

Upgrade 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.....	I
1 Overview.....	1
2 Considerations.....	2
3 Preparations.....	5
4 Typical Upgrading Processes.....	6
4.1 Single-Management Node Upgrading.....	6
4.2 Multi-Management Node Upgrading.....	8
Glossary.....	10

1 Overview

To upgrade a cloud platform, you need to upgrade the management node, compute nodes, storage nodes, and network nodes to the latest version and update basic software packages, software library dependencies, and core virtualization tools. This document describes how to upgrade ZStack Cloud.

Limitations

This document applies to cloud platform upgrading of the same repo, which means that the operating system (OS) version of the hosts is consistent with the management nodes. For example, the OS of the hosts and management nodes on the Cloud is CentOS 7.6.

**Note:**

If you need to upgrade host OS or upgrade the cloud platform of multiple repos, contact the official technical support for help.

Upgrading Mechanism

ZStack Cloud provides the following upgrading mechanisms:

- Seamless upgrading: seamlessly upgrades ZStack Cloud of any old version to the latest.
- Lossless upgrading: does not affect the services that VM instances are running during ZStack Cloud upgrading.

2 Considerations

When you upgrade ZStack Cloud, note that:

- During the upgrading, the management nodes are inaccessible and you cannot apply VM and volume resources. Therefore, we recommend that you upgrade the cloud platform during business troughs to avoid resource application and business change needs.
- After the management node upgrading is completed, all hosts, primary storages, backup storages, VPC vRouters are reconnected and related resources are auto-upgraded. During the connection, you cannot perform operations on VM instances and volumes.
- If an error occurs during the upgrading and interrupts the upgrading, you can troubleshoot the error. After the error is solved, you can upgrade the cloud platform again.
- Starting from ZStack Cloud 4.3.12, the QEMU version is automatically upgraded from 2.12 to 4.2.
 - If you deploy a new Cloud by using the ISO of 4.3.12 or a later version, QEMU 4.2 is installed by default. If you upgrade your Cloud to 4.3.12 or a later version, QEMU 2.12 is used by default.
 - To use the Cloud properly, make ensure that all hosts in the same cluster use the same QEMU version. Therefore, if you upgrade your Cloud to 4.3.12 or a later version, you could not expand the capacity by adding hosts (installed using the ISO of 4.3.12 or a later version) to the existing cluster. To expand the capacity, use a new cluster.
- Starting from ZStack Cloud 4.0.0, we bring you the following enhancements:
 - vRouter is upgraded to VPC vRouter.

Starting from 4.0.0, vRouter is upgraded to VPC vRouter and vRouter network is upgraded to VPC network. vRouter is no longer available on the UI. The seamless upgrade does not affect your business continuity.
 - User Group and User are replaced by Enterprise Management Account System.

Starting from 4.0.0, User Group and User are replaced by Enterprise Management Account System. User Group and User are no longer available on the UI. You cannot login to the Cloud by using a user or user group account. Before you implement upgrading, migrate the user and user group account data to Enterprise Management.

**Note:**

User accounts created by the admin and have the admin permissions are also cancelled. Platform admins in Enterprise Management have the equivalent permissions. You can use Enterprise Management to create platform managers based on your business needs.

- The integration of AD/LDAP and accounts is adjusted.

Starting from 4.0.0, the integration of AD/LDAP and accounts is managed by Enterprise Management. Before you implement upgrading, migrate the AD/LDAP account data managed by the original account system to Enterprise Management.

