

OpenStack Architecture



Foreword

- This course describes the origin, version evolution, and functions of OpenStack, the overall architecture of OpenStack, its core components, and the differences between OpenStack and virtualization and cloud computing.

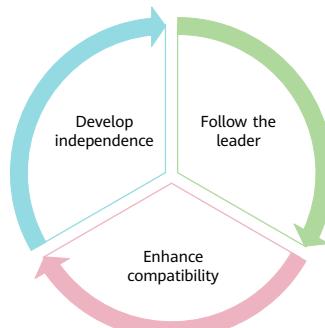
Objectives

- Upon completion of this course, you will understand:
 - The origin, version evolution, and functions of OpenStack.
 - OpenStack architecture and its components.
 - Differences between virtualization and cloud computing.

Contents

- 1. OpenStack Overview**
2. OpenStack Architecture
3. OpenStack Core Services
4. Interactions Between OpenStack Projects

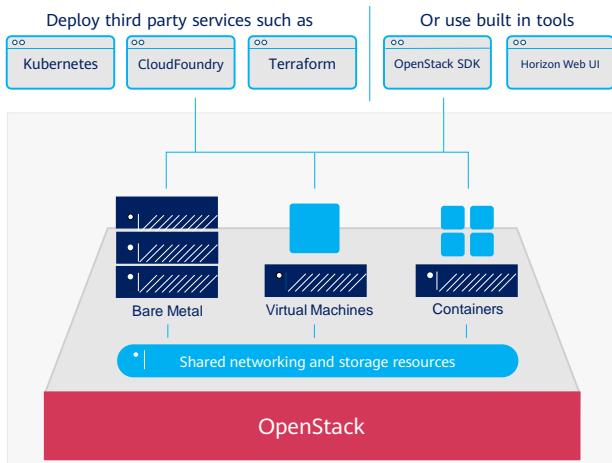
Origin of OpenStack



- In 2006, Amazon launched Amazon Web Services (AWS), which opened a new chapter in the history of cloud computing.
- National Aeronautics and Space Administration (NASA) and Rackspace together launched OpenStack as an open source cloud software project in July 2010.
- OpenStack has been learning from AWS since its birth and provides open interfaces compatible with various AWS services.

- The development of OpenStack is closely related to cloud computing. It is well known that Amazon is the first vendor to propose the concept of cloud computing, which is driven by its business model at that time. Amazon is the world's most well-known e-commerce website. During peak hours, e-commerce transactions require great computing power. However, such great computing power is not required during off-peak hours, so Amazon tried to open the idle computing power to users. After a period of development, cloud computing was widely recognized in 2006. Amazon Web Services (AWS) launched the Elastic Compute Cloud (EC2) service, which has high scalability and has attracted the attention of many vendors.
- NASA has also been studying services that provide similar functions, but they met technical challenges.
- Rackspace was the second largest cloud computing vendor in the United States at that time, but its scale was only 5% of that of Amazon.
- NASA and Rackspace decided to open source OpenStack and leverage the power of the community to enhance OpenStack functions. OpenStack began in 2010 as a joint project of Rackspace and NASA. The vision of OpenStack is to build a cloud operating system for data centers to greatly improve the operating efficiency of the data centers.
- AWS provides powerful functions and is still developing. OpenStack has been learning from AWS since its birth and provides open interfaces compatible with various AWS services.
- Although OpenStack does not provide as complete sets of services as AWS at present, OpenStack is an open-source project and does not charge copyright fees.

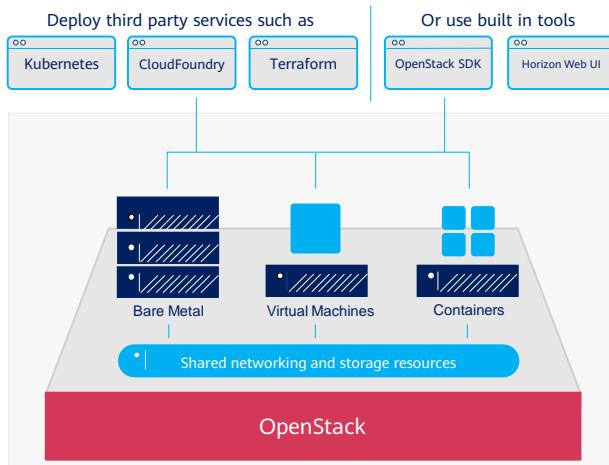
What Is OpenStack?



- It provides a cloud infrastructure for virtual machines (VMs), bare metal, and containers.
- It controls large pools of compute, storage, and network resources.
- It manages all resources through APIs or a dashboard.

- OpenStack is a cloud operating system that controls large pools of compute, storage, and network resources throughout a data center, all managed and provisioned through APIs with common authentication mechanisms. A dashboard is also available, giving administrators control while empowering their users to provision resources through a web interface.

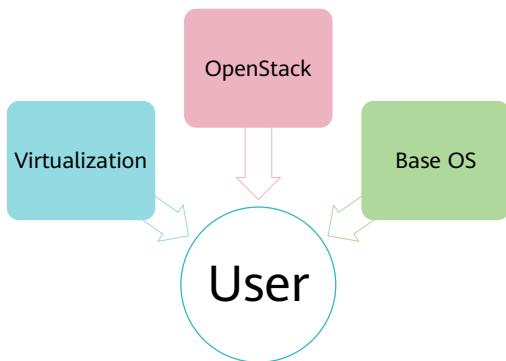
What Can OpenStack Do?



- OpenStack provides an Infrastructure as a Service (IaaS) solution through a variety of complementary services. Each service offers an Application Programming Interface (API) to facilitate integration.
- The OpenStack project is an open source cloud computing platform that supports all types of cloud environments. The project aims for simple implementation, massive scalability, and a robust feature set.

- OpenStack is a community, a project, and open-source software application. It provides open-source software for building public and private clouds. It also provides a cloud platform or tool set to deploy clouds and helps organizations run clouds that provide services for virtual computing or storage, providing scalable and flexible cloud computing for public clouds, private clouds, big clouds, and small clouds.
- As an open-source cloud computing management platform, OpenStack consists of multiple main components. OpenStack supports almost all types of cloud environments. It aims to provide a cloud computing management platform featuring simple implementation, massive scalability, a rich set of functions, and unified standards. OpenStack provides an Infrastructure as a Service (IaaS) solution through a variety of complementary services. Each service provides an API for integration.

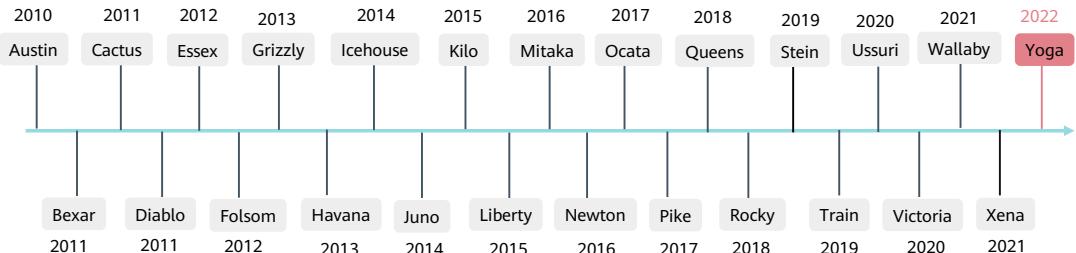
How Does OpenStack Work?



- OpenStack is essentially a series of commands compiled into scripts. Those scripts are bundled into packages called projects that relay tasks that create cloud environments.
- In order to create those environments, OpenStack relies on two other types of software:
 - Virtualization software creates a layer of virtual resources abstracted from hardware.
 - A base operating system (OS) carries out commands given by OpenStack scripts.
- OpenStack itself does not virtualize resources, but rather uses them to build a cloud.
- All the three technologies — OpenStack, virtualization, and the base OS — must work together.

Open-Source OpenStack Version Evolution

- OpenStack releases two major versions each year, generally in April and mid-October. The versions are named from A to Z.



- The first release of OpenStack is code-named Austin, which is named after the capital of Texas, where Rackspace is located. A new version is planned to be released every several months and named in the sequence of 26 English letters from A to Z. The releases are usually named after the geographic region where the summit is held.
- In 2017, Huawei has become the first Asian vendor to be elected as a platinum member of the OpenStack Foundation.
- The OpenStack Foundation allows a maximum of eight platinum members and 24 gold members. In addition to Huawei, platinum members include AT&T, Ericsson, Intel, Rackspace, Red Hat, SUSE, and Tencent. Gold members include 99Cloud, China Mobile, China Telecom, China Unicom, Cisco, EasyStack, FiberHome, Inspur, H3C, ZTE, and more.

OpenStack Design Principles

Open

- Make everything open-source.
- Reuse existing open-source projects.

Flexible

- Use tailorable architecture.
- Design and implement functions using plug-ins.

Scalable

- Include multiple independent projects.
- Use multiple independent components in each project.
- Use a decentralized architecture.
- Use a stateless architecture.

- Open:
 - The source code and the design and development processes are open.
 - Do not reinvent the wheel but stand on the shoulders of giants.
 - No irreplaceable private or commercial component is used.
- Flexible:
 - Tailored architecture and customizable component scope.
 - A large number of drivers and plug-ins.
 - Easy configuration of system functions and features based on configuration items.
- Scalable:
 - Loosely coupled architecture: Components communicate with each other through RESTful APIs, and message bus communication is used within a component.
 - Decentralized architecture: Core components do not have central nodes, effectively preventing single points of failure.
 - Stateless architecture: Components do not have local persistent data. All persistent data is stored in the database.

OpenStack and Virtualization

- OpenStack only functions as a control plane. It does not contain the components of a system data plane, like hypervisors and storage and network devices.
- Virtualization is one of the underlying technologies of OpenStack, but is not a core concern of OpenStack.
- Key differences between OpenStack and virtualization:

OpenStack

- Does not provide virtualization technologies.
- Uses multiple technologies to manage resource pools.
- Provides unified management APIs for external communications.

Virtualization

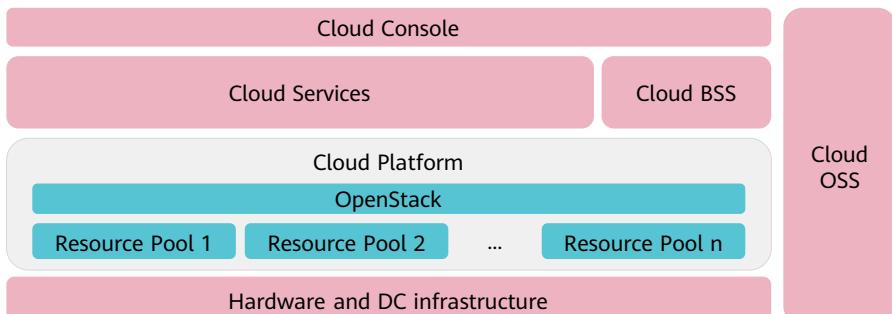
- Supports environmental isolation and resource reuse.
- Reduces isolation loss and improves efficiency.
- Provides advanced virtualization features.



- OpenStack preferentially focuses on the control plane and how to abstract various resources such as compute, storage, and network resources into resource pools. On this basis, control operations are performed on various logical objects in the resource pool, and the control operations are packaged into user-oriented services. Currently, the data plane and management plane are not the focus of OpenStack.

OpenStack and Cloud Computing

- OpenStack is only a key component of cloud computing:
 - Kernel, backbone, framework, and bus
- To build cloud computing using OpenStack, we need:

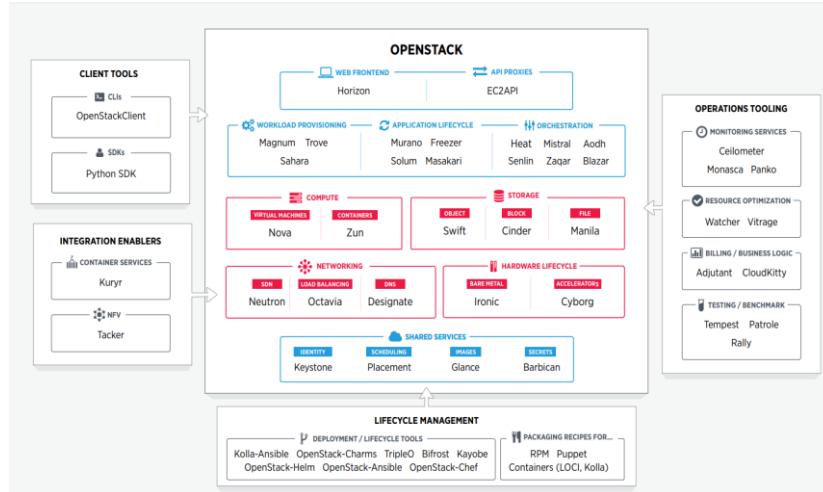


- OpenStack is a framework. Based on OpenStack, hardware and software components in multiple domains, such as compute, storage, network, management, operation, and maintenance, are integrated to form an overall solution oriented to service scenarios.
- OpenStack focuses on the openness of the framework, prosperity and activeness of the ecosystem, and service capabilities, high reliability, high performance, scalability, easy operation, and easy maintenance on the control plane.
- Cloud BSS: Cloud Business Support System
- Cloud OSS: Cloud Operation Support System
- The key differences between cloud computing and virtualization are as follows:
 - Cloud computing features service-oriented IT capabilities, on-demand use, pay-per-use billing, and multi-tenant isolation.
 - Virtualization features environment isolation, resource reuse, isolation loss reduction, running efficiency improvement, and advanced virtualization features.

Contents

1. OpenStack Overview
- 2. OpenStack Architecture**
3. OpenStack Core Services
4. Interactions Between OpenStack Projects

OpenStack Architecture



14 Huawei Confidential

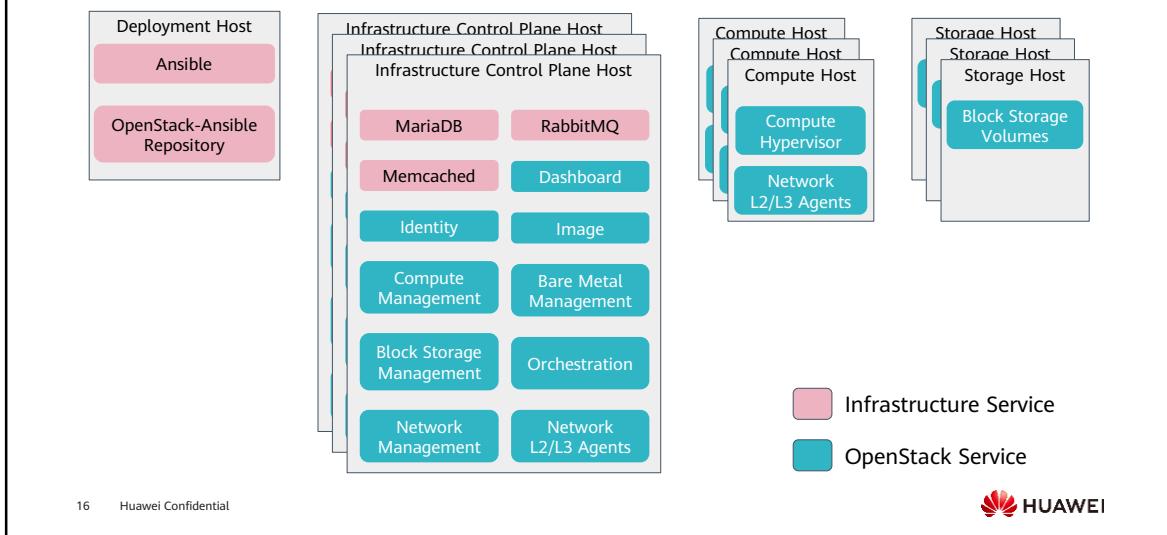


- OpenStack is broken up into services to allow you to plug and play components depending on your needs. The OpenStack map gives you an "at a glance" view of the OpenStack landscape to see where those services fit and how they can work together.

Logical Architecture of OpenStack

- To design, deploy, and configure OpenStack, administrators must understand its logical architecture.
- Internally, OpenStack services are composed of several processes. All services (except Keystone) have at least one API process, which listens for API requests, preprocesses them and passes them on to other parts of the service.
- For communication between the processes of one service, an AMQP message broker is used. The service's state is stored in a database. When deploying and configuring your OpenStack cloud, you can choose among several message broker and database solutions, such as RabbitMQ, MySQL, MariaDB, and SQLite.
- Users can access OpenStack via the web-based user interface implemented by the Horizon Dashboard, via command-line clients and by issuing API requests through tools like browser plug-ins or curl.

OpenStack Production Environment Deployment Architecture

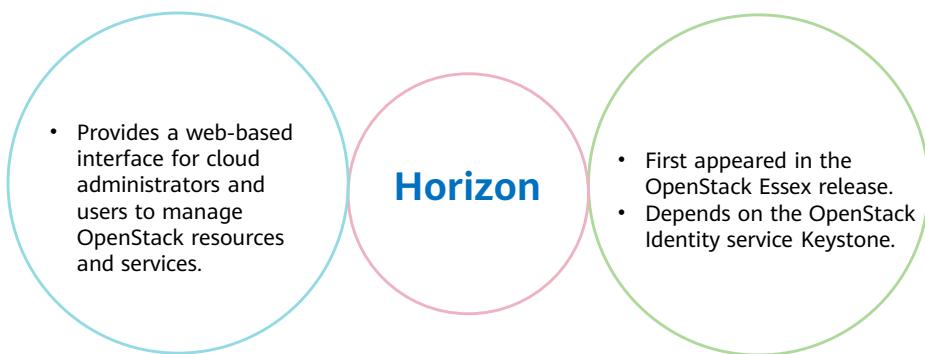


- In OpenStack production environments, you can deploy service nodes, controller nodes, compute nodes, network nodes, and storage service nodes.
- It is recommended that more than three controller nodes be deployed in the production environment and other nodes be deployed as required.
- If only for test purposes, OpenStack services can be deployed on a single node.

Contents

1. OpenStack Overview
2. OpenStack Architecture
- 3. OpenStack Core Services**
4. Interactions Between OpenStack Projects

Dashboard Service: Horizon



Identity Service: Keystone

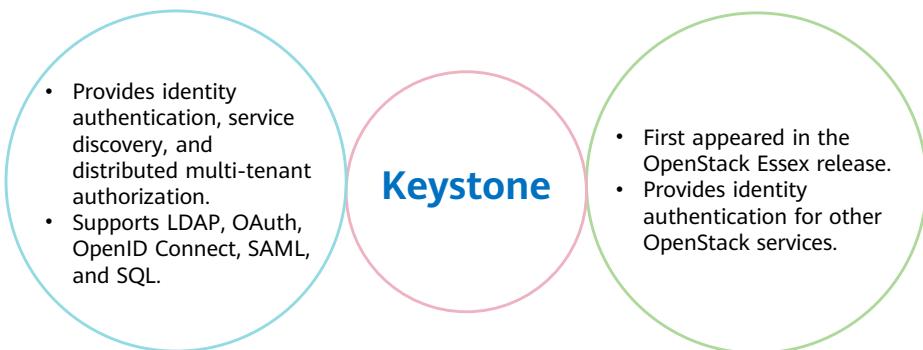
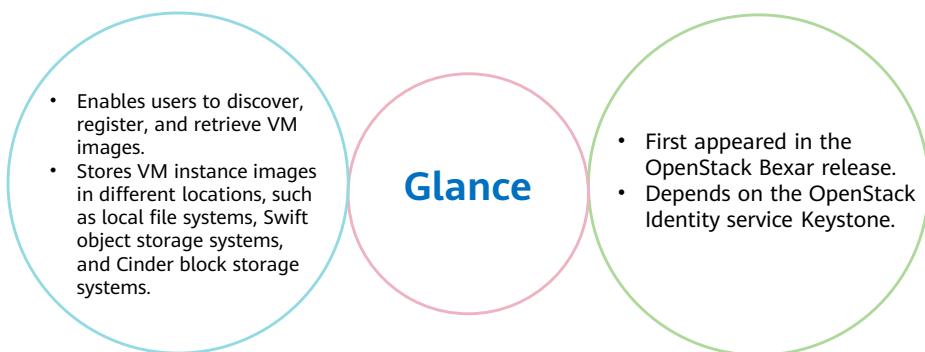
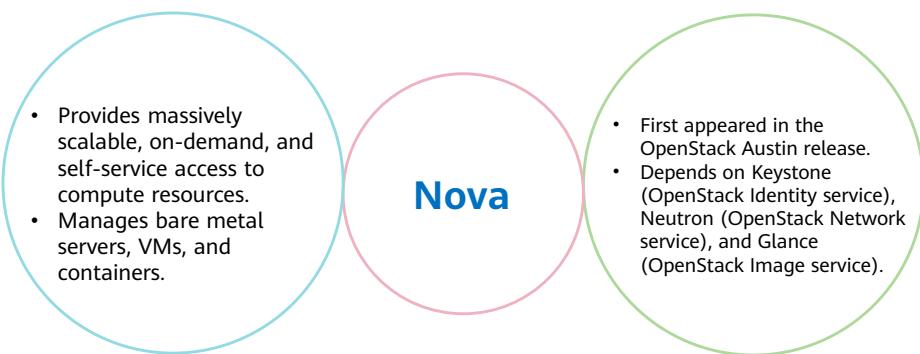


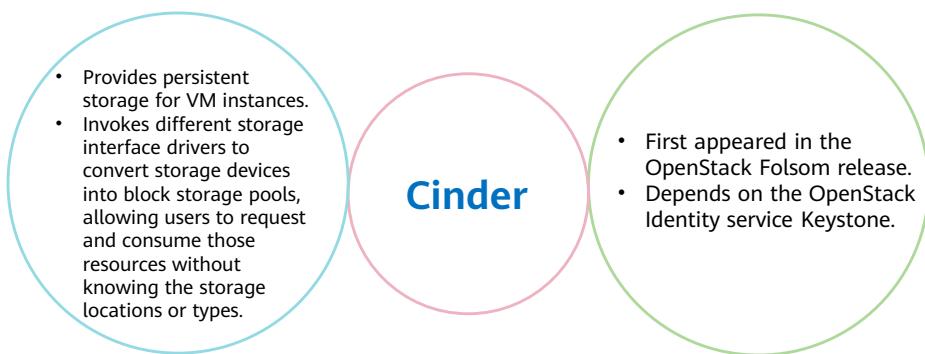
Image Service: Glance



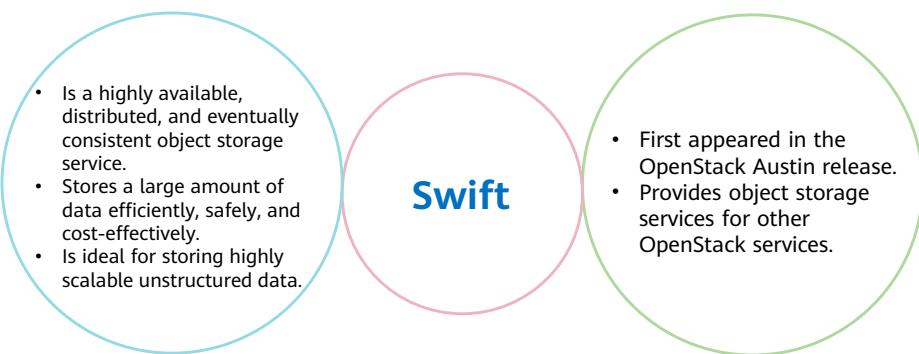
Compute Service: Nova



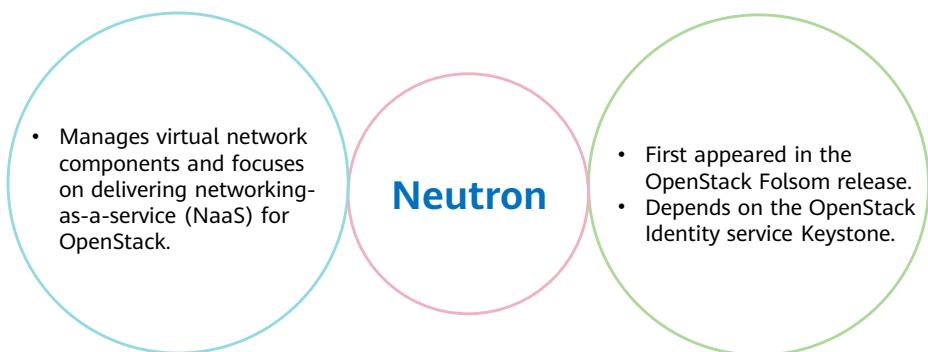
Block Storage Service: Cinder



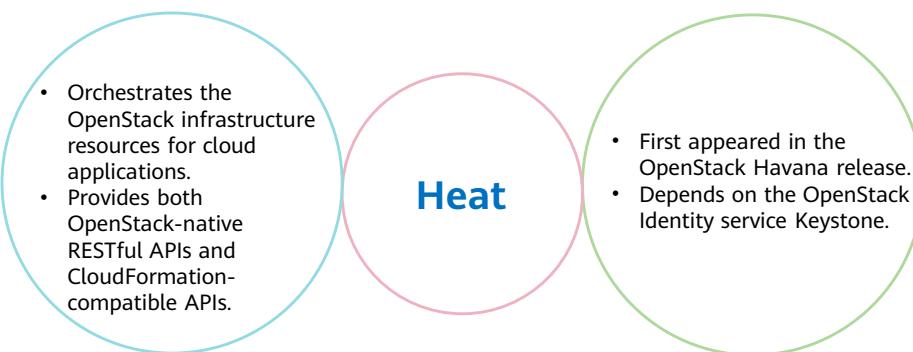
Object Storage Service: Swift



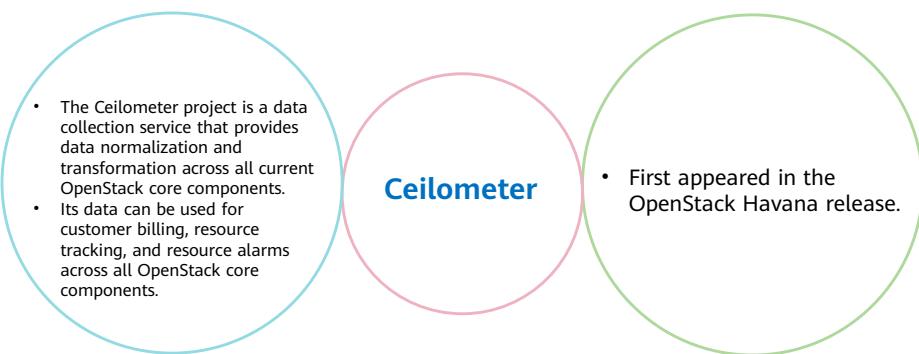
Networking Service: Neutron



Orchestration Service: Heat



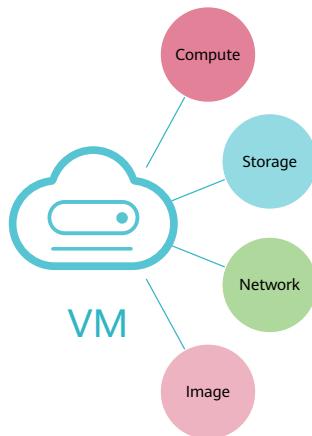
Telemetry Service: Ceilometer



Contents

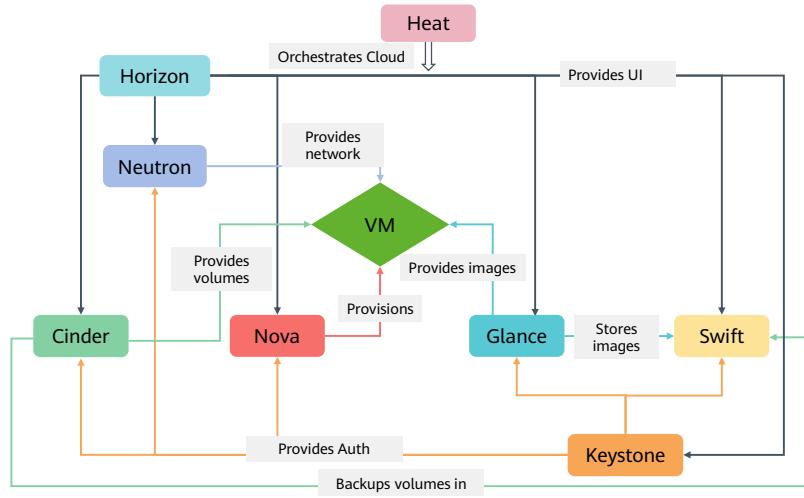
1. OpenStack Overview
2. OpenStack Architecture
3. OpenStack Core Services
- 4. Interactions Between OpenStack Projects**

Question: What Resources Are Required for Creating a VM?



- The resources for creating a VM instance in OpenStack are similar to those for creating a physical PC.

Service Interactions for Creating a VM in OpenStack



Quiz

1. Why is OpenStack called a cloud operating system?

- 1. Let's understand "cloud" and "operating system" separately:
 - Cloud generally refers to cloud computing, which focuses on IT capabilities provisioned as services, on-demand use, and pay-per-use billing.
 - The functions of an operating system include resource abstraction (for example, underlying compute, storage, and network resources are abstracted as a unified interface for upper-layer applications to invoke), resource allocation and load scheduling, application lifecycle management, system O&M, and man-machine interactions. OpenStack has the preceding capabilities and therefore can be called a cloud operating system.

Summary

- This course described the origin, version evolution, definition, architecture, and core components of OpenStack, as well as the differences between open-source OpenStack and cloud computing or virtualization.

More Information

- OpenStack Community
 - <https://www.openstack.org/>

Acronyms

- AWS: Amazon Web Services (AWS) is a web services system developed by Amazon. It allows users to rent applications to run their own VMs.
- API: Application Programming Interface (API) is a particular set of rules and specifications that are used for communication between software programs.
- BSS: is short for Business Support System.
- EC2: Elastic Compute Cloud (EC2) is a web service system developed by Amazon. It allows users to rent applications to run their own VMs.
- IaaS: Infrastructure as a Service (IaaS) is a service model in which IT infrastructure resources are provided as services over the Internet and billed on a pay-per-use basis.

Acronyms

- NASA: National Aeronautics and Space Administration (NASA) is an independent agency of the US federal government responsible for the civil space program, aeronautics research, and space research.
- OSS: Operation Support System

Thank you.

把数字世界带入每个人、每个家庭、

每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.

Copyright©2022 Huawei Technologies Co., Ltd.
All Rights Reserved.

The information in this document may contain predictive statements including, without limitation, statements regarding the future financial and operating results, future product portfolio, new technology, etc. There are a number of factors that could cause actual results and developments to differ materially from those expressed or implied in the predictive statements. Therefore, such information is provided for reference purpose only and constitutes neither an offer nor an acceptance. Huawei may change the information at any time without notice.



OpenStack Dashboard Management



Foreword

- This course describes the positioning and functions of the OpenStack Dashboard service (Horizon), its interaction with other services, architecture, and GUIs.

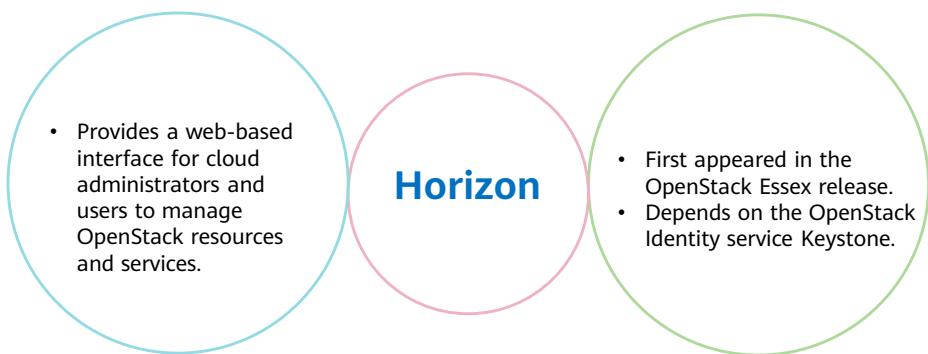
Objectives

- Upon completion of this course, you will understand:
 - What Horizon is and what functions it provides.
 - The architecture of Horizon.
 - The GUIs of Horizon.

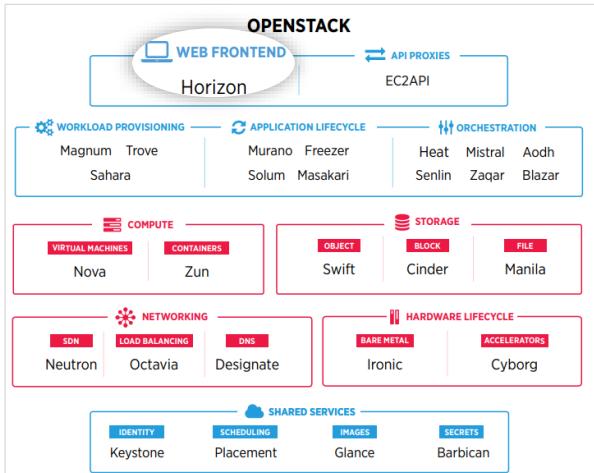
Contents

- 1. Horizon Overview**
2. Horizon Architecture
3. Horizon GUIs

What Is Horizon?



Positioning of Horizon in OpenStack



6 Huawei Confidential

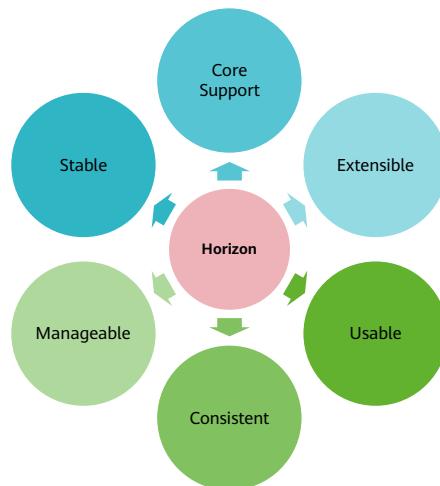
Horizon

- Horizon, a global component of OpenStack, provides a web-based user interface to OpenStack services.
- It allows administrators and users to manage the lifecycle of resources and instances and connect horizon plugins.



- Horizon is an OpenStack project. It provides a web-based user interface (also called Dashboard) to demonstrate OpenStack functions. Generally, we start with Horizon or Dashboard to understand OpenStack. Users cannot add a new OpenStack function by configuring Horizon. However, Horizon can be easily extended to include more functionalities because it only integrates some API functions of OpenStack.

Horizon Core Values

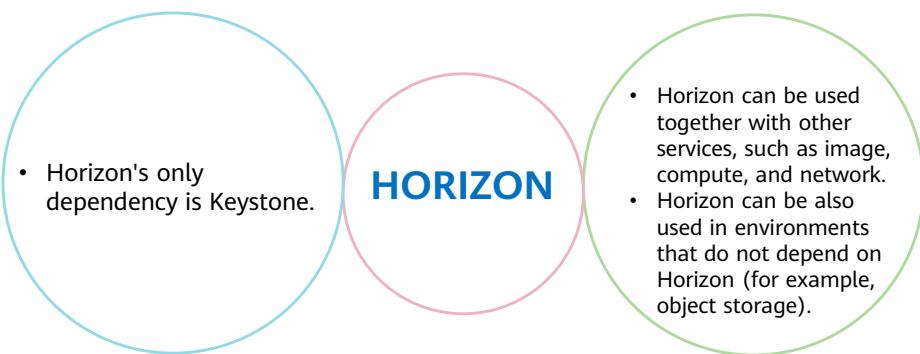


7 Huawei Confidential



- Core Support: Out-of-the-box support for all core OpenStack projects.
- Extensible: Anyone can add a new component as a "first-class citizen".
- Manageable: The core codebase should be simple and easy-to-navigate.
- Consistent: Visual and interaction paradigms are maintained throughout.
- Usable: Provides an awesome interface that people want to use.
- Stable: A reliable API with an emphasis on backwards-compatibility.

Interactions with Other Services

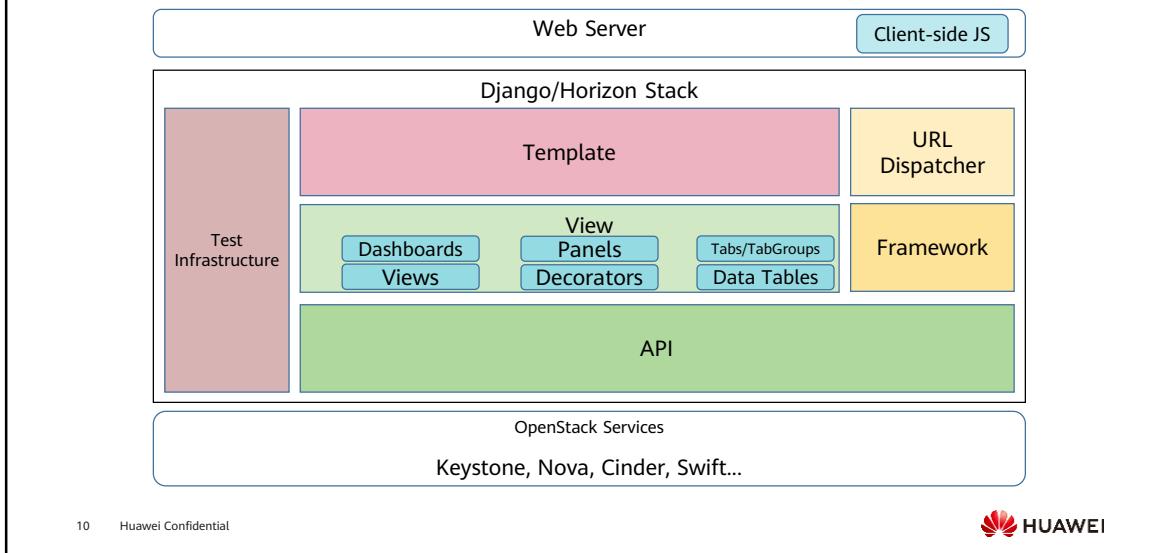


- With the Horizon control panel, users can easily access compute, storage, and network resources on the cloud platform through browsers. For example, users can start VM instances, create subnets, assign IP addresses, and set access control.

Contents

1. Horizon Overview
- 2. Horizon Architecture**
3. Horizon GUIs

Horizon Architecture



- The following figure shows the Django-based architecture of Horizon. The underlying API module `openstack_dashboard.api` encapsulates the APIs of other OpenStack projects for other Horizon modules to invoke.
- This API module provides only a subset of APIs of other projects.
- Horizon modularizes all elements on pages and encapsulates common elements on web pages such as forms and tables into Python classes, for example, the View module in the figure. Each of these components has its own HTML template. When rendering the entire page, Horizon finds the number of components on the current page, renders each component into an HTML segment, combines the HTML segments into a complete HTML page, and returns the HTML page to the browser.

Horizon Architecture

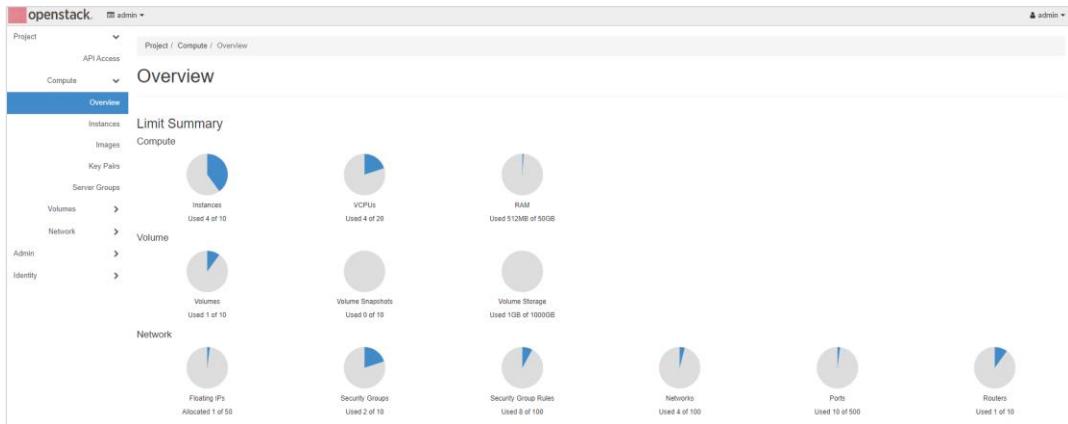
- Horizon is a Django-based web application. Developers can also extend any existing dashboard to include more functionalities using many front-end technologies.
- In keeping with Django's design philosophy, business logic is separated from presentation logic. Django views represent business logic, and a template system is a tool that controls presentation and presentation-related logic.
- Adhering to this philosophy and complying with the DRY principle, Horizon emphasizes high availability for code, provides an extensible dashboard framework, and reuses existing templates to develop and manage OpenStack websites.
- The design of the Horizon panel is divided into three layers: Dashboard -> PanelGroup -> Panel.

- Django is a widely-used open-source Python-based web framework.
- Django follows the Don't Repeat Yourself (DRY) principle and emphasizes high reusability of code.
- A website program consists of three parts: service logic code (Python), static files (JS/CSS), and templates (Jinja and Mako templates in Python, and Jade template in NodeJS). After a user sends a request to the web server, the server program finds the template corresponding to the current URL, fills in the template variables, and returns HTML source code in character string format to the browser. The browser then renders the page.

Contents

1. Horizon Overview
2. Horizon Architecture
- 3. Horizon GUIs**

OpenStack Horizon GUIs - Project



13 Huawei Confidential



- The screenshot is from the lab environment.
- As shown in this figure, the entire page consists of the Dashboards, PanelGroups, Panels, and the page rendered after a Panel is clicked.
- **Project** represents the Dashboard, **Compute** under **Project** represents the PanelGroup, and **Overview** under **Compute** represents the Panel. The area on the right is the page rendered by clicking **Overview**.
- A project is an organization unit in the cloud and is also called a tenant. A user can be a member of one or multiple projects. In a project, users can create and manage instances.
- On the **Project** page, users can view and manage resources in a selected project, including instances, images, key pairs, and host groups.

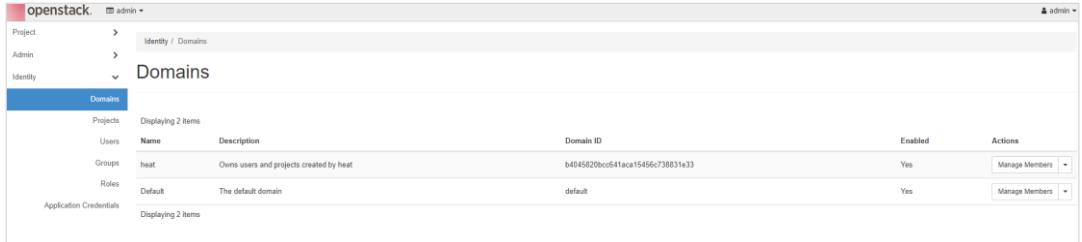
OpenStack Horizon GUIs - Admin

The screenshot shows the OpenStack Horizon Admin interface. The left sidebar has categories: Project, Admin, Compute, Volume, Network, System, and Identity. The 'Overview' tab is selected under Admin. The main content area displays a 'Usage Summary' section with a date range selector and a table of resource usage for the 'admin' project.

Project Name	VCPUs	Disk	RAM	VCPU Hours	Disk GB Hours	Memory MB Hours
admin	4	4GB	512MB	121.34	121.34	15531.02

- The screenshot is from the lab environment.
- The **Admin** page displays the resources (such as compute, storage, network, and system settings) that can be managed by administrators.

OpenStack Horizon GUIs - Identity



The screenshot shows the OpenStack Horizon Identity interface. The left sidebar has 'Project' and 'Admin' collapsed, and 'Identity' expanded, with 'Domains' selected. The main content area shows a table for 'Domains'. The table has columns: Projects, Users, Groups, Roles, and Application Credentials. Under 'Projects', it says 'Displaying 2 items'. Under 'Users', there is one item named 'heat'. Under 'Groups', there is one item named 'heat'. Under 'Roles', there is one item named 'Default'. Under 'Application Credentials', it says 'Displaying 2 items'. The table includes columns for 'Name', 'Description', 'Domain ID', 'Enabled', and 'Actions'. The 'heat' user has a Domain ID of 'b4045820bcc641aca15456c738831e33', is Enabled (Yes), and has a 'Manage Members' button. The 'Default' role has a Domain ID of 'default', is Enabled (Yes), and has a 'Manage Members' button.

- The screenshot is from the lab environment.
- The **Identity** page offers the authentication management function.

Quiz

1. Which of the following is the correct sequence of layers in Horizon panel design?
 - A. Dashboard -> PanelGroup -> Panel
 - B. PanelGroup -> Dashboard -> Panel
 - C. Dashboard -> Panel -> PanelGroup
 - D. Panel -> PanelGroup -> Dashboard

- 1. A

Summary

- This course described the definition, positioning, functions, architecture, and GUIs of Horizon.

More Information

- OpenStack Community
 - <https://www.openstack.org/>

Acronyms

- API: Application Programming Interface (API) is a particular set of rules and specifications that are used for communication between software programs.
- DRY: Don't Repeat Yourself (DRY) is a principle of reducing code repetitions in software design and calculation to increase software flexibility and simplicity and avoid code conflicts.
- HTML: HyperText Markup Language (HTML) is the standard markup language for World Wide Web documents designed to be displayed in a web browser.
- URL: A Uniform Resource Locator (URL) is the address of a website on the Internet. It indicates the location of a resource as well as the protocol used to access it. Each file on the Internet has a unique URL that contains information about the location of the file and how the browser should handle the file.

Acronyms

- WSGI: Web Server Gateway Interface (WSGI) is an interface that specifies how web servers should forward requests to Python applications or frameworks.
- Web: World Wide Web (Web) is a global, interactive, dynamic, cross-platform, distributed, graphical information system based on the hypertext and HTTP.

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and
organization for a fully connected,
intelligent world.

Copyright©2022 Huawei Technologies Co., Ltd.
All Rights Reserved.

The information in this document may contain predictive
statements including, without limitation, statements regarding
the future financial and operating results, future product
portfolio, new technology, etc. There are a number of factors that
could cause actual results and developments to differ materially
from those expressed or implied in the predictive statements.
Therefore, such information is provided for reference purpose
only and constitutes neither an offer nor an acceptance. Huawei
may change the information at any time without notice.



OpenStack Identity Management



Foreword

- This course describes the positioning and functions of the OpenStack Identity service (Keystone), its interactions with other services, object models, and working principles.

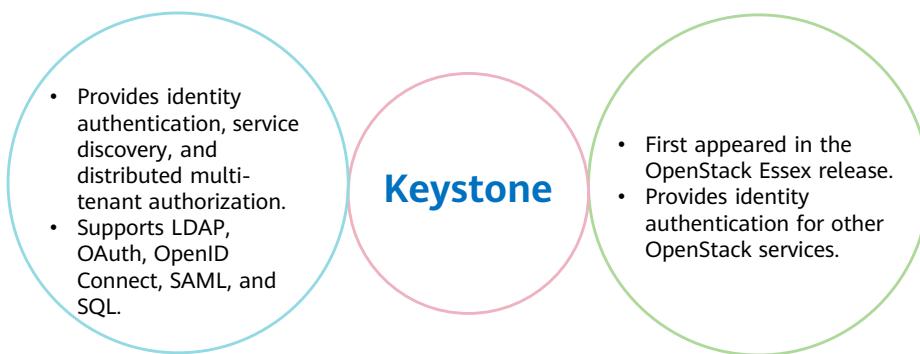
Objectives

- Upon completion of this course, you will understand:
 - The positioning and functions of Keystone in OpenStack and its interaction with other services.
 - The architecture, components, object models, and working principles of Keystone.

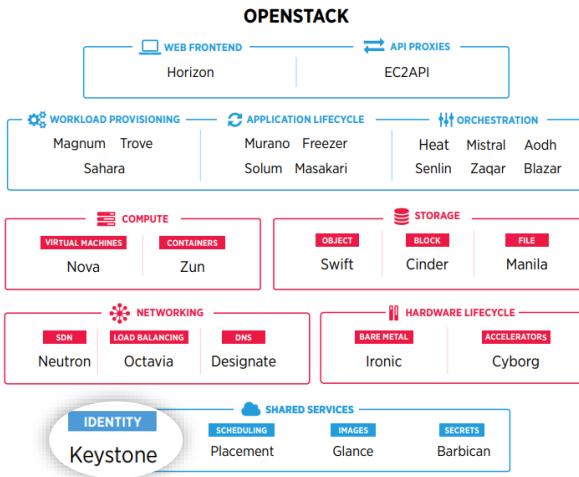
Contents

- 1. Keystone Overview**
2. Keystone Architecture
3. Keystone Object Models
4. Keystone Working Principles and Processes

Identity Service: Keystone



Positioning of Keystone in OpenStack



6 Huawei Confidential

Keystone

- OpenStack Identity, code-named Keystone, is the default identity management system for OpenStack.
- Keystone is a shared service in OpenStack. It provides authentication for other projects.



Basic Concepts

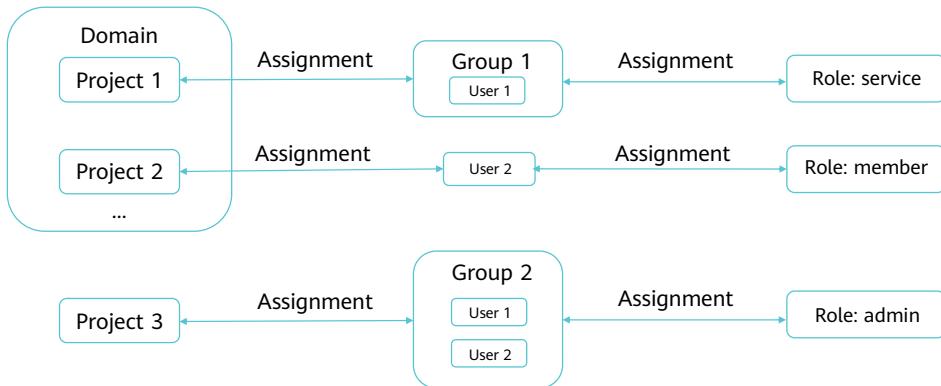
Domain	A container for users, projects, and groups.
User	A digital representation of a person, system, or service that uses OpenStack cloud services through Keystone.
Group	A collection of users. A role granted to a group applies to all users in the group. You can grant a role to a user by adding the user to a specific group.
Project	A collection of resources accessible to services. A project must be unique within a given domain.
Role	A defined set of user rights and privileges to perform a specific set of operations.
Service	An OpenStack service that provides one or more endpoints through which users can access resources and perform operations.
Endpoint	A network-accessible address that you can use to access a service.
Token	A credential that enables access to specific resources.
Credential	Data that confirms the identity of the user, for example, a user name and password.

- Domain: A domain can correspond to a large organization or a data center and **must be globally unique**. A cloud user is the owner of a domain and can create multiple projects, users, groups, and roles in the domain. The user can also centrally manage projects.
- User: Keystone uses authentication information (such as credentials and passwords) to verify the validity of user requests. If a user passes the authentication, Keystone assigns a specific token to the user. The token can be used to authenticate subsequent resource access. Users are not globally unique, but only unique to their domains.
- Group: A group is a container representing a collection of users. The administrator can add users to a group and assign roles directly to the group. This way, all users in the group enjoy the role permissions assigned to the group. By introducing the concept "group", Keystone centrally manages user groups and user permissions.
- Project: A project is a collection of resources accessible to services. When creating a VM or creating a volume in Cinder, you need to specify a project. A user is bound to certain projects by default. To access resources in a project, a user must have been assigned the permission or specific role required to access the project. **A project does not need to be globally unique. It only needs to be unique in a domain.**
- Role: Different roles represent different permissions. The role assigned to a user determines whether the user has the permission to access specific resources. A user can be assigned a role in a domain or project. If a user is assigned a role in a domain, the user has the same role for all projects in the domain, and the role for a specific project has only the access permission for that project. Roles can be inherited. In a project tree, having the permission to access the parent project also means having the permission to access the child projects. **Each role must be**

globally unique.

- Service: Nova, Swift, Glance, Cinder, and more. A service can determine whether a user has the permission to access its resources based on the user, tenant, and role information. A service provides one or more endpoints through which users can access resources and perform operations.
- Endpoint: An endpoint is a network-accessible address through which you can access a service. It can be regarded as a service access point. If you need to access a service, you must know its endpoint. Generally, a URL represents an endpoint.
- Token: A token is a credential that enables access to specific resources. No matter which access method is used, Keystone is to provide a token for external systems to access OpenStack resources.
- Credential: A credential is data that confirms the identity of a user, for example, user name and password.

Logical Relationships Between Basic Concepts



- The preceding figure shows the logical relationships between domains, projects, groups, users, and roles.
- A Role Assignment is a triplet formed by Role, Resource, and Identity.
- Resource: provides data related to domains and projects.

Functions of Keystone in OpenStack



10 Huawei Confidential

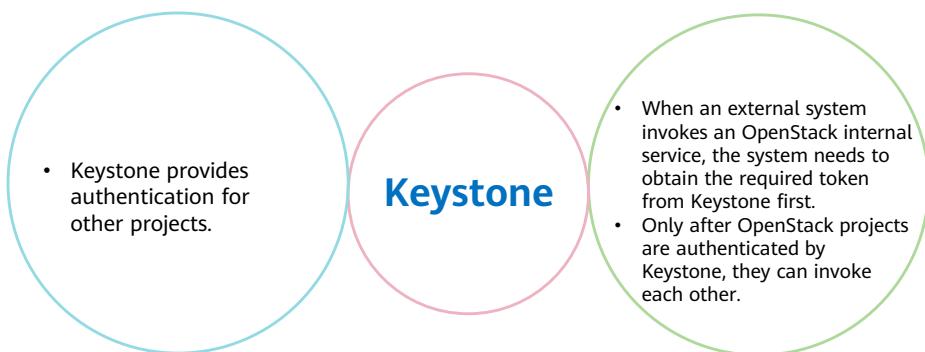
Keystone

- Keystone bridges users and OpenStack services.
- Users obtain tokens and service catalogs from Keystone. When accessing services, users send their own tokens. Related services invoke Keystone to verify the validity of tokens.



- As an independent security authentication module in OpenStack, Keystone authenticates OpenStack users, manages tokens, provides service catalogs for accessing resources, and controls access based on user roles.
- Keystone is required for authentication of the username and password for accessing the system, token issuing, service endpoint registration, and verification of user permissions to access specific resources.
- Identity: provides authentication credentials as well as user and user group data.
- Token: After confirming the identity of a user, Keystone provides the user with a token that can be used for subsequent resource requests.
- Catalog: provides a service catalog for external systems. The service catalog stores endpoint information of all OpenStack services.
- Policy: is a rule-based identity authentication engine that defines the mapping between actions and user roles through configuration files.
- Resource: provides data related to domains and projects.
- Assignment: provides data about roles and role assignments and is responsible for role authorization.

Interaction with Other Services

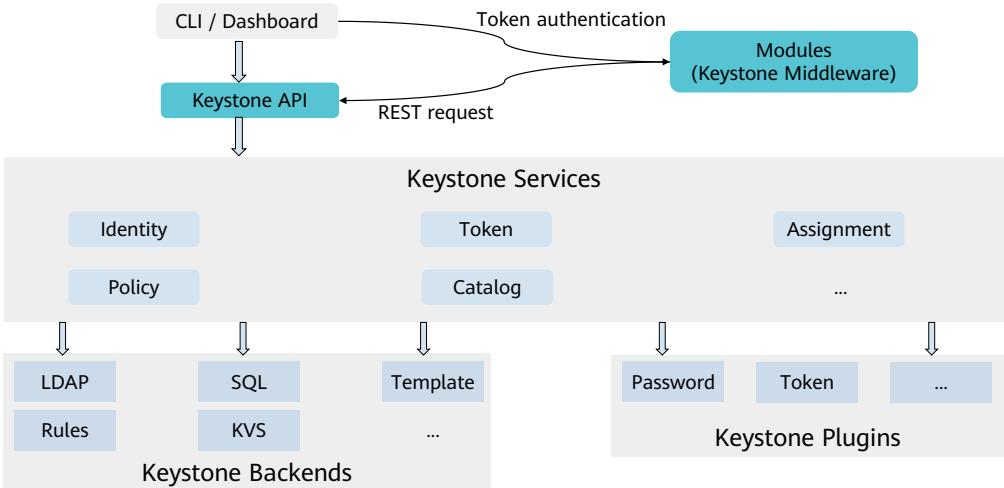


- In the OpenStack architecture, Keystone functions as a service bus. Other services, such as Nova, Glance, Horizon, Swift, Cinder, and Neutron, register their endpoints through Keystone. Any invocation of these services must be authenticated by Keystone, and the endpoint of the service is required for access.

Contents

1. Keystone Overview
- 2. Keystone Architecture**
3. Keystone Object Models
4. Keystone Working Principles and Processes

Keystone Architecture



13 Huawei Confidential



- Keystone Middleware is provided by Keystone to verify token validity.
 - For example, a PKI token is provided when a client accesses resources provided by Keystone. Tokens can be verified on the middleware so that Keystone does not need to verify them upon each access. The prerequisite is that the middleware has cached related certificates and keys for signature authentication of the token.
 - If the token is not of the PKI type, a session connected to the Keystone service needs to be obtained from keystoneauth and then the API provided by Keystone is invoked to verify the token validity.
- In addition to the background database, the Keystone project mainly includes an API service process for processing RESTful requests. These APIs cover various services provided by Keystone, such as Identity, Token, Catalog, and Policy. The functions provided by these services are implemented by backend drivers.

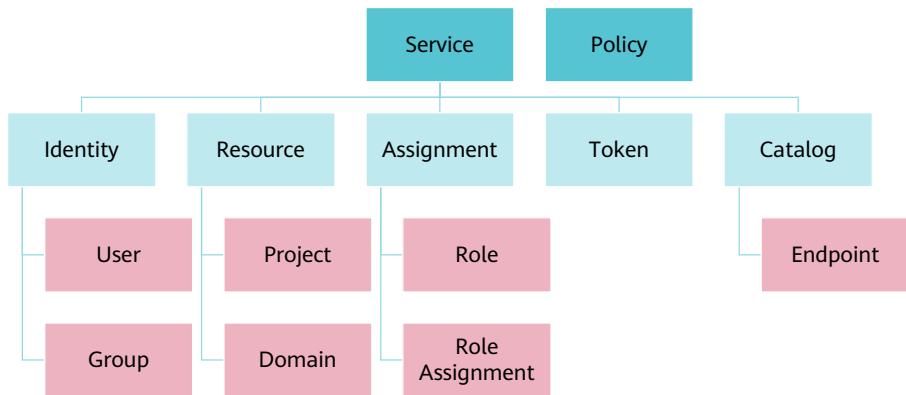
Functions of Keystone Components

Keystone APIs	<ul style="list-style-type: none">Receive external requests.
Keystone Middleware	<ul style="list-style-type: none">Caches tokens to reduce the pressure on Keystone services.
Keystone Services	<ul style="list-style-type: none">Provide different authentication or authorization services.
Keystone Backends	<ul style="list-style-type: none">Implement Keystone services. Different backends provide different services.
Keystone Plugins	<ul style="list-style-type: none">Provide authentication methods, such as password and token.

Contents

1. Keystone Overview
2. Keystone Architecture
- 3. Keystone Object Models**
4. Keystone Working Principles and Processes

Keystone Object Models



- Keystone mainly manages objects, including Identity, Resource, Assignment, Token, Catalog, and Service. These objects are implemented through other smaller objects.
- Additionally, the Policy defines the policies for accessing various OpenStack resources and services.

Keystone Object Model - Service

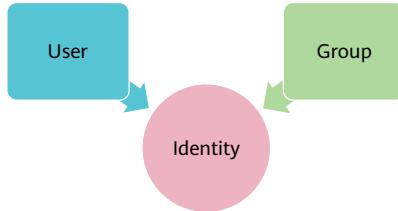
- Keystone is a set of internal services that are made available to one or more endpoints.
- Keystone internal services include Identity, Resource, Assignment, Token, and Catalog.
- You can combine Keystone internal services as needed.
 - For example, during identity authentication, after the identity service is used to authenticate user or project credentials and the authentication succeeds, a token is then created and returned.



- In addition to providing internal services, Keystone interacts with other OpenStack services, such as compute, storage, and image services. Specifically, it provides one or more endpoints through which users can access resources and perform operations.

Keystone Object Model - Identity

- The Identity service provides identity authentication, as well as user and user group data.

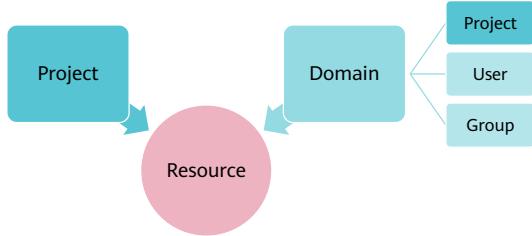


- A user is the one using OpenStack services and must belong to a specific domain. User names are not globally unique in the OpenStack system, but they are unique in the domain where they belong.
- Multiple users are managed as a whole in a group. A group must belong to a specific domain. Group names are not globally unique in the OpenStack system, but they are unique in the domain where they belong.

- Generally, the identity service manages user and user group data, and processes all CRUD operations associated with these data.
- In some complex cases, user and user group data is managed by authoritative backend services.
 - For example, if the identity service acts as the frontend of the LDAP server, an authoritative information source, the identity service accurately relays the LDAP information.
- Keystone provides internal services and external services. Internal services can be implemented in Keystone and results can be directly returned. Keystone can also interact with other OpenStack services or components. After the interaction is complete, Keystone provides one or more endpoints for users. These endpoints can be considered as access paths or links. Users can use these endpoints to access resources and perform operations.

Keystone Object Model - Resource

- The resource service provides data about projects and domains.

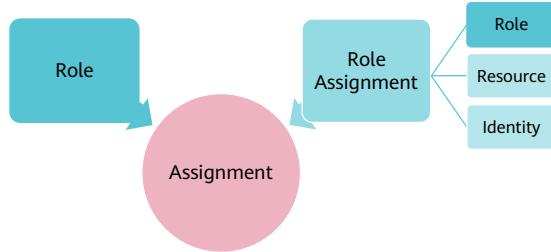


- A project is the basic unit for managing OpenStack resources. All resources in the OpenStack system belong to a specific project.
- A domain manages projects, users, and groups as a whole. Each resource belongs to a specific domain. The default domain name of Keystone is "Default".

- A project must belong to a specific domain. All project names are not globally unique in the OpenStack system, but are unique in the domain where they belong.
- If you do not specify a domain when creating a project, add the project to the default domain.

Keystone Object Model - Assignment

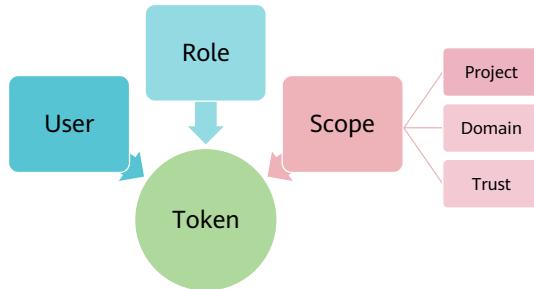
- The assignment service provides data about roles and role assignments.



- A role specifies the authorization level of an end user. Roles can be granted at the domain or project level. You can assign roles to a single user or group. A role name is unique within its domain.
- A Role Assignment is a triplet comprising a role, a resource, and an identity.

Keystone Object Model - Token

- The token service provides credentials for users to access services. It represents the user account information.
- A token contains the information about users, scopes (project, domain, or trust), and roles.



Keystone Object Model - Catalog

- The catalog service provides a registry for querying endpoints to enable external access to OpenStack services.

```
{  
    "catalog": [  
        {  
            "name": "Keystone",  
            "type": "identity",  
            "endpoints": [  
                {  
                    "interface": "public",  
                    "url": "https://identity.example.com:5000/"  
                }  
            ]  
        }  
    ]  
}
```

- An endpoint template is a set of URLs that are classified as public, internal, or admin.
 - public: Public URLs are accessed by end users or users of other services, usually on public networks.
 - internal: Internal URLs are accessed by end users, usually on the internal, private network.
 - admin: Admin URLs are accessed by service administrators, usually on secure networks.

- Users and OpenStack services can obtain endpoints of other services through Catalog. These endpoints are maintained by Keystone when services are registered through Keystone. A catalog is a collection of endpoints and provides the endpoint registry for querying endpoints so that external systems can access OpenStack services.
- An endpoint is essentially a URL that provides an entry for a service. Each service can have one or more endpoints. To access a service, you only need to know the endpoint of the service. This figure shows an endpoint displayed in the catalog. The service name is Keystone, the type is Identity, and the access endpoint entry is Public. Users can directly access the endpoint.
- OpenStack uses three endpoint variants for each service: admin, internal, and public. They are open to different users or services. For example, a public URL is generally open to all users, and users can access the public URL through an external network. Generally, the public URL is used on a public network interface. The admin URL is restricted to some users or URLs and can be accessed only by users with specific operation permissions. Generally, the admin URL is provided only for users with management rights and is used on secure network interfaces. An internal URL is restricted to the hosts that contain OpenStack services. Generally, internal URLs are used for internal components of OpenStack to communicate with each other and are used on unmetered internal network interfaces.

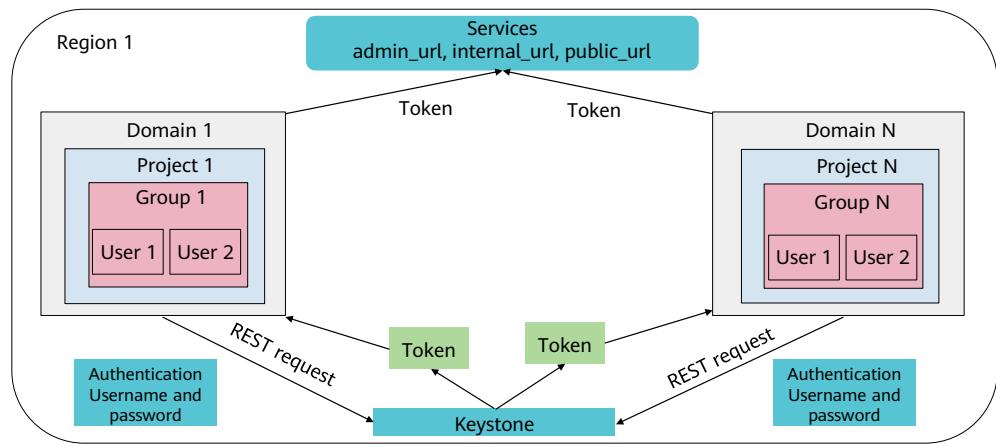
Keystone Object Model - Policy

- Each OpenStack service defines the policies for access its resources in the related policy file.
- An access policy is similar to a permissions set in Linux. Users or user groups with different roles have different permissions.

```
{  
    "admin_required": "role:admin",  
    "cloud_admin": "rule:admin_required and domain_id:admin_domain_id",  
  
    "default": "rule:admin_required",  
  
    "identity:get_service": "rule:admin_or_cloud_admin",  
    "identity:list_services": "rule:admin_or_cloud_admin",  
    "identity:create_service": "rule:cloud_admin"  
}
```

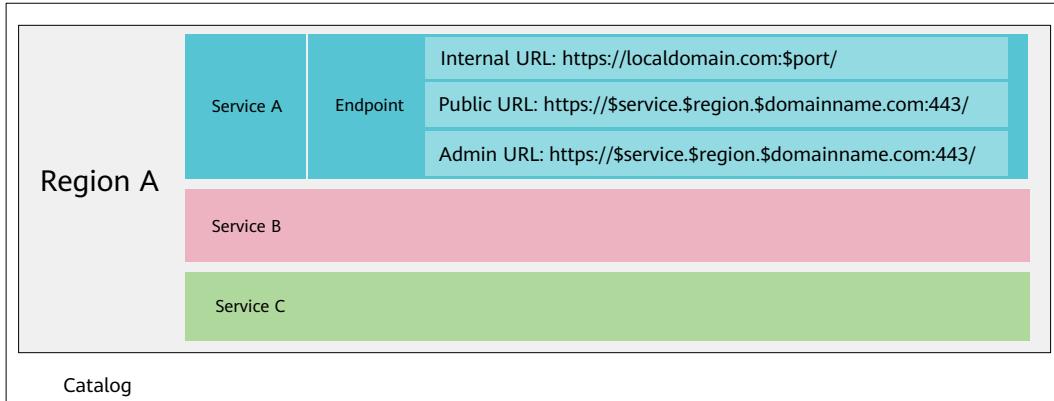
- Access policy rules are defined in a JSON file whose name is **policy.json**.
 - The policy file path is */etc/SERVICE_NAME/policy.json*, for example, */etc/keystone/policy.json*.

Keystone Object Model Allocation Example



Keystone Object Model Allocation Example

- Region, Service, and Endpoint:



- A catalog contains Services (in Keystone) from different regions. Each Service has different types of endpoints.
- What do users do during the interaction with Services in Keystone? Common users use Keystone to authenticate identities, obtain identity tokens, and obtain service catalogs to be accessed. Admin User has high-level rights and is used only for management operations. It can manage users, projects, and roles in Keystone, manage user roles in specific projects, and manage different services and endpoints in services. Finally, the Service in Keystone verifies the validity of the token for the user, locates other Services, and provides the location endpoint for the user. A Service can also invoke other Services.

Keystone Object Model Use Examples

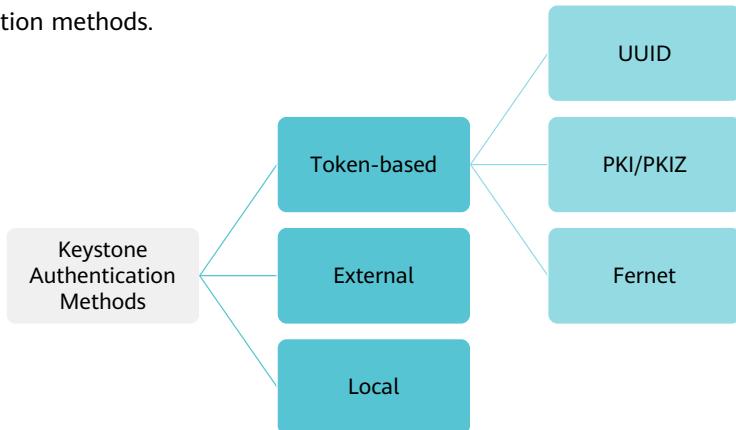
- User:
 - Obtains a token.
 - Obtains a service catalog.
- Admin User:
 - Manages users, projects, and roles.
 - Manages the roles of users in a specific project.
 - Manages services and their endpoints.
- Service:
 - Verifies tokens.
 - Locates other Services.
 - Invokes other Services.

Contents

1. Keystone Overview
2. Keystone Architecture
3. Keystone Object Models
- 4. Keystone Working Principles and Processes**

Keystone Authentication Methods

- **Authentication** is the most important function of Keystone. Keystone supports multiple authentication methods.



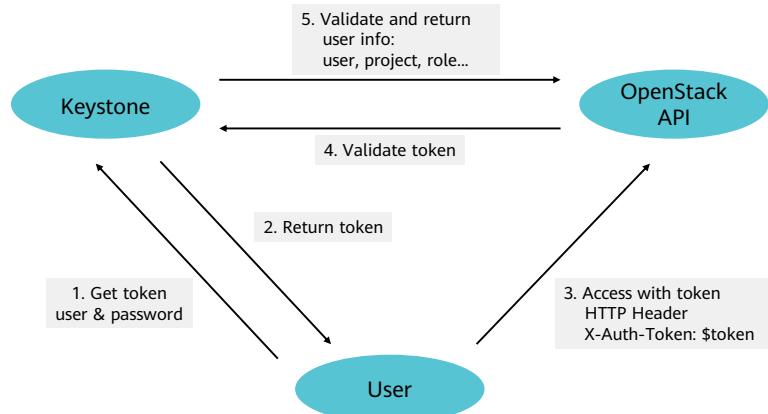
- UUID: Universal Unique Identifier
- PKI: Public Key Infrastructure

Differences Between Keystone Authentication Methods

Token-based Authentication	External Authentication	Local Authentication
<ul style="list-style-type: none">The most commonly used method, easy to use.An HTTP header "X-Auth-Token" is added when an authentication request is sent. Keystone then compares the token value in the header to that in the database.	<ul style="list-style-type: none">A third-party authentication system is integrated and the REMOTE_USER information is added to the authentication request.	<ul style="list-style-type: none">This is the default authentication method. Username and password are used for authentication.

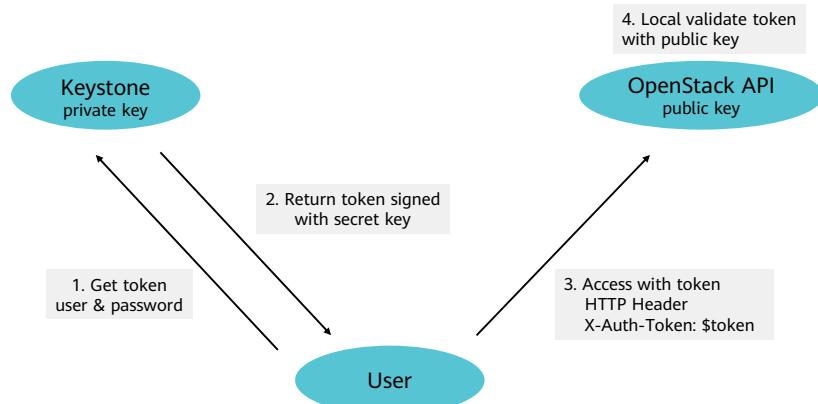
Token-based authentication is widely used in production environments and is the one you should focus on.

Keystone Token-based Authentication - UUID



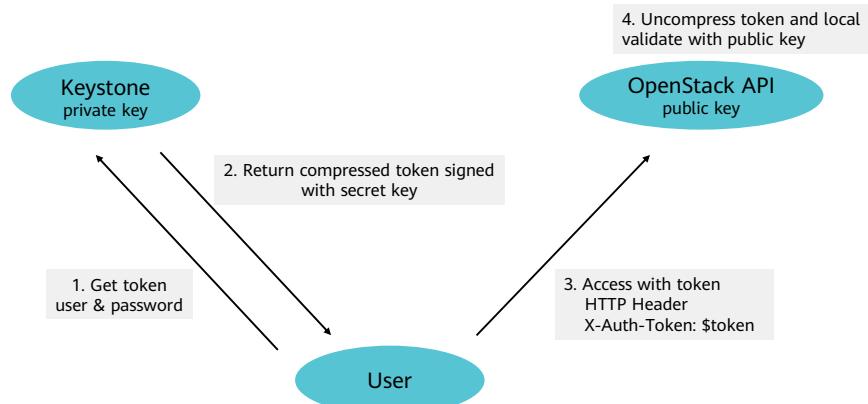
- UUID is short for Universally Unique Identifier.
- A UUID is a 32-byte random character string and does not carry any other information. It is used only as a token ID. When a request is sent, the token ID is transferred in X-Auth-Token.
- After receiving the token, the OpenStack API requests Keystone to verify the token and obtains related user information.

Keystone Token-based Authentication - PKI



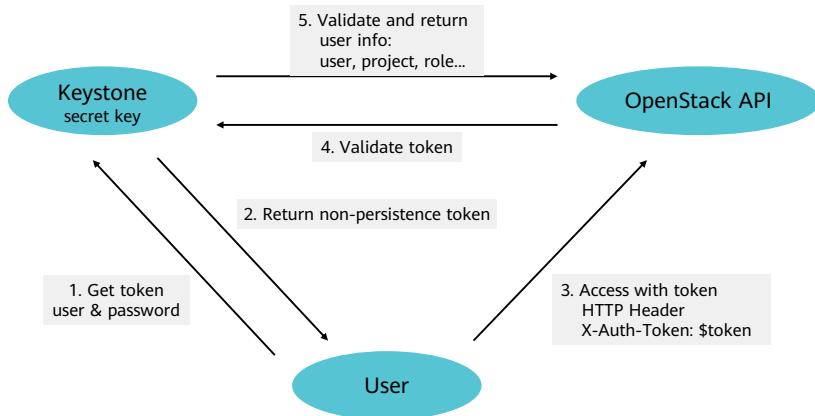
- PKI is short for Public Key Infrastructure.
- PKI is essentially used for digital signatures. After the Keystone private key digitally signs the token, the API server of each OpenStack service uses the public key to locally verify the signed token.
- The authentication process is similar to that shown in the preceding figure. A user sends the username and password to Keystone. Keystone uses the private key to encrypt the key and generate a token and returns the token to the client. Each time the client sends a resource or service invoking request to OpenStack, the token is carried. OpenStack service APIs use the local public key to verify the token.
- Unlike UUID, PKI tokens contain more user information and also digital signatures to support local authentication, avoiding repeated Keystone authentications.
- However, this will make the PKI token size larger than the HTTP header size when the OpenStack scale is large, causing an authentication failure.

Keystone Token-based Authentication - PKIZ



- PKI tokens carry a large amount of data. To address this problem, PKIZ tokens have been developed. A PKIZ token is a compression of a PKI token, but the compression effect is limited.
- Generally, a PKIZ token is about 90% of the size of its corresponding PKI token. Therefore, large token sizes cannot be completely avoided using PKIZ tokens.
- As shown in the preceding figure, the authentication process is basically the same as that of PKI tokens.
- The only difference is that the token is compressed when Keystone generates the token and returns it to the client.

Keystone Token - based Authentication - Fernet



- UUID, PKI, and PKIZ tokens are permanently stored in databases. Accumulated tokens may deteriorate database performance. You need to periodically delete tokens from databases.
- In case there are too many tokens in a database, current OpenStack versions use Fernet tokens by default. Fernet tokens contain a limited amount of user data and use symmetric encryption. This kind of tokens does not need to be stored in databases, but their keys need to be changed periodically.
- The authentication process is as follows: A user sends the username and password to Keystone. Keystone uses the private key to generate a temporary token and returns the token to the client. Each time the client sends a resource or service invoking request to OpenStack, the token is carried. After receiving the request, OpenStack service APIs sends the token to Keystone to verify the token. A message is returned when the verification is successful.
- This process seems to be the same as the UUID authentication process, but they are actually different. The UUID authentication process does not include the encryption and decryption processes. After generating a token, Keystone needs to cache the token locally to facilitate subsequent verification. However, Fernet performs peer-to-peer verification and does not need to cache tokens. It only decrypts the token and does not require persistently stores the token. Fernet token sizes are proper and therefore are suitable for multi-data-center scenarios.

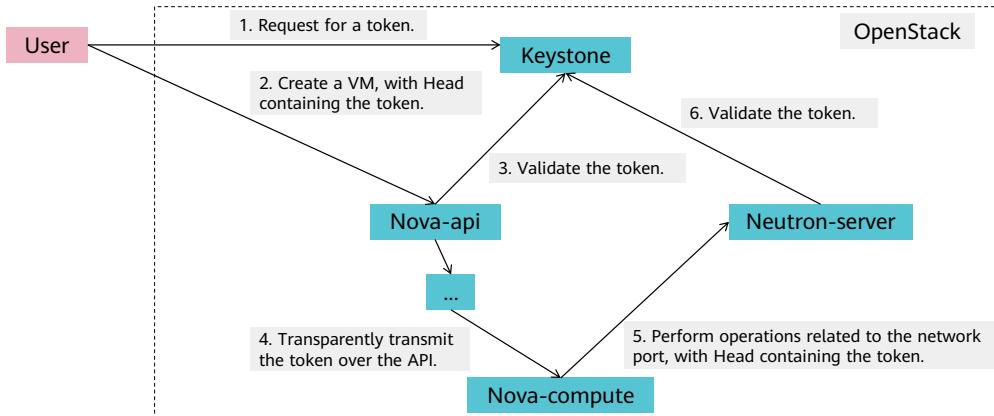
How Do I Choose a Keystone Token - based Authentication Method?

Token Type	UUID	PKI	PKIZ	Fernet
Size	32 bytes	KB level	KB level	About 255 bytes
Local Authentication	Not supported	Supported	Supported	Not supported
Keystone Load	Large	Small	Small	Large
Stored in Databases	Yes	Yes	Yes	No
Information Contained	None	Users, catalogs, and more	Users, catalogs, and more	Users and more
Encryption Method	None	Asymmetric encryption	Asymmetric encryption	Symmetric encryption (AES)
Compressed	No	No	Yes	No

Currently, the newly released OpenStack versions use **Fernet tokens** by default.

- When choosing a token, you should consider multiple factors, including Keystone server loads, region quantity, security factors, maintenance costs, and token maturity.
 - The region quantity affects the size of PKI and PKIZ tokens.
 - For security purposes, the private key on the Keystone server needs to be kept secure when PKI tokens are used, and the keys need to be periodically changed when Fernet tokens are used, but the keys do not need to be maintained when UUID keys are used.
 - In terms of security, maintenance cost, and maturity, the priority for choosing a token type is as follows: UUID > PKI/PKIZ > Fernet.
- - If the Keystone server has light loads and there are fewer than three regions, choose UUID tokens.
 - If the Keystone server has heavy loads and there are fewer than three regions, choose PKI/PKIZ tokens.
 - If the Keystone server has light loads and there are no fewer than three regions, choose UUID tokens.
 - If the Keystone server has heavy loads and there are no fewer than three regions, the latest OpenStack versions use Fernet tokens by default.

OpenStack Authentication Process - Creating a VM



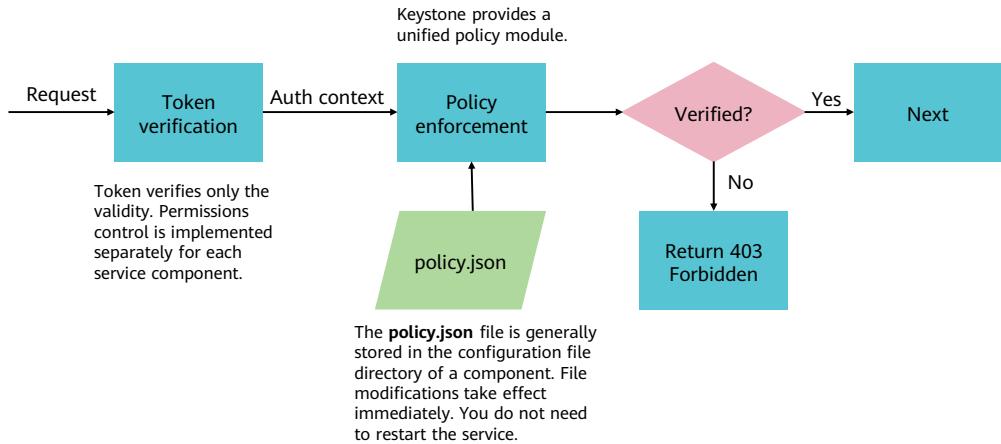
Keystone only checks whether the token is valid. How is permissions control managed for each service?

- Let's take VM creation as an example to learn about the entire OpenStack authentication process.
- To use OpenStack, you need to provide the username and password for Keystone to obtain the token. After obtaining the token, you need to send a VM creation request to Nova. Nova invokes compute resources and manages the VM lifecycle. Therefore, the creation request needs to be sent to Nova. The request header carries a token. After receiving the request, Nova-api sends the token to Keystone to check whether the token is valid. After the verification is successful, a message is returned to Nova, and Nova starts to create a VM. We do not talk about how to use Nova here. To create a VM, you need to prepare not only compute resources such as CPUs and memory, but also network and storage resources. The following uses network resources as an example. Nova-api transparently transmits the token to Nova-compute, Nova-compute sends a network-related operation request to Neutron-server. The request header also carries the token. After receiving the request, Neutron sends the token to Keystone for verification. The corresponding operation is performed only after the verification is successful.
- In this process, tokens must be carried when different services are invoked, and Keystone only verifies the validity of tokens. How is the operation permissions control of each service implemented?

Discussion: How Is RBAC Implemented?

- During VM creation, different OpenStack services interact with each other and Keystone issues and validates the token. So, how does each service verify user permissions?
 - For example, how does a service check whether the user has the permission to create VMs or modify VM flavors?
- I will give you 5 minutes to think about or discuss this question: how is role-based access control (RBAC) implemented in OpenStack?
 - What are some examples of RBAC in our daily life?
 - Which part of this chapter describes Keystone access control?

RBAC - Process



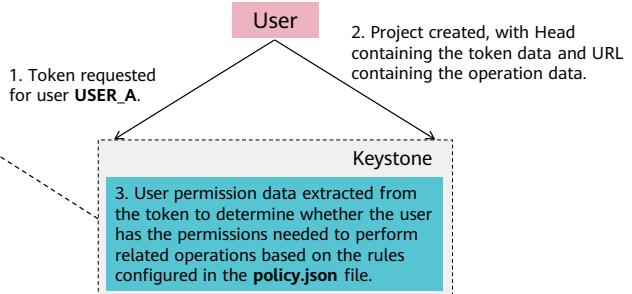
- In OpenStack, RBAC is used for access control. In RBAC, permissions are associated with roles. Users can obtain the permissions of a role by becoming members of that role. RBAC greatly simplifies permissions management. Permissions are directly assigned to roles, and roles are assigned to users. This permission design is clear and easy to manage. RBAC authentication defines relationships between who, what, and how. "Who" represents the owner or subject of permissions, such as User and Role. "What" represents Operation or Object. "How" represents specific permissions, authorization, or privilege. RBAC describes "who" performs "how" operations on "what". As shown in the figure, the client sends a request. The Token module of Keystone verifies the token validity. After the verification is successful, the Policy module verifies the authentication context. The **policy.json** file is a key mechanism for implementing RBAC, which has been mentioned in the Keystone Object Model – Policy part. Generally, the file is generally stored in the configuration file directory of a component. The file takes effect upon the modification. You do not need to restart the service. If the verification is successful, the system performs the next step. If the verification fails, the system returns "403 Forbidden", indicating that the permissions authentication failed.

RBAC - Principles

```
{  
  ...  
  "all_admins": [  
    [ "role:admin"  
    ],  
    [ "role:internal_admin"  
    ]  
  ],  
  ...  
  "identity:list_projects": [  
    [ "rule:all_admins"  
    ]  
  ],  
  "identity:create_projects": [  
    [ "role:admin"  
    ]  
  ]  
  ...  
}
```

The policy module requires the following data for detection:

- Data from the **policy.json** file
- Data added by auth_token to the HTTP header
- User request data



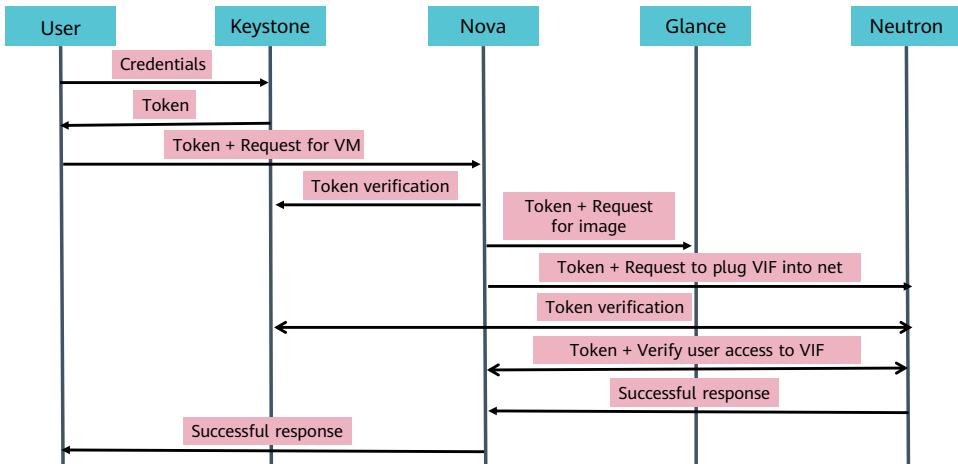
- The Policy module requires three types of data during verification: The first is the **policy.json** file, which is stored in the service configuration directory. The second is the token data added by auth_token to the HTTP header, that is, the token data used in token-based authentication. The third is user request data.
- The **policy.json** file defines the roles (**admin** and **internal_admin**) contained in **all_admin**. It also defines the rules specified in **list_project** for **all_admin**. The **admin** role is required for creating a project.
- During the processing, the system verifies the token validity and checks whether the user has the corresponding role and permissions in the **policy.json** file based on the user request.

