuration:** Select the VM instance to be configured. You can configure the VM instance by setting the following parameters:

— **Name:** Set the name of the destination VM instance.

— **NIC:** Configure the NIC information.

■ **Network:** Select the network for the destination VM instance.

■ **IP Address:** Optional. Configure the IP address of the destination NIC.

**Note:**

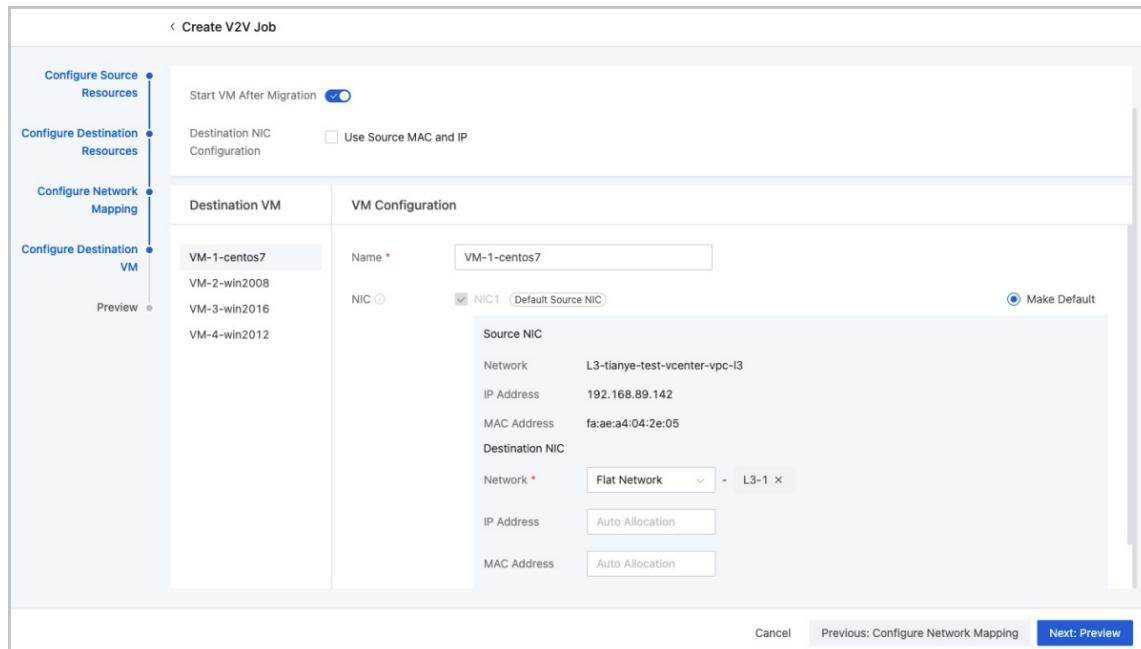
If not configured, the IP address of the destination NIC will be allocated by the system.

■ **MAC Address:** Optional. Configure the MAC address of the destination NIC.

**Note:**

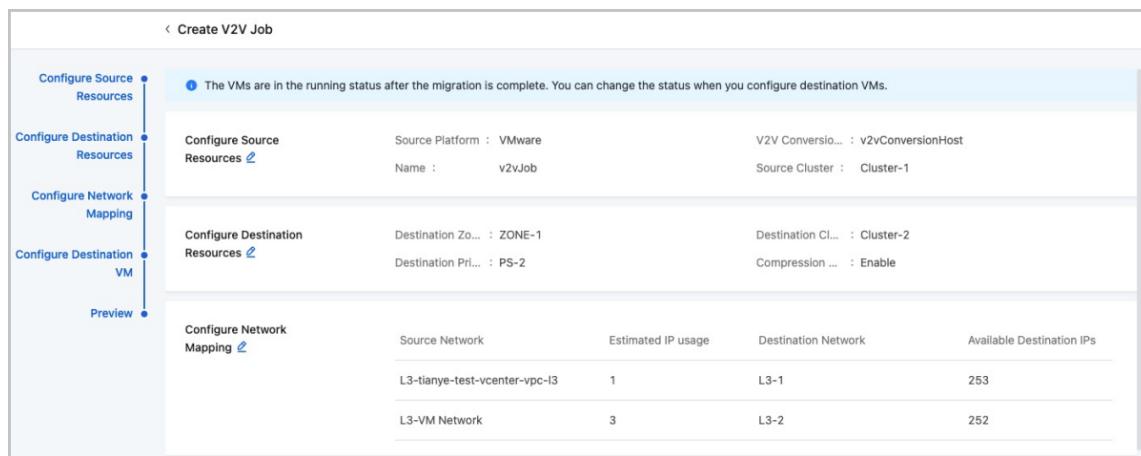
If not configured, the MAC address of the destination NIC will be the same as that of the source NIC after migration.