- Starting from ZStack Cloud 3.9.0, if you use c74 ISO and QEMU 2.9, the libvirt version is automatically upgraded to 4.9.0.
 - If you use open-source Ceph distributed storage and enable the CEPHX (Ceph authentication) feature, when you hot-plug VM CD-ROM, an error may occur because libvirt of the new version does not support hot plugging. You can contact the official technical support when necessary.
 - Starting from 3.2.0, libvirt updates the format of shared volumes to raw. Therefore, when you create a shared volume, the format of the volume is raw. This type of volume does not allow you to create snapshots and resize capacities, or create images for powered-on VM instances to which this type of volume is attached. In later versions of ZStack Cloud, these limitations will be eliminated.
 - The libvirt auto-upgrading feature is enabled by default. You can disable the feature by using the following method:

Enter `/usr/local/zstack/apache-tomcat/webapps/zstack/WEB-INF/classes/` and set the following parameter in the **zstack.properties** configuration file:

```
updatePkgWhenConnect = false
# Disable libvirt auto-upgrading.
```

Restart the management node to make the modification take effect.

- Starting from ZStack Cloud 3.7.1, ISO of the c76 and c74 editions are available and multiple repos are supported. When you upgrade the cloud platform, note that:
 - Starting from 3.7.1, ISO of the c72 edition is no longer used for installation and deployment of the new cloud platform. If you need to expand the capacity or upgrade the operating system, contact the official technical support for help.

- Starting from 3.7.1, the local repo of ISO of the c72 edition is redirected to ISO of the c74 edition. If you use offline upgrading, you need to obtain ISO of the c74 edition to update the local repo.

3 Preparations

When you upgrade the cloud platform, you may need the following software packages. Before the upgrading, prepare the packages based on your needs:

- ZStack Cloud custom ISO:
 - C76: ZStack-Cloud-x86_64-DVD-4.3.12-c76.iso
 - Download address: [Click here](#)
- ZStack Cloud installation package:
 - Software: ZStack-Cloud-installer-4.3.12.bin
 - Download address: [Click here](#)
- Upgrade script:
 - Software: ZStack-upgrade
 - Download address: [Click here](#)
- Multi-MN-HA:
 - Software: ZStack-Multinode-HA-Suite-4.3.12.tar.gz
 - Download address: [Click here](#)

**Note:**

After you download the software packages or scripts, check the MD5 hash of the packages or scripts. If the MD5 hash is inconsistent with that on the official website, download again.

4 Typical Upgrading Processes

ZStack Cloud provides single-management node and multi-management node deployment methods. The two deployment methods have different upgrading processes.

- For more information about single-management node upgrading, see [Single-Management Node Upgrading](#).
- For more information about multi-management node upgrading, see [Multi-Management Node Upgrading](#).

4.1 Single-Management Node Upgrading

Context

ZStack Cloud provides ISO of two editions: c76 and c74. The upgrading process of ISO of the c74 edition is the same as the upgrading process of ISO of the c76 edition. This topic takes c76 ISO as an example to describe the upgrading process of a single-management node platform.

Procedure

1. Obtain software packages for upgrading.

See [Preparations](#) to obtain the packages you need and save the packages in the `/root/` directory.

- Incremental upgrading requires connection to the public network.
- Offline upgrading does not require connection to the public network but requires the bin package, ISO package, and upgrade script.

2. Disable VM HA globally.

Login to the UI, choose **Settings > Platform Setting > Global Setting > Advanced** and set **VM HA** to **false**.

3. Back up the database and upgrading script.

Before you upgrade the cloud platform, back up the database and upgrading script, in case of any unexpected situations.

- Run the following command on the management node to back up the database in the `/var/lib/zstack/mysql-backup/` directory:

```
[root@localhost ~]# zstack-ctl dump_mysql --file-name zstack-db-backup
```

- Run the following command on the management node to back up the upgrading script in the `/root/` directory:

```
[root@localhost ~]# cp /usr/local/bin/zstack-upgrade /root/zstack-upgrade-bk
```

4. Upgrade the cloud platform.

You can upgrade the cloud platform by using the incremental upgrading or offline upgrading method:

- Run the following command on the management node to implement incremental upgrading:

```
[root@localhost ~]# bash ZStack-Cloud-installer-4.3.12.bin -u -P MySQL_ROOT_PASSWORD
```



Note:

If the root password of the database is the default password, you do not need to specify `-P MySQL_ROOT_PASSWORD`.