Question: How Does Keystone Handle Authentication and Permissions Control?

- When a user creates a VM on the OpenStack dashboard, how does Keystone authenticate the user and verify that the user has the permissions needed to create VMs?
- When a user creates a VM on the OpenStack CLI, how does Keystone authenticate the user and verify that the user has the permission to create VMs?
- Do the two methods differ from each other in Keystone?

- Keystone works the same in terms of authentication and permission control on both the OpenStack Dashboard and OpenStack CLI. It issues and validates tokens, and implements permission control through the **policy.json** file.

Summary: How Does Keystone Implement Authentication and Permissions Control?



40 Huawei Confidential



- The user sends basic information, usually the username and password, to Keystone. After the authentication, Keystone returns a token to the user. The user sends a VM creation request carrying the token information to Nova. After receiving the request, Nova sends the token to Keystone for authentication. After the authentication is successful, Nova starts to create a VM. Nova sends an image application request carrying the token information to Glance, and sends a network request carrying the token information. After receiving the request, Glance and Neutron verify the token validity with Keystone (only one line is used in the figure). If the verification is successful, the corresponding operation is performed and a completion message is returned. After the VM is created, Nova returns a message to the user, indicating that the VM has been created. Then, the user can use the VM.

Quiz

1. Does Keystone depend on other OpenStack services?
2. (Single-answer question) Which of the following Keystone components caches tokens?
 - A. Keystone API
 - B. Keystone Middleware
 - C. Keystone Services
 - D. Keystone Plugins

- 1. Keystone does not depend on other OpenStack services and provides other services with authentication services. As an independent security authentication component in OpenStack, Keystone authenticates OpenStack users, manages tokens, provides service catalogs for accessing resources, and controls access based on user roles.
- 2. B

Summary

- This course described the positioning and functions of the OpenStack Identity service (Keystone), its interaction with other services, related concepts, and working principles, helping you further understand the security assurance mechanism of OpenStack.

More Information

- OpenStack Community
 - <https://www.openstack.org/>

Acronyms

- LDAP: The Lightweight Directory Access Protocol (LDAP) is an open, vendor-neutral, industry standard application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network.
- SAML: Security Assertion Markup Language. It is an XML-based open-standard for transferring identity data between two parties: an identity provider (IdP) and a service provider (SP).
- SQL: The Structured Query Language (SQL) is a domain-specific programming language and a language for database query and program design. It is used to access data and query, update, and manage relational database systems (RDBSs).
- CRUD: The abbreviation of the first letter of the following words: Create, Retrieve, Update, and Delete. These are four basic functions of databases or persistent storage in software systems.

Acronyms

- UUID: Universally Unique Identifier (UUID) is a software construction standard as well as a part of the distributed computing environment of the Open Software Foundation (OSF). Its aim is to enable all elements in a distributed system to have unique identification information. Their uniqueness does not depend on a central authority.
- PKI: is a collection of hardware, software, personnel, policies, and regulations used to generate, manage, store, distribute, and revoke keys and certificates based on the public-key cryptography.

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and
organization for a fully connected,
intelligent world.

Copyright©2022 Huawei Technologies Co., Ltd.
All Rights Reserved.

The information in this document may contain predictive
statements including, without limitation, statements regarding
the future financial and operating results, future product
portfolio, new technology, etc. There are a number of factors that
could cause actual results and developments to differ materially
from those expressed or implied in the predictive statements.
Therefore, such information is provided for reference purpose
only and constitutes neither an offer nor an acceptance. Huawei
may change the information at any time without notice.



OpenStack Image Management



Foreword

- This course describes the positioning and functions of Glance in OpenStack and its interaction with other services. It also describes the working principles and processes of Glance to demonstrate how to create a Glance image.

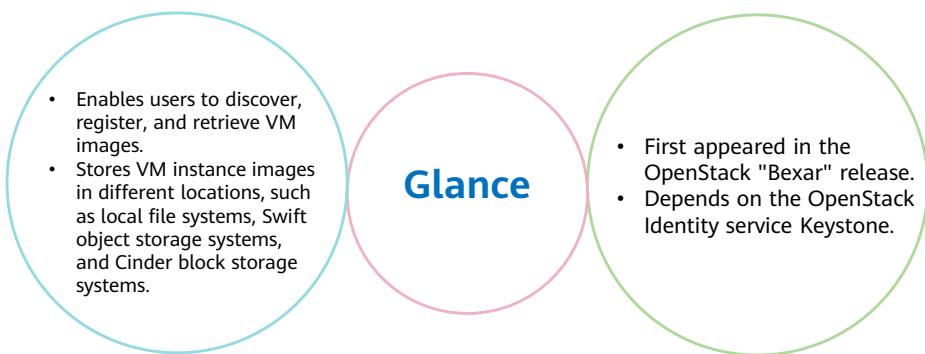
Objectives

- Upon completion of this course, you will understand:
 - The positioning and functions of Glance in OpenStack and its interaction with other services.
 - The architecture, components, and working principles of Glance.
 - The image creation process.

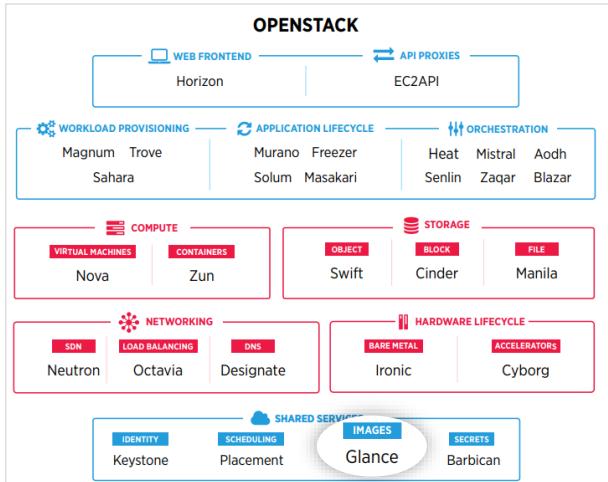
Contents

- 1. Glance Overview**
2. Glance Architecture
3. Glance Working Principles and Processes
4. Glance Image Creation

Image Service: Glance



Positioning of Glance in OpenStack



6 Huawei Confidential

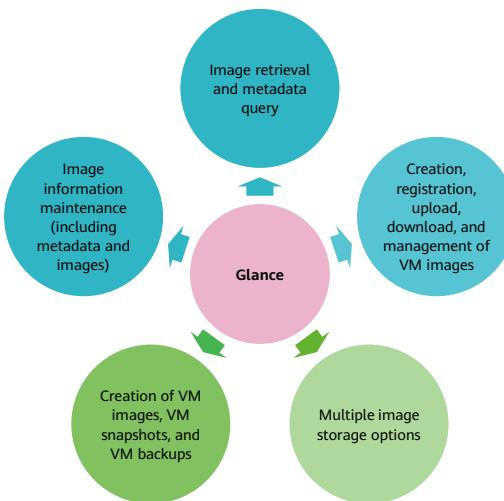
Glance

- Glance has a RESTful API that allows you to query VM image metadata or retrieve the actual image.
- As shown in the figure, Glance belongs to the shared services layer. Users can upload and discover data assets that are meant to be used in conjunction with other services.



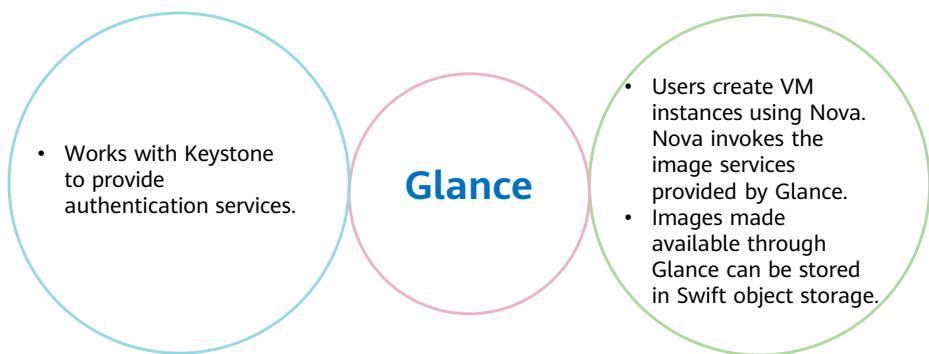
- Data assets currently include images and metadata definitions.
 - Images:** Glance image services include discovering, registering, and retrieving VM images. Glance has a RESTful API that allows querying of VM image metadata as well as retrieval of actual images. VM images made available through Glance can be stored in a variety of locations from simple file systems to object-storage systems like the OpenStack Swift project.
 - Metadata definitions:** Glance hosts a metadefs catalog. This provides the OpenStack community with a method of programmatically determining various metadata key names and valid values that can be applied to OpenStack resources. What we are talking about here is just a catalog. The keys and values will do nothing unless they are applied to individual OpenStack resources using APIs or client tools provided by services responsible for these resources.

Glance Functions



- When creating a VM on OpenStack, you must select the OS to be installed for the VM. Glance offers a range of OS images for you to choose from.
- Image metadata is stored in the database. Images are stored in various backend stores through Glance Store Drivers.

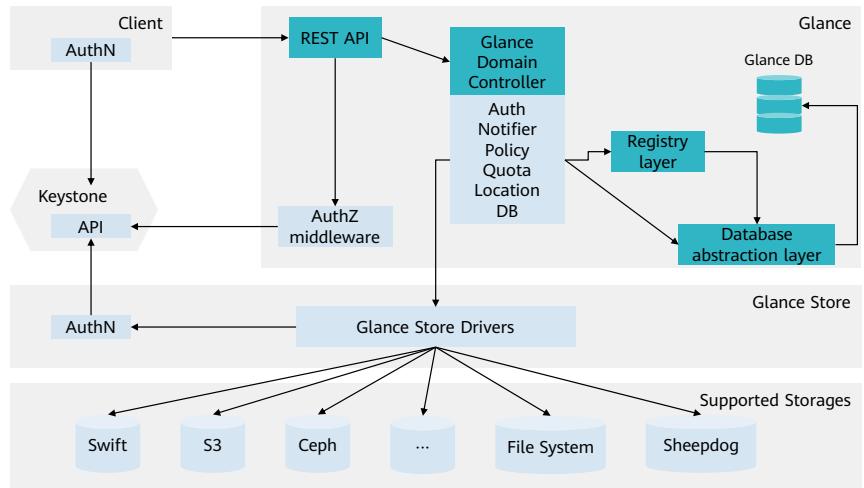
Interactions with Other Services



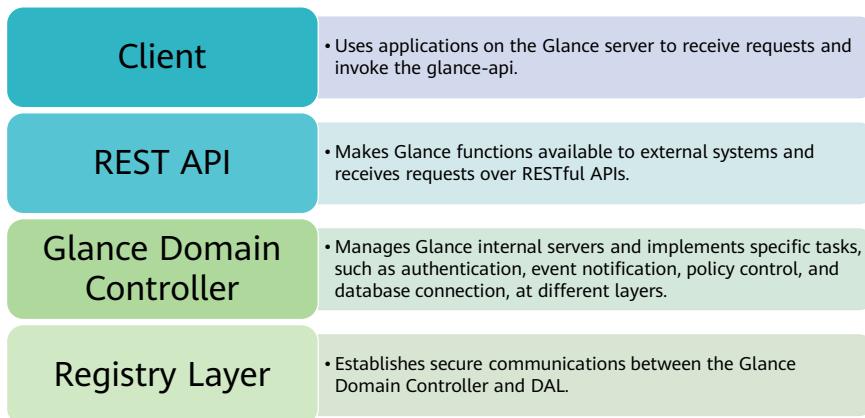
Contents

1. Glance Overview
- 2. Glance Architecture**
3. Glance Working Principles and Processes
4. Glance Image Creation

Glance Architecture



Functions of Glance Components (1)



- **Client:** A client is the Glance service application user, which is the OpenStack command line tool, Horizon, or Nova service.
- **REST API:** Glance has a client-server architecture that provides a REST API for the user through which requests to the server can be performed.
- **Glance Domain Controller:** It is the main middleware implementation in Glance, which is equivalent to a dispatcher. Its role is to distribute the operations of Glance internal services to all layers (Auth, Notifier, Policy, Quota, Location, DB connection). Specific tasks are implemented by each layer.
- **Registry Layer:** It is an optional layer used to organize secure communication between the Glance Domain Controller and the Glance DB by using a separate service.

Functions of Glance Components (2)

Database Abstraction Layer

- Provides unified APIs for Glance and the databases.

Glance DB

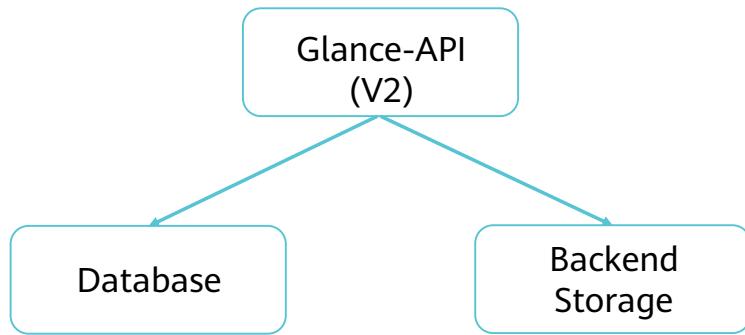
- Is shared among all components and stores management and configuration data.

Glance Store

- Interacts with external storage backends or local file systems to permanently store image files.
- Provides a unified API to access different storage backends.

- Glance DB:** Database Abstraction Layer (DAL).
- Glance uses a central database (Glance DB) that is shared among all the components in the system.
- Glance Store:** is the communication layer between Glance and external storage backends or local file system and provides a uniform interface to access storage backends. All operations on image files are performed by invoking the Glance Store library.

Glance Architecture (Simplified)



- In releases earlier than Newton, Glance supports REST API V1 and V2.
- In REST API V2, Glance-Registry was integrated into Glance-API. When receiving a request related to image metadata, Glance-API directly operates the database without invoking Glance-Registry.
- In REST API V1, Glance-Registry, like Glance-API, is also a WSGI server. However, Glance-Registry processes RESTful requests related to image metadata. After receiving a RESTful request related to metadata from a user, Glance-API forwards the request to Glance-Registry. Note that the RESTful APIs provided by Glance-Registry are provided for Glance-API and are not exposed to external OpenStack users.
- In the Newton release, V1 was outdated. Since the Stein release, Glance-Registry has been deprecated and replaced by Glance-API. The Store module interface is used to support various storage backend systems, including Amazon S3, Cinder/Swift, Ceph, and Sheepdog in the Glance architecture.

Contents

1. Glance Overview
2. Glance Architecture
- 3. Glance Working Principles and Processes**
4. Glance Image Creation

Images, Instances, and Flavors in OpenStack

Image	Instance	Flavor
<ul style="list-style-type: none">A VM image contains a virtual disk that has a bootable operating system installed on it. It provides a template for a VM.	<ul style="list-style-type: none">An instance is a VM running in an OpenStack system.	<ul style="list-style-type: none">A flavor defines the number of virtual CPUs, RAM size, and ephemeral disk size that an instance can have.

- Relationships among images, instances, and flavors:
 - You can launch any number of instances from the same image.
 - Each launched instance is a copy of the image. Modifications to an instance do not affect the image.
 - When launching an instance, you must specify a flavor. The resources available to the instance depends on the flavor.

- When creating an instance, you must specify the image and flavor.

Glance Image Disk Formats

- When adding an image to Glance, you must specify the disk format and container format of the VM image.

Disk Format	Description
raw	An unstructured disk image format.
vhd	A common disk format used by virtual machine monitors from VMware, Xen, Microsoft, VirtualBox, and others.
vhdx	An enhanced version of the vhd format. It has support for larger disk sizes and other enhanced functions.
vmdk	A common disk format.
vdi	A disk format supported by VirtualBox and QEMU.
iso	An archive format for CD-ROMs or DVDs.
ploop	A disk format supported and used by Virtuozzo to run OS Containers.
qcow2	A disk format supported by the QEMU emulator that can expand dynamically and supports copy-on-write.
aki	Amazon Kernel Image
ari	Amazon Ramdisk Image
ami	Amazon Machine Image

- Convert other images to the formats supported by OpenStack before importing them.

Glance Image Container Formats

- When adding an image to Glance, you must specify the disk format and container format of the VM image.

Container Format	Description
bare	There is no container or metadata envelope for the image.
ovf	This is the OVF container format.
ova	This indicates what is stored in Glance is an OVA tar archive.
docker	This indicates what is stored in Glance is a Docker tar archive of the container filesystem.
compressed	The exact format of the compressed file is not specified.
aki	This indicates what is stored in Glance is an Amazon kernel image.
ari	This indicates what is stored in Glance is an Amazon ramdisk image.
ami	This indicates what is stored in Glance is an Amazon machine image.

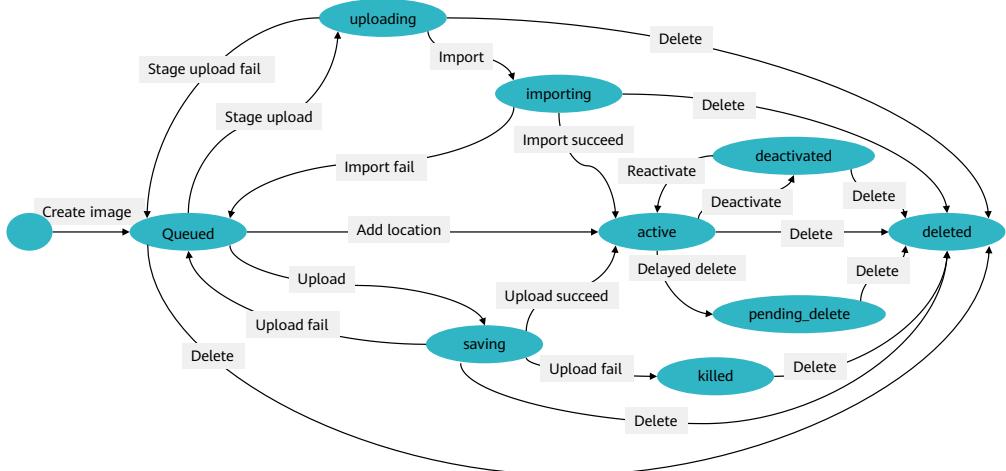
- The container format refers to whether the VM image is in a file format that also contains metadata about the actual VM.
- Note that the container format string is not currently used by Glance or other OpenStack components, so it is safe to simply specify bare as the container format if you are unsure.

Glance State Machines

- Glance has two types of machine states: image states and task states.

Image Status	Description	Task Status	Description
queued	The image identifier has been reserved in glance-registry, but the image data has not been uploaded and the image size has not been initialized.	pending	The task is suspended.
saving	The raw image data is being uploaded to Glance.	processing	The task is being processed.
uploading	The "import data-put" request is invoked for the image.	success	The task was successfully executed.
importing	The image is being imported, but is not ready for use.	failure	The task execution failed.
active	The image has been created and can be used.		
deactivated	This image can only be accessed by administrators.		
killed	An error occurred when uploading the image and the image is unavailable.		
deleted	The image data is still reserved in Glance, but cannot be used. The image will be automatically deleted at a later date.		
pending_delete	This is similar to "deleted", but Glance has not yet removed the image data. However, an image in this state is not recoverable.		

Image Status Transition in Glance

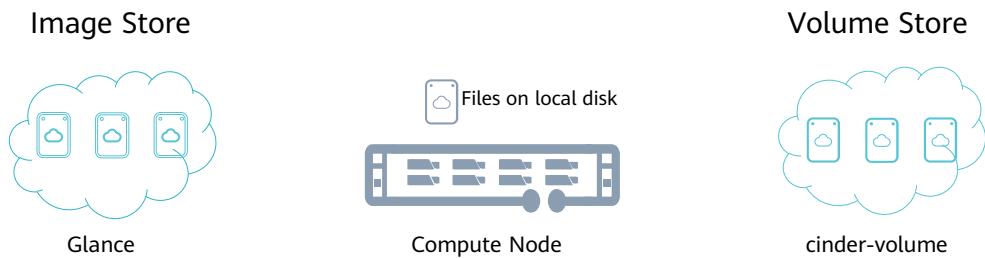


19 Huawei Confidential



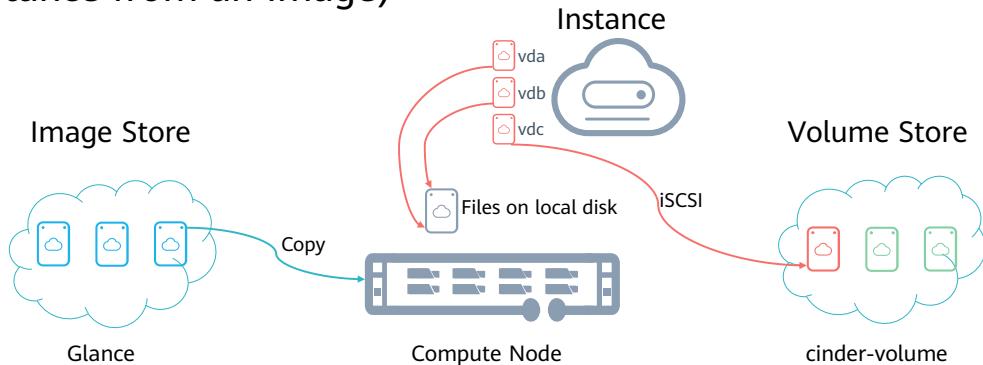
- queued: No image data has been uploaded to Glance. Only metadata in the database exists in Glance.
- saving: An image's raw data is currently being uploaded to Glance. When an image is registered with a call to POST /images and there is an x-image-meta-location header present, that image will never be in the saving status (as the image data is already available in some other location).
- active: An image is fully available in Glance.
- deactivated: Access to image data is not allowed to any non-admin user. Prohibiting downloads of an image also prohibits operations like image export and image cloning that may require image data.
- killed: An error occurred during the uploading of an image's data, and the image is not readable.
- deleted: Glance has retained the information about the image, but it is no longer available to use. An image in this state will be removed automatically at a later date.
- pending_delete: This is similar to deleted. However, Glance has not yet removed the image data. An image in this state is not recoverable.

Interaction Between Images and Instances (Before the Instance Is Launched)



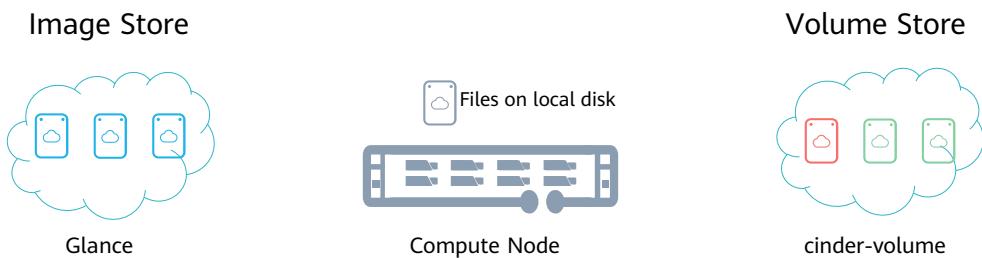
- A Glance store contains a certain number of images, a compute node contains available vCPU, memory, and local disk resources, and a cinder-volume contains a certain number of volumes.

Interaction Between Images and Instances (Launch an Instance from an Image)



- When launching an instance, you need to select an image, a flavor, and any optional attributes. The selected flavor provides a system disk marked as **vda** and an ephemeral disk marked as **vdb**, and the volume provided by cinder-volume is mapped to the third virtual disk **vdc**.
- The image service copies the basic image from an image store to a local disk. **vda** is the first disk accessed by the instance. A smaller image file indicates that only less data should be copied over the network, that is, the instance can be launched at a faster speed.
- When the instance is launched, a blank ephemeral disk **vdb** is created. This disk will be also deleted when the instance is deleted.
- The compute node uses iSCSI to connect to a volume provided by cinder-volume. This volume is mapped to the third disk **vdc**. Once the compute node provides vCPU and memory resources for the instance, the instance is launched from the root volume **vda**. Then, the instance runs and modifies the data on disks (the red icons above are disks).
- If the cinder-volume is on an independent network, the **my_block_storage_ip** option in the configuration file of the storage node redirects the image traffic to the compute node.
- Note:
 - Some details in this example scenario may differ from those in the actual environment. For example, the actual environment can use storage backends and network protocols different from those in this example. A common scenario is that disks **vda** and **vdb** are stored on the SAN storage device instead of a local disk.

Interaction Between Images and Instances (After Instance Deletion)



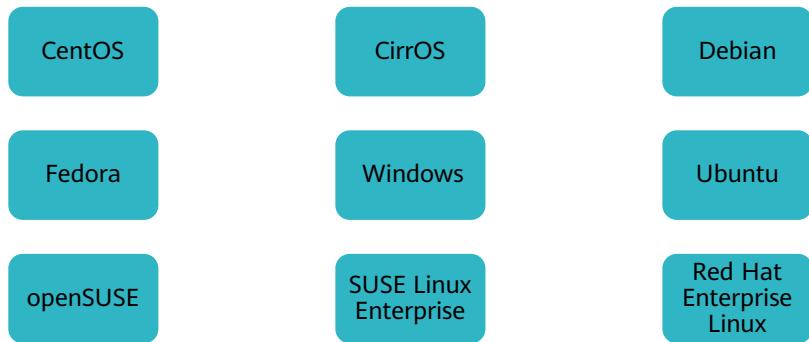
- After the instance is deleted, all resources except the Cinder volumes will be reclaimed. Additionally, the ephemeral disk is cleared regardless of whether it is encrypted, and memory and vCPU resources will be released. During this process, the image keeps unchanged.
- Note:
 - If you select the "Delete volume upon deleting instance" option when creating an instance, the Cinder volumes will also be deleted when the instance is deleted.

Contents

1. Glance Overview
2. Glance Architecture
3. Glance Working Principles and Process
- 4. Glance Image Creation**

Glance Image Creation - Download an Image File

- The simplest way to create a Glance image is to download the OpenStack image file officially released by the system provider. Most images come with **cloud-init** pre-installed. This package supports SSH key pair login and user data ingestion.



- To download the image, visit the OpenStack community website:
 - <https://docs.openstack.org/image-guide/obtain-images.html>

Glance Image Creation - Manually Create an Image

- If the downloaded image does not meet requirements, you can manually create a Glance image file.
- To create an Ubuntu 18.04 image:
 - Use virt-manager to create an Ubuntu 18.04 VM and install the OS on it.
 - Log in to the VM and install the **cloud-init** package.
 - Stop the VM.
 - Pre-delete the VM.
 - Undefine the VM.
 - Create an image.
 - Upload the image.

```
$ sudo apt install cloud-init
```

```
$ sudo shutdown -h now
```

```
$ sudo virt-sysprep -d VM_ID
```

```
$ virsh undefine VM_ID
```

```
$ qemu-img create
```

```
$ openstack image create
```

- The virt-manager is a graphical tool for managing VMs. It provides basic VM management functions, such as starting, suspending, restarting, stopping, forcibly stopping/restarting, and migrating VMs.

Glance Image Creation - Common Tools

- Image creation tools
 - Diskimage-builder
 - This is an automated disk image creation tool that can be used to create Fedora, Red Hat Enterprise Linux, Ubuntu, Debian, CentOS, and openSUSE images.
 - Example: `$ disk-image-create ubuntu vm`
 - Packer
 - Images that are created using this tool can adapt to different cloud platforms, and are ideal for users who use multiple cloud platforms.
 - virt-builder
 - It is used to quickly create a VM and can create various VM images for local or cloud use within several minutes or even shorter time.

Glance Image Creation - Convert an Image

- Command to convert an image: **qemu-img convert**

Image Format	qemu-img Parameter
QCOW2 (KVM, Xen)	qcow2
QED (KVM)	qed
RAW	raw
VDI (VirtualBox)	vdi
VHD (Hyper-V)	vpc
VMDK (VMware)	vmdk

- Example: Convert a RAW image to a QCOW2 image.

```
$ qemu-img convert -f raw -O qcow2 image.img image.qcow2
```

- VBoxManage: Convert a VDI image (VirtualBox) to a RAW image.

```
$ VBoxManage clonehd image.vdi image.img -format raw
```

Quiz

1. (Single-answer question) Which of the following Glance components is shared by all components and stores management and configuration data?
 - A. Glance Store
 - B. Glance DB
 - C. Glance API
 - D. Registry Layer

- 1. B

Summary

- This course described the positioning, functions, architecture, and working principles of the OpenStack Image service (Glance), its interactions with other services, and image creation operations, helping you further understand the OS sources of instances during instance provisioning in OpenStack.

More Information

- OpenStack Community
 - <https://www.openstack.org/>

Acronyms

- API: Application Programming Interface (API) is a particular set of rules and specifications that are used for communication between software programs.
- Amazon S3: Amazon Simple Storage Service (Amazon S3) provides cloud storage through web service interfaces (REST, SOAP, and BitTorrent). It allows users to easily store files on network servers.
- WSGI: Web Server Gateway Interface (WSGI) is an interface that specifies how web servers should forward requests to Python applications or frameworks.

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and
organization for a fully connected,
intelligent world.

Copyright©2022 Huawei Technologies Co., Ltd.
All Rights Reserved.

The information in this document may contain predictive
statements including, without limitation, statements regarding
the future financial and operating results, future product
portfolio, new technology, etc. There are a number of factors that
could cause actual results and developments to differ materially
from those expressed or implied in the predictive statements.
Therefore, such information is provided for reference purpose
only and constitutes neither an offer nor an acceptance. Huawei
may change the information at any time without notice.



OpenStack Compute Management



Foreword

- This course describes the positioning and functions of the OpenStack Dashboard service (Horizon), its interactions with other services, architecture, and GUIs. It also describes the working principles and processes of Nova and typical operations.

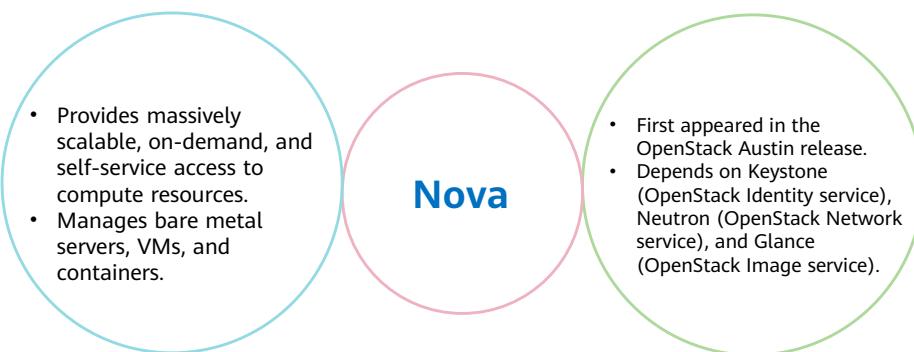
Objectives

- Upon completion of this course, you will understand:
 - The positioning and functions of Nova in OpenStack and its interactions with other services.
 - The architecture, components, and working principles of Nova.
 - The typical operations in Nova.

Contents

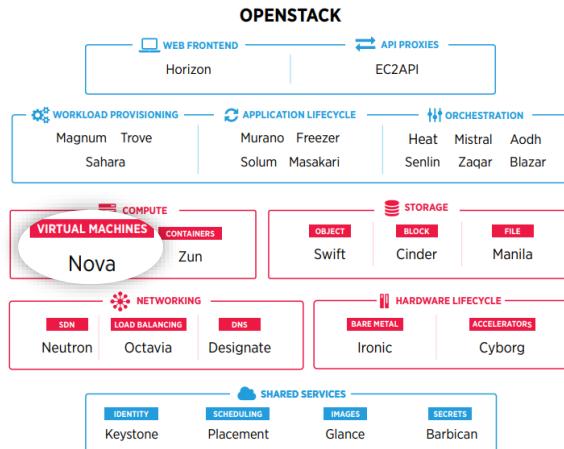
- 1. Nova Overview**
- 2. Nova Architecture
- 3. Nova Working Principles and Processes
- 4. Nova Typical Operations

Compute Service: Nova



- Nova provides compute, storage, and network services in the initial OpenStack releases.
- Now, Nova provides only the compute service, depending on Keystone (OpenStack Identity service), Neutron (OpenStack Network service), and Glance (OpenStack Image service).

Positioning of Nova in OpenStack



Nova

- Nova is a core module of OpenStack and provisions compute resources.
- Nova does not include virtualization software. Instead, it defines drivers that interact with underlying virtualization mechanisms that run on your host operating system, and exposes functionality over a web-based API.



- As shown in the figure, Nova belongs to the compute service layer. Users can use Horizon, Nova clients, APIs, or CLIs to create and manage compute instances.

Mission and Functions of Nova

Mission: Implement services and associated libraries to provide massively scalable, on demand, self-service access to compute resources.

What does Nova do?

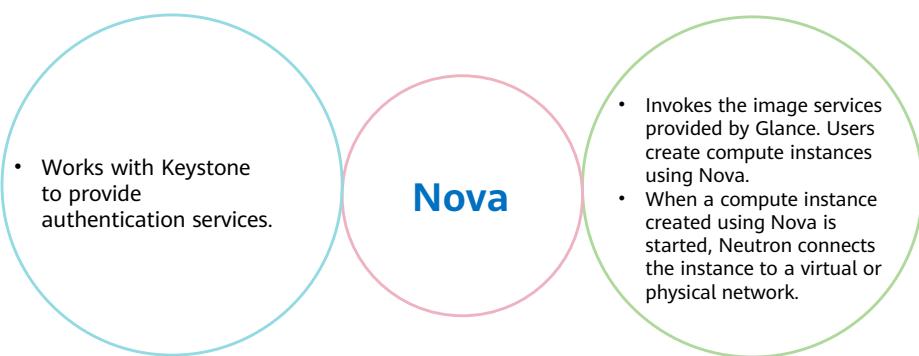
- VM lifecycle management
- Lifecycle management of other compute resources

What does Nova not do?

- Managing the physical hosts VMs run on
- Comprehensive system status monitoring

- Nova is the core of OpenStack and has the following characteristics:
 - It is one of the first two OpenStack projects.
 - It provides the most complex functions and has the largest code size among OpenStack projects.
 - Most integration projects work with Nova.
 - Its contributors have the greatest influence in the community.

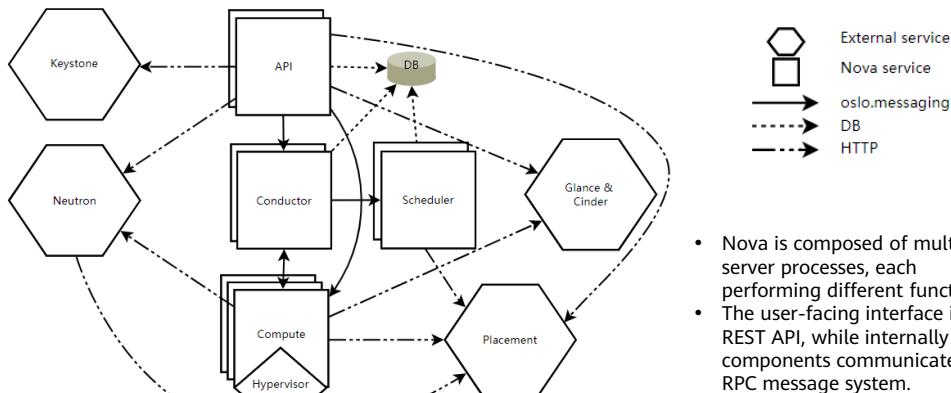
Interactions with Other Services



Contents

1. Nova Overview
- 2. Nova Architecture**
3. Nova Working Principles and Processes
4. Nova Typical Operations

Nova System Architecture



10 Huawei Confidential

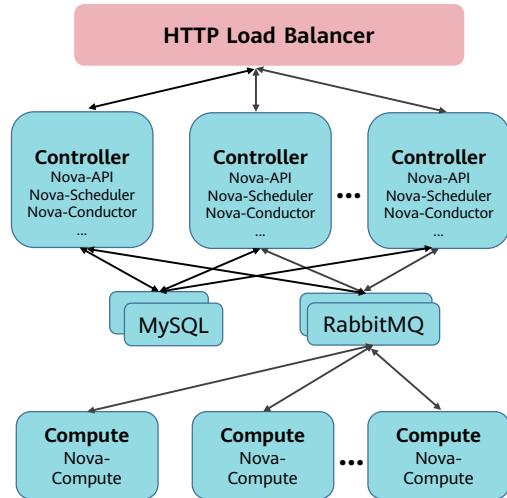


- Nova is composed of multiple server processes, each performing different functions.
- The user-facing interface is a REST API, while internally Nova components communicate via an RPC message system.

- **DB:** SQL database for data storage.
- **API:** Component that receives HTTP requests, converts commands and communicates with other components via the oslo.messaging queue or HTTP.
- **Scheduler:** Decides which host gets each instance.
- **Compute:** Manages communication with hypervisor and virtual machines.
- **Conductor:** Handles requests that need coordination (build/resize), acts as a database proxy, or handles object conversions.
- **Placement:** Tracks resource provider inventories and usages.
- RPC: Remote Procedure Call (RPC) is a computer communication protocol that allows programs running on a computer to invoke sub-programs on another computer. The programmer does not need to program for the interaction.
- The API servers process REST requests, which typically involve database reads/writes, optionally sending RPC messages to other Nova services, and generating responses to the REST calls.
- RPC messaging is done via the oslo.messaging library, an abstraction on top of message queues.
- Nova uses a messaging-based, "shared nothing" architecture and most of the major Nova components can be run on multiple servers, and have a manager

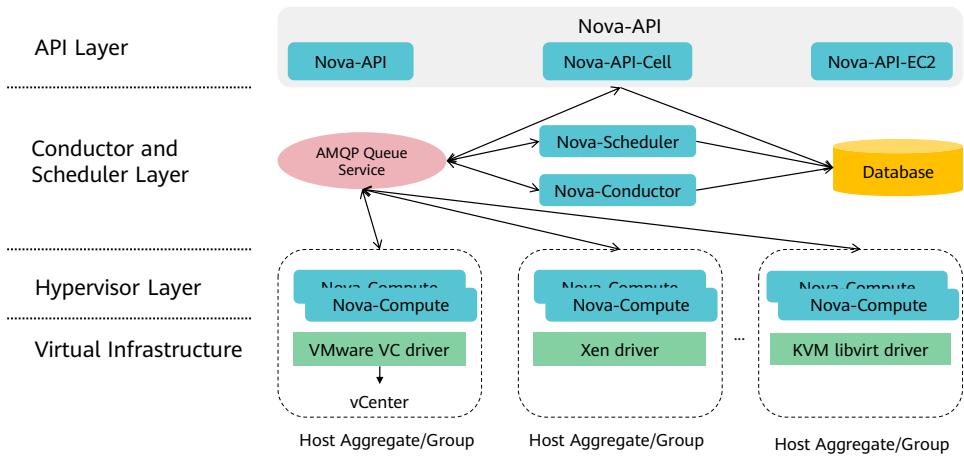
that is listening for RPC messages.

Physical Deployment of Instances



- The architecture is decentralized.
- Components are not locally persistent.
- Horizontal scalability is supported.
- Generally, Nova-API, Nova-Scheduler, and Nova-Conductor components are deployed on the controller nodes.
- Multiple controller nodes are deployed for HA and load balancing.
- The system capacity can be expanded by adding controller nodes and compute nodes.

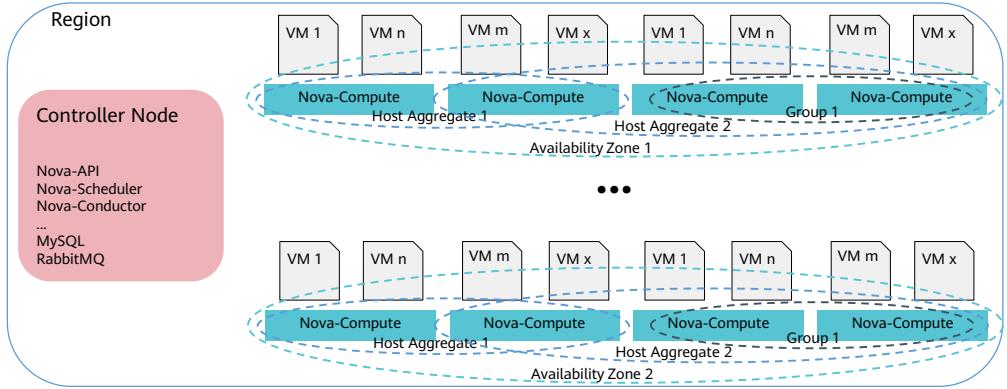
Nova Service Architecture



- The Nova components can be distributively deployed and can be connected to different virtualization platforms using virtDriver.

Nova Resource Pool Management

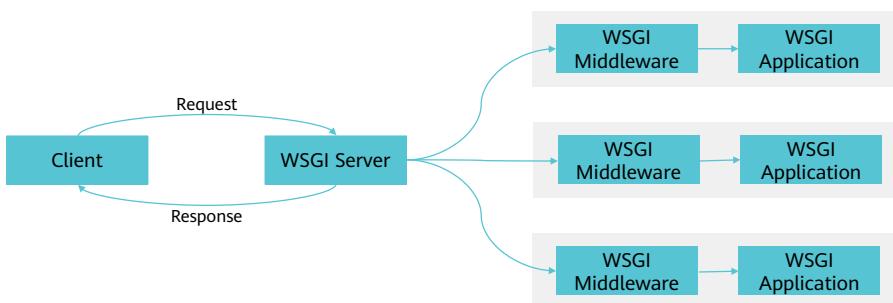
- Region > Availability Zone > Host Aggregate



13 Huawei Confidential



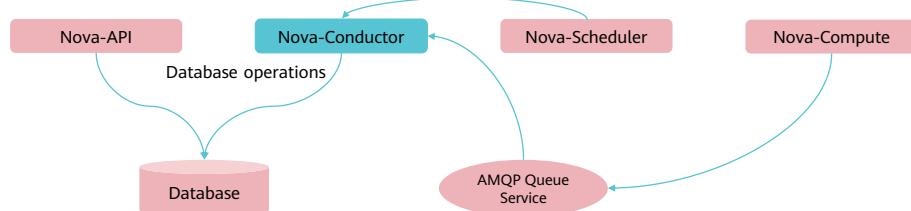
Nova Components - API



- Nova-API:
 - Receives and processes requests from external systems over RESTful APIs.
 - Validates and restrains the transferred parameters.
 - Verifies requested resource quotas and reserves resources accordingly.
 - Creates, updates, deletes, and queries resources.
 - Provides the entry for VM lifecycle management.

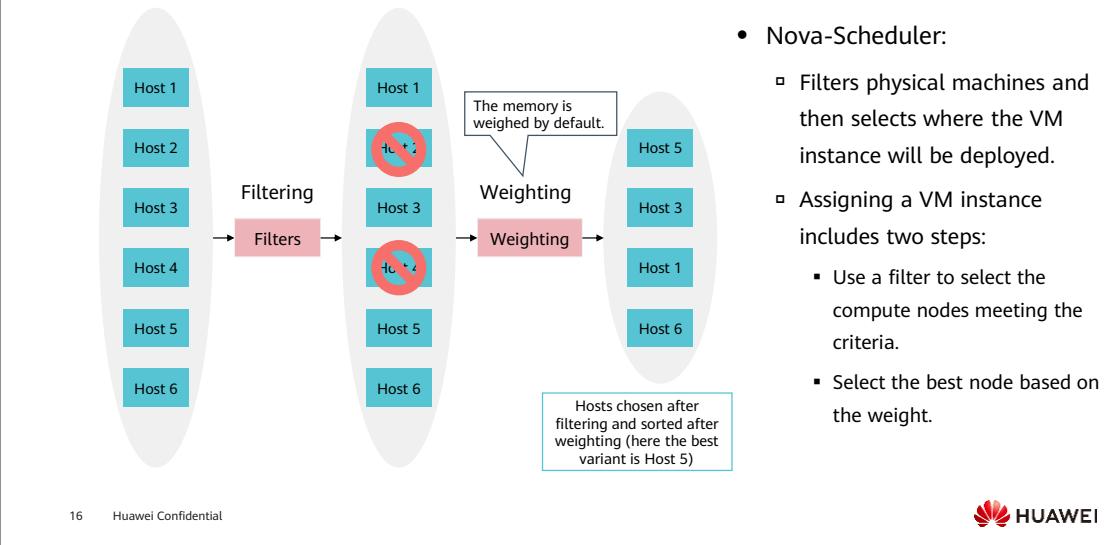
- WSGI: Web Server Gateway Interface

Nova Components - Conductor



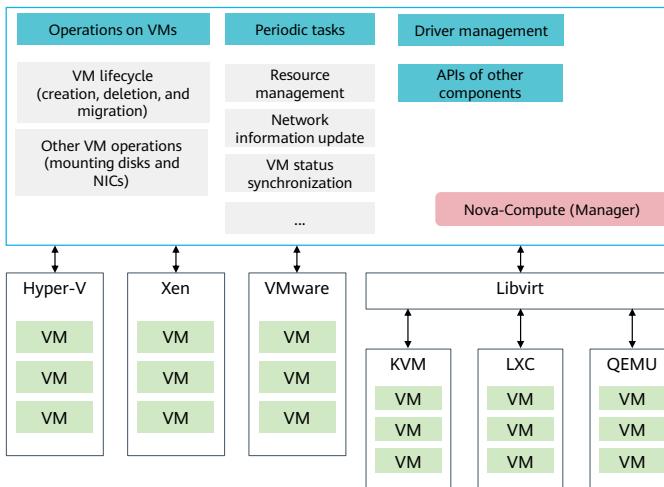
- Nova-Conductor:
 - Provides database operations and decouples Nova-Compute and the database.
 - Provides complex process control, such as creation, cold migration, live migration, VM flavor adjustment, and VM rebuilding.
 - Provides dependencies of other components. For example, Nova-Compute can be started only after Nova-Conductor is successfully started.
 - Periodically writes the heartbeats of other components.

Nova Components - Scheduler



- Nova-Scheduler determines the physical machine where the VM is to be assigned. This process mainly includes two steps: filtering and weighting. When creating a VM, users raise their requirements on resources, such as CPUs, memory, and disks. OpenStack then defines these requirements in the flavor, and users only need to specify the flavor they want when creating a VM.
- The scheduling process is as follows:
 - Use a filter to select the compute nodes meeting the criteria.
 - Select the optimal node based on the weight.

Nova Components - Compute



17 Huawei Confidential



- Nova-Compute framework
 - Manager
 - Driver
- Virtualization platforms connected with Nova-Compute
 - KVM
 - VMware
 - Xen
 - LXC
 - QEMU
 - ...

- The executor of VM lifecycle operations invokes the driver of the corresponding hypervisor.
- The underlying layer connects to different virtualization platforms, such as KVM, VMware, Xen, and Ironic.
- Built-in periodic tasks are used to update resources and synchronize the VM status.
- The resource management module (resource_tracker) works with the plug-in mechanism to collect statistics on resources.

Contents

1. Nova Overview
2. Nova Architecture
- 3. Nova Working Principles and Processes**
4. Nova Typical Operations

VM States

ID	Name	Status	Task State	Power State	Networks
bc9caedc-d415-48e2-936a-9a880f3d6bf1	lft_01	ACTIVE	-	Running	sriov3_net=129.1.223.6
7dd682c2-0605-4d2d-b3aa-907c2fa39e8e	vm_yqb	ACTIVE	-	Running	ovs_net=129.1.211.37
bdf7e69a-4dec-4754-8a13-4883e9001437	yy_1	ACTIVE	-	Running	ovs_net=129.1.211.38

- VM States:
 - **vm_state**: indicates the VM state recorded in the database.
 - **task_state**: indicates the current state of a VM task. The value can be **Intermediate** or **None**.
 - **power_state**: indicates the VM state obtained from the hypervisor.
 - **status**: indicates the VM state displayed externally.
- Relationships between states:
 - The system records only **vm_state**, **task_state**, and **power_state**.
 - The result of **status** is generated based on both **vm_state** and **task_state**.
- Example:
 - If the value of **vm_state** is **active** and that of **task_state** is **rebooting**, **REBOOT** will be displayed for **status**.
 - If the value of **vm_state** is **building**, **BUILD** will be displayed for **status**.

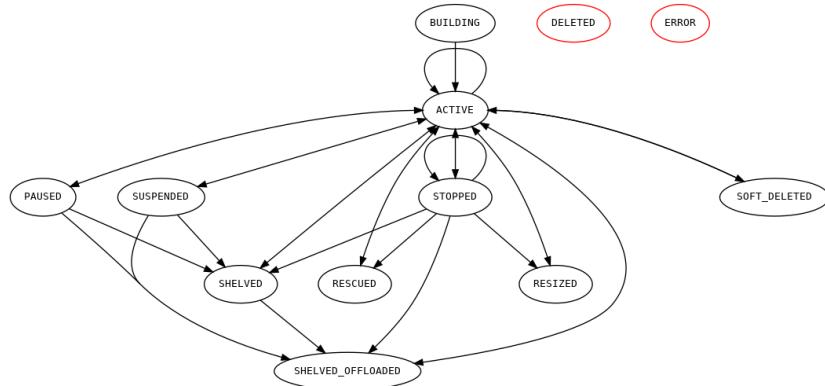
VM States

vm_state	task_state	status
active	rebooting	REBOOT
	reboot_pending	REBOOT
	reboot_started	REBOOT
	rebooting_hard	HARD_REBOOT
	reboot_pending_hard	HARD_REBOOT
	reboot_started_hard	HARD_REBOOT
	rebuild_block_device_mapping	REBUILD
	rebuilding	REBUILD
	rebuild_spawning	REBUILD
	migrating	MIGRATING
	resize_prep	RESIZE
	resize_migrating	RESIZE
	resize_migrated	RESIZE
	resize_finish	RESIZE
	default	ACTIVE

vm_state	task_state	status
stopped	resize_prep	RESIZE
	resize_migrating	RESIZE
	resize_migrated	RESIZE
	resize_finish	RESIZE
	default	SHUTOFF

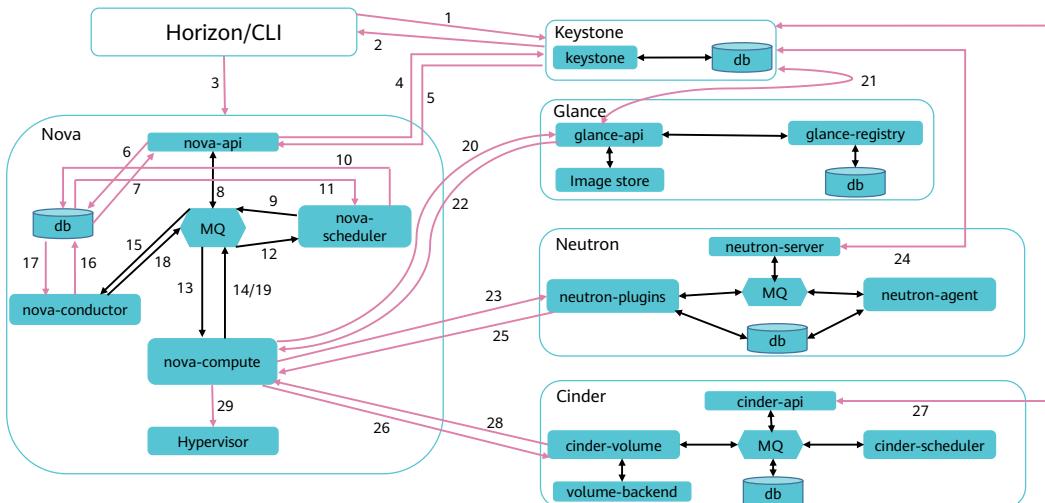
VM State Transitions

VM state transitions allowed by OpenStack



- For details about the VM states and task states for various commands issued by users, see <https://docs.openstack.org/nova/latest/reference/vm-states.html?highlight=vm>.

Nova VM Creation Process



22 Huawei Confidential



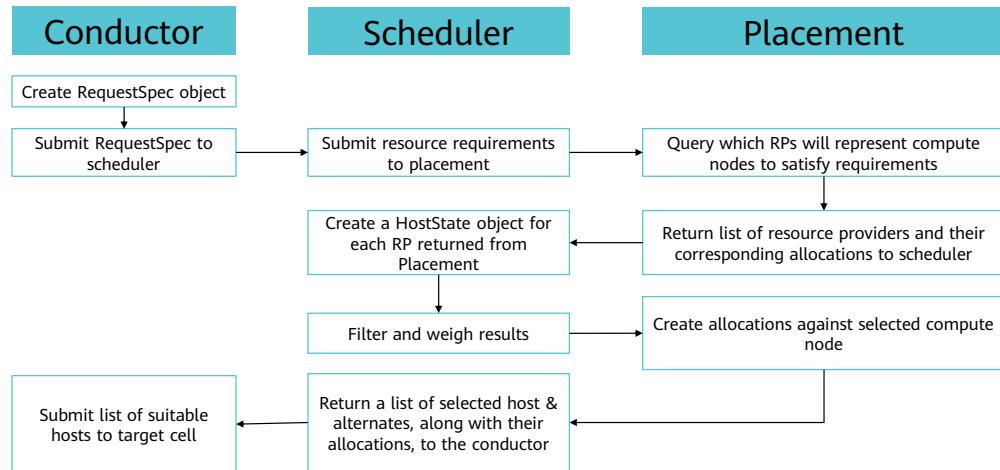
- Step 1: The Horizon Dashboard or OpenStack CLI gets user credentials and authenticates with Keystone via the RESTful API.
- Step 2: Keystone authenticates the user with the user credentials and then generates and sends back an auth-token.
- Step 3: The Horizon or CLI sends a boot instance request, which carries the auth-token, to nova-api over the RESTful API.
- Step 4: nova-api gets the request and sends that request to Keystone for validation of the auth-token and access permission.
- Step 5: Keystone validates the token and sends the updated authentication headers with roles along with the permissions. (Note: Some operations require role permissions.)
- Step 6: After getting the response from Keystone, nova-api interacts with nova-database.
- Step 7: nova-api creates initial database entry for the new instance or VM.
- Step 8: nova-api sends the rpc.call request to nova-scheduler expecting to get updated instance entry with Host ID specified.
- Step 9: nova-scheduler picks the request from the queue.
- Step 10: nova-scheduler talks to nova-database to locate an appropriate host using the filtering and weighting mechanism.
- Step 11: nova-scheduler returns the updated instance entry with the appropriate host ID after filtering and weighting.

- Step 12: nova-scheduler sends the rpc.cast request to nova-compute for launching an instance on the appropriate host.
- Step 13: nova-compute picks the request from the queue.
- Step 14: nova-compute sends the rpc.call request to nova-conductor to get the VM or instance information.
- Step 15: nova-conductor picks the request from the queue.
- Step 16: nova-conductor interacts with nova-database based on the request message.
- Step 17: nova-conductor gets the instance information from nova-database.
- Step 18: nova-conductor sends the instance information to the queue.
- Step 19: nova-compute picks the instance information from the queue.
- Step 20: nova-compute sends an HTTP request using the auth-token obtained from the Keystone RESTful API to glance-api to get the image required for creating the VM.
- Step 21: glance-api validates the auth-token with Keystone.
- Step 22: After the token is verified, nova-compute gets the image URL.
- Step 23: nova-compute sends an HTTP request using the auth-token obtained from the Keystone RESTful API to neutron-server to get the network required for

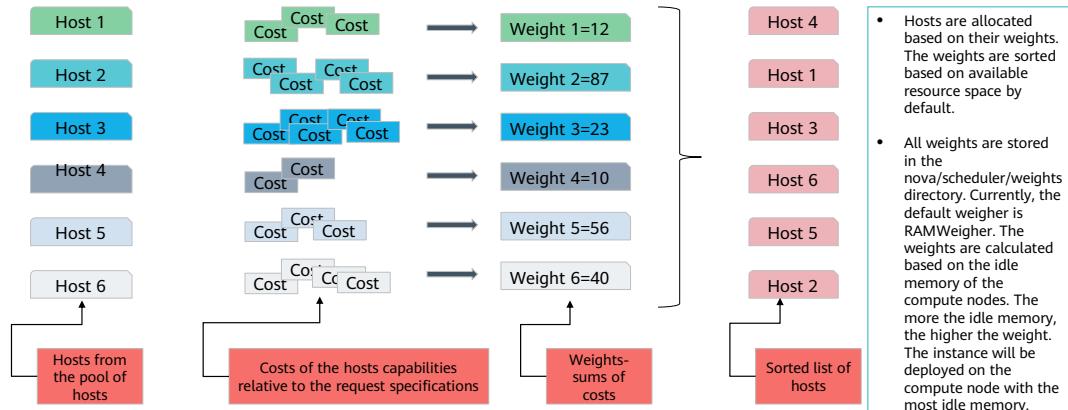
creating the VM.

- Step 24: neutron-server validates the auth-token with Keystone.
- Step 25: After the token is verified, nova-compute gets the network information.
- Step 26: nova-compute sends an HTTP request using the auth-token obtained from the Keystone RESTful API to cinder-api to get the persistent storage required for creating the VM.
- Step 27: cinder-api validates the auth-token with Keystone.
- Step 28: After the token is verified, nova-compute gets the block storage information.
- Step 29: nova-compute generates data for the hypervisor driver and executes the request on the hypervisor.

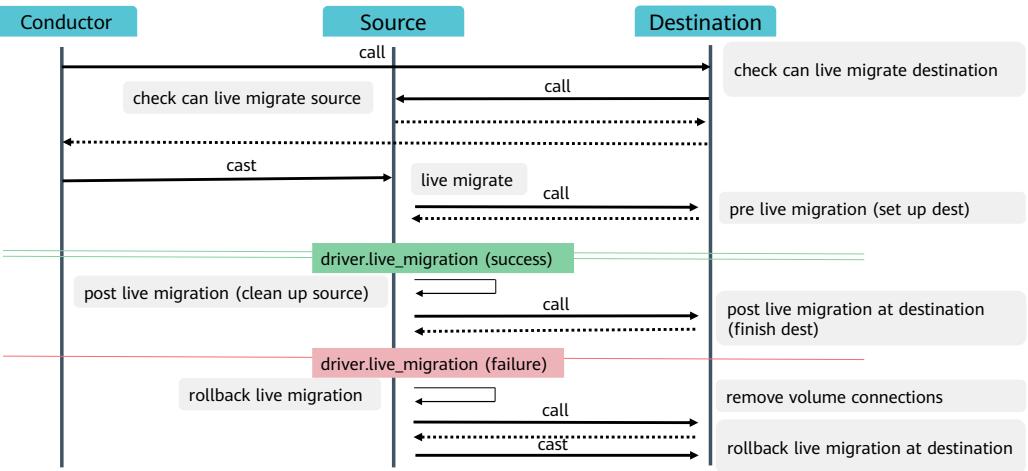
Nova Scheduling Process



Nova Filter Scheduler



Live Migration Principles



- After the migration is successful, information about the source node will be deleted.
- If the migration fails, a rollback is performed and the information about the destination node is cleared.

Contents

1. Nova Overview
2. Nova Architecture
3. Nova Working Principles and Processes
- 4. Nova Typical Operations**

Nova Typical Operations

Category	Description
VM lifecycle management	VM creation, deletion, startup, shutdown, restart, rebuilding, flavor change, pause, pause cancellation, suspension, resume, migration, online migration, locking, unlocking, evacuation, rescue, unrescue, shelving, shelving deletion, shelving restoration, backup, VM image export, as well as list, details, and information query and password change.
Volume and snapshot management	These operations are essentially the encapsulations of Cinder APIs and include creating or deleting a volume or snapshot, listing volumes or snapshots, and querying their details.
Operations on volumes	Attaching or detaching a volume to or from a VM, and querying VM the volume list and details.
Operations on networks	These operations are essentially the encapsulations of Neutron APIs and include creating or deleting a virtual network, and querying the virtual network list and details.
Operations on NICs	Attaching or detaching a NIC to or from a VM, and querying the VM NIC list.
Operations on images	These operations are essentially the encapsulations of Glance APIs, and include creating or deleting an image, as well as querying the image list and details.
Operations on other resources	Operations on flavors, host aggregates, key pairs, and quotas.

Major Operation Objects of Nova (1)

Name	Description	Remarks
Server	VM	The most important data object in Nova.
Server metadata	VM metadata	It is used to add additional description information in key-value format to a VM.
Flavor	Flavor template of a VM	It is used to define the VM type, for example, a VM with two vCPUs, 4 GB memory, and 40 GB local storage space. A flavor is created by the system administrator and used by common users for VM creation.
Quota	Resource quota	It is used to specify the limit of the logical resources that can be used by a tenant.
Hypervisor/node	Node	For virtualization technologies such as KVM and Xen, a node corresponds to a physical host. For vCenter, a node corresponds to a cluster.
Host	Host	For virtualization technologies such as KVM and Xen, a host corresponds to a physical host and also a node. For vCenter, a host corresponds to a set of vCenter environment.
Host aggregate	Host aggregate	A host aggregate contains multiple hosts. Physical hosts in a host aggregate have the same physical resource features, for example, the CPU model.

Major Operation Objects of Nova (2)

Name	Description	Remarks
Server group	A VM affinity or anti-affinity group	VMs in the same affinity group are scheduled to the same physical host during creation. VMs in the same anti-affinity group are scheduled to different physical hosts during creation.
Service	A Nova service	It manages the status of Nova-related services, including nova-compute, nova-conductor, nova-scheduler, nova-novncproxy, nova-consoleauth, and nova-console.
BDM	Block device mapping	It is a block storage device used to describe the information about the storage device of a VM.
Image	Image file	It contains the operating system and is used to create VMs.

Quiz

1. (Single-answer question) Which of the following Nova processes is responsible for managing the VM lifecycle?
 - A. Nova-API
 - B. Nova-Compute
 - C. Nova-Conductor
 - D. Nova-Scheduler

- 1. B

Summary

- This course described the positioning, functions, architecture, and working principles of the OpenStack Compute service (Nova), its interactions with other services, and typical operations, helping you further understand instance provisioning in OpenStack.

More Information

- OpenStack Community
 - <https://www.openstack.org/>

Acronyms

- API: Application Programming Interface (API) is a particular set of rules and specifications that are used for communication between software programs.
- CLI: Command-Line Interface (CLI) is a means of communication between a program and its user, based solely on textual input and output. Commands are input with the help of a keyboard or similar device and are interpreted and executed by applications. Results are output as text or graphics to the interface.
- EC2: Elastic Compute Cloud (EC2) is a web service system developed by Amazon, which allows users to rent applications to run their own VMs.
- HTTP: Hypertext Transfer Protocol (HTTP) is an application-layer protocol used for communication between web servers and browsers or other programs.

Acronyms

- KVM: Kernel-based Virtual Machine (KVM) is an open-source virtualization technology built in Linux. Specifically, KVM helps users turn Linux into a hypervisor that enables a host computer to run multiple isolated virtual environments, that is virtual clients or VMs.
- MQ: A distributed message queue (MQ) is used for message transmission for each service and service management. The MQ service can transmit messages inside a zone or across zones and must be scaled up horizontally to support large-capacity concurrent message requests and provide software development kits (SDKs) for other services.
- QEMU: The Quick Emulator (QEMU) is an emulation processor, written by Fabrice Bellard, that distributes source code under a general public license (GPL).
- Web: World Wide Web (Web) is a global, interactive, dynamic, cross-platform, distributed, graphical information system based on the hypertext and HTTP.

Acronyms

- WSGI: Web Server Gateway Interface (WSGI) is an interface that specifies how web servers should forward requests to Python applications or frameworks.
- Xen: A Xen hypervisor is an open source VMM that adopts the paravirtualization technology and implements CPU scheduling and memory allocation among VMs. The Xen hypervisor virtualizes a hardware layer and controls VM operations, but does not deal with the network, storage device, video, and other input/output (I/O).

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and
organization for a fully connected,
intelligent world.

Copyright©2022 Huawei Technologies Co., Ltd.
All Rights Reserved.

The information in this document may contain predictive
statements including, without limitation, statements regarding
the future financial and operating results, future product
portfolio, new technology, etc. There are a number of factors that
could cause actual results and developments to differ materially
from those expressed or implied in the predictive statements.
Therefore, such information is provided for reference purpose
only and constitutes neither an offer nor an acceptance. Huawei
may change the information at any time without notice.



OpenStack Storage Management



Foreword

- This course describes the storage types provided by OpenStack. Users can select storage services based on service demands. It focuses on the positioning, functions, architecture, and working principles of Cinder (block storage service) and Swift (object storage service) in OpenStack, and their interactions with other services.

Objectives

- Upon completion of this course, you will understand:
 - The differences between OpenStack storage types.
 - The positioning and functions of Cinder in OpenStack and its interactions with other services.
 - The positioning and functions of Swift in OpenStack and its interactions with other services.
 - The architecture and working principles of Cinder.
 - The architecture and working principles of Swift.

Contents

- 1. OpenStack Storage Overview**
2. Block Storage Service: Cinder
3. Object Storage Service: Swift

OpenStack Storage Types

- Two OpenStack storage types are available: ephemeral storage (non-persistent storage) and persistent storage.

Ephemeral Storage

- With ephemeral storage, the disks associated with VMs are ephemeral, meaning that all data in a VM will disappear when the VM is terminated, restarted, or deleted.
- If you only deploy OpenStack Compute service (Nova), the disks associated with VMs are ephemeral by default, meaning that from the user's point of view they disappear when a VM is terminated.
- By default, data in the ephemeral storage is stored as files on local disks of compute nodes.

Persistent Storage

- Persistent storage means that the storage resource outlives any other resource and is always available regardless of whether the VM is terminated, thereby maintaining data availability and security.
- OpenStack explicitly supports three types of persistent storage: object storage, block storage, and file-based storage.

- Ephemeral disks can be:
 - Created and attached locally on the storage of compute nodes.
 - Hosted on external storage by the means of NFS mount. (When using this method to create an ephemeral disk, you can migrate the VM among multiple compute nodes because the root disk of the VM is located on the shared storage that can be accessed by multiple physical hosts.)

Differences Between OpenStack Storage Types

	Application	Accessed Through	Accessible From	Managed By	Persists Until	Size Determined By	Example of Typical Usage
Ephemeral storage	Running an OS and providing scratch space	A file system	Within a VM	Nova	VM is terminated	Administrator configuration of size settings, known as flavors	10 GB first disk, 20 GB second disk
Block storage	Add additional persistent storage to a VM	A block device that can be partitioned, formatted, and mounted (such as, <code>/dev/vdc</code>)	Within a VM	Cinder	Deleted by user	User specification in initial request	1 TB disk
Object storage	Store data, including VM images	The REST API	Anywhere	Swift	Deleted by user	Amount of available physical storage and data copies	Tens of TBs of dataset storage
Shared file system storage	Add additional persistent storage to a VM	A Shared File Systems service share that can be partitioned, formatted and mounted (such as <code>/dev/vdc</code>)	Within a VM	Manila	Deleted by user	<ul style="list-style-type: none"> • User specification in initial request • Requests for extension • Available user-level quotes • Limitations applied by administrators 	NFS

OpenStack Persistent Storage

Block Storage (Cinder)

- It stores data in volumes that can be directly attached to hosts. Block storage is usually used as the host storage space or to store database applications. Both DAS and SAN environments can provide block storage.

Object Storage (Swift)

- It manages data as objects. An object name represents a domain address. Objects can be accessed via RESTful APIs.

File Storage (Manila)

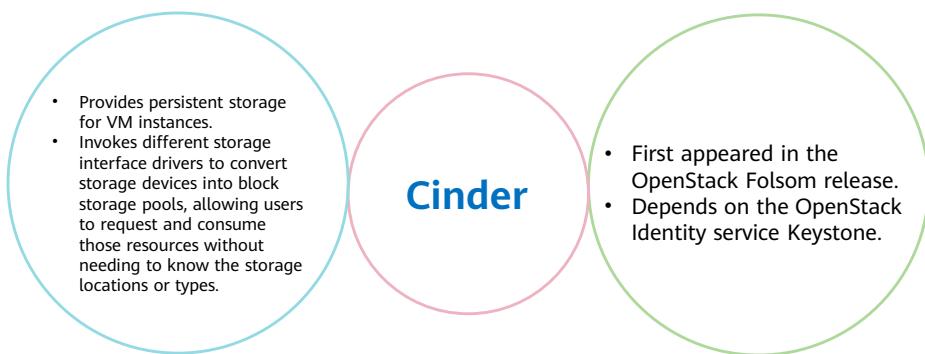
- It stores data in files and folders. With a file system added to the storage system, data can be accessed using the NFS or CIFS protocol.

Manila is rarely used. This chapter mainly describes Cinder and Swift.

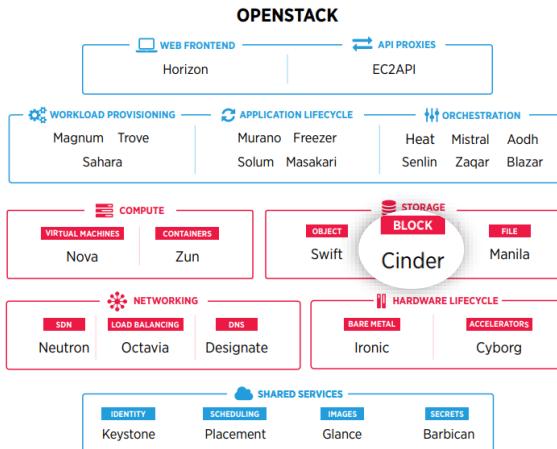
Contents

1. OpenStack Storage Overview
2. **Block Storage Service: Cinder**
 - Cinder Overview
 - Cinder Architecture
 - Cinder Working Principles
 - Cinder Exercises
3. Object Storage Service: Swift

Block Storage Service: Cinder



Positioning of Cinder in OpenStack



Cinder

- Cinder is the OpenStack Block Storage service for providing volumes to Nova virtual machines, Ironic bare metal hosts, containers and more.
- Cinder has a unified interface for backend storage devices and also provides a set of drivers to support different storage protocols. In this way, different vendors' storage devices are integrated in OpenStack.



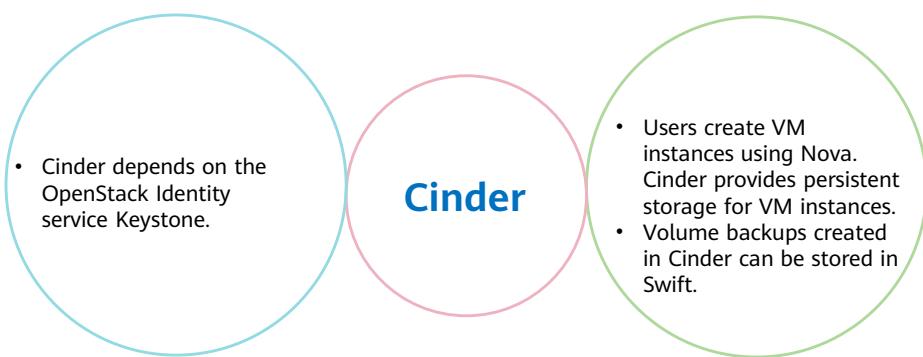
- Cinder was originally known as nova-volume when it was a component of Nova. Then, it was developed separately as an OpenStack component. Therefore, the design architecture of Cinder is similar to that of Nova. The functions of each subcomponent of Cinder are basically the same.

Cinder Functions

- Cinder introduces logical volumes between VMs and storage devices. Cinder is not a storage technology and does not manage or provide services for block devices.
- Cinder serves as an abstraction layer, providing unified interfaces for different technologies of backend storage devices.
- Different block device service vendors integrate those interfaces with OpenStack as drivers in Cinder.

- Cinder serves as an abstraction layer, providing unified interfaces for different storage technologies (such as DAS, NAS, SAN, object storage, and distributed file systems).

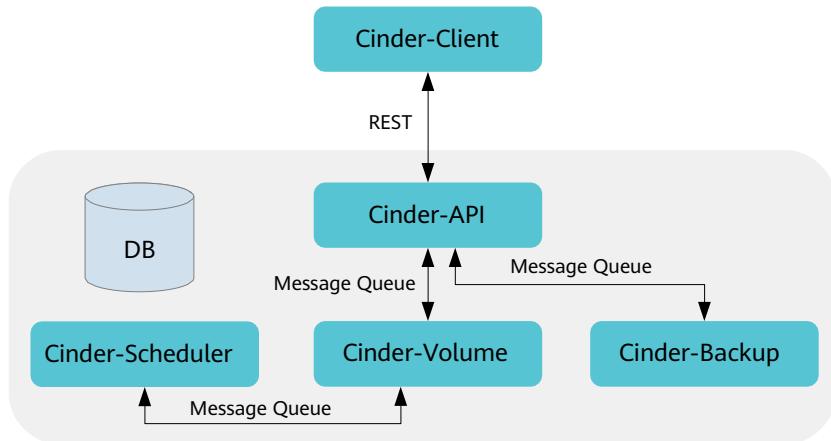
Interactions with Other Services



Contents

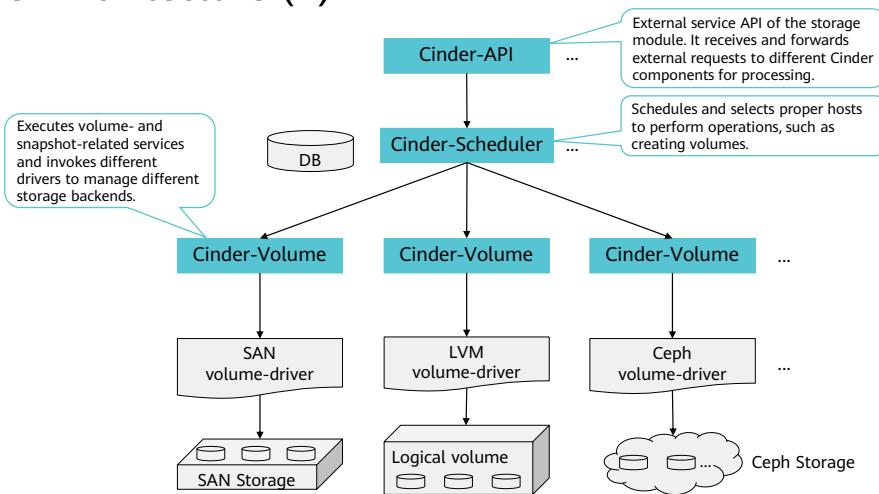
1. OpenStack Storage Overview
2. **Block Storage Service: Cinder**
 - Cinder Overview
 - **Cinder Architecture**
 - Cinder Working Principles
 - Cinder Exercises
3. Object Storage Service: Swift

Cinder Architecture (1)



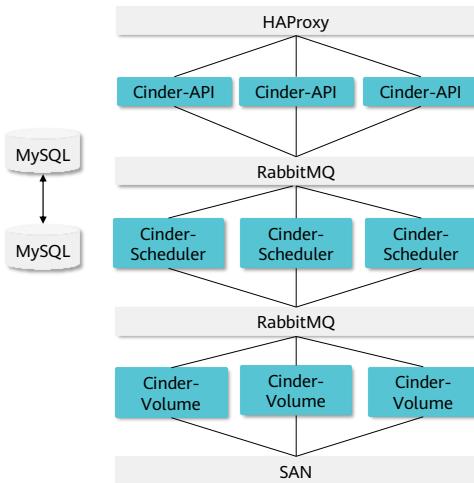
- Cinder-Client encapsulates REST APIs provided by Cinder, so that users can access these APIs in CLI mode.
- Cinder-API provides a REST API to the external to parse operation requirements and route the API to find the troubleshooting method. Operations include adding, deleting, modifying, and querying volumes (creating volumes from existing volumes, images, or snapshots); adding, deleting, modifying, querying, and backing up snapshots; managing volume types; attaching and detaching volumes (via Nova).
- Cinder-Scheduler collects capacity and capability information reported by the backend, and completes scheduling from volumes to specified cinder-volumes based on preset algorithms.
- Cinder-Volume is deployed on multiple nodes. Different configuration files are used to enable connection to different backend devices. Storage vendors insert driver codes to enable interaction with storage devices to collect capacity and capability information and perform volume operations.
- Cinder-Backup backs up data from volumes to other storage media (with driver provided by Swift, Ceph, and TSM at present).
- SQL DB provides data such as storage volumes, snapshots, backups, and services and supports SQL databases, including MySQL, PostgreSQL, and Microsoft SQL Server.

Cinder Architecture (2)



- By default, Cinder uses Logical Volume Manager (LVM) as backend storage. LVM abstracts logical volumes between the operating system and physical storage resources to address the problems of traditional disk partition management tools.
- LVM combines various physical volumes such as disk partitions into a volume group. LVM creates a logical volume from the volume group and then installs file systems such as ext3 and ReiserFS on the logical volume.
- Cinder drivers are available to enable storage devices developed based on different technologies (for example, SAN, Ceph, and Sheepdog) or by different vendors (for example, EMC and Huawei) to serve as backends for OpenStack Cinder.

Cinder Deployment (for SAN Storage)



- Cinder-API, Cinder-Scheduler, and Cinder-Volume can be deployed on the same node or on different nodes.
- Cinder-API works in AA mode, HAProxy is used as LB, and requests are distributed to multiple Cinder APIs.
- Cinder-Scheduler also works in AA mode. RabbitMQ distributes tasks to three nodes evenly, and the capability information reported by Cinder-Volume is collected from RabbitMQ. During the scheduling, Cinder-Scheduler ensures data consistency through reserved resources in the database.
- Cinder-Volume also works in AA mode. It reports the same backend capacity and capability information, and accepts the request for processing.
- RabbitMQ supports active/standby or cluster deployment.
- MySQL supports active/standby or cluster deployment.

Cinder Components - API

- Cinder-API makes REST APIs available, parses operation requests, and makes processing decisions:
 - Create, delete, list, or show volumes.
 - Create, delete, list, or show snapshots.
 - Attach or detach volumes (invoked by Nova).
 - Operations on:
 - Volume types
 - Quotas
 - Backups

Cinder Components - Scheduler

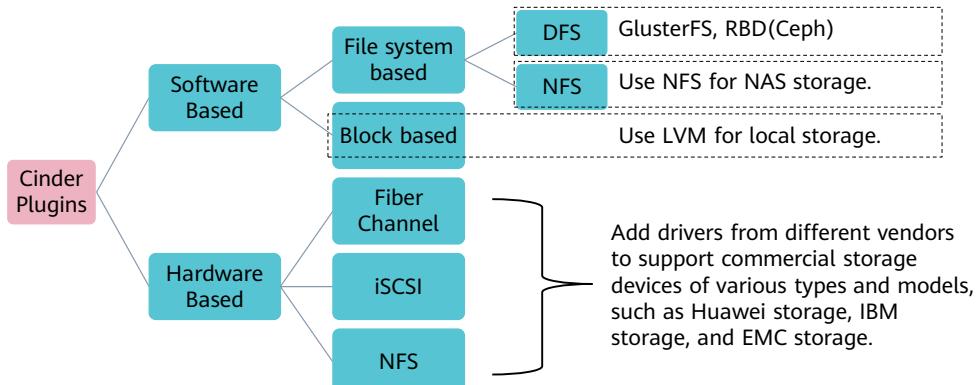
- Cinder-Scheduler collects capacity and capability information reported by the backend, and completes scheduling from volumes to specified cinder-volumes based on preset algorithms.
- Cinder-Scheduler identifies appropriate backends through filtering and weighting.



- Backends are filtered based on their capabilities.
 - Drivers periodically report the capability and status of backends.
 - The administrator creates a volume type.
 - Users specify a volume type when creating a volume.

Cinder Components - Volume

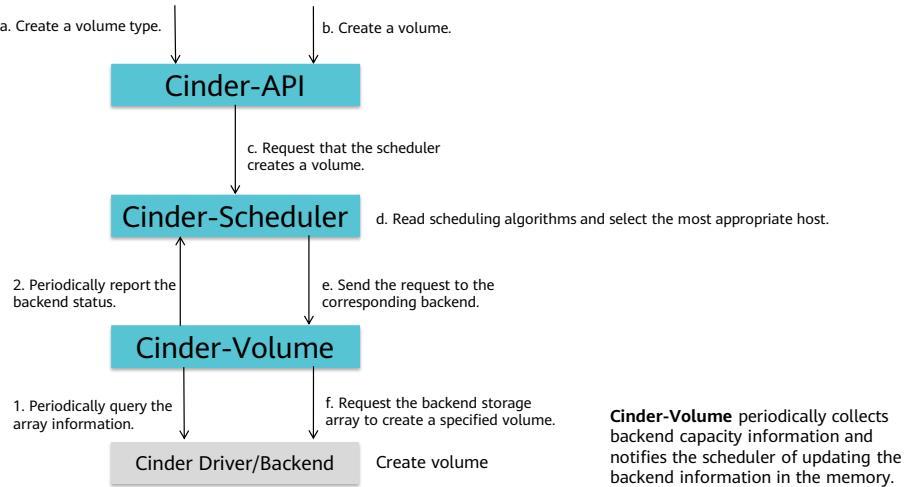
- Cinder-Volume is deployed on multiple nodes. Different configuration files are used to enable connection to different backend devices. Storage vendors insert driver codes to enable interaction with storage devices to collect capacity and capability information and perform volume operations.



Contents

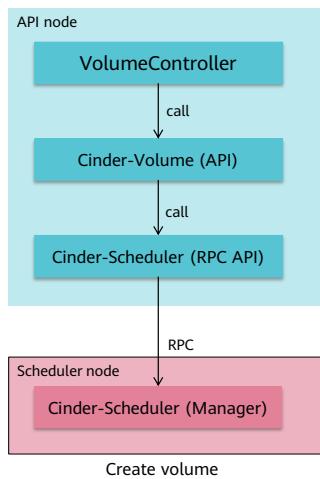
1. OpenStack Storage Overview
2. **Block Storage Service: Cinder**
 - Cinder Overview
 - Cinder Architecture
 - **Cinder Working Principles**
 - Cinder Exercises
3. Object Storage Service: Swift

Cinder Volume Creation Process



- The purpose of creating volume types is to distinguish different storage backends, such as SSD, SATA, high-performance, and low-performance devices. With different customized volume types, the system automatically selects appropriate storage backends during volume creation.

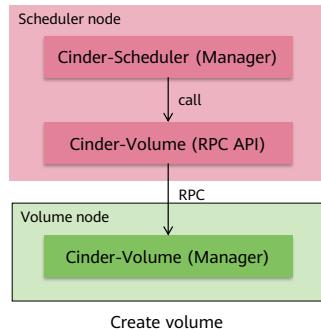
Cinder Volume Creation Process - Cinder-API



Cinder-API

- Check the validity of parameters (for example, check whether the entered users, permissions, or resources exist).
- Prepare the parameter dictionary to be created, and reserve and submit quotas.
- Create related data records in the database.
- Send requests and parameters to the Cinder-Scheduler through message queues.

Cinder Volume Creation Process - Cinder-Scheduler

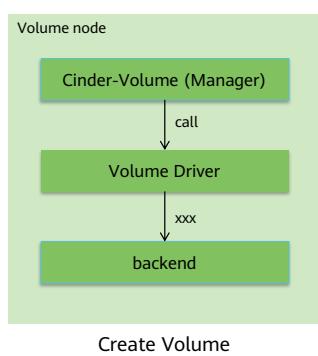


Cinder-Scheduler service

- Extract the received request parameters.
- Use the configured filter to filter backends based on input parameters.
 - Availability_zone_filter
 - Capacity_filter
 - Capabilities_filter
 - Affinity_filter (SameBackendFilter/DifferentBackendFilter)
 - ...
- Weigher calculates the weights of the backend.
 - CapacityWeigher/AllocatedCapacityWeigher
 - ChanceWeigher
 - GoodnessWeigher
 - ...
- Select the most appropriate backend and send the request to a specified backend through message queues.

- Similar to Nova-Scheduler, Cinder-Scheduler uses the filter to identify storage backends meeting the criteria, uses Weigher to calculate the backend weights and sort backends by weight, and then selects the most appropriate storage backend.

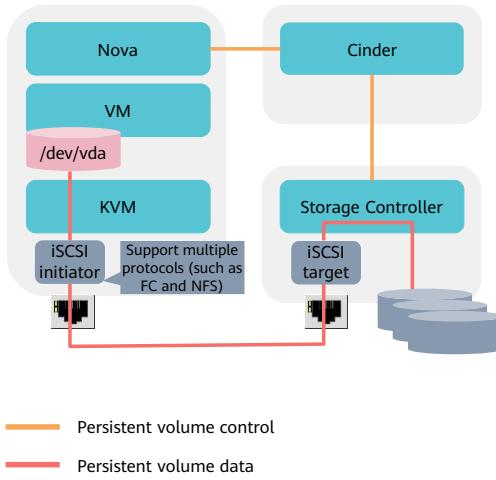
Cinder Volume Creation Process - Cinder-Volume



Cinder-Volume service

- Extract the received request parameters.
- Invoke the required driver to create a volume at the backend.
- Use the model returned by the driver to update records in the database.

Cinder Volume Attachment Process



Volume attachment is a process where Nova and Cinder work together to attach a remote volume to the host that runs the VM and then the attached volume is mapped to an internal VM using the VM management program.

- Nova invokes Cinder API to create a volume and transmit host information, such as the host name, iSCSI initiator name, and FC WWPNs.
- Cinder-API sends the information to Cinder-Volume.
- Cinder-Volume finds the corresponding Cinder Driver based on the host information saved during volume creation.
- Cinder Driver notifies the storage device that the host is allowed to access this volume and returns the connection information of the storage device, such as iSCSI IQN, portal, FC Target WWPN, and NFS path.
- Nova invokes the code for identifying disks on hosts based on storage types (Cinder provides the brick module for reference) to identify disks or file devices.
- Nova notifies Cinder that the volume has been attached.
- Nova sends the host device information to hypervisor to attach the volume to the VM.

Contents

1. OpenStack Storage Overview
2. **Block Storage Service: Cinder**
 - Cinder Overview
 - Cinder Architecture
 - Cinder Working Principles
 - **Cinder Exercises**
3. Object Storage Service: Swift

Cinder Main Operations

Category	Command	Category	Command
Volume operations	create	Snapshot operations	snapshot-create
	delete		snapshot-delete
	show		snapshot-list
	rename		snapshot-rename
	upload-to-image		snapshot-reset-state
	extend		snapshot-show
	force-delete		snapshot-metadata
	list		snapshot-metadata-show
	migrate		snapshot-metadata-update-all
	reset-state		backup-create
Backup operations	rate-limits		backup-delete
	retype		backup-list
	set-bootable		backup-restore
	manage		backup-show
	unmanage		backup-export
	metadata		backup-export

Cinder mainly manages volumes, snapshots, and backups:

Volume:
Create, delete, scale, attach, and detach block device volumes.

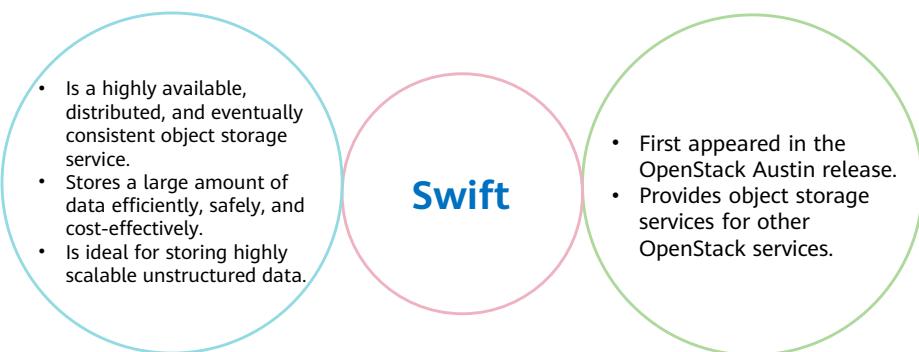
Snapshot:
Create, delete, and roll back snapshots of block device volumes.

Backup:
Back up and restore block device volumes.