- **Boot Partition:** If the VM instance to be migrated has multiple boot partitions, specify one as the root volume for the VM instance.

Figure 6-5: Configure Destination VMs / VMs Have NIC Attached

e) Confirm and submit.

Confirm the information about the V2V job. You can modify the information by clicking the **Edit** icon next to each step.

Figure 6-6: Confirm and Submit

Configure Destination VM		Destination VM	NIC Name	Source NIC Info		Destination NIC Information		
VM-1-centos7		VM-1-centos7	NIC-1 Default NIC	Network : L3-tianye-test-vcenter-v... IP Address : 192.168.89.142 MAC Address : fa:ae:a4:04:2e:05	Network : Flat Network-L3 IP Address : Auto Allocation MAC Address : Auto Allocation			
VM-2-win2008		VM-2-win2008	NIC-1	Network : L3-VM Network IP Address : Nothing obtained MAC Address : 00:50:56:9d:0b:1e	Network : VPC Network-L3 IP Address : Auto Allocation MAC Address : Auto Allocation			
VM-3-win2016		VM-3-win2016	NIC-1 Default NIC	Network : L3-VM Network IP Address : Nothing obtained MAC Address : 00:50:56:9d:8c:d7	Network : VPC Network-L3 IP Address : Auto Allocation MAC Address : Auto Allocation			
VM-4-win2012		VM-4-win2012	NIC-1 Default NIC	Network : L3-VM Network IP Address : Nothing obtained MAC Address : 00:50:56:9d:d3:57	Network : VPC Network-L3 IP Address : Auto Allocation MAC Address : Auto Allocation			

Cancel Previous: Configure Destination VM OK

What's next

So far, we introduced the VMware-based V2V migration practice.

6.2 Source Cloud Platform: KVM

Context

Scenario: Due to business needs, you need to migrate VM instances from your KVM cloud platform to the current cloud. Assume that:

- You deployed a KVM-based open-source cloud platform and the latest ZStack Cloud Private Cloud.
- You prepared a storage server and added it to the destination cluster as a compute node. You use this compute node as the V2V conversion host.
- You purchased and installed the Migration Service module.

The following table lists the information about the source and the destination cloud platform.

Source Cloud Platform	Destination Cloud Platform
An open-source, KVM-based cloud platform <ul style="list-style-type: none"> • Primary storage type: SAN storage • Number of appliance VMs: 4 	ZStack Cloud Private Cloud <ul style="list-style-type: none"> • Version: the latest version • Primary storage type: SharedBlock • Network: public network

The workflow is as follows:

1. Add a V2V conversion host.

2. Create a V2V job to migrate the 4 VM instances from the KVM cloud platform to the current cloud.

Procedure

1. Add a V2V conversion host.

In this scenario, you will add a compute node prepared in the destination cluster as the V2V conversion host.

On the main menu of ZStack Cloud, choose **Platform O&M > Migration Service > V2V Conversion Host**. On the **V2V Conversion Host** page, click **Add V2V Conversion Host**. Then, the **Add V2V Conversion Host** page is displayed.

On the displayed page, set the following parameters:

- **Name:** Enter a name for the V2V conversion host.
- **Description:** Optional. Enter a description for the V2V conversion host.
- **Type:** Select KVM Platform.



Note:

The type of the V2V conversion host must be consistent with that of the source platform you selected when you create a V2V job.

- **Host:** Select a host from the destination cluster as the V2V conversion host.



Note:

A host cannot be used as a V2V conversion host for both the VMware platform type and the KVM platform type at the same time.

- **Cache Path:** Enter a local path on the V2V conversion host as the storage path.



Note:

During the V2V migration, the VM system and data are first cached in the V2V conversion host and then imported into the target primary storage.

- **Migration Network:** Optional. If you deployed an independent network for V2V migration, enter the CIDR of the network.