- Run the following commands on the management node to implement offline upgrading:

```
[root@localhost ~]# bash zstack-upgrade -r ZStack-Cloud-x86_64-DVD-4.3.12-c76.iso
[root@localhost ~]# bash ZStack-Cloud-installer-4.3.12.bin -u -P MySQL_ROOT_PASSWORD
```



Note:

If the root password of the database is the default password, you do not need to specify `-P MySQL_ROOT_PASSWORD`.

5. Clean up the browser cache.

To make sure that the upgraded platform works as expected, after the upgrading is completed, you need to login to the UI platform and press `Ctrl+F5` or `Ctrl+Shift+R` to clean up the browser cache.

6. Enable VM HA globally.

Login to the UI, choose **Settings > Platform Setting > Global Setting > Advanced** and set **VM HA** to **true**.

4.2 Multi-Management Node Upgrading

Context

ZStack Cloud provides ISO of two editions: c76 and c74. The upgrading process of ISO of the c74 edition is the same as the upgrading process of ISO of the c76 edition. This topic takes c76 ISO as an example to describe the upgrading process of a multi-management node platform.

Procedure

1. Obtain software packages for upgrading.

See [Preparations](#) to obtain the ISO package, bin package, upgrading script, multi-MN-HA you need and save the packages or scripts in the `/root/` directory of the management nodes.

2. Disable VM HA globally.

Login to the UI, choose **Settings > Platform Setting > Global Setting > Advanced** and set **VM HA** to **false**.

3. Back up the database and upgrading script.

Before you upgrade the cloud platform, back up the database and upgrading script, in case of any unexpected situations.

- Run the following command on the management nodes respectively to back up the database in the `/var/lib/zstack/mysql-backup/` directory:

```
[root@localhost ~]# zstack-ctl dump_mysql --file-name zstack-db-backup
```

- Run the following command on the management nodes respectively to back up the upgrading script in the `/root/` directory:

```
[root@localhost ~]# cp /usr/local/bin/zstack-upgrade /root/zstack-upgrade-bk
```

4. Update the local repo.

Run the following command on the management nodes respectively to update the local repo:

```
[root@localhost ~]# bash zstack-upgrade -r ZStack-Cloud-x86_64-DVD-4.3.12-c76.iso
```

5. Obtain the IP address of the management node that corresponds to the VIP you use.

Run the following command to obtain the IP address of the management node that corresponds to the VIP you use. The management node that corresponds to the **yes** result is the management node you need:

```
[root@localhost ~]# zsha2 status
```

6. Decompress the Multi-MN-HA file and grant the decompressed files execution permission.

Run the following commands on the management node that corresponds to the VIP you use to decompress the Multi-MN-HA file and grant the decompressed files *zsha2* and *zstack-hamon* execution permission:

```
[root@localhost ~]# tar zxvf ZStack-Multinode-HA-Suite-4.3.12.tar.gz
#Decompress the Multi-MN-HA file
[root@localhost ~]# chmod +x zsha2 zstack-hamon      #Grant the
decompressed files execution permission
```

7. Upgrade Multi-MN-HA

Run the following command on the management node that corresponds to the VIP you use to upgrade Multi-MN-HA:

```
[root@localhost ~]# ./zsha2 upgrade-ha
```

8. Upgrade the cloud platform.

Run the following command on the management node that corresponds to the VIP you use to upgrade the management nodes:

```
zsha2 upgrade-mn -peerpass password ZStack-Cloud-
installer-4.3.12.bin
```



Note:

-peerpass is optional. You can use the parameter to set the password of SSH login to the peer management nodes.

9. Clean up the browser cache.

To make sure that the upgraded platform works as expected, after the upgrading is completed, you need to login to the UI platform and press **Ctrl+F5** or **Ctrl+Shift+R** to clean up the browser cache.

10. Enable VM HA globally.

Login to the UI, choose **Settings > Platform Setting > Global Setting > Advanced** and set **VM HA** to **true**.

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.