Contents

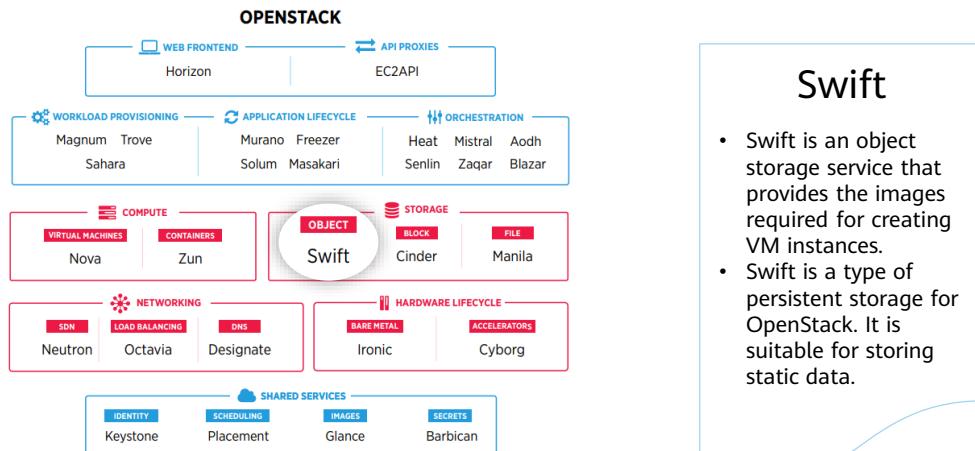
1. OpenStack Storage Overview
2. Block Storage Service: Cinder
- 3. Object Storage Service: Swift**
 - Swift Overview
 - Swift Architecture
 - Swift Working Principles

Object Storage Service: Swift



- OpenStack Object Storage (swift) is used for redundant, scalable data storage using clusters of standardized servers to store petabytes of accessible data. It is a long-term storage system for large amounts of static data which can be retrieved and updated. Object Storage uses a distributed architecture with no central point of control, providing greater scalability, redundancy, and permanence. Objects are written to multiple hardware devices, with the OpenStack software responsible for ensuring data replication and integrity across the cluster. Storage clusters scale horizontally by adding new nodes. If a node fails, OpenStack replicates its content from other active nodes. OpenStack uses software logic to ensure data replication and distribution across different devices.
- Object Storage is ideal for cost effective, scale-out storage. It provides a fully distributed, API-accessible storage platform that can be integrated directly into applications or used for backup, archiving, and data retention.

Positioning of Swift in OpenStack



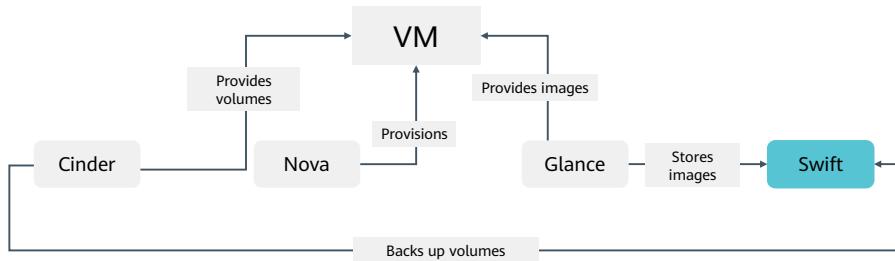
Swift

- Swift is an object storage service that provides the images required for creating VM instances.
- Swift is a type of persistent storage for OpenStack. It is suitable for storing static data.



- Swift is one of the first two OpenStack projects. In 2010, Rackspace contributed Swift and NASA contributed Nova to OpenStack, and the OpenStack project began.
- Static data refers to the data that is not updated for a long time or is seldom updated in a certain period, such as VM images, multimedia data, and backup files.
- Cinder is more suitable for real-time data update.

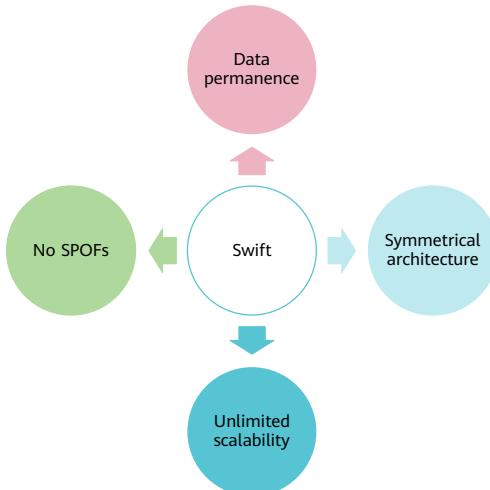
Functions of Swift in OpenStack



- Swift is not a file system or real-time data storage system. It is a long-term storage system for a permanent type of static data. The static data can be retrieved, adjusted, and then updated if necessary.
- Examples of data that best fit this object storage are VM images, pictures, emails, and archive backups.
- Swift has no central unit or master point of control and hence delivers remarkable scalability, redundancy, and permanence.

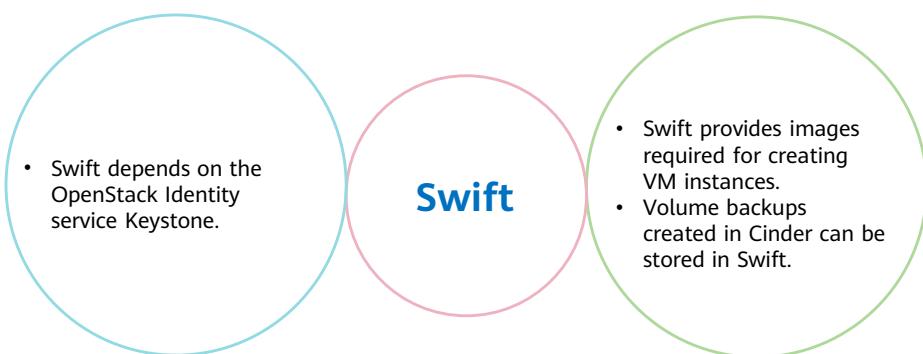
- Swift is often used to store images or backup copies of VM instance volumes.
- Like other OpenStack projects, Swift provides RESTful APIs as the access entry. Each stored object is a RESTful resource and has a unique URL.
- You can send an HTTP request to transfer some data as an object to Swift or request a stored object from Swift.

Swift Characteristics



- Data permanence
 - Theoretically, if Swift has five zones and 5×10 storage nodes in an environment, there will be three data copies and the data permanence SLA reaches 99.99999999%.
- Symmetrical architecture
 - A symmetric architecture means that each node in Swift is exactly the same as others, thereby greatly reducing the system maintenance costs.
- Unlimited scalability
 - The scalability includes two aspects: one is the unlimited scalability of storage capacity, and the other is the linear improvement of Swift performance (such as QPS and throughput). Due to the symmetrical architecture, it is easy to expand the Swift capacity by just adding nodes. The system automatically migrates data to balance loads among storage nodes.
- Free of single points of failure (SPOFs)
 - In scenarios where large-scale Internet applications are used, the single point of failure has always been a tricky problem. Taking databases for example, generally, only the active/standby HA mode can be used, and there is only one active node. Additionally, during the implementation of other open-source storage systems, how to store metadata is always a headache. Metadata can be stored only on a single node that is likely to become a bottleneck. Once an exception happens to this node, the whole cluster will be affected.
 - Metadata in Swift is evenly and randomly stored, and is stored with multiple copies, like object file storage. Moreover, in a Swift cluster, no role is deployed on a single node. It is a useful way to keep services free from SPOFs in terms of architecture and design.

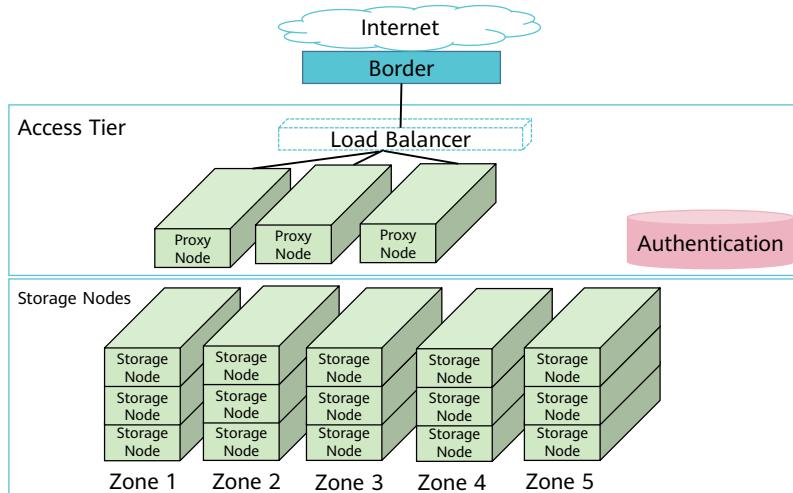
Interactions with Other Services



Contents

1. OpenStack Storage Overview
2. Block Storage Service: Cinder
- 3. Object Storage Service: Swift**
 - Swift Overview
 - Swift Architecture
 - Swift Working Principles

Swift Architecture



35 Huawei Confidential

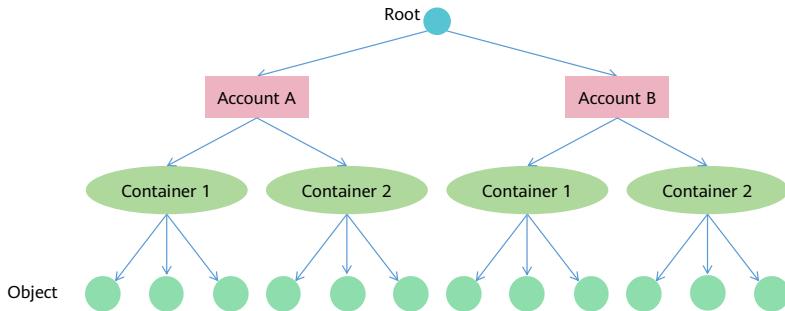


- Swift can be divided into the access layer (Access Tier) and storage layer (Storage Nodes).
- Access Tier consists of the Proxy Node and the Authentication service, which are responsible for RESTful request authentication and user identity authentication, respectively.
 - The Proxy Server runs on the Proxy Node to process users' RESTful requests. When receiving a user request, the Proxy Server forwards the identity information to the Authentication service for processing.
 - The Proxy Server can use Memcached, a high-performance distributed memory object caching system, to cache data and objects, reducing the number of database reads and improving user access speed.
 - When receiving an access request from a user, the Proxy Node forwards the request to the corresponding storage node.
- The storage layer consists of a series of physical storage nodes, which store object data.
- The storage layer is divided into five physical hierarchies:
 - Region: It is a geographically isolated area. Each Swift system has at least one region by default.
 - Zone: Each region is divided into different zones to achieve isolation from hardware. A zone represents a group of independent storage nodes.
 - Storage Node: It is a physical node that stores object data.
 - Device: It can be simply regarded as a disk.

- Partition: It refers to the directory of the file system on a device and is totally different from the hard disk partition.

Swift Data Model

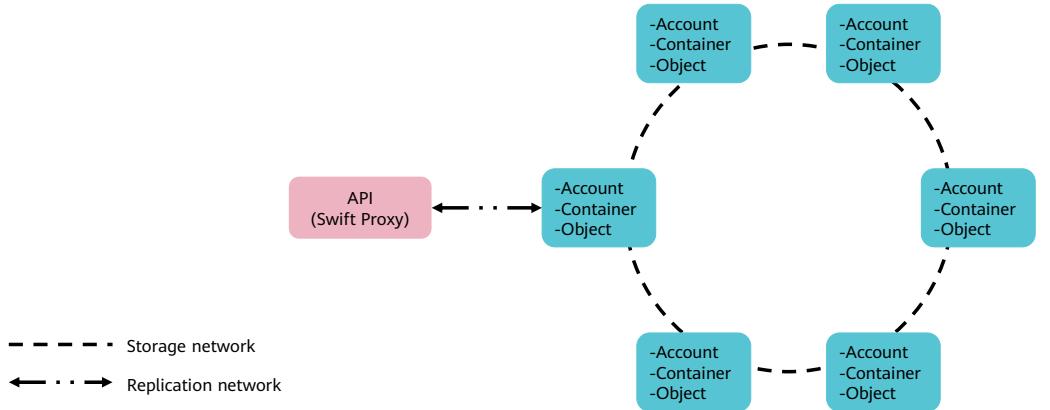
- Swift has three logical layers: account, container, and object.
- The nodes at each layer can be expanded infinitely.



- As shown in the figure, objects stored on each storage node are logically divided into three layers: account, container, and object.
- Note that containers cannot be nested or contain lower-level containers. An object consists of metadata and content. Swift requires that an object must be stored in a container. Therefore, an account must have at least one container to provide object storage.
- Corresponding to the preceding three-layer structure, the following three services run on the storage node: Account Server, Container Server, and Object Server. (The details will be described later in the Swift part.)
- Run the **swift stat** command to view information about accounts, containers, and objects in Swift.
- Swift defines rings for accounts, containers, and objects. These rings (account, container, and object rings) map virtual nodes (partitions) to a group of physical storage devices.
- A ring records the mapping between storage objects and physical locations. The mapping information is maintained through zones, devices, partitions, and replicas.

Swift Architecture

- Swift has a fully symmetric, resource-oriented, distributed system architecture. All components are scalable, eliminating single points of failure (SPOFs) to maximize uptime.



37 Huawei Confidential

- A storage location is given in one of three formats:
 - /account
 - The account storage location is a uniquely named storage area that contains the metadata (descriptive information) about the account itself as well as the list of containers in the account.
 - Note that in Swift, an account is not a user identity. When you hear account, think storage area.
 - /account/container
 - The container storage location is the user-defined storage area within an account where metadata about the container itself and the list of objects in the container will be stored.
 - /account/container/object
 - The object storage location is where the data object and its metadata will be stored.

Swift Components (1)

Proxy Server	Authentication Server	Cache Server
<ul style="list-style-type: none">A proxy service provides object service APIs for external systems. Because stateless REST request protocols are used, horizontal expansion can be performed to balance loads.	<ul style="list-style-type: none">An authentication service verifies user identity information and obtains an object access token. The token is valid for a certain period of time. The authentication service verifies the validity of the token and caches it until it expires.	<ul style="list-style-type: none">A cache service caches object service tokens, accounts, and containers, but does not cache object data. The cache service uses the Memcached cluster, and Swift uses the consistency hash algorithm to allocate cache addresses.

- Proxy Server is the core of Swift and runs the swift-proxy-server process. It provides Swift API services and is responsible for tying together the rest of the Swift architecture. For each request, it will look up the location of the account, container, or object in the ring and route the request accordingly.

Swift Components (2)

Account Server	Container Server	Object Server
<ul style="list-style-type: none">Provides account metadata and statistics, and maintains services in the container list. Information about each account is stored in an SQLite database.	<ul style="list-style-type: none">Provides container metadata and statistics, and maintains services in the object list. Information about each container is stored in an SQLite database.	<ul style="list-style-type: none">Provides object metadata and content services. The content of each object is stored in files in a file system and metadata is stored as a file attribute. The XFS file system supporting extended attributes is recommended.

Swift Components (3)

Auditor	Replicator	Updater
<ul style="list-style-type: none">Checks the integrity of objects, containers, and accounts. If any bit-level error is found in a file, the system isolates the file and copies another replica to overwrite the local damaged replica. Other errors are recorded in logs.	<ul style="list-style-type: none">Checks whether local partition replicas are consistent with remote replicas. If they are inconsistent, the system updates the remote replicas using the Push method and ensures that the objects marked to be deleted are removed from the file system.	<ul style="list-style-type: none">Serializes objects that fail to be immediately updated due to heavy loads into the queue of the local file system, so that they can be asynchronously updated after services are restored.

- The Account Reaper service removes data from deleted accounts in the background, as well as all containers and objects contained in them.

Swift APIs

- Swift makes HTTP-based REST service APIs available externally through Proxy-Server to perform CRUD operations on accounts, containers, and objects.
- Summary of Swift RESTful APIs

Resource Type	URL	GET	PUT	POST	DELETE	HEAD
Accounts	/account/	Obtains the container list.	-	-	-	Obtains account metadata.
Containers	/account/container	Obtains the object list.	Creates a container.	Updates container metadata.	Deletes a container.	Obtains container metadata.
Objects	/account/container/object	Obtains object content and metadata.	Creates, updates, or copies an object.	Updates object metadata.	Deletes an object.	Obtains object metadata.

- CRUD: It is short for Create, Retrieve, Update, and Delete.
- Swift APIs provide the following functions:
 - Store objects. The number of objects is not limited. The maximum size of a single object is 5 GB by default. You can set the maximum size as required.
 - If the size of an object exceeds the maximum value, the object can be uploaded and stored using the large object middleware.
 - Compress objects.
 - Delete objects. Batch deletion is supported.

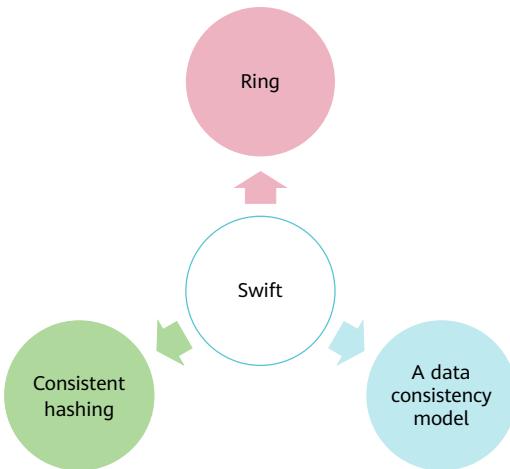
Contents

1. OpenStack Storage Overview
2. Block Storage Service: Cinder
- 3. Object Storage Service: Swift**
 - Swift Overview
 - Swift Architecture
 - **Swift Working Principles**

Swift Working Principles

- The Proxy Server processes object access requests, and the Authentication service authenticates users. After receiving a user request, the Proxy Server forwards the request to the Account Server, Container Server, and Object Server on the storage node for performing object operations. Auditor, Updater, and Replicator are responsible for data consistency between objects and their replicas.

Key Technologies of Swift



- Swift is based on consistent hashing. It computes how to evenly distribute objects to virtual nodes in virtual space, greatly reducing the amount of data to be moved when nodes are added or deleted.
- Swift abandons strict consistency and uses an eventual consistency model to ensure high availability and enable infinite horizontal expansion. If data inconsistency occurs, background service processes synchronize data through detection and replication protocols within a certain time window to ensure final consistency.
- Ring evenly maps virtual nodes (partitions) to a group of physical devices. In Swift, Ring uses zones to ensure that data is physically isolated. Replicas of each partition must be placed in different zones.

- A size of the virtual space is usually 2 to the power of n , facilitating efficient shift operations. Then, a virtual node is mapped to an actual physical storage device by using a unique ring structure, to complete an addressing process.

Quiz

1. What types of storage are available in OpenStack?
2. (Single-answer question) Which of the following is not a key technology of Swift?
 - A. Ring
 - B. Consistent hashing
 - C. A data consistency model
 - D. RAID

- 1. OpenStack supports ephemeral storage and persistent storage.
- 2. D

Summary

- This course described the storage types supported by OpenStack, the positioning, functions, architecture, and working principles of the OpenStack Block Storage service (Cinder) and Object Storage service (Swift), their interactions with other services.

More Information

- OpenStack Community
 - <https://www.openstack.org/>

Acronyms

- API: Application Programming Interface (API) is a particular set of rules and specifications that are used for communication between software programs.
- CRUD: It is short for Create, Retrieve, Update, and Delete. These are four basic functions of databases or persistent storage in software systems.
- CIFS: Common Internet File System (CIFS) is a protocol used for network file access. Windows clients use CIFS to send file access requests to Windows servers.
- DAS: Direct Attached Storage (DAS) is a mode for connecting storage devices and servers, indicating that storage devices use cables such as optical fibers to directly connect to servers.
- NFS: Network File System (NFS) is a file sharing service that allows a dedicated server to manage storage space through the file system and allows users to remotely access files on the server through the network using the NFS protocol or Common Internet File System (CIFS) protocol.
- SAN: Storage Area Network (SAN) is a type of storage that uses a high-speed (optical fiber) network to connect professional servers. The SAN is located at the back end of the host cluster.

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and
organization for a fully connected,
intelligent world.

Copyright©2022 Huawei Technologies Co., Ltd.
All Rights Reserved.

The information in this document may contain predictive
statements including, without limitation, statements regarding
the future financial and operating results, future product
portfolio, new technology, etc. There are a number of factors that
could cause actual results and developments to differ materially
from those expressed or implied in the predictive statements.
Therefore, such information is provided for reference purpose
only and constitutes neither an offer nor an acceptance. Huawei
may change the information at any time without notice.



OpenStack Network Management



Foreword

- This course describes Linux network virtualization technologies, the positioning and functions of Neutron in OpenStack, and interactions between Neutron and other services. It also introduces basic concepts in Neutron, the architecture, working principles, operations, and common network traffic models in Neutron.

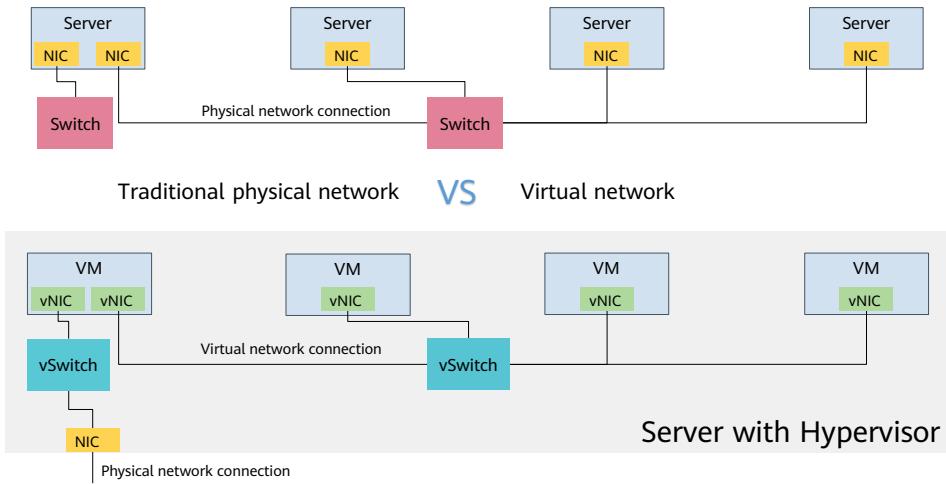
Objectives

- Upon completion of this course, you will understand:
 - Linux network virtualization.
 - The positioning and functions of Neutron in OpenStack and its interactions with other services.
 - The network concepts, architecture, and common network traffic analysis in Neutron.

Contents

- 1. Linux Network Virtualization Technologies**
2. Neutron Overview
3. Neutron Concepts
4. Neutron Architecture
5. Typical Neutron Operations and Processes
6. Neutron Network Traffic Analysis

Physical Network vs. Virtual Network



5 Huawei Confidential



- The core function of Neutron is to abstract and manage Layer 2 physical networks. After physical servers are virtualized, virtual NICs (vNICs) and virtual switches (vSwitches) provide VM network functions. These vNICs are connected to vSwitch ports. The vSwitches then access external physical networks through the physical NICs of physical servers.

Linux Network Virtualization Technologies

NIC Virtualization

- TAP
- TUN
- VETH

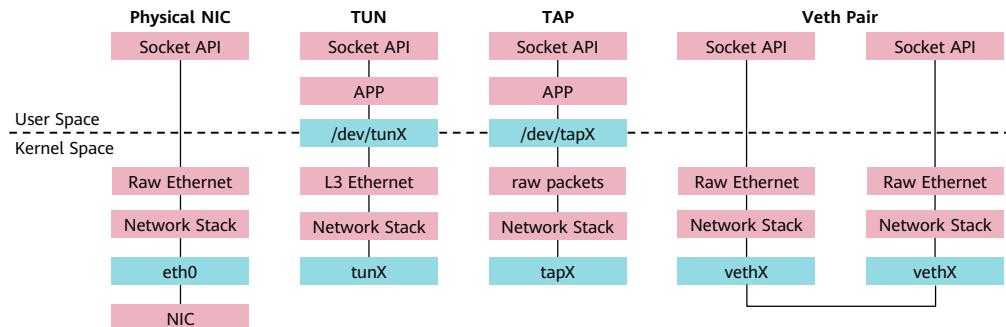
Switch Virtualization

- Linux Bridge
- Open vSwitch

Network Isolation

- Network Namespace

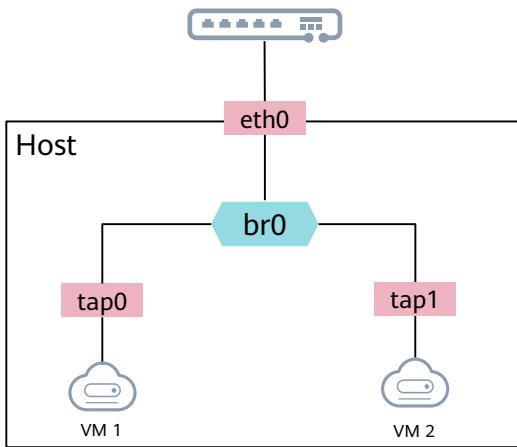
Linux NIC Virtualization - TAP, TUN, and VETH



- **TAP device:** It simulates a Layer 2 network device to receive and send Layer 2 network packets.
- **TUN device:** It simulates a Layer 3 network device to receive and send Layer 3 network packets.
- **VETH:** VETH interfaces are virtual Ethernet interfaces that always exist in pairs. The network packets sent by one end are received by the other end, establishing a tunnel between two network bridges.

- TAP and TUN provide a data transmission mechanism for user space on a host. They virtualize a set of network interfaces that are same as the physical interfaces. The virtualized interfaces can be configured with IP addresses and can route traffic. The difference is that the traffic is transmitted only within the host.
- TAP and TUN are slightly different. TUN operates in Layer 3 carrying IP packets, whereas TAP operates in Layer 2 carrying Ethernet frames.
- Veth-Pair refers to virtual network devices that appear in pairs. One end of a VETH device connects to the protocol stack, and the other end of the device connects to the other VETH device. Data is transmitted from one end to the other end. Due to this feature, Veth-Pair is often used to connect different virtual network components to construct large-scale virtual network topologies, such as connecting Linux Bridge, OVS, and LXC containers. A common example of Veth-Pair is that it is used in OpenStack Neutron to build complex networks.

Linux Switch Virtualization - Linux Bridge

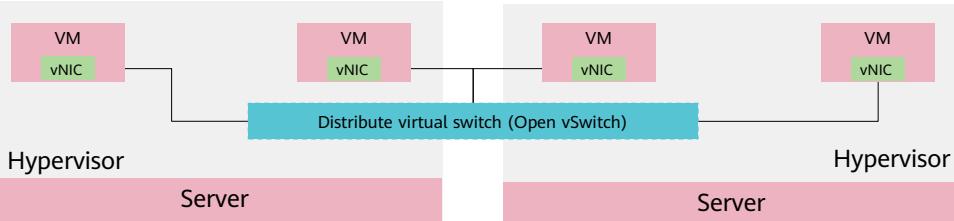


- Linux bridge: a Layer 2 network device that functions like a physical switch
- A bridge can bind other network devices on Linux and virtualize them as ports.
- Binding a device to a bridge is equivalent connecting a network cable to a terminal by plugging it into a physical switch port.
- Use **brctl** to configure Linux bridges:
 - brctl addbr BRIDGE
 - brctl addif BRIDGE DEVICE

- The preceding figure shows the structure of a Linux bridge. The bridge **br0** binds the physical device **eth0** and the virtual devices **tap0** and **tap1**. However, the upper-layer network protocol stack sees only **br0** and does not need to know bridging details.
- When receiving a data packet, these bound devices will send the data packet to **br0** for forwarding based on the mapping between the MAC addresses and ports.
- The bridge works at Layer 2. Therefore, you do not need to set IP addresses for the slave devices **eth0**, **tap0**, and **tap1** bound to **br0**. For the upper-layer router, they are in the same subnet. Therefore, you only need to set an IP address for **br0**. Because **br0** has its own IP address, it can be added to the routing table and used to send data. However, the actual sending process is completed by a secondary device.
- **eth0** has its own IP address. If **eth0** is bound to **br0**, the IP address of **eth0** will become invalid and user programs cannot receive data from this IP address. Only the data packets whose destination address is the IP address of **br0** are received by Linux.
- **brctl addbr BRIDGE**: Add a bridge.
- **brctl addif BRIDGE DEVICE**: Add an interface to a bridge.

Linux Switch Virtualization - Open vSwitch

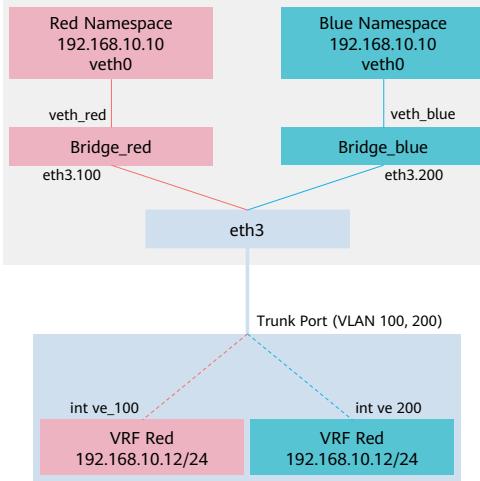
- Open vSwitch is a virtual switch at the product level.
 - A Linux bridge is ideal for small-scale communications within a host.
 - Open vSwitch is more suitable for large-scale communications between multiple hosts.



- Common Open vSwitch commands:
 - ovs-vsctl add-br BRIDGE
 - ovs-vsctl add-port PORT
 - ovs-vsctl show BRIDGE
 - ovs-vsctl dump-ports-desc BRIDGE
 - ovs-vsctl dump-flows BRIDGE

- Open vSwitch connects vNICs to physical NICs and bridges vNICs on the same physical server. Actually, Linux Bridge can play such a role well. Why do we still need Open vSwitch?
- The introduction of Open vSwitch makes it easier to manage virtual networks and monitor network status and traffic in the cloud environment.
- Similar to configuring a physical switch, you can allocate VMs connected to the Open vSwitch to different VLANs to isolate networks. You can also configure QoS for VMs on Open vSwitch ports. Open vSwitch also supports many standard management interfaces and protocols, such as NetFlow and sFlow. These interfaces can be used to monitor traffic.
- Open vSwitch implements distributed virtual switches (DVSs) on various virtualization platforms (such as Xen and KVM) in the cloud environment. vSwitches on one physical server can be transparently connected to vSwitches on another physical server.

Linux Network Isolation - Network Namespace



- A network namespace can create multiple isolated network spaces with independent network configurations. For instance, they can have different network devices, routing tables, and iptables.
- VMs in different network spaces run as if they were in independent networks.

```
$ ip netns help
Usage: ip netns list
      ip netns add NAME
      ip netns delete NAME
      ip netns identify PID
      ip netns pids NAME
      ip netns exec NAME cmd ...
      ip netns monitor
```

- Network namespaces usually work with Virtual Routing and Forwarding (VRF). VRF is an IP technology that allows multiple instances of a routing table to work simultaneously within the same router.
- You can use a VETH device to connect two network namespaces and use a bridge to connect multiple network namespaces.

Discussion: What Linux Network Virtualization Technologies Are There?

- The following is a screenshot of what is returned by **ip address** on an OpenStack node. Please discuss or think about the Linux network virtualization technologies involved in this figure.

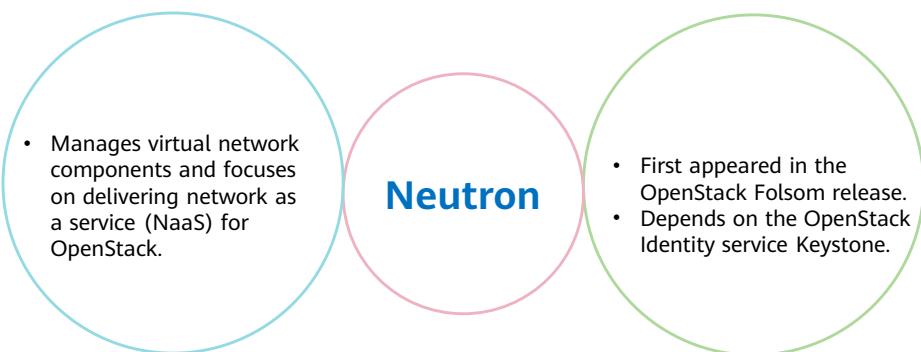
```
osbash@controller:~$ ip address
...
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
...
7: tapc1d0ccdc-08@if2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master brq5fe28ac7-4e state UP group default qlen 1000
...
4: brq5fe28ac7-4e: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
...
10: vxlan-28: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1450 qdisc noqueue master brq7b350e42-8c state UNKNOWN group default qlen 1000
```

- Here we have a question for discussion. The following is the **ip address** screenshot on the OpenStack node. Please discuss or think about the Linux network virtualization technologies involved in this figure. *enp0s3* is the host physical NIC. *tapxxxx* is the tap device. *brqxxxx* is the bridge device. *vxlan* is the VXLAN sub-interface.

Contents

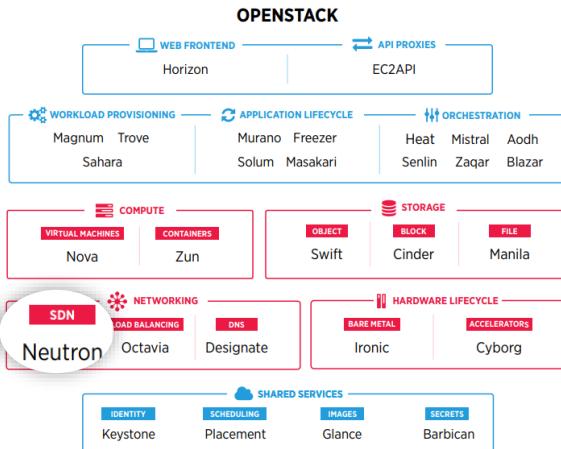
1. Linux Network Virtualization Technologies
- 2. Neutron Overview**
3. Neutron Concepts
4. Neutron Architecture
5. Typical Neutron Operations and Processes
6. Neutron Network Traffic Analysis

Networking Service: Neutron



- Based on the software-defined networking (SDN) concept, Neutron manages network resources in network virtualization. Neutron is designed to deliver network as a service (NaaS). It complies with the SDN-based network virtualization principles and fully uses Linux network-related technologies in the Linux system.

Positioning of Neutron in OpenStack



Neutron

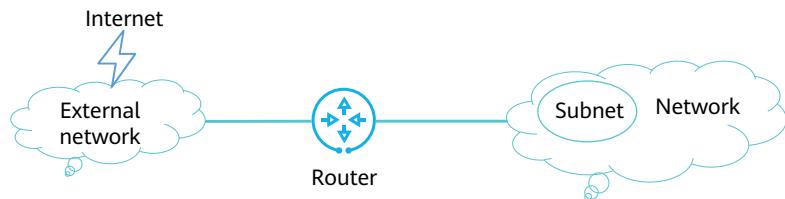
- OpenStack Neutron is an SDN network project focused on providing NaaS in virtual computing environments.
- Neutron allows users to create interface devices managed by other OpenStack services and connect them to the network.



- Neutron is an OpenStack project to provide NaaS between interface devices (e.g., vNICs) managed by other OpenStack services (e.g., Nova).
- OpenStack Networking (Neutron) allows you to create and attach interface devices managed by other OpenStack services to networks. Plugins can be implemented to accommodate different networking equipment and software, providing flexibility to OpenStack architecture and deployment.

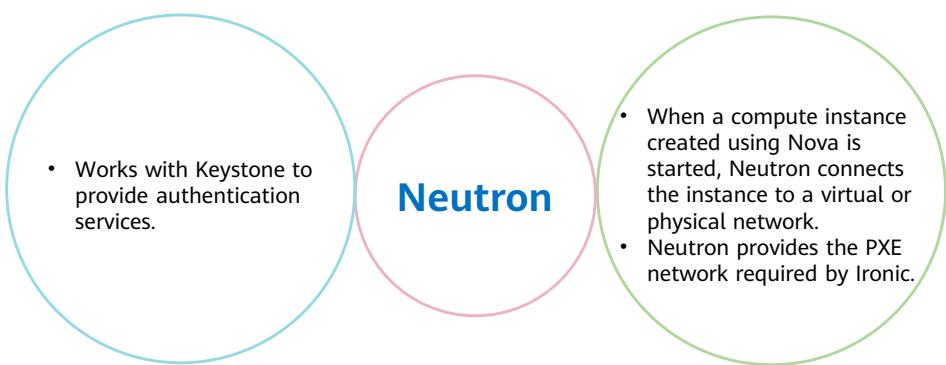
Neutron Functions

- Neutron manages all networking facets for the Virtual Networking Infrastructure (VNI) and the access layer aspects of the Physical Networking Infrastructure (PNI) in your OpenStack environment.
- Neutron provides networks, subnets, and routers as object abstractions. Each abstraction has functionality that mimics its physical counterpart: networks contain subnets, and routers route traffic between different subnets and networks.



- Neutron is only a management or control system and cannot implement any network functions. It is only used to configure or drive Linux functions. Essentially, Neutron uses Linux to implement network functions.
- The entire physical network where OpenStack resides is generalized into a network resource pool in Neutron. By flexibly dividing and managing physical network resources, Neutron provides an independent virtual network environment for each tenant on the same physical network.
- As shown in the figure, in the Neutron network structure, there must be at least one external network object created by the administrator to connect the OpenStack environment to the Internet. This way, tenants can create their own private internal networks and create VMs in the networks. To enable VMs on the internal network to access the Internet, you must create a router to connect the internal network to the external network.
- The network, subnet, and router concepts will be described in detail in the following sections.

Interactions with Other Services

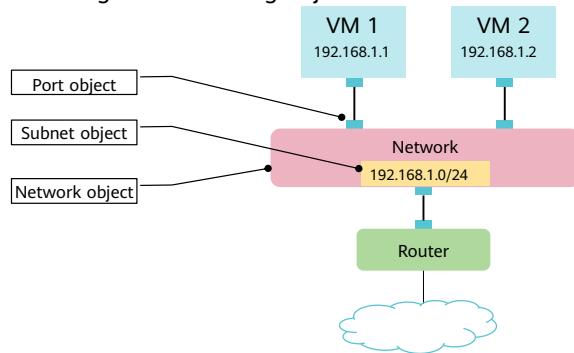


Contents

1. Linux Network Virtualization Technologies
2. Neutron Overview
- 3. Neutron Concepts**
4. Neutron Architecture
5. Typical Neutron Operations and Processes
6. Neutron Network Traffic Analysis

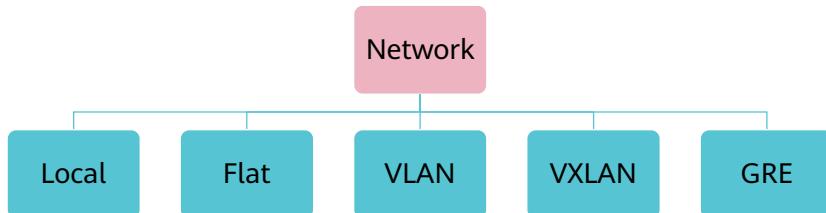
Neutron Concepts

- Neutron is a virtual network service that provides network connectivity and addressing services for compute resources.
- Neutron abstracts the network to manage the following objects:
 - Networks
 - Subnets
 - Ports
 - Routers
 - Floating IP addresses



Neutron Concept - Network

- Network
 - A network is an isolated, virtual Layer 2 broadcast domain. It can also be seen as a virtual or logical switch.
 - Neutron supports different types of networks, including local, flat, VLAN, VXLAN and GRE networks.



- VLAN, VXLAN, or GRE networks are usually used in the production environment.

Neutron Concepts - Subnet

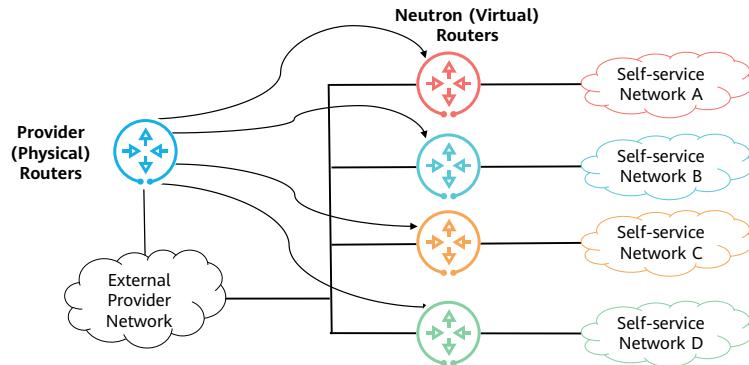
- Subnet
 - A subnet is a segment of IPv4 or IPv6 addresses. The IP addresses of the VMs are allocated from the subnet. The IP address range and mask must be defined for each subnet.
 - A subnet must be associated with a network.
 - Optional attributes of a subnet: DNS, gateway IP address, and static route.

Neutron Concepts - Port

- Port
 - A port is a virtual port on a logical network switch.
 - A VM is attached to a network through a port.
 - A port is always associated with an IP address and a MAC address.

Neutron Concepts - Router

- Router
 - A router is used to connect the subnets of a network or different networks of a tenant. It also connects internal and external networks.

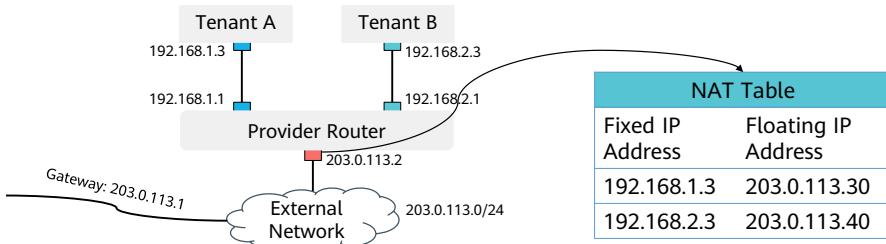


Neutron Concepts - Fixed IP Address

- Fixed IP address
 - A fixed IP address is the IP address assigned to each port, similar to the IP address assigned to a NIC in the physical environment.

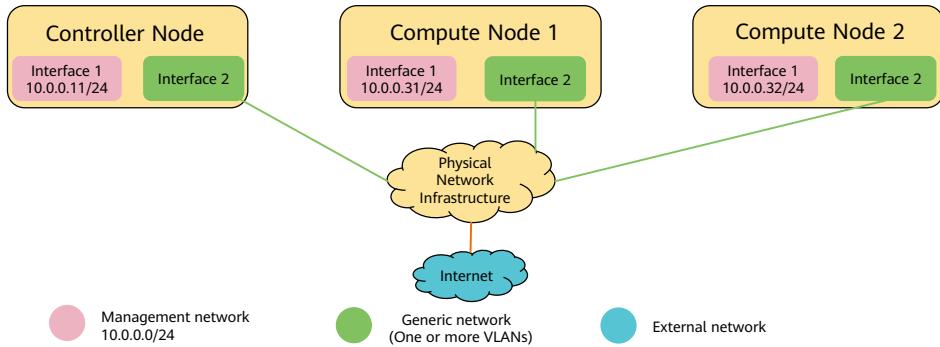
Neutron Concepts - Floating IP Address

- Floating IP address
 - A floating IP address is a special port created on the external network and can be bound to a port on any network. After you bind a floating IP address to a port, the bottom layer forwards the traffic sent to the floating IP address to the fixed IP address corresponding to the port using NAT forwarding.
 - External networks and VMs can access each other through floating IP addresses.



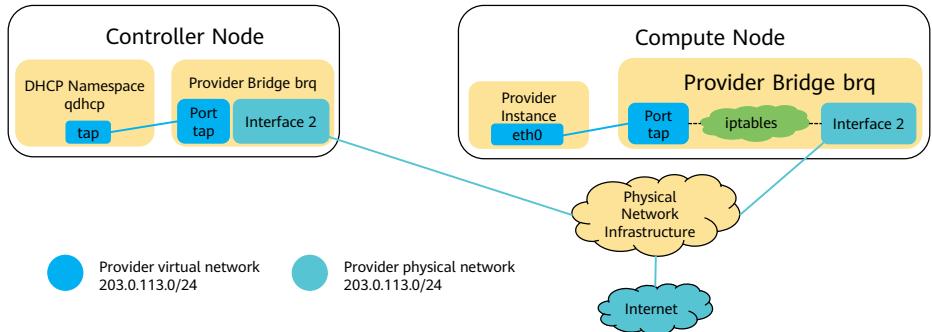
Neutron Concepts - Physical Network

- Physical network
 - The network connecting with different OpenStack nodes in a physical network environment is the physical network. Each physical network supports one or more virtual networks in Neutron.



Neutron Concepts - Provider Network

- Provider network
 - A provider network is created by an OpenStack administrator and directly corresponds to a network segment of the existing physical network in the data center.
 - A provider network usually uses either VLAN or flat configurations and can be shared by multiple tenants.



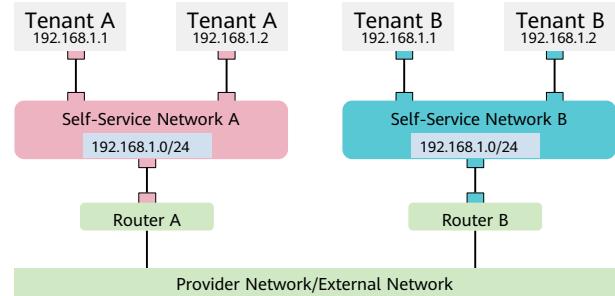
26 Huawei Confidential



- A provider network is created by an OpenStack administrator and directly corresponds to a network segment of the existing physical network in the data center. A provider network usually uses either VLAN or flat configurations and can be shared by multiple tenants. Provider networks are created based on physical networks.
- A provider network is created by an OpenStack administrator using Neutron and maps to an external network. Provider networks are used to connect VMs or networks in Neutron to external networks through particular mapping relationships.

Neutron Concepts - Self-Service Network

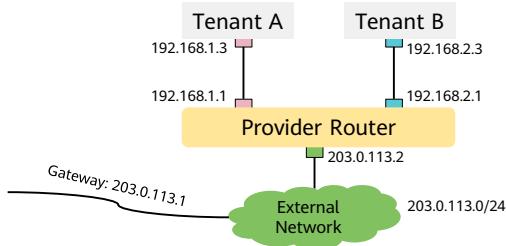
- Self-service network (also called a tenant network or project network)
 - A self-service network is a virtual network created by OpenStack tenants. It is connected only within the local network and cannot be shared among tenants.
 - Self-service networks are usually deployed using VXLANs or in a GRE protocol and can communicate with provider networks through the SNAT of the virtual router.



- The network segments in different self-service networks can be the same. For example, the internal networks of different companies in a physical environment can be the same. Self-service networks communicate with external physical networks through a router. Similarly, companies in a physical environment access the Internet through the router or firewall. The self-service network is somewhat synonymous with what we usually refer to as the private network.

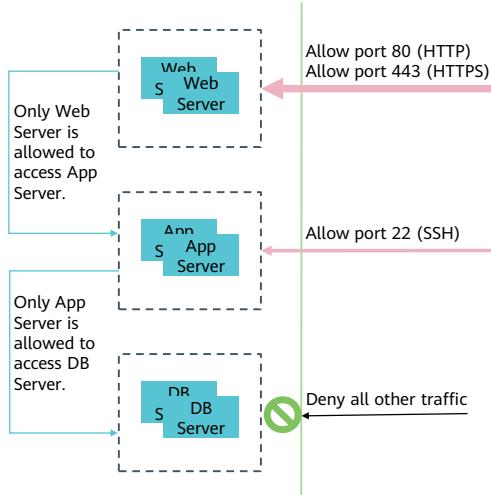
Neutron Concepts - External Network

- External network (also called a "public network")
 - An external network is a provider network through which a physical network can communicate with the data center or Internet. Ports on external networks can access the Internet.
 - The virtual router of a tenant is usually connected to this network. After a floating IP address is created and bound to a VM, the VM can communicate with external networks.



- An external network is similar to the public IP address segment used in the physical environment. The difference is that the physical network corresponding to external network in OpenStack may not be directly connected to the Internet, but may be only an internal private network in the data center.

Neutron Concepts - Security Group



- **Security group:**

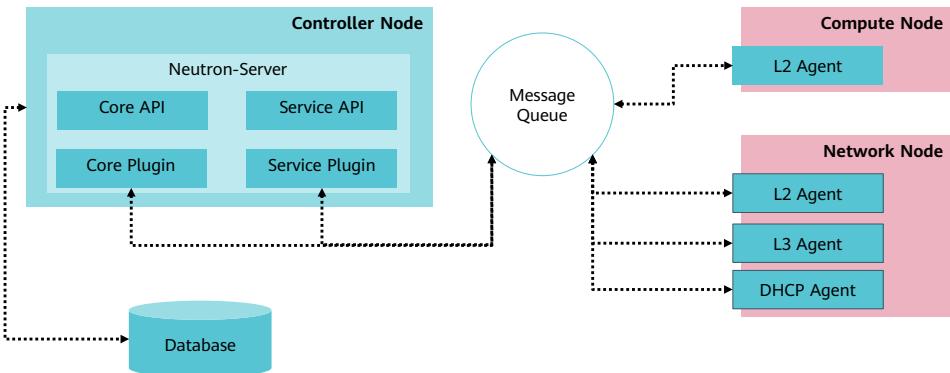
- A security group is a group of policies applied to Neutron ports. These policies define the rules for inbound and outbound traffic of VMs.
- Security groups are implemented based on Linux iptables.
- Security groups deny all traffic by default. Traffic is only allowed through when there is a specific rule allowing it.
- Each OpenStack project has a default security group that contains the following rules by default:
 - Deny all inbound traffic and allow all outbound traffic

- In a security group, you can configure policies based on different protocols, port numbers, destination addresses, and source addresses.

Contents

1. Linux Network Virtualization Technologies
2. Neutron Overview
3. Neutron Concepts
- 4. Neutron Architecture**
5. Typical Neutron Operations and Processes
6. Neutron Network Traffic Analysis

Neutron Architecture



31 Huawei Confidential



- Neutron architecture principles
 - Unified APIs
 - Minimized core part
 - Pluggable, open architecture
 - Scalable
- Message Queue
 - Neutron-Server uses message queues to exchange messages with other Neutron agents, but does not use message queues to exchange messages with other OpenStack components (for example, Nova).
- L2 Agent
 - It is used to connect ports and devices so that they are in a shared broadcast domain. L2 agents usually run on the hypervisor.
- L3 Agent
 - It is used to connect the tenant network to the data center or Internet. In real deployment environments, multiple L3 agents run at the same time.

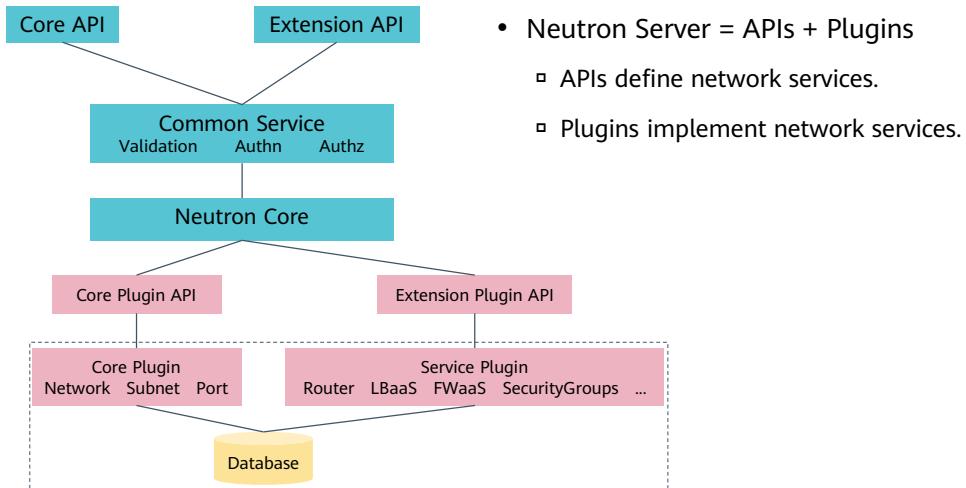
- DHCP agent
 - It is used to automatically configure VM networks.
- Advanced Service
 - It provides LB, firewall, and VPN services.

Neutron Architecture

- The Neutron architecture depends on plug-ins.
Different plugins provide different network services.
- Neutron components include:

Neutron Server	Plugin	Agent	
<ul style="list-style-type: none">Provides network APIs for external systems and invokes plugins to process requests.	<ul style="list-style-type: none">Processes the requests from the Neutron Server and maintains the network status, and then invokes the Agent to process requests.	<ul style="list-style-type: none">Processes the requests from plugins and invokes the underlying virtual or physical network devices to implement various network functions.	<ul style="list-style-type: none">✓ Neutron Server✓ Core Plugin✓ Service Plugin<ul style="list-style-type: none">• L3 Service Plugin• LB Service Plugin• Firewall Service Plugin• VPN Service Plugin✓ Various agents<ul style="list-style-type: none">• L2 (ovs-agent)• L3 Agent• DHCP Agent• MetaData Agent

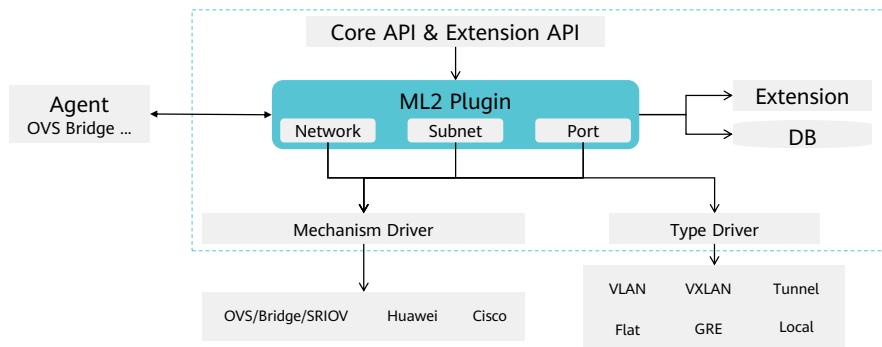
Neutron Components - Neutron Server



- According to the Neutron Server architecture, it consists of APIs and Plugins. APIs define various network services (such as subnets and ports), and Plugins implement various network services (such as routers, LBaaS, FWaaS, and security groups). This mode allows systems to connect to different network backends.

Neutron Components - Core Plugin

- Core Plugin has an open framework. It mainly refers to the ML2 plugin. Under each plugin, Layer 2 network services supported by different vendors and backend technologies are integrated.
 - Core Plugin invokes different underlying network technologies through the Type Driver and Mechanism Driver to implement Layer 2 communications.



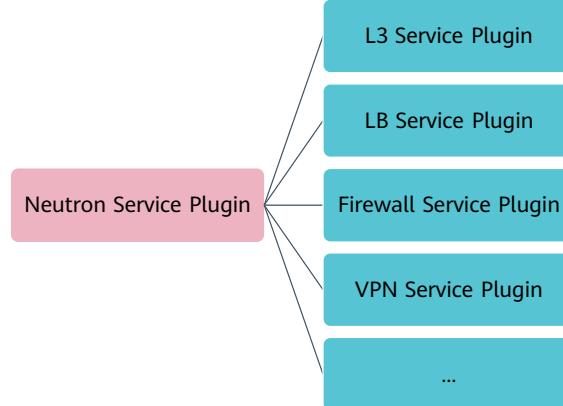
35 Huawei Confidential



- ML2: Modular Layer 2
- Core Plugin provides basic network functions and uses different drivers to invoke underlying network implementation technologies.
- The drivers of the ML2 plugin are classified into the following types:
 - Type Driver: defines the network type. Each network type corresponds to a Type Driver.
 - Mechanism Driver: connects to different Layer 2 network technologies and physical switching devices, such as OVS and Linux Bridge. The Mechanism Driver obtains underlying network information from the Type Driver, ensuring that the underlying technology can be used to correctly configure the Layer 2 network.

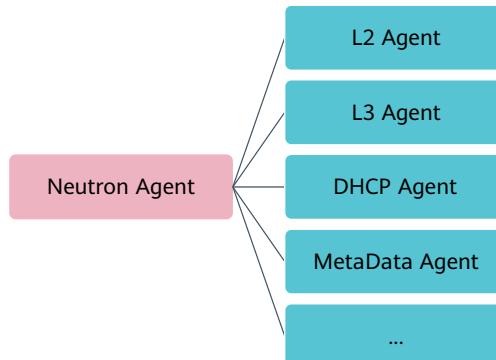
Neutron Components - Service Plugin

- Service plugins implement high-level network services, such as routing, load balancing, firewall, and VPN services.



Neutron Components - Agent

- Neutron Agent provides layer 2 and layer 3 network connections for VMs, enables conversion between virtual networks and physical networks, and provides extended services.



Contents

1. Linux Network Virtualization Technologies
2. Neutron Overview
3. Neutron Concepts
4. Neutron Architecture
- 5. Typical Neutron Operations and Processes**
6. Neutron Network Traffic Analysis

Neutron Operations - Common Commands

- `neutron net-create`
- `neutron net-list`
- `neutron subnet-list`
- `neutron port-create`
- `neutron router-interface-add`
- `neutron agent-list`

- There are some commands for Neutron operations: **neutron net-create** for creating networks, **neutron net-list** for viewing the subnet list, **neutron subnet-list** for viewing the subnet list, **neutron agent-list** for viewing the agent list, **neutron port-create** for creating ports, and **neutron router-interface-add** for creating router interfaces.
- For more commands, see "Hands-on Exercises: Neutron Operations." You can run the help command to view the usage of Neutron commands, including how to manage networks, subnets, ports, routers, floating IP addresses, security groups and rules, and test VM instance access.

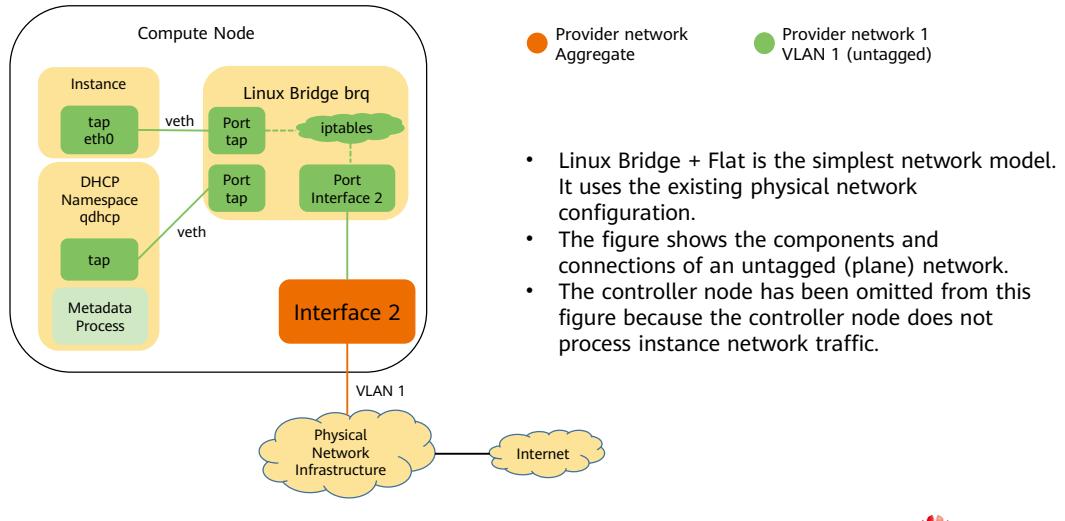
Contents

1. Linux Network Virtualization Technologies
 2. Neutron Overview
 3. Neutron Concepts
 4. Neutron Architecture
 5. Typical Neutron Operations and Processes
- 6. Neutron Network Traffic Analysis**
- Linux Bridge + Flat/VLAN Network
 - Open vSwitch + VXLAN Network

Typical Network Scenarios for Neutron

- Neutron supports different network technologies and types, and you can combine network models on demand.
- The following two network combinations are commonly used in OpenStack production environments:
 - Linux Bridge + Flat/VLAN Network
 - Provides only basic network connectivity. Virtual networks, routes, and load balancing are provided by physical devices.
 - Is a simple, efficient network model ideal for private cloud networks of small- and medium-sized enterprises.
 - Open vSwitch + VXLAN Network
 - Provides the isolation capabilities for multi-tenant and large-scale networks, ideal for large-scale private and public cloud networks.

Linux Bridge + Flat Network

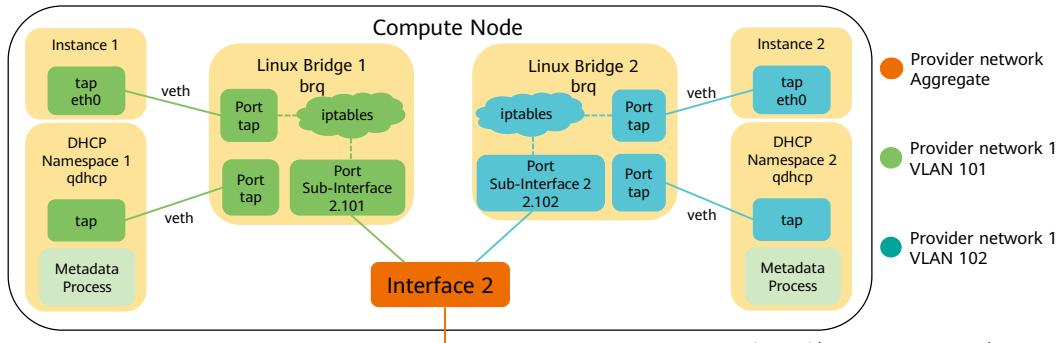


42 Huawei Confidential



- The flat network is similar to the physical network that is directly connected using network cables. OpenStack does not isolate networks.
- In the figure above, interface 2 does not contain the VLAN tagging.

Linux Bridge + VLAN Network

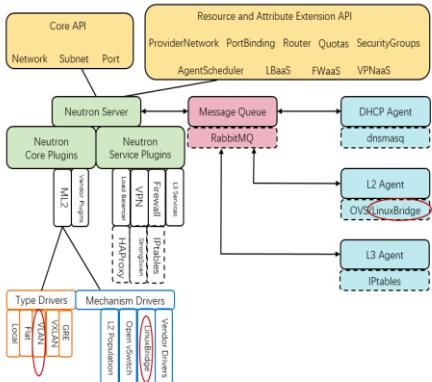


This figure depicts a virtual connection between components of two tagged (VLAN) networks. Essentially, each network uses a separate bridge that contains a port on the VLAN sub-interface on the provider's physical network interface.

- Linux Bridge + VLAN supports the VLAN isolation on existing physical networks.
- The controller node has been omitted from this figure because the controller node does not process instance network traffic.

- In the figure above, interface 2 needs to pass through multiple VLANs. The connected physical switches need to be configured in trunk mode and allow the VLANs to pass.

Linux Bridge + VLAN Implementation

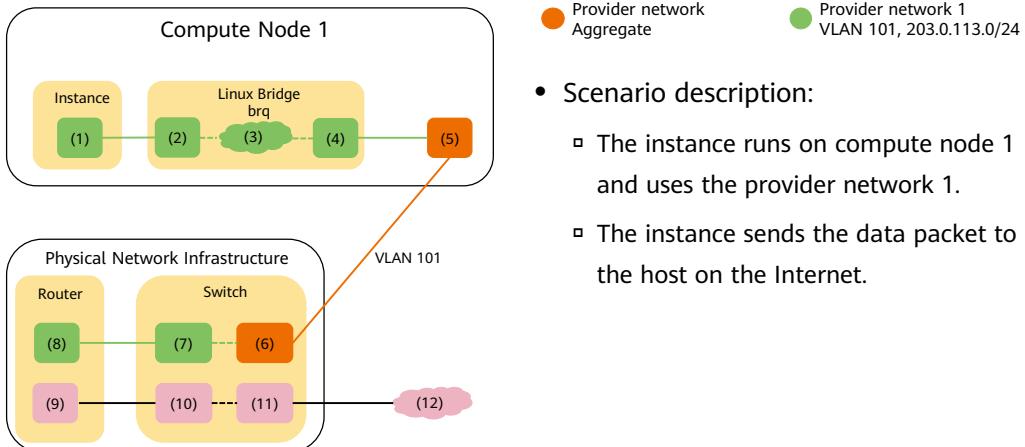


- In a Linux Bridge + VLAN network:
 - The Type Driver of ML2 represents a VLAN.
 - The Mechanism Driver of ML2 is Linux Bridge.
 - L2 Agent represents Linux Bridge.

Linux Bridge + VLAN Scenario

- When Linux Bridge + VLAN is used for a provider network, network traffic can be classified as follows:
 - North-south traffic: communication traffic between VMs and external networks (for example, the Internet)
 - East-west traffic: traffic between VMs
 - Traffic between the provider network and the external network: The switching and routing are implemented by physical network devices.
- The follow-up network traffic analysis is based on the following example:
 - Provider network 1 (VLAN)
 - VLAN 101 (tagged), IP address segment **203.0.113.0/24**, gateway **203.0.113.1** (on physical network devices)
 - Provider network 2 (VLAN)
 - VLAN 102 (tagged), IP address segment **192.0.2.0/24**, gateway **192.0.2.1** (on the vRouter port)

North-South Traffic Analysis for VMs Using Fixed IP Addresses

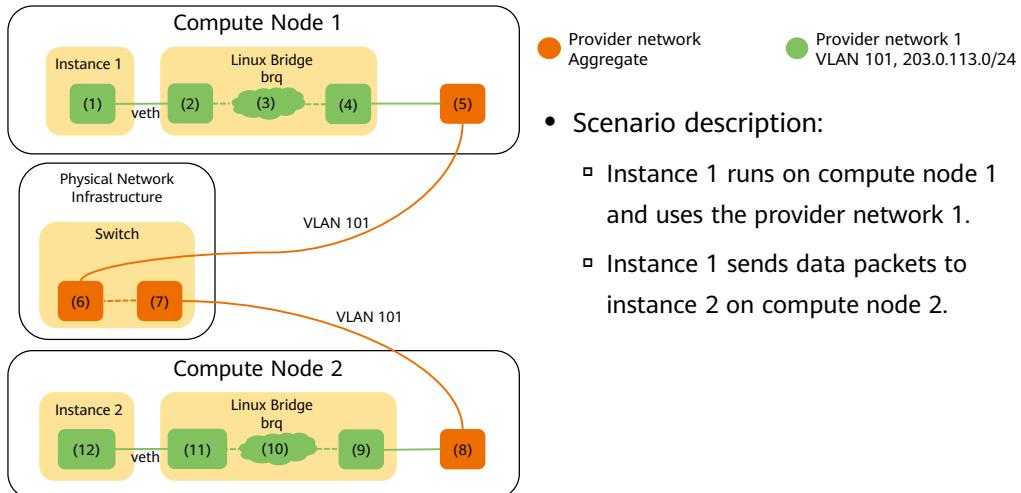


46 Huawei Confidential



- The following operations involve compute node 1:
 - The VM data packet is forwarded by the vNIC (1) to port (2) on Provider Bridge through a veth pair.
 - The security group rule (3) on Provider Bridge checks the firewall and records connection tracking information.
 - The VLAN sub-interface (4) on Provider Bridge forwards the data packet to the physical NIC (5).
 - The physical interface (5) adds VLAN tag 101 to the data packet and forwards the tagged packet to the physical switch port (6).
- The following operations involve physical network devices:
 - The switch removes VLAN tag 101 from the data packet and forwards the packet to router (7).
 - The router routes the data packet from the gateway (8) of Provider Network 1 to the gateway (9) of External Network and forwards this packet to the switch port (10) of the external network.
 - The switch forwards the data packet to the external network (11).
 - External network (12) receives the data packet.

East-West Traffic Analysis for VMs on the Same Network

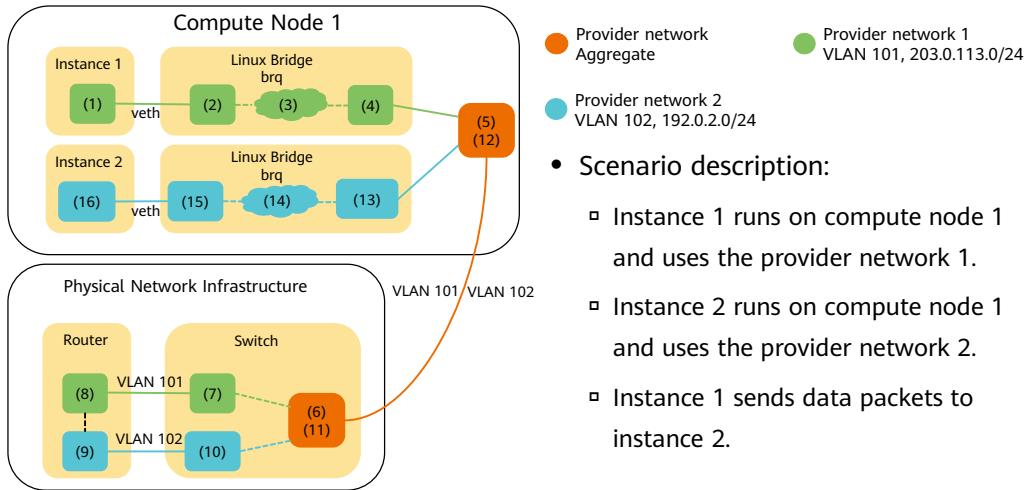


47 Huawei Confidential



- The following operations involve compute node 1:
 - The data packet on VM 1 is forwarded by the vNIC (1) to port (2) on Provider Bridge through a veth pair.
 - The security group rule (3) on Provider Bridge checks the firewall and records connection tracking information.
 - The VLAN sub-interface (4) on Provider Bridge forwards the data packet to the physical NIC (5).
 - The physical interface (5) adds VLAN tag 101 to the data packet and forwards the tagged packet to the physical switch port (6).
- The following operations involve physical network devices:
 - The switch forwards the data packet to the switch port (7) connected to compute node 2.
- The following operations involve compute node 2:
 - The physical NIC (8) of compute node 2 removes VLAN tag 101 from the data packet, and then forwards the data packet to the VLAN sub-interface (9) of Provider Bridge.
 - The security group rule (10) on Provider Bridge checks the firewall and records connection tracking information.
 - The vNIC (11) on Provider Bridge forwards the data packet to the NIC (12) of the VM 2 using the veth pair.

East-West Traffic for VMs on Different Networks



48 Huawei Confidential

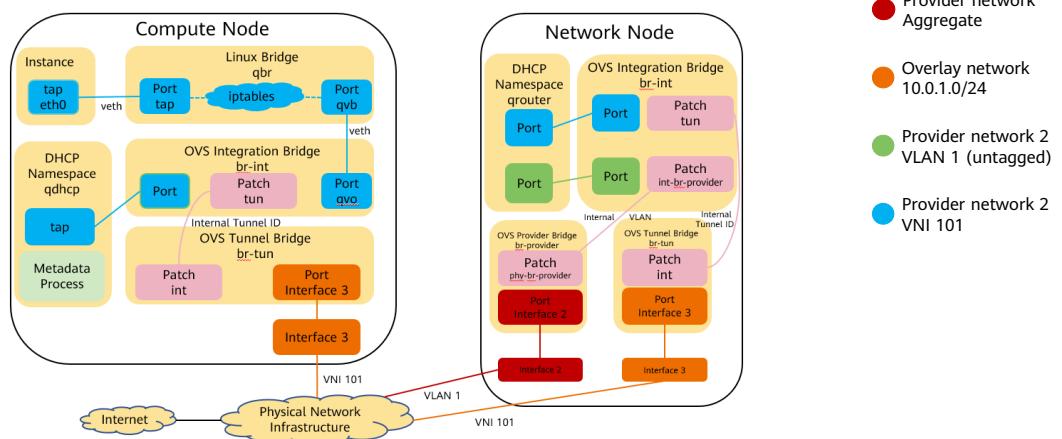


- The following operations involve compute node 1:
 - The data packet on VM 1 is forwarded by the vNIC (1) to port (2) on Provider Bridge through a veth pair.
 - The security group rule (3) on Provider Bridge checks the firewall and records connection tracking information.
 - The VLAN sub-interface (4) on Provider Bridge forwards the data packet to the physical NIC (5).
 - The physical interface (5) adds VLAN tag 101 to the data packet and forwards the tagged packet to the physical switch port (6).
- The following operations involve physical network devices:
 - The switch removes VLAN tag 101 from the data packet and forwards the packet to router (7).
 - The router forwards the data packet from the gateway (8) of Provider Network 1 to the gateway (9) of Provider Network 2.
 - The router sends the data packet to the switch port (10).
 - The switch tags the data packet with VLAN tag 102 and forwards the tagged packet to the port (11) connected to compute node 1.
- The following operations involve compute node 1:
 - The physical NIC (12) of compute node 1 removes VLAN tag 102 from the data packet and forwards the packet to the VLAN sub-interface (13) of Provider Bridge.
 - The security group rule (14) on Provider Bridge checks the firewall and records connection tracking information.
 - The vNIC (15) on Provider Bridge forwards the data packet to the NIC (16) of the VM 2 using the veth pair.

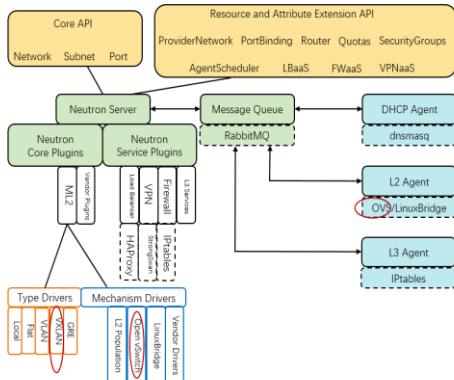
Contents

1. Linux Network Virtualization Technologies
 2. Neutron Overview
 3. Neutron Concepts
 4. Neutron Architecture
 5. Typical Neutron Operations and Processes
- 6. Neutron Network Traffic Analysis**
- Linux Bridge + Flat/VLAN Network
 - Open vSwitch + VXLAN Network

Open vSwitch + VXLAN Network



Open vSwitch + VXLAN Implementation

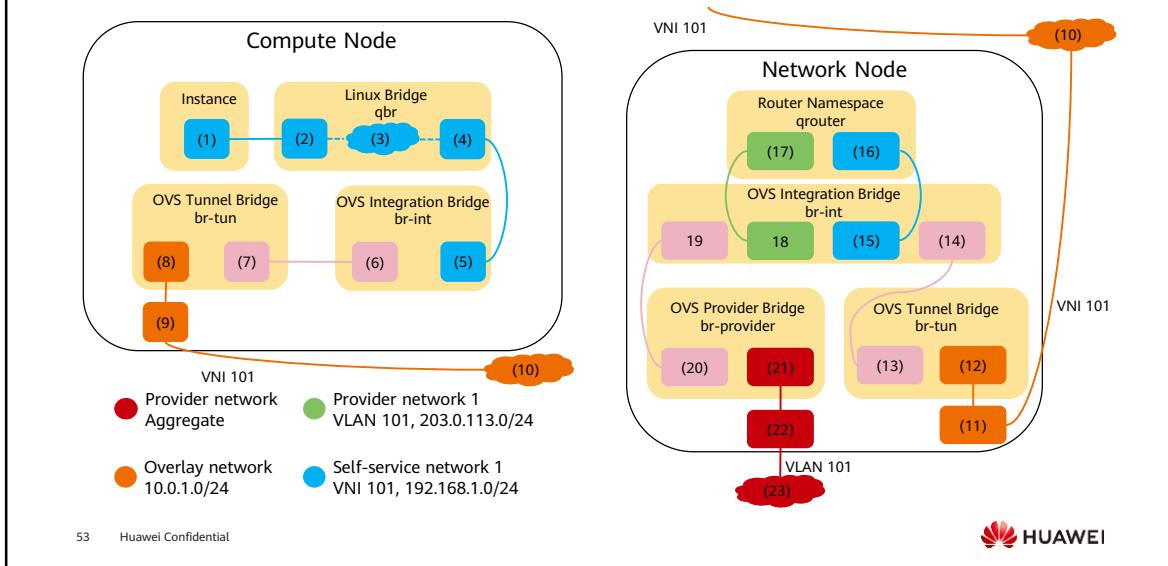


- In an Open vSwitch + VXLAN network:
 - The Type Driver of ML2 represents a VXLAN.
 - The Mechanism Driver of ML2 represents an Open vSwitch.
 - L2 Agent represents an Open vSwitch.

Open vSwitch + VXLAN Scenario Description

- When Open vSwitch + VXLAN is used for a self-service network, network traffic can be classified as follows:
 - North-south traffic: communication traffic between VMs and external networks (for example, the Internet)
 - East-west traffic: traffic between VMs
 - Traffic between the provider network and the external network: The switching and routing are implemented by physical network devices.
- The follow-up network traffic analysis is based on the following example:
 - Provider network 1 (VLAN): VLAN 101 (tagged)
 - Self-service network 1 (VXLAN): VXLAN 101 (VNI)
 - Self-service network 2 (VXLAN): VXLAN 102 (VNI)
 - Self-service router: The gateway is on provider network 1 and connects to self-service network 1 and self-service network 2.

North-South Traffic Analysis for VMs Using Fixed IP Addresses

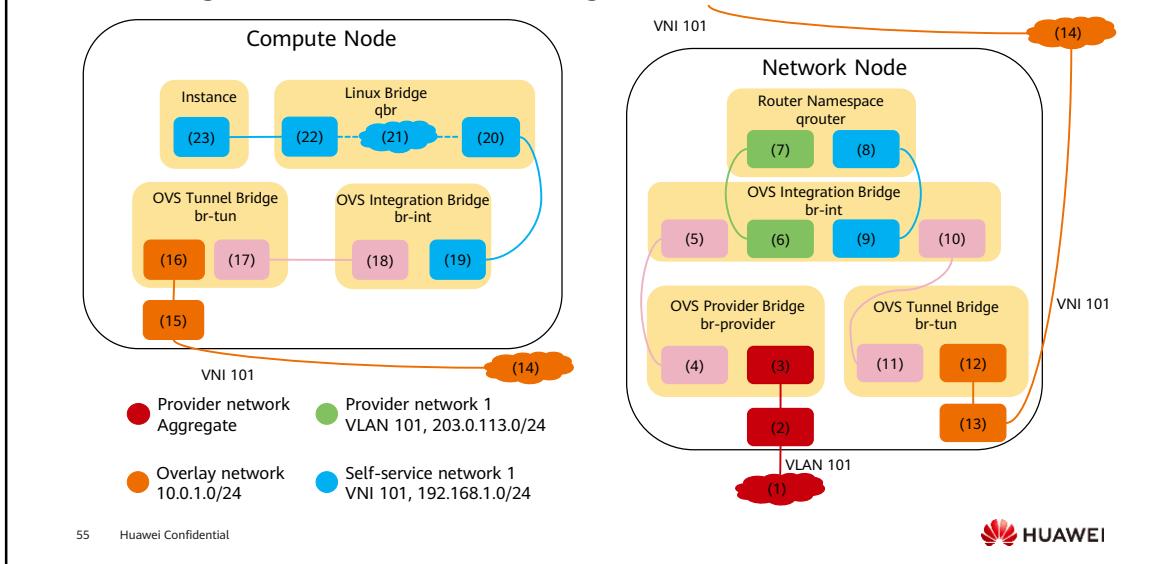


- Scenario description:
 - The instance runs on compute node 1 and uses self-service network 1.
 - The instance sends the data packet to the host on the Internet.
- The following operations involve compute node 1:
 - The instance interface (1) forwards the data packet to the security group bridge instance port (2) via veth pair.
 - The security group rule (3) of the security bridge processes the firewall and connection tracking of the data packet.
 - The security group bridge OVS port (4) forwards the data packet to the OVS integration bridge security group port (5) via veth pair.
 - The OVS integration bridge adds an internal VLAN tag to the data packet.
 - The OVS integration bridge exchanges the internal VLAN tag for an internal tunnel ID.
 - The OVS integration bridge patch port (6) forwards the data packet to the OVS tunnel bridge patch port (7).
 - The OVS tunnel bridge (8) wraps the packet using VNI 101.
 - The underlying physical interface (9) for overlay networks forwards the packet to the network node via overlay network (10).

- The following operations involve the network node:
 - The underlying physical interface (11) for overlay networks forwards the packet to the OVS tunnel bridge (12).
 - The OVS tunnel bridge unpacks the packet and adds an internal tunnel ID to it.
 - The OVS tunnel bridge exchanges the internal tunnel ID for an internal VLAN.
 - The OVS tunnel bridge patch port (13) forwards the packet to the OVS integration bridge patch port (14).
 - The OVS integration bridge port (15) for self-service networks removes the internal VLAN tag and forwards the packet to the self-service network interface (16) in the router namespace.
 - The router forwards the data packet to the OVS integration bridge port (18) for provider networks.
 - The OVS integration bridge adds an internal VLAN tag to the data packet.
 - The OVS integration bridge int-br-provider patch port (19) forwards the data packet to the OVS provider bridge phy-br-provider patch port (20).
 - The OVS provider bridge phy-br-provider exchanges the internal VLAN tag with the actual VLAN tag 101.
 - The OVS provider bridge br-provider port (21) forwards the packet to the physical interface (22).
 - The physical interface forwards the data packet to the Internet (23)

through the physical network infrastructure.

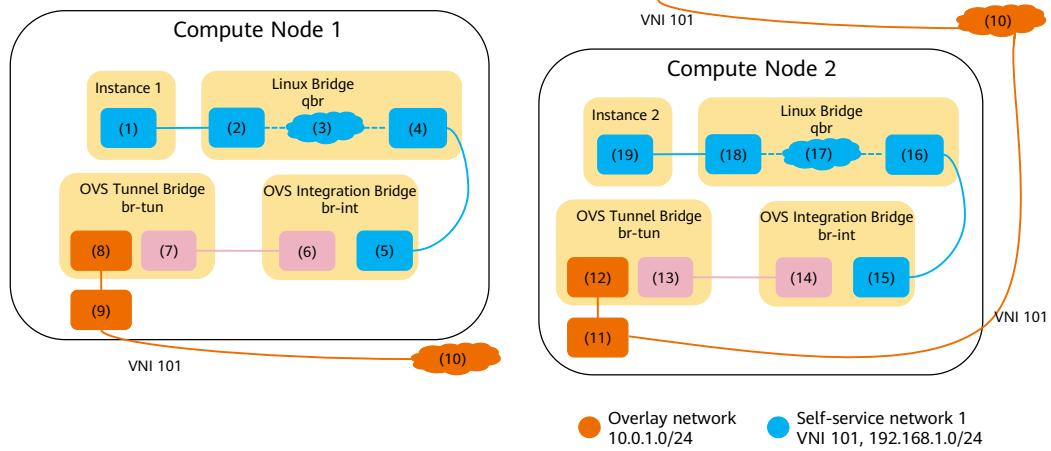
Accessing a VM with a Floating IP from an External Network



- Scenario description:
 - The instance runs on compute node 1 and uses self-service network 1.
 - The host on the Internet sends the data packet to the instance.
- The following operations involve the network node:
 - The physical network infrastructure (1) forwards the packet to the provider physical network interface (2).
 - The provider physical network interface forwards the data packet to the OVS provider bridge br-provider interface (3).
 - The OVS provider bridge exchanges the VLAN tag 101 with an internal VLAN tag.
 - The OVS provider bridge phy-br-provider port (4) forwards the data packet to the OVS integration bridge int-br-provider port (5).
 - The provider network OVS integration bridge port (6) removes the internal VLAN tag and forwards the packet to the provider network interface (6) in the router namespace.
 - The router forwards the data packet to the self-service network OVS integration bridge port (9).
 - The OVS integration bridge adds an internal VLAN tag to the data packet.
 - The OVS integration bridge exchanges the internal VLAN tag for an internal tunnel ID.
 - The OVS integration bridge patch-tun patch port (10) forwards the data packet to the OVS tunnel bridge patch-int patch port (11).
 - The OVS tunnel bridge (12) wraps the packet using VNI 101.
 - The underlying physical interface (13) for overlay networks forwards the packet to the network node via overlay network (14).

- The following operations involve the compute node:
 - The underlying physical interface (15) for overlay networks forwards the packet to the OVS tunnel bridge (16).
 - The OVS tunnel bridge unpacks the packet and adds an internal tunnel ID to it.
 - The OVS tunnel bridge exchanges the internal tunnel ID for an internal VLAN.
 - The OVS tunnel bridge patch-int patch port (17) forwards the data packet to the OVS integration bridge patch-tun patch port (18).
 - The OVS integration bridge removes the internal VLAN tag from the data packet.
 - The OVS integration bridge security group port (19) forwards the data packet to security group bridge OVS port (20) via veth pair.
 - The security group rule (21) of the security bridge processes the firewall and connection tracking of the data packet.
 - The security group bridge instance port (22) forwards the packet to the instance port (23) via veth pair.

East-West Traffic for VMs on the Same Network



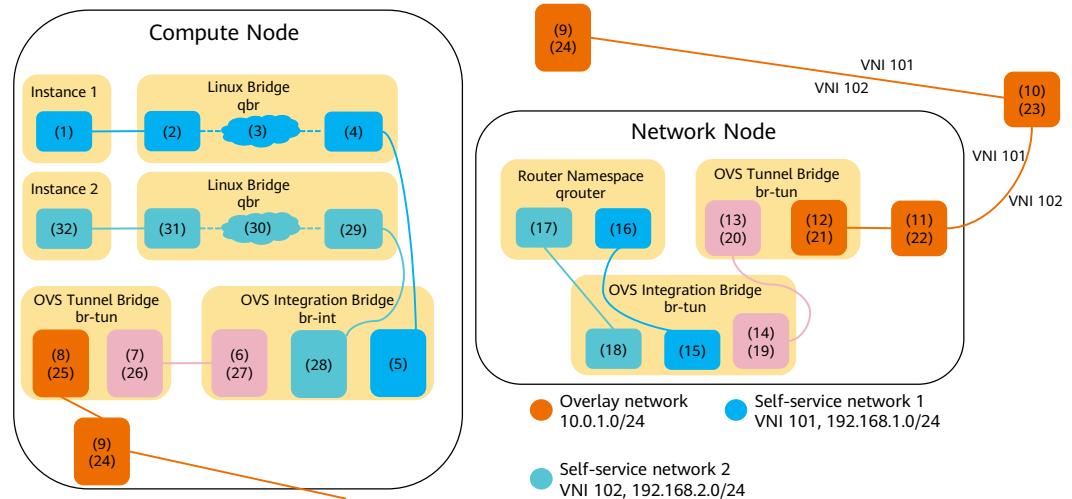
57 Huawei Confidential



- Scenario description:
 - Instance 1 runs on compute node 1 and uses self-service network 1.
 - Instance 2 runs on compute node 2 and uses self-service network 1.
 - Instance 1 sends the data packet to instance 2.
- The following operations involve compute node 1:
 - The interface (1) of instance 1 forwards the data packet to the security group bridge instance port (2) via veth pair.
 - The security group rule (3) of the security bridge processes the firewall and connection tracking of the data packet.
 - The security group bridge OVS port (4) forwards the data packet to the OVS integration bridge security group port (5) via veth pair.
 - The OVS integration bridge adds an internal VLAN tag to the data packet.
 - The OVS integration bridge exchanges the internal VLAN tag for an internal tunnel ID.
 - The OVS integration bridge patch port (6) forwards the data packet to the OVS tunnel bridge patch port (7).
 - The OVS tunnel bridge (8) wraps the packet using VNI 101.
 - The underlying physical interface (9) for overlay networks forwards the packet to the compute node 2 via the overlay network (10).

- The following operations involve compute node 2:
 - The underlying physical interface (11) for overlay networks forwards the packet to the OVS tunnel bridge (12).
 - The OVS tunnel bridge unpacks the packet and adds an internal tunnel ID to it.
 - The OVS tunnel bridge exchanges the internal tunnel ID for an internal VLAN.
 - The OVS tunnel bridge patch-int patch port (13) forwards the packet to the OVS integration bridge patch-tun patch port (14).
 - The OVS integration bridge removes the internal VLAN tag from the data packet.
 - The OVS integration bridge security group port (15) forwards the data packet to security group bridge OVS port (16) via veth pair.
 - The security group rule (17) of the security bridge processes the firewall and connection tracking of the data packet.
 - The security group bridge instance port (18) forwards the packet to port (19) of instance 2 via veth pair.