Note:

- If you deployed an independent network for V2V migration, you could add the network to the Cloud directly.
 - In a V2V migration scenario, the migration network is used to convert data migrated from the destination primary storage to the V2V conversion host.
 - Using an independent migration network can avoid network congestion and improve transmission efficiencies.
 - If not set, the management network will be used by default for V2V migration.
- **Upstream Bandwidth:** Optional. Set the upstream bandwidth of the V2V conversion host. This parameter limits the speed of uploading data from the V2V conversion host to the destination primary storage. The upstream bandwidth must be an integer ranging from 1 Mbps to 32 Gbps. Unit: Mbps and Gbps.
- **Downstream Bandwidth:** Optional. Set the downstream bandwidth for the V2V conversion host. This parameter limits the speed of downloading data from the source primary storage to the V2V conversion host. The downstream bandwidth must be an integer ranging from 1 Mbps to 32 Gbps. Unit: Mbps and Gbps.

Figure 6-7: Add V2V Conversion Host

The screenshot shows the 'Add V2V Conversion Host' dialog box. The 'Name' field is populated with 'v2vConversionHost-KVM'. The 'Description' field is empty. Under the 'Type' section, 'KVM Platform' is selected. The 'Host' field contains 'DELL-EMC-47'. The 'Cache Path' field is set to '/v2v'. The 'Migration Network' field shows '172.20.1.0/24'. The 'Upstream Bandwidth' field has '1' in the input box and 'Gbps' in the dropdown menu. The 'Downstream Bandwidth' field also has '1' in the input box and 'Gbps' in the dropdown menu. At the bottom right of the dialog are 'Cancel' and 'OK' buttons.

2. Create a V2V migration job to migrate 4 KVM instances from the source cloud platform to the current cloud.

On the main menu of ZStack Cloud, choose **Platform O&M > Migration Service > V2V Migration**. On the **V2V Migration** page, click **Create V2V Job**. Then, the **Create V2V Job** page is displayed.

- a) Configure the source resources.

Set the following parameters:

- **Name:** Enter a name for the V2V job.
- **Description:** Optional. Enter a description for the V2V job.
- **Source Platform:** Select KVM.
- **V2V Conversion Host:** Select a V2V conversion host of the KVM type you added before.
- **Source Host IP:** Enter the IP address of the source host.
- **Source Host SSH Port:** Set the SSH port of the source host. Default: 22.
- **SSH Username:** Enter the username. Default: root.
- **SSH Password:** Enter the corresponding SSH password.
- **Virsh Info:** If not selected, the virtual resources of the source host are not remotely accessed through virsh.
- **Source VM Info:** Obtain information about the running or paused VM instances that are available for migration.
- **Source VM:** Select four KVM instances from the source host.



Note:

- Do not power off the VM instances to be migrated.
 - If you select more than one VM instance, corresponding V2V jobs will be created in bulk. Note that one V2V job corresponds to one source VM instance.
- **Pause VM:** If selected, the source VM instances will be paused when a V2V job starts.

Figure 6-8: Configure Source Resources

The screenshot shows the 'Create V2V Job' interface with the 'Configure Source Resources' step selected. The 'Source Platform' is set to KVM. The 'V2V Conversion Host' is 'v2vConversionHost-KVM'. The 'Source Host IP' is '172.20.1.51', 'Source Host SSH Port' is '22', and 'SSH Username' is 'root'. The 'SSH Password' option is selected. In the 'Source VM Info' section, there is a list of VM instances: '52361ea66e3947e985ec5...', '80db64f2b63d47c68709a3...', '487e60dacbed44ddda0f6ae...', and 'b814f4415533438a88a252...'. A note says '17 running or paused VM instances on the selected source host can be migrated.' There is also a 'Select Source VM(4/50)' button and a checkbox for 'Do not stop VM instances to be migrated.' At the bottom, there are 'Cancel' and 'Next: Configure Destination Resources' buttons.

b) Configure the destination resources.

Set the following parameters:

- **Destination Zone:** By default, the current zone is displayed.
- **Destination Cluster:** Select a destination cluster. Then, the estimated CPU usage and memory usage are displayed.
 - Estimated CPU usage: displays the number of the used CPUs of the source VM instance and the total number of available CPUs in the destination cluster.
 - Estimated memory usage: displays the used memory size of the source VM instance and the total available memory size in the destination cluster.
- **Destination Primary Storage:** Select a destination primary storage. Then, the estimated primary storage usage is displayed.
 - Estimated storage usage: displays the used storage of the source VM instance and the total available storage of the destination primary storage.