East-West Traffic for VMs on Different Networks



59 Huawei Confidential



- Scenario description:
 - Instance 1 runs on compute node 1 and uses self-service network 1.
 - Instance 2 runs on compute node 1 and uses self-service network 2.
 - Instance 1 sends the data packet to instance 2.
- The following operations involve compute node 1:
 - The interface (1) of instance 1 forwards the data packet to the security group bridge instance port (2) via veth pair.
 - The security group rule (3) of the security bridge processes the firewall and connection tracking of the data packet.
 - The security group bridge OVS port (4) forwards the data packet to the OVS integration bridge security group port (5) via veth pair.
 - The OVS integration bridge adds an internal VLAN tag to the data packet.
 - The OVS integration bridge exchanges the internal VLAN tag for an internal tunnel ID.
 - The OVS integration bridge patch port (6) forwards the data packet to the OVS tunnel bridge patch port (7).
 - The OVS tunnel bridge (8) wraps the packet using VNI 101.
 - The underlying physical interface (9) for overlay networks forwards the packet to the network node via overlay network (10).

- The following operations involve the network node:
 - The underlying physical interface (11) for overlay networks forwards the packet to the OVS tunnel bridge (12).
 - The OVS tunnel bridge unpacks the packet and adds an internal tunnel ID to it.
 - The OVS tunnel bridge exchanges the internal VLAN tag for an internal tunnel ID.
 - The OVS tunnel bridge patch-int patch port (13) forwards the data packet to the OVS integration bridge patch-tun patch port (14).
 - The OVS integration bridge port (15) for self-service network 1 removes the internal VLAN tag and forwards the packet to interface (16) of self-service network 1 in the router namespace.
 - The router sends the data packet to the next-hop IP address through interface (17) of self-service network 2, which is usually the gateway IP address on self-service network 2.
 - The router forwards the data packet to the OVS integration bridge port (18) of self-service network 2.
 - The OVS integration bridge adds an internal VLAN tag to the data packet.
 - The OVS integration bridge exchanges the internal tunnel ID for an internal VLAN.
 - The OVS integration bridge patch-int patch port (19) forwards the data packet to the OVS tunnel bridge patch-int patch port (20).
 - The OVS tunnel bridge (21) wraps the packet using VNI 102.
 - The underlying physical interface (22) for overlay networks forwards the packet to the compute node via the overlay network (23).

- The following operations involve the compute node:
 - The underlying physical interface (24) for overlay networks forwards the packet to the OVS tunnel bridge (25).
 - The OVS tunnel bridge unpacks the packet and adds an internal tunnel ID to it.
 - The OVS tunnel bridge exchanges the internal VLAN tag for an internal tunnel ID.
 - The OVS tunnel bridge patch-int patch port (26) forwards the data packet to the OVS integration bridge patch-tun patch port (27).
 - The OVS integration bridge removes the internal VLAN tag from the data packet.
 - The vethOVS integration bridge security group port (28) forwards the data packet to security group bridge OVS port (29) via pair.
 - The security group rule (30) of the security bridge processes the firewall and connection tracking of the data packet.
 - The veth security group bridge instance port (31) forwards the packet to the instance port (32) via pair.

Quiz

1. What network virtualization technologies does Linux use?
2. What components does Neutron have? What are their functions?
3. What are the Neutron network traffic models?

- 1. Linux mainly includes three types of network virtualization technologies: NIC virtualization (TUN, TAP, and VETH), switch virtualization (Linux Bridge and Open vSwitch), and network isolation (Network Namespace).
- 2. Neutron consists of components such as Neutron Server, Plugin, and Agent. Neutron Server provides OpenStack network APIs, receives requests, and invokes plugins to process the requests. Plugins process the requests sent by Neutron Server, maintain the status of the OpenStack logical network, and invoke agents to process the requests. Agents process plugin requests and implement various network functions on the network provider. In addition, the database is used to store OpenStack network status information, including networks, subnets, ports, and routers.
- 3. Linux Bridge + Flat/VLAN network and Open vSwitch + VXLAN network.

Summary

- This course described the positioning, functions, architecture, working principles, and common network traffic models of the OpenStack Network service (Neutron), and its interactions with other services.

More Information

- OpenStack Community
 - <https://www.openstack.org/>

Acronyms

- DNS: Domain Name Service (DNS) is highly available and scalable. It stably, securely, and intelligently converts website domain names or application resources to interconnect the IP addresses of enterprises and developer PCs. In addition to managing domain names, DNS routes end user requests to required websites or application resources.
- DHCP: Dynamic Host Configuration Protocol (DHCP) is a client-server network protocol. A DHCP server provides configuration parameters specific to the DHCP client host requesting information the host requires to participate on the Internet network. DHCP also provides a mechanism for allocating IP addresses to hosts.
- GRE: Generic Routing Encapsulation (GRE) is used for encapsulating IP datagrams tunneled through the Internet. GRE serves as a Layer 3 tunneling protocol and provides a tunnel for transparently transmitting data packets.
- LXC: Linux Container (LXC) is a kernel virtualization technology that provides lightweight virtualization to isolate processes and resources. It does not require instruction interpretation and is not as complex as full-virtualization. It is similar to Namespace in C++.
- NIC: Network Interface Card (NIC) is a computer circuit board or card that is installed in a computer so that it can be connected to a network.

Acronyms

- OVS: Open vSwitch (OVS) is a production quality, multilayer virtual switch licensed under the open source Apache 2.0 license. OVS is designed to automate (configuration, management, and maintenance) large networks through programmatic expansion. In addition, it supports standard management interfaces and protocols.
- QoS: Quality of Service (QoS) is a commonly-used performance indicator of a telecommunication system or channel. Depending on the specific system and service, it may relate to jitter, delay, packet loss ratio, bit error ratio, and signal-to-noise ratio. It is used to measure the quality of the transmission system and the effectiveness of the services that run on it. It is also used to evaluate the ability of a service provider to meet the demands of users.
- SNAT: Source Network Address Translation. If an internal IP address initiates a connection to the services on the public network, the gateway on the router or firewall translates the private IP address into a public IP address. This process is known as SNAT. SNAT lets you use private IP addresses to access the external network.
- VLAN: A Virtual Local Area Network (VLAN) is a group of hosts with a common set of requirements that communicate as if they were attached to the same broadcast domain, regardless of their physical location. VLAN membership can be configured through software. There is no need to physically relocate devices or connections. Network resources and users are logically divided based on a certain principle and a physical LAN is logically divided into multiple broadcasting domains (VLANs). The hosts on a VLAN can directly communicate with each other, but if they are on different VLANs, they cannot. This efficiently suppresses broadcast packets.

Acronyms

- VXLAN: Virtual Extensible Local Area Network (VXLAN) is a network virtualization technology, and attempts to improve extension during deployment of large-scale cloud computing. It uses a VLAN-like encapsulation technology to encapsulate MAC-based Layer 2 Ethernet frames into Layer 3 UDP packets.
- VNI: A VXLAN Network Identifier (VNI) is similar to a VLAN ID and used for differentiating VXLAN segments. VMs in different VXLAN segments cannot communicate with each other at Layer 2.
- VRF: Virtual Routing and Forwarding (VRF) is a technology applied to computer networks. VRF allows multiple independent instances to exist in the routing table of a router. Multiple instances can use the same or overlapping IP addresses without conflicts.
- VPN: A Virtual Private Network (VPN) is a system configuration that allows a subscriber to build a private network via connections to different network switches that may include private network capabilities. This technology uses cryptography to build a secure channel in a communications network.

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and
organization for a fully connected,
intelligent world.

Copyright©2022 Huawei Technologies Co., Ltd.
All Rights Reserved.

The information in this document may contain predictive
statements including, without limitation, statements regarding
the future financial and operating results, future product
portfolio, new technology, etc. There are a number of factors that
could cause actual results and developments to differ materially
from those expressed or implied in the predictive statements.
Therefore, such information is provided for reference purpose
only and constitutes neither an offer nor an acceptance. Huawei
may change the information at any time without notice.



OpenStack Orchestration Management



Foreword

- This course describes the positioning, functions, and architecture of Heat in OpenStack, its interactions with other services, and typical orchestration scenarios.

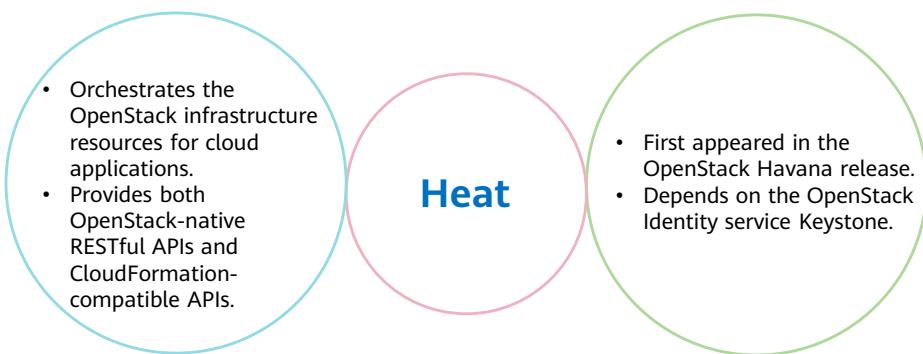
Objectives

- Upon completion of this course, you will understand:
 - The functions of Heat.
 - The positioning and functions of Heat in OpenStack and its interactions with other services.
 - The typical orchestration scenarios of Heat.

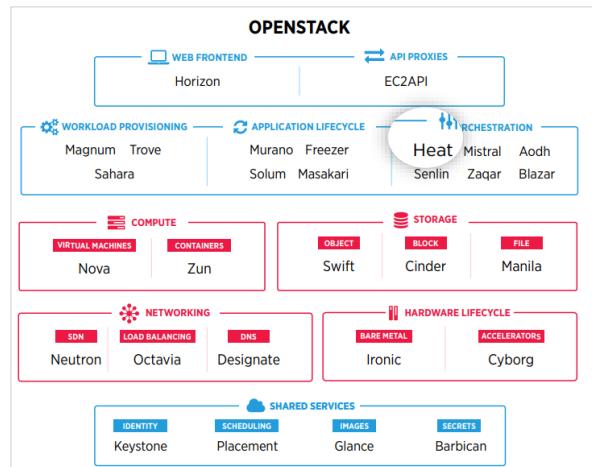
Contents

- 1. Heat Overview**
2. Heat Architecture
3. Typical Orchestration Scenarios of Heat

Orchestration Service: Heat



Positioning of Heat in OpenStack



Heat

- Heat is an OpenStack orchestration service. It orchestrates infrastructure resources for cloud applications.
- Heat provides both an OpenStack-native REST API and an AWS CloudFormation-compatible Query API.

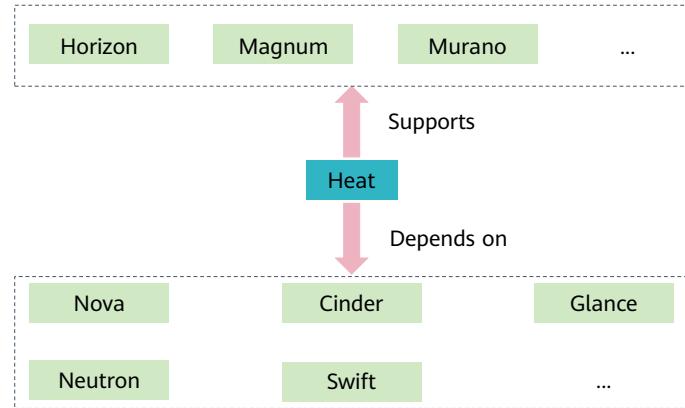
- Heat orchestrates infrastructure resources for cloud applications based on templates in the form of text files that can be treated like code.
- Heat provides both an OpenStack-native REST API and a CloudFormation-compatible Query API.
- Heat also provides an autoscaling service that integrates with OpenStack Telemetry, so you can include a scaling group as a resource in a template.

Heat Functions

- Heat is a service to orchestrate composite cloud applications using a declarative template format through an OpenStack-native REST API. The software integrates other core components of OpenStack into a one-file template system.
 - A Heat template describes the infrastructure for a cloud application in text files which are readable and writable by humans, but can also be managed by version control tools.
 - Templates specify the relationships between resources. This enables Heat to call out to the OpenStack APIs to create all the parts of your infrastructure to ensure everything is in place for your application to launch.

- The templates allow you to create most OpenStack resource types such as instances, floating IP addresses, volumes, security groups, and users. Heat provides advanced functionality such as instance high availability and nested stacks.

Interactions with Other Services

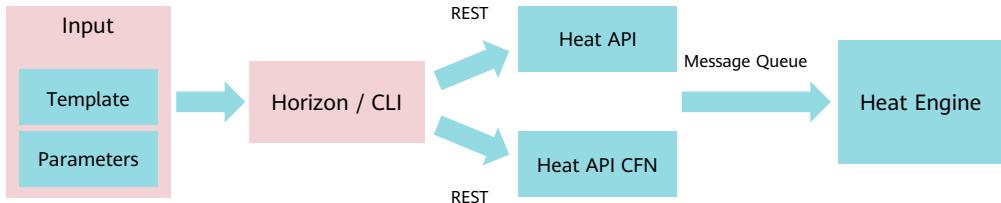


- Heat is a component based on underlying services such as Nova and Neutron and functions as an external interface of OpenStack. You do not need to directly access other OpenStack services. Instead, you only need to write resource requirements in the Heat template. Heat automatically invokes related service interfaces to configure the required resources.

Contents

1. Heat Overview
- 2. Heat Architecture**
3. Typical Orchestration Scenarios of Heat

Heat Architecture



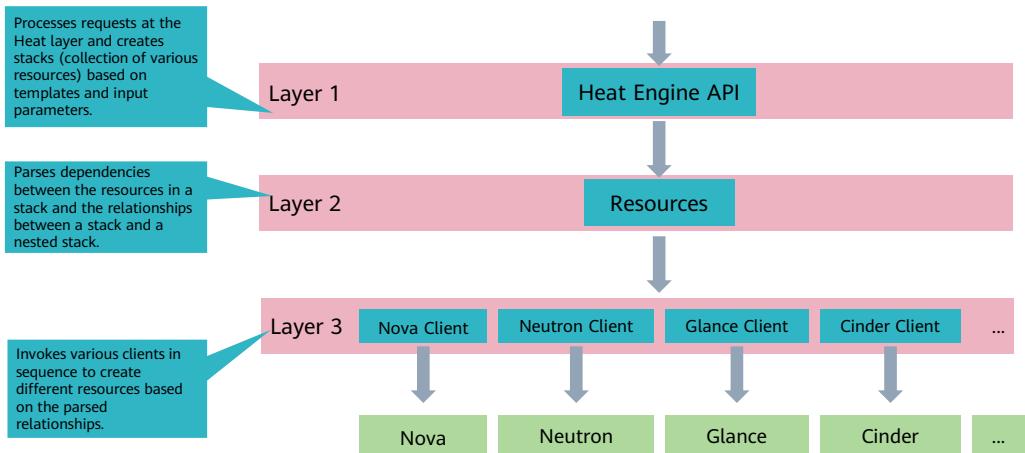
- After a user submits a request containing a template and parameters in Horizon or CLI, Horizon or CLI converts the request into a REST API call and then calls heat-api or heat-api-cfn. Heat-api and Heat-api-cfn verify the correctness of the template and transfer the template to Heat Engine through the message queue. Heat Engine then processes the request.
- A template in Heat is a collection of OpenStack resources, such as VMs, networks, storage devices, alarms, floating IP addresses, security groups, scaling groups, and nested stacks. By defining a template, you can describe the resources to be created in the template. You can use this template to create required resources for multiple times.

Heat Components

heat-api	heat-api-cfn	heat-engine
<ul style="list-style-type: none">This component provides an OpenStack-native REST API that processes API requests by sending them to heat-engine over RPC.	<ul style="list-style-type: none">It provides an AWS Query API that is compatible with AWS CloudFormation and processes API requests by sending them to heat-engine over RPC.	<ul style="list-style-type: none">The core element of Heat architecture. Its main responsibility is to orchestrate the launching of templates and return events back to the API consumer.

- heat-api: provides an OpenStack-native REST API that processes API requests by sending them to heat-engine. It is the entry for other components to interact with Heat.
- heat-api-cfn: provides an AWS CloudFormation-compatible API that processes API requests by sending them to heat-engine.
- heat-engine: is the core element of Heat. It schedules tasks and manages resource lifecycles. It does not provide the resource creation function. It only orchestrates resources.

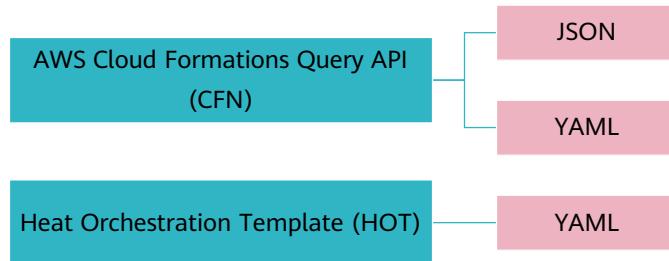
Heat Engine Architecture



- Heat Engine provides the following functions:
 - Layer 1 processes requests at the Heat layer and creates stacks (collection of various resources) based on templates and input parameters.
 - Layer 2 parses the dependency relationship between resources in a stack and the relationship between a stack and a nested stack.
 - Layer 3 invokes various clients in sequence to create various resources based on the parsed relationships.

Heat Template

- A Heat template is a collection of OpenStack resources, such as VMs, networks, storage devices, alarms, floating IP addresses, security groups, scaling groups, and nested stacks. By defining a template, you can describe the resources to be created in the template. You can then use this template repeatedly to create resources.



- HOT is in the process of surpassing the functionality of the CFN. The following uses the HOT template as an example.

Default Heat Template Compilation Language - YAML

- YAML Ain't Markup Language
 - Uses indentation (one or more spaces).
 - Uses hyphens (-) to represent arrays.
 - Use a colon (:) to mark each key-value pair in mappings.

```
invoice: 34843
date :
bill-to: *id001
  given : Chris
  family : Dumars
  address:
    lines: |
      458 Walkman Dr.
      Suite #292
      city : Royal Oak
      state : MI
      postal : 48046
ship-to: *id001
product:
  - sku       : BL394D
  quantity   : 4
  description: Basketball
  price      : 450.00
  - sku       : BL4438H
  quantity   : 1
  description: Super Hoop
  price      : 2392.00
tax : 251.42
total: 4443.52
```

- <https://yaml.org/start.html>

Heat Template - "Hello World"

Create a VM
using the
specified key pair,
image, and flavor.

```
heat_template_version:  
  
description: Simple template to deploy a single compute instance  
  
resources:  
    my_instance:  
        type: OS::Nova::Server  
        properties:  
            key_name: my_key  
            image: F18-x86_64-cfntools  
            flavor: m1.small
```

- `heat_template_version`: Each HOT template must include a key with a valid HOT version (for example, 2015-10-15). The value is not displayed due to QA requirements.
- `description`: This optional key allows for giving a description of the template, or the workload that can be deployed using the template.

HOT Template Structure

```
heat_template_version:  
description:  
# a description of the template: Template description. This attribute is optional.  
parameter_groups:  
# a declaration of input parameter groups and order: Input parameter groups and input  
sequence. This attribute is optional.  
parameters:  
# declaration of input parameters: Input parameters. This attribute is optional.  
resources:  
# declaration of template resources: Resources to be defined in the template, such as compute,  
storage, and network resources.  
outputs:  
# declaration of output parameters: Output parameters. This attribute is optional.  
conditions:  
# declaration of conditions: Conditions. This attribute is optional.
```

Mandatory: It specifies the version of the Heat template. Different versions support different functions.

Mandatory: This section with at least one resource should be defined in any HOT template.

- **heat_template_version:** The following values are supported. You are advised to select a Heat template version based on the actual OpenStack version.
 - 2013-05-23
 - 2014-10-16
 - 2015-04-30
 - 2015-10-15
 - 2016-04-08
 - 2016-10-14 or newton
 - 2017-02-24 or ocata
 - 2017-09-01 or pike
 - 2018-03-02 or queens
 - 2018-08-31 or rocky

HOT Template - resources Section

```
resources:  
  <resource ID>:  
    type: <resource type>  
    properties:  
      <property name>: <property value>  
    metadata:  
      <resource specific metadata>  
    depends_on:  
      <resource ID or list of ID>  
    update_policy:  
      <update policy>  
    deletion_policy:  
      <deletion policy>  
    external_id:  
      <external resource ID>  
    condition:  
      <condition name or expression or boolean>
```

- resource ID
 - A resource ID which must be unique within the resources section of the template.
- type
 - The resource type, such as OS::Nova::Server or OS::Neutron::Port. This attribute is required.
- properties
 - A list of resource-specific properties. The property value can be provided in place, or via a function. This section is optional.
- metadata
 - Resource-specific metadata. This section is optional.
- depends_on
 - Dependencies of the resource on one or more resources of the template. This attribute is optional.
- update_policy
 - Update policy for the resource, in the form of a nested dictionary. This attribute is optional.
- deletion_policy
 - Deletion policy for the resource. The allowed deletion policies are Delete, Retain, and Snapshot. This attribute is optional. The default policy is to delete the physical resource when deleting a resource from the stack.

- `external_id`
 - Allows for specifying the `resource_id` for an existing external (to the stack) resource. This attribute is optional.
- `condition`
 - Condition for the resource, which decides whether to create the resource or not. This attribute is optional.
 - It is supported since the Newton version.

HOT Template - Querying a Resource Type

- A Heat template supports a large number of resources. When defining resources, you can run related commands to query what parameters and resource types are needed.
 - Search for the resource to be created.

- \$ openstack orchestration resource type list

```
osbash@controller:~$ openstack orchestration resource type list | grep Server
| OS::Heat::DeployedServer
| OS::Nova::Server
| OS::Nova::ServerGroup
```

- Show resource details.

- \$ openstack orchestration resource type show NAME

```
osbash@controller:~$ openstack orchestration resource type show OS::Nova::Server
resource_type: OS::Nova::Server
properties:
    admin_pass:
        description: The administrator password for the server.
        immutable: false
```

Heat Stack

- A stack is a collection of resources. It is the basic unit for managing a group of resources, also the minimum unit for user operations.
- You can manage the stack lifecycle to automate application deployment and resource management.
- Stack example:

```
$ openstack stack create --template server_console.yaml --parameter "image=ubuntu" STACK_NAME
```

Field	Value
id	70b9feca-8f99-418e-b2f1-cc38d61b3ffb
stack_name	MYSTACK
description	The heat template is used to demo the 'console_urls' attribute of OS::Nova::Server.
creation_time	
updated_time	None
stack_status	CREATE_IN_PROGRESS
stack_status_reason	

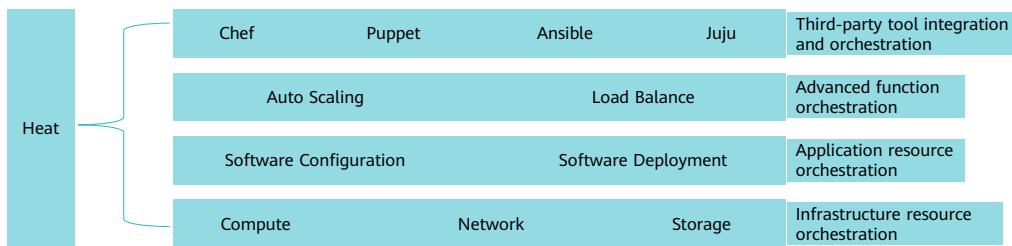
Common Heat Stack Commands

- stack list
- stack create
- stack show
- stack delete
- stack output list
- stack resource list
- stack event show

Contents

1. Heat Overview
2. Heat Architecture
- 3. Typical Orchestration Scenarios of Heat**

Heat Orchestration Scenarios



- Heat provides different types of orchestration for different types of resources:
 - Infrastructure resource orchestration: Basic resources, such as compute, storage, and network resources are orchestrated, so users can create custom scripts to configure VMs.
 - Application resource orchestration: Complex VM configuration is sometimes required for software installation and configuration.
 - Advanced function orchestration: Load balancing and auto scaling may be needed for applications.
 - Third-party tool integration and orchestration: Users can reuse the existing Ansible Playbook configuration in environments to save time.

Infrastructure Resource Orchestration with Heat

- Heat provides OpenStack resources with different resource types:
 - Taking VM resources as an example, Heat provides the OS::Nova::Server and some parameters (such as key, image, and flavor). You can define the parameters in a template or provide them during stack creation.
- Create a resource using a template:

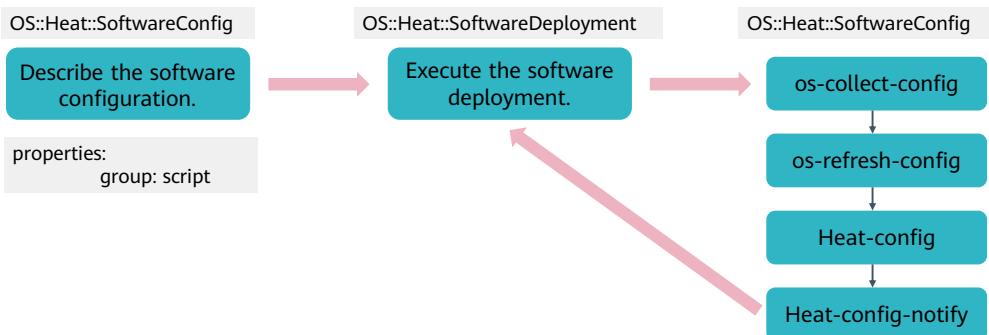
```
$ openstack stack create -template  
server_console.yaml --parameter  
"image=ubuntu" STACK_NAME
```

```
# server_console.yaml  
  
heat_template_version:  
  
description: |  
    The heat template is used to demo the 'console_urls' attribute  
    of OS::Nova::Server.  
  
parameters:  
    image:  
        type: string  
    flavor:  
        type: string  
        default: m1.small  
  
resources:  
    server:  
        type: OS::Nova::Server  
        properties:  
            image: { get_param: image }  
            flavor: { get_param: flavor }  
  
outputs:  
    single_console_type:  
        value: { get_attr: server, console_urls, novnc }  
        description: console URL for the server (novnc in this case)  
    all_console_urls:  
        value: { get_attr: [server, console_urls] }  
        description: all available console URLs for the server
```

- For more Heat template examples, visit the following website:
 - https://github.com/openstack/heat-templates/blob/master/hot/server_console.yaml

Software Configuration and Deployment Orchestration with Heat

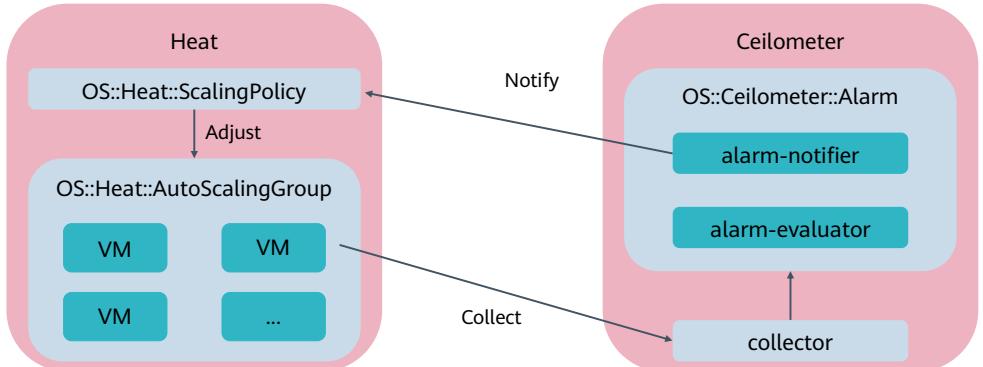
- Heat provides different resource types to support software configuration and deployment orchestrations. The most commonly used resource types are OS::Heat::SoftwareConfig and OS::Heat::SoftwareDeployment.



- Heat provides different resource types to support software configuration and deployment orchestrations. The following are some examples of resource types:
 - OS::Heat::CloudConfig: indicates the configuration used when the VM boot program is started. It is referenced by OS::Nova::Server.
 - OS::Heat::SoftwareConfig: describes the software configuration.
 - OS::Heat::SoftwareDeployment: executes the software deployment.
 - OS::Heat::SoftwareDeploymentGroup: executes software deployment for a group of VMs.
 - OS::Heat::SoftwareComponent: describes the software configuration based on different stages of the software lifecycle.
 - OS::Heat::StructuredConfig: is similar to OS::Heat::SoftwareConfig, but uses a map to describe its configuration.
 - OS::Heat::StructuredDeployment: executes the configuration corresponding to OS::Heat::StructuredConfig.
 - OS::Heat::StructuredDeploymentsGroup: executes the configuration corresponding to OS::Heat::StructuredConfig for a group of VMs.

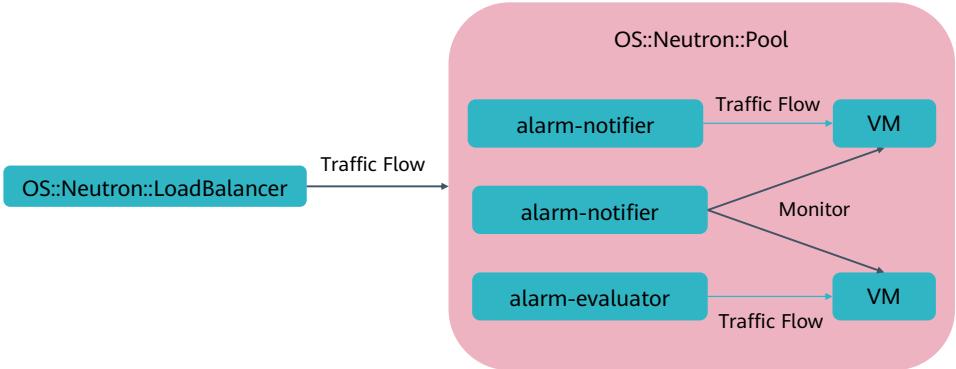
Resource Auto Scaling Orchestration with Heat

- Heat provides auto scaling groups and scaling policies. It works with Ceilometer to automatically scale resources based on different items, for example, loads.



Load Balancing Orchestration with Heat

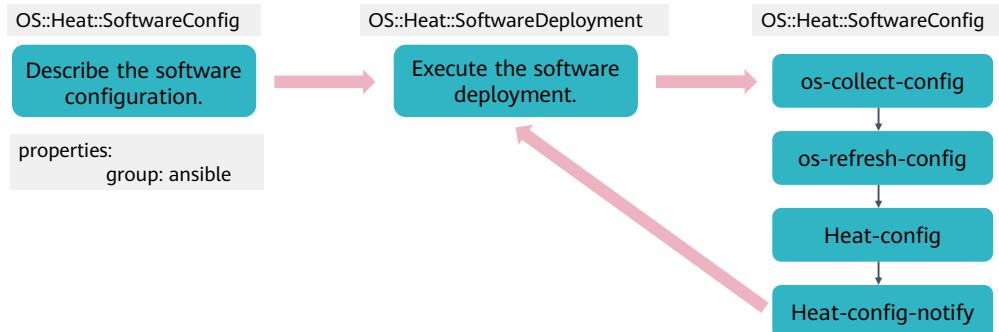
- Heat provides automated load balancing orchestration that is implemented by a group of different resource types.



- Load balancing is an advanced function and is implemented by a group of different resource types. The resource types are as follows:
 - OS::Neutron::Pool: defines a resource pool that usually consists of VMs.
 - OS::Neutron::PoolMember: defines the members in a resource pool.
 - OS::Neutron::HealthMonitor: defines a health monitor that monitors the resource status based on user-defined protocols, for example TCP, and sends the monitoring message to the OS::Neutron::Pool to adjust request distribution.
 - OS::Neutron::LoadBalancer: associates a resource pool to define the entire load balancing.

Heat-Configuration Management Tool Integration

- Heat supports popular management tools such as Chef, Puppet, and Ansible by collaboratively using OS::Heat::SoftwareConfig and OS::Heat::SoftwareDeployment.



- Numerous configuration management tools, such as Chef, Puppet, and Ansible, emerge, as DevOps becomes popular. In addition to providing a platform framework, these tools provide the scripts that can be flexibly configured and referenced for middleware and software deployments.

Quiz

1. (Single-answer question) Which of the following components is not part of Heat?
 - A. Heat-api
 - B. Heat-server
 - C. Heat-engine
 - D. Heat-cfn-api

- 1. B

Summary

- This course described the positioning, functions, and architecture of the OpenStack Orchestration service (Heat), its interactions with other services, and typical orchestration scenarios.

More Information

- OpenStack Community
 - <https://www.openstack.org/>

Acronyms

- API: Application Programming Interface (API) is a particular set of rules and specifications that are used for communication between software programs.
- AWS: Amazon Web Services (AWS) is a web services system developed by Amazon, which allows users to rent applications to run their own VMs.
- CLI: Command-Line Interface (CLI) is a means of communication between a program and its user, based solely on textual input and output. Commands are input with the help of a keyboard or similar device and are interpreted and executed by applications. Results are output as text or graphics to the interface.
- RPC: Remote Procedure Call (RPC) is a computer communication protocol that allows programs running on a computer to invoke sub-programs on another computer. The programmer does not need to program for the interaction.

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and
organization for a fully connected,
intelligent world.

Copyright©2022 Huawei Technologies Co., Ltd.
All Rights Reserved.

The information in this document may contain predictive
statements including, without limitation, statements regarding
the future financial and operating results, future product
portfolio, new technology, etc. There are a number of factors that
could cause actual results and developments to differ materially
from those expressed or implied in the predictive statements.
Therefore, such information is provided for reference purpose
only and constitutes neither an offer nor an acceptance. Huawei
may change the information at any time without notice.



OpenStack Telemetry Management



Foreword

- This course describes the positioning, functions, development and derivations, architecture, and data management capability of the OpenStack Telemetry service (Ceilometer).

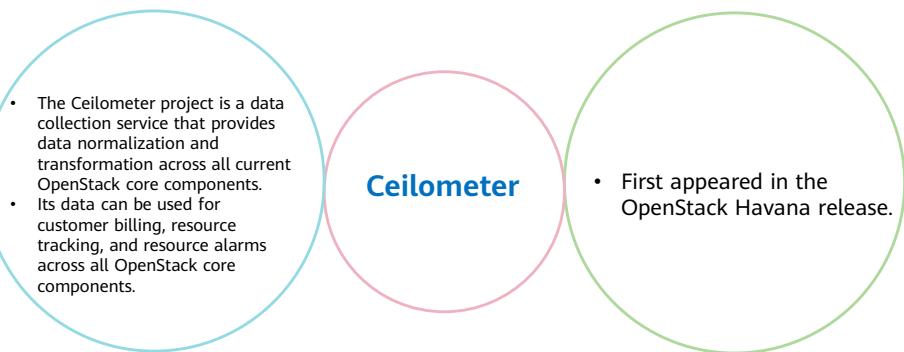
Objectives

- Upon completion of this course, you will understand:
 - What Ceilometer is.
 - The positioning, functions, development and deviation, and architecture of Ceilometer in OpenStack.
 - Ceilometer data management.

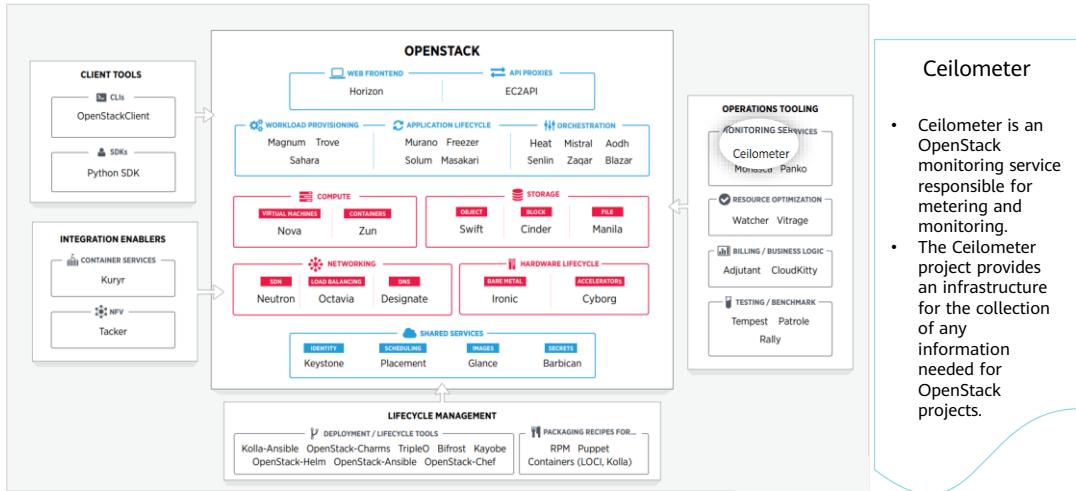
Contents

- 1. Ceilometer Overview**
2. Ceilometer Architecture
3. Ceilometer Data Management

Telemetry Service: Ceilometer



Positioning of Ceilometer in OpenStack



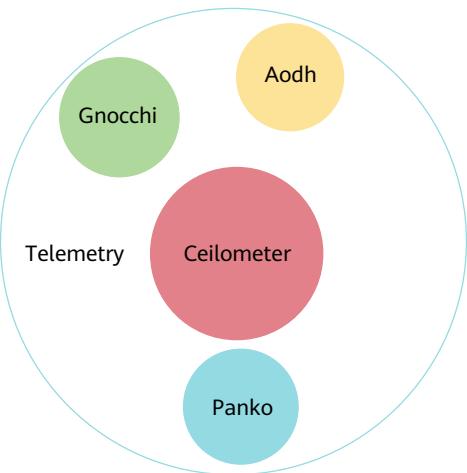
6 Huawei Confidential

Ceilometer

- Ceilometer is an OpenStack monitoring service responsible for metering and monitoring.
- The Ceilometer project provides an infrastructure for the collection of any information needed for OpenStack projects.



Ceilometer Development and Derivations



7 Huawei Confidential

- As shown in the figure, Ceilometer is the core component, the source of the Telemetry project.
- Other subprojects in Telemetry are Ceilometer-derived improvements.

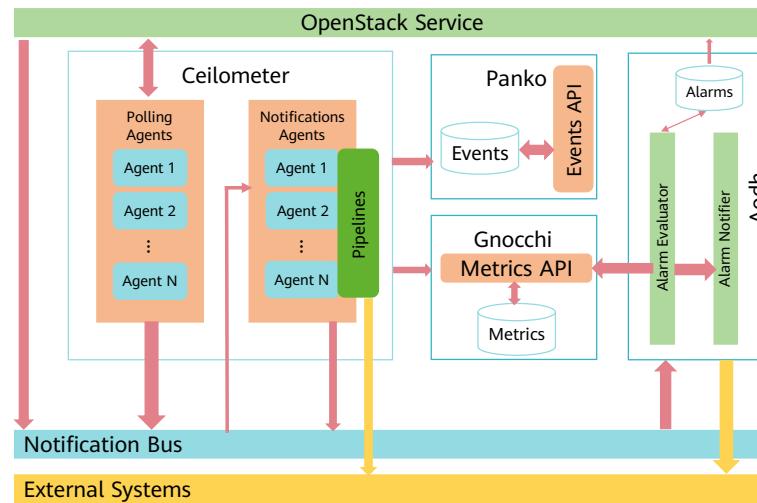


- The Telemetry project provides metering and monitoring functions in OpenStack. Its mission is to reliably collect data on the utilization of the physical and virtual resources comprising deployed clouds, persist these data for subsequent retrieval and analysis, and trigger actions when defined criteria are met.
- The Telemetry project includes the following subprojects:
 - Aodh: is an alarming service that can send alerts when user defined rules are broken. Its functionalities are derived from Ceilometer.
 - Panko: is an event storage service that provides the ability to store and querying event data generated by Ceilometer. Its functionalities are derived from Ceilometer.
 - Ceilometer: is the source of the Telemetry project. It provides a unified framework for collecting and saving various resource usage data.
 - Gnocchi: addresses the performance problems of the Ceilometer project in data storage design. It enables storage and indexing of time series data.

Contents

1. Ceilometer Overview
- 2. Ceilometer Architecture**
3. Ceilometer Data Management

Ceilometer Architecture



9 Huawei Confidential



- Ceilometer services are designed to scale horizontally. Additional workers and nodes can be added depending on the expected load.
- Ceilometer offers two core services:
 - Polling Agent: daemon designed to poll OpenStack services and build Meters.
 - Notification Agent: daemon designed to listen to notifications on message queue, convert them to events and samples, and apply pipeline actions.

Ceilometer Working Processes

After obtaining measurement data in one of two ways, Ceilometer converts the data into samples in a standard format and sends the samples to the Notification Agent through the notification bus.

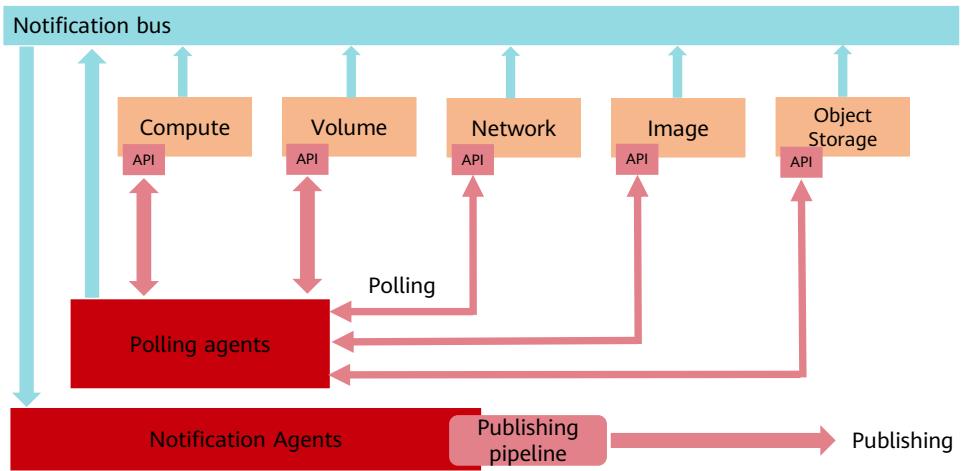
The Notification Agent converts and publishes samples based on a user-defined pipeline.

- Method 1: A third party sends data in the form of notification messages to the notification bus. The Notification Agent takes notification messages from the notification bus and extracts measurement data.
- Method 2: The Polling Agent collects information from local or remote service entities over APIs or other communication protocols at a regular interval.
- Data collected by Ceilometer can be published to multiple destinations.
 - gnocchi, which publishes samples/events to Gnocchi API;
 - notifier, a notification based publisher which pushes samples to a message queue which can be consumed by an external system;
 - prometheus;
 - zaqar, a multi-tenant cloud messaging and notification service for web and mobile developers;
 - file, which publishes samples to a file with specified name and location.

Contents

1. Ceilometer Overview
2. Ceilometer Architecture
- 3. Ceilometer Data Management**

Ceilometer - Data Collection

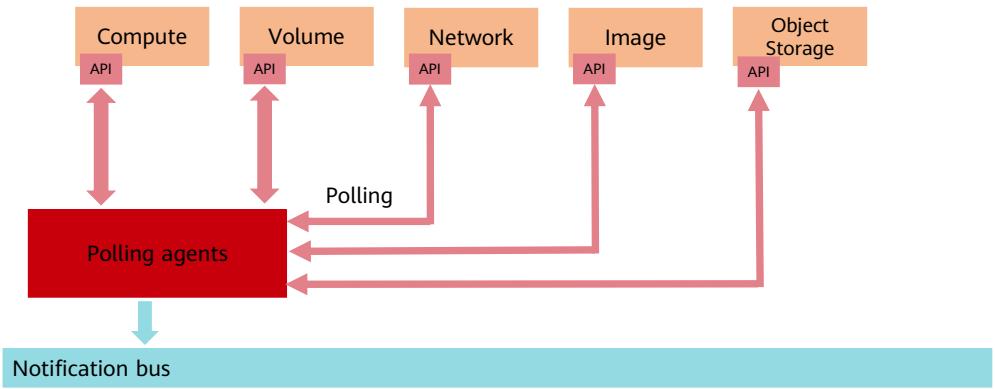


12 Huawei Confidential

 HUAWEI

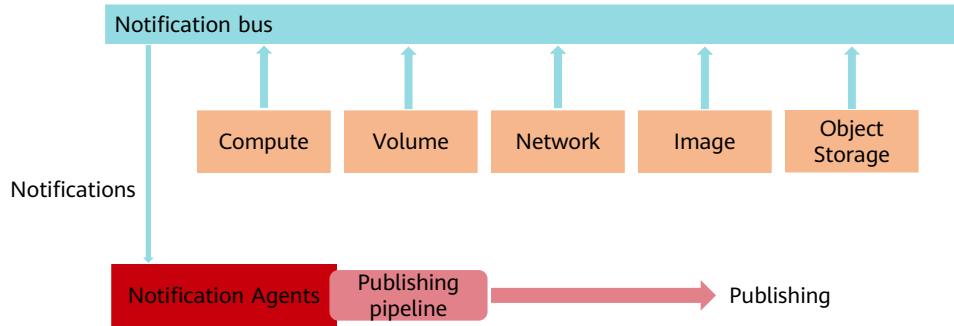
- The Ceilometer project created two data collection methods:
 - Method 1: A third party sends data in the form of notification messages to the notification bus. The Notification Agent takes notification messages from the notification bus and extracts measurement data.
 - Method 2: The Polling Agent collects information from local or remote service entities over APIs or other communication protocols at a regular interval.

Data Collection - Polling Agent: Asking for Data



- Method 2: The Polling Agent collects measurement data from local OpenStack services or remote service entities over APIs or other communication protocols at a regular interval, and sends the data to the notification bus. The Notification Agent takes messages generated on the notification bus and transforms them into Ceilometer samples or events.

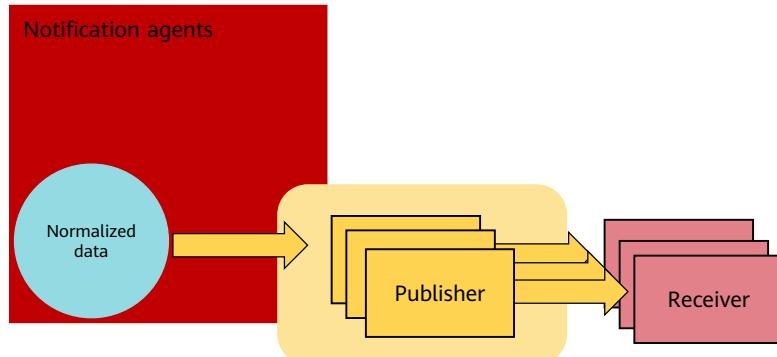
Data Collection - Notification Agent: Listening for Data



- **Notification Agent:** The heart of the system is the notification daemon (agent-notification) which monitors the message queue for data sent by other OpenStack components such as Nova, Glance, Cinder, Neutron, Swift, Keystone, and Heat, as well as Ceilometer internal communication.
- The notification daemon loads one or more listener plugins, using the namespace `ceilometer.notification`. Each plugin can listen to any topic. The listeners grab messages off the configured topics and redistribute them to the appropriate plugins to be processed into events and samples.

Ceilometer - Data Processing (1)

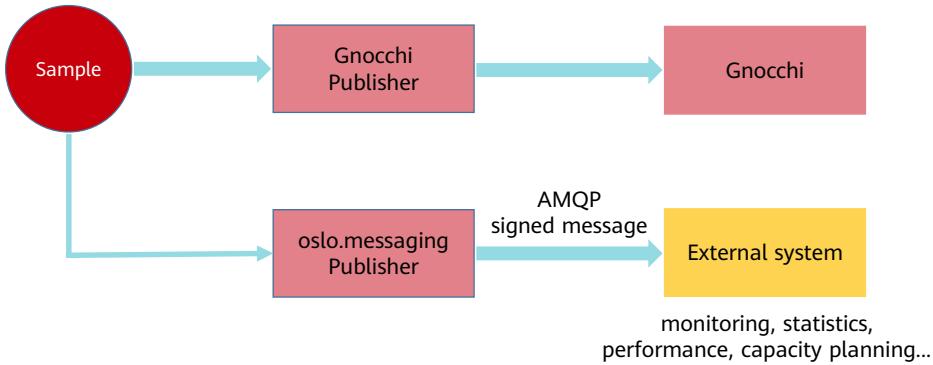
Pipeline manager



- Ceilometer offers the ability to take data gathered by the agents, manipulate it, and publish it in various combinations via multiple pipelines.
- In Ceilometer, the sampling frequency and publishing method of measurement data may vary according to application scenarios.
- Ceilometer uses pipelines to solve the problems in the sampling frequency and publishing method.
- Ceilometer allows multiple pipelines at the same time. Each pipeline definition consists of two parts: source and sink.
 - A source defines the data to be measured, the sampling frequency, the endpoints on which the data is to be sampled, and the sink that the data will be sent to.
 - A sink defines the transformers that will transform the data and the publishers that will publish the data.

Ceilometer - Data Processing (2)

Publishing data



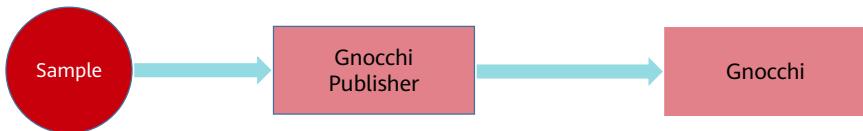
16 Huawei Confidential



- After obtaining measurement data, Ceilometer converts the data into samples in a standard format and sends the samples to the Notification Agent through the notification bus.
- The Notification Agent converts and publishes samples based on the user-defined pipeline.
- As shown in the preceding figure, two different publishers (oslo.messaging on the message bus and Gnocchi) are defined to publish a sample to different data receivers. That is, a sample can be published to multiple destinations. As shown in the preceding figure, the sample is sent to Gnocchi over Gnocchi API for data storage, and to notifier, which pushes the sample to a message queue which can be consumed by an external system.
- The following publisher types are supported:
 - gnocchi, which publishes samples/events to Gnocchi API;
 - udp, which publishes samples using UDP packets to a UDP address and port that can be configured by the administrator;
 - http, which targets a REST interface;
 - file, which publishes samples to a file with specified name and location;
 - prometheus, which publishes samples to Prometheus Pushgateway.

Ceilometer - Data Storage and Access

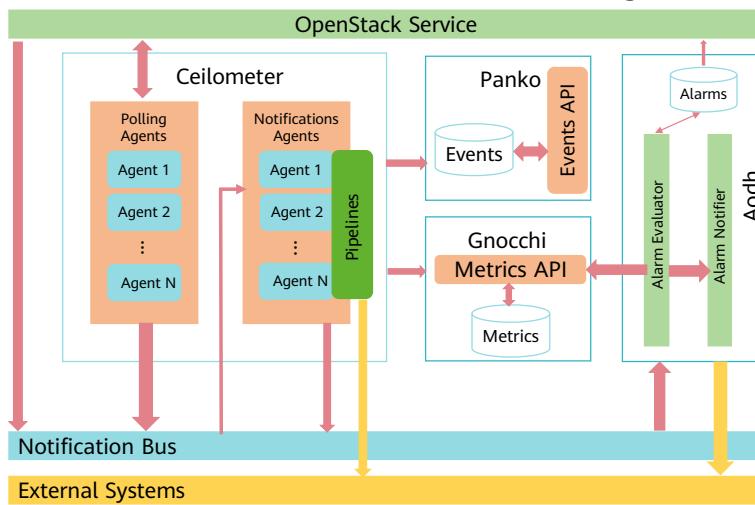
Ceilometer is designed solely to generate and normalize cloud data. The data created by Ceilometer can be published to any number of targets.



The recommended workflow is to push data to Gnocchi for efficient time-series storage and resource lifecycle tracking.

- Ceilometer generates a large amount of data. Common databases cannot meet storage requirements and become performance bottlenecks. The Telemetry community recommends that Gnocchi be used to save samples.
- Gnocchi is an open-source time series database. The problem that Gnocchi solves is the storage and indexing of time series data and resources at a large scale. This is useful in modern cloud platforms which are not only huge but also are dynamic and potentially multi-tenant. Gnocchi takes all of that into account.
- Gnocchi has been designed to handle large amounts of aggregates being stored while being performant, scalable and fault-tolerant.
- Data created by Ceilometer can be published to any number of destinations using publishers.

Ceilometer - Alarm Data Processing



- Aodh provides alerts and trigger actions against metric or event data collected by Ceilometer.
- Aodh allows users to set alarms based on evaluation of a collection of samples or a dedicated event.
- When setting an alarm, the user invokes the Aodh API server to specify the alarm trigger conditions and actions to be taken.



- Aodh consists of the following services, each of which is designed to scale horizontally:
 - API: provides RESTful APIs for users.
 - Alarm Evaluator: periodically checks whether the trigger conditions of alarms except the event-type alarms are met.
 - Alarm Listener: checks whether the trigger conditions of the corresponding event-type alarms are met based on the event messages on the Notification Bus.
 - Alarm Notifier: executes the user-defined action when the trigger conditions of alarms are met.
- When creating or modifying an alarm, users can set different actions to be triggered when the alarm is reported. When Alarm Evaluator periodically checks the alarm status or Alarm Listener checks the received event, if Alarm Evaluator or Alarm Listener detects that an action has been defined for the alarm status, the action will be invoked by the Alarm Notifier service.

Quiz

1. What are the functions of Ceilometer?
2. What data collection methods does Ceilometer provide?

- 1. Ceilometer is one of the OpenStack monitoring services. It is responsible for metering and monitoring. The Ceilometer project provides an infrastructure to collect any information needed regarding OpenStack projects. Its data can be used to provide customer billing, resource tracking, and alarming capabilities across all OpenStack core components.
- 2. The Ceilometer project created two methods to collect data: (1) The Polling Agent collects information from local or remote service entities over APIs or other communication protocols at a regular interval. (2) A third party sends data in the form of notification messages to the notification bus. The Notification Agent takes notification messages from the notification bus and extracts measurement data.

Summary

- This course described the positioning, functions, and architecture, and data management of the OpenStack Telemetry service (Ceilometer). You will have a better understanding of the customer billing, resource tracking, and alarming functions of OpenStack core components.

More Information

- OpenStack Community
 - <https://www.openstack.org/>

Acronyms

- API: Application Programming Interface (API) is a particular set of rules and specifications that are used for communication between software programs.

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and
organization for a fully connected,
intelligent world.

Copyright©2022 Huawei Technologies Co., Ltd.
All Rights Reserved.

The information in this document may contain predictive
statements including, without limitation, statements regarding
the future financial and operating results, future product
portfolio, new technology, etc. There are a number of factors that
could cause actual results and developments to differ materially
from those expressed or implied in the predictive statements.
Therefore, such information is provided for reference purpose
only and constitutes neither an offer nor an acceptance. Huawei
may change the information at any time without notice.



HUAWEI CLOUD Stack Architecture and Components



Foreword

- The advent of new DC technologies and business requirements has created tremendous challenges for traditional DCs. In response to these challenges, Huawei created a next-generation solution: HUAWEI CLOUD Stack. This lesson covers problems faced by traditional IT systems and enterprises and describes some of the challenges involved in digital transformation. It describes the HUAWEI CLOUD Stack solution and its components.

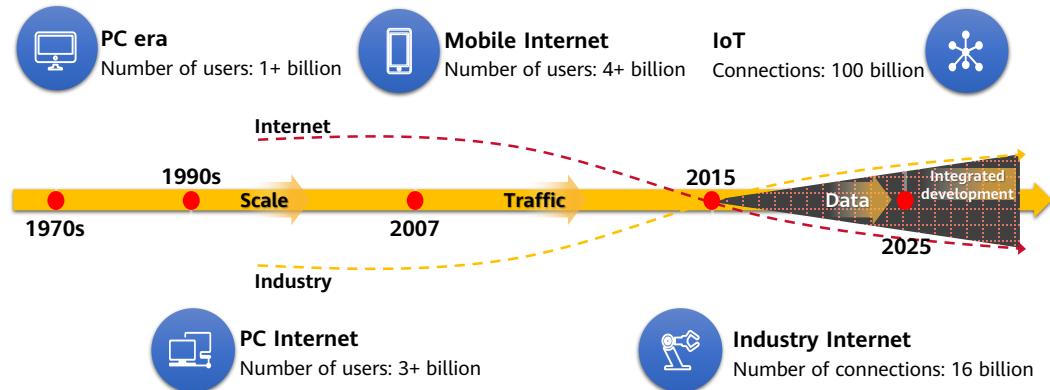
Objectives

- Upon completion of this course, you will understand:
 - The challenges facing and needs of enterprises undergoing digital transformation.
 - The HUAWEI CLOUD Stack solution and its architecture.
 - The HUAWEI CLOUD Stack platform components: FusionSphere OpenStack, ManageOne, eSight, FusionCare, and CloudNetDebug.
 - The HUAWEI CLOUD Stack common components, including load balancing, DNS, clock synchronization, DMK, API Gateway, Combined API, CCS, SDR, TaskCenter, and GaussDB.

Contents

- 1. HUAWEI CLOUD Stack Solution and Architecture**
2. HUAWEI CLOUD Stack Product Components and Common Components

Digital Transformation in Mobile Internet and Industrial Internet

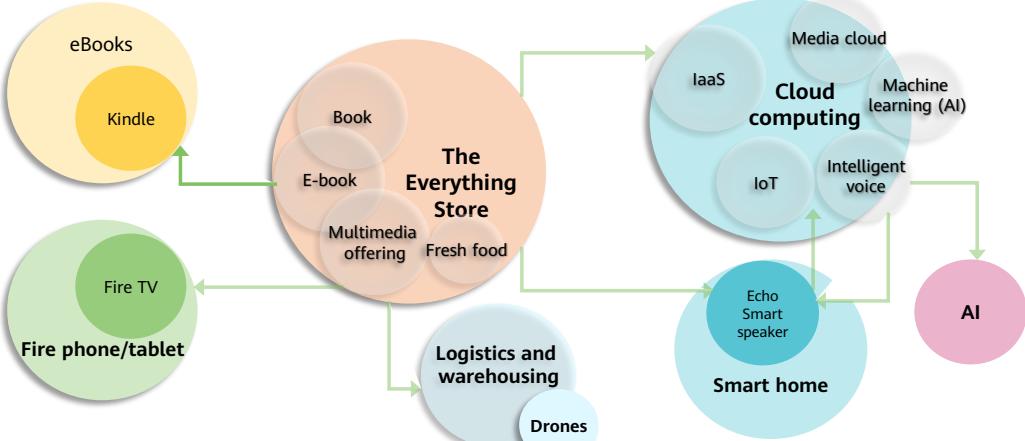


Digital transformation: With technologies like cloud computing, big data, AI, IoT, and 5G, enterprises can improve efficiency internally and services externally.

- Industrial Internet is developed from the consumer Internet. It indicates that traditional industries leverage big data, cloud computing, smart terminals, and network advantages to boost efficiency internally and improve services externally. It provides an important way for traditional industries to transform and upgrade through Internet+.
- The number of PC users reached 1 billion in 30 years. The number of Internet users reached 3 billion in 20 years. The number of mobile Internet users reached 4 billion within only about 10 years. With the development of the Internet of Things (IoT), the connections are shifted from between people to between everything. The number of connections increase exponentially. By 2015, the number of connections has reached 16 billion. It is estimated that by 2025, the number of connections will reach 100 billion. In the near future, all things will be connected.
- The Internet has evolved from the consumer Internet to the industrial Internet. The consumer Internet has enriched people's communication and life, while the industrial Internet has connected different enterprises as well as upstream and downstream industries. Furthermore, the industrial Internet has connected individuals and data between enterprises and reconstructed the service chain and industry chain of traditional industries.

- In terms of the economics, in the PC era, enterprises made profits by selling a large number of hardware devices (profiting from large-scale sales). In the consumer Internet era, traffic was used for yielding profits. A large number of Over The Top (OTT) vendors started to seize the entrances (such as computers, mobile phones, and tablets) to Internet by providing various applications for users through the Internet to make profits. In the industrial Internet era, enterprises can make profits from technologies through a large amount of data, for example, improving workflows and efficiency through big data.

Amazon Continuously Incubates New Business Models Through Digital Platforms



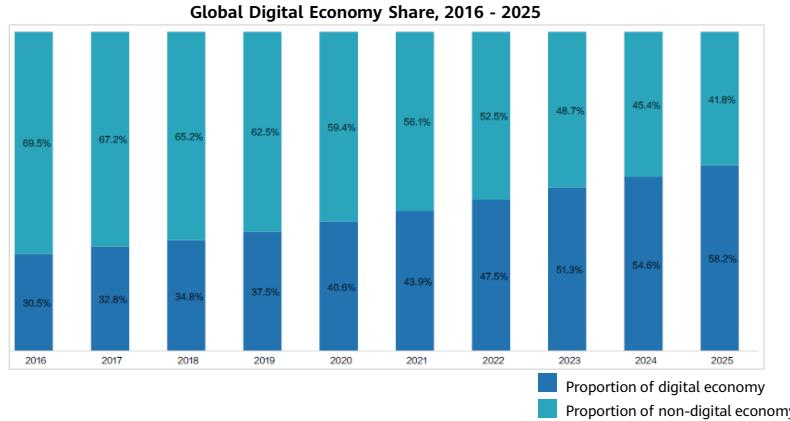
7 Huawei Confidential



- By building a digital platform, Amazon has developed the "flywheel" strategy, which indicates that each business module of a company is interconnected and promotes each other, like a flywheel. The idea is that a flywheel takes a lot of effort at the start, but once it gets spinning, it continues to quickly gain momentum and spin faster. The customer experience is the starting point for the Amazon Flywheel. Specifically, Amazon improves customer experience by striving for more profits for customers, which is consistent with Huawei's core values. Amazon attracts more customers to buy their self-developed products and products from third-party sellers. In return, customers creates more expenditures for Amazon. With the increased sales, Amazon can have stronger bargaining power, which allows Amazon's self-developed products to be sold at lower prices, attracting more customers. The flywheel effect enables Amazon's businesses to be fully interconnected and promote each other, thereby driving its rapid development.

- With digital transformation, Amazon has built its own development concepts: structure reconstruction and data operation.
 - Amazon has reconstructed its structure by deriving new services from core services, starting from e-commerce services. The new services include logistics robots, logistics drones, Kindle, Echo, and AWS. As the growth of e-commerce services slows down, these new services will be derived from core services and reconstructed for future transformation. Amazon has been regarded to be in the process of transformation. Disaggregation and reconstruction are digital strategic ideas that are much more important than developing a new technology and developing a new product.
 - As a big data company, Amazon's data operations and data-based idea require that managers and sales personnel must keep in contact with data analysts in their management and sales operations, respectively. The data used must be objective and authentic and is not cleared in a timely way. Bezos put forward six basic requirements for platform implementation, including building service-based external data and functional architectures. Amazon emphasizes data governance, and big data includes not only data analysis, but also data collection, storage, organization, and sharing.

Digital Products and Services Accelerate the Arrival of a Digital Era



According to IDC's research, the global digital economy driven by digital products and services will account for 58.2% by 2025.

- Digital transformation has become an inevitable trend for enterprises' future innovation and development since the benefits it has brought. In addition to Amazon, many enterprises (such as Huawei, Alibaba, Tencent, and Jingdong) are also undergoing digital transformation in their ways. According to the research of International Data Corporation (IDC), the global digital economy driven by digital products and services will account for 58.2% by 2025.
- Terms:
 - IDC, as a wholly-owned subsidiary of International Data Group (IDG, Inc.), is a global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. It often publishes some market news, forecast reports, and articles about hot topics discussed by senior analysts in the industry.

Policy-Driven Transformation



Faster innovation and more agility for emergency response



More new capabilities, higher quality development



More open, more inclusive ecosystems

The China's 14th Five-Year Plan promotes the use of **hybrid clouds** to develop industry solutions.



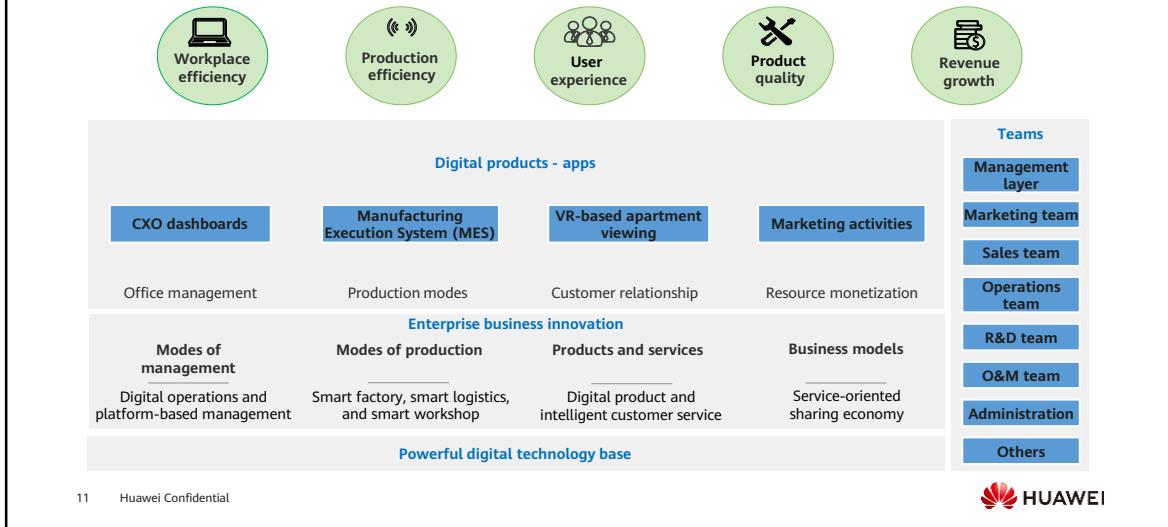
Implement the **Cloud-based, Data-Driven Transformation** plan to promote digital transformation for the entire industry chain with the use of data. Build international industrial Internet platforms and digital transformation benchmark in key industries and regions.

Improve national e-Gov networks and intensively build e-Gov cloud platforms and data center systems to speed up the cloud migration of e-Gov information systems.

Accelerate the iterative upgrade of cloud operating systems and promote innovative technologies, such as ultra-large distributed storage, elastic computing, and virtual data isolation, to enhance cloud security. **Focus on hybrid clouds** to develop industry solutions and promote system integration and O&M management cloud services.

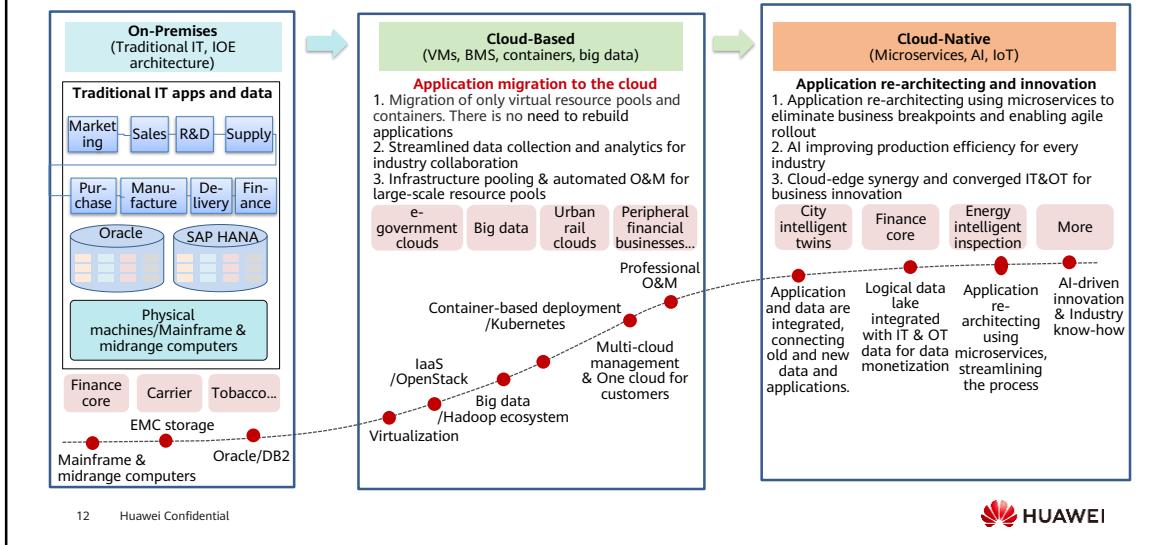
- Digital transformation has become a common practice. With the digital convergence of the physical and information worlds, industries, such as manufacturing, retail, finance, construction, and real estate, are changing, accelerating the formation of new digital industry ecosystems, such as new manufacturing, retail, finance, and services.
- With the deepening of digital transformation, the China's 14th Five-Year Plan promotes the use of hybrid clouds to develop industry solutions, accelerating the iterative upgrade of cloud operating systems and promoting innovative technologies, such as ultra-large distributed storage, elastic computing, and virtual data isolation, to enhance cloud security. **The industry solutions focus on hybrid clouds** to promote system integration and O&M management cloud services.

Industry-Driven Transformation



- Enterprises should abandon the old strategy "me too but cheaper". Instead, they should respond to fast-changing customer requirements and adopt new technologies and business models for innovation.
- To quickly response to customer requirements, enterprises need to implement real-time management and precise decision-making through digital transformation of all business processes, such as operation management, production and manufacturing, products and services, and marketing and business models. Industry 4.0 has led to a new production and manufacturing management model. Users' individual requirements drive the optimization of product experience. New marketing models and new business models (with focus being shifted from selling products to selling services) are driving the new growth of enterprise businesses.

The Evolution of Digital Transformation



- Digital transformation is divided into three phases: on-premises, cloud-based, and cloud-native. In fact, 80% of customers are still in the cloud-based phase, in which customers need to migrate their applications to the cloud using virtualized resources, containers, and BMS service without changing their applications. This migration greatly improves resource provisioning and O&M efficiency. In this scenario, customers focus on the stable and reliable cloud platform, automated management capabilities, and whether northbound and southbound interfaces are open. After all workloads are migrated to cloud, customers will be in the cloud-native phase. Applications and data will be transformed and reconstructed, which can bring uncertain challenges for customers, independent software vendors (ISVs), and vendors. The cloud-based and cloud-native models will coexist for about over ten years.

What Clouds Are Required for Government and Enterprise Digital Transformation?



Scattered resources make it difficult for different departments to collaborate.



Data storms cannot be analyzed or processed in real time, which makes it decision-making harder.



Existing systems are complex and have a massive volume of data and diverse interfaces, making customer-oriented innovation difficult.



Tailored to government and enterprise needs
One unified cloud from the customer's perspective



Cross-domain synergy for real-time operations



Innovation from a foundation to accelerate application innovation

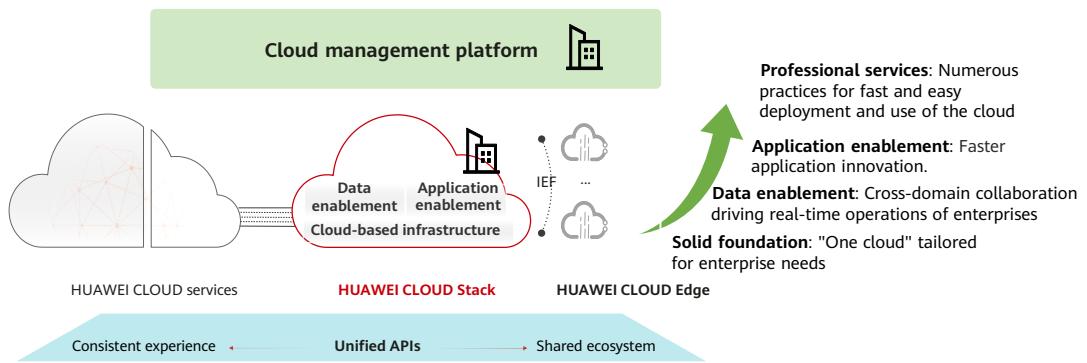
13 Huawei Confidential



- The cloud-based and cloud-native phases are closely related to clouds in digital transformation. What kind of cloud does government and enterprise customers need during digital transformation? To answer this question, we need to first understand the problems and challenges faced by government and enterprise customers.
 - In traditional government and enterprise IT systems, system functions are usually fragmented. Each business department has its own private cloud.
 - Each business department needs to process a large volume of data, which may cause data storms. As a result, business departments cannot analyze and process data in real time, adversely affecting management decision-making.
 - Existing systems are complex and have a massive number of data and interfaces, making customer-oriented innovation difficult.
- How can customers manage inventory resources when applications are smoothly migrated to the cloud in the cloud-based phase? How are resources shared and scheduled on demand? How can customers smoothly migrate their applications to the cloud? How can customers ensure reliable running of applications in the cloud without traditional mainframe, midrange computers, and cluster servers? These issues are the primary issues to be considered during the intelligent

upgrade of governments and enterprises.

HUAWEI CLOUD Stack: Tailored to the Needs of Government and Enterprise Digital Transformation



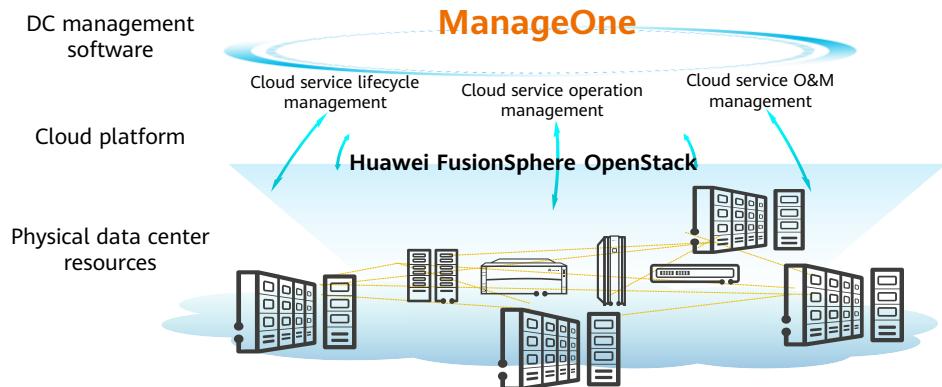
14 Huawei Confidential



- HUAWEI CLOUD and HUAWEI CLOUD Stack are designed with **the same architecture, APIs, and backbone versions**. They aim to **deliver the same cloud service experience and share the same ecosystems**. Because of these, Huawei is able to quickly synchronize rich cloud services, capabilities, as well as ecosystem resources from the public cloud to the customer's local data center (as well as HUAWEI CLOUD Stack on customer premises). In this way, Huawei can accelerate intelligent upgrade for government and enterprise customers. HUAWEI CLOUD Stack supports intelligent upgrade policies for government and enterprise customers, which can be implemented according to the following phases:
 - Cloud-based infrastructure builds a solid foundation and enables services to be migrated to the cloud.
 - Data enablement facilitates the development of logical data lakes.
 - Application enablement facilitates application rebuilding and innovation, opening the cloud native era.
 - Finally, best practices help customers quickly build the cloud and enjoy reliable services, and allow clouds to match and be integrated with government and enterprise architectures.

What Is HUAWEI CLOUD Stack?

Physical distribution, logical unification, service-driven, O&M collaboration, and service awareness



15 Huawei Confidential



- The advent of new DC technologies and business demands poses tremendous challenges to traditional DCs. To rise to these challenges, Huawei launches a next-generation HUAWEI CLOUD Stack solution.
- Within the HUAWEI CLOUD Stack solution, FusionSphere OpenStack is used as the cloud platform to consolidate resources across physical DCs, and ManageOne as DC management software to manage multiple DCs in a unified manner. A close synergy between FusionSphere and ManageOne allows convergence of multiple DCs, improving overall enterprise IT efficiency. The solution also delivers a rich store of cloud services in compute, storage, network, security, disaster recovery (DR) and backup, big data, database, and platform as a service (PaaS) categories.

- HUAWEI CLOUD Stack is a service-driven data center (DC) solution that features unified management of physically discrete but logically unified resources, cloud-pipe synergy, and service awareness. It supports sustainable service development of enterprises or branches and meets full lifecycle management requirements.
 - Physical distribution indicates that multiple DCs of an enterprise are distributed in different regions. By deploying a unified cloud platform, enterprises can consolidate physically dispersed IT resources to provide services in a unified manner.
 - Logical unification indicates that DC management software uniformly manages multiple DCs in different regions. It involves the following aspects:
 - Provides a unified O&M platform to manage and schedule resources from DCs in different regions.
 - Provides a unified operation management platform, which manages cloud services through a unified operation management interface. Cloud services are decoupled from the operations module, which eases the tight coupling of multiple components and accelerates version release.

HUAWEI CLOUD Stack Advantages

Reliability

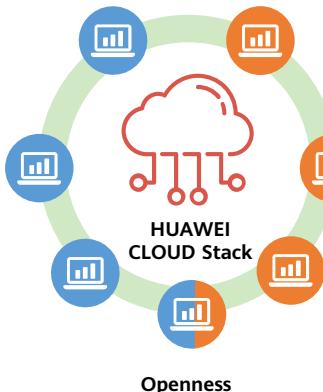
This solution enhances the reliability of the entire system, of individual devices, and of the data. The distributed architecture of the cloud platform improves the overall system reliability and reduces the system reliance on the reliability of a single device.

Availability

The system delivers remarkable availability by employing hardware/link redundancy, high-availability clusters, loose coupling between applications and the lower level hardware, and designing fault tolerance into the applications.

Security

The solution complies with industry standards for security to ensure that your DC is safe. It addresses the security of networks, hosts, virtualization, and data.



Maturity
HUAWEI CLOUD Stack uses an architecture with hardware, and software that have been tested in large-scale commercial deployments and includes an IT management solution that complies with Information Technology Infrastructure Library (ITIL) standards.

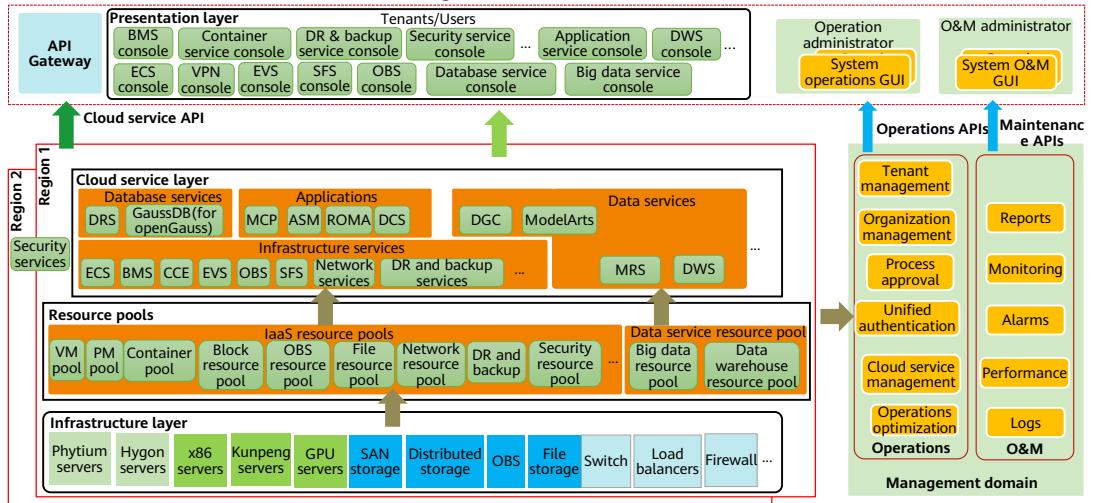
Advancement
Advanced cloud computing technologies and concepts make the value proposition clear. Virtualization and techniques like dynamic resource deployment ensure the effectiveness and practicality of the technologies and deployment modes available.

Scalability
DC resources must be flexibly adjusted to adapt to changing service loads and the IT infrastructure has to be only loosely coupled with service systems so that users can add IT hardware devices as needed when capacity expansion is required.

- Terms:

- Information Technology Infrastructure Library (ITIL) is a widely recognized set of practice guidelines for effective IT service management. ITIL is an IT service management standard library developed by the British National Computer and Telecommunications Administration (CCTA) in the late 1980s. It transforms the best practices of IT management in various industries in the UK into a standard, improving the utilization of IT resources and service quality.
- An Independent Software Vendor (ISV) makes and sells software products that run on one or more computer hardware or operating system (OS) platforms.

HUAWEI CLOUD Stack System Architecture



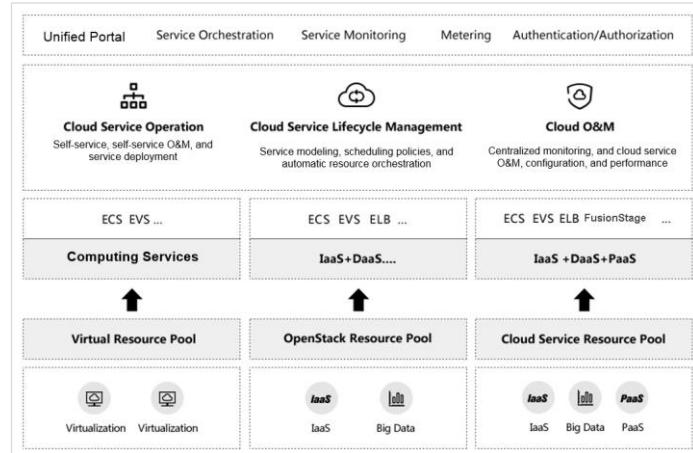
18 Huawei Confidential



- The HUAWEI CLOUD Stack solution consists of four layers:
 - The infrastructure layer supports multi-architecture computing by supporting CPUs of different architectures, including x86, Kunpeng, Phytium, and Hygon. It also supports GPU computing, distributed storage, centralized storage, switches, load balancers, and firewalls.
 - The resource pool layer uses cloud platform software to enable and operate hardware resource pools. At this layer, IaaS, DR, big data, and data warehouse resources can be controlled.
 - At the cloud service layer, HUAWEI CLOUD Stack enables and controls cloud services.
 - The operations and maintenance management platform, ManageOne, is deployed at the top presentation layer, which provides an entry for tenants and O&M management. ManageOne uses Console Home to integrate the consoles of various cloud services and provide a unified portal for using cloud services.

- ManageOne also provides system-level O&M capabilities for the cloud platform to implement end-to-end monitoring of cloud services, including the monitoring of cloud service resources, tenant resources, and the compute, storage, and network infrastructure resources that the cloud services depend on. It collects and displays alarm information about the monitored objects, and provides reports, large screens, and advanced O&M data analysis capabilities based on these monitoring and alarm data.
- The figure shows some cloud services supported by HUAWEI CLOUD Stack 8.1.1. Different versions support different cloud services. This HCIP-Cloud Computing course focuses on IaaS (compute, storage, and network) services.
- Notably, new cloud services will be first rolled out on HUAWEI CLOUD for consumers. After a period of time, if enterprise customers (business customers) with a large base demand the cloud services, the services will be added to HUAWEI CLOUD Stack. Therefore, services on HUAWEI CLOUD are updated faster than those on HUAWEI CLOUD Stack.

HUAWEI CLOUD Stack Solution Application Scenario: Converged Resource Pool

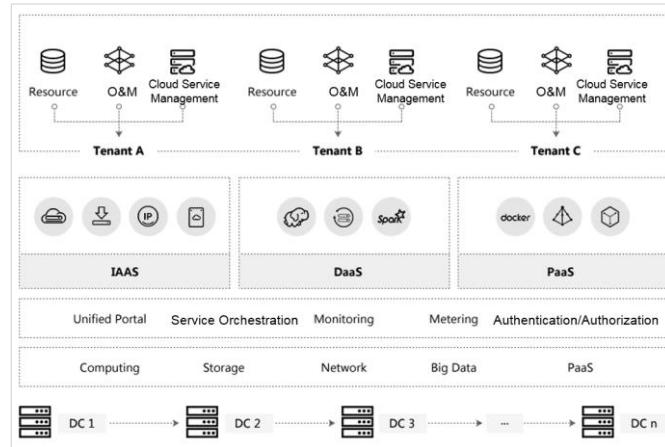


20 Huawei Confidential



- In the course of cloud transformation, most enterprises use converged resource pools. The figure on the left illustrates a typical architecture. The new cloud is seamlessly interconnected with the existing IT infrastructure. The customer's legacy VMware resource pools and other hardware are managed in a unified manner, allowing for unified provisioning, maintenance, and monitoring of resources and applications. In addition, a converged resource pool supports unified yet hierarchical and domain-based management. The architecture can be perfectly matched to the organizational structures of large organizations like enterprises and telecom carriers.

HUAWEI CLOUD Stack Solution Application Scenario: Hosting Cloud

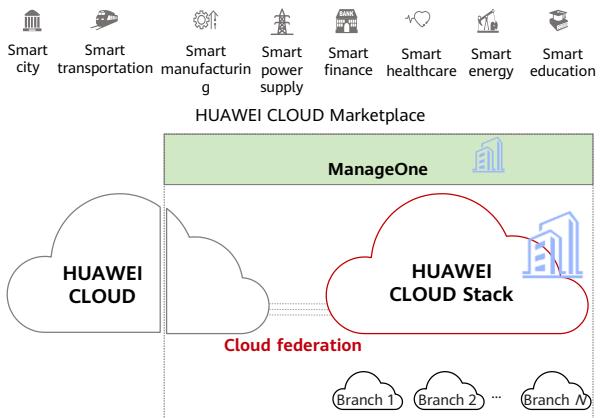


21 Huawei Confidential



- ISP: Internet Service Provider
- Leveraging advantages in network and local services, carriers, industry leaders, or ISPs can build a public cloud-like platform to provide full-stack cloud services and resources for government, enterprise, and industry customers in different industry scenarios, but without relying on a public network. The figure on the left shows the architecture.

HUAWEI CLOUD Stack Solution Application Scenario: Hybrid Cloud



- Hybrid cloud solutions include a management plane hybrid cloud and federated cloud.
 - Management plane hybrid cloud: ManageOne manages multiple public and private cloud environments through management APIs.
 - Federated cloud: HUAWEI CLOUD Stack has a brand-new hybrid cloud solution that uses a federated cloud architecture, where a private cloud and Huawei's public cloud are seamlessly connected and management is unified through IAM. A combination of federated authentication and individual user permissions settings ensures that the permissions for the private cloud and HUAWEI CLOUD accounts are kept consistent, allowing private cloud Virtual Data Center (VDC) users to access HUAWEI CLOUD Console and use HUAWEI CLOUD services.

22 Huawei Confidential

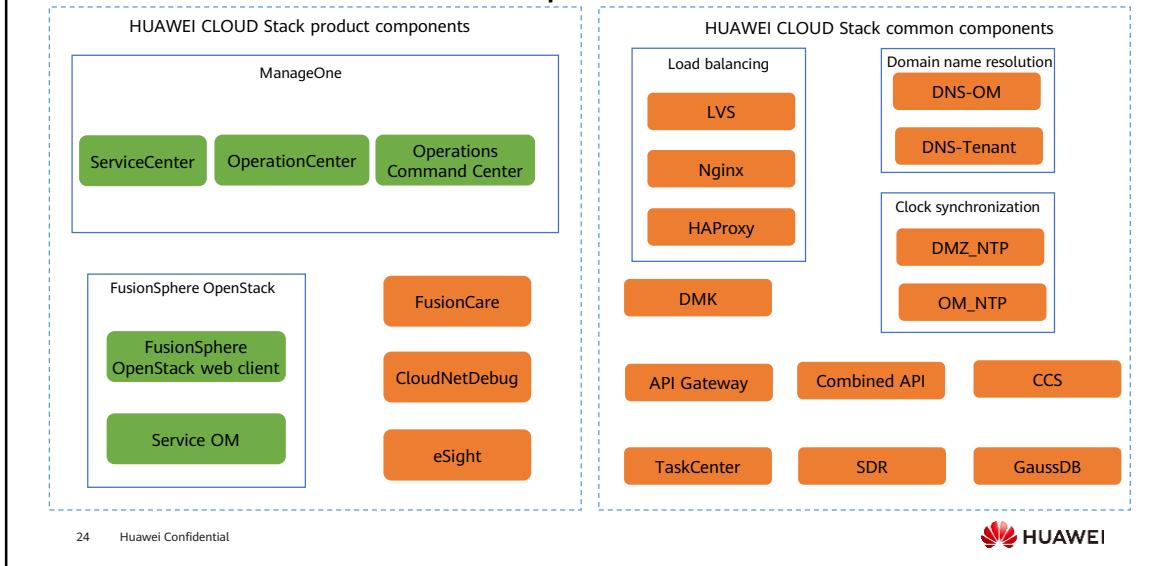


- Terms:
 - Identity & Access Management manages account information, role permission, access control, and logs.

Contents

1. HUAWEI CLOUD Stack Solution and Architecture
2. **HUAWEI CLOUD Stack Product Components and Common Components**

HUAWEI CLOUD Stack Components



- HUAWEI CLOUD Stack product components:
 - The Cloud Provisioning Service (CPS) is a component for providing the infrastructure virtualization function and used to deploy and upgrade the cloud platform at the IaaS layer.
 - Service OM is a management tool for resource pools (compute, storage, and network resources) and infrastructure cloud services (ECS, EVS, and VPC).
 - Portal of ServiceCenter: ManageOne Operation Portal
 - Portal of OperationCenter: ManageOne Maintenance Portal
 - Portal of Operations Command Center: ManageOne Operations Command Center
 - FusionCare: A tool specific to O&M personnel for unified health check and FusionSphere offline log collection.
 - CloudNetDebug: An O&M tool, which helps O&M personnel capture packets automatically.
 - eSight: It manages servers, storage devices, and network devices in a unified manner.

- HUAWEI CLOUD Stack common components:
 - Linux Virtual Server (LVS) is a Linux server cluster system that provides level-1 load balancing for hybrid cloud common services.
 - Nginx provides a reverse proxy for the cloud service console page to implement load balancing of services and data on each console node and distribute traffic. Cloud service requests are delivered by the LVS and forwarded to the Nginx. The Nginx forwards the cloud service requests to the cloud service console.
 - HAProxy balances cloud service workloads from the console node to the service node. Cloud service requests are sent from the console node to HAProxy. Then, HAProxy forwards the requests to the service nodes of the required cloud service.
 - Domain Name System (DNS) provides the domain name resolution service for cloud services, ManageOne, and tenant VMs.
 - Network Time Protocol (NTP) provides time synchronization for hybrid cloud services, ManageOne, and tenant VMs.
 - Deploy Management Kit (DMK) is a unified deployment and configuration platform on which all services can be installed and upgraded.
 - API Gateway provides API management as well as API intranet and extranet isolation functions. When a user accesses a cloud service API, the user does not call the service API directly, but accesses the API of the service registered on API Gateway. In this way, invalid requests are shielded, preventing the internal management API from being exposed.
 - Combined API provides backend services for Elastic Cloud Server (ECS), Elastic Volume Service (EVS), and Volume Backup Service (VBS). It serves as the server side of the console.
 - TaskCenter is used to view the creation of service instances such as ECSs.
 - Service Detail Record (SDR) provides metering and charging files of each cloud service.
 - Cloud Configuration Service (CCS) allows users to access third-party cloud resources based on the hybrid cloud, and provides capabilities of cross-cloud management and deployment.

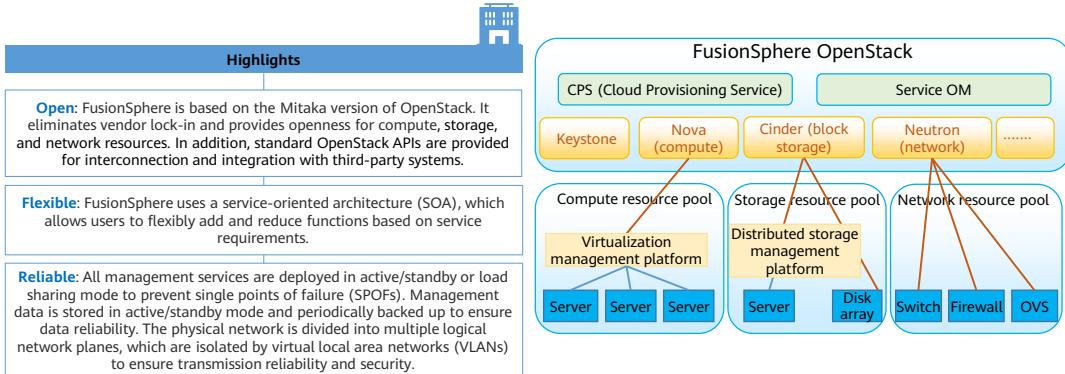
- GaussDB provides common databases for cloud services.

Contents

1. HUAWEI CLOUD Stack Solution and Architecture
2. **HUAWEI CLOUD Stack Product Components and Common Components**
 - Introduction to Product Components
 - Introduction to Common Components

FusionSphere OpenStack Introduction

- Huawei FusionSphere solution is a cloud operating system solution designed for customers in a wide range of industries. FusionSphere is based on the open OpenStack architecture and is designed for enterprise cloud computing data centers. It provides powerful virtualization functions and resource pool management capabilities, comprehensive cloud infrastructure components and tools, and open standard APIs, helping customers horizontally integrate physical and virtual resources of data centers and vertically optimize service platforms.



FusionSphere CPS Introduction

- The Cloud Provisioning Service (CPS) is a component for providing infrastructure virtualization. It is used to deploy and upgrade a cloud platform at the IaaS layer. From an external perspective, CPS is used to deploy, configure, and upgrade IaaS services.



Similar to the relationship between libvirt and Nova, software such as UVP and LVM provides single-node capabilities, and CPS provides cross-host software management and configuration after encapsulating the software.

- Terms:
 - Unified Virtualization Platform (UVP): Huawei's unified virtualization platform, which is a key technical platform for Huawei cloud-computing-based data center solutions. UVP is the combination of EulerOS and KVM.
 - Logical Volume Manager (LVM) provides high-level hard disk storage, enabling the system administrator to allocate storage space to applications and users more conveniently. Storage volumes under the LVM can be easily changed in size and removed as required. The administrator is allowed to manage storage volumes based on user groups and customize the names of storage volumes.

FusionSphere CPS Functions

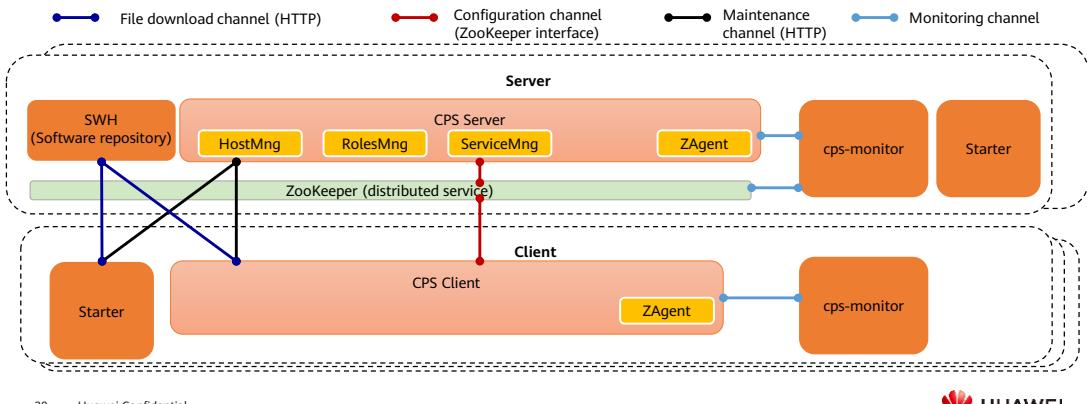
- CPS functions are classified into two types. One is closely related to underlying tools, and the other is more about orchestration and management.

Category	Function	Description
Hardware-related to the IaaS layer	OS Installation	You can use onboard PXE and iPXE tools to install hosts over the network, but PXE can be disabled to prevent hosts from being reinstalled using by mistake in otherwise stable scenarios.
	Kernel configuration	You can optimize the OS based on different service deployment and performance requirements. The kernel configuration can be adjusted on a host-by-host basis.
	Network management	You can configure the network plane, Neutron, and QoS, and bind NICs.
	Disk management	You can configure partitions based on roles. You can create, delete, and scale out partitions, and scale out, create, and delete system VGs. You can also switch partitions between VGs without service interruption.
	Resource isolation	You can configure resource groups, evenly distribute CPUs among NUMA nodes, bind virtual cores to different CPU cores, and bind CPU cores to NUMA nodes where the physical NICs of the CPU cores do not reside.
Software orchestration and management	Software installation	You can deploy, migrate, and query roles, as well as update (add or delete) component members in a role, and undeploy components.
	Software management	You can deploy and undeploy roles (component instances), add, delete, modify, and query roles (components), monitor components (components restart upon exceptions), check component status (component fault alarms report upon exceptions), and perform active/standby switchover. It also allows you to manage multi-NE host groups, including adding, deleting, and modifying host groups, and modifying component configurations in a host group.
	Software upgrade	CPS allows for unified upgrade orchestration of all managed software. You can specify the components to be upgraded and the batches in which the components are upgraded to ensure that services are not interrupted during the upgrade. With CPS, if an upgrade fails, you can roll back the system to the state before upgrade.
	Host management and maintenance	You can restart and power off hosts, dynamically change the passwords of the root and fsp users for hosts, and view host-related alarms, including host fault alarms, UVP-related alarms, and alarms about IaaS-layer CPU usage or memory usage exceeding the threshold. It allows you to manage certificates (such as changing the password of the fsp user or those of other OpenStack users, configuring the password expiration time, and disabling password-free login), and provides host tags for maintenance personnel to identify host information.

- Terms:
 - PXE: A technology that enables computers to boot from the network. This technology is the successor of Remote Initial Program Load (RPL). The PXE works in client/server mode. The PXE client resides in the ROM of a network card. When the computer boots up, the BIOS invokes the PXE client to the memory. The PXE client obtains an IP address from the DHCP server and downloads the operating system from the remote server through TFTP.
 - Quality of Service (QoS): A commonly-used performance indicator of a telecommunication system or channel. Depending on the specific system and service, it may relate to jitter, delay, packet loss ratio, bit error ratio, and signal-to-noise ratio. It functions to measure the quality of the transmission system and the effectiveness of the services, as well as the capability of a service provider to meet the demands of users.
 - Non-Uniform Memory Access (NUMA) is a computer architecture that enables memory to be shared by multiple processors. In NUMA mode, a processor is divided into multiple nodes, and each node is allocated with local storage space. The processors of all nodes can access all physical memories, but the time required for accessing the memory on the local node is much shorter than that on a remote node.

FusionSphere CPS Deployment

- CPS uses a client/server (C/S) architecture. The CPS Server component is deployed on controller nodes in active/standby mode (one active and two standby nodes) to receive messages from the FusionSphere OpenStack web client or CLI.
- The CPS Client component is deployed on all nodes that function as active nodes. It receives messages from the CPS Server and makes the messages take effect on the nodes.



- A FusionSphere OpenStack cluster contains three controller nodes deployed in load balancing mode. However, the CPS Server components are deployed on these nodes as one active node and two standby nodes.
- In HUAWEI CLOUD Stack, controller nodes and management nodes must be differentiated.
 - If a customer has only FusionSphere OpenStack deployed, controller nodes (three nodes in typical configuration) are used as management nodes.
 - If a customer has a set of HUAWEI CLOUD Stack deployed, the system requires controller nodes as basic management nodes (three in typical configuration) and cloud service management nodes (planned based on the number of installed cloud services).
- FusionSphere CPS architecture is described as follows:
 - Starter:** It is packed with the host OS and is responsible for loading the host OS configuration and loading and starting other modules of the CPS Client.
 - cps-monitor (local monitoring service):** It provides the monitoring function for locally deployed services. If the service heartbeat is lost, cps-monitor restarts the service.

- Distribute Service (DS): It provides the configuration, naming, and distributed lock (using ZooKeeper) for the CPS system.
- Software House (SWH): It manages software packages.
- CPS Server: It manages hosts and service deployment.
- CPS Client: It collects and reports host information (capabilities and deployment service information), is used to deploy local services, and provides distributed consistency data services for local deployment services.

FusionSphere CPS Console

- The CPS login address can be obtained from the table exported using HUAWEI CLOUD Stack Deploy during the installation. If CPS has too many permissions granted, random parameter changes can create problems for upper-layer services. This is why the CPS system has only one admin account by default, and only one user can log in to the CPS system at a time. After HUAWEI CLOUD Stack is installed, SSO is automatically configured. You can use the O&M center account to log in to CPS. If SSO is manually disabled, you can use the admin password of CPS to log in to CPS.

Host ID	Host Name	IP Address	OM IP	BMC IP	Node Type	CPU Type	Status	Tag	OS Version	Progress
7984ED33-2594-808D-E	Controller01	172.28.0.3	10.200.1...	10.154.8...	Controller	x86_64	normal		UVP KVM	<div style="width: 100%;">100%</div>
5784ED33-2594-008A-E	Controller02	172.28.0.4	10.200.1...	10.154.8...	Controller	x86_64	normal		UVP KVM	<div style="width: 100%;">100%</div>
8D84ED33-2594-7C81-E	Controller08	172.28.0.9	10.200.1...	10.154.8...	Compute	x86_64	normal		UVP KVM	<div style="width: 100%;">100%</div>
8994ED33-2594-518E-E	Controller01	172.28.0.2	10.200.1...	10.154.8...	Controller	x86_64	normal		UVP KVM	<div style="width: 100%;">100%</div>
4F5C1409-E26B-F240-E	Compute06	172.28.0.6	10.200.1...	10.154.8...	Compute	x86_64	normal		UVP KVM	<div style="width: 100%;">100%</div>
69003409-E26B-538E-E	Compute09	172.28.0...	10.200.1...	10.154.8...	Compute	x86_64	normal		UVP KVM	<div style="width: 100%;">100%</div>
15E3548A-1690-2C82-E	Compute08	172.28.0...	10.200.1...	10.154.8...	Compute	x86_64	normal		UVP KVM	<div style="width: 100%;">100%</div>
CCT86789-B23B-044D-E	CCT978B-B23B-044D-E	172.28.0...	10.200.1...	10.154.8...	Compute	x86_64	normal		UVP KVM	<div style="width: 100%;">100%</div>
578E8C1E-881C-A845-E	578E8C1E-881C-A845-E	172.28.0.9	10.200.1...	10.154.8...	Compute	x86_64	normal		UVP KVM	<div style="width: 100%;">100%</div>
800E0D2D-DC48-E588-E	MRS1_03	172.28.0...	10.200.17.8	10.154.8...	Compute	x86_64	normal		UVP KVM	<div style="width: 100%;">100%</div>

Total Records: 47 | 1 2 3 4 5 >

Details | Delete | Tag Management

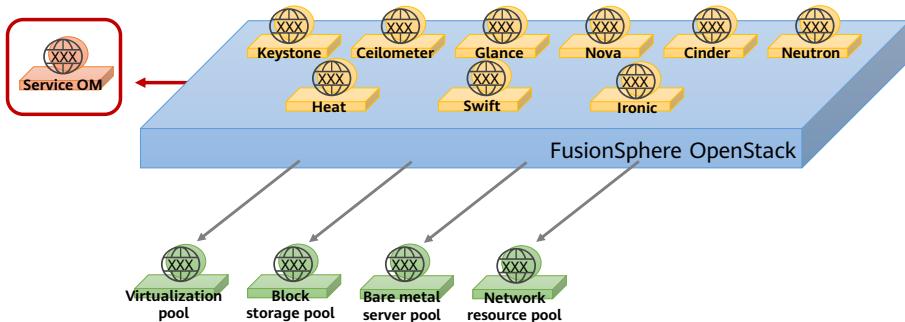
32 Huawei Confidential



- HUAWEI CLOUD Stack Deploy (HCSD) is an automatic installation platform of HUAWEI CLOUD Stack. It allows engineers to install the OS, platform components, common components, and cloud services in HUAWEI CLOUD Stack in one-click mode.

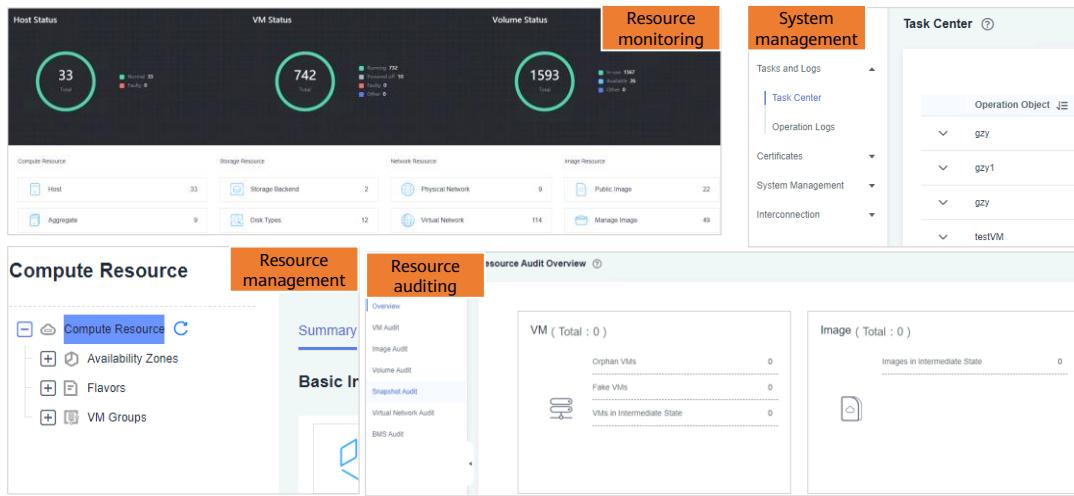
Service OM Overview

- Administrators use Service OM to manage, control, and configure compute, storage, and network resource pools and infrastructure cloud services (such as ECS, EVS, and VPC).



- Service OM is a resource management tool in FusionSphere OpenStack. Administrators can log in to Service OM to manage the FusionSphere OpenStack resource pools.
- FusionSphere OpenStack does not have the Horizon component. Instead, Service OM provides dashboards.

Service OM Function Classification



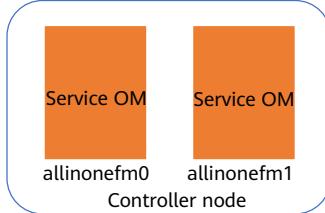
34 Huawei Confidential



- Service OM provides the following functions:
 - Resource monitoring: It monitors the status of hosts, VMs, and disks, and records the number of resources (compute, storage, network, and image resources) in a resource pool.
 - Resource management: It manages infrastructure resources (including compute, storage, network, image, and BMS resources), such as creating, deleting, and modifying resources. If gPaaS and AI DaaS services are available at a site, you can manage gPaaS and AI DaaS services. gPaaS and AI DaaS services are not involved in this course.
 - Resource auditing: On the FusionSphere OpenStack cloud platform, a service failure occurs and the system reports an alarm if problems such as residual resources and unavailable resources occur because of unplanned system failures (such as host reboot and process restart), or backup recovery. To improve maintenance efficiency, FusionSphere collects audit items related to frequently reported alarms. You can view and handle audit items on Service OM to ensure normal service running. Resources that can be audited include VMs, images, volumes, snapshots, virtual networks, and BMSs.
 - System management: includes tasks and logs, users and certificates, system management, and interconnection.

Service OM Deployment

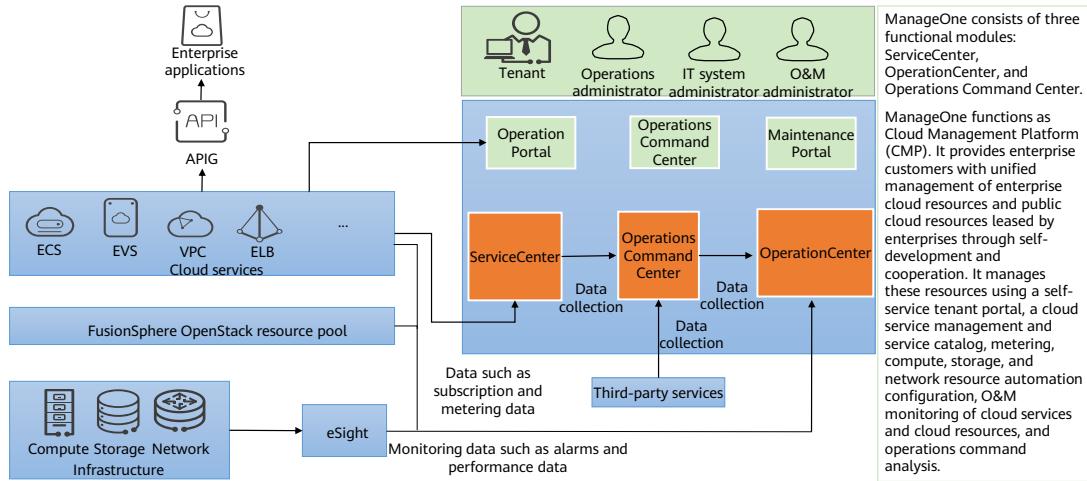
- During automated software installation using HUAWEI CLOUD Stack Deploy, HUAWEI CLOUD Stack Deploy invokes the CPS to create VMs allinonefm0 and allinonefm1 and deploys them as an active/standby pair. The VMs run on the controller node.



Name	Host ID	Host Group	Availability Z...	Status	Power Status	Flavor	CPU Archite...	IP Address	Batch Cold ...	Batch Live...	Operation
allinonefm1	8F84ED33-25...	manage-aggr	manage-az	Running	Running	6vCPUs 14GB	X86/Intel	10.200.16.24...	Supported	Supported	VNC Login More ▾
allinonefm0	6C84ED33-2...	manage-aggr	manage-az	Running	Running	6vCPUs 14GB	X86/Intel	10.200.16.24...	Supported	Supported	VNC Login More ▾

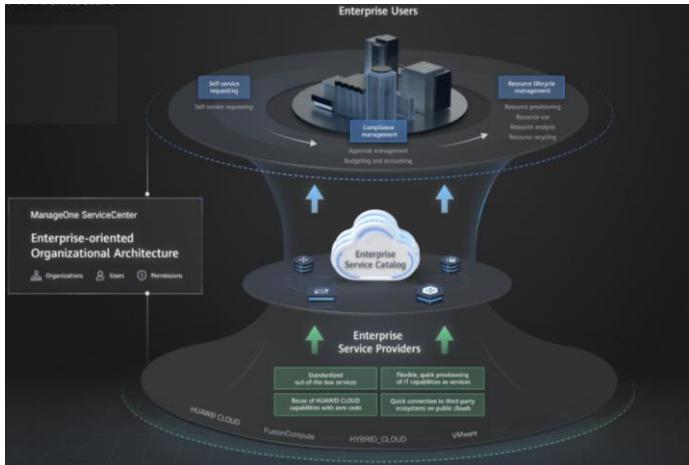
- FusionSphere OpenStack OM and Service OM are the same product used in different scenarios. In HUAWEI CLOUD Stack, Service OM is used. In the telecom cloud NFV architecture, FusionSphere OpenStack OM is used. However, Service OM is identified as FusionSphere OpenStack OM on the CPS page.
- For details about the login scheme, see *HUAWEI CLOUD Stack 8.X Account List*.

ManageOne Solution Overview



- Cloud Management Platform (CMP): In HUAWEI CLOUD Stack, only ManageOne can be regarded as the CMP.
- ManageOne is a larger cloud platform than FusionSphere OpenStack. FusionSphere OpenStack can manage only compute, storage, and network resource pools, but cannot manage some resource pools such as containers and databases. Therefore, FusionSphere OpenStack cannot meet the requirements of CMP.

Introduction to ManageOne ServiceCenter



ServiceCenter is a ManageOne portal for tenants and operation management. It provides cloud service operations integration and integrates multiple cloud services into ManageOne. Console Home integrates various cloud service consoles to provide a unified portal for users to access cloud services. Service orchestration enables cloud service capabilities to be orchestrated into cloud services that can be applied for by users and displays them in the service catalog.

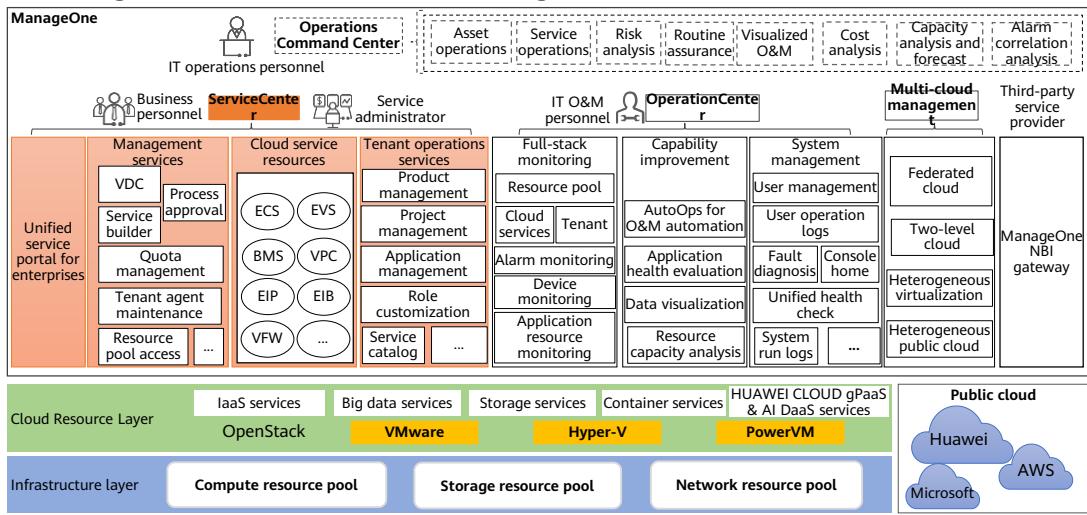
ServiceCenter reconstructs enterprise IT architecture, redefining IT operations, transforming enterprise IT services from passive services to active services and providing self-service access for users.

The reform on the service supply side frees IT administrators from complex and repeated configuration work and enables them to focus on providing efficient and high-quality services for businesses.

ServiceCenter helps you establish a complete operations process for service consumption. Business personnel can quickly subscribe to cloud services on the portal of ServiceCenter, making service subscriptions much easier.



ManageOne ServiceCenter Logical Architecture



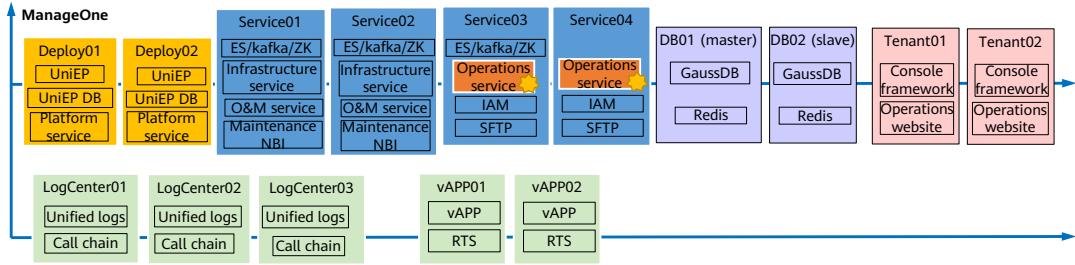
38 Huawei Confidential



- You only need to pay attention to the ManageOne ServiceCenter. ManageOne ServiceCenter is used for cloud service resource (such as ECSs and EVSs) management, tenant operations (such as metering and charging and project management), and operations management (such as process approval and quota management). It provides services for business personnel and service administrators through a unified portal.
- For details about operations, see *HUAWEI CLOUD Stack ManageOne ServiceCenter Introduction* in this course.

ManageOne ServiceCenter: Component Deployment Logical Diagram

Component	Node	VMs	Mandatory/Optional	Remarks
ManageOne	ManageOne-Deploy01~02	2	Mandatory	Nodes where the deployment system and basic platform services are co-deployed. The log partition is 15 GB and the opt partition is 55 GB.
	ManageOne-Service01~04	4	Mandatory	Service cluster nodes, including operations and maintenance nodes
	ManageOne-DB01~02	2	Mandatory	Database nodes, including databases of operations, maintenance, IAM, and unified log services
	ManageOne-Tenant01~02	2	Mandatory	Tenant console nodes, where the tenant portal is deployed
	ManageOne-LogCenter01~03	3	Optional	Unified log components, which are mandatory in private cloud scenarios
	ManageOne-vAPP01~02	2	Optional	Service builder component, which is used for resource combination and orchestration



39 Huawei Confidential



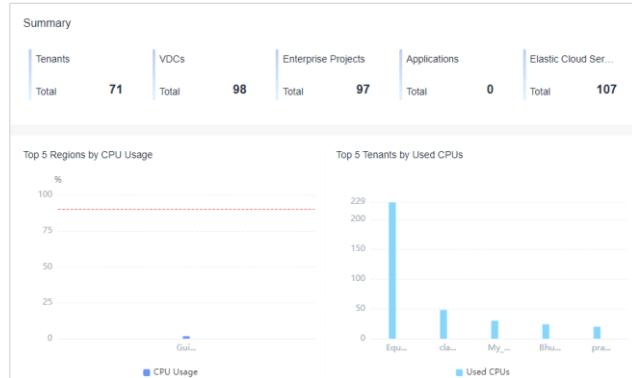
- To deploy the ManageOne platform, 15 management VMs need to be created (automatically created by HUAWEI CLOUD Stack Deploy) in the FusionSphere OpenStack resource pool. Among the 15 management VMs, 10 are mandatory and 5 are optional. For details, see the table on the slide.
 - ManageOne-Deploy01 and ManageOne-Deploy02 are deployed as deployment nodes in active/standby mode. They provide basic capabilities such as management, upgrades, and backup of service nodes.
 - ManageOne-Service01 and ManageOne-Service02 are deployed as O&M nodes in active/standby mode. Related services are deployed on these nodes. These nodes provide basic ManageOne service functions such as alarm and capacity functions.
 - ManageOne-Service03 and ManageOne-Service04 are deployed as operations nodes in active/standby mode. Basic services of ManageOne Operation Portal are deployed on these nodes. These nodes provide functions such as organization management, quota management, and metering management.
 - ManageOne-DB01 and ManageOne-DB02 are deployed as database nodes in active/standby mode. Database services are deployed on the nodes to

provide basic database functions.

- ManageOne-Tenant01 and ManageOne-Tenant02 are deployed as ManageOne tenant nodes in active/active mode. They provide services related to ManageOne Operation Portal.
- ManageOne-LogCenter01 to ManageOne-LogCenter03 are deployed as log center nodes in active/active mode. Log-related services are deployed on these nodes to provide the log center function. The number of log center nodes varies depending on the deployment scale and the number of regions. There may be zero or multiple log center nodes.
- ManageOne-vAPP01 and ManageOne-vAPP02 are deployed as application management nodes in active/standby mode. These nodes can provision resources based on applications.
- ServiceCenter is installed on the ManageOne-Service03 and ManageOne-Service04 management VMs.

ManageOne ServiceCenter Login Portal

- You can obtain the login address of ServiceCenter from the table exported using the automated installation tool HUAWEI CLOUD Stack Deploy during the installation. By default, the system creates the **bss_admin** account. The administrator can log in to the system as the **bss_admin** user to create other operations administrator accounts or create a VDC administrator.
- The ServiceCenter homepage is different depending on whether a user logs in to the ServiceCenter as an operations administrator or a VDC administrator.



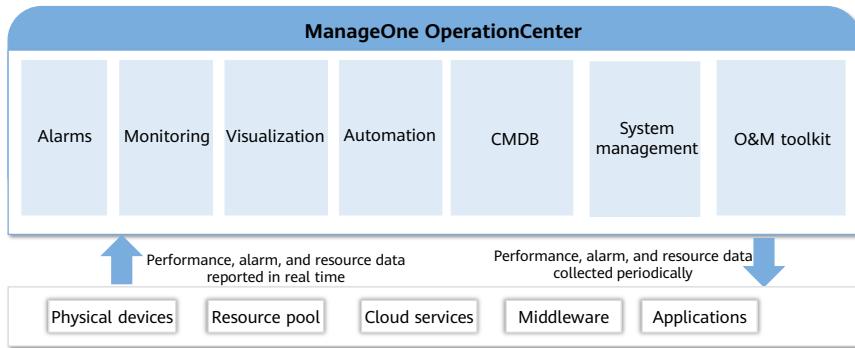
41 Huawei Confidential



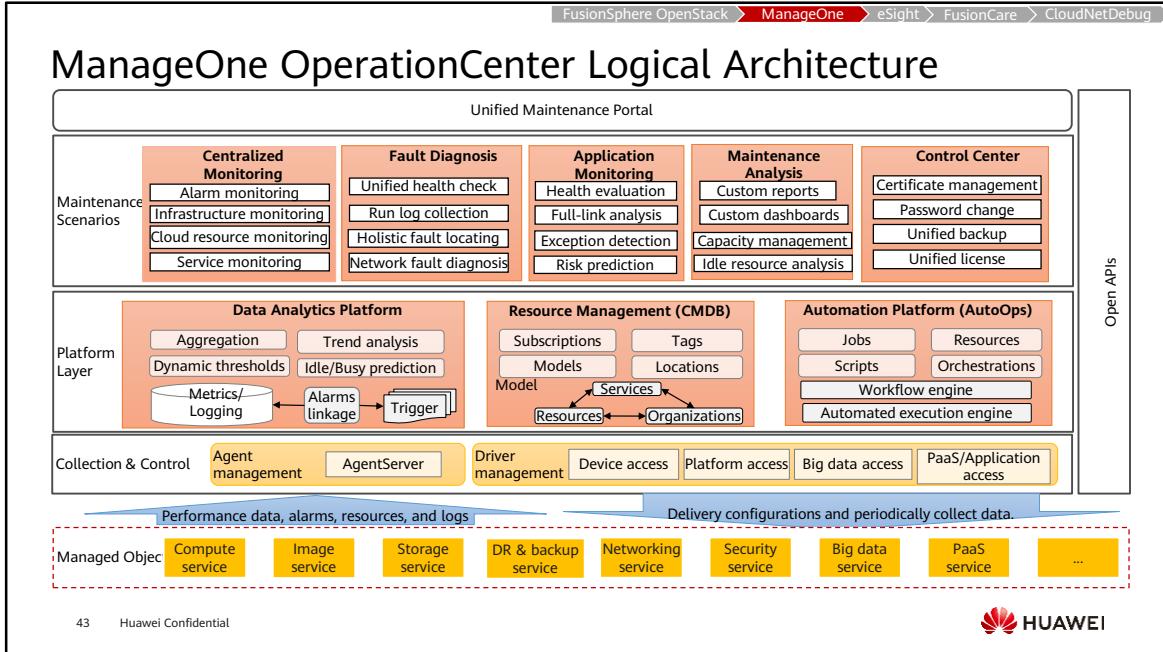
- For details about operations roles, see *HUAWEI CLOUD Stack Operations* in this course.
- The operation administrator page displays the global resource usage, and the VDC administrator page displays the resource usage in the VDC.

Introduction to ManageOne OperationCenter

- OperationCenter is the only portal for ManageOne O&M management. It provides cloud service O&M management and end-to-end monitoring for cloud services. It also monitors cloud services, tenant resources, and infrastructure (compute, storage, and network) that the cloud services depend on. It collects and displays alarm information about the monitored objects, and provides reports, large screens, and advanced O&M data analysis capabilities based on these monitoring and alarm data. In addition, ManageOne OperationCenter integrates cloud service O&M systems for unified O&M.



- For details about O&M, see *HUAWEI CLOUD Stack O&M*. You need to have a general understanding of the functions of OperationCenter in this course.

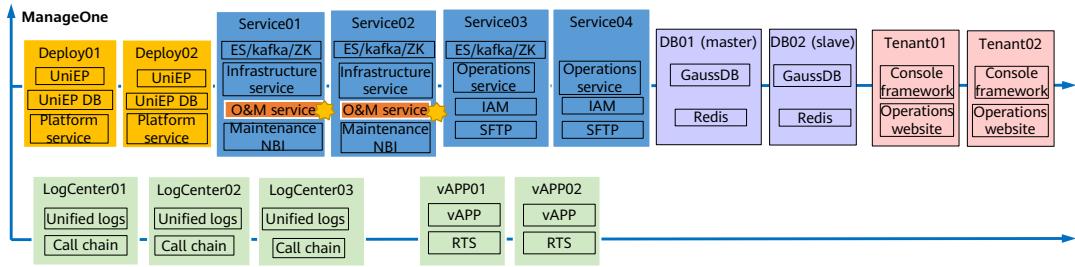


- ManageOne OperationCenter, a centralized O&M platform, uses the distributed software architecture of mainstream microservices in the industry and is designed for different O&M scenarios. OperationCenter is a one-stop automated O&M tool that provides a unified portal for users to monitor, manage, and control resources in the data center.
- Based on the hierarchical decoupling architecture, ManageOne OperationCenter is classified into the following parts:
 - Collection & Control: ManageOne can obtain massive volumes of data of full-stack devices through Agent and driver interconnection.
 - Platform layer: The CMDB, data analytics platform, and automated O&M platform form the O&M foundation. The three platforms accumulate O&M data and provide open O&M capabilities.
 - Maintenance scenarios: Focusing on customer values and business scenarios, ManageOne builds one-stop, scenario-based maintenance capabilities that cover monitoring, management, and control to match customer maintenance organizations.
 - Open APIs: ManageOne offers standard data access capabilities and provides maintenance data for third parties through northbound APIs.
- For details about the logical O&M architecture, see *HUAWEI CLOUD Stack*

ManageOne OperationCenter Introduction in this course.

ManageOne OperationCenter: Component Deployment Logical Diagram

Component	Node	VMs	Mandatory/Optional	Remarks
ManageOne	ManageOne-Deploy01~02	2	Mandatory	Nodes where the deployment system and basic platform services are co-deployed. The log partition is 15 GB and the opt partition is 55 GB.
	ManageOne-Service01~04	4	Mandatory	Service cluster nodes, including operations and maintenance nodes
	ManageOne-DB01~02	2	Mandatory	Database nodes, including databases of operations, maintenance, IAM, and unified log services
	ManageOne-Tenant01~02	2	Mandatory	Tenant console nodes, where the tenant portal is deployed
	ManageOne-LogCenter01~03	3	Optional	Unified log components, which are mandatory in private cloud scenarios
	ManageOne-vAPP01~02	2	Optional	Service builder component, which is used for resource combination and orchestration



44 Huawei Confidential



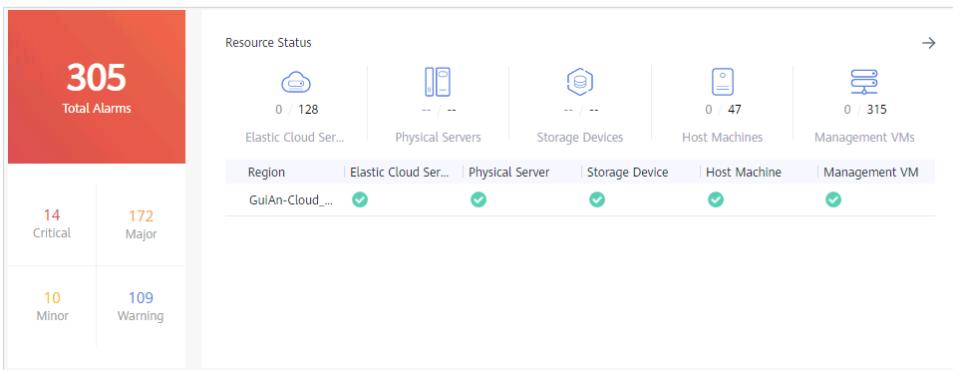
- To deploy the ManageOne platform, 15 management VMs need to be created (automatically created by HUAWEI CLOUD Stack Deploy) in the FusionSphere OpenStack resource pool. Among the 15 management VMs, 10 are mandatory and 5 are optional. For details, see the table on the slide.
 - ManageOne-Deploy01 and ManageOne-Deploy02 are deployed in active/standby mode. They provide basic capabilities such as management, upgrades, and backup of service nodes.
 - ManageOne-Service01 and ManageOne-Service02 are deployed as O&M nodes in active/standby mode. Related services are deployed on these nodes. These nodes provide basic ManageOne service functions such as alarm and capacity functions.
 - ManageOne-Service03 and ManageOne-Service04 are deployed as operations nodes in active/standby mode. Basic services of ManageOne Operation Portal are deployed on these nodes. These nodes provide functions such as organization management, quota management, and metering management.
 - ManageOne-DB01 and ManageOne-DB02 are deployed as database nodes in active/standby mode. Database services are deployed on the nodes to

provide basic database functions.

- ManageOne-Tenant01 and ManageOne-Tenant02 are deployed as ManageOne tenant nodes in active/active mode. They provide services related to ManageOne Operation Portal.
- ManageOne-LogCenter01 to ManageOne-LogCenter03 are deployed as log center nodes in active/active mode. Log-related services are deployed on these nodes to provide the log center function. The number of log center nodes varies depending on the deployment scale and the number of regions. There may be zero or multiple log center nodes.
- ManageOne-vAPP01 and ManageOne-vAPP02 are deployed as application management nodes in active/standby mode. These nodes can provision resources based on applications.
- Components related to OperationCenter are installed on ManageOne-Service01 and ManageOne-Service02 management VMs.

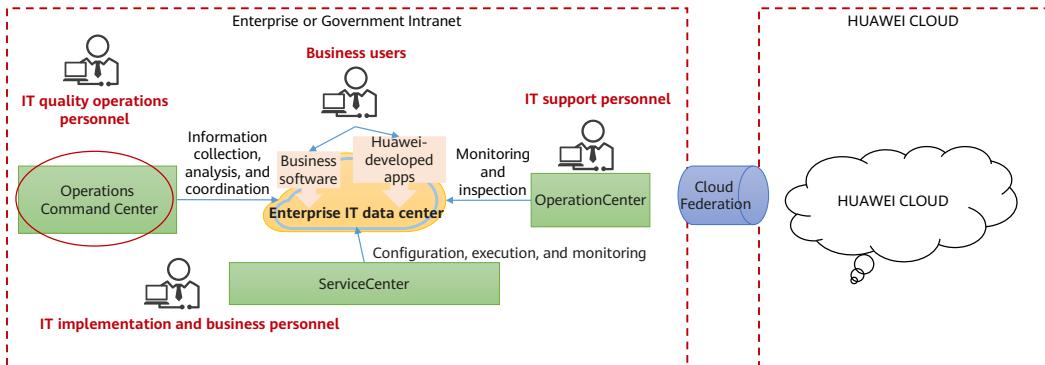
ManageOne OperationCenter Login Portal

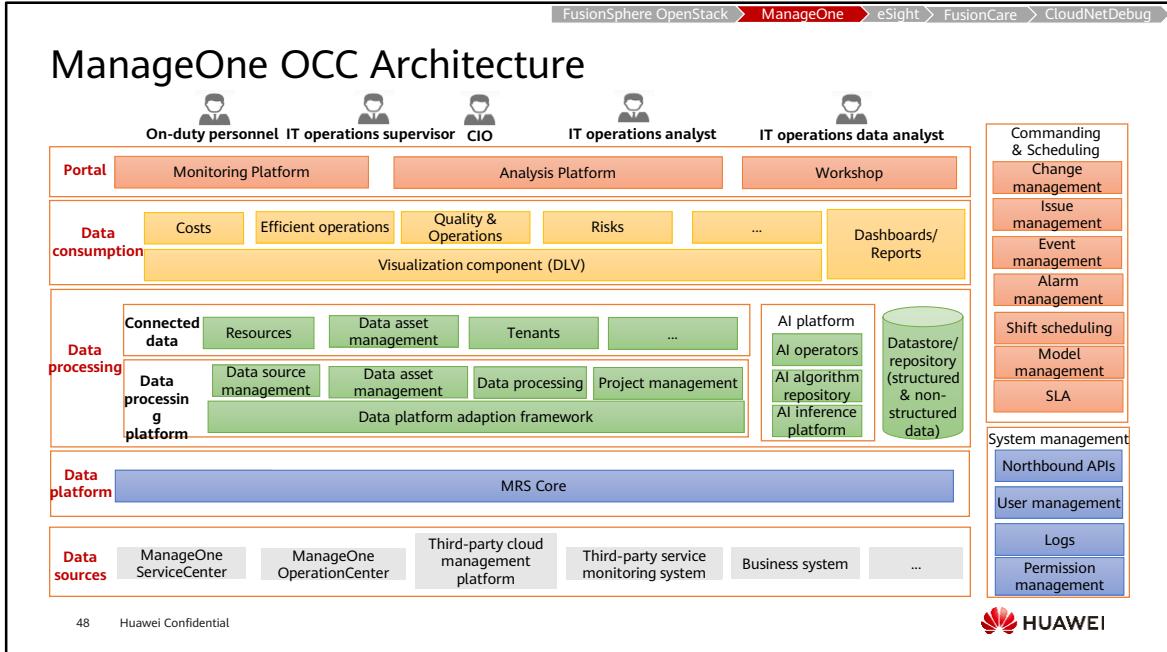
- You can obtain the login address of ManageOne OperationCenter from the table exported using HUAWEI CLOUD Stack Deploy during the installation. By default, the system creates the admin account. The administrator can log in to the system as the admin user to create other administrator accounts. After HUAWEI CLOUD Stack is installed, SSO is automatically configured. You can use a ManageOne OperationCenter account to log in to CPS, Service OM, FusionCare, and CloudNetDebug.



Introduction to ManageOne Operations Command Center

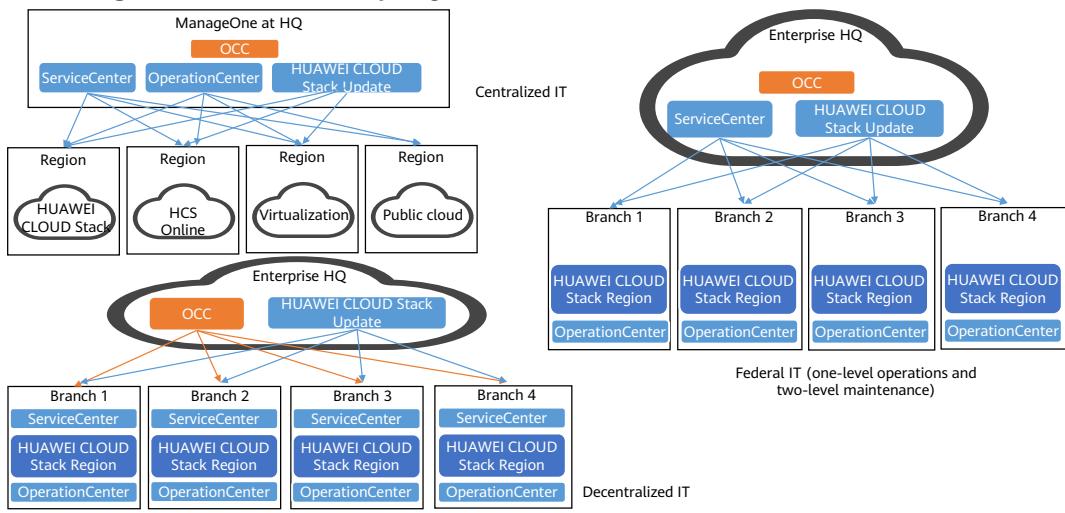
- Operations Command Center (OCC) is the brain of HUAWEI CLOUD Stack. It offers real-time data insights, collaborative command and control, and intelligent operations to help governments and enterprises slash operational costs, improve efficiency, boost operational quality, control risks, guarantee compliance, and make data-driven decisions.





- **Data sources:** OCC data can come from ServiceCenter, OperationCenter, business systems, third-party cloud platforms, and service business systems. The collected data is transmitted to the data platform layer.
- **Data platform:** The data platform collects data from different data sources and stores the data in HDFS or OBS buckets. The big data service MapReduce (MRS), is used as the underlying data platform. Users are unaware of MRS when accessing the OCC page.
- **Data processing:** Data stored in MRS needs to be processed before being used. Some AI algorithms are used to process data.
- **Data consumption:** The processed data is transferred to the data consumption layer. To facilitate data usage, this layer uses the visualized component (DLV) for better data consumption or enables data to be displayed on large screens or reports.
- **Portal:** Currently, OCC consists of the Monitoring and Analysis platforms as well as Workshop. The Command platform is in the planning phase. For details about the platforms, see the following content.

ManageOne OCC Deployment Scenarios

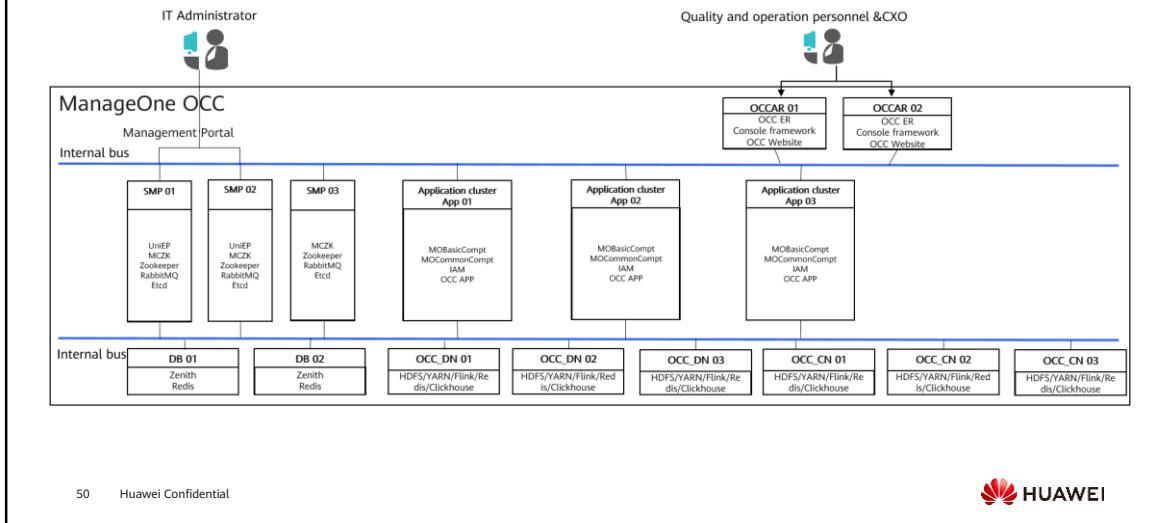


49 Huawei Confidential



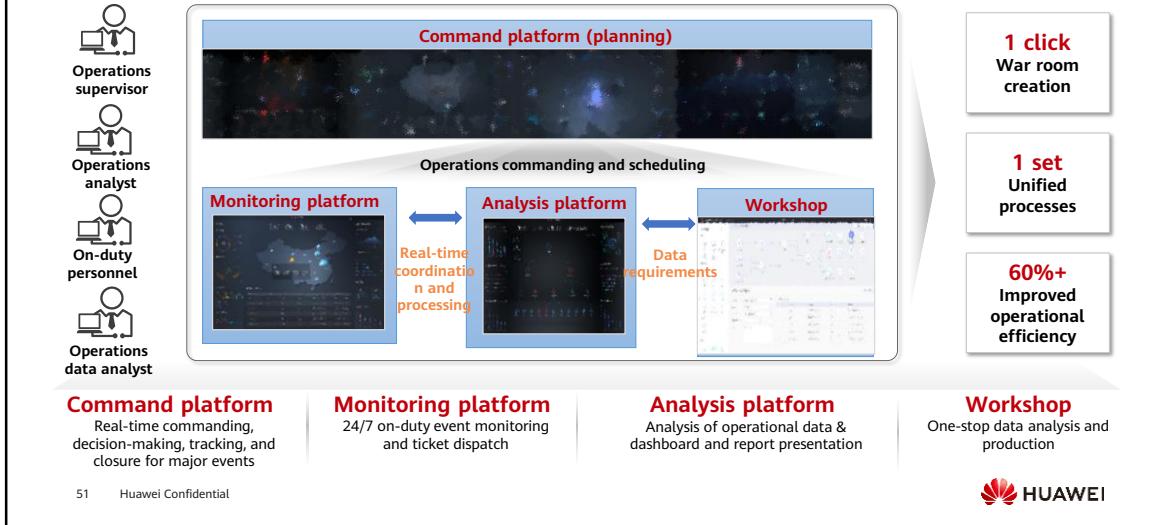
- **Centralized IT:** ManageOne ServiceCenter, OperationCenter, and OCC, as well as HUAWEI CLOUD Stack Update are deployed in the enterprise HQ. The enterprise HQ performs O&M operations for branches in a unified manner. No component of ManageOne is deployed in each region of branches. The resource pools are connected to the ManageOne ServiceCenter and OperationCenter of the enterprise HQ for management and control. The enterprise HQ can upgrade components in each region using HUAWEI CLOUD Stack Update.
- **Decentralized IT:** ManageOne OCC and HUAWEI CLOUD Stack Update are deployed in the enterprise HQ. ServiceCenter and OperationCenter are deployed in branches. Branches perform their own O&M operations, and the enterprise HQ performs the unified operations command. The enterprise HQ can upgrade components in each region using HUAWEI CLOUD Stack Update.
- **Federal IT:** ManageOne ServiceCenter, OCC, and HUAWEI CLOUD Stack Update are deployed in the enterprise HQ. OperationCenter is deployed in branches. Branches perform their own maintenance operations, and the enterprise HQ performs the unified operations management. The enterprise HQ can upgrade components in each region using HUAWEI CLOUD Stack Update.

ManageOne OCC Deployment Architecture



- At least 16 management VMs are required for OCC deployment. The nodes are described as follows:
 - ManageOne-MRSDN01 to ManageOne-MRSDN03 are MRS data nodes deployed in cluster mode. At least three nodes are deployed for scale-out.
 - ManageOne-MRSCN01 to ManageOne-MRSCN03 are MRS controller nodes deployed in cluster mode. At least three nodes are deployed for scale-out.
 - ManageOne-OCCDB01 to ManageOne-OCCDB02 are OCC database nodes deployed in active/standby mode. The nodes are not shared with OperationCenter and ServiceCenter databases.
 - ManageOne-OCCAPP01 to ManageOne-OCCAPP03 are OCC application nodes deployed in cluster mode. At least three nodes are deployed for scale-out.
 - OCCAR01 to OCCAR02 are OCC Portal nodes deployed in active/standby mode. The nodes provide web services for quality operations personnel and CXOs.
 - SMP01 to SMP03 are deployed in load balancing mode. The deployment portal components of the CloudScope platform (O&M platform for gPaaS & AI DaaS services, not involved in this course) deployed on the nodes are responsible for governance of microservices of OCC components.

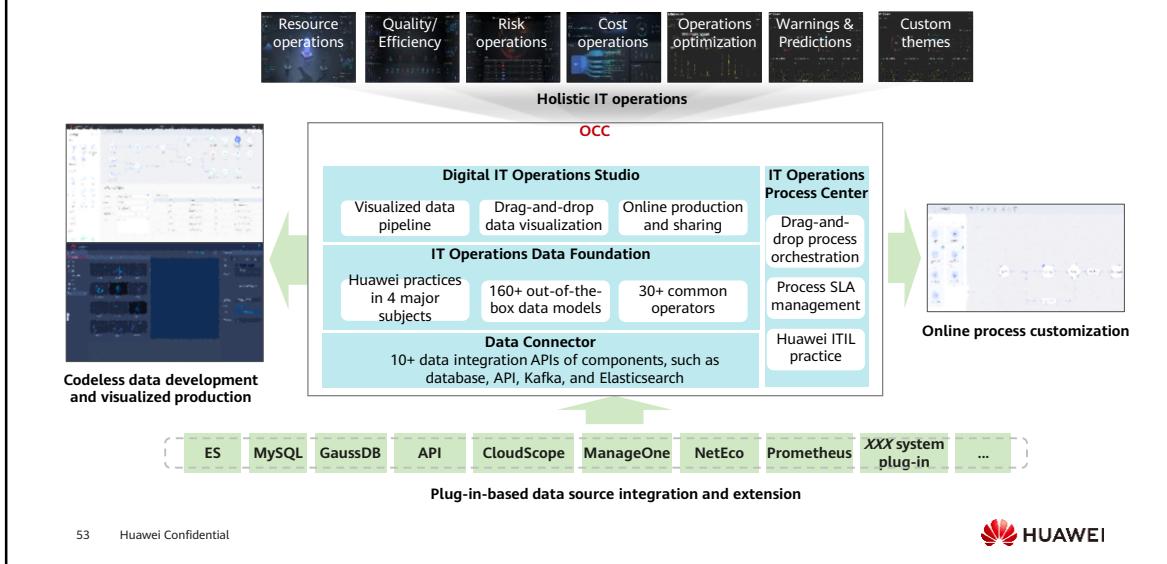
Seamless Coordination Between Four Platforms to Drive Digital Operations



- Monitoring platform:
 - This platform displays and monitors data center running status on the comprehensive data center dashboard, resource dashboard, quality dashboard, and application topology dashboard.
 - It allows you to perform routine scheduling, dispatch tickets, make shift schedules, hand over shift tasks, and view operation logs.
- Command platform:
 - This platform demarcates and locates faults and traces tasks based on the data center topology and application topology.
 - It allows the operations team to cooperate well to cope with major faults and emergencies and provides suggestions for decision-making to implement unified scheduling and commanding.

- Analysis platform:
 - This platform streamlines full-stack data, provides suggestions on resource optimization and energy efficiency analysis in all domains based on AI data models, and predicts resource trends by application and data center.
 - It also provides business operations reports in resources, services, and costs.
- Workshop:
 - Workshop provides a data processing platform which allows you to prepare data services based on a given procedure.

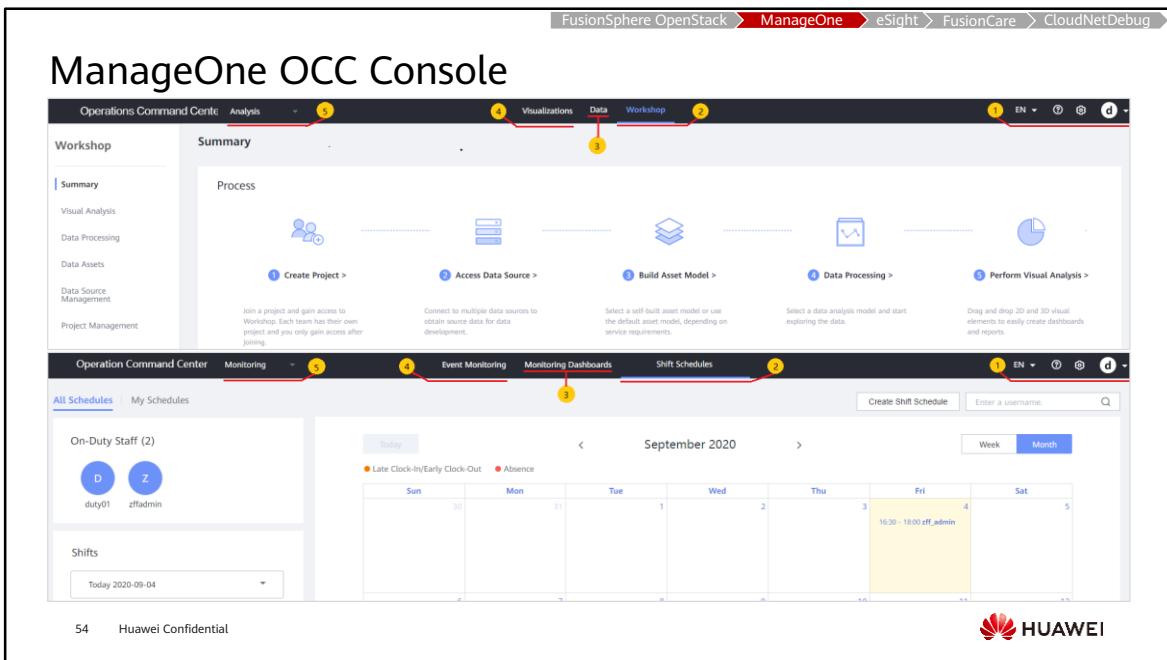
OCC Open Ecosystem Extended Architecture



53 Huawei Confidential



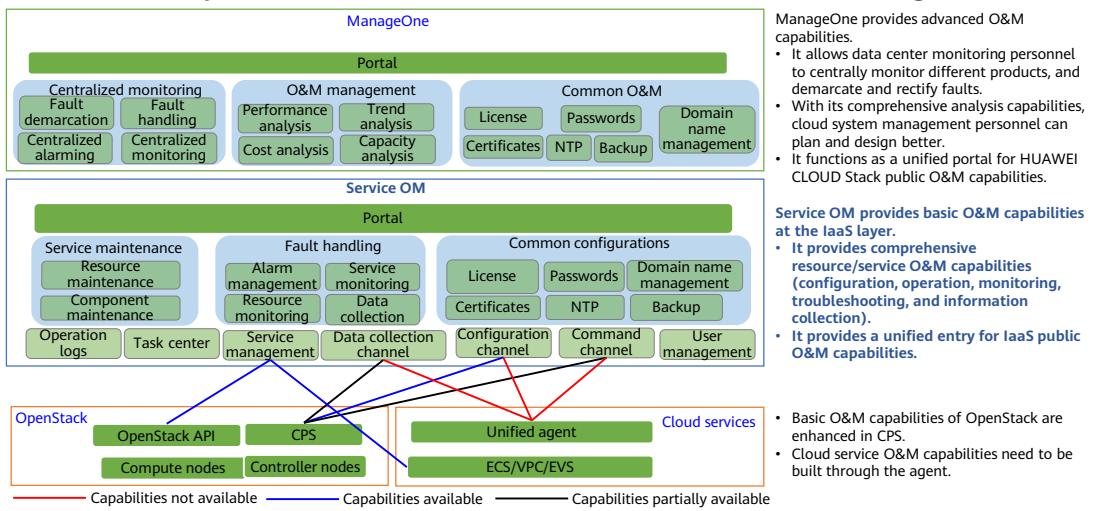
- OCC drives holistic IT operations, including the operations of resources, risks, costs. In addition, plug-in-based data source integration and extension are supported in the southbound. Data can be obtained not only from ServiceCenter and OperationCenter, but also from third-party products such as ElasticSearch, databases, and Prometheus.
- In OCC, **codeless data development and visualized production can be performed. It allows partners to customize their own operations analysis reports and dashboards in drag-and-drop mode.**



- Analysis platform GUI description:
 - No. 1: Language switch button, help center/product version query, configuration management (creating users, setting security policies, and viewing operation logs), and information about the current login user from left to right.
 - No. 2: Production functions (**Summary, Project Management, Data Source Management, Data Assets, Data Service Mall, Data Processing, and Visual Analysis**)
 - No. 3: Data functions. On this page, you can:
 - Subscribe to secret or top secret data assets created by other users.
 - View public data assets published by other users.
 - View all data assets in the project that the current logged-in account belongs to.
 - No. 4: Visualization functions. On this page, you can:
 - Subscribe to secret or top secret dashboards and reports published by other users.
 - View public dashboards or reports published by other users.
 - View all published dashboards and reports in the project that the current logged-in account belongs to.
 - No. 5: Platform switch button, which can be used to redirect to the monitoring platform.

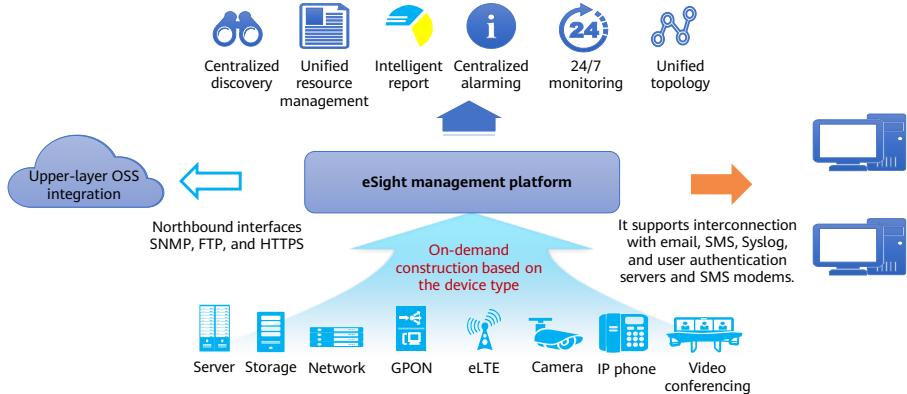
- Monitoring platform GUI description:
 - No. 1: Language switch button, help center/product version query, configuration management (creating users, setting security policies, and viewing operation logs), and information about the current login user from left to right.
 - No. 2: Shift schedules. On this page, you can set shift time and shift transfer times for staff members to properly manage your workforce and improve operations efficiency.
 - No. 3: Dashboard monitoring function. You can subscribe to diverse dashboards containing comprehensive O&M data to stay informed of resource status, quickly identify idle resources, and scale resources in a timely manner.
 - No. 4: Event monitoring function, which receives and displays alarm information reported by local ManageOne Maintenance Portal in real time.
 - No. 5: Platform switch button, which can be used to redirect to the analysis platform.

Relationships Between CPS, Service OM, and ManageOne



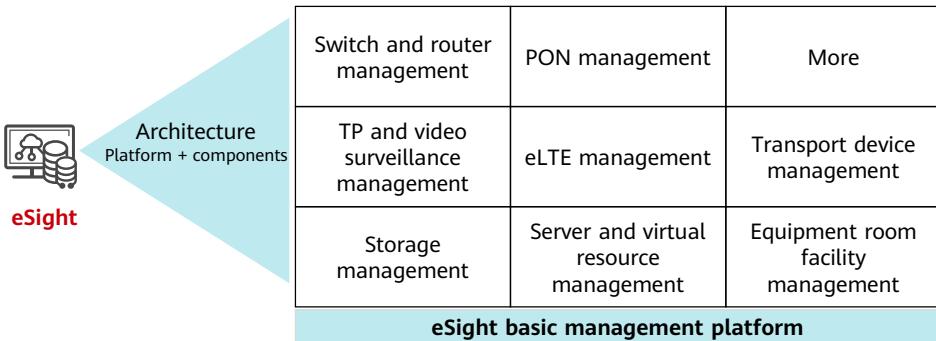
eSight Introduction

- eSight is a component of ManageOne. It comprehensively monitors the infrastructure that cloud services depend on, collects monitoring data such as alarms and performance data, and reports them to ManageOne Maintenance Portal. In addition, it can interconnect with the customer's Operations support system (OSS) through an NBI protocol such as SNMP, FTP, or HTTPS, and send SMS push messages or email.



- Terms:
 - OSS: Operations Support System
 - GPON: Gigabit Passive Optical Network

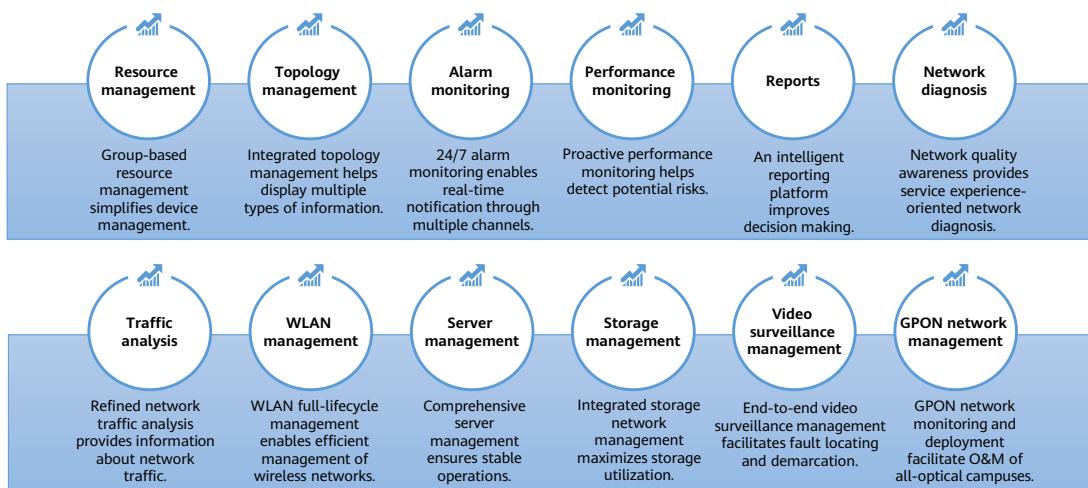
eSight Architecture



- Network management: manages wired and wireless convergence, network traffic, MPLS VPN, and security policies, and monitors the network quality to implement proactive O&M and fast fault demarcation, simplifying wired and wireless network O&M.
- Server management: monitors server and component status in real time, and configures visualized batch deployment and batch firmware upgrade, helping enterprise users simplify server O&M management.
- Virtual resource management: centrally monitors and manages virtual compute facilities, such as VMware ESX/ESXi Server, VMware vCenter Server, and Huawei FusionCompute and FusionAccess. The managed objects also include virtual servers and VMs.
- Storage management: analyzes and resolves various faults and bottlenecks on the storage network, predicts the capacity usage trend, and guides users to scale resources. This helps enterprises improve management efficiency and properly use storage resources in physical and virtual environments.
- Video surveillance management: offers discovery, service topology, performance and data analysis for video surveillance service resources, improving video surveillance device management quality and efficiency.
- PON network management: monitors the running status of the GPON network and obtains the overall layout of the GPON network. This helps maintenance personnel quickly locate and rectify faults on the GPON network.
- eLTE wireless access management: implements remote monitoring and maintenance for CPEs, base stations, and core network devices, helping users perform quick deployment of the eLTE network, device monitoring, quick fault

locating, and remote CPE maintenance and adjustment.

eSight Functions

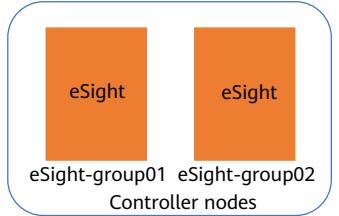


eSight GUI



eSight Deployment Modes

- In HUAWEI CLOUD Stack, eSight is deployed in active/standby mode and runs on eSight-group01 and eSight-group02 management VMs.
- eSight-group01 and eSight-group02 are running on controller nodes. You can view details about the VMs on Service OM.

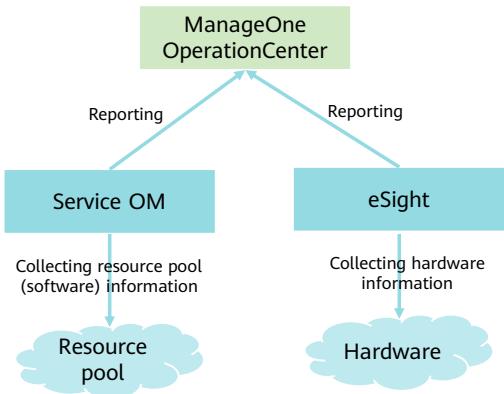


Name	Host ID	Host Group	Availability Z...	Status	Power Status	Flavor	CPU Archite...	IP Address	Batch Cold ...	Batch Live Migration
eSight-group02	1884ED33-25...	manage-aggr	manage-az	Running	Running	8vCPUs 32GB	X86/intel	10.200.16.161	Supported	Supported
eSight-group01	6C84ED33-2...	manage-aggr	manage-az	Running	Running	8vCPUs 32GB	X86/intel	10.200.16.160	Supported	Supported

- For details about the login scheme, see *HUAWEI CLOUD Stack 8.X Account List*.

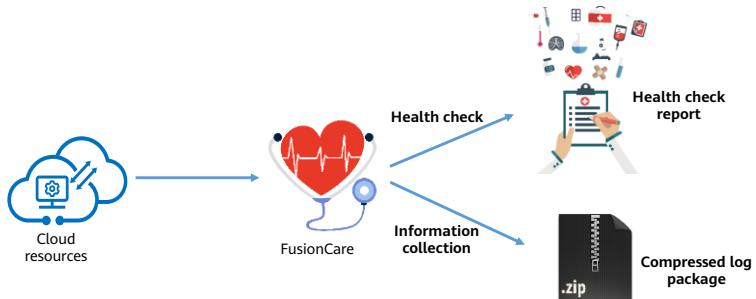
Relationships Between FusionSphere OpenStack, eSight, and ManageOne

- Service OM collects information about software resource pools, including compute, storage, and network resources. The information to be collected includes alarms and performance data.
- eSight collects hardware (servers, storage devices, switches, and routers) information, such as alarms and performance data.
- Service OM and eSight report collected information to ManageOne Maintenance Portal, and the information is displayed on a unified GUI.



Introduction to FusionCare

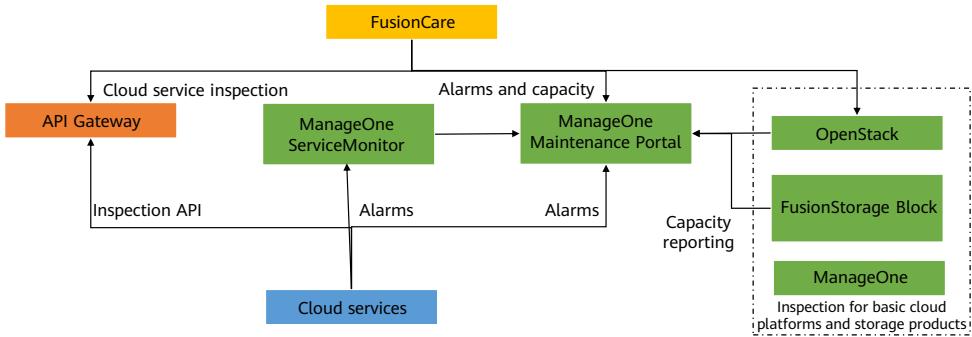
- FusionCare provides health check and information collection. With FusionCare health check, technical support engineers and maintenance engineers can check node health to obtain health check reports with just a few clicks. With FusionCare, engineers can collect logs for troubleshooting quickly and easily.



- The automated acceptance function is added to FusionCare used in 8.1.X. This function supports automated commissioning and acceptance of gPaaS & AI DaaS services, and provides acceptance test reports in Word format. This function will not be described in detail because this course does not involve gPaaS & AI DaaS services. Note that infrastructure cloud services are commissioned using HUAWEI CLOUD Stack Deploy.

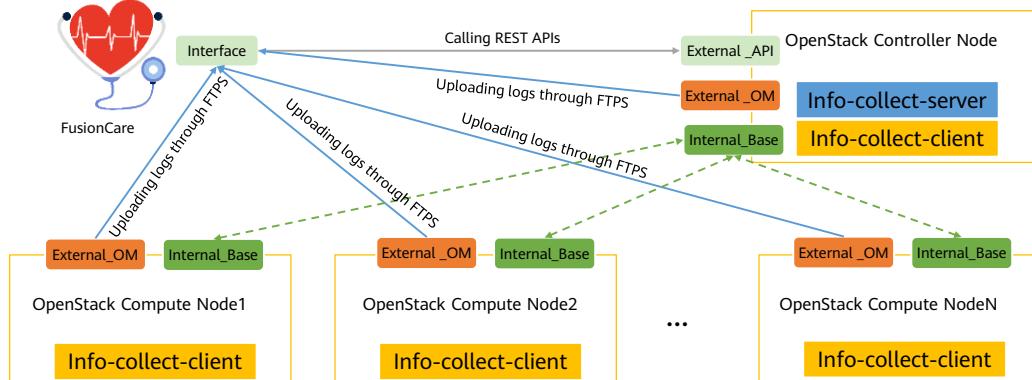
FusionCare Inspection Principles

- Cloud service health check: Each cloud service registers a health check API with API Gateway so that FusionCare can check basic cloud platforms, infrastructure cloud services, and gPaaS and AI DaaS services.
- Inspection for basic cloud platforms and storage products: FusionCare calls the API of each product to perform inspection.



FusionCare Log Collection Principles

- FusionCare invokes Info-collect-server in FusionSphere OpenStack through the API plane to send inspection requests and receives logs from Info-collect-client on each node through the External_OM plane. FusionCare must communicate with both External_API and External_OM.



- In FusionSphere OpenStack, info-collect is used for inspection and log collection. The info-collect module is deployed in C/S mode. A server is deployed on a controller node to receive external inspection and log collection requests. A client is deployed on each node to check inspection items, collect logs, and upload logs using FTPS.
- Only controller nodes of FusionSphere OpenStack are configured with the IP address of the API plane as the reverse proxy for receiving external requests. Each node is configured with the IP address of the External_OM plane for uploading logs and logging in to the node during O&M. The functions of the three planes in health check and log collection scenarios are as follows:
 - External_API: receives FusionCare health check and inspection API requests and reports health check and log collection results.
 - Internal_Base: used for internal communication between the server and client of the info-collect module. The info-collect-server module sends requests to info-collect-client to perform inspection and log collection tasks.
 - External_OM: used to upload logs to FusionCare using FTPS.

Services Supported by FusionCare

Component	Service	Optional/Mandatory (Full Scenarios)	Optional/Mandatory (Independent Deployment of a Global Zone)
FusionSphere OpenStack	FusionSphere OpenStack	Mandatory	Mandatory
	Service OM/OpenStack OM	Mandatory	Mandatory
Cloud management service	ManageOne	Mandatory	Mandatory
Basic services and common components	IaaS service	Optional	N/A
	API Gateway	Mandatory	Mandatory
Security services	FusionGuard HSS, CBH, WAF, CSP, ISAP, SOC, and DSC	Optional	N/A
AI services	MRS, DWS, DGC, ModelArts, and GES	Optional	Optional Only DWS and MRS are supported.
Storage services	OBS 3.0	Optional	N/A
Container services	CCE, SWR, and ASM	Optional	N/A
Applications	ROMA Connect, DCS, APM, AOM, ServiceStage, LTS, and BCS	Optional	N/A
Database services	RDS for MySQL, DDS, GaussDB(for openGauss), and DRS	Optional	N/A
IoT services	IoTDA, IoT, and DRIS	Optional	N/A

FusionCare Console

Health Check Tasks

Name	Start Time	Execution Duration	Status	Progress	Task Scenario	Task Policy	Object Check Pass Rate	Check Item Pass Rate	Created	Operation
CCE	2022-01-26 14:45:45	14m45s	Finished	100%	Routine health ...	Real-time task	50%	93.75%	admin	Modify Export Report

Basic Information

Name: CCE	Status: Finished
Task Scenario: Routine health check	
Task Policy: Real-time task	
Start Time: 2022-01-26 14:45:45	
End Time: 2022-01-26 14:49:39	
Duration: 14m45s	

Object Check Pass Rate

By environment: 50% Failed Objects

Check Item Pass Rate

By environment: 93.75% Passed Checks

Component Check Result

Object Check Details	Check Item Fault Details					
Environment Name: HUAWEI_CLOUD_Stack	Product Type: CCE	Object Name: CCE-GaussDB-CCE01	Object Type: CloudDB	Object IP/ID: 10.200.18.70	Status: Failed	Operation: Details Retry

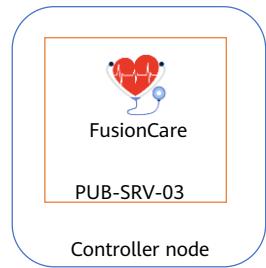
67 Huawei Confidential



- You can log in to FusionCare from ManageOne Maintenance Portal in SSO mode. After FusionCare is installed using HUAWEI CLOUD Stack Deploy, SSO is automatically configured.

FusionCare Deployment Mode

- In HUAWEI CLOUD Stack, FusionCare is deployed on a single-node. It runs on the PUB-SRV-03 management VM.
- The PUB-SRV-03 management VM runs on a controller node. You can view details about the VM on Service OM.

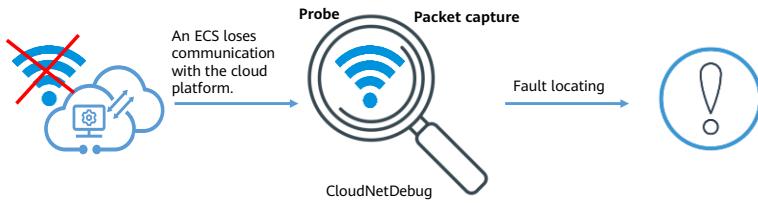


Name	Host ID	Host Group	Availability Z...	Status	Power Status	Flavor	CPU Archite...	IP Address	Batch Cold ...	Batch Live Migration
PUB-SRV-04	B984ED33-25...	manage-aggr	manage-az	Running	Running	4vCPUs 8GB	X86/intel	10.200.16.233	Supported	Supported
PUB-SRV-03	5784ED33-25...	manage-aggr	manage-az	Running	Running	4vCPUs 8GB	X86/intel	10.200.16.232	Supported	Supported
PUB-SRV-02	7986ED33-25...	manage-aggr	manage-az	Running	Running	4vCPUs 8GB	X86/intel	10.200.16.231	Supported	Supported
PUB-SRV-01	9D84ED33-2...	manage-aggr	manage-az	Running	Running	4vCPUs 8GB	X86/intel	10.200.16.230	Supported	Supported

- For details about the login scheme, see *HUAWEI CLOUD Stack 8.X Account List*.

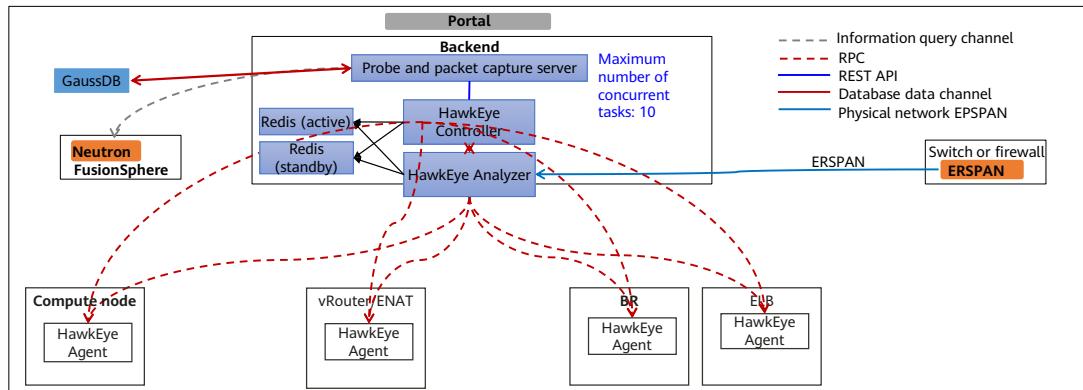
Introduction to CloudNetDebug

- CloudNetDebug is an O&M tool that helps O&M personnel capture packets automatically. It integrates probe and packet capture to handle various network problems that may occur in a data center. The probe can automatically check whether the service network has been interrupted and if there is packet loss. Packet capture functions include automatic and multi-point collaborative packet capture based on service flows, single-point VM NIC packet capture, and host NIC packet capture.



CloudNetDebug Architecture

- CloudNetDebug consists of a Server and an Agent.
 - The Server is deployed on a VM of a controller node. The probe/packet capture server, HawkEye Controller, HawkEye Analyzer, and Redis are deployed on the Server.
 - The Agent is deployed on compute nodes and network nodes.



70 Huawei Confidential



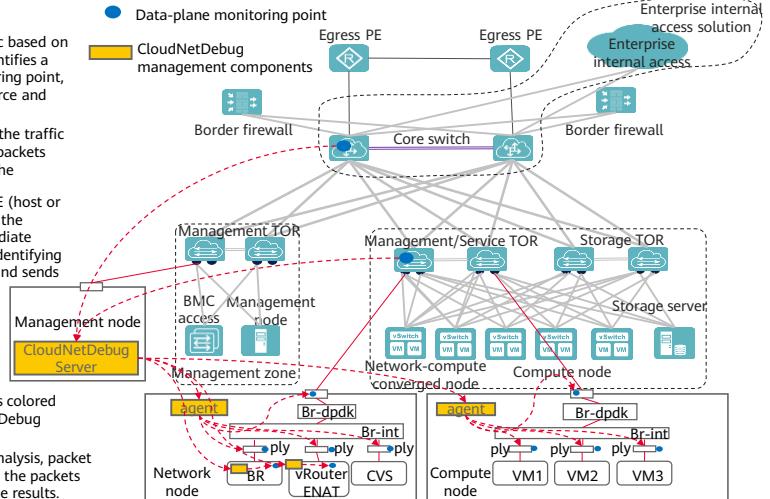
- CloudNetDebug of the current version supports packet capture and probe for vRouter or ENAT, Board Router (BR), ELB, and hardware switches or firewalls on compute and network nodes. For details, see the CloudNetDebug feature specifications list. The architecture on this slide uses vRouter or ENAT, BR, ELB, and hardware switch/firewall as an example.
- The probe or packet capture server interacts with the portal, responds to user operations on the GUI, and delivers tasks to hkeEyeController through the REST API. hkeEyeController delivers the probe and packet capture tasks to the agents of the target compute nodes and network nodes using RPC messages. After the tasks are complete, hkeEyeAnalyzer obtains the result from agents, reports the result to hkeEyeController, and saves the result file in Redis. hkeEyeController reports the result to the probe or packet capture server. The server saves the result in the GaussDB database and displays the result on the portal.

- When CloudNetDebug is used to query VM information, the probe or packet capture server invokes the Neutron component of FusionSphere OpenStack to obtain information.
- To use CloudNetDebug to perform probe and packet capture on switches or firewalls, you need to enable the Encapsulated Remote Switched Port Analyzer (ERSPAN) feature on the physical switches. After the feature is enabled, hkeEyeAnalyzer becomes the remote mirroring device of the switches or firewalls. The switches or firewalls encapsulate the mirrored packet into an IP packet through a GRE tunnel and route the IP packet to the destination port of hkeEyeAnalyzer.

Basic Principles of Probe

Probe service process:

- ① CloudNetDebug identifies the type of traffic based on a 5-tuple entered by the administrator, identifies a traffic injection point, intermediate monitoring point, and termination point; and obtains the source and destination MAC addresses of the traffic.
- ② CloudNetDebug identifies the agent where the traffic injection point is located, injects simulated packets into the gateway or ply bridge, and colors the simulated packets.
- ③ After the packets are injected, the virtual NE (host or gateway) identifies whether the traffic with the colored packets passes through the intermediate monitoring point on the traffic path. After identifying the traffic, the virtual NE copies the traffic and sends it to the CloudNetDebug server.
- ④ After receiving the colored packets, the physical switch matches the packet with the ACL rules of the switch, mirrors the colored packets, and sends them to the remote CloudNetDebug server.
- ⑤ The agent of the termination point identifies colored packets, copies the packets to the CloudNetDebug server, and terminates the traffic.
- ⑥ The CloudNetDebug server performs path analysis, packet loss detection, and delay detection based on the packets sent by the agent and switch, and reports the results.

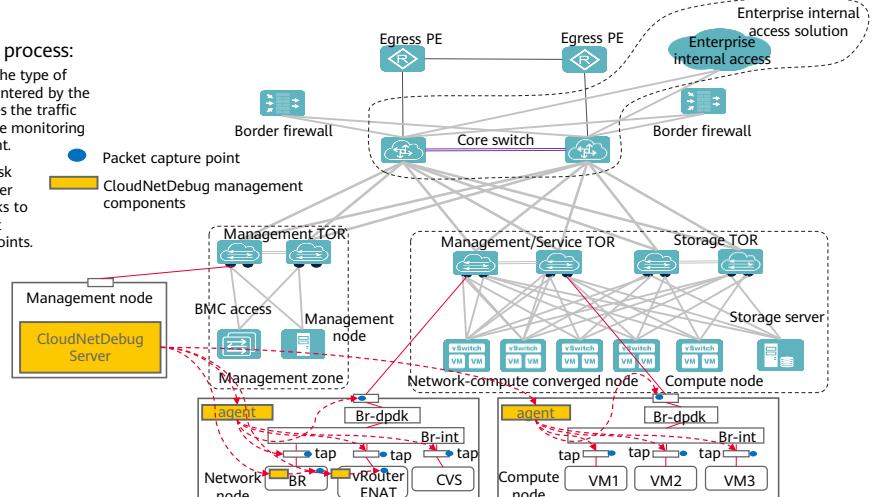


- CVS is a component responsible for layer-4 load balancing in ELB. It provides enhanced features based on the native LVS.
- ply bridge: It is one of the internal bridges of Open Virtual Switch (OVS) and is mainly used to filter unicast packets with non-local MAC addresses.
- Br-int bridge: It is one of the internal bridges of Open Virtual Switch (OVS) and is mainly used to forward packet frames.
- Br-dpdk bridge: This bridge exists only when the Data Plane Development Kit (DPDK) technology is enabled on the node. It is mainly used to process high-speed packets to improve packet processing efficiency.