- **Compression mode:** Choose whether to enable the compression mode. By default, the compression mode is enabled.

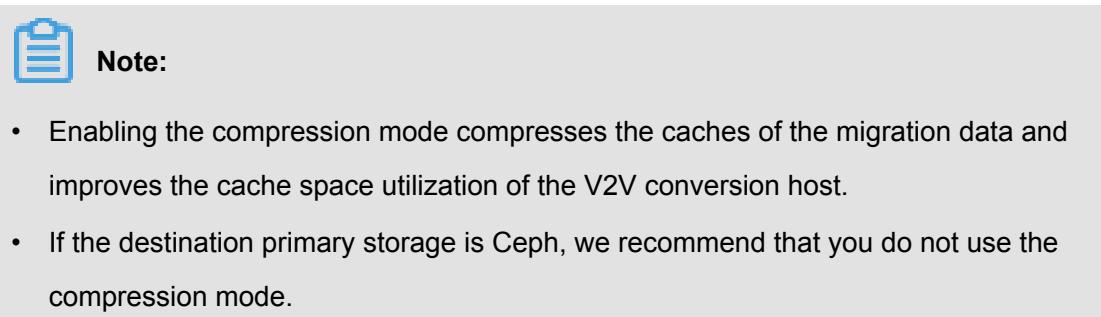
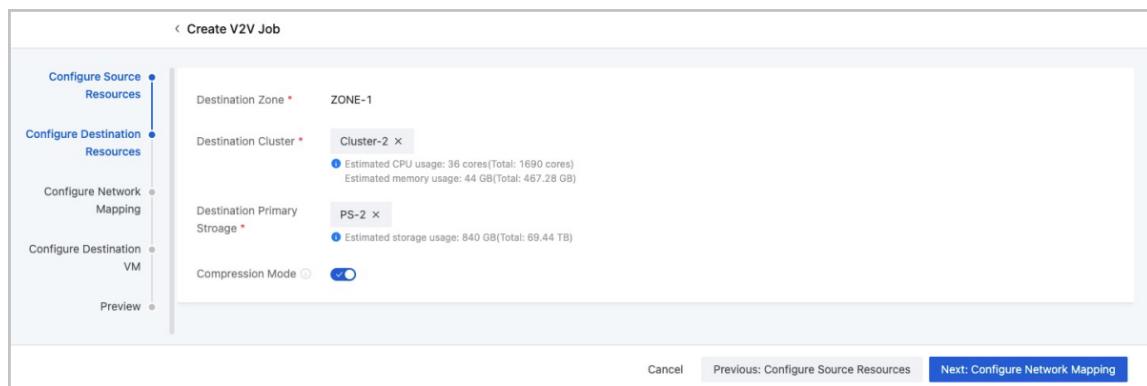


Figure 6-9: Configure Destination Resources



c) Configure the network mapping.

In this scenario, a chosen VM instance does not have a NIC attached.

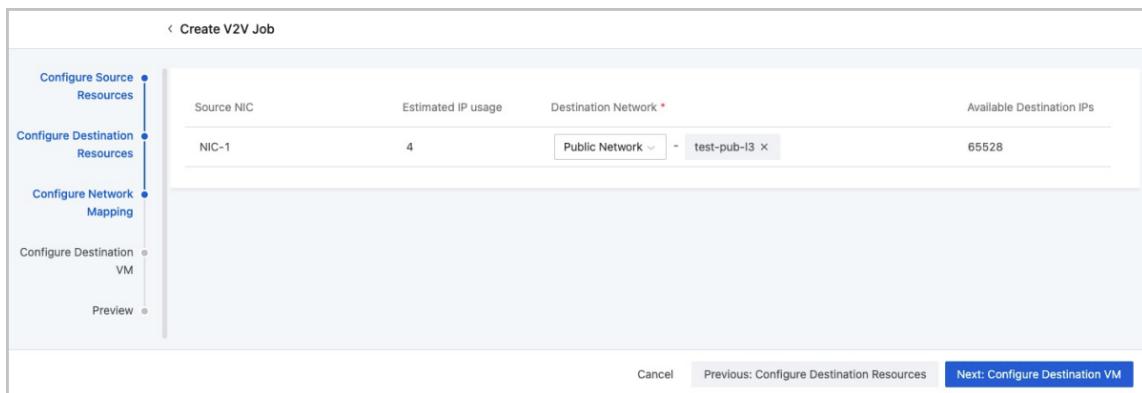
1. For the source VM instance that has a NIC attached,

Set the following parameters:

- **Destination Network:** Select a destination network as needed. The destination network is the network attached to the specified destination cluster.