Basic Principles of Packet Capture

Packet capture service process:

- ① CloudNetDebug identifies the type of traffic based on a 5-tuple entered by the administrator, and identifies the traffic injection point, intermediate monitoring point, and termination point.
- ② After the packet capture task starts, CloudNetDebug server delivers packet capture tasks to all agents and starts packet capture at all monitoring points.
- ③ The agent captures packets based on the packet filtering requirements, completes the task of capturing packets at the specified time, and temporarily saves the captured files to the local host.
- ④ The server checks a packet and obtains the packet capture file from the agent for the O&M administrator to download.



73 Huawei Confidential



- CVS is a component responsible for layer-4 load balancing in ELB. It provides enhanced features based on the native LVS.
- br-int bridge: It is one of the internal bridges of Open Virtual Switch (OVS) and is mainly used to filter unicast packets with non-local MAC addresses.
- br-int bridge: It is one of the internal bridges of Open Virtual Switch (OVS) and is mainly used to forward packet frames.
- br-dpdk bridge: This bridge exists only when the Data Plane Development Kit (DPDK) technology is enabled on the node. It is mainly used to process high-speed packets to improve packet processing efficiency.

CloudNetDebug Features

Service Type	Probe Supported	Protocols Supported by Probe	Bidirectional Probe Supported	Packet Capture Supported
VPC L2	Yes	TCP/UDP/ICMP	Yes	Yes
VPC L3	Yes	TCP/UDP/ICMP	Yes	Yes
VPC Peer	Yes	TCP/UDP/ICMP	Yes	Yes
Basic Direct Connect	Yes	TCP/UDP/ICMP	Yes	Yes
EIP	Yes	TCP/UDP/ICMP	Yes	Yes
Enhanced Direct Connect	Yes	Inbound: not supported Outbound: TCP/UDP/ICMP	NULL	Yes
SNAT	Yes	TCP/UDP	Yes	Yes
ELB	Yes	TCP/UDP	Yes	Yes
VPC Endpoint	Yes	TCP/UDP	Yes	Yes
Packet capture on a VM	NULL	NULL	NULL	Yes
Packet capture on a host	NULL	NULL	NULL	Yes

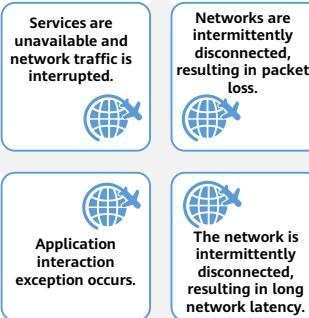
CloudNetDebug Application Scenarios

Objective: Determine whether traffic has been interrupted on the virtual or physical network, and, if it has, on which NE on the virtual network.

Measure: Use the probe tool (recommended) and packet capture tool. If the probe tool does not support this service scenario, use the service flow packet capture tool. If the service flow packet capture tool does not support this service scenario, use flexible VM NIC packet capture and host NIC packet capture to demarcate and locate the fault.

Objective: Search for the evidence of application interaction exceptions for fault locating.

Measure: Capture packets on the VM NIC, select a packet capture point, and perform bidirectional packet capture. Use Wireshark to analyze application interaction packets and locate the application interaction exception point. The tool does not support locating of service interaction exceptions, but can provide proof (if other network problems are excluded, the problem is a service interaction problem.) and problem basis (the packet capture file is provided for fault locating.) for such problems.



Objective: Determine whether the packet loss occurs on the virtual or physical network, and further the NE where the packet loss occurs on the virtual network.

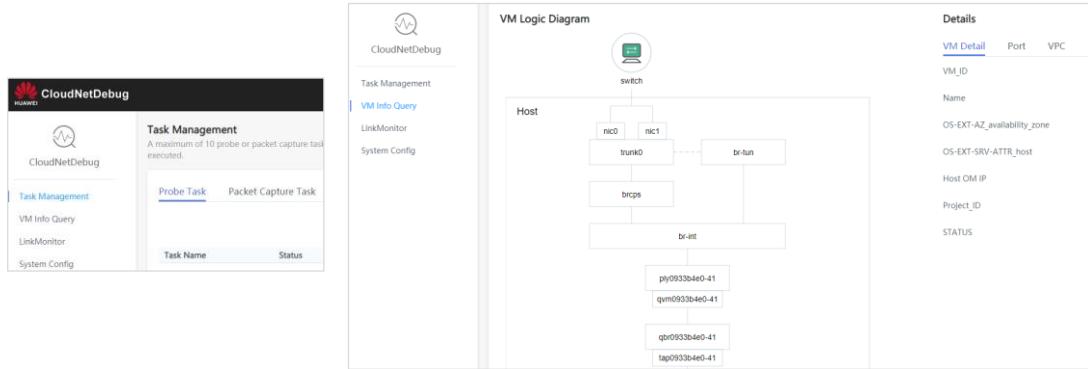
Measure: Use the probe tool (recommended) and packet capture tool. If the probe tool does not support this service scenario, use the service flow packet capture tool. If the service flow packet capture tool does not support this service scenario, use flexible VM NIC packet capture and host NIC packet capture to demarcate and locate the fault.

Objective: Locate the position where the delay is long and locate the NE where the long delay occurs on the virtual network.

Measure: A solution will be provided for the probe tool in the future.

- Currently, HUAWEI CLOUD Stack 8.1.X cannot resolve the issues of intermittent network disconnection and long network latency.

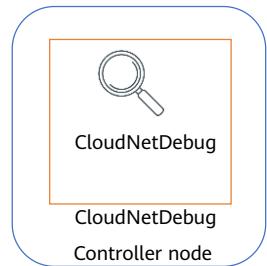
CloudNetDebug Console



- You can log in to CloudNetDebug from ManageOne Maintenance Portal in SSO mode. After CloudNetDebug is installed using HUAWEI CLOUD Stack Deploy, SSO is automatically configured.

CloudNetDebug Deployment Mode

- In HUAWEI CLOUD Stack, CloudNetDebug is deployed on a single-node. It runs on the CloudNetDebug management VM.
- The CloudNetDebug management VM runs on a controller node. You can view details about the VM on Service OM.



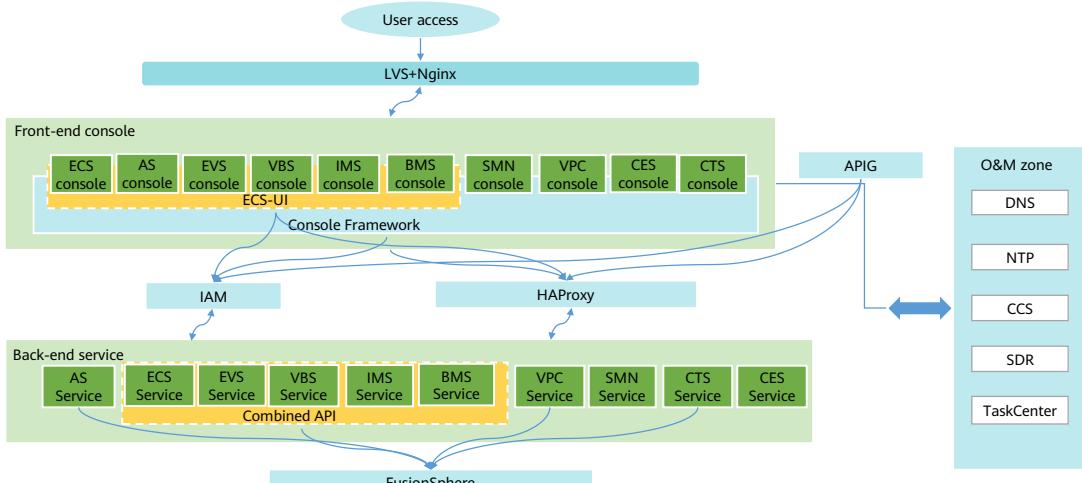
Name	Host ID	Host Group	Availability Z...	Status	Power Status	Flavor	CPU Archite...	IP Address	Batch Cold ...	Batch Live Migration
CloudNetDebug	8184ED33-25...	manage-aggr	manage-az	Running	Running	8vCPUs 16GB	X86/intel	10.200.16.88	Supported	Supported

- For details about the login scheme, see *HUAWEI CLOUD Stack 8.X Account List*.

Contents

1. HUAWEI CLOUD Stack Solution and Architecture
2. **HUAWEI CLOUD Stack Product Components and Common Components**
 - Introduction to Product Components
 - Introduction to Common Components

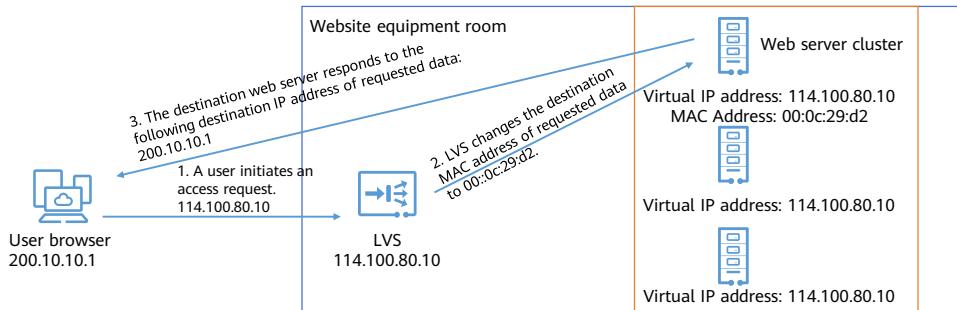
HUAWEI CLOUD Stack Public Load Balancing Solution



- The load balancing solutions for IaaS services and gPaaS & AI DaaS services in HUAWEI CLOUD Stack are different. This section describes only the load balancing solution for IaaS services.
- LVS and Nginx are required for load balancing when users access cloud service consoles. HAProxy is required for load balancing when cloud service consoles access cloud services.
- The cloud service access process is as follows:
 - Users-Firewalls-LVS-Nginx-Frontend console-APIG-HAProxy-Cloud services
 - Cloud services-HAProxy-Console-Ngnix-Users

LVS

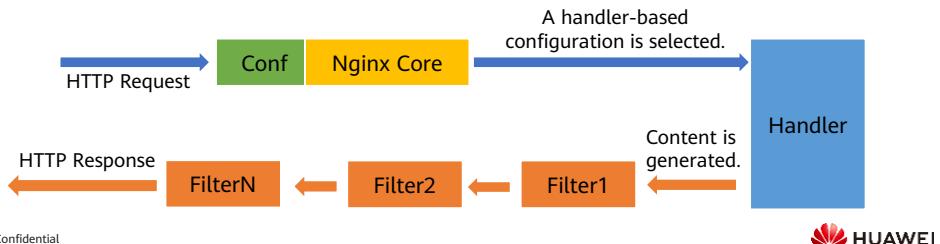
- LVS supports layer-4 load balancing. As it is built at the transport layer of the OSI model, it offers high efficiency.
- An LVS system has two packet forwarding modes:
 - In NAT mode, packets are forwarded by changing the IP address (at layer 3 of the OSI model).
 - In DR mode, packets are forwarded by changing the MAC address (at layer 2 of the OSI model).
- The DR mode is used in the cloud service framework.



- The preceding figure shows the forwarding process in DR mode.
 - In DR mode, LVS and the RealServer cluster must be bound to the same floating IP address (the RealServer cluster binds the floating IP address to the local loopback link). Requests are received by the LVS but returned to the user by the RealServer that provides services without passing through the LVS. When receiving a request, the LVS only needs to change the MAC address to that of a RealServer in the configuration file. Then, the packet is forwarded to the RealServer for processing. In this case, the source and destination IP addresses remain unchanged. After the RealServer receives the packet forwarded by the LVS, the MAC address and IP address carried by the packet are detected to be those of the RealServer at the data link layer and the network layer, respectively. Therefore, the packet is accepted and the RealServer cannot detect the existence of the LVS. The RealServer returns the response to the source IP address (that is, the IP address of the user) without passing through the LVS.
- The current version uses the DR mode. After a service request reaches the LVS node, the LVS node replaces the destination MAC address with that of the backend Nginx node. After receiving the request, Nginx matches the MAC address with its local MAC address. If they are matched, Nginx forwards the request based on specified rules.

Nginx

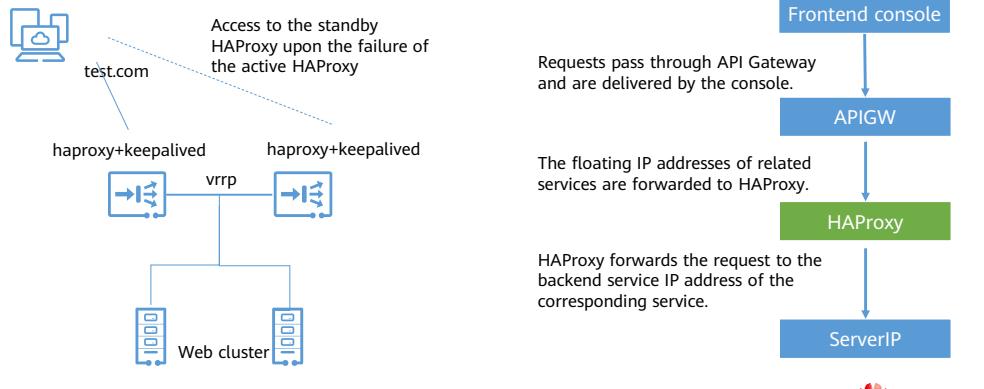
- Nginx supports layer-7 load balancing. It is built at the application layer of the OSI model, and forwards packets based on URLs. URLs and other data can be modified during forwarding.
- Nginx modules are classified by the following function types:
 - Handlers: This type of module processes requests, outputs content, and modifies header information. Generally, there can be only one Handler module.
 - Filters: This type of module modifies content output by other processor modules. Nginx outputs the final content.
 - Proxies: This type of module belongs to the HTTP upstream modules of Nginx. These modules interact with backend services, such as FastCGI, to function as service proxies and implement load balancing.



- Nginx is a layer-7 load balancing service. In HUAWEI CLOUD Stack, Nginx is mainly used for load balancing on cloud service consoles. After receiving a request, Nginx searches for the IP address of the backend service based on the domain name and distributes the request to the backend service based on the configured forwarding rule. The current version uses the IP hash forwarding mode.

HAProxy

- HAProxy supports layer-4 and layer-7 load balancing. In the cloud service framework, layer-4 forwarding is adopted and data is forwarded based on IP address and port number. The URL and other data can be modified during the forwarding process.



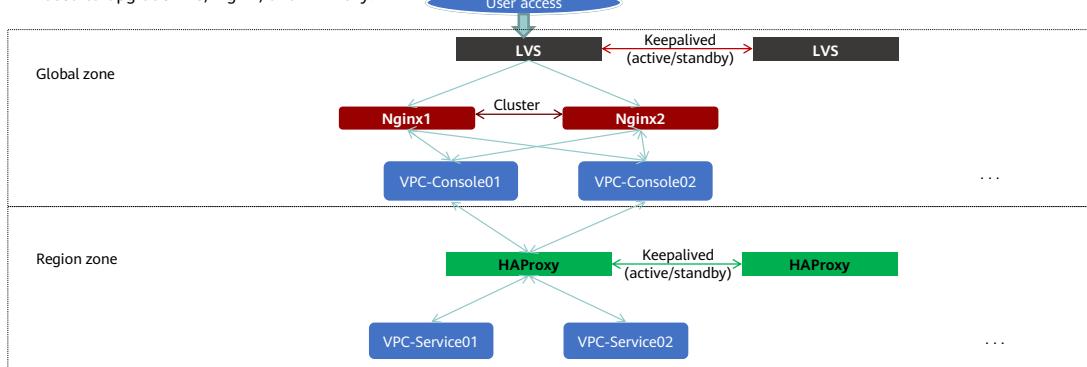
82 Huawei Confidential



- HAProxy can supplement some disadvantages of Nginx by supporting session persistence and cookie guidance. In addition, HAProxy can detect the status of backend servers by obtaining specified URLs. Similar to LVS, HAProxy is only a type of load balancing software. HAProxy has a higher load balancing speed than Nginx and is better than Nginx in concurrent processing.
- HAProxy is deployed in active/standby mode. The active and standby HAProxy nodes maintain the active/standby relationship through the heartbeat cable Keepalived, synchronize data using the VRRP protocol, and provide a floating IP address (always on the active server) for clients to access. For example, when a client accesses **test.com**, the domain name is resolved to the floating IP address of HAProxy, based on the load balancing policy of HAProxy, the backend server is selected to respond. When the active HAProxy breaks down, the floating IP address is switched to the other server.
- In HUAWEI CLOUD Stack, requests are delivered by the console and pass through APIG. The floating IP addresses of related services are forwarded to HAProxy. HAProxy forwards the requests to the backend service IP addresses of the corresponding servers.

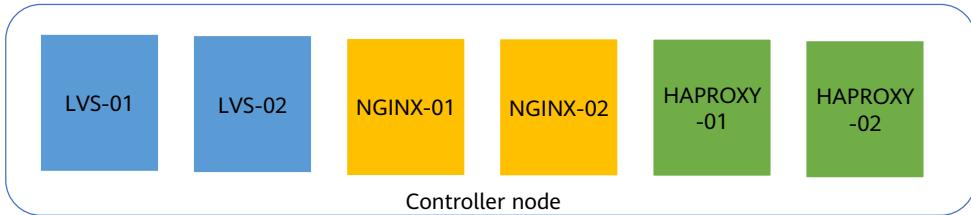
LVS+Nginx+HAProxy Deployment Mode (1)

- LVS, Nginx, and HAProxy are deployed on two separate nodes. LVS and HAProxy are deployed in active/standby mode, and Nginx is deployed in cluster mode.
- LVS, Nginx, and HAProxy are deployed in one-click mode using HUAWEI CLOUD Stack Deploy without manual intervention. DMK is used to upgrade LVS, Nginx, and HAProxy.



- LVS provides load balancing services for multiple Nginx servers through OSI layer-4 forwarding. It is called level-1 LB because it is the load balancing at the first layer in the Global zone.
- Nginx provides load balancing services for multiple console servers through OSI layer-7 forwarding. It is called level-2 LB because it is the load balancing at the second layer in the Global zone.
- HAProxy provides load balancing services for servers in the Region zone through OSI layer-4 forwarding.

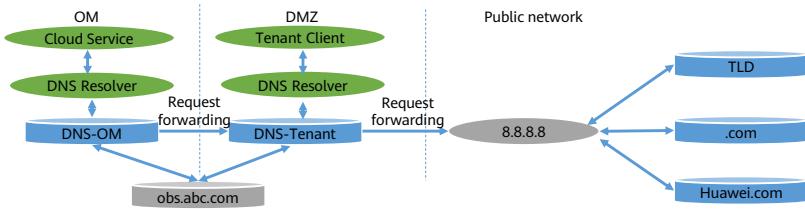
LVS+Nginx+HAProxy Deployment Mode (2)



Name	Host ID	Host Group	Availability Z...	Status	Power Status	Flavor	CPU Archite...	IP Address	Batch Cold ...	Batch Live Migration
LVS-02	9D84ED33-2...	manage-aggr	manage-az	Running	Running	2vCPUs 2GB	X86/Intel	10.200.5.26	Supported	Supported
LVS-01	1884ED33-25...	manage-aggr	manage-az	Running	Running	2vCPUs 2GB	X86/Intel	10.200.5.25	Supported	Supported
NGINX-02	8184ED33-25...	manage-aggr	manage-az	Running	Running	2vCPUs 3GB	X86/Intel	10.200.5.28	Supported	Supported
NGINX-01	9D84ED33-2...	manage-aggr	manage-az	Running	Running	2vCPUs 3GB	X86/Intel	10.200.5.27	Supported	Supported
HAProxy-02	8184ED33-25...	manage-aggr	manage-az	Running	Running	2vCPUs 4GB	X86/Intel	10.200.16.229	Supported	Supported
HAProxy-01	1884ED33-25...	manage-aggr	manage-az	Running	Running	2vCPUs 4GB	X86/Intel	10.200.16.228	Supported	Supported

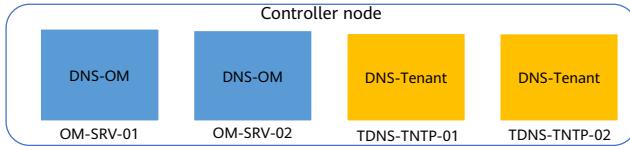
HUAWEI CLOUD Stack Domain Name Service

- The domain name service consists of the management side and the tenant side.
 - DNS-OM: functions as the local DNS server to provide domain name resolution for cloud services and resolve public domain names as a proxy.
 - DNS-Tenant: functions as the local DNS server to provide domain name resolution for tenant VMs. It also functions as the public network egress of DNS-OM and as a proxy to resolve public network domain names.
- Domain name resolution of management VMs: Management VMs send a domain name resolution request to DNS-OM through DNS Resolver. If DNS-OM has a record of the domain name resolution, it directly returns the resolution result. Otherwise, DNS-OM forwards the request to DNS-Tenant. If DNS-Tenant still cannot resolve the domain name, DNS-Tenant forwards the request to the external DNS.
- Domain name resolution of tenant VMs: A tenant VM sends a domain name resolution request to DNS-Tenant through DNS Resolver. If DNS-Tenant has a record of the domain name resolution, it directly returns the resolution result. Otherwise, DNS-Tenant forwards the request to an external DNS.



DNS Deployment

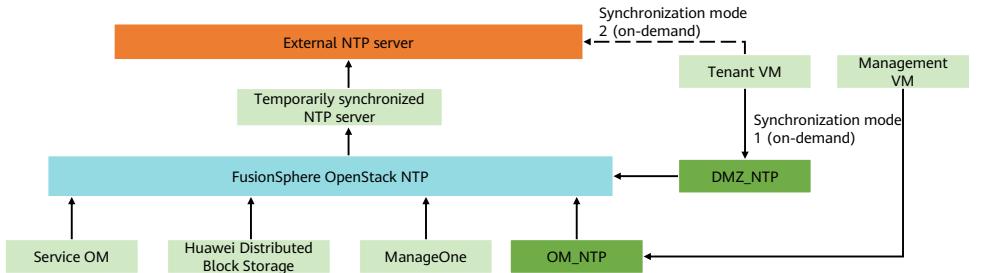
- DNS at the common component layer includes DNS-OM deployed on the management network plane and NTP-Tenant deployed on the tenant plane. VM nodes accommodating DNS-OM are OM-SRV-01 and OM-SRV-02, which are deployed in active/standby mode. VM nodes accommodating DNS-Tenant are TDNS-TNTP-01 and TDNS-TNTP-02, which are deployed in active/standby mode.
- DNS component is deployed in one-click mode using HUAWEI CLOUD Stack Deploy without manual intervention. You can view VM details on Service OM.



Name	Host ID	Host Group	Availability Z...	Status	Power Status	Flavor	CPU Archite...	IP Address	Batch Cold ...	Batch Live Migration
OM-SRV-02	1884ED33-25...	manage-aggr	manage-az	Running	Running	4vCPUs 8GB	X86/Intel	10.200.16.237	Supported	Supported
OM-SRV-01	8184ED33-25...	manage-aggr	manage-az	Running	Running	4vCPUs 8GB	X86/Intel	10.200.16.236	Supported	Supported
TDNS-TNTP-02	4C85ED33-2...	manage-aggr	manage-az	Running	Running	2vCPUs 4GB	X86/Intel	10.200.5.7	Supported	Supported
TDNS-TNTP-01	5784ED33-25...	manage-aggr	manage-az	Running	Running	2vCPUs 4GB	X86/Intel	10.200.5.6	Supported	Supported

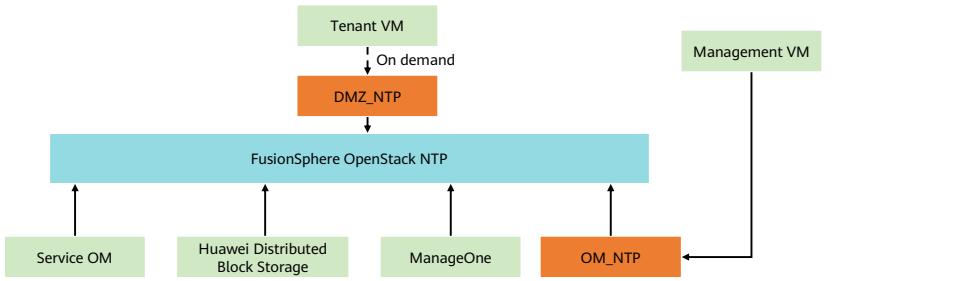
HUAWEI CLOUD Stack Clock Synchronization with External NTP Server

- The NTP service of FusionSphere OpenStack at the resource pool layer obtains clock sources from external NTP servers.
- Service OM, Huawei Distributed Block Storage (including FusionStorage Manager (FSM) and FusionStorage Agent (FSA)), and ManageOne at the resource pool layer as well as OM_NTP at the common component layer obtain clock sources from the NTP service of FusionSphere OpenStack.
- DMZ_NTP at the common component layer obtains clock sources from the NTP service of FusionSphere OpenStack.
- Management VMs where cloud services, common components, and management domain ManageOne reside obtain clock sources from OM_NTP at the common component layer.
- Tenant VMs can obtain clock sources from DMZ_NTP at the common component layer or an external NTP server based on the actual situation.



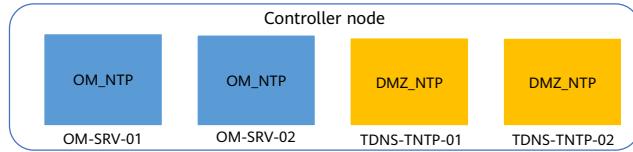
HUAWEI CLOUD Stack Clock Synchronization without External NTP

- Service OM, Huawei Distributed Block Storage, and ManageOne at the resource pool layer as well as OM_NTP at the common component layer obtain clock sources from the NTP service of FusionSphere OpenStack.
- DMZ_NTP at the common component layer obtains clock sources from the NTP service of FusionSphere OpenStack.
- Management VMs where cloud services, common components, and management domain ManageOne reside obtain clock sources from OM_NTP at the common component layer.
- Tenant VMs can obtain clock sources from DMZ_NTP at the common component layer based on the actual situation.



NTP Deployment

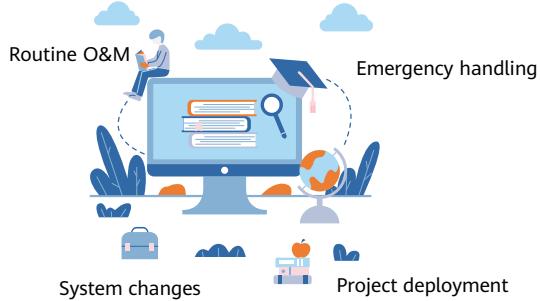
- NTP at the common component layer includes OM_NTP deployed on the management network plane and DMZ_NTP deployed on the tenant network plane. VM nodes accommodating OM_NTP are OM-SRV-01 and OM-SRV-02, which are deployed in active/standby mode. VM nodes accommodating DMZ_NTP are TDNS-TNTP-01 and TDNS-TNTP-02, which are deployed in active/standby mode.
 - OM_NTP corresponds to the management side and provides clock synchronization services for management VMs.
 - DMZ_NTP corresponds to the tenant side and provides clock synchronization services for tenant VMs. DMZ_NTP also functions as the upper-level clock source of OM_NTP and obtains time from the external clock source.

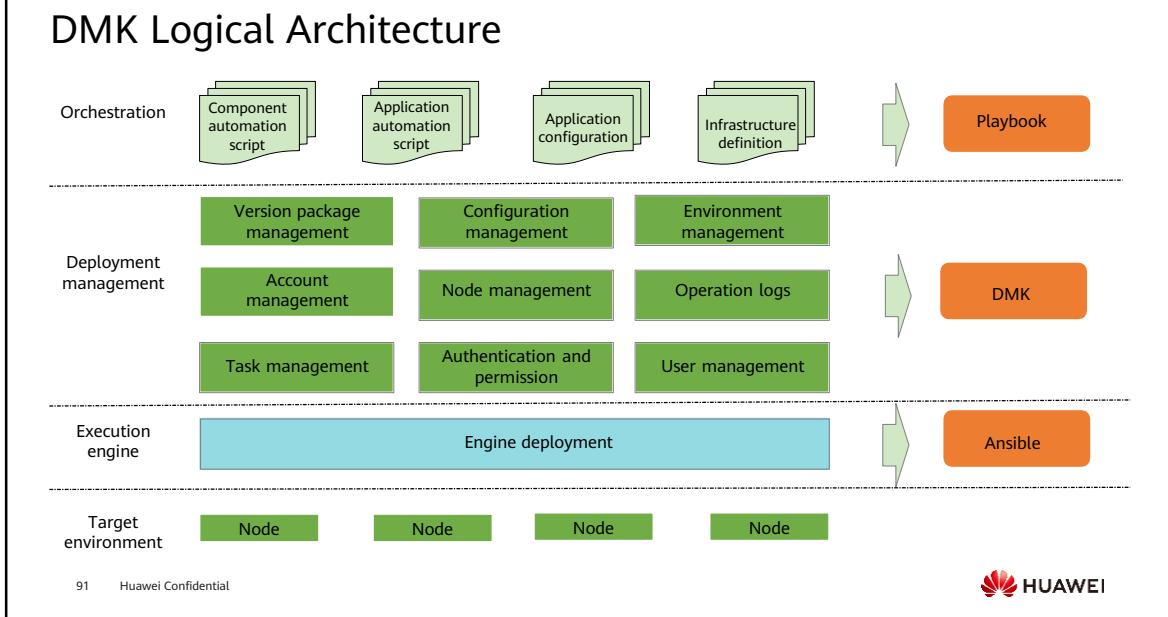


Name	Host ID	Host Group	Availability Z...	Status	Power Status	Flavor	CPU Archite...	IP Address	Batch Cold ...	Batch Live Migration
OM-SRV-02	1884ED33-25...	manage-aggr	manage-az	Running	Running	4vCPUs 8GB	X86/Intel	10.200.16.237	Supported	Supported
OM-SRV-01	8184ED33-25...	manage-aggr	manage-az	Running	Running	4vCPUs 8GB	X86/Intel	10.200.16.236	Supported	Supported
TDNS-TNTP-02	4C85ED33-2...	manage-aggr	manage-az	Running	Running	2vCPUs 4GB	X86/Intel	10.200.5.7	Supported	Supported
TDNS-TNTP-01	5784ED33-25...	manage-aggr	manage-az	Running	Running	2vCPUs 4GB	X86/Intel	10.200.5.6	Supported	Supported

DMK

- Deploy Management Kit (DMK) is a unified deployment and configuration platform on which services can be installed and upgraded. You can quickly deploy IaaS services, components, and some O&M tools using DMK platform, shortening the time required for installation. DMK is an Ansible-based automated execution engine that implements automated O&M capabilities. O&M operations include deployment, upgrade, rollback, and the uninstallation of services and applications, node management, and configuration management.

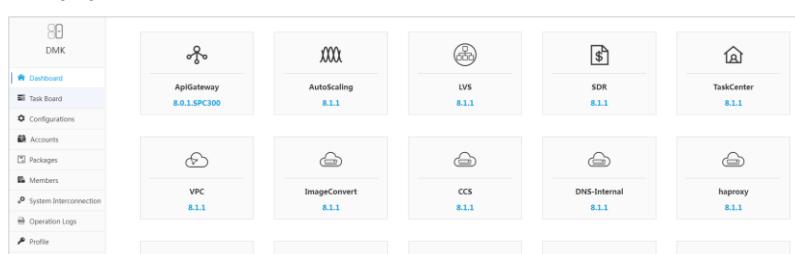


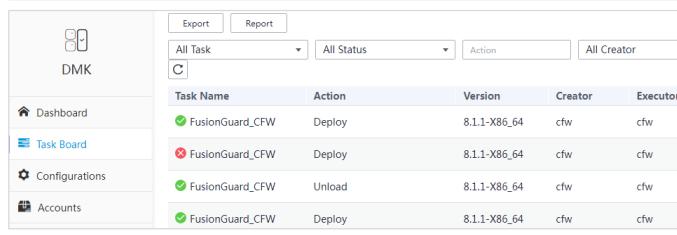


- DMK uses Ansible, an open-source automatic O&M tool, to execute various configurations and installation tasks. DMK has various deployment management tools, such as those for configuration management and node management. DMK provides various orchestration methods, such as component automation scripts and application configuration. An Ansible playbook (Ansible task configuration file in YAML format, which can define multiple tasks in a script and be automatically executed by Ansible) is also used.

Load Balancing > DNS > Clock Synchronization > DMK > APIG > Combined API > CCS > SDR > TaskCenter > GaussDB

DMK Example (1)

- Dashboard:


- Task Board


Task Name	Action	Version	Creator	Executor
FusionGuard_CFW	Deploy	8.1.1-X86_64	cfw	cfw
FusionGuard_CFW	Deploy	8.1.1-X86_64	cfw	cfw
FusionGuard_CFW	Unload	8.1.1-X86_64	cfw	cfw
FusionGuard_CFW	Deploy	8.1.1-X86_64	cfw	cfw

92 Huawei Confidential

 HUAWEI

- On the DMK page, you can use the deployment wizard to create a task.
 - Step 1: Configure a service. Select the required service, version, and operation. You can also directly modify the configuration file (optional).
 - Step 2: On the **Hosts and User Configuration** page, select the node (group) to which the service belongs and the account name for performing the operation. You can also directly modify the hosts configuration file (optional).
 - Step 3: Execute the task. During the execution, you can view the task details.

DMK Example (2)

- Configuration management

The screenshot shows a web-based interface for managing configurations. At the top, there are tabs for "Public Configuration" and "Change Tracking". Below this, a dropdown menu shows "Public Configurations" and an "Edit" button. The main area displays a list of configuration items with line numbers:

```

1 + g_12_rgids;
2 + allow_access_remote_host: 192.168.21.21|192.168.21.22
3 + g_bssi:
4 + ip: 127.0.0.1:8090
5 + url: no_bss
6 + g_clouds:
7 + reg_ip: ac-taskcenter.mcie.com
8 + server_port: 28938;
9 + g_console:
10 + current: "\u0FFE$"
11 + httpcenter:
12 - https://docs.elab-hcie.com/mohelpcenter/operation
13 + home:
14 + address:

```

- SSH account management

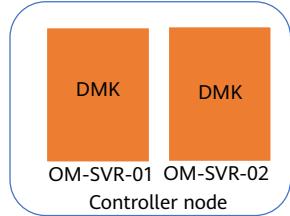
The screenshot shows a table of SSH accounts. The columns are: Account Name, Description, Type, Creator, and Teams. There are five entries:

Account Name	Description	Type	Creator	Teams
osuser	osuser	Password	cloud_dns	CLOUD_DNS
root	root	Password	AutoScaling	AutoScaling
autoscaling	autoscaling	Password	AutoScaling	AutoScaling
osuser	osuser	Password	vpc	VPC
root	root	Password	cloud_dns	CLOUD_DNS

- DMK allows you to view the configuration information and change records of cloud platform components, as well as manage (modify, add, and delete) SSH accounts in HUAWEI CLOUD Stack.

DMK Deployment

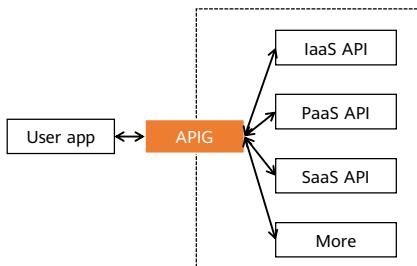
- DMK is deployed together with other cloud services on the OM-SVR01 and OM-SVR02 nodes in active/standby mode. They are deployed in one-click mode using HUAWEI CLOUD Stack Deploy without manual intervention.
- DMK provides a portal for users to log in on. You are advised not to log in to DMK to avoid misoperations that may cause HUAWEI CLOUD Stack component configuration exceptions.



Name	Host ID	Host Group	Availability Z...	Status	Power Status	Flavor	CPU Archite...	IP Address	Batch Cold ...	Batch Live Migration
OM-SRV-02	1884ED33-25...	manage-aggr	manage-az	Running	Running	4vCPUs 8GB	X86/intel	10.200.16.237	Supported	Supported
OM-SRV-01	8184ED33-25...	manage-aggr	manage-az	Running	Running	4vCPUs 8GB	X86/intel	10.200.16.236	Supported	Supported

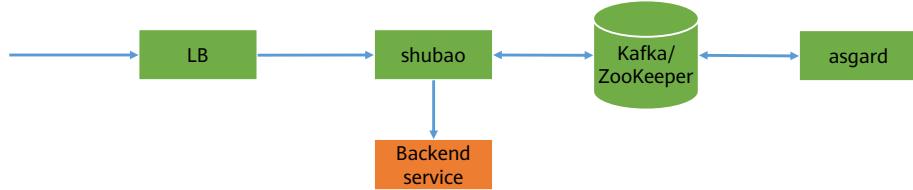
API Gateway

- API Gateway (APIG) is used with industry solutions to provide high-performance, highly available, and secure API hosting services. It is an end-to-end product that covers API running, management, analysis, and security. It decouples backend services and data from upper-layer applications, helps customers efficiently expand services, and connects customers with vendors of backend services and applications to build a developer ecosystem.
- APIG is used by cloud services in HUAWEI CLOUD Stack. It allows internal services to register APIs and opens APIs to tenants. It registers, forwards, and balances APIs in the infrastructure and gPaaS & AI DaaS service scenarios.



Feature	Note
Management APIs	Enable, disable, and upgrade APIs.
Flow control	Configuration of maximum API requests, maximum user requests, and thresholds for excluded tenants
Authentication	Token or AK/SK authentication
Security	Anti-brute force cracking and anti-replay attacks

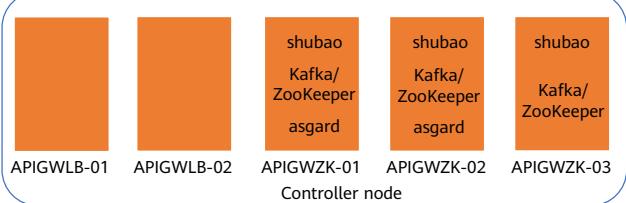
APIG Architecture



Component	Function
LB	Reverse proxy and load balancing when APIs on the management plane are called
shubao	Core component in APIG, which receives, authenticates, and forwards API requests
Kafka/ZooKeeper	Message queue, which transfers the number of API call times and the blacklist and whitelist
asgard	Used for calculating and processing API flow control.

APIG Deployment Mode

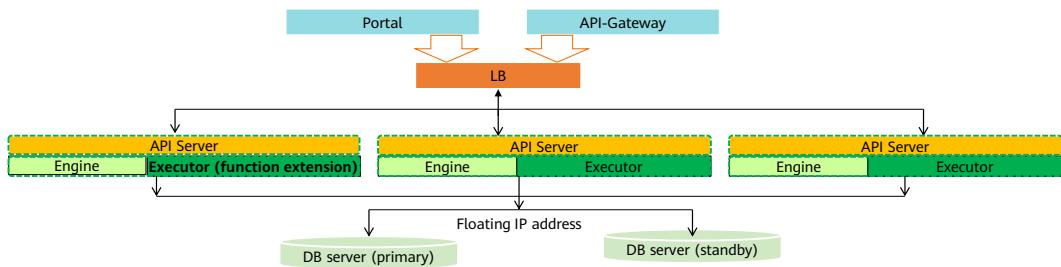
- APIG consists of two reverse proxy and load balancing VMs (APIGWLB VMs) deployed in active/active mode for calling management plane APIs and three component VMs (APIGWZK) deployed in cluster mode. These VMs are deployed in one-click mode using HUAWEI CLOUD Stack Deploy without manual intervention.
- asgard is not deployed on APIGWZK-03.



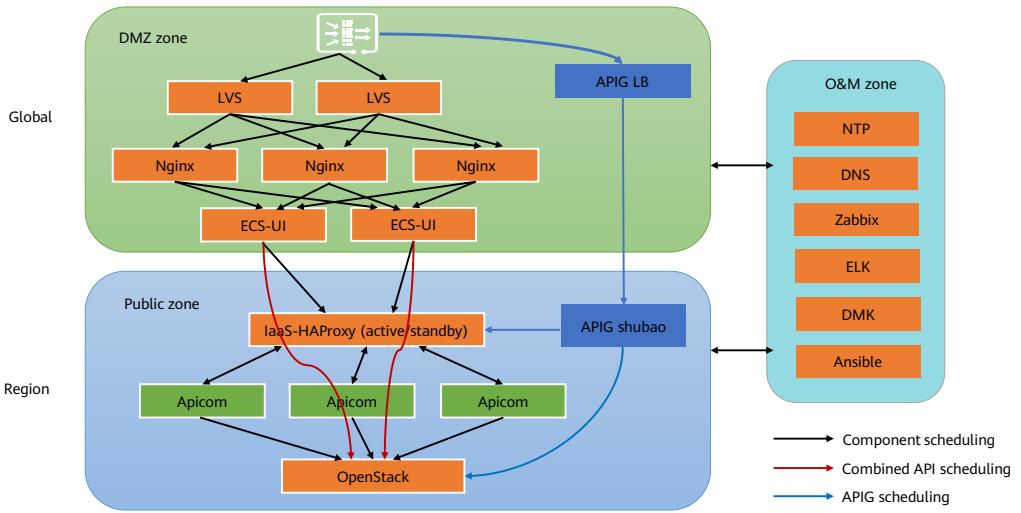
Name	Host ID	Host Group	Availability Z...	Status	Power Status	Flavor	CPU Archite...	IP Address	Batch Cold ...	Batch Live Migration
APIGWZK-03	4C85ED33-2...	manage-aggr	manage-az	Running	Running	2vCPUs 4GB	X86/intel	10.200.16.16	Supported	Supported
APIGWZK-02	5784ED33-25...	manage-aggr	manage-az	Running	Running	2vCPUs 4GB	X86/intel	10.200.16.15	Supported	Supported
APIGWZK-01	8184ED33-25...	manage-aggr	manage-az	Running	Running	2vCPUs 4GB	X86/intel	10.200.16.14	Supported	Supported
APIGWLB-02	8184ED33-25...	manage-aggr	manage-az	Running	Running	2vCPUs 2GB	X86/intel	10.200.5.9	Supported	Supported
APIGWLB-01	8F84ED33-25...	manage-aggr	manage-az	Running	Running	2vCPUs 2GB	X86/intel	10.200.5.8	Supported	Supported

Combined API

- Combined API provides backend services for ECS, EVS, and VBS. It acts as the server side of the console. As a public service platform, Combined API supports the persistence of cloud service requests, responses, and subtasks. Currently, the following services are hosted: ECS, EVS, VBS, ELB, IMS, VPC, and BMS.
 - Combined API provides the APIs of multiple services.
 - Cloud service applications are sent from cloud service consoles to Combined API. Both the consoles and Combined API need to be authenticated by IAM.
 - Combined API can provide services through APIG.



Position of Combined API in HUAWEI CLOUD Stack



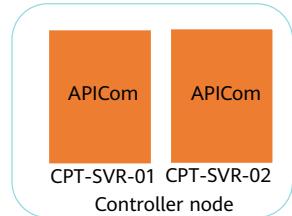
99 Huawei Confidential



- APICom in the green parts indicates Combined API. The frontend ECS UI invokes the Nova component of the backend OpenStack through APICom. The blue parts indicate the components corresponding to APIG described in the previous sections.

Combined API Deployment Mode

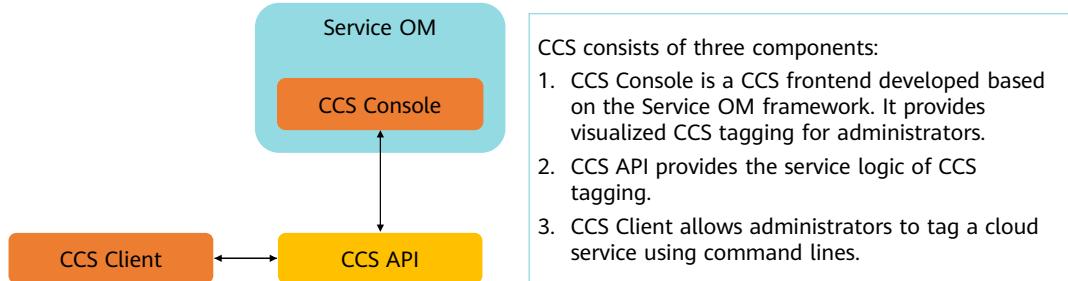
- Combined API (APICom) is deployed on two management VMs: CPT-SVR-01 and CPT-SVR-02 in active/standby mode. These VMs are deployed in one-click mode using HUAWEI CLOUD Stack Deploy without manual intervention. Like other components, the component version is upgraded separately using DMK.
- You can log in to Service OM to view details about CPT-SVR-01 and CPT-SVR-02 management VMs.



Name	Host ID	Host Group	Availability Z...	Status	Power Status	Flavor	CPU Archite...	IP Address	Batch Cold ...	Batch Live Migration
CPT-SRV-02	5784ED33-25...	manage-aggr	manage-az	Running	Running	4vCPUs 10GB	X86/Intel	10.200.16.3	Supported	Supported
CPT-SRV-01	AB84ED33-2...	manage-aggr	manage-az	Running	Running	4vCPUs 10GB	X86/Intel	10.200.16.2	Supported	Supported

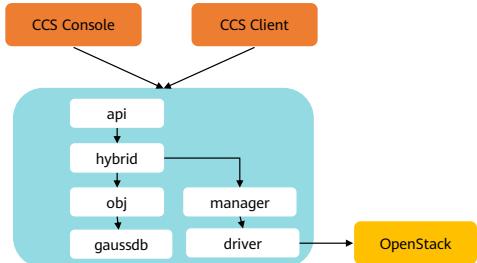
CCS Overview

- In HUAWEI CLOUD Stack, Cloud Configuration Service (CCS) manages tags for cloud regions, AZs, ECS flavors, EVS disk types, and external networks, and allows you to query tags for cloud services such as ECS, EVS, and VPC.



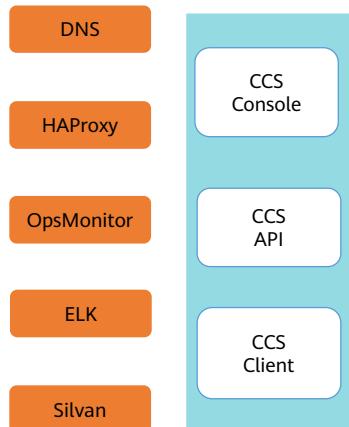
CCS Service Process

- 1. CCS Console or Client delivers tag adding, deletion, modification, and query services.
- 2. The API layer is a RESTful API encapsulated based on WSGI. After receiving the request, the API layer delivers it to the hybrid layer for implementing service functions.
- 3. If a tag is of a cloud region, AZ, ECS flavor, or EVS disk type, it is recorded in the database or queried from the database.
- 4. If a tag is of an external network type, the hybrid layer forwards the tag to the driver layer through the manager layer. The driver layer calls the Neutron API of OpenStack to synchronize external network tags attribute of Neutron with the tag and records the tag in the database.



- Web Server Gateway Interface (WSGI), a simple and universal interface between a Python-defined web server and a web application or framework.

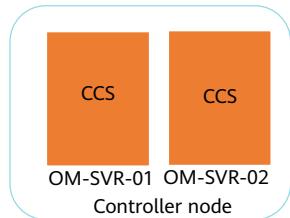
CCS External Dependency



- Domain Name Service (DNS) maps a CCS domain name to a CCS floating IP address.
- HAProxy is used for mapping a CCS floating IP address to a host IP address.
- OpsMonitor monitors the CCS status.
- ELK collects CCS logs.
- CCS domain name is registered with Silvan for query.
- ManageOne ServiceCenter synchronizes AZs through CCS.
- CCS interacts with OpenStack services to provide support for external services.
- When a tenant VM is created using ECS, the resource query API of CCS is called to query related tags.
- EVS queries volume type tags in a specified AZ.
- VPC queries tags in a specified AZ.

CCS Deployment Mode

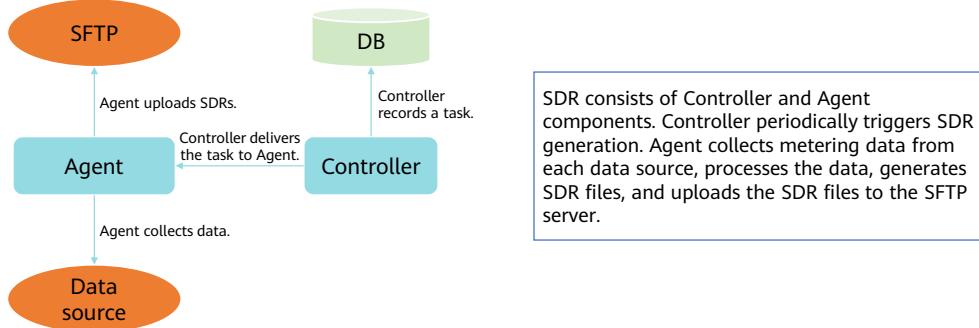
- CCS is deployed together with other cloud services in active/standby mode on OM-SVR01 and OM-SVR02 VMs. GaussDB used by CCS is deployed on PUB-DB-01 and PUB-DB-02 management VMs. These VMs are deployed in one-click mode using HUAWEI CLOUD Stack Deploy without manual intervention.



Name	Host ID	Host Group	Availability Z...	Status	Power Status	Flavor	CPU Archite...	IP Address	Batch Cold ...	Batch Live Migration
OM-SRV-02	1884ED33-25...	manage-aggr	manage-az	Running	Running	4vCPUs 8GB	X86/intel	10.200.16.237	Supported	Supported
OM-SRV-01	8184ED33-25...	manage-aggr	manage-az	Running	Running	4vCPUs 8GB	X86/intel	10.200.16.236	Supported	Supported

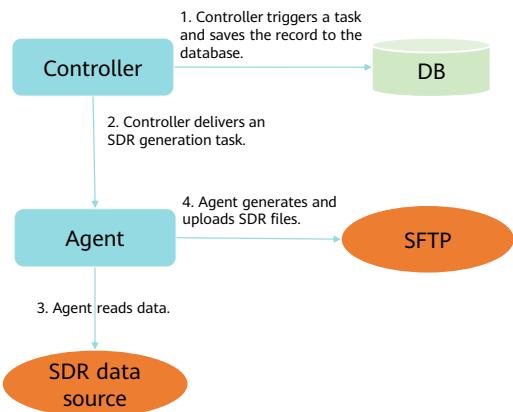
SDR Overview

- Service Detail Record (SDR) is a public component that accurately calculates cloud service resources and generates offline SDR files. These files are collected by the billing system to determine the total bill.
- SDR collects data and uploads SDR files. Each service provides SDR processing logic to generate offline SDR files.

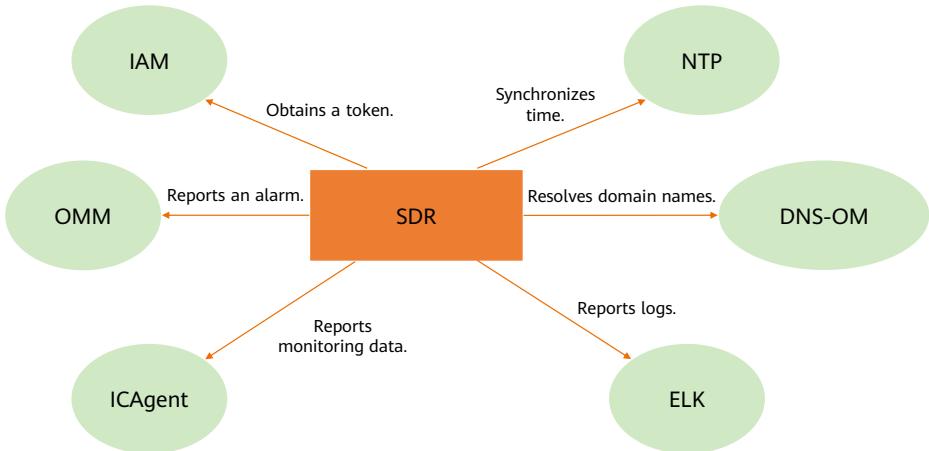


SDR Service Process

- 1. Controller periodically triggers a task and records the task in the database.
- 2. Controller delivers an SDR generation task to Agent.
- 3. Agent collects data from each data source.
- 4. After data collection is complete, SDR files are generated and uploaded to the SFTP server.
- SDR files are uploaded to **/opt/meterfiles/uploads**. Each service has an independent folder for storing SDR files.



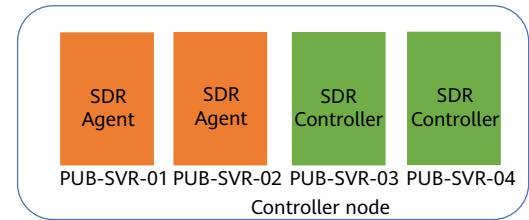
SDR External Dependency



- Identity and Access Management (IAM): ManageOne identity management and access control service
- Operation and Maintenance Management (OMM): an internal management service of ManageOne
- ICAgent: Info Collect Agent, which is installed on a VM on the cloud platform

SDR Deployment Mode

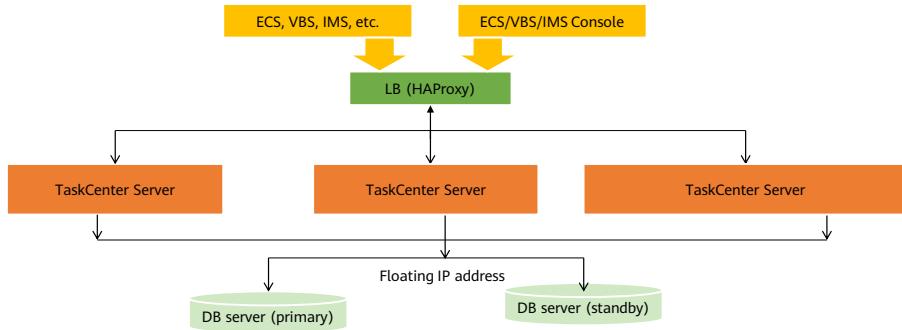
- SDR Controller and Agent nodes are stateless nodes and deployed in 2+2 cluster mode. These nodes use HAProxy for load balancing and are deployed in one-click mode using HUAWEI CLOUD Stack Deploy without manual intervention.
- Agent and Controller are deployed together with other cloud services. Agent is deployed on PUB-SVR01 and PUB-SVR02 nodes, and Controller is deployed on PUB-SVR03 and PUB-SVR04 nodes. GaussDB used by SDR is deployed on PUB-DB-01 and PUB-DB-02 management VMs.



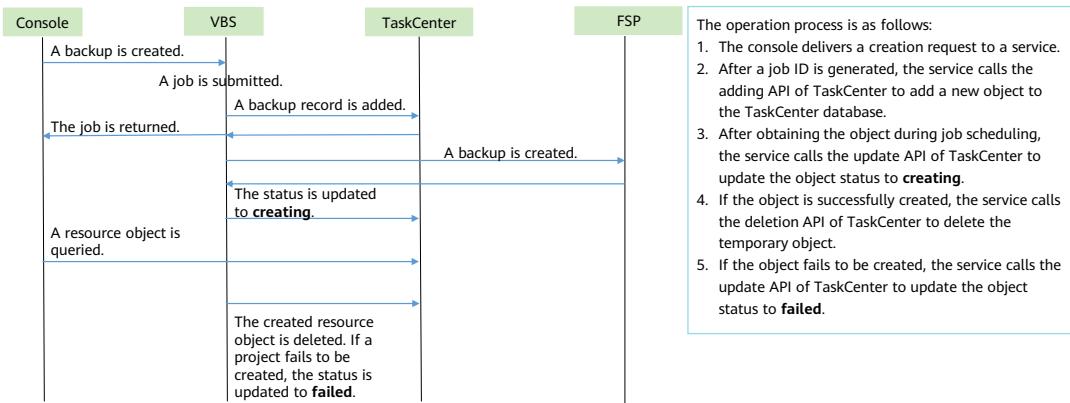
Name	Host ID	Host Group	Availability Z...	Status	Power Status	Flavor	CPU Archite...	IP Address	Batch Cold ...	Batch Live Migration
PUB-SRV-04	B984ED33-25...	manage-aggr	manage-az	Running	Running	4vCPUs 8GB	X86/Intel	10.200.16.233	Supported	Supported
PUB-SRV-03	5784ED33-25...	manage-aggr	manage-az	Running	Running	4vCPUs 8GB	X86/Intel	10.200.16.232	Supported	Supported
PUB-SRV-02	7986ED33-25...	manage-aggr	manage-az	Running	Running	4vCPUs 8GB	X86/Intel	10.200.16.231	Supported	Supported
PUB-SRV-01	9D84ED33-2...	manage-aggr	manage-az	Running	Running	4vCPUs 8GB	X86/Intel	10.200.16.230	Supported	Supported

TaskCenter Overview

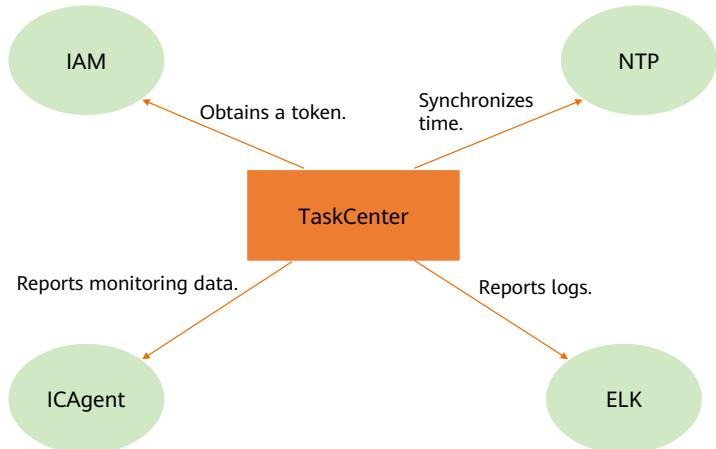
- TaskCenter is a unified task management GUI that allows O&M personnel to register or host tasks for unified management. In addition, TaskCenter allows users to manage periodic resource collection tasks by default and modify their scheduling period.



TaskCenter Service Process

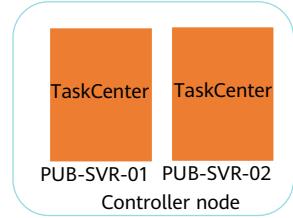


TaskCenter External Dependency



TaskCenter Deployment Mode

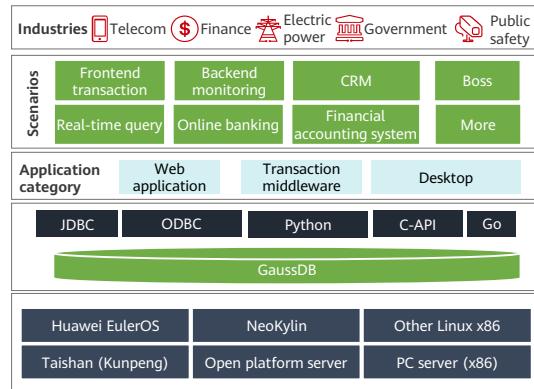
- TaskCenter Service nodes are stateless nodes and deployed in two-node cluster mode. These nodes use HAProxy for load balancing and are deployed in one-click mode using HUAWEI CLOUD Stack Deploy without manual intervention.
- TaskCenter and other cloud services are deployed together on PUB-SVR-01 and PUB-SVR-02 management VMs. GaussDB used by TaskCenter is deployed on PUB-DB-01 and PUB-DB-02 management VMs.



Name	Host ID	Host Group	Availability Z...	Status	Power Status	Flavor	CPU Archite...	IP Address	Batch Cold ...	Batch Live Migration
PUB-SRV-04	B984ED33-25...	manage-aggr	manage-az	Running	Running	4vCPUs 8GB	X86/Intel	10.200.16.233	Supported	Supported
PUB-SRV-03	5784ED33-25...	manage-aggr	manage-az	Running	Running	4vCPUs 8GB	X86/Intel	10.200.16.232	Supported	Supported
PUB-SRV-02	7986ED33-25...	manage-aggr	manage-az	Running	Running	4vCPUs 8GB	X86/Intel	10.200.16.231	Supported	Supported
PUB-SRV-01	9D84ED33-2...	manage-aggr	manage-az	Running	Running	4vCPUs 8GB	X86/Intel	10.200.16.230	Supported	Supported

GaussDB Components

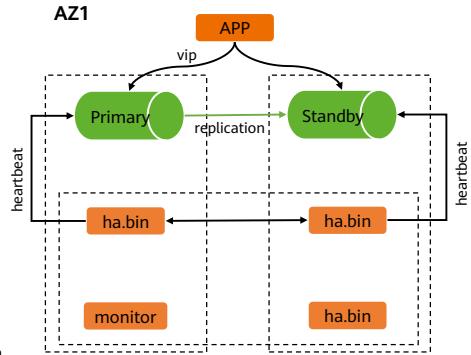
- GaussDB is a Huawei-developed database management system that provides general database management functions. It is developed based on PostgreSQL 9.2 and has enhanced compatibility, performance, security, availability, and maintainability.
- It applies to the following typical applications:
 - Data is mainly inserted, deleted, and queried, and rarely updated.
 - Transactional applications requiring high data integrity.
 - The data size is less than 500 GB.
- HUAWEI CLOUD Stack uses GaussDB as the relational database to store product component data, such as metadata of OpenStack components and data on ManageOne Maintenance Portal and Operation Portal.



- As shown in the architecture diagram, GaussDB can run on EulerOS, NeoKylin, and other Linux OSs, and supports Arm and x86. Applications can access GaussDB in different modes, such as JDBC and ODBC.
 - Java Database Connectivity (JDBC) is an API for the Java programming language that defines how a client may access a database. It provides methods for querying and updating data in a database.
 - Open Database Connectivity (ODBC) is a data access application programming interface (API) that supports access to any data source that can use the ODBC driver.
- Currently, GaussDB has two architectures. OMMHA is used in single-AZ active/standby mode, and DBMHA is used in dual-AZ mode.

GaussDB Deployment Architecture: OMMHA

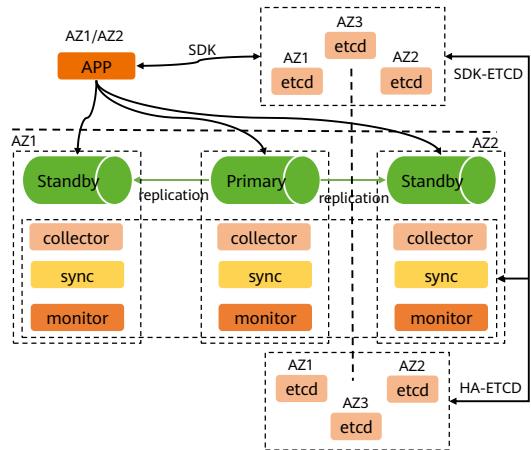
- GaussDB-OMMHA cluster:
 - It is deployed in a single AZ and has two database nodes deployed in active/standby mode.
 - Services access the active node through the floating IP address.
 - If the primary node is faulty, the standby node automatically becomes the primary node and the floating IP address is bound to the new primary node.
- Highlights:
 - The primary/standby structure is simple and reliable.
 - It provides VIP access for external systems.
 - Data is physically replicated from the primary database to the standby database, and the delay is short.
- Disadvantage: Split-brain may occur when the network between nodes is isolated.



- OMMHA consists of monitor and ha.bin components. The monitor component is responsible for handling ha.bin process exceptions. The ha.bin component is responsible for detecting whether the local node is alive and can communicate with the peer ha.bin component. If the local node is not alive or cannot communicate with the peer component, the local node becomes the standby node.

GaussDB Deployment Architecture: DBMHA

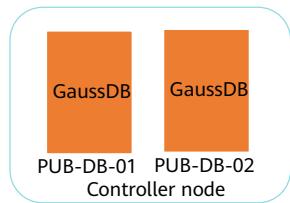
- GaussDB-DBMHA cluster (SDK):
 - One primary and two standby DB nodes are deployed in different AZs. Two nodes (in active/standby mode) are deployed in the active AZ, and one node is deployed in the standby AZ. If the primary node is faulty, services are preferentially switched to the standby node in the same AZ. If both nodes in the active AZ are faulty, services are switched to the standby node in the standby AZ.
 - A service uses the floating IP address to access the primary node through the SDK or uses a local IP address to access the primary and standby nodes (read/write isolation).
 - One set of GaussDB-DBMHA HA can host a maximum of 50 GaussDB DR clusters.
 - If HA-ETCD is unavailable, GaussDB clusters hosted by HA-ETCD are not affected.
- Highlights:
 - Unified HA architecture, three database nodes (one primary node and two standby nodes), distributed arbitration (etcd), and anti-split-brain (avoiding active-active deployment)
 - DR capabilities are provided through the cross-AZ and cross-region deployment.
 - External systems can access the database using VIP or SDK
- Disadvantage: A large number of resources are occupied. (The arbitration etcd and SDK etcd need to be provided.)



- collector, sync, monitor, ha-etcd, and sdk-etcd constitute the DBMHA HA service.
 - collector collects server and database status information and reports the information to ha-etcd for information exchange between databases.
 - sync synchronizes information from ha-etcd to the local host.
 - When ha-etcd is faulty, the cluster can continue to run based on local information without strongly depending on ha-etcd.
 - monitor maintains the information consistency between the database, ha-etcd, and sdk-etcd, monitors the running status of each part, and rectifies exceptions in a timely manner.
 - ha-etcd stores the status information of each component for arbitration.
 - sdk-etcd stores information about the primary and standby database nodes, which is used by service nodes to access correct hosts.

GaussDB Deployment Mode

- In HUAWEI CLOUD Stack, there are public GaussDB and products as well as dedicated GaussDB and products for cloud services, which are deployed in one-click mode using HUAWEI CLOUD Stack Deploy without manual intervention.
- The following uses GaussDB in OMMHA architecture as an example:
 - Public GaussDB is deployed on PUB-DB-01 and PUB-DB-02 management VMs and runs on controller nodes in active/standby mode.
 - Services such as ManageOne, CC, and AS with their own GaussDB databases do not share their GaussDB databases with other components and run on controller nodes in active/standby mode.



Name	Host ID	Host Group	Availability Z...	Status	Power Status	Flavor	CPU Archite...	IP Address	Batch Cold ...	Batch Live Migration
ManageOne-DB02	1884ED33-25...	manage-aggr	manage-az	Running	Running	4vCPUs 14GB	X86/Intel	10.200.16.190	Supported	Supported
ManageOne-DB01	4C85ED33-2...	manage-aggr	manage-az	Running	Running	4vCPUs 14GB	X86/Intel	10.200.16.189	Supported	Supported

Name	Host ID	Host Group	Availability Z...	Status	Power Status	Flavor	CPU Archite...	IP Address	Batch Cold ...	Batch Live Migration
PUB-DB-02	4C85ED33-2...	manage-aggr	manage-az	Running	Running	8vCPUs 8GB	X86/Intel	10.200.16.235	Supported	Supported
PUB-DB-01	7986ED33-25...	manage-aggr	manage-az	Running	Running	8vCPUs 8GB	X86/Intel	10.200.16.234	Supported	Supported

- This course involves only IaaS-layer databases. For details about databases in gPaaS & AI DaaS services, see the HCIE-Cloud Computing courses.

Quiz

1. (Single-answer question) Which of the following components manages tags in HUAWEI CLOUD Stack?
 - A. SDR
 - B. Apicom
 - C. HAProxy
 - D. CCS
2. (Multiple-answer question) An enterprise cloud platform administrator wants to view the performance metrics of Huawei switches in a cloud data center. Which of the following platforms can be used to obtain performance metrics?
 - A. Service OM
 - B. Service Center
 - C. eSight
 - D. Operation Center

- Answers:

- 1. D
 - 2. CD

Summary

- This course describes the following:
 - Challenges and requirements of enterprise digital transformation
 - HUAWEI CLOUD Stack Solution and Architecture
 - HUAWEI CLOUD Stack platform components: FusionSphere OpenStack, ManageOne, eSight, FusionCare, and CloudNetDebug
 - HUAWEI CLOUD Stack common components, including LVS, DNS, NTP, DMK, APIG, Combined API, CCS, SDR, TaskCenter, and GaussDB

Recommendations

- Huawei Talent:
 - <https://e.huawei.com/en/talent/portal/#/>
- Huawei Cerification:
 - <https://forum.huawei.com/enterprise/en/forum-813.html>

Acronyms

Acronym	Full Name	Description
IoE	IBM Oracle EMC	As three IT giants outside China, IBM represents hardware and overall solution service providers, Oracle represents databases, and EMC represents data storage.
BMS	Bare Metal Server	BMS is used to run applications that require high performance on the cloud.
IEF	Intelligent EdgeFabric	IEF is used to manage edge cloud nodes.
ISP	Internet Service Provider	An ISP is a commercial company or organization that provides network access and related services for customers.
API	Application Programming Interface	A particular set of rules and specifications that are used for communication between software programs.
SOA	Service-oriented Architecture	It is a software architecture compared with monolithic and microservice architectures.
CPS	Cloud Provisioning Service	CPS is used for installing HUAWEI CLOUD Stack components and configuring clusters.
UVP	Unified Virtualization Platform	UVP is a server OS in HUAWEI CLOUD Stack, including KVM and EulerOS.
LVM	Logical Volume Manager	LVM is used to manage logical volumes in an OS.
VG	Volume Group	VG is a logical group of hard disks.
SWH	Software Hub	SWH is used by the cloud deployment platform to store software.
AZ	Availability Zone	AZs represent physical areas in HUAWEI CLOUD Stack.
ELK	Elasticsearch, Logstash, Kibana	As a log platform, it is used to collect log data from the service side.
FSM	FusionStorage Manager	It functions as the Huawei distributed storage management platform that allows administrators log in to this platform to perform routine O&M operations.

Thank you.

把数字世界带入每个人、每个家庭、

每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.

Copyright©2022 Huawei Technologies Co., Ltd.
All Rights Reserved.

The information in this document may contain predictive statements including, without limitation, statements regarding the future financial and operating results, future product portfolio, new technology, etc. There are a number of factors that could cause actual results and developments to differ materially from those expressed or implied in the predictive statements. Therefore, such information is provided for reference purpose only and constitutes neither an offer nor an acceptance. Huawei may change the information at any time without notice.



Service OM Resource Management



Foreword

- In HUAWEI CLOUD Stack, resource pools (compute, storage, and network resources) and infrastructure services (ECS, EVS, and VPC) can be managed on Service OM. This course describes how to manage resources on Service OM.

Objectives

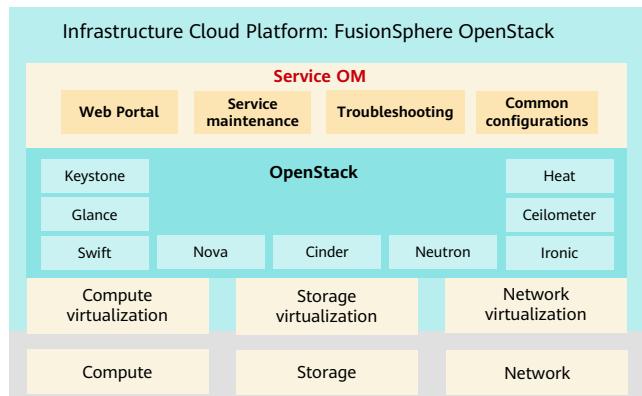
- Upon completion of this course, you will be able to understand:
 - The concept of Service OM.
 - Compute resource management on Service OM.
 - Storage resource management on Service OM.
 - Network resource management on Service OM.

Contents

- 1. Introduction to Service OM**
2. Compute Resource Management on Service OM
3. Storage Resource Management on Service OM
4. Network Resource Management on Service OM

Service OM Overview

- In HUAWEI CLOUD Stack, Service OM is the operation and management page of FusionSphere OpenStack and is a tool for managing resource pools (compute, storage, and network resources) and infrastructure cloud services.



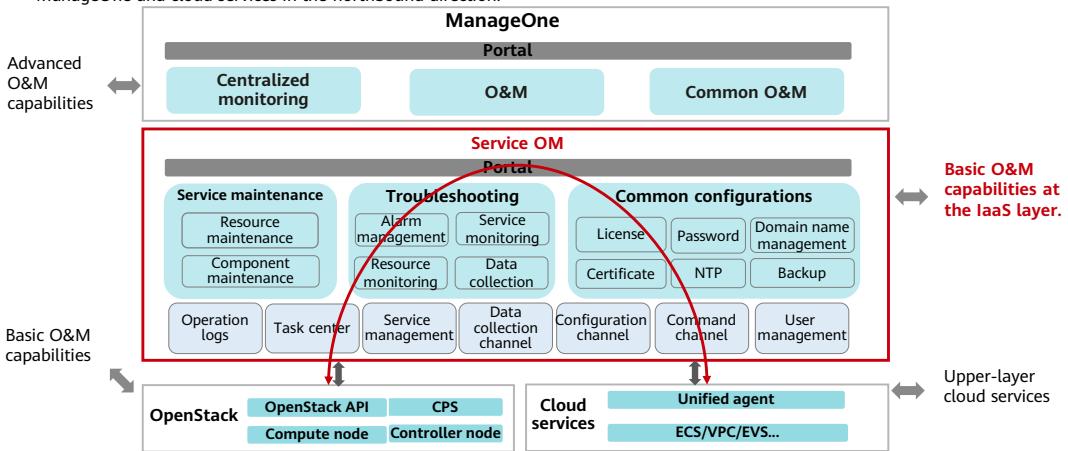
5 Huawei Confidential



- FusionSphere OpenStack OM is the operation and management page of FusionSphere OpenStack. FusionSphere OpenStack OM monitors and manages hardware and software of FusionSphere, supports automatic resource provisioning and automatic infrastructure O&M, and provides a management page for administrators. FusionSphere OpenStack OM is usually installed on VMs managed by FusionSphere OpenStack in active/standby mode.
- In HUAWEI CLOUD Stack 6.3 and later versions, Service OM is used for FusionSphere OpenStack in hybrid or private cloud scenarios, and OpenStack OM is used in NFV scenarios. Service OM helps administrators manage and configure resource pools (such as compute, storage, and network resource pools) and infrastructure cloud services.

Service OM Positioning

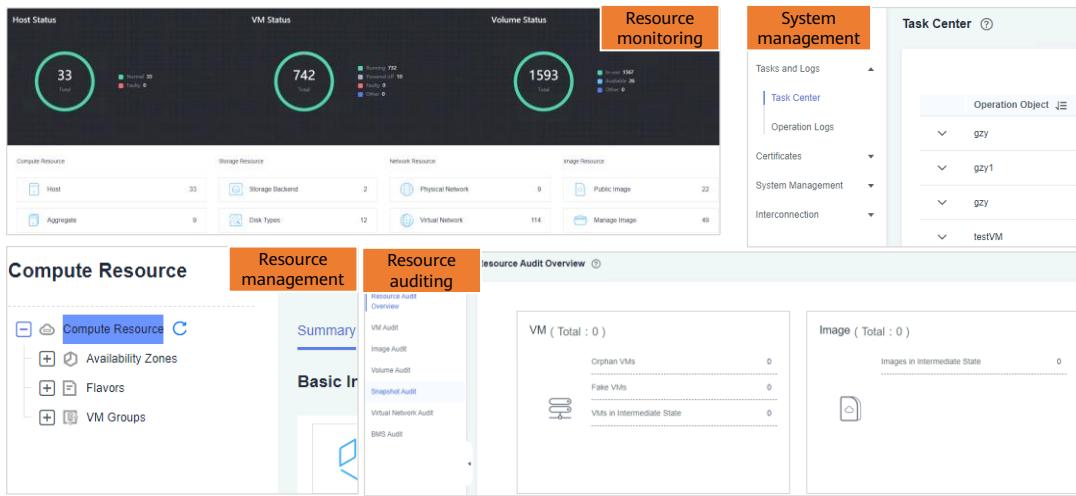
- Service OM interconnects with FusionSphere OpenStack components in the southbound direction and interconnects with ManageOne and cloud services in the northbound direction.



6 Huawei Confidential

- When a user creates and uses a cloud service on ManageOne Operation Portal, the user needs to invoke OpenStack components based on the cloud service configuration on Service OM. Then, OpenStack components allocate underlying resources to complete the task.
- CPS:
 - FusionSphere OpenStack provides basic O&M capabilities.
 - Cloud service O&M capabilities rely on the agent mechanism.
- Service OM:
 - Service OM provides basic O&M capabilities at the IaaS layer.
 - It provides overall resource and service O&M capabilities, such as configuration, operation, monitoring, troubleshooting, and information collection.
 - It provides a unified entry for IaaS public O&M capabilities.
- ManageOne:
 - ManageOne provides advanced O&M capabilities.
 - It allows data center monitoring personnel to centrally monitor different products, and demarcate and rectify faults.
 - ManageOne also offers comprehensive analysis capabilities for cloud system management personnel to perform better planning and design.
 - It provides a unified entry for HUAWEI CLOUD Stack public O&M capabilities.

Service OM Functions



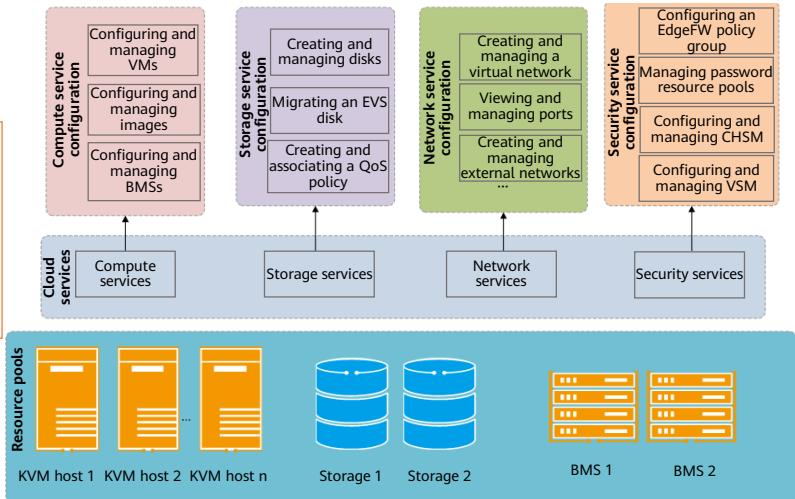
7 Huawei Confidential



- Service OM provides the following functions:
 - Resource monitoring: Service OM monitors the status of hosts, VMs, and disks, and records the number of resources (including compute, storage, network, and image resources) in a resource pool.
 - Resource management: Service OM helps you manage infrastructure resources (including compute, storage, network, image, and BMS resources). For example, you can create, delete, and modify resources. If gPaaS and AI DaaS services are deployed at a site, you can also manage gPaaS and AI DaaS resources. However, the management of gPaaS and AI DaaS resources is not involved in this course.
 - Resource auditing: On the FusionSphere OpenStack cloud platform, the system reports an alarm if problems such as residual resources and unavailable resources occur due to unexpected system failures (such as host reboot and process restart) or backup recovery. To improve maintenance efficiency, FusionSphere OpenStack collects audit items related to frequently reported alarms. You can view and handle audit items on Service OM to ensure normal service running. Resources that can be audited include VMs, images, volumes, snapshots, virtual networks, and BMSs.
 - System management: includes tasks and logs, users and certificates, system management, and interconnection.

Service OM Logical Architecture

Service OM helps you configure and manage compute, storage, security, and network services to provide reliable compute, storage, network, and security resources for tenant services.



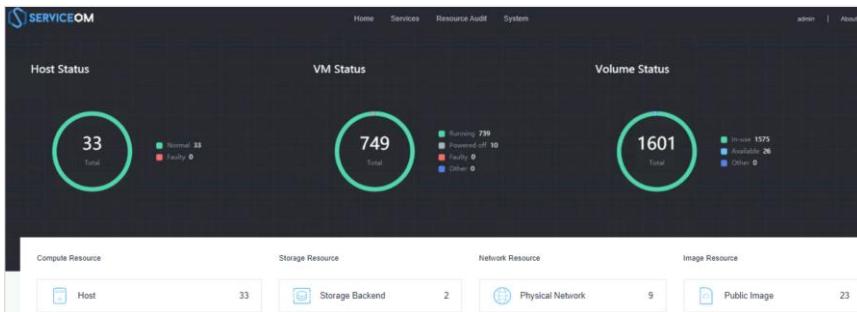
8 Huawei Confidential



- The logical structure of cloud service resource management is divided into three layers: resource pool layer, cloud service layer, and cloud service configuration layer from bottom to top. The cloud service configuration layer consists of compute, storage, network, and security resource configuration. In HUAWEI CLOUD Stack 8.X, KVM is usually used as a compute resource pool. On Service OM, administrators can configure and manage VMs, storage services, network services, and security services to provide reliable compute, storage, network, and security resources for tenants.
- A cloud-hosted hardware security module (CloudHSM or CHSM) is a cryptographic device that provides cryptographic services for application systems of multiple tenants through networks by using virtualization technologies in a cloud computing environment.
- A virtual security module (VSM) is a cryptographic service instance that is created on a CloudHSM using virtualization technologies and provides similar services as a CloudHSM.
- BMS management: BMSs are used to provision compute instances that have high performance requirements, for example, to deploy database applications, or to provision dedicated physical servers. A BMS is a physical server without an OS installed before instance deployment. It provides physical resources for creating compute instances. You can perform routine management and maintenance of the BMS in the configuration center, ensuring that the instance services deployed on the BMS are running properly.
- For details about compute, network, and storage service configurations, see the following slides.

Service OM Login

- Log in to ManageOne Maintenance Portal. In the **Common Links** area in the lower right corner of the homepage, click **Service OM**. The Service OM page (SSO) is then displayed.



- SSO: Single Sign-On

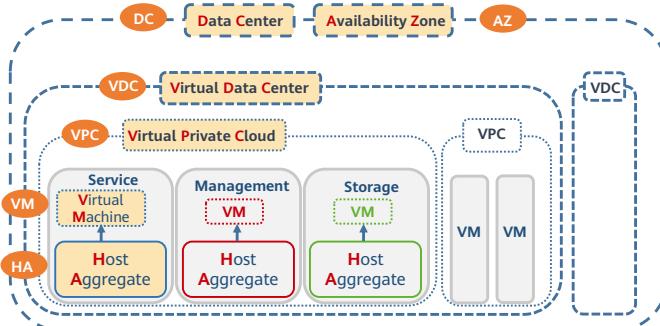
Contents

1. Introduction to Service OM
- 2. Compute Resource Management on Service OM**
3. Storage Resource Management on Service OM
4. Network Resource Management on Service OM

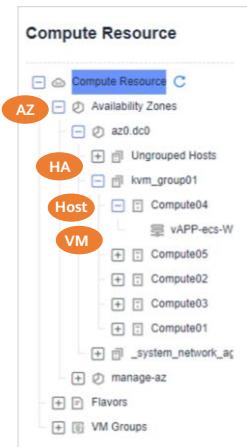
- Tenants can use cloud service resources such as ECSs, BMSs, and value-added services such as AS and IMS only after these resources are configured on Service OM. This section uses the configuration required for creating ECSs as an example.

Compute Resource Model

- Administrators can view and manage all compute resources managed in AZs on Service OM.



11 Huawei Confidential



- A data center (DC) is a physical data center.
- An availability zone (AZ) is a logical zone of physical resources, including compute, storage, and network resources. Regions are geographically diverse and provide the highest isolation level among other isolation methods in the figure. An AZ provides lower isolation level than a geographical region. A geographic region can contain multiple AZs. AZs are physically isolated from each other. The failure of one AZ does not affect other AZs. Theoretically, AZs can be deployed across DCs, but DCs must be interconnected through a high-speed network.
- A virtual data center (VDC) is a virtual resource pool consisting of compute, network, and storage resources. It provides resources for users to deploy applications. Resources in different VDCs are isolated from each other.
- A Virtual Private Cloud (VPC) is a secure, isolated, and logical network environment. It has an independent IP address space and is isolated from other VM networks that are not in the VPC.

- A host group, a logical group in FusionSphere OpenStack, consists of a group of physical hosts and related metadata. A host group consists of a group of compute servers with the same hardware configuration and is logically divided by the administrator in the system. On Service OM, a host group is a combination of hosts of the same virtualization type. You are advised to put hosts providing the same type of resources into the same group, facilitating flavor creation and maintenance.
- A host is a node providing compute capabilities in FusionSphere OpenStack. It consists of one or more physical servers, which run virtualization software to offer users with services, such as ECS. You can perform routine management and maintenance for hosts in the configuration center, ensuring that the VM services deployed on the host are running properly.
- Host group management: After creating a host group and determining its AZ and member hosts, you can use the hosts in the host group to create VMs. The tags configured for a host group can apply to VM flavors. When such VM flavors are used to create VMs, the system selects only the hosts that fully meet the tag requirements in the host group to create VMs.
- Compute instances on Service OM include VM resources and BMS resources. This section uses VM resources as an example to describe compute resource management. An AZ can contain multiple host groups, a host group can contain multiple hosts, and multiple VMs can be created on a host. Tenants can log in to ManageOne Operation Portal as a VDC administrator or VDC operator and create compute instances such as ECSs in VPCs. These VMs are created on hosts. Administrators can create a host group based on the virtualization type and add qualified hosts to the host group.

Compute Resource Overview on Service OM

- Service OM manages the configurations of compute resources, including images, BMSs, VMs, and hosts. You can click **Compute Resource** in the service list to configure and manage VMs and hosts, **Image Resource** to configure and manage images, and **Bare Metal Resource** to configure and manage BMS instances.

The screenshot shows the Service OM interface. On the left, there's a sidebar with categories like Services, Resource Audit, Resource (with Compute Resource highlighted), Storage Resource, Network Resource, Image Resource (highlighted), Bare Metal Resource, Enterprise Application, ROMA Connect-MQS, ROMA Connect-Server&Link, ROMA Connect-FDI, and ROMA Connect-APIC. The main area is titled 'Compute Resource' and has tabs for Summary (selected), Configuration, Host Groups, Hosts, VMs, Flavors, and VM Groups. It features icons for Availability Zones, Host Groups, VMs, and Hosts, each with a count: 3, 9, 749, and 33 respectively. A blue thought bubble contains the text: "Which compute-related resources need to be prepared before ECS provisioning? What are the functions of a VM group?" At the bottom left, it says "13 Huawei Confidential". The HUAWEI logo is at the bottom right.

- Before provisioning cloud service ECSs, administrators need to configure flavors and images on Service OM. Scheduling policies between VMs can be managed by VM groups.
- The following sections provide more information about these issues.

Key Concept: Host Group

- ECSs are divided into general-purpose ECSs, GPU ECSs, and USB-passthrough ECSs based on their flavors, such as CPUs and memory. A host group is a group of hosts of the same virtualization type. Host groups are also divided into general-purpose host groups, GPU host groups, and other types of host groups, just like ECSs. When you create an ECS, the system will find a host group whose resource type matches the resource type of the ECS, and then create the ECS.
- When creating a host group, you need to specify the host group name, AZ, member hosts, and resource types.

The screenshot shows the 'Compute Resource' interface with the 'Host Groups' tab selected. At the top, there are four buttons: '+ Create Host Group', '+ Create VM', '+ Create Flavor', and '+ Create VM Group'. Below the tabs, there are filters for 'All availability zones', 'All vendors', and 'Name', along with a 'Fuzzy search' field and a clear button. The main table lists two host groups:

Name	Host Gro...	Availabil...	Hosts	Used/Tot...	Allocate...	Allocate...	CPU Ven...	Operation
manage...	e6b3962...	manage-az	10	22...	50...	52...	Intel	Delete
kvm_gro...	c27669e...	az0 dc0	3	17...	86...	0/6	Intel	Delete

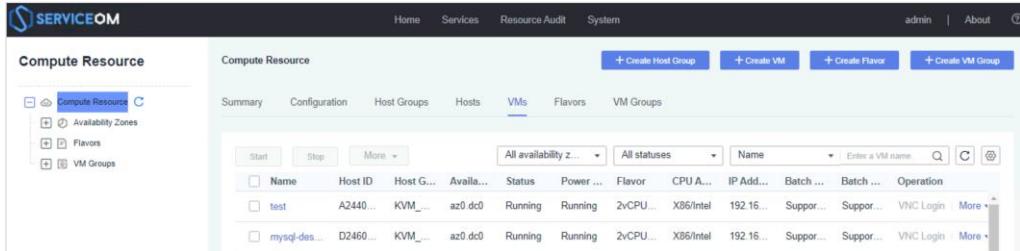
Key Concept: Host

- On Service OM, you can manage hosts that have been added to a cluster. For example, you can isolate, safely restart, and safely power off hosts, and view hardware details of hosts.
- If you want to add hosts to a cluster, you need to log in to the FusionSphere OpenStack web client, not Service OM.

The screenshot shows the FusionSphere Cloud Provisioning Service interface. At the top, there is a navigation bar with links for Home, Services, Resource Audit, System, and buttons for +Create Host Group, +Create VM, +Create Flavor, and +Create VM Group. Below the navigation bar is a search bar with dropdowns for filters like Availability Zones, Service Status, Isolation Status, Host Groups, Vendors, and Name, along with an 'Enter Host Name' input field and a search icon. The main content area has tabs for Compute Resource (selected), Summary, Configuration, Host Groups, Hosts (selected), VMs, Flavors, and VM Groups. Under the Compute Resource tab, there is a sidebar with options for Compute Resource, Availability Zones, Flavors, and VM Groups. The main panel displays a table titled 'Capacity Expansion' with a header row containing columns for PXE Boot Hosts, Wait for IP, Data, Host ID, and several host-related fields (Host IP, MAC Address, IP, BMC IP, CPU, Status). The 'Capacity Expansion' tab is highlighted in blue.

Key Concept: VM

- On Service OM, you can manage lifecycles of management VMs, migrate VMs, and view VM details.
- When using HUAWEI CLOUD Stack to provision VMs, you need to use the ECS service on ManageOne Operation Portal to create VMs. Created VMs cannot be deleted on Service OM.
- When creating an ECS image, you can create a VM on Service OM, install UVP VMTools and Cloud-Init, and then create an image.

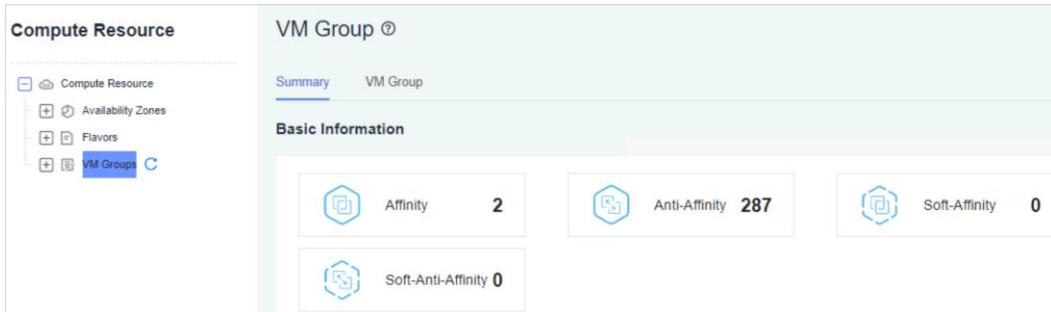


The screenshot shows the Service OM interface for managing Compute Resources. The left sidebar has a tree view with 'Compute Resource' selected, under which 'Availability Zones', 'Flavors', and 'VM Groups' are listed. The main area is titled 'Compute Resource' and contains tabs for 'Summary', 'Configuration', 'Host Groups', 'Hosts', 'VMs' (which is selected), 'Flavors', and 'VM Groups'. Below these tabs is a search bar with filters for 'Start', 'Stop', 'More', 'All availability z...', 'All statuses', 'Name', and 'Enter a VM name'. A table lists two VM entries: 'test' and 'mysql-des...'. The 'test' VM has columns: Name (test), Host ID (A2440...), Host G... (KVM...), Availa... (az0 dc0), Status (Running), Power ... (Running), Flavor (2vCPU... X86/Intel), CPU A... (192.16...), IP Add... (Support...), Batch ... (Support...), Batch ... (Support...), and Operation (VNC Login, More). The 'mysql-des...' VM has similar columns.

Name	Host ID	Host G...	Availa...	Status	Power ...	Flavor	CPU A...	IP Add...	Batch ...	Batch ...	Operation
test	A2440...	KVM...	az0 dc0	Running	Running	2vCPU... X86/Intel	192.16...	Support...	Support...	Support...	VNC Login / More
mysql-des...	D2460...	KVM...	az0 dc0	Running	Running	2vCPU... X86/Intel	192.16...	Support...	Support...	Support...	VNC Login / More

Key Concept: VM Group

- A VM group allows you to configure the policy used for scheduling VMs in the group. During VM creation, you can specify a VM group for the VM. Based on the VM group policy, the system can define the policy used for scheduling VMs in the VM group.



17 Huawei Confidential



- There are four types of VM groups: anti-affinity, affinity, soft-anti-affinity, and soft-affinity:
- Anti-affinity: VMs in the same VM group must reside on different hosts. To create a VM in a specified anti-affinity VM group, the VM cannot be created on the same host where another VM (if any) in the VM group resides. Otherwise, the VM fails to be created. After the VM is created, the anti-affinity policy becomes invalid when VM migration is performed.
- Affinity: The VMs in the same VM group must all run on the same host. When you create a VM by assigning it to an affinity VM group, you do not need to specify a host for the VM if the VM group already contains other VMs. The system automatically selects a host that meets the affinity policy to create the VM. After the VM is created, the affinity policy becomes invalid when VM migration is performed.
- Soft-anti-affinity: During VM scheduling, the host weight is calculated based on the soft-anti-affinity and memory. If host resources are sufficient, VMs in the same soft-anti-affinity group will not be allocated to the same host. If resources are insufficient or the value of **Randomly select the number of hosts during VM scheduling** for Nova is greater than 1, anti-affinity rules may be overridden.
- Soft-affinity: During VM scheduling, the host weight is calculated based on the soft-affinity and memory. If host resources are sufficient, VMs in the same soft-affinity group will be scheduled to the same host. If resources are insufficient or the value of **Randomly select the number of hosts during VM scheduling** for Nova is greater than 1, affinity rules may be overridden.

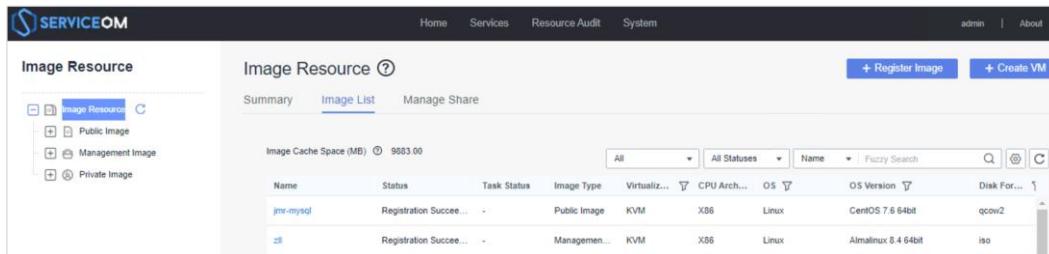
Key Concept: Flavor

- Before creating an ECS, you need to create a flavor for the ECS on Service OM. The ECS flavor contains **vCPUs**, **Memory**, **ECS Type**, and **Flavor Name** on the **Create ECS** page.
- When creating a flavor, you can configure the number of vCPUs, memory size, and resource type, and use host groups to meet different performance requirements. This can also help standardize the resource usage of compute instances in the system.

Name	Type	Boot De...	vCPUs	Memory ...	Disk (GB)	CPU A...	CPU V...	Flavor...	Resourc...	Cust...	Operation
zli	VM	Cloud disk	2	16384	--	X86	Intel	Non-pred...	General-...	trust...	Delete
csje_ykg	VM	Cloud disk	2	4096	--	X86	Intel	Non-pred...	General-...	trust...	Delete

Key Concept: Image

- An image is a backup of a VM, including an OS and application software. It is used to provision VMs and applications. Image configuration management on Service OM includes image registration, image management, and sharing management.



The screenshot shows the Service OM web interface. At the top, there is a navigation bar with links for Home, Services, Resource Audit, System, and user admin. Below the navigation bar is a sidebar titled "Image Resource" containing categories: Image Resource (selected), Public Image, Management Image, and Private Image. The main content area is titled "Image Resource" and displays a table of registered images. The table has columns for Name, Status, Task Status, Image Type, Virtualiz..., CPU Arch..., OS, OS Version, Disk For..., and a small thumbnail icon. Two rows are visible: one for "jne-mysql" (Public Image, KVM, X86, Linux, CentOS 7.6 64bit, qcow2) and another for "zli" (Management Image, KVM, X86, Linux, Almalinux 8.4 64bit, iso). At the bottom right of the main content area, there are buttons for "+ Register Image" and "+ Create VM".

- Public images are standard images, including the common standard OS and preinstalled public applications, provided by the cloud platform system. Public images are visible to all users and are easy to manage. You can conveniently use a public image to create an ECS or BMS.
- Management images are created by administrators used only by O&M personnel to create VMs. They are invisible to tenants on ManageOne Operation Portal.
- Private images created based on ECSs or external image files are visible only to users who create them. Private images include OSs, preinstalled public applications, user's private applications, and user's service data.
- You need to upload the created image files to the specified storage directory and register the images. The registered image can be used to create compute instances. The system administrator or O&M personnel can register an image on Service OM.
- On Service OM, you can download, modify, and upload images (public images or management images).
- You can set the folder where the image file is stored on the local PC as a shared folder to share the local image with other users. You can also take a note of the shared path, username, and password of the image file.

Preparing Compute Resources Before Provisioning ECS

- Creating a host group



- Configuring ECS flavors



- Creating a public image for an ECS



Registering an image

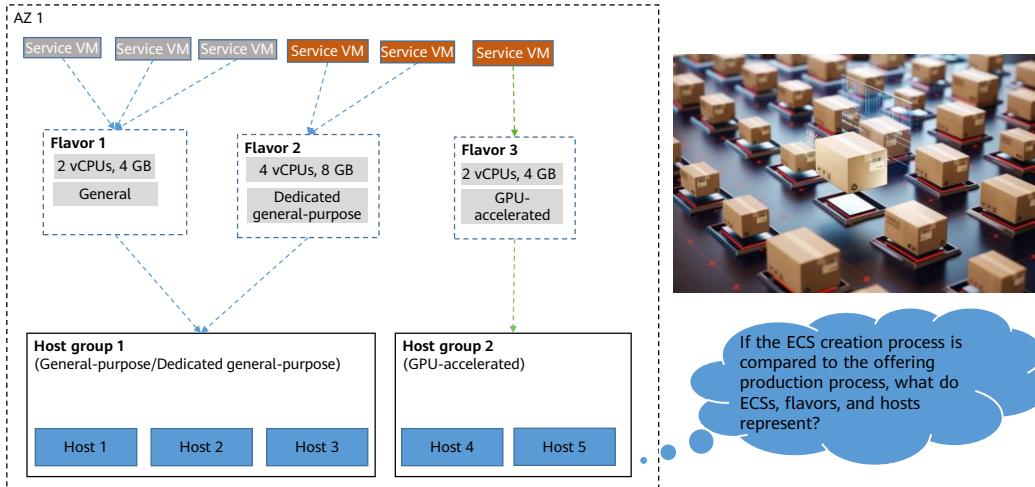


Creating an image

What are the differences between image registration and image creation?

- Before creating an ECS, the administrator needs to configure the ECS flavor and image.
- Before using an image to create a compute instance, you must register the image. Registering images is to upload the created image files to the specified storage directory and register the images. The registered image can be used to create compute instances. The system administrator or O&M personnel can register an image on Service OM. Administrators can find the required public image in the image list after registering the image, synchronize the image, and download the created image. If an administrator needs to install software on the original image and then create another image, the administrator can use the registered image to create a VM, install the required software, and use the VM to create an image.

Relationships Between ECSs, Flavors, and Hosts



- Host group: A host group is a logical group of hosts using the same virtualization type. For example, there are general-purpose and GPU-accelerated host groups.
- Flavor: When requesting an ECS on ManageOne, you need to select a flavor for the ECS. The ECS flavor includes ECS types, vCPUs, and memory.
- If the ECS is regarded as a product, the flavors are similar to the size of the product designed by the designer, the image is similar to the standard production mold, the host group is a different production line, and the host in the host group is the machine that produces the product.

Contents

1. Introduction to Service OM
2. Compute Resource Management on Service OM
- 3. Storage Resource Management on Service OM**
4. Network Resource Management on Service OM

Service OM Storage Resource Overview

- Service OM provides storage resources for EVSs. You can select a disk type for Service OM on the EVS creation page.

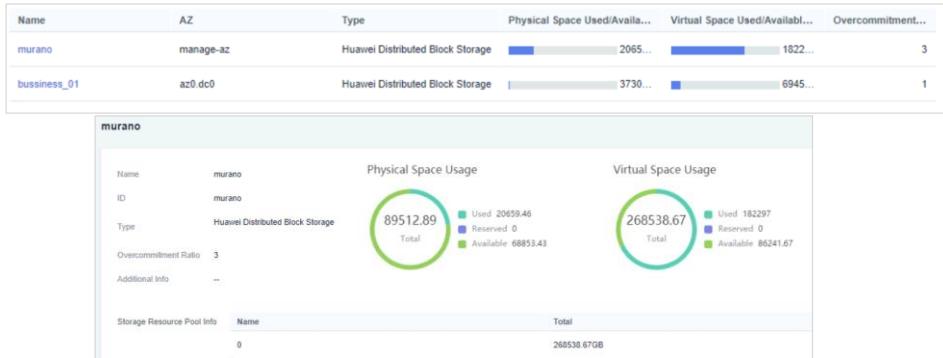
The screenshot shows the Service OM Storage Resource Overview interface. On the left is a sidebar with a tree view of storage resources: Storage Resource (selected), AZ, Storage Backend, Disk Types, Disks, QoS, and Disk Migration. The main area has tabs: Overview (selected), Storage Backend, Disk Types, and Disks. Under Storage Backend, there's a 'Basic Info' section with icons for Availability Zone (2), Storage Backend (2), Disk Types (12), and Disks (1601). Below this are sections for Physical Capacity (Physical Capacity 24386.32GB / Total 841559.75GB) and Virtual Capacity (Used 251749GB / Total 1020585.53GB). At the top right are buttons for '+ Create Disk Type' and '+ Create Disk'.

Which of the following storage-related resources need to be prepared before EVS provisioning? What functions are provided by QoS and disk migration?

- Administrators need to create a disk type for a storage backend. Tenants can select a disk type to create an EVS disk.

Key Concept: Storage Backend (1)

- A storage backend is a logical storage device that stores EVS disk resources. A storage backend device contains one or more storage pools on a storage array (Huawei Distributed Block Storage, Huawei SAN storage, or heterogeneous storage).
- Service OM allows you to view storage backend details.



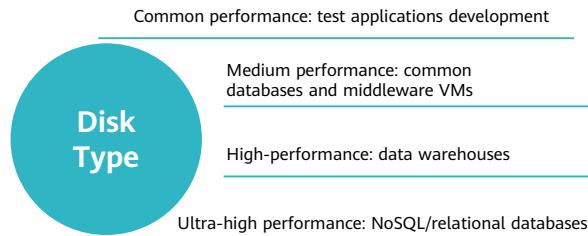
Key Concept: Storage Backend (2)

- To add new storage backend to a cluster, log in to the FusionSphere OpenStack web client, instead of Service OM.

The image shows two screenshots of the FusionSphere OpenStack web client. The left screenshot displays the 'Cluster Management' page with a 'Storage Cluster' section containing two HUAWEI Cinder backends (cinder-lvm01 and cinder-lvm02) and a '+' icon for adding more. The right screenshot is a detailed configuration dialog titled 'Configure Storage Cluster' under 'Configure Parameter'. It includes fields for 'Storage Type' (Huawei Distributed ...), 'Storage Backend Name' (murano), 'AZ' (manage+az), 'Storage Backend Configuration' (Storage Backend Name: murano), and 'General Configuration' (Floating IP Address: 10.200.16.153, Block Storage Client Management IP Address: 10.200.17.53, 10.200.17.1).

Key Concept: Disk Type

- You can select a disk type when creating an EVS disk. A disk type corresponds to a storage backend device for a group of disks. You can divide types of EVS disks based on storage backend types to meet different performance requirements.

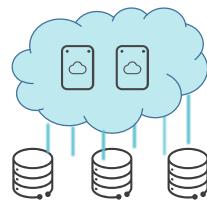


- Based on performance differences of storage backend used by disks, typical disk types and their application scenarios are as follows:
 - Common performance: EVS disks of this type are suitable for scenarios that require large capacity and low read/write rate, and have a small volume of transactions, such as the scenario for developing test applications.
 - Medium performance: EVS disks of this type are suitable for scenarios that require common performance but rich enterprise-class features. They can be used in common databases, application VMs, and middleware VMs.
 - High performance: EVS disks of this type are suitable for scenarios that require high performance, fast read and write speed, and large throughput, such as data warehouses.
 - Ultra-high performance: EVS disks of this type are suitable for data-intensive scenarios that require very high I/O performance, such as NoSQL and relational databases.

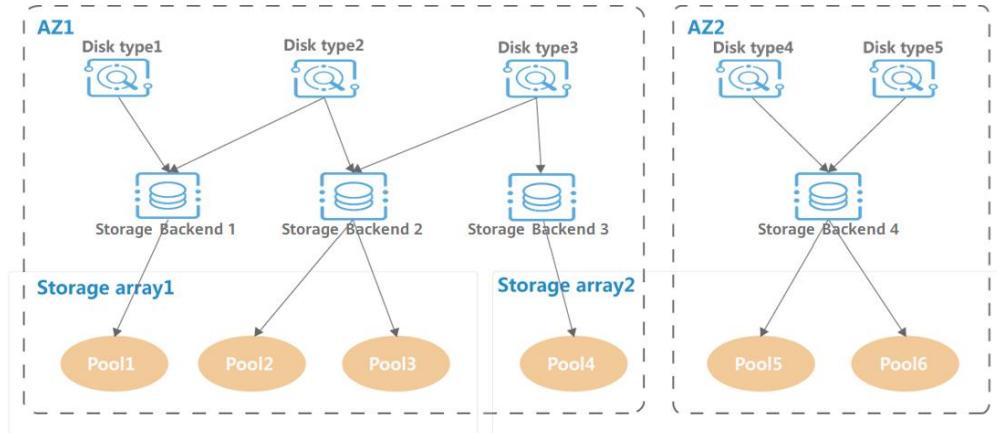
Key Concept: Disk

- A disk is the main storage medium of a computer. It is a storage device that uses the magnetic recording technology to store data. You can create a disk on Service OM and mount it to a management VM. EVS disks created by tenants are displayed on the **Disks** page of Service OM.
- On Service OM, you can create, modify, mount, migrate, and delete disks. You can also view disks created by the EVS service on ManageOne Operation Portal but cannot perform operations on them.

All Availability Zones			
Name	Status	Capacit...	Disk Types
test-volume-0...	In-use	40	CSJC_jmr
mysql-dest-vo...	In-use	40	CSJC_jmr



Relationship Between Disk Type, Storage Backend, and Storage Array



- A storage array may belong to different AZs. For example, Pool4 on Storage array2 belongs to AZ1 while Pool5 and Pool6 belong to AZ2.
- A storage backend device belongs to only one AZ.
- A storage pool belongs to only one storage backend device.
- A disk type belongs to only one AZ.
- A storage backend device can contain one or more storage pools, but the storage pools must be on the same storage array, for example, storage backend 2.
- A disk type can contain multiple storage backends from the same AZ. The storage backends can be on the same or different storage arrays in the same AZ.
- Multiple disk types can be created for a storage backend device, for example, storage backend 1. Different disk types can be configured with different value-added features, such as SmartThin, SmartTier, and SmartDedupe.

Key Concept: QoS

- QoS can meet the specific performance requirements of some services. It applies to scenarios with clear performance requirements. QoS restricts the maximum traffic (IOPS or bandwidth) or available resources (I/O priority) of edge services to ensure the performance of critical services. After a QoS policy is created and associated with a disk type, the QoS policy can be applied to disks provisioned using the disk type.

Create QoS Policy

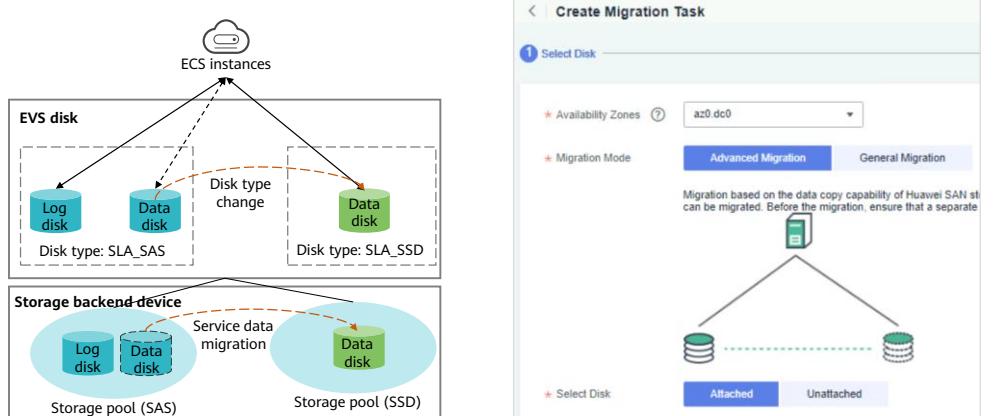
Name	<input type="text" value="zhangsan"/>
IOPS Upper Limit	<input type="text"/>
Max IOPS Upper Limit	<input type="text" value="40"/>
Min IOPS Upper Limit	<input type="text"/>
Bandwidth Upper Limit (MB/s)	<input type="text"/>
Max Bandwidth Upper Limit	<input type="text" value="40"/>
Min Bandwidth Upper Limit	<input type="text"/>
I/O Priority	<input type="checkbox"/> Enable

Confirm **Cancel**



Key Concept: Disk Migration

- Disk migration ensures that disks can be migrated within a storage array or between storage arrays in the same AZ without interrupting services to precisely match service requirements.



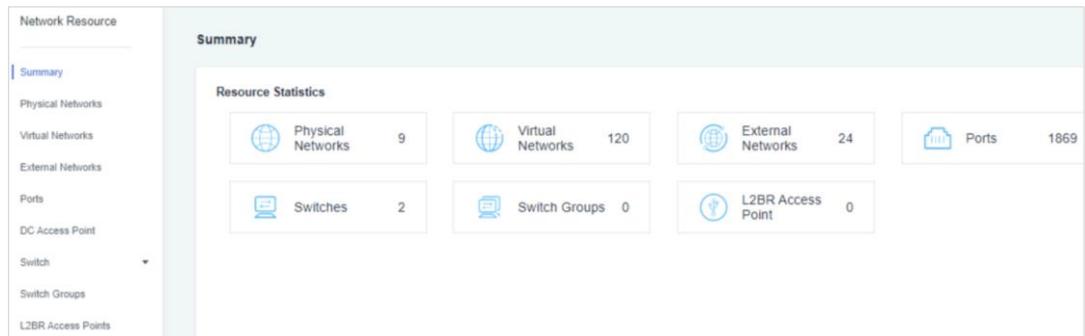
- The preceding figure shows the implementation principle of changing the disk type. In the figure, two disks are attached to an instance. One of the disks serves as a log disk, and the other serves as a data disk. The original type of the two disks is SLA_SAS. The data disk requires high service performance. Therefore, disks with higher performance are required to carry services. The disk type of the data disk is changed from SLA_SAS to SLA SSD, seamlessly migrating service data to a disk of the target disk type. The storage backend device performs service data migration. After service data migration, the system automatically attaches the destination disk to the instance, without service interruption. In addition, the source disk will be deleted to release storage resources for other services.
- Advanced migration:** The migration is performed based on the data copy capability of Huawei SAN storage devices. It applies only to scenarios where Huawei SAN storage is used and efficient batch migration is required. Attached, unattached, and shared disks can be migrated using this mode. Before the migration, ensure that a separate storage link has been configured between the source storage backend where the disks reside and the target storage backend.
- General migration:** The migration is implemented based on the data copy capability of compute hosts and applies to scenarios where Huawei SAN storage, Huawei Distributed Block Storage, or third-party SAN storage is used. As data copy requires compute host resources, this mode can be used only when a small number of disks need to be migrated. It does not apply to storage device replacement. Shared disks cannot be supported. SCSI disks can be migrated only when the ECSs are shut down.

Contents

1. Introduction to Service OM
2. Compute Resource Management on Service OM
3. Storage Resource Management on Service OM
- 4. Network Resource Management on Service OM**

Service OM Network Resource Overview

- Service OM network resources provide network resources for network cloud services. Administrators can view the numbers of created physical networks, virtual networks, external networks, ports, DC access points, switches, switch device groups, and Layer 2 Bridge (L2BR) access points on Service OM.



32 Huawei Confidential



- An administrator can:
 - View all ports in use, such as ports used by VM NICs and DHCP services. Detect the port status and collect necessary information for troubleshooting VM network faults.
 - Create virtual networks or view, modify, delete, and manage created virtual networks.
 - View physical networks and synchronize cloud configurations of physical networks.
 - Create a DC access point and manage created physical DC resources that are used to carry DC services on the tenant plane.
 - Add switches, view switch information, modify the NETCONF protocol of switches, configure the switch vendor driver, view or modify basic BGP information, and configure BGP peers.
 - Create and manage device groups.
 - Create an L2BR access point and manage the created L2BR resources on the tenant side.

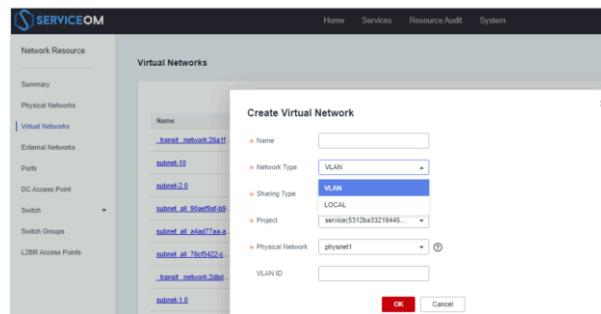
Key Concept: Physical Network

- On Service OM, you can only view physical networks. To create a physical network, choose **Configuration > Network** on the FusionSphere OpenStack web client. After a physical network is added, you must configure NIC mapping so that the physical network can be used on Service OM.

The screenshot shows the Service OM web interface. The top navigation bar includes Home, Services, Resource Audit, and System. On the left, a sidebar lists Network Resource (Summary, Physical Networks, Virtual Networks), Configuration (Summary, Network, Disk, Resource Isolation, Kernel Option, System, OpenStack), and Monitoring (CPU, Memory, Network, Storage). The main content area is titled "Physical Networks". It displays a table with columns Name, VLAN Pool, and Description. One entry is shown: physnet1, 1-4000, default physical network. Below this is a "Network" configuration section with a warning message: "Modifying the configuration of an existing physical network will result in the web page unavailability for a few seconds due to network restart. Exercise caution when Any change in physical network configuration will affect VM traffic. You are advised to perform this operation when no VM is running. Consecutive physical network configuration changes may cause VMs to be stuck in the ERROR state. Exercise caution when performing this operation." A sub-table titled "Configure Physical Network" shows an entry: enat-dpdk, 1 ~ 4000. The HUAWEI logo is in the bottom right corner.

Key Concept: Virtual Network

- A virtual network must be carried on a physical network. Virtual networks can be created on Service OM. Each subnet added to the VPC service on ManageOne Operation Portal automatically generates a virtual network. In this case, you can view but cannot modify virtual networks on Service OM.
- There are two types of virtual networks: VLAN and LOCAL.
 - VLAN: indicates a network with a VLAN ID. The network can be mapped to a physical network. Multiple virtual networks of the VLAN type can be created on a physical network.
 - LOCAL: indicates a local virtual network. Packets of VMs created on this network cannot access physical networks.



Key Concept: External Network

- An external network is used to connect to networks outside the system. A network outside the system indicates a network where users reside and can be an enterprise's internal network or a public network (such as the Internet).
- The external network dummy_external_network is used as a direct network in a VPC.

Name	ID	Physical Network	Network Type	VLAN ID	Resource Label	Created At	Description	Operation
dummy_external_ne...	90c8...	--	LOCAL		Used For: VPC Group: group1 Display Name: dummy_exte... Availability Zone: bms:hcs81	04/19/2022 16:59:....		Modify Set Resource Label More ▾

Administrators can create EIP and VPN external networks as IP address pools for services such as EIP and VPN.

Resource label configuration

* Display Name

zs-EIP

This is the external network name displayed on the tenant portal.

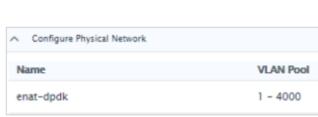
* Used For

EIP VPN

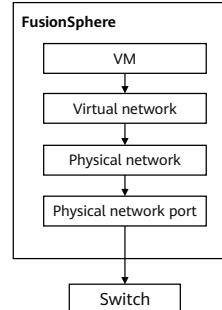
- An external network is a network outside a data center, such as the Internet or a private network deployed by an enterprise. When deploying a data center network, users need to communicate with an external network. External connections can be established and VDCs can communicate with each other only after an external network is created.
- In HUAWEI CLOUD Stack, the following external network types are available:
 - dummy_external_network: It is created by default during HUAWEI CLOUD Stack installation and is used by a VPC. After a tenant is created on ManageOne, you need to bind this network to the tenant to ensure that the VPC can be properly created.
 - external_relay_network: It is an internal public network plane, which is automatically generated based on the network segment planned by the user during HUAWEI CLOUD Stack installation. When an ECS is bound to an external Internet address, an internal public network address is automatically assigned to the ECS for NAT and message forwarding of internal components. No user management is required.
 - eip_external_network: It is an external network for configuring EIPs. It is used for creating EIPs to enable ECSs to communicate with the Internet.
You need to configure the external network based on the actual production environment requirements.
 - vpn_external_network: It is used to configure a VPN external network, which is used to establish an encrypted communication tunnel between a remote user and a VPC. **Configure the external network based on the actual production environment requirements.**

Relationships Between Physical Networks, Virtual Networks, and External Networks

- A physical network plane contains virtual switching devices, such as VLAN pools and OVSs, and needs to be mapped to physical NICs of servers. A physical network can be mapped to a pair of NICs. Once a NIC is mapped to a physical network, it cannot be mapped to other physical networks.



- A virtual network is a plane that is carried on a physical network and directly provides network services for VMs. Multiple virtual networks can be created based on a physical network.
- An external network is a special virtual network and can be a VLAN or local network. If the external network is a VLAN network, it must be carried on a physical network and traffic passes through the physical network. If the external network is a LOCAL network, it is not carried on the physical network and traffic does not pass through the physical network.



RH servers are used as an example.



Quiz

1. (Single-answer question) Which of the following statements is false about Service OM?
 - A. A VDC operator can create a public image.
 - B. Service OM administrators can create an external network for a VPN.
 - C. Service OM administrators can view private images on Service OM.
 - D. Service OM administrators can create a disk type on Service OM.

- Answers:
 - A

Summary

- This course describes Service OM, the HUAWEI CLOUD Stack resource management platform, including the introduction to compute, storage, and network resource management.

Recommendations

- Huawei Talent:
 - <https://e.huawei.com/en/talent/portal/#/>
- Huawei Certification:
 - <https://forum.huawei.com/enterprise/en/forum-813.html>

Acronyms

Acronym	Full Name	Description
AZ	Availability Zone	An AZ is a logical zone of physical resources, including compute, storage, and network resources.
BMS	Bare Metal Service	A BMS is a physical server dedicated for tenants.
CHSM	Cloud-hosted Hardware Security Module	A cloud-hosted hardware security module is a cryptographic device that provides cryptographic services for application systems of multiple tenants through networks by using virtualization technologies in a cloud computing environment.
DC	Data Center	A data center houses computer systems and related components (such as telecommunications and storage systems).
ECS	Elastic Cloud Service	An ECS is a compute server that consists of vCPUs, memory, OS, and EVS disks and allows on-demand allocation and elastic scaling.
EIP	Elastic IP Address	An EIP is a static IP address that can be directly accessed from an extranet. An extranet can be the Internet or an internal LAN of an enterprise.
ELB	Elastic Load Balance	ELB distributes incoming traffic across multiple backend servers based on specified forwarding policies.
EVS	Elastic Volume Service	EVS is a virtual block storage service that provides block storage for ECSs and BMSs.
IOPS	input/output operations per second	IOPS is a performance metric.
NFV	Network Function Virtualization	NFV is a concept of network architecture.
OVS	Open Virtual Switch	Open-source virtual switches are designed to automate (configuration, management, and maintenance) large networks through programmatic expansion.

Acronyms

Acronym	Full Name	Description
QoS	Quality of Service	QoS is used to measure the transmission quality and service validity of a transmission system and evaluate the capability of a service provider to meet customer requirements.
VDC	Virtual Data Center	A VDC is a new type of data center that applies cloud computing to Internet data center (IDC).
VPC	Virtual Private Cloud	VPC enables you to provision logically isolated virtual networks for cloud servers.
VPN	Virtual Private Network	VPN builds encrypted communication tunnels between local data centers and VPCs.
VSM	Virtual Security Module	A VSM is a cryptographic service instance that is created on a CloudHSM using virtualization technologies and provides similar services as a CloudHSM.

Thank you.

把数字世界带入每个人、每个家庭、

每个组织，构建万物互联的智能世界。

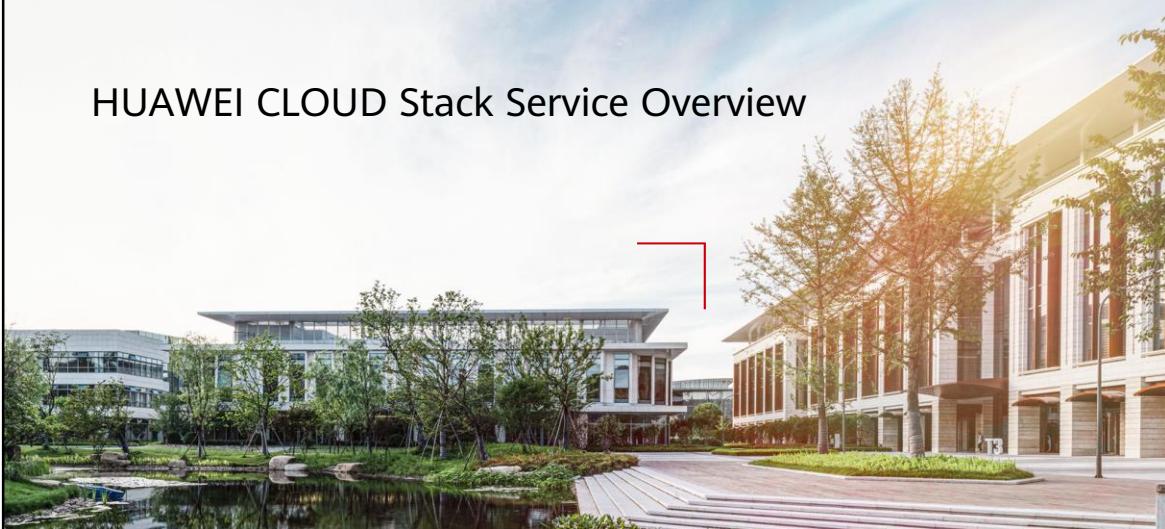
Bring digital to every person, home, and organization for a fully connected, intelligent world.

Copyright©2022 Huawei Technologies Co., Ltd.
All Rights Reserved.

The information in this document may contain predictive statements including, without limitation, statements regarding the future financial and operating results, future product portfolio, new technology, etc. There are a number of factors that could cause actual results and developments to differ materially from those expressed or implied in the predictive statements. Therefore, such information is provided for reference purpose only and constitutes neither an offer nor an acceptance. Huawei may change the information at any time without notice.



HUAWEI CLOUD Stack Service Overview



Foreword

- This course describes HUAWEI CLOUD Stack compute, storage, and network cloud services.

Objectives

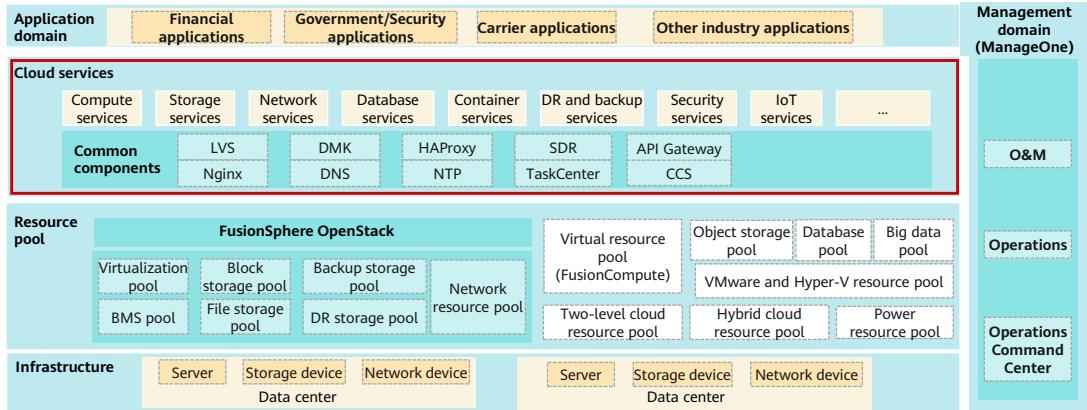
- Upon completion of this course, you will understand:
 - The positioning and classification of HUAWEI CLOUD Stack cloud services
 - HUAWEI CLOUD Stack compute services
 - HUAWEI CLOUD Stack storage services
 - HUAWEI CLOUD Stack network services

Contents

- 1. Introduction to HUAWEI CLOUD Stack Cloud Services**
2. Introduction to HUAWEI CLOUD Stack General Services
3. Cloud Migration Cases

Positioning of HUAWEI CLOUD Stack Cloud Services

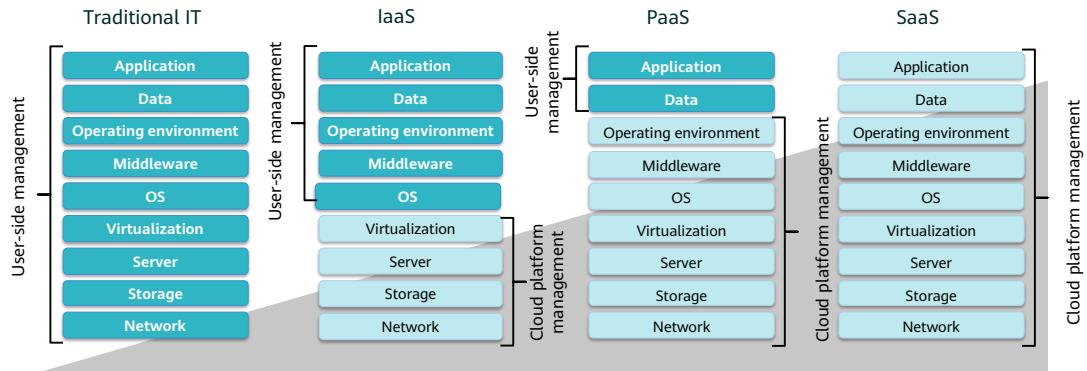
- Cloud services interconnect with resources provided by the resource pool layer of multiple data centers and provide infrastructure for various industry applications.



Contents

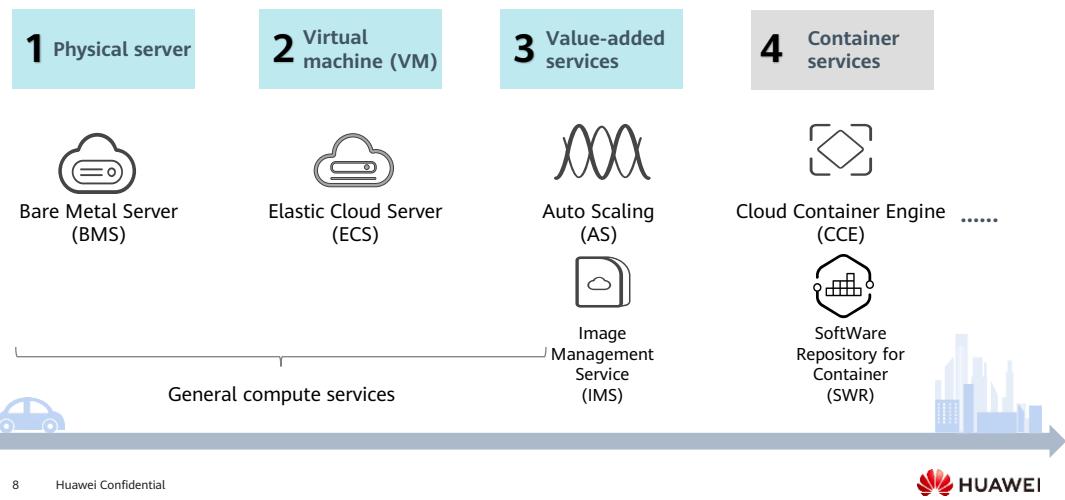
1. Introduction to HUAWEI CLOUD Stack Cloud Services
- 2. Introduction to HUAWEI CLOUD Stack General Services**
3. Cloud Migration Cases

Evolution of Cloud Computing Models



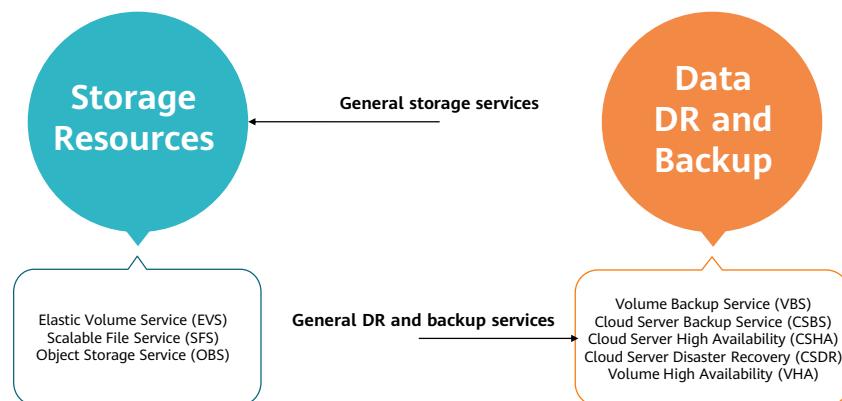
- Cloud services, including IaaS, PaaS, and SaaS services, allow you to obtain required IT resources and capabilities in self-service, on-demand, and online mode.
- Infrastructure as a Service (IaaS): The cloud platform provides infrastructure resources (such as servers, storage devices, networks, and virtual resources) and maintains related resources. Users only need to pay attention to systems and applications.
- Platform as a Service (PaaS): The cloud platform provides infrastructure (such as servers, storage devices, networks, and virtual resources) and application deployment environment (such as operating systems, middleware, and software running environment) and maintains related resources. Users only need to focus on applications and data.
- Software as a Service (SaaS): The cloud platform provides all resources, services, and maintenance. Users only need to use applications.
- Compared with full-process and full-device purchase for traditional IT, cloud services sell IT devices as services, allowing customers to select devices on demand. Cloud services are more flexible and cost-effective than traditional IT.

Compute Cloud Services



- Based on compute instances and functions, compute services can be classified into physical servers, VMs, value-added services, and container services. Other compute services include heterogeneous compute services.
- CCE is a highly scalable, high-performance, enterprise-class Kubernetes service for you to run containers. With CCE, you can easily deploy, manage, and scale containerized applications in the cloud.
- SWR allows you to easily manage the full lifecycle of container images and facilitates secure and reliable deployment of images for your applications. SWR can either work with CCE or be used as an independent container image repository.
- The ECS, BMS, IMS, and AS services will be described in the following sections.

Storage Cloud Services

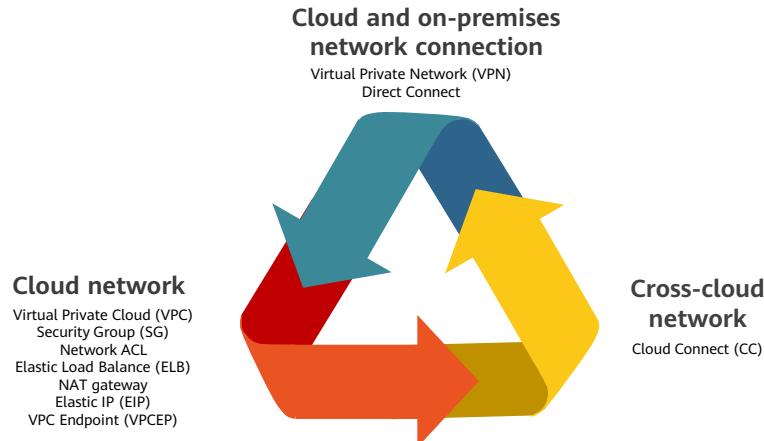


9 Huawei Confidential



- Storage services can be classified into storage resource services and data DR and backup services. Storage resource services include EVS, SFS, and OBS.
- Data DR and backup services are described as follows:
 - VBS can create a backup for an EVS disk and use the backup data to restore the EVS disk to maximally ensure user data security and correctness and service security.
 - CSBS can create backups of the configuration specifications and data on system and data disks for ECSs or BMSs, and restore the service data of ECSs or BMSs using the backups.
 - CSHA provides HA protection for ECSs between intra-city data centers. If the production center becomes faulty, services on the protected ECSs can be automatically or manually switched to the DR center.
 - CSDR provides remote DR protection for ECSs and BMSs. If a disaster occurs in the production center, ECSs and BMSs protected by CSDR can be restored in the remote DR center.
 - VHA provides local storage active-active protection for EVS disks on ECSs and BMSs.

Network Cloud Services



10 Huawei Confidential



- As shown in the figure, network services can be classified into services for the cloud network, cloud and on-premises network connection, and cross-cloud network. The network services in the figure will be described in the following sections.

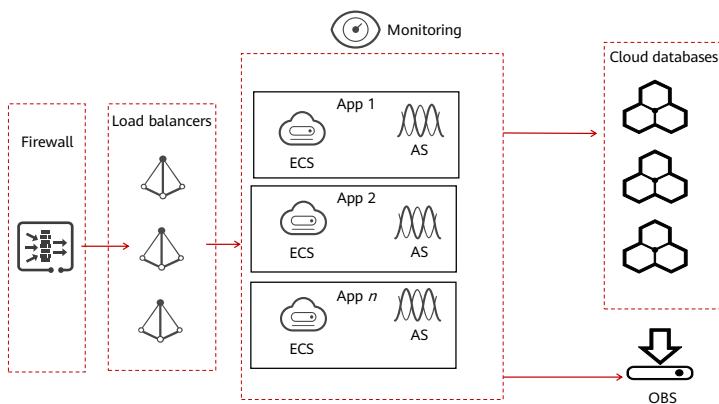
Contents

1. Introduction to HUAWEI CLOUD Stack Cloud Services
2. Introduction to HUAWEI CLOUD Stack General Services
- 3. Cloud Migration Cases**

A Cloud Migration Case Tailor-Made for Promotions and Flash Sales

Business scenarios involving burst traffic: e-commerce promotions, hot topic forwarding, and limited-time offers

Business issues to be resolved



- Large volume user access
- System pressure due to high-volume transaction services, for example, flash sales
- Idle resources after promotions are over
- Malicious attacks and buying

Key services:

ELB
Web Application Firewall (WAF)
AS
OBS



- Traffic passes through the firewall and then enters the cloud. If traffic is heavy and high service reliability is required, ELB can be used to distribute network traffic to backend servers for load balancing. AS can be used to add or delete backend compute instances based on detailed policies. Service data can be processed by cloud databases. It is recommended that persistent data be stored in OBS. If services have high security requirements, security services such as Web Application Firewall (WAF) can be used.

Quiz

1. (Multiple-answer question) Which of the following services are HUAWEI CLOUD Stack general cloud services?
 - A. BCS
 - B. ECS
 - C. ELB
 - D. IMS

- Answers:
 - BCD

Summary

- This course described:
 - The positioning and classification of HUAWEI CLOUD Stack cloud services
 - HUAWEI CLOUD Stack compute services
 - HUAWEI CLOUD Stack storage services
 - HUAWEI CLOUD Stack network services

Recommendations

- Huawei Talent:
 - <https://e.huawei.com/en/talent/portal/#/>
- Huawei Certification:
 - <https://forum.huawei.com/enterprise/en/forum-813.html>

Acronyms

Acronym	Full Name	Description
AS	Auto Scaling	AS automatically scales resources to keep up with service demands based on pre-configured AS policies.
BMS	Bare Metal Server	A BMS is a physical server dedicated for tenants.
CC	Cloud Connect	CC allows you to quickly build high-speed, high-quality, and stable networks between VPCs across regions.
CCE	Cloud Container Engine	CCE provides highly scalable, high-performance enterprise-class Kubernetes clusters and supports Docker containers.
CSBS	Cloud Server Backup Service	CSBS can create backups for ECSs and BMSs.
CSDR	Cloud Server Disaster Recovery	CSDR provides remote DR protection for ECSs and BMSs.
CSHA	Cloud Server High Availability	CSHA provides HA protection for ECSs between intra-city data centers.
ECS	Elastic Cloud Server	An ECS is a compute server that consists of vCPUs, memory, OS, and EVS disks, and allows on-demand allocation and elastic scaling.
ELB	Elastic Load Balance	ELB distributes incoming traffic across multiple backend servers based on specified forwarding policies.

Acronyms

Acronym	Full Name	Description
EVS	Elastic Volume Service	EVS is a virtual block storage service that provides block storage for ECSs and BMSS.
IMS	Image Management Service	IMS allows you to easily create images and manage the image lifecycle.
OBS	Object Storage Service	OBS is an object-based storage service that provides massive, secure, highly reliable, and low-cost data storage.
SFS	Scalable File Service	SFS provides an on-demand, scalable, and high-performance shared file system for ECSs.
SWR	SoftWare Repository for Container	SWR manages container images throughout their lifecycles.
VBS	Volume Backup Service	VBS can create backups for EVS disks and use backups to restore EVS disks.
VHA	Volume High Availability	VHA provides local storage active-active protection for EVS disks on ECSs and BMSS.
VPC	Virtual Private Cloud	VPC enables you to provision logically isolated virtual networks for cloud servers.
VPN	Virtual Private Network	VPN establishes encrypted communication tunnels between local data centers and VPCs.

Thank you.

把数字世界带入每个人、每个家庭、

每个组织，构建万物互联的智能世界。

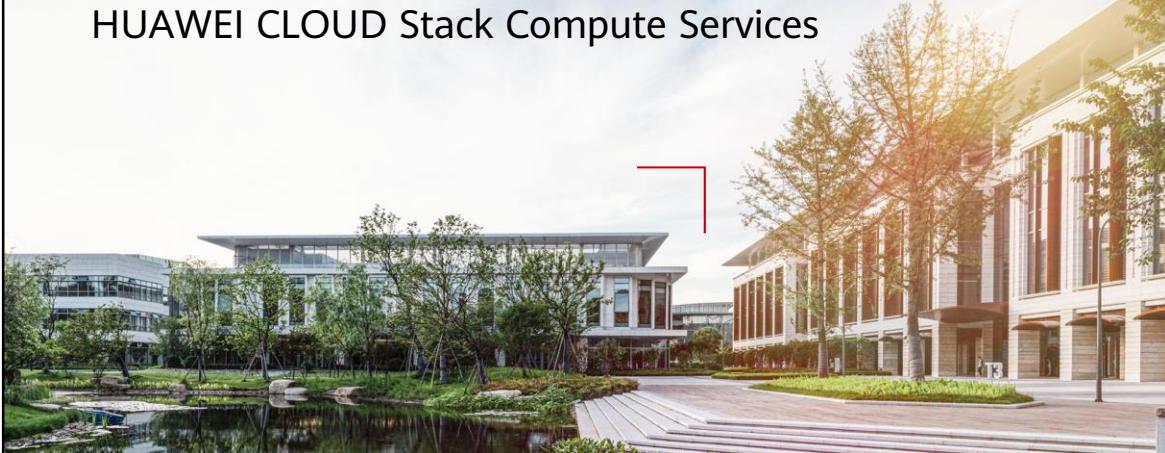
Bring digital to every person, home, and organization for a fully connected, intelligent world.

Copyright©2022 Huawei Technologies Co., Ltd.
All Rights Reserved.

The information in this document may contain predictive statements including, without limitation, statements regarding the future financial and operating results, future product portfolio, new technology, etc. There are a number of factors that could cause actual results and developments to differ materially from those expressed or implied in the predictive statements. Therefore, such information is provided for reference purpose only and constitutes neither an offer nor an acceptance. Huawei may change the information at any time without notice.



HUAWEI CLOUD Stack Compute Services



Foreword

- This course describes basic compute cloud services at the IaaS layer of HUAWEI CLOUD Stack, including ECS, BMS, IMS, and AS.

Objectives

- Upon completion of this course, you will:
 - Understand basic compute cloud services of HUAWEI CLOUD Stack.
 - Learn about functions, features, and application scenarios of ECS, BMS, AS, and IMS.

Contents

- 1. Overview of HUAWEI CLOUD Stack Compute Services**
2. HUAWEI CLOUD Stack Compute Services
3. Compute Service Case Study

Compute Services on the Tenant Portal

- After logging in to ManageOne Operation Portal as a tenant, you can see the compute services in the service list.

The screenshot shows the HUAWEI CLOUD Stack tenant portal interface. At the top, there is a navigation bar with links for Home, Resources, Application, Report, System, and English. Below the navigation bar, there are dropdown menus for Region (set to hangzhou) and Resource Set (set to zj-hz-1_zhangsan). A search bar is present with the placeholder "Enter a name to search for a service." On the left side, there is a sidebar with a "Service List" icon and a "Cloud Domain Name Service" entry. The main content area is titled "Basic cloud services" and contains three columns: Computing, Storage, and Network. The "Computing" column lists several services: Service_154c, Image Management Service, Cloud Container Engine, Auto Scaling, Elastic Cloud Server, and Bare Metal Server. The "Storage" column lists: Cloud Server Backup Service, Volume Backup Service, Elastic Volume Service, and Object Storage Service 3.0. The "Network" column lists: Virtual Private Cloud, Elastic Load Balance, Elastic IP, Network ACL, Virtual Private Network, Direct Connect, VPC Endpoint, Cloud Domain Name Service, and Cloud Firewall. A red box highlights the "Basic cloud services" section under the Computing heading.

Basic cloud services		
Computing	Storage	Network
Service_154c	Cloud Server Backup Service	Virtual Private Cloud
Image Management Service	Volume Backup Service	Elastic Load Balance
Cloud Container Engine	Elastic Volume Service	Elastic IP
Auto Scaling	Object Storage Service 3.0	Network ACL
Elastic Cloud Server		Virtual Private Network
Bare Metal Server		Direct Connect
		VPC Endpoint
		Cloud Domain Name Service
		Cloud Firewall

Compute Service Overview

Cloud Service	Description
ECS	An Elastic Cloud Server (ECS) is a cloud server that consists of vCPUs, memory, images, and Elastic Volume Service (EVS) disks, allowing for on-demand allocation and elastic scaling. It is used together with cloud services such as Virtual Private Cloud (VPC), Network ACL, and Cloud Server Backup Service (CSBS) to construct an efficient, reliable, and secure computing environment, ensuring stable and continuous services.
BMS	A Bare Metal Server (BMS) is a physical server dedicated for a specific user. It provides remarkable computing performance and helps ensure stability for key applications. The BMS service can be used with other cloud services, such as VPC, to provide you with the consistency and stable performance of hosted servers combined with the scalability of cloud resources.
IMS	Image Management Service (IMS) allows you to create ECSs from images. An image is an ECS template that contains an OS or service data and may also contain proprietary software and application software, such as database software. Images are classified as either public, private, or shared. You can apply for an ECS using a public, private, or shared image. You can also create a private image using an ECS or an external image file.
AS	Auto Scaling (AS) automatically adjusts resources to keep up with changes in demand based on pre-configured AS policies. You can specify AS configurations and policies as required. These configurations and policies free you from repeatedly adjusting resources in response to service changes and demand spikes. They help reduce resource requirements and labor costs.

Contents

1. Overview of HUAWEI CLOUD Stack Compute Services

2. HUAWEI CLOUD Stack Compute Services

- ECS

- BMS

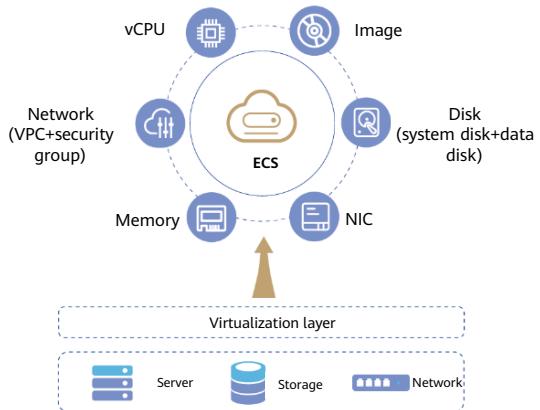
- IMS

- AS

3. Compute Service Case Study

ECS

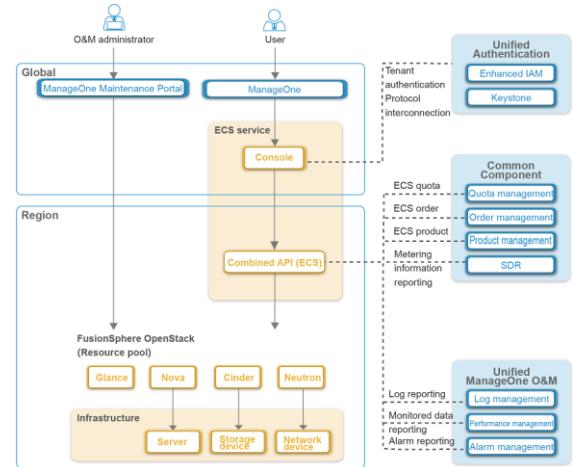
- An ECS is a cloud server that consists of vCPUs, memory, EVS disks, and other required resources. ECSs allow for on-demand allocation and elastic scaling.
- After an ECS is created, you can use it on the cloud just like using your local computer or physical server. The cloud platform provides you with relatively inexpensive compute and storage resources on demand and simplifies management and maintenance, enabling you to stay focused on services.



- The ECS service works with cloud services such as VPC and CSBS to provide an efficient, reliable, and secure computing environment for your data and applications.
- The ECS service allows you to:
 - Customize the flavor, image, network, disk, authentication mode, and number of ECSs when creating ECSs.
 - Manage the lifecycle of an ECS, including starting, stopping, restarting, and deleting an ECS. Clone an ECS, create an ECS snapshot, and manage the watchdog status and HA status. Modify vCPUs and memory of an ECS.
 - Expand the capacity of EVS disks attached to an ECS, attach EVS disks to an ECS, detach EVS disks from an ECS, and use shared EVS disks for an ECS.
 - Change and reinstall the ECS OS, and create a private image using an existing ECS.
 - Bind an elastic IP address (EIP) to and unbind an EIP from an ECS.

ECS Logical Architecture

- You can use a tenant API to invoke FusionSphere OpenStack components on ManageOne Operation Portal to create and manage ECSs.



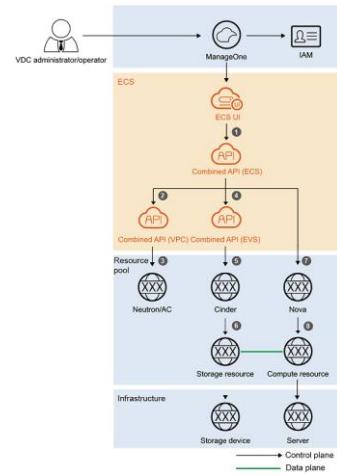
9 Huawei Confidential



- Console: ECS UI is a console centered on ECS and manages relevant resources.
- Combined API (ECS): Combined API provides the backend service for ECSs, serves as the server end of ECS UI, and can invoke FusionSphere OpenStack components. Requests sent by an ECS from the console are forwarded by ECS UI to Combined API and are returned to ECS UI after being processed by Combined API.
- Resource pool: Glance manages images. Nova manages the lifecycle of compute instances in the FusionSphere OpenStack environment, including batch creation, on-demand scheduling, and instance stopping. Cinder provides persistent block storage for running instances. Its pluggable driver facilitates the creation and management of block storage devices. Neutron provides APIs for defining network connectivity and addressing.
- Unified authentication: provides unified identity authentication during login.
- Common components: Combined API reports ECS quota, order, product, and metering and charging information to the ManageOne operation module.
- Unified O&M: Combined API reports ECS log, monitoring, and alarm information to the ManageOne O&M module.

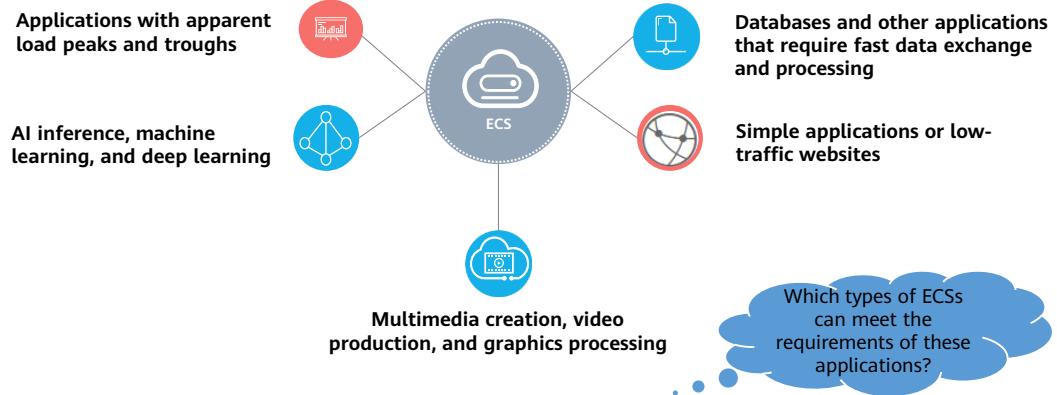
ECS Workflow

- The workflow is as follows:
 - Submit an ECS creation request on the ECS page (step 1 in the figure).
 - Create network resources (steps 2 and 3 in the figure).
 - The ECS API in Combined API calls the VPC API in Combined API.
 - The VPC API calls Neutron to create network resources such as EIPs and ports.
 - Create storage resources (steps 4 to 6 in the figure).
 - The ECS API in Combined API calls the EVS API in Combined API.
 - The EVS API calls Cinder.
 - Cinder creates volumes in the storage pool based on the policy for requesting storage resources.
 - Create compute resources (steps 7 and 8 in the figure).
 - The ECS API sends the request to Nova.
 - Nova creates an ECS in the compute resource pool.



ECS Application Scenarios

- You can select different types of ECSs for different applications.



- Simple applications or low-traffic websites, such as blogs and enterprise official website, have relatively low requirements on the server computing and storage performance. A general-purpose ECS can meet the requirements.
- Multimedia making, video making, and graphic processing require ECSs to provide good graphic processing capabilities. You can choose ECSs with excellent CPU and GPU computing performance, such as GPU graphics-accelerated or GPU computing-accelerated ECSs, to meet your service requirements.
- Databases and other applications that require fast data exchange and processing: For applications that require high I/O capabilities of servers, such as high-performance relational databases and NoSQL databases, you can use ultra-high I/O ECSs.
- For applications with apparent load peaks and troughs, such as video websites, school course selection systems, and game companies, the number of visits may increase significantly within a short time. To improve resource utilization and ensure that your applications run properly, you can use AS to work with ECSs. AS policies can be configured to automatically add or remove ECSs as the service volume changes. Generally, general-purpose ECSs can work with the AS service to meet requirements.
- AI inference, machine learning, and deep learning: AI-accelerated ECSs use Huawei's Ascend 310 chips. They are suitable for scenarios that require real-time, highly concurrent massive computing, such as, AI inference, machine learning, and video encoding and decoding.

Contents

1. Overview of HUAWEI CLOUD Stack Compute Services

2. HUAWEI CLOUD Stack Compute Services

- ECS

- BMS

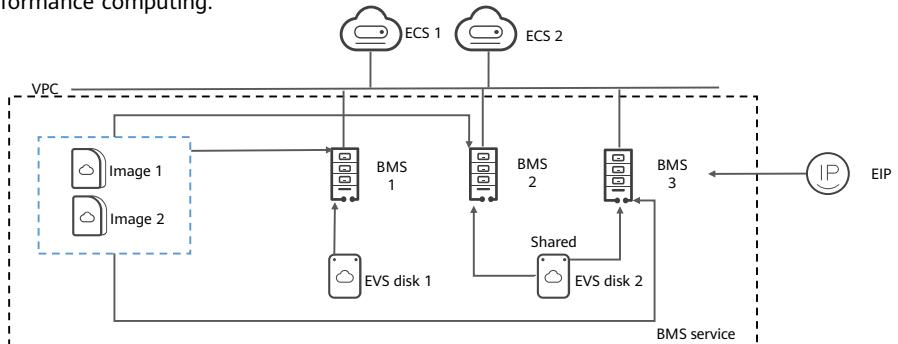
- IMS

- AS

3. Compute Service Case Study

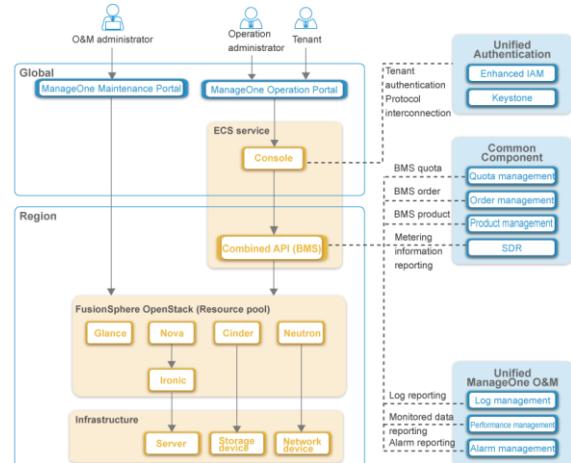
BMS

- The BMS service provides dedicated physical servers where you can run demanding workloads that you would rather not run on VMs for performance or security reasons, and without sacrificing the scalability of a cloud-based service. It is ideal for core databases, critical application systems, and high-performance computing.



BMS Logical Architecture

- You can use a tenant API to invoke FusionSphere OpenStack components on ManageOne Operation Portal to create and manage BMSS.



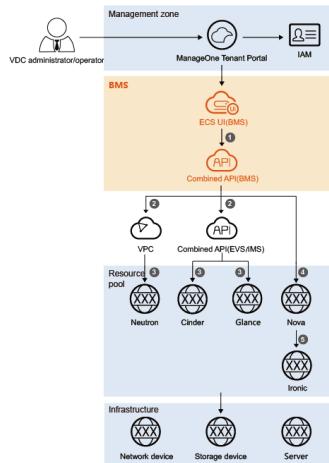
14 Huawei Confidential



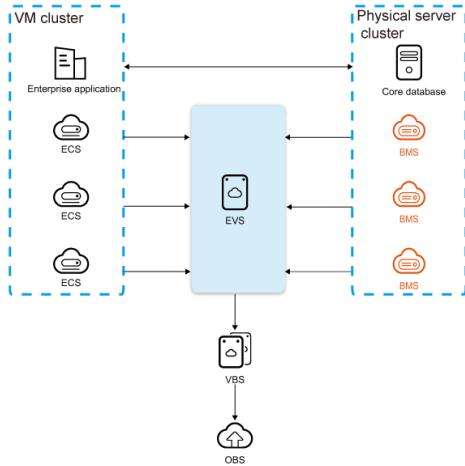
- The BMS service architecture consists of the cloud service layer and FusionSphere OpenStack infrastructure layer.
- The cloud service layer consists of the BMS Console layer and BMS Service layer.
 - The BMS Console layer consists of the BMS UI, which is the user interface of the BMS. It functions as the entry for user requests and uses Identity and Access Management (IAM) for identification and access management and is hosted in the ECS UI.
 - The BMS Service layer contains BMS service and BMS plugin (SDR). BMS service is the logical processing layer of the BMS. It is hosted in Combined API and uses eSight to monitor and generate alarms. BMS plugin (SDR) is an extension plug-in of the SDR system and is used for metering.
- The infrastructure layer consists of FusionSphere OpenStack management services and BMS resource pools. Ironic is a core component of the Bare Metal Server in the OpenStack system and manages bare metal servers. By working with components such as Nova and Neutron, the BMS network can be a virtual network consisting of pure software or a network consisting of proprietary hardware devices managed by a central controller. Different networking modes may be used in various scenarios to deliver a user experience similar to that with the ECS service.

BMS Workflow

- The workflow is as follows:
 - A user applies for resources on the BMS GUI, and the request is sent to Combined API.
 - Combined API (BMS) calls the APIs of EVS, VPC, and IMS.
 - VPC calls Neutron to create an EIP or a port. EVS calls Cinder to create an EVS disk based on the policy for requesting storage resources. IMS calls Glance to query image information.
 - BMS sends the creation request to Nova.
 - Nova sends the request to Ironic to create a BMS.



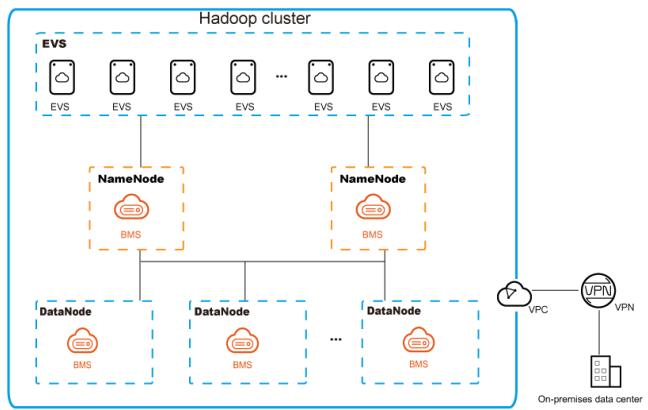
BMS Application Scenario: Core Database



- Some customers require that instead of deploying their mission-critical database applications on VMs, they be deployed on BMSs, which provide dedicated resources, isolated networks, and guaranteed performance.

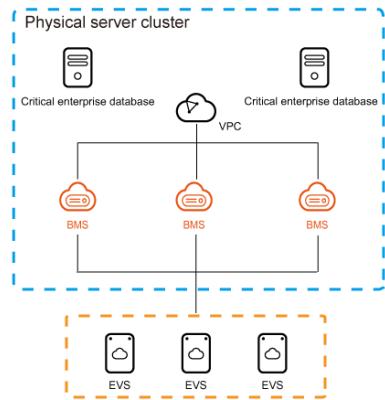
BMS Application Scenario: High Performance Computing (HPC)

- BMS is suitable for supercomputing centers, gene sequencing, graphics rendering, and other high-performance computing scenarios where massive data sets need to be processed with high performance, stability, and in near real-time, and where performance loss and hyperthreading from virtualization are unacceptable.



BMS Application Scenario: Applications with High Security and Supervision Requirements

- For finance, securities, and other industries where there are strict regulatory compliance requirements and for other customers with demanding requirements for data security, BMS provides dedicated resources, good data isolation, data manageability, and traceability.



Contents

1. Overview of HUAWEI CLOUD Stack Compute Services

2. HUAWEI CLOUD Stack Compute Services

- ECS
- BMS
- **IMS**
- AS

3. Compute Service Case Study

IMS

IMS allows you to easily create images and manage image lifecycles.

An image is an ECS or BMS template that contains an operating system (OS) and preinstalled software.

Image Types:

Public image: A public image is provided by the cloud platform and is visible to all users.

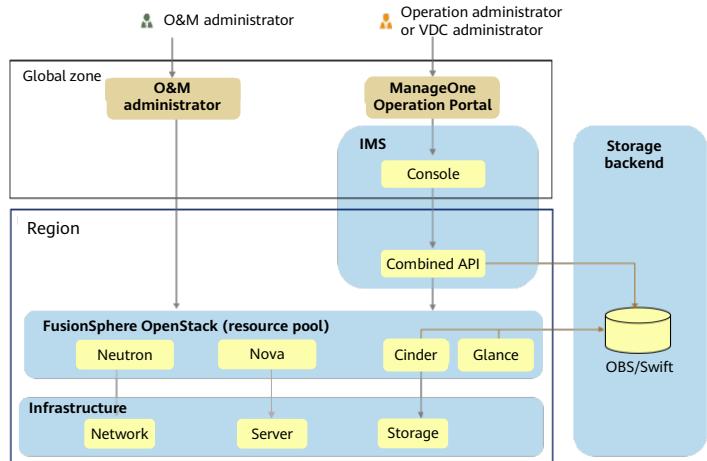
Private image: A private image is created from an ECS or external image file and visible only to the user who created it. It contains an OS, public applications, private applications, and service data.

Shared image: A private image can be shared with other users on the console or using an API. You can query a list of the images shared with you on the console or using an API, and you can create ECSs or BMSs using the shared images.

- Based on user services, private images can be classified into the following types:
 - System disk image: It is an image created using the system disk and contains an OS, public applications, and private applications. A system disk image can be used to create a system disk or an ECS. When you use it to create ECSs, you do not need to configure the ECSs repeatedly.
 - Data disk image: It contains service data only. A data disk image can only be used to create a data disk and cannot be used to create an ECS. You can use EVS disks created using an existing data disk image to migrate and share service data among multiple ECSs.
 - Full-ECS image: It contains an OS, public applications, private applications, and service data. A full-ECS image can only be used to create an ECS and cannot be used to create a system or data disk. You can use the ECSs created from it to quickly migrate a whole ECS.
- You can share your private images with other users. If you are a multi-project user, the image sharing function allows you to use images conveniently in multiple projects in the same region. You can share images, stop sharing images, and add or delete tenants that can use the shared images. If other users share private images with you, you can choose to accept or reject the images, and you can delete shared images you have previously accepted.

IMS Logical Architecture

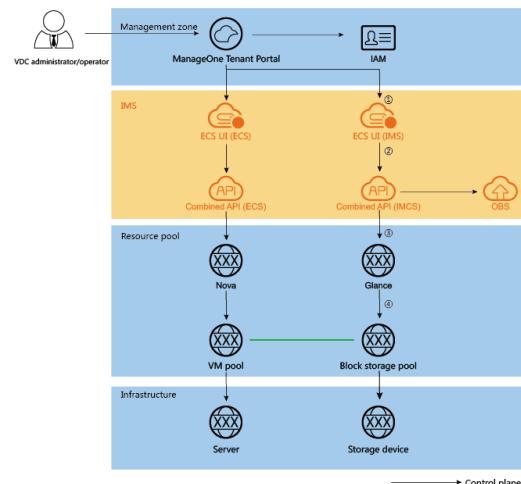
- You can use a tenant API to invoke FusionSphere OpenStack components on ManageOne Operation Portal to create and manage private images.



- Infrastructure: provides network devices, servers, and storage devices.
- API layer: Requests sent from the IMS console are forwarded by ECS UI (IMS) to Combined API (IMS) and are returned to ECS UI (IMS) after being processed by Combined API (IMS).
- Storage backend: It can be Swift or OBS for storing image files.

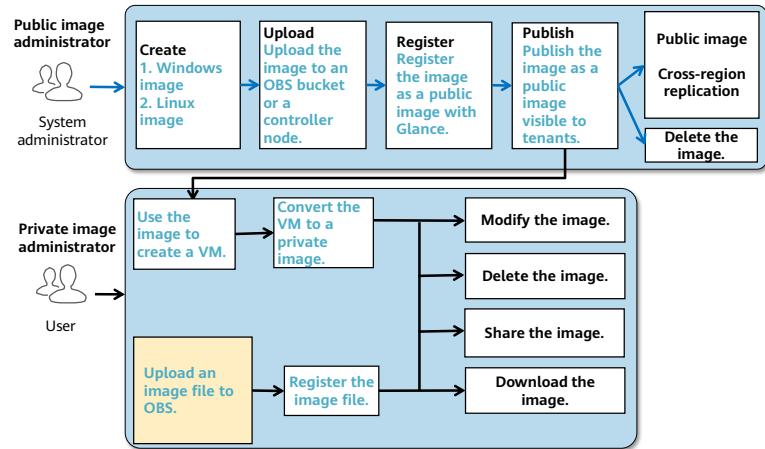
IMS Workflow

- The workflow is as follows:
 - A user selects an ECS from ManageOne Operation Portal (ManageOne Tenant Portal) in B2B scenarios to create an image. IMS identifies the corresponding system disk based on the ECS.
 - After receiving the request, Combined API checks and creates an image bucket.
 - Combined API calls the upload-to-image API of Cinder to create an image.
 - Cinder calls the Glance API to create image metadata and calls the glance image-upload API to change the image status to active.



IMS Application Scenarios

- Creating an ECS using an image.
- Creating a private image using an ECS.
- Creating a private image using an external file.
- Migrating or sharing data using data disk images.



Contents

1. Overview of HUAWEI CLOUD Stack Compute Services

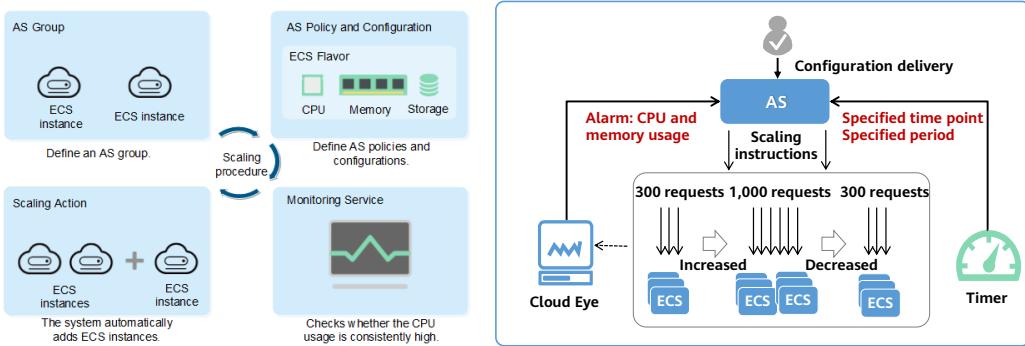
2. HUAWEI CLOUD Stack Compute Services

- ECS
- BMS
- IMS
- AS

3. Compute Service Case Study

AS

- AS automatically adjusts resources to keep up with changes in demand based on pre-configured AS policies. You can specify AS configurations and policies as required. These configurations and policies free you from repeatedly adjusting resources in response to service changes and demand spikes. They help reduce resource requirements and labor costs.

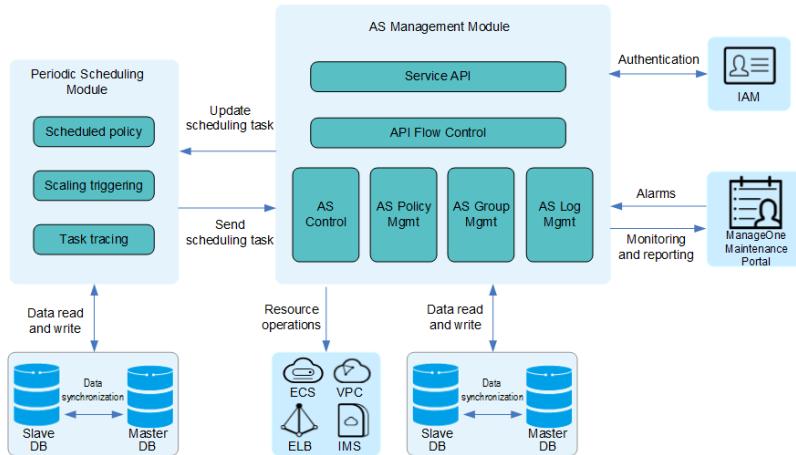


25 Huawei Confidential



- An AS group consists of a collection of instances that apply to the same scenario. It is the basis for enabling or disabling AS policies and performing scaling actions. An instance is an ECS in the AS group.
- An AS policy specifies the conditions for triggering a scaling action as well as the operation that will be performed. If the conditions are met, a scaling action is triggered automatically.
- AS supports the following policies:
 - Alarm:** AS automatically increases or decreases the number of ECSs in an AS group or sets the number of ECSs to a specified value if the monitoring system generates an alarm for a configured metric, such as the CPU usage.
 - Periodic:** AS increases or decreases the number of ECSs in an AS group or sets the number of ECSs to a specified value at a configured interval, such as one day, one week, or one month.
 - Scheduled:** AS automatically increases or decreases the number of ECSs in an AS group or sets the number of ECSs to a specified value at a specified time.
- An AS configuration is an ECS template in an AS group, specifying specifications of the ECS to be added, including the ECS type, vCPUs, memory, images, disks, and login mode. A scaling action adds instances to or removes instances from an AS group.

AS Logical Architecture



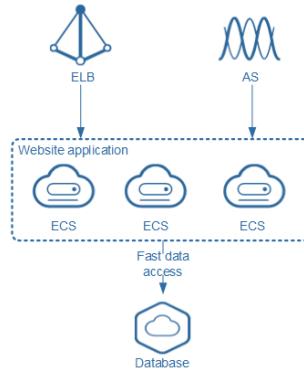
26 Huawei Confidential



- The AS management module creates and manages AS groups, including managing the expected number, minimum number, and maximum number of instances in an AS group, the AZ, VPC, subnet, and security group to which the AS group belongs, the health check mode of the AS group, and the instance removal policy, as well as creates and manages AS configurations. If you have special requirements on the ECSs for resource expansion, use a new template or an existing ECS to create an AS configuration so that specifications of all ECSs to be added to the AS group during scaling actions will meet your requirements. If an AS configuration is not used by any AS group, you can delete it. You can also use the AS management module to create and manage AS policies, including setting alarm, scheduled, and periodic policies, and enabling, disabling, or deleting AS policies, as well as control scaling actions. After a scheduled scaling action configured on the periodic scheduling module is triggered or an alarm is received from ManageOne, the AS management module reads details about the AS group and configuration from the database, verifies the parameter validity, and updates the scaling action in the periodic scheduling module in real time. The periodic scheduling module collects metric data, performs health checks, and executes scaling actions.
- Functions of the databases (master/slave): The databases of the scaling management module are used to store configuration information about AS groups, AS configurations, and AS policies. The databases of the periodic scheduling module are used to store task information.
- ManageOne Maintenance Portal regularly obtains the monitoring data of each ECS in the AS group, and sends an alarm to the AS management module when the acquired data reaches the alarm threshold.

AS Application Scenario: Website Application

- **Specific scenarios:**
 - Enterprise websites, e-commerce, and mobile applications
- **Service characteristics:**
 - Abrupt increases in service requests and other significant fluctuations in traffic volumes.
- **Common deployment:**
 - AS automatically adds instances to an AS group for applications and removes unneeded ones. In this way, you do not need to prepare a large number of ECSs for an expected marketing activity or for unexpected peak hours. AS helps ensure system reliability and reduces operating costs.



AS Application Scenario: Data Processing

- **Specific scenarios:**

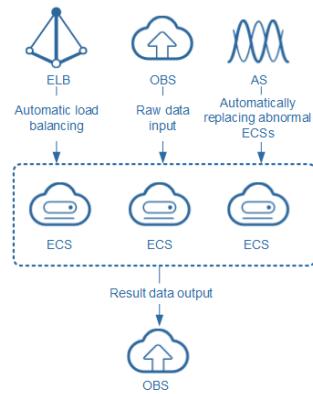
- Video websites, media codec applications, media content backhaul applications, heavy-traffic content management systems, and distributed high-speed cache systems

- **Service characteristics:**

- Compute and storage resources need to be dynamically adjusted based on data processing workloads. ECSs in an AS group need to be checked, and unhealthy ECSs are automatically replaced.

- **Common deployment:**

- With AS, ELB, and OBS, data to be processed is sent back to OBS buckets for processing. ECSs in an AS group process data, and the number of ECSs is adjusted based on the service load.



Contents

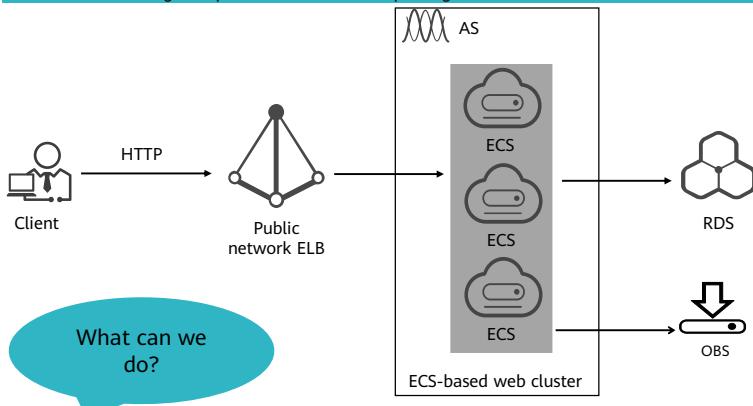
1. Overview of HUAWEI CLOUD Stack Compute Services
2. HUAWEI CLOUD Stack Compute Services
- 3. Compute Service Case Study**

Case Study

Background: A company wants different departments to share basic service packages. When processing e-commerce and game services, the company wants to adjust ECS resources based on the resource usage at specific times or on a repeating schedule.

Service issues to be resolved

- Massive concurrent user sessions
- Transaction processing pressure due to transaction services, for example, flash sales
- Idle resources after promotions



Key services:

ECS
ELB
AS
(Optional) Relational Database Service (RDS)
OBS

Quiz

1. (Multiple-answer question) To handle an upcoming large-scale promotion, a small e-commerce enterprise needs to purchase corresponding cloud services. Which of the following cloud services can be used together by the e-commerce enterprise to reduce costs?
 - A. ECS
 - B. IMS
 - C. BMS
 - D. AS

- Answers:
 - ABD

Summary

- This course focused on:
 - Basic compute cloud services of HUAWEI CLOUD Stack
 - Functions, features, and application scenarios of ECS, BMS, AS, and IMS

Recommendations

- Huawei Talent:
 - <https://e.huawei.com/en/talent/portal/#/>
- Huawei Certification:
 - <https://forum.huawei.com/enterprise/en/forum-813.html>

Acronyms

Acronym	Full Name	Description
API	Application Programming Interface	A particular set of rules and specifications that are used for communication between software programs.
AS	Auto Scaling	AS automatically scales resources to keep up with service demands based on pre-configured AS policies.
BMS	Bare Metal Server	A BMS is a physical server dedicated for you.
ECS	Elastic Cloud Server	An ECS is a compute server that consists of vCPUs, memory, OS, and EVS disks and allows on-demand allocation and elastic scaling.
ELB	Elastic Load Balance	ELB distributes incoming traffic across multiple backend servers based on specified forwarding policies.
EVS	Elastic Volume Service	EVS is a virtual block storage service, which provides block storage space for ECSs and BMSs.
IAM	Identity and Access Management	IAM manages account information, role permission, access control, and logs.
IMS	Image Management Service	IMS allows you to easily create images and manage image lifecycles.
OBS	Object Storage Service	OBS provides massive, secure, highly reliable, and low-cost data storage.
VPC	Virtual Private Cloud	VPC enables you to provision logically isolated virtual networks for cloud servers.

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and
organization for a fully connected,
intelligent world.

Copyright©2022 Huawei Technologies Co., Ltd.
All Rights Reserved.

The information in this document may contain predictive
statements including, without limitation, statements regarding
the future financial and operating results, future product
portfolio, new technology, etc. There are a number of factors that
could cause actual results and developments to differ materially
from those expressed or implied in the predictive statements.
Therefore, such information is provided for reference purpose
only and constitutes neither an offer nor an acceptance. Huawei
may change the information at any time without notice.



HUAWEI CLOUD Stack Storage Services



1 Huawei Confidential



Foreword

- This course describes basic storage cloud services at the infrastructure as a service (IaaS) layer of HUAWEI CLOUD Stack, including Elastic Volume Service (EVS), Scalable File Service (SFS), and Object Storage Service (OBS).

Objectives

Upon completion of this course, you will understand:

- HUAWEI CLOUD Stack basic storage services.
- Functions, features, and application scenarios of EVS, SFS, and OBS.

Contents

- 1. Overview of HUAWEI CLOUD Stack Basic Storage Services**
2. Introduction to HUAWEI CLOUD Stack Storage Services
3. Storage Solution Design

Storage Services on the Tenant Portal

- After logging in to ManageOne Operation Portal as a tenant, you can see the storage services in the service list.

The screenshot shows the ManageOne Operation Portal interface. At the top, there is a navigation bar with links for Home, Resources, Application, Report, System, and English. Below the navigation bar, there are dropdown menus for Region (set to hangzhou) and Resource Set (set to zj-hz-1_zhangsan). A search bar is also present. On the left side, there is a sidebar with a 'Service List' menu item and a 'Cloud Domain Name Service' icon. The main content area is titled 'Basic cloud services' and lists several services under 'Storage': Cloud Server Backup Service, Volume Backup Service, Elastic Volume Service, and Object Storage Service 3.0. This 'Storage' section is highlighted with a red box. To the right of the storage services, there is another column titled 'Network' which lists various network-related services like Virtual Private Cloud, Elastic Load Balance, and Cloud Firewall. The bottom right corner of the screenshot features the Huawei logo.

Storage Type

Block Storage	File Storage	Object Storage
EVS	SFS	OBS
Block storage is used to map the entire raw disk space to hosts or VMs. Users can format the storage into a file system as required.	File storage is like a shared folder where users can directly store their data, for example, a remote shared Windows directory.	Object storage does not have a directory structure, and data is stored in a flat manner and is identified by their unique ID.

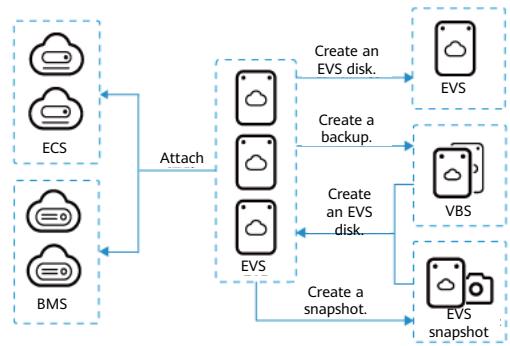
- Block storage chunks data into arbitrarily organized, evenly sized volumes and stores them as separate pieces. Each block of data is given a unique identifier, which allows a storage system to place the smaller pieces of data wherever is the most convenient.
- In file storage, data is stored as a single piece of information inside a folder, just like you organize pieces of paper inside a manila folder. When you need to access that piece of data, your computer needs to know the path to find it. Data stored in files is organized and retrieved using a limited amount of metadata that tells the computer exactly where the file itself is kept. It is like a library card catalog for data files.
- Object storage, also known as object-based storage, is a flat structure in which files are broken into pieces and spread out among hardware. In object storage, the data is broken into discrete units called objects and is kept in a single repository, instead of being kept as files in folders or as blocks on servers. A universally unique identifier is assigned to every object in an OBS system and allows the object storage system to differentiate objects from one another and find the data without needing to know the exact physical drive, array, or site where the data is.
- EVS works as the block storage service and provides block storage resources for upper-layer applications. SFS works as the block storage, stores files for the video cloud and media cloud, and can be used as content resource pools. OBS 3.0 works as the object storage service and is used as an image resource pool for backup and archiving.

Contents

1. Overview of HUAWEI CLOUD Stack Basic Storage Services
2. **Introduction to HUAWEI CLOUD Stack Storage Services**
 - EVS
 - SFS
 - OBS
3. Storage Solution Design

EVS

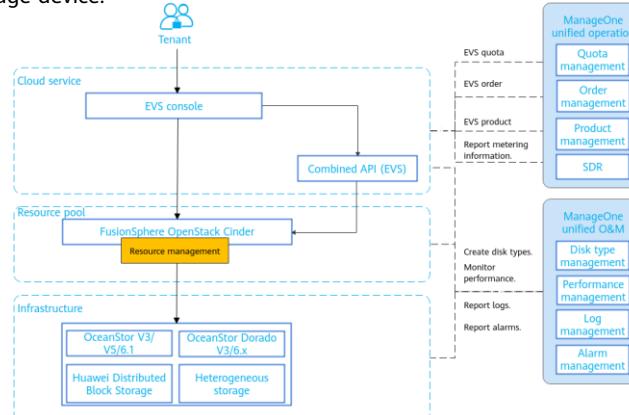
- EVS is a virtual block storage service which provides block storage space for Elastic Cloud Servers (ECSs) and Bare Metal Servers (BMSs). You can create EVS disks on the console and attach them to ECSs and BMSs. The method for using EVS disks is the same for using disks on physical servers. However, EVS disks have higher data reliability and I/O throughput, and are easier to use. They are suitable for file systems, databases, or system software or applications that require block storage devices.



- Elastic attaching and detaching: An EVS disk is like a raw, unformatted, external block device that you can attach to a single instance.
- Multiple disk types: A disk type represents storage backends used by a group of disks. You can divide types of EVS disks based on storage backend types to meet different performance requirements.
- Elastic scalability is supported and the maximum capacity of a single disk is 64 TB. You can configure the storage capacity as required.
- Snapshot: You can back up your data by taking a snapshot of your disk data at a specific point in time to prevent data loss caused by data tampering or misdeletion and ensure a quick rollback in the event of a service fault. You can also create disks from snapshots and attach them to other instances to provide data resources for a variety of services.
- Backup: You can create backups for EVS disks and restore EVS disks using backups.
- Shared disks are supported. Multiple instances can access (read and write) a shared disk at the same time, meeting the requirements of key enterprises that require cluster deployment and high availability (HA).

EVS Logical Architecture

- EVS includes components such as the EVS console, EVS service API, FusionSphere OpenStack Cinder, and storage device.



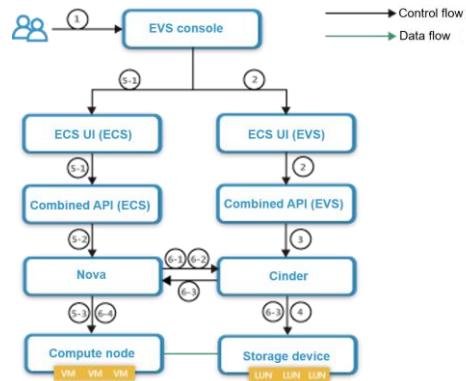
9 Huawei Confidential

HUAWEI

- **EVS console:** provides tenants with an entry to EVS. Tenants can apply for EVS disks on the console.
- **Combined API (EVS):** The EVS service API encapsulates or combines the logic based on the native Cinder interface to implement some EVS functions. The EVS service API can be invoked by the EVS console or tenants.
- **FusionSphere OpenStack Cinder:** provides persistent block storage to manage block storage resources. It is mainly used to create disk types in EVS. Disks are created on the storage device and attached to ECSs or BMSs.
- **Infrastructure:** refers to the physical storage device that provides block storage based on physical resources. The following storage devices can function as the storage backend of EVS: Huawei SAN storage (OceanStor V3/V5/6.1 and OceanStor Dorado V3/6.x), Huawei Distributed Block Storage, and heterogeneous storage (such as HP 3PAR 8000 series).
- **ManageOne unified operation:** provides quota management, order management, product management, and resource metering and charging for EVS.
- **ManageOne unified O&M:** provides disk type management, performance monitoring, logging, and alarm reporting for EVS.

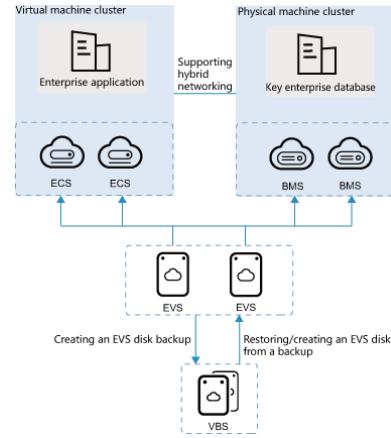
EVS Workflow

- The workflow is as follows:
 - A VDC administrator or VDC operator applies for storage resources on the EVS console.
 - The EVS console sends the request to the combined API (ECS) through ECS UI (EVS).
 - The combined API distributes the request to Cinder.
 - Cinder creates volumes in the storage pool according to the policy for storage resource application.
 - The VDC administrator or VDC operator attaches the requested storage resources to ECSS on the EVS console.
 - Nova instructs Cinder to attach EVS disks.



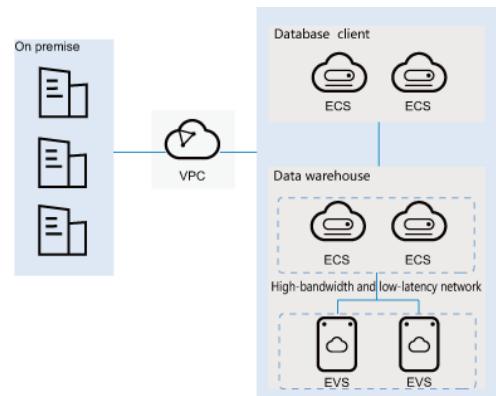
EVS Application Scenario: Relational Databases

- The core database of services needs to support mass access at traffic peaks, and requires disks with persistent and stable high performance and low latency. The disk type with ultra-high performance implements a combination of excellent performance and superior reliability, to meet low latency and high I/O performance needs in data-intensive scenarios, such as relational databases. The figure shows the scenario-based architecture. Disks with the ultra-high-performance service level offer the following specifications:
 - Latency: < 1 ms
 - Performance: 2000 IOPS/TB to 20,000 IOPS/TB



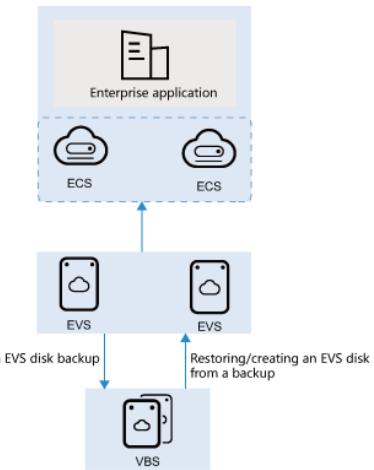
EVS Application Scenario: Data Warehouse

- Deploy data warehouses in scenarios with intensive data reads. It is recommended that you use the high-performance disk to meet the requirements for low latency, high read and write speed, and large throughput. The figure shows the scenario-based architecture. Disks with the high performance service level offer the following specifications:
 - Latency: 1 ms to 3 ms
 - Performance: 500 IOPS/TB to 4000 IOPS/TB



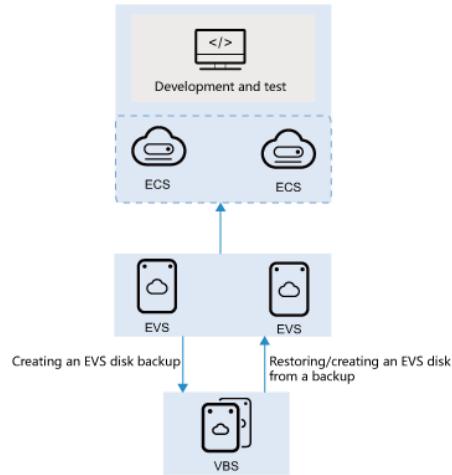
EVS Application Scenario: Enterprise Application System

- This scenario is mainly used to deploy key enterprise applications. It is recommended that you use medium-performance disks for scenarios that require common performance but rich enterprise-class features, such as common databases, application VMs, and middleware VMs. The figure shows the scenario-based architecture. Disks with the medium performance service level offer the following specifications:
 - Latency: 3 ms to 10 ms
 - Performance: 250 IOPS/TB to 1000 IOPS/TB



EVS Application Scenario: Development and Testing

- This scenario is used to deploy development and testing programs, in addition to deployment and O&M, which commonly run on common disks. The figure shows the scenario-based architecture. Disks with the common performance service level offer the following specifications:
 - Latency: 10 ms to 20 ms
 - Performance: 5 IOPS/TB to 25 IOPS/TB

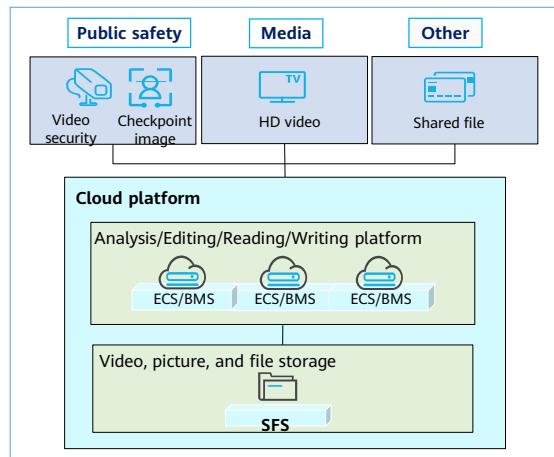


Contents

1. Overview of HUAWEI CLOUD Stack Basic Storage Services
2. **Introduction to HUAWEI CLOUD Stack Storage Services**
 - EVS
 - SFS
 - OBS
3. Storage Solution Design

SFS

- SFS provides an on-demand, scalable, and high-performance shared file system for ECSs. In compliance with the Network File System (NFS) and Common Internet File System (CIFS) protocols, SFS can support storage of PB-level files. With the scalable performance, SFS can seamlessly handle data-intensive and high-bandwidth applications.

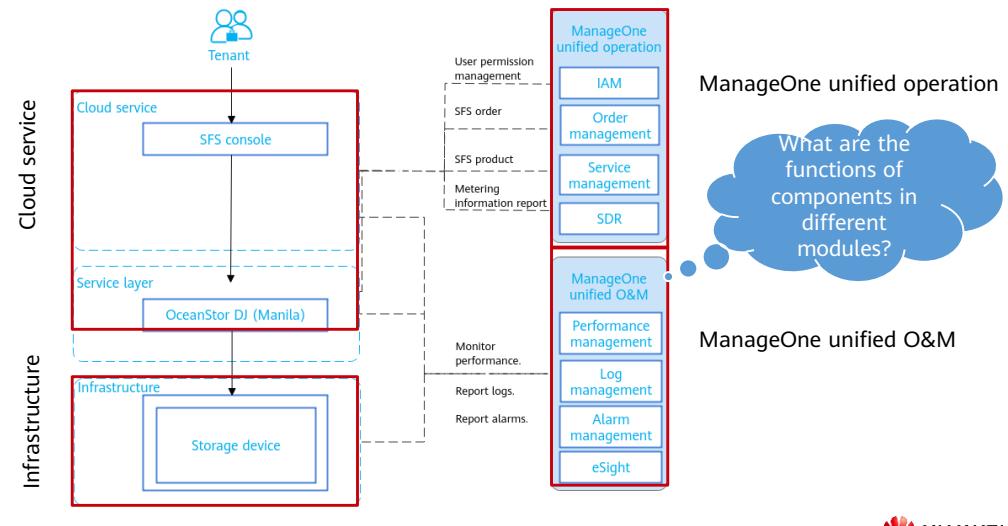


16 Huawei Confidential



- Before using SFS, pay attention to the following:
 - Before using SFS, you must create a file system.
 - After a file system is created, you need to attach it to an ECS.
 - You can manage file systems, including adjusting capacity, and viewing, uninstalling, restoring, and deleting file systems.

SFS Logical Architecture



17 Huawei Confidential

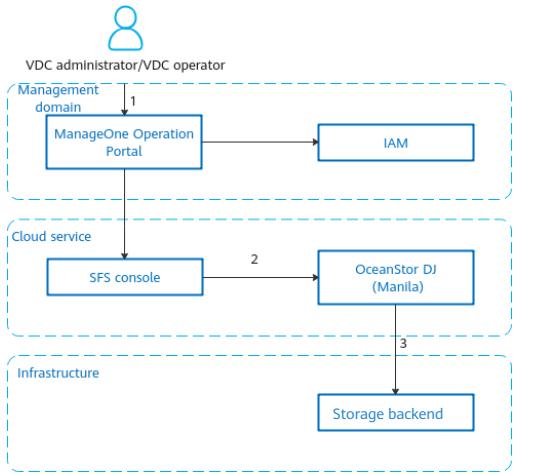
HUAWEI

- ManageOne unified operation includes the following components:
 - IAM: provides identity identification and access management for SFS.
 - Order management: manages orders submitted by users.
 - Service management: Different services are defined based on the registered cloud services, and unified service management is provided.
 - SDR: supports metering and billing for resources.
- ManageOne unified O&M includes the following components:
 - Performance management: monitors performance indicators of infrastructure and analyzes monitoring data.
 - Log management: aggregates operation and run logs of tenants and allows tenants to query logs.
 - Alarm management: supports the operations, such as receiving, storing, centrally monitoring, and centrally querying alarm data, helping O&M personnel quickly rectify faults based on alarm information.
 - eSight: provides performance monitoring and alarm generation for the storage device.

- Cloud service components include:
 - SFS console: provides the SFS management console.
 - OceanStor DJ (Manila): functions as the SFS server and receives requests from the SFS console.
- Infrastructure components include the file storage device that provides file system storage space for the SFS. The following storage devices are supported: OceanStor 9000, OceanStor Dorado 6.x, and OceanStor 6.1 series.

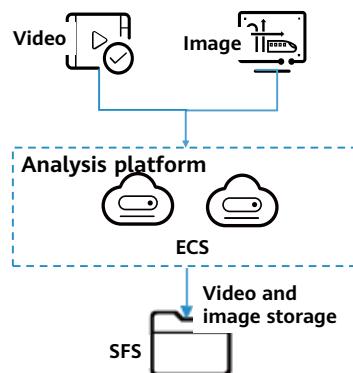
SFS Workflow

- A user applies for file storage resources on the SFS console.
- The SFS console invokes the API of OceanStor DJ (Manila) to deliver the request to the storage device.
- OceanStor DJ (Manila) invokes the storage device API to create or manage file systems.



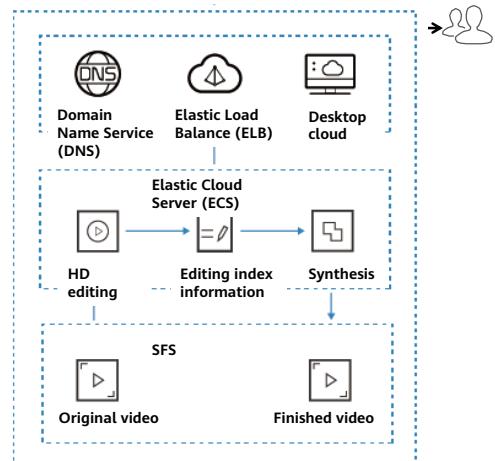
SFS Application Scenario: Video Cloud

- SFS is used to store video and image files for video cloud environments.
 - Generally, a video file is a large file of about 1 GB to 4 GB.
 - Images are classified into checkpoint images and analysis images. Generally, there are a mass number of small images (about 2 billion images per year) with sizes ranging from 30 KB to 500 KB.



SFS Application Scenarios: Media Processing

- High-bandwidth, large-capacity SFS is used for media processing. Shared file storage facilitates multi-layer HD and 4K video editing, transcoding, composition, and video on demand (VoD).

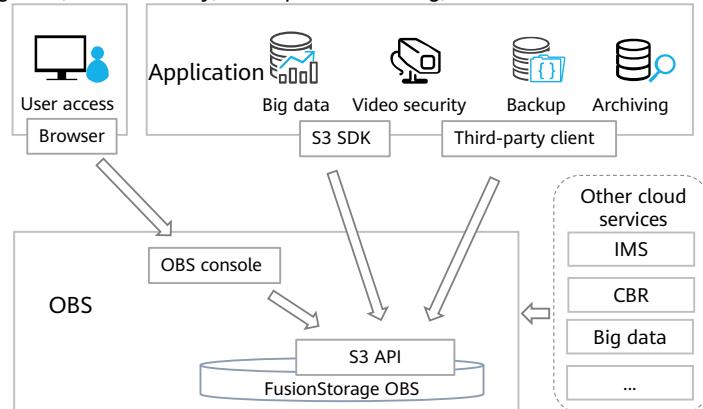


Contents

1. Overview of HUAWEI CLOUD Stack Basic Storage Services
2. **Introduction to HUAWEI CLOUD Stack Storage Services**
 - EVS
 - SFS
 - OBS
3. Storage Solution Design

OBS

- OBS features large capacity, elastic scalability, high reliability, and architecture decoupling. It can be used in big data, video security, backup and archiving, and other cloud services on the private cloud.



23 Huawei Confidential

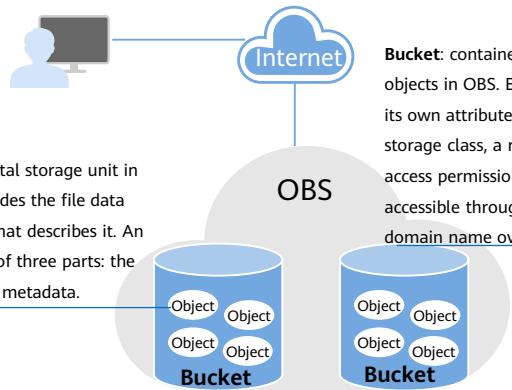
HUAWEI

- OBS is a cloud storage service that provides capabilities for mass, secure, reliable, and cost-effective data storage. With OBS, you can easily create, modify, and delete buckets, as well as uploading, downloading, and deleting objects. OBS is a cloud storage service that can store unstructured data such as documents, images, and audiovisual videos, combining the advantages of block storage (direct and fast access to disks) and file storage (distributed and shared).
- The OBS system and a single bucket do not have restrictions on the total data volume and number of objects or files, providing users ultra-large capacity to store files of any type. OBS can be used by common users, websites, enterprises, and developers. OBS provides APIs based on HTTP/HTTPS. Users can use the OBS console or client to access and manage data stored in OBS. Besides, OBS supports OBS APIs, facilitating data management and development of several types of upper-layer service application.

OBS Product Architecture and Related Concepts

- Bucket
- Object
- AK/SK
- Region
- Endpoint
- Quota

Object: a fundamental storage unit in OBS. An object includes the file data and any metadata that describes it. An object is composed of three parts: the data, a key, and the metadata.

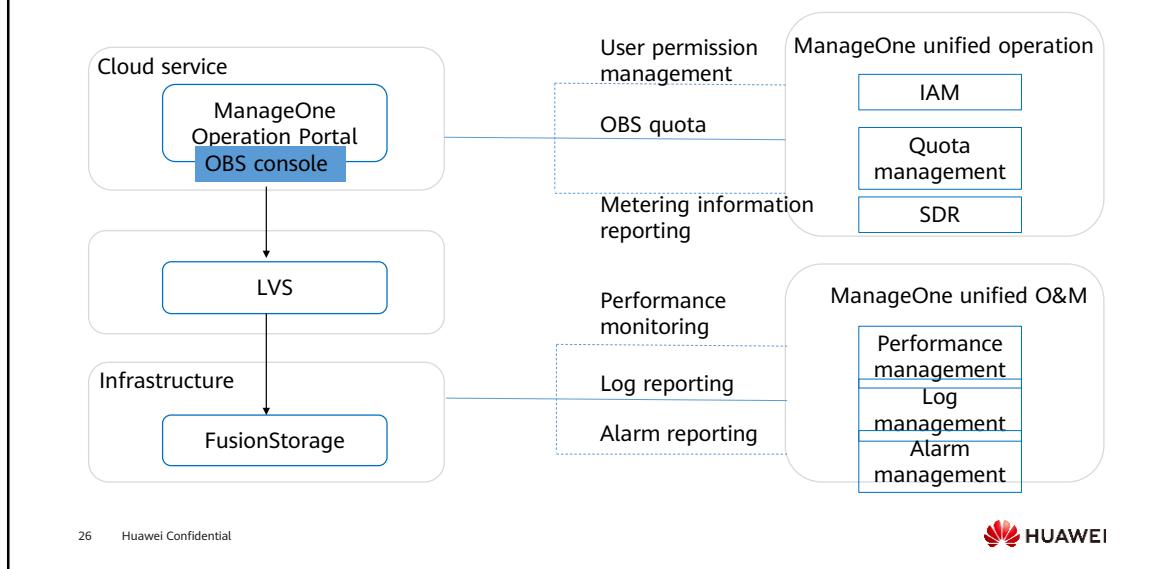


Bucket: containers for storing objects in OBS. Each bucket has its own attributes, such as a storage class, a region, and access permissions. A bucket is accessible through its access domain name over the Internet.

- A bucket is a container that stores objects in OBS. OBS provides flat storage in the form of buckets and objects. Unlike the conventional multi-layer directory structure of file systems, all objects in a bucket are stored at the same logical layer.
- Each OBS bucket name must be unique and cannot be changed. When a bucket is created, its access control list (ACL) is generated by default. The items in the ACL include permissions of authorized users such as the read (READ), write (WRITE), and full control (FULL_CONTROL) permissions. Only the user with required permission can operate the bucket.
- An object is a basic data storage unit of OBS. It consists of file data and metadata that describes the data attributes. Data uploaded to OBS is stored into buckets as objects.

- An object consists of data, metadata, and a key.
 - A key specifies the name of an object. An object key is a string ranging from 1 to 1024 characters in UTF-8 format. Each object in a bucket must have a unique key.
 - Metadata describes the object. Metadata contains system metadata and user metadata. All the metadata is uploaded to OBS as key-value pairs. System metadata is automatically generated by OBS and is used for processing object data. It includes object attributes such as **Date**, **Content-length**, **Last-modify**, and **Content-MD5**. User metadata is specified by users to describe objects when they upload the objects.
 - Data is the information contained in an object.
- OBS supports Access Key ID (AK)/Secret Access Key (SK) authentication, that is, OBS authenticates the ID of a request sender through AK and SK encryption.
- Endpoint: OBS provides an endpoint for each region. An endpoint can be regarded as the domain name of OBS in a region and is used to process access requests in the region.

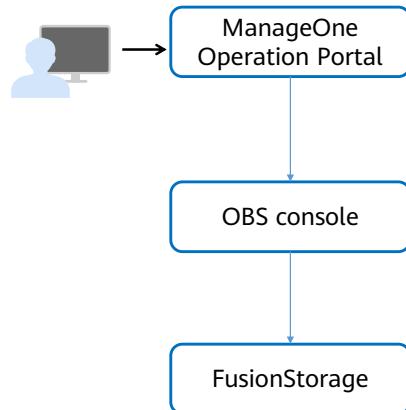
OBS Logical Architecture



- On the OBS console of ManageOne Maintenance Portal, users can use the LVS common component to invoke FusionStorage storage resources.

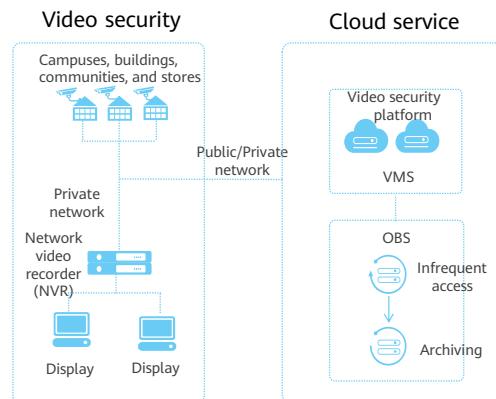
OBS Workflow

- A resource administrator applies for object storage resources on the OBS console.
- The OBS console invokes the S3 APIs of the FusionStorage object and Hadoop Distributed File System (HDFS) storage device to create a bucket.



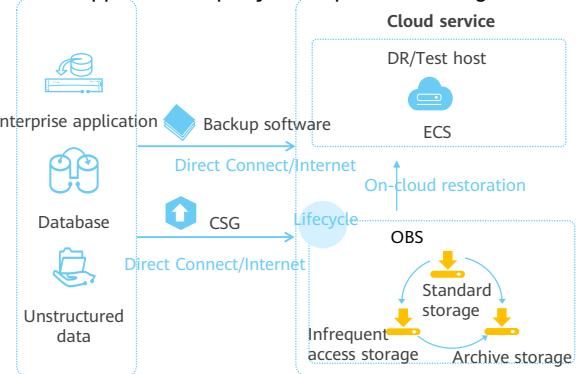
OBS Application Scenario: Video Security

- OBS provides large storage capacity for video security solutions to store mass unstructured video data as high-quality files.



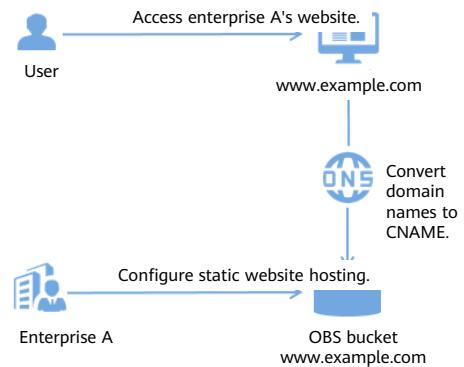
OBS Application Scenario: Backup and Archiving

- OBS is a durable, expandable, and secure solution for backing up and archiving users' key data. Its high durability and secure infrastructure provide an advanced data protection and disaster recovery (DR) solution. OBS supports third-party backup and archiving software.



OBS Application Scenario: Hosting a Static Website in OBS

- Scenario description: A customer wants to host a static website in OBS.
- Pain points: only static pages available on the website
- Solution: Use static website hosting of OBS.
 - Step 1: Prepare static website pages.
 - Step 2: Upload the page files to a bucket.
 - Step 3: Enable static website hosting for the bucket.



Comparison Between EVS, OBS, and SFS

Item	EVS	SFS	OBS
Usage mode	Provides persistent block storage for compute services such as ECS and BMS. EVS disks feature high availability, high durability, and low latency. Users can format, create file systems, and persistently store data on EVS disks.	Provides ECSS with a high-performance shared file system that supports on-demand auto scaling. The file system complies with the standard file protocols and delivers scalable performance, supporting mass amount of data and bandwidth-demanding applications.	Provides REST APIs that are compatible with Amazon S3. Users can use browsers or third-party tools to access OBS and use RESTful APIs to perform secondary development on OBS.
Data access mode	Limits data access within the internal network of a data center.	Limits data access within the internal network of a data center.	Allows data access on the public network, meeting requirements of Internet applications.
Sharing mode	Supports EVS disk sharing. A shared EVS disk can be attached to up to 16 ECSS in the cluster management system.	Supports data sharing. A file system can be mounted to a maximum of 256 ECSS.	Supports data sharing. Anonymous access is allowed, and the quantity of access users is unlimited.
Storage capacity	A single disk supports a maximum of 64 TB.	The maximum capacity of a single file is 240 TB, and the file system capacity can be scaled to the PB level.	The capacity is unlimited. Therefore, planning is not required.
Storage backend	Supports Huawei SAN storage, FusionStorage, and heterogeneous storage.	OceanStor 9000	FusionStorage OBS
Recommended scenario	Database, enterprise office applications, and development and testing	Media processing and file sharing	Big data storage, video security storage, and backup and archiving. It can also provide storage for other private cloud services (such as IMS).

Contents

1. Overview of HUAWEI CLOUD Stack Basic Storage Services
2. Introduction to HUAWEI CLOUD Stack Storage Services
- 3. Storage Solution Design**

Storage Solution Design Discussion

Background: A large video website supports mass video upload/download, VOD, bullet comments, and forum functions. Video uploaders, video browsing users, and platform maintenance personnel demand excellent user experience. It is your job to design the corresponding solution.

- Which of the following cloud storage services do you recommend? Why?
A. EVS B. OBS C. SFS
- Key points:
 - Mass data
 - Visitors log in to the GUI and there is service traffic generated.
 - The overall solution needs to be implemented with other computing and network services.

Quiz

1. (True or false) The general migration function of EVS disks cannot be implemented online.
 - A. True
 - B. False
2. (Single-answer question) How many servers can a shared EVS disk be attached to at most?
 - A. 5
 - B. 7
 - C. 8
 - D. 16

- Answers:

- B
 - D

Summary

- This course focused on:
 - HUAWEI CLOUD Stack basic storage services.
 - Functions, features, and application scenarios of EVS, SFS, and OBS.

Acronyms

Acronym	Full Name	Description
BMS	Bare Metal Server	BMS provides dedicated physical servers for tenants.
ECS	Elastic Cloud Server	An ECS is a computing server that consists of CPUs, memory, images, and EVS disks and allows on-demand allocation and elastic scaling.
ELB	Elastic Load Balance	ELB is a service that automatically distributes incoming traffic across multiple backend cloud servers based on a specified forwarding policy.
EVS	Elastic Volume Service	EVS is a virtual block storage service, which provides block storage space for ECSs and BMSs.
OBS	Object Storage Service	OBS is an object-based storage service that provides mass, secure, highly reliable, and low-cost data storage.
SFS	Scalable File Service	SFS provides a scalable and high-performance shared file system for ECSs.
VDC	Virtual Data Center	A VDC is a new type of data center that applies cloud computing to Internet data center (IDC).
VPC	Virtual Private Cloud	A VPC provides an isolated virtual network for cloud servers.

Recommendations

- Huawei Talent:
 - <https://e.huawei.com/en/talent/portal/#/>
- Huawei Certification:
 - <https://forum.huawei.com/enterprise/en/Huawei-Technical-Certification/forum/911>

Thank you.

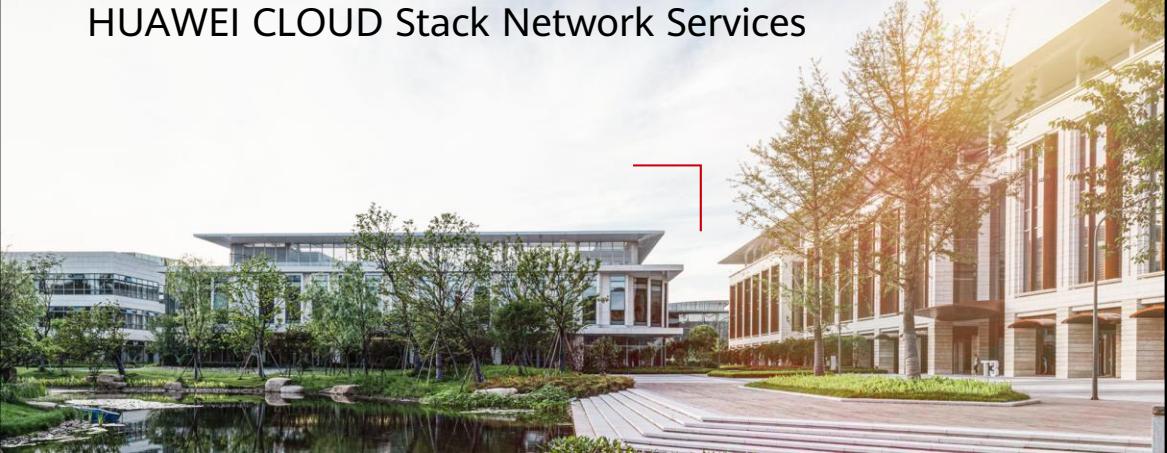
把数字世界带入每个人、每个家庭。
每个组织，构建万物互联的智能世界。
Bring digital to every person, home, and organization for a fully connected, intelligent world.

Copyright©2022 Huawei Technologies Co., Ltd.
All Rights Reserved.

The information in this document may contain predictive statements including, without limitation, statements regarding the future financial and operating results, future product performance, market position, etc. There are numerous factors that could cause actual results and developments to differ materially from those expressed or implied in the predictive statements. Therefore, such information is provided for reference purpose only and constitutes neither an offer nor an acceptance. Huawei may change the information at any time without notice.



HUAWEI CLOUD Stack Network Services



Foreword

- This course describes network services at the IaaS layer of HUAWEI CLOUD Stack, including general network services and network interworking services.

Objectives

- Upon completion of this course, you will understand:
 - What HUAWEI CLOUD Stack network services are.
 - The functions, architectures, and use cases of VPC, SG, Network ACL, EIP, and ELB.
 - The network interworking solutions for different scenarios.

Contents

- 1. Overview of HUAWEI CLOUD Stack Network Services**
2. General Network Services
3. Interworking Services
4. Value-Added Services
5. Network Design

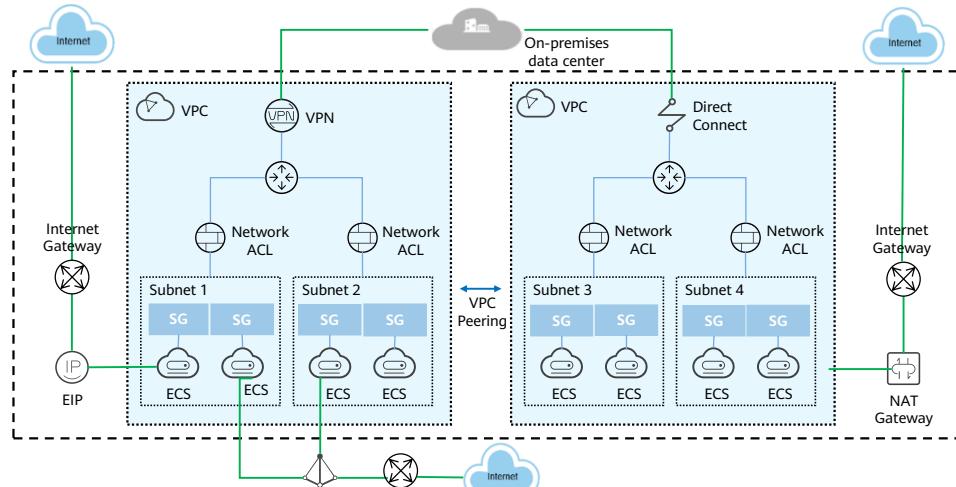
Network Services on the Tenant Portal

- After logging in to ManageOne Operation Portal as a tenant, you can see network services in the service list. You can apply for a network service only after the administrator finished dividing external networks on Service OM.

The screenshot shows the ManageOne Tenant Portal interface. At the top, there is a navigation bar with tabs: Home, Resources, Application, Report, System, and Eng. Below the navigation bar, there are two dropdown menus: Region (set to Hangzhou) and Resource Set (set to zj-hz-1_zhangsan). A search bar below the dropdowns contains the placeholder text "Enter a name to search for a service." Under the search bar, there is a section titled "Basic cloud services" which is divided into three columns: Computing, Storage, and Network. The Network column is highlighted with a red box. The services listed under Network are: Virtual Private Cloud, Elastic Load Balance, Elastic IP, Network ACL, Virtual Private Network, Direct Connect, VPC Endpoint, Cloud Domain Name Service, and Cloud Firewall.

Computing	Storage	Network
Service_154c	Cloud Server Backup Service	Virtual Private Cloud
Image Management Service	Volume Backup Service	Elastic Load Balance
Cloud Container Engine	Elastic Volume Service	Elastic IP
Auto Scaling	Object Storage Service 3.0	Network ACL
Elastic Cloud Server		Virtual Private Network
Bare Metal Server		Direct Connect
		VPC Endpoint
		Cloud Domain Name Service
		Cloud Firewall

HUAWEI CLOUD Stack Network Service Overview



6 Huawei Confidential

 HUAWEI

- There are the following types of network services:
 - General network cloud services: VPC, SG, Network ACL, and ELB
 - Intra-cloud communications: VPCEP and VPC Peering
 - Cross-region communications on the cloud: CC and VPN
 - Communications between a cloud and the Internet: EIP and NAT Gateway
 - Communications between a cloud and a local data center: VPN and Direct Connect
- Cloud Domain Name Service (CloudDNS):
 - CloudDNS provides highly available and scalable authoritative DNS services that translate domain names into IP addresses required for network connection, reliably directing end users to your applications.

Network Services and Bearer NEs

Service	Mandatory/Optional	NE
Virtual Private Cloud (VPC)	Mandatory	vRouter/Border Router
Security Group (SG)	Mandatory	N/A
Network ACL	Mandatory	N/A
Elastic IP (EIP)	Mandatory	ENAT (co-deployed with vRouter)
Elastic Load Balance (ELB)	Optional	CVS/Nginx
Virtual Private Network (VPN)	Optional	VGW
Direct Connect	Optional	Basic Direct Connect: vRouter Enhanced Direct Connect: L3GW
NAT Gateway	Optional	NATGW
VPC Endpoint (VPCEP)	Optional	EGW
Layer 2 Bridge (L2BR)	Optional	L2BR
Cloud Connect (CC)	Optional	vRouter

Contents

1. Overview of HUAWEI CLOUD Stack Network Services

2. General Network Services

- VPC

- Security Group and Network ACL

- ELB

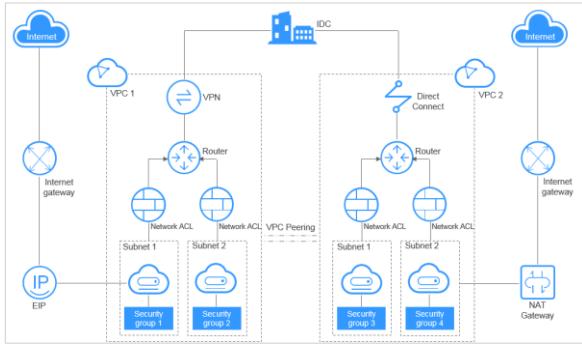
3. Interworking Services

4. Value-Added Services

5. Network Design

Virtual Private Cloud

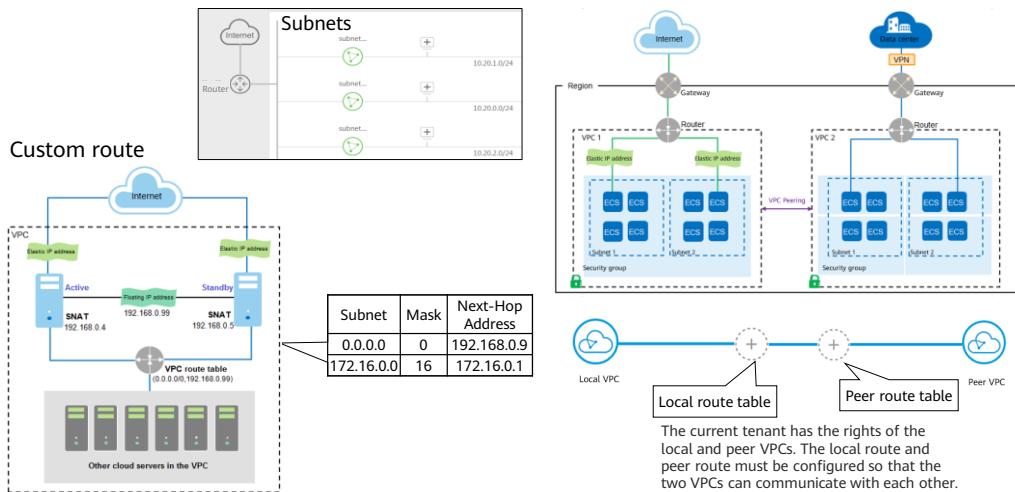
- Virtual Private Cloud (VPC) enables you to provision logically isolated, configurable, and manageable virtual networks for cloud servers, improving the security of system resources and simplifying network deployment. Cloud servers can be Elastic Cloud Servers (ECSs) or Bare Metal Servers (BMSs).



- You can select **IP address ranges**, create **subnets**, customize **security groups**, and configure **route tables** and **gateways**. With a VPC, you can easily manage and configure internal networks and change network configurations flexibly and securely. You can also customize access rules to control cloud server access within a security group and across different security groups and network ACLs to control cloud server access in subnets.

- Almost all network cloud services are associated with VPC. VPC is the core of these services.

VPC-related Concepts

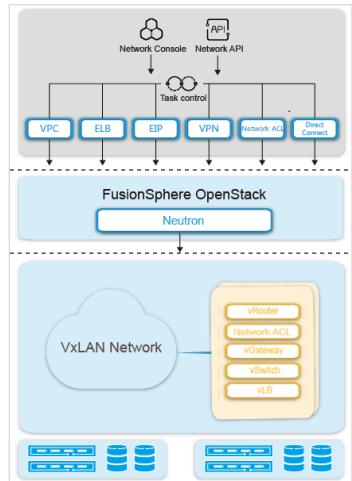


10 Huawei Confidential



- A subnet is a CIDR block in a VPC. Multiple subnets can be created for a VPC to manage cloud servers with different service requirements and provide cloud servers with IP address management and DNS services.
- By default, cloud servers in all subnets of the same VPC can communicate with one another, while cloud servers in different VPCs cannot.
- You can use desired routing policies to control network traffic forwarding on your VPC, the Internet, and a hybrid cloud.
- For details about VPC Peering, see the following sections.

VPC Logical Architecture



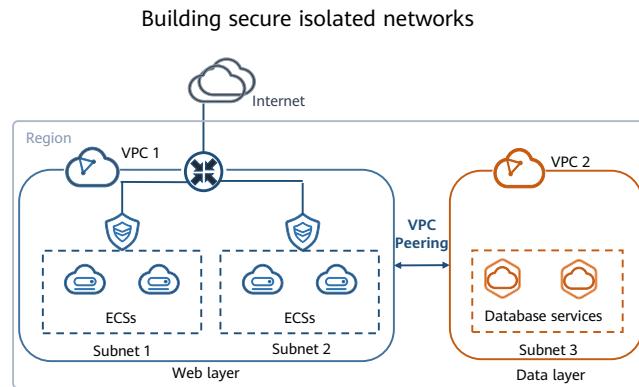
Service presentation and O&M layer:
Provides the GUI for users.

Service collaboration layer:
Implements collaboration among compute,
storage, and network resources.

Network control layer and resource pool:
Provides software-based distributed virtual network
functions including vSwitch, vFW, and vRouter.

- When a user performs VPC-related operations on ManageOne Operation Portal, the instructions sent by the user are interconnected with FusionSphere OpenStack, which invokes the Neutron component to provision underlying network resources.

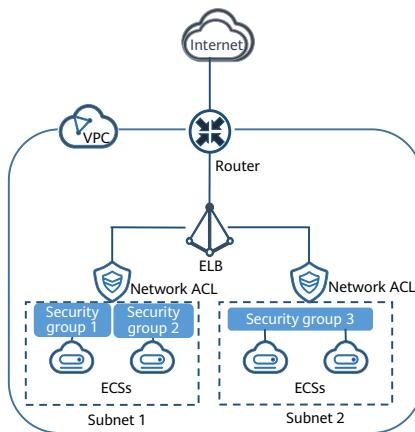
VPC Use Case: Building Secure Isolated Networks



- VPC allows you to deploy a network environment that is isolated from the Internet. You can place multi-tier web applications into different security zones, and configure access control rules for each security zone as required. For example, you can create two VPCs, add web servers to one VPC, and add database servers to the other. Then, you can create security groups and network ACLs for the two VPCs and configure inbound and outbound rules so that the web servers can communicate with the extranet while the database servers cannot communicate with the extranet. The purpose is to achieve security protection on database servers, meeting high security requirements.

VPC Use Case: Hosting Web Applications

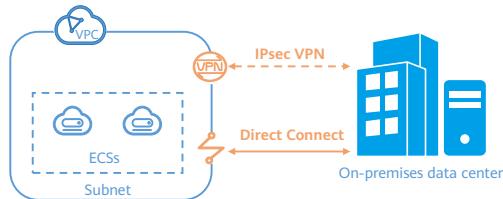
Hosting common web applications



- You can deploy common web applications in a VPC.
- You can use an EIP or NAT gateway to let web applications communicate with the extranet. You can use security groups and network ACLs to perform access control, achieving security protection on web applications. You can use load balancers to handle traffic bursts.

VPC Use Case: Connecting to On-Premises Data Centers

Extending your corporate network into the cloud



- You can use a VPN or Direct Connect connection to connect a VPC to your local data center.
- You can deploy applications in the cloud and deploy database servers in your local data center. Resources for applications in the cloud are highly scalable. You can connect a VPC to your local data center. This reduces IT O&M costs and protects enterprise core data from being leaked, allowing you to easily deploy hybrid clouds.

Contents

1. Overview of HUAWEI CLOUD Stack Network Services

2. General Network Services

- VPC

- Security Group and Network ACL

- ELB

3. Interworking Services

4. Value-Added Services

5. Network Design

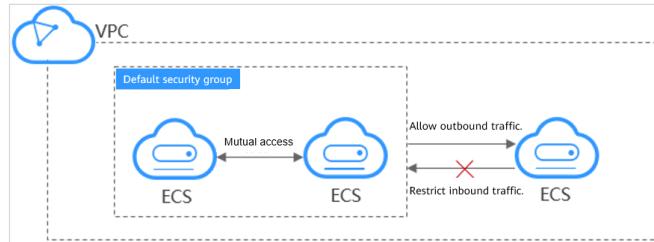
- Next, we need to consider how to filter traffic of compute instances or CIDR blocks in a VPC to ensure service security. Let's talk about Security Group and Network ACL.

Security Group

- A security group is a collection of access control rules for cloud servers that have the same security requirements and are mutually trusted within a project. A whitelist policy (allowed rules) is supported. You can define inbound and outbound rules to control traffic to and from the cloud servers in a security group, making your VPC more secure.

Your account automatically comes with a default security group that allows all outbound traffic and denies all inbound traffic. Your cloud servers in this security group can communicate with each other without any additional rules configured.

East-west traffic protection: Security groups provide VM NIC-specific protection for east-west traffic.



- Security Group provides rules for filtering the network packets sent and received by VM ports. After a VM port is associated with a security group, rules provided by the security group are used for filtering network packets sent and received by the VM port. Only the packets that comply with the rules are allowed to pass.

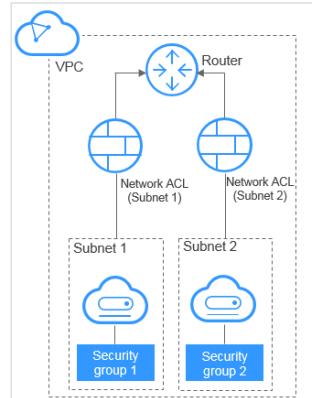
Network ACL

- A network ACL is an optional layer of security at the subnet level. It uses inbound and outbound access control list (ACL) rules associated with subnets to control data flows in and out of subnets. It supports blacklists and whitelists (allow and deny rules).

East-west traffic protection: Network ACLs provide subnet-specific protection for east-west traffic.

North-south traffic protection: Inter-VPC traffic such as EIP and VPC interworking traffic is protected by network ACLs.

A network ACL is an **optional** layer of security for your subnets. After you associate one or more subnets with a network ACL, you can control traffic in and out of the subnets. A network ACL can be associated with multiple subnets. However, each subnet can only be added to a single network ACL.



Network ACL vs Security Group

Item	Security Group	Network ACL
Protection object	Operates at the ECS level.	Operates at the subnet level
Configuration policy	Only supports allow rules.	Supports both allow and deny rules.
Priority	If rules conflict, the overlapping elements of these rules take effect.	If rules conflict, the rule with the highest priority takes effect.
Application operation	By default, you must select a security group when creating an ECS. The selected security group takes effect for that ECS.	You cannot select a network ACL when creating a subnet. You must create a network ACL, associate subnets with the network ACL, add inbound and outbound rules, and enable the network ACL. Then, the network ACL takes effect for the associated subnets and ECSSs in the subnets.
Packet filtering	Only supports packet filtering based on a 3-tuple (protocol, port, and destination IP address).	Supports packet filtering based on a 5-tuple (protocol, source port, destination port, source IP address, and destination IP address).

- Network ACL and Security Group use Linux iptables at the underlying layer. In essence, Network ACL and Security Group realize security control by means of the OVS security module, that is, orchestrating iptables capabilities.
- Network ACL and Security Group share the security policy capacity because they share one module at the underlying layer. Network ACL and Security Group reuse the resource usage and throughput performance of OVS

Contents

1. Overview of HUAWEI CLOUD Stack Network Services

2. General Network Services

- VPC
- Security Group and Network ACL
- **ELB**

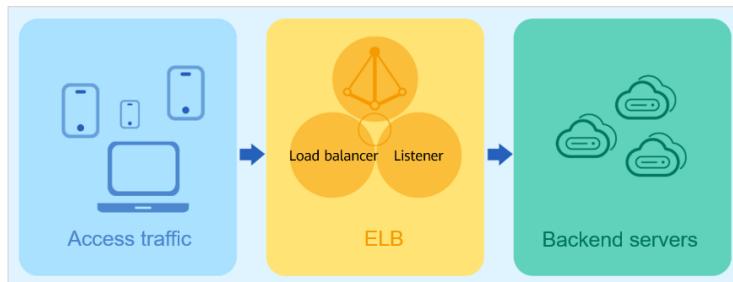
3. Interworking Services

4. Value-Added Services

5. Network Design

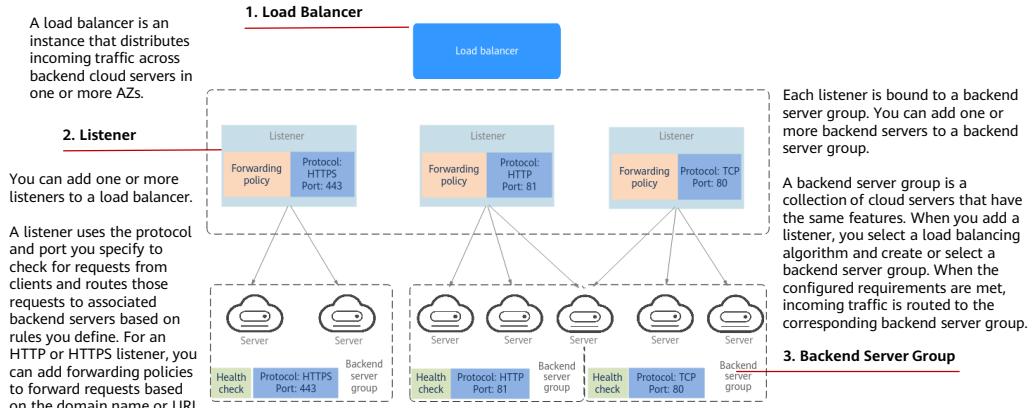
Elastic Load Balance

- Elastic Load Balance (ELB) is a service that automatically distributes incoming traffic across multiple backend cloud servers based on predefined forwarding policies. ELB can expand the access handling capability of application systems through traffic distribution and achieve a higher level of fault tolerance and performance. ELB also improves system availability by eliminating single points of failure (SPOF).



- A backend cloud server processes client requests forwarded by a load balancer. When adding a listener to a load balancer, you specify a backend server group to receive requests from the load balancer using the port and protocol you specify for the backend server group and the load balancing algorithm you select.
- A backend server group is a collection of cloud servers that have the same features. When you add a listener, you select a load balancing algorithm and create or select a backend server group. When the configured requirements are met, incoming traffic is routed to the corresponding backend server group.

ELB-related Concepts



- **Load balancer:** Load balancer object. You need to specify a virtual IP address.
- **Listener:** You need to specify the listening protocol number and port number. A listener is a process that checks for connection requests using a protocol and port for connections from clients to the load balancer, and a protocol and port for connections from the load balancer to backend cloud servers.
- You can also configure health checks for a backend server group to check the health of backend servers in the group. When a backend server is unhealthy, the load balancer stops routing new requests to this server until it recovers.

ELB Functions



Auto Scaling

- ELB seamlessly integrates with AS to automatically expand load distribution and backend processing capabilities based on traffic volume, ensuring service availability.



Sticky Sessions

- Access requests from a given user within a certain period of time are forwarded to the same backend cloud server for processing, which ensures user access continuity.



Multi-Protocol Support

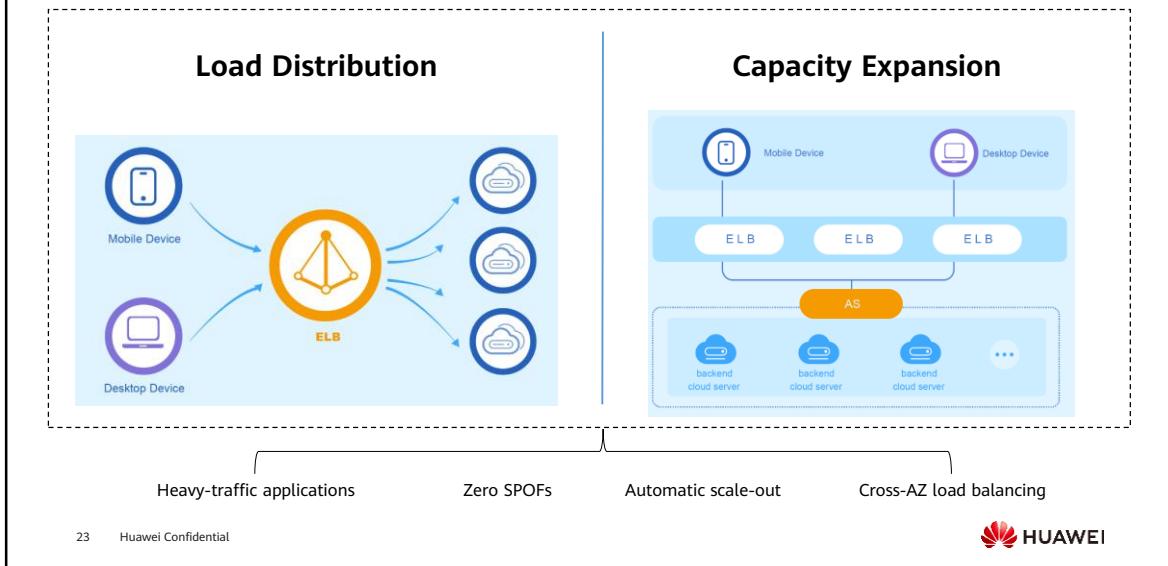
- TCP, UDP, HTTP, and HTTPS are all supported, making it easier to meet requirements for high performance, massive concurrent connections, and flexible and secure services.



Health Check

- The statuses of backend cloud services are periodically checked to ensure that traffic is being forwarded to normal backend cloud servers to ensure high availability.

ELB Use Cases

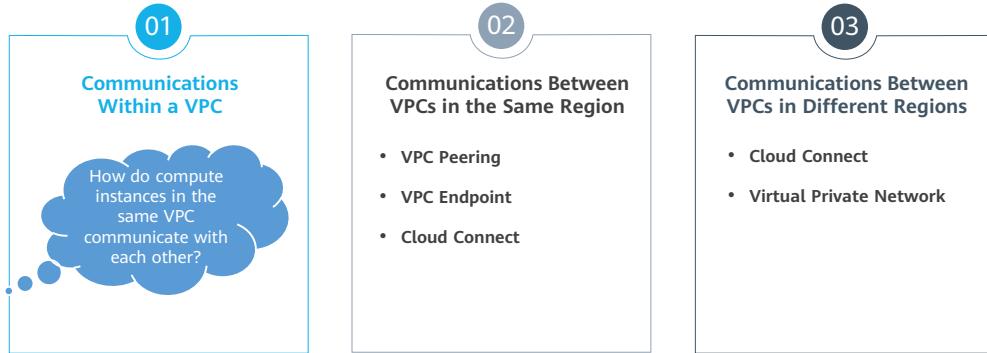


- **Load Distribution:** For websites with heavy traffic or internal office systems of governments or enterprises, ELB helps distribute service loads to multiple backend cloud servers, improving service processing capabilities. ELB also performs health checks on backend cloud servers to automatically remove malfunctioning ones and redistribute service loads among backend cloud server groups. A backend cloud server group consists of multiple backend cloud servers.
- **Capacity Expansion:** In scenarios where traffic fluctuates obviously, for example, video or e-commerce websites that feature unpredictable service expansion, ELB can automatically scale its handling capacity. The backend cloud server group can work with Auto Scaling (AS) to ensure smooth and stable operations while minimizing the costs.
- For services with high volume of traffic, ELB is used to improve the access efficiency.
- For services that require high reliability, ELB can be used to eliminate single points of failure, and cross-AZ load balancing can be used to ensure service continuity.
- In a system that needs to scale out, ELB can work with AS so that the system can automatically add or remove backend cloud servers. This improves service scalability.

Contents

1. Overview of HUAWEI CLOUD Stack Network Services
2. General Network Services
- 3. Interworking Services**
 - Intra-Cloud Communications
 - Communications Between the Cloud and the Internet
 - Communications Between the Cloud and On-Premises Data Centers
4. Value-Added Services
5. Network Design

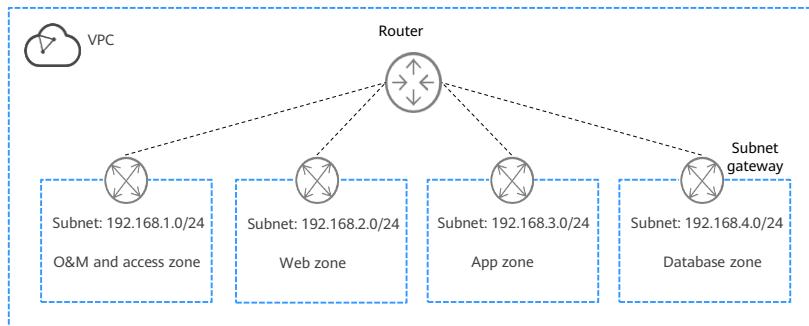
Intra-Cloud Communications



- This section describes network services of HUAWEI CLOUD Stack based on network interworking in the same VPC, network interworking between different VPCs in a region, and network interworking between different VPCs in different regions.
- You can use the default routes of a VPC to enable communications between compute instances in the VPC. You can also configure custom routes, security groups, and network ACLs to control communications between compute instances in the VPC.
- Different VPCs in a region can communicate with each other through VPC Peering, VPCEP, and CC.
- Different VPCs in different regions can communicate with each other through services such as CC and VPN.

Communications Within a VPC

- By default, all ECSs in subnets of the same VPC can communicate with each other. You can use security groups or network ACLs to control incoming and outgoing traffic.

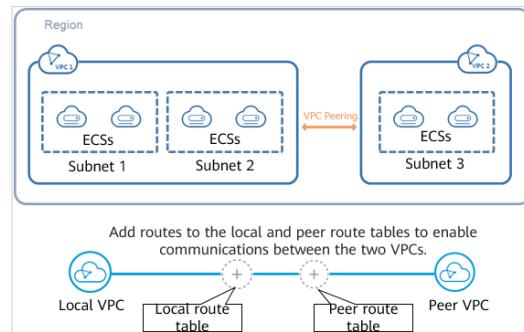


- By default, ECSs in all subnets of the same VPC can communicate with one another, but ECSs in different VPCs cannot. When you create a VPC, the system automatically creates a default route table. The routes in the default route table ensure that all subnets in the VPC can communicate with each other. You can also add custom routes to route traffic to a specified destination.
- Setting up a website:
 - Deploy all servers in one VPC so that they can communicate with each other.
 - Create separate subnets for web, application, and database zones.
 - Create a subnet for the O&M and access zone, which is used to deploy bastion hosts or management and authentication devices, facilitating remote access, service deployment, and O&M.
 - Configure network ACLs for subnets to control traffic between them.

Communications Between Different VPCs in the Same Region: VPC Peering

- A VPC peering connection uses private IP addresses to route traffic between two VPCs. ECs in either VPC can communicate with each other just as if they were in the same VPC.

If a VPC peering connection is established between two VPCs, add routes to the VPCs so that they can communicate with each other.

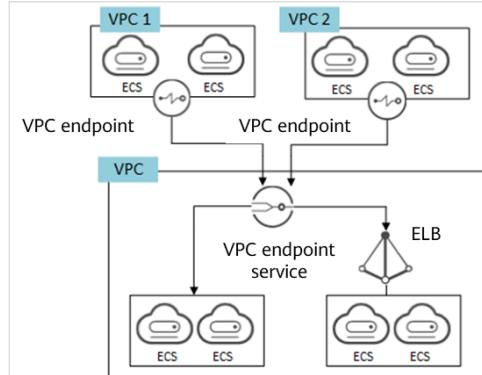


- A VPC peering connection can be created between two VPCs in the same region. VPCs can belong to different tenants.
- Only one VPC peering connection can be created between two VPCs.
- A VPC peering connection is actually used to connect two CIDR blocks in two VPCs. The two CIDR blocks cannot overlap.
- After a VPC peering connection is created, you need to add routes for the local and peer VPCs to enable communications between the two VPCs.
- Peering relationships are not transitive. For example, even if there are peering connections between VPC 1 and VPC 2 and between VPC 1 and VPC 3, those connections do not enable communications between VPC 2 and VPC 3.

VPC Endpoint

- VPC Endpoint (VPCEP) is a cloud service that extends VPC capabilities. It provides secure and private channels to connect VPCs to endpoint services, providing powerful and flexible networking without having to use EIPs.

VPCEP consists of two types of resources: VPC endpoint services that are created by service providers, and VPC endpoints that are created by service users.



- VPCEP provides two types of resources: VPC endpoint services and VPC endpoints.
- VPC endpoint services: cloud services or users' private services that can be configured in VPCEP to provide services to users. For example, you can create an application in a VPC and configure it as a service supported by VPCEP. This service is a VPC endpoint service.
- VPC endpoints are channels for connecting VPCs to VPC endpoint services. You can create an application in your VPC and configure it as a VPC endpoint service. A VPC endpoint can be created in another VPC in the same region and then used as a channel to access the VPC endpoint service.

Communications Between VPCs in the Same Region: VPC Peering and VPC Endpoint

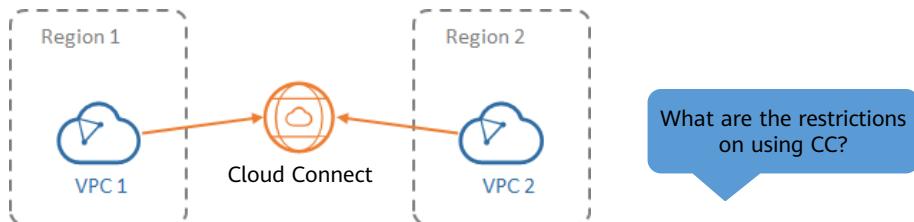


Item	VPC Peering	VPC Endpoint
Security	All resources in a VPC, such as ECSS, load balancers, and virtual IP addresses, are accessible.	Only the ECSS, load balancers, and virtual IP addresses in the VPC for which VPC endpoint services are created can be accessed.
CIDR block overlap	Not supported	Supported
VPN and Direct Connect	Not supported	Supported

- Cloud Connect can also be used to enable communications between VPCs in the same region.

Communications Between Different VPCs in Different Regions: Cloud Connect

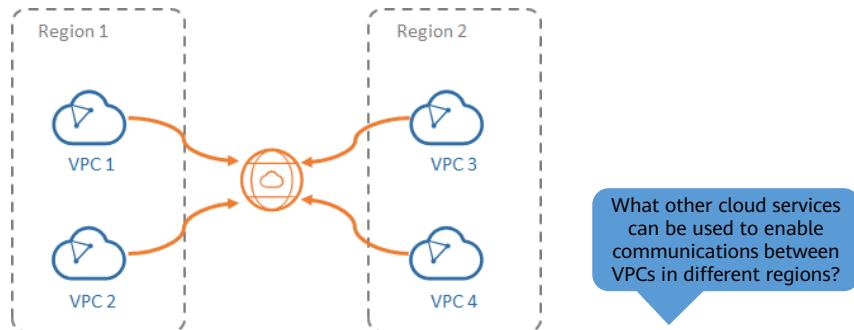
- Cloud Connect (CC) allows you to quickly build stable, high-speed, and high-quality networks between VPCs across regions.
- With CC, you can load network instances in different regions to a cloud connection to enable communications between private networks. The network instances can be VPCs in the same region or authorized VPCs in different regions.



- By default, a maximum of six network instances can be loaded to a cloud connection in each region.
- By default, a maximum of six regions where network instances can be loaded to a cloud connection are supported.
- A VPC can be loaded to only one cloud connection.
- A maximum of 50 CIDR blocks can be loaded to each network instance.
- For a cloud connection, ensure that the CIDR blocks of all network instances do not overlap and that subnet CIDR blocks are unique. Otherwise, network communications may fail.
- When you load a VPC to a cloud connection and enter VPC CIDR blocks, loopback addresses, multicast addresses, or broadcast addresses are not allowed.

CC Use Case

- CC helps you establish secure and reliable private network communications among VPCs in different regions and create a network with a more flexible topology.



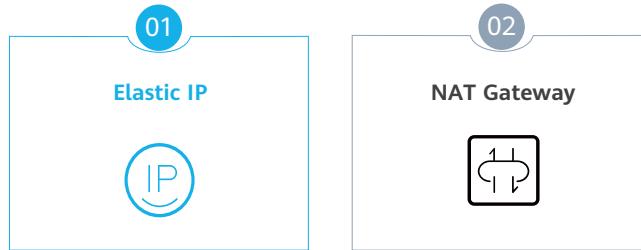
- VPN can be used to enable communications between VPCs in different regions and will be detailed later.

Contents

1. Overview of HUAWEI CLOUD Stack Network Services
2. General Network Services
- 3. Interworking Services**
 - Intra-Cloud Communications
 - **Communications Between the Cloud and the Internet**
 - Communications Between the Cloud and On-Premises Data Centers
4. Value-Added Services
5. Network Design

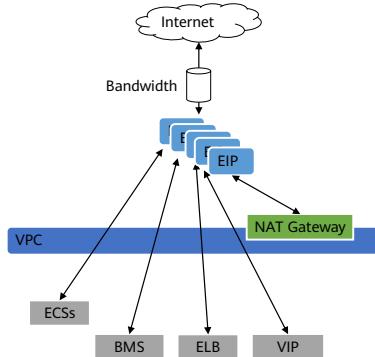
Communications Between the Cloud and the Internet

- Private and public IP addresses need to be translated for communications between a cloud and the Internet. Elastic IP and NAT Gateway can enable communications between a cloud and the Internet.

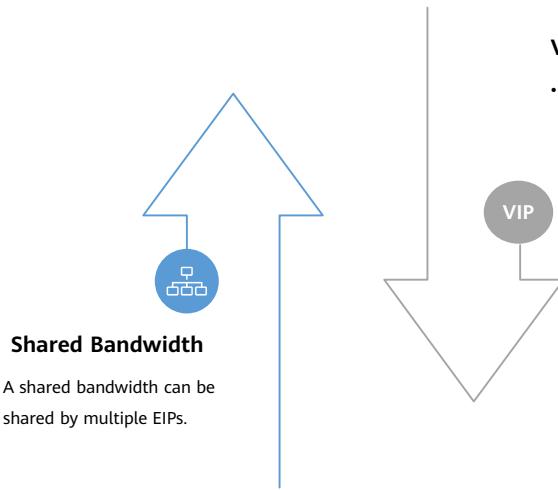


Elastic IP

- An elastic IP address (EIP) is a static IP address that can be directly accessed from an extranet. The extranet can be the Internet or an enterprise LAN. EIPs are mapped to bound instances using NAT.
- EIPs are mapped to cloud resources using NAT.
- Cloud resources can only communicate with the Internet when they have EIPs assigned.
- Both shared and dedicated bandwidths are supported.



EIP-related Concepts

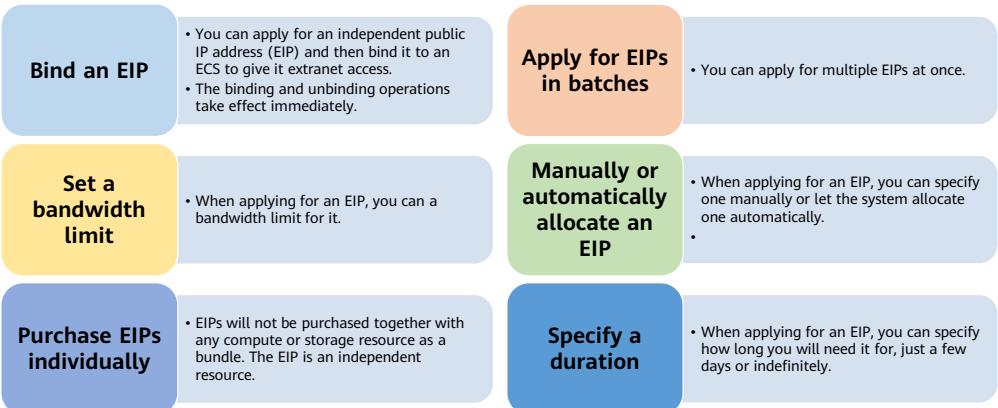


Virtual IP Address

- A virtual IP address (VIP) is a private IP address. You can use either of them to access cloud servers.

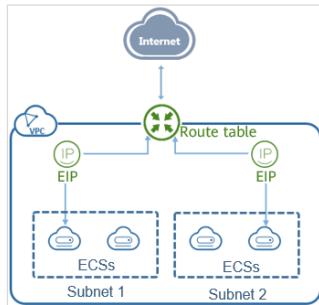
- A VIP is used for active/standby cloud server switchover to achieve high availability (HA).
- A VIP can be bound to multiple cloud servers deployed in active/standby mode. You can bind the VIP with an EIP so that you can access the cloud servers that have the same VIP bound from an extranet to improve DR performance.

EIP Functions



EIP Use Cases: A Single Cloud Server Accesses an Extranet

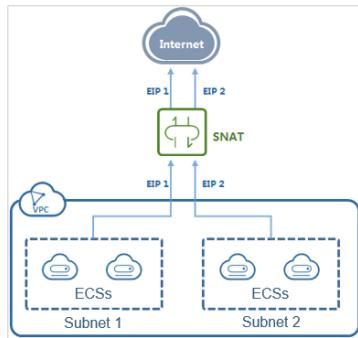
Using an EIP to let a cloud server in a VPC access an extranet



To let a single cloud server in a VPC access the extranet, bind an EIP.

EIP Use Cases: Multiple Cloud Servers Access an Extranet

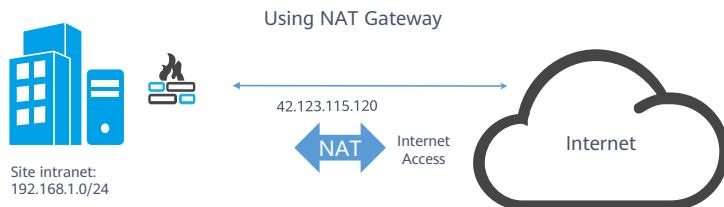
Using EIP and NAT Gateway to enable cloud servers in a VPC to access an extranet



To let multiple cloud servers in a VPC access the extranet, use an EIP and a NAT gateway. Create a NAT gateway. Create a SNAT rule. Add the target EIP and the target subnet to the SNAT rule to let the cloud servers in the subnet access the extranet over the EIP.

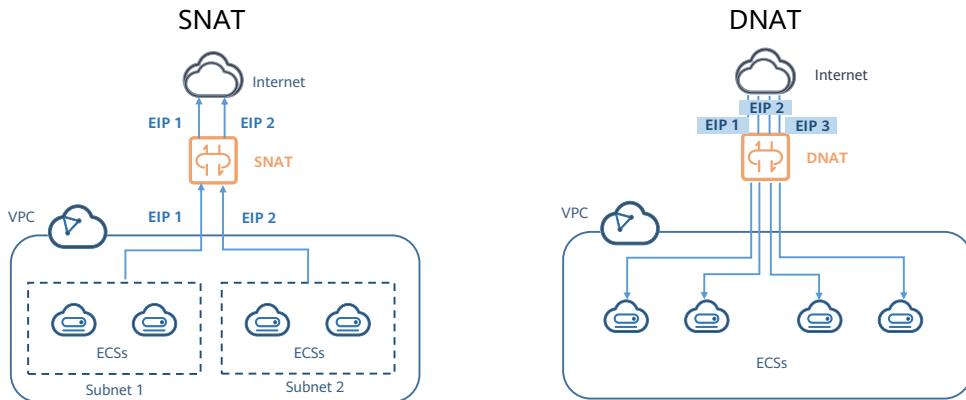
NAT Gateway

- NAT Gateway provides network address translation (NAT) for cloud servers (ECSs and BMSs) in a VPC so that multiple cloud servers can share EIPs to access the Internet or provide Internet services. NAT Gateway supports source NAT (SNAT) and destination NAT (DNAT).



- NAT Gateway: A NAT gateway provides NAT for cloud servers within a VPC so that multiple cloud servers can share an EIP to access an extranet or provide services for an extranet. Multiple types of NAT gateways are provided, each of which has specific specifications. You can change your NAT gateway type as required. If an enterprise has multiple cloud servers, the cost of EIPs is high. To save IP addresses, you can use the SNAT function of the NAT gateway. The SNAT function is used to translate the private IP address into an extranet IP address by binding an EIP. This enables multiple cloud servers in a VPC to share an EIP to access the extranet.

NAT Gateway Functions



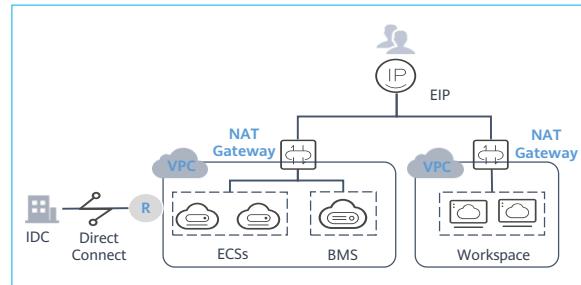
- If cloud servers in a VPC need to provide services for an extranet, you can use the DNAT function of the NAT gateway. The DNAT function is used to map the private IP address, protocol, and port of a cloud server in a VPC to a public IP address, protocol, and port by binding an EIP to the cloud server so that services deployed on the cloud server can be accessed by an extranet.
- The SNAT function maps the IP addresses of a subnet in a VPC to an EIP, thereby allowing the cloud servers in the subnet to access an extranet. After the SNAT function is enabled for a subnet, all cloud servers in the subnet can access an extranet using the same EIP. DNAT, in contrast to SNAT, maps an EIP to the IP addresses of a subnet in a VPC.

NAT Gateway Use Cases

- NAT Gateway is widely used by enterprises because it is more secure and easier to manage, reduces O&M workload, and saves IP addresses.

For Internet, e-commerce, and financial enterprises, security must be considered while designing the architecture. NAT Gateway is used as a security isolation mechanism to prevent VMs from being bound to EIPs directly.

For gaming and video enterprises with services that need Internet access, DNAT is used to fully utilize EIP ports.

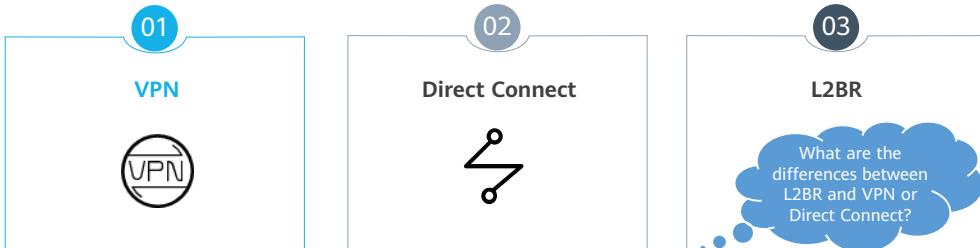


Contents

1. HUAWEI CLOUD Stack Network Services
2. General Network Services
- 3. Interworking Service**
 - Intra-Cloud Communications
 - Communications Between the Cloud and the Internet
 - Communications Between the Cloud and On-Premises Data Centers**
4. Value-Added Services
5. Network Design

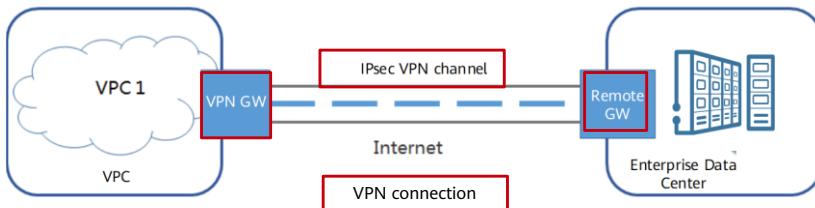
Communications Between the Cloud and On-Premises Data Centers

- VPN, Direct Connect, and L2BR can enable communications between the cloud and on-premises data centers.



Virtual Private Network

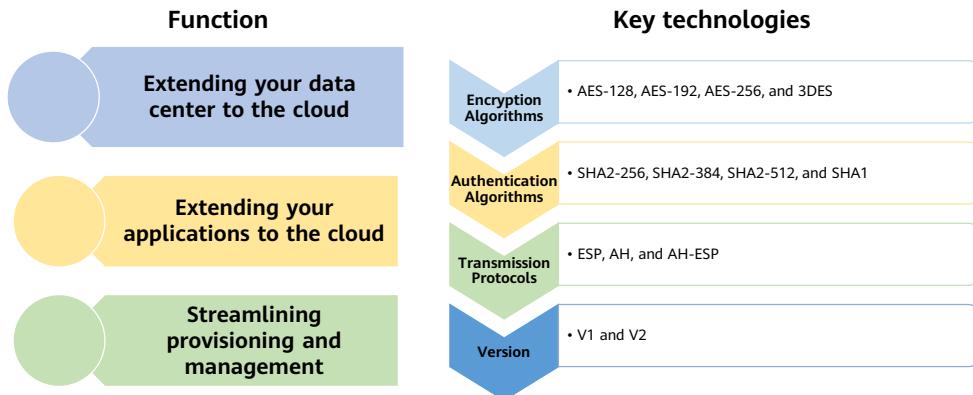
- Virtual Private Network (VPN) provides end-to-end private communications channels. The IPsec VPN service establishes an encrypted communications tunnel between remote users and a VPC on the public network so that the remote users can access service resources in the VPC through a secure IPsec VPN over a routing network.



- A VPN is a secure and encrypted communications tunnel established between your data center and a HUAWEI CLOUD Stack VPC. The tunnel complies with industry standards.
- By default, ECSs or BMSs in a VPC cannot communicate with your data center or private network. To enable communications between them, use a VPN. With VPN, you can connect to a VPC and access the resources deployed there from your data center.
- A VPN gateway is an egress gateway for a VPC. With a VPN gateway, you can create a secure, reliable, and encrypted connection between a VPC and an on-premises data center or between two VPCs in different regions.
- A remote gateway is used to communicate with ECSs or BMSs in specific VPCs. The gateway records VPN public IP addresses of your data center or VPCs in other regions.
- A VPN connection is an Internet-based IPsec encryption technology. With the tunnel encryption technology, VPN connections use encrypted security services to establish confidential and secure communications tunnels between different networks.
- A VPN connection connects VPN gateways and remote gateways of your data center and establishes a secure and reliable communications tunnel between a VPN gateway and the remote gateway in an on-premises data center.

VPN Functions and Key Technologies

- The VPN service allows the ECSs in a VPC to communicate with your on-premises data center or private network. With VPN, you can connect to the VPC and access the resources deployed there from your data center.

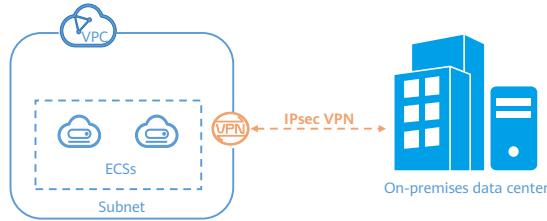


- Professional network hardware devices are used to establish an encrypted communications tunnel for network connectivity.

VPN Use Case: Connecting a VPC to an On-Premises Data Center

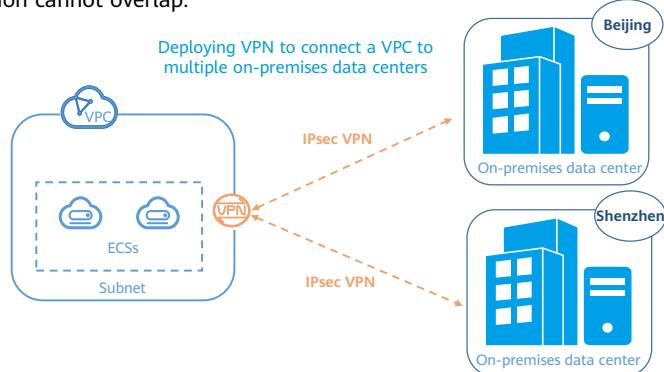
- With a VPN connecting you to a VPC, you can easily access cloud servers and block storage resources in the cloud from your on-premises data center. You can migrate applications to the cloud, start additional web servers, and expand the computing capacity on a network. By creating a hybrid cloud, you can reduce your IT O&M costs and protect enterprise core data from being exposed to the Internet.

Deploying VPN to connect a VPC to one on-premises data center



VPN Use Case: Connecting a VPC to Multiple On-Premises Data Centers

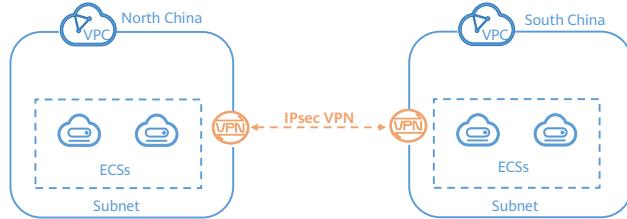
- You can use a VPN to connect a VPC to multiple traditional data centers, making it easy for you to use cloud servers and block storage resources on the cloud. The subnet CIDR blocks of each site involved in the VPN connection cannot overlap.



VPN Use Case: Connecting VPCs Across Regions

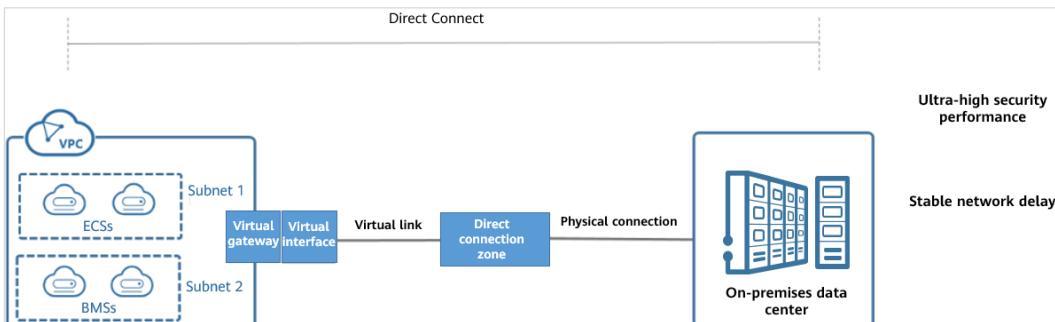
- In this case, a VPN tunnel is established between two VPCs in different regions to enable mutual access between the two VPCs.

Deploying VPN to connect VPCs across regions



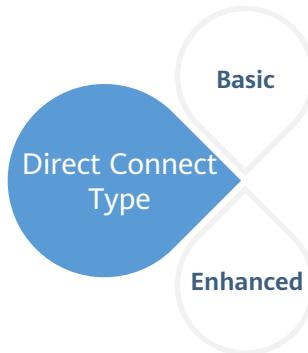
Direct Connect

- Direct Connect enables you to set up a dedicated connection between your on-premises data center and a VPC. The connection features high security, high speed, low latency, stability, and reliability.



- You can set up multiple connections between compute resources of VPCs in different regions to connect your on-premises network, data center, and colocation center to VPCs. This enables you to use legacy facilities and enjoy cloud computing advantages.
- A connection is a leased physical connection of a carrier used to connect your on-premises data center to a Direct Connect access point. This type of connection enables you to create multiple virtual interfaces to connect to your VPCs.
- A virtual gateway is a logical gateway for accessing a VPC through a Direct Connect connection. A virtual gateway can be associated with the VPC. Multiple VPCs can share one virtual gateway. If you have multiple connections, you can use one virtual gateway to access the same VPC.
- A virtual interface links a connection with one or more virtual gateways, each of which is associated with a VPC, so that your on-premises network can access all these VPCs.

Direct Connect Classification



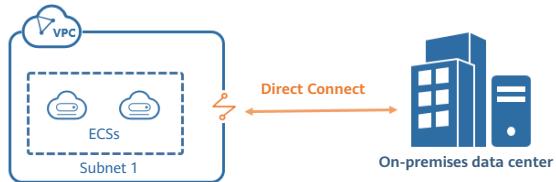
Basic Direct Connect

Basic Direct Connect does not depend on hardware devices, so it is easy to deploy and scale out.

Enhanced Direct Connect

A hardware switch, like a Direct Connect gateway, provides better forwarding performance. Both static and dynamic routes are supported, simplifying deployment.

Direct Connect Use Case: Connecting Cloud Servers to an On-Premises Data Center Through a Dedicated High-Speed Line