2. For the source VM instance that does not have a NIC attached,

Go to the next step to manually configure the destination NIC.

Figure 6-10: Configure Network Mapping

d) Configure destination VM instances.

configure the destination VM instance by setting the following parameters:

- **Start VM After Migration:** Choose whether to automatically start the destination VM instance after the migration.
- **VM Configuration:** Select the VM instance to be configured. You can configure the VM instance by setting the following parameters:
 - **Name:** Set the name of the destination VM instance.
 - **NIC:** Configure the NIC information.
 - **Network:** Select the network for the destination VM instance.
 - **IP Address:** Optional. Configure the IP address of the destination NIC.



Note:

If not configured, the IP address of the destination NIC will be allocated by the system.

- **MAC Address:** Optional. Configure the MAC address of the destination NIC.



Note:

If not configured, the MAC address of the destination NIC will be the same as that of the source NIC after migration.

- **Boot Partition:** If the VM instance to be migrated has multiple boot partitions, specify one as the root volume for the VM instance.



Note:

Before you migrate a VM instance to the current cloud, make sure that the VM instance has at least one NIC attached.

Figure 6-11: Configure Destination VMs

The screenshot shows the 'Create V2V Job' interface with the 'Configure Destination VM' step selected. On the left, a vertical navigation bar lists steps: 'Configure Source Resources', 'Configure Destination Resources', 'Configure Network Mapping', 'Configure Destination VM', and 'Preview'. The 'Configure Destination VM' step is highlighted. A 'Start VM After Migration' toggle switch is turned on. The main area displays 'Destination VM' details and 'VM Configuration' settings. Under 'VM Configuration', the 'Name' is set to '52361ea66e3947e985...', 'CPU' is 8 Cores, 'Memory' is 16 GB, 'Platform' is Linux, and 'VirtIO' is enabled. Under 'Volume', three volumes are listed: 'vda' (Root Volume 100 GB), 'sdb' (Data Volume 100 GB), and 'sdd' (Data Volume 100 GB). Under 'NIC', 'NIC1' is selected with 'Network' set to 'Public Network'. At the bottom, there are 'Cancel', 'Previous: Configure Network Mapping', and 'Next: Preview' buttons.

a) Confirm and submit.

Confirm the information about the V2V job. You can modify the information by clicking the **Edit** icon next to each step.

Figure 6-12: Confirm and Submit

Create V2V Job

The VMs are in the running status after the migration is complete. You can change the status when you configure destination VMs.

Configure Source Resources	Source Platform : KVM Name : v2vJob-KVM Source Host S... : 22	V2V Conversio... : v2vConversionHost-KVM Source Host IP : 172.20.1.51		
Configure Destination Resources	Destination Zo... : ZONE-1 Destination Pri... : PS-2	Destination Cl... : Cluster-2 Compression ... : Enable		
Configure Network Mapping	Configure Network Mapping			
Configure Destination VM	Source NIC NIC-1	Estimated IP usage 4	Destination Network test-pub-l3	Available Destination IPs 65528
Preview	Configure Destination VM			
	Destination VM	Destination Volume Information	Destination NIC Information	
	Name : 52361ea66e3947e9... CPU : 8 Memroy : 8GB Platform : △ Linux VirtIO : Enable	vda Root Volume 100 GB sdb Data Volume 100 GB sdd Data Volume 100 GB	NIC1 Default NIC Network : Public Network-test-... IPv4 Address : Auto Allocation MAC Address : fa:e6:ba:27:c3:00	
	Name : 487e60dacbed44dd... CPU : 8 Memroy : 8GB Platform : △ Linux VirtIO : Enable	vda Root Volume 100 GB	NIC1 Default NIC Network : Public Network-test-... IPv4 Address : Auto Allocation MAC Address : fa:98:8d:03:bc:00	
	Name : b814f4415533438a... CPU : 12 Memroy : 12GB Platform : △ Linux VirtIO : Enable	vda Root Volume 200 GB	NIC1 Default NIC Network : Public Network-test-... IPv4 Address : Auto Allocation MAC Address : fa:da:69:ce:a1:00	

Cancel Previous: Configure Destination VM OK

What's next

So far, we introduced the KVM-based V2V migration practice.

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 an 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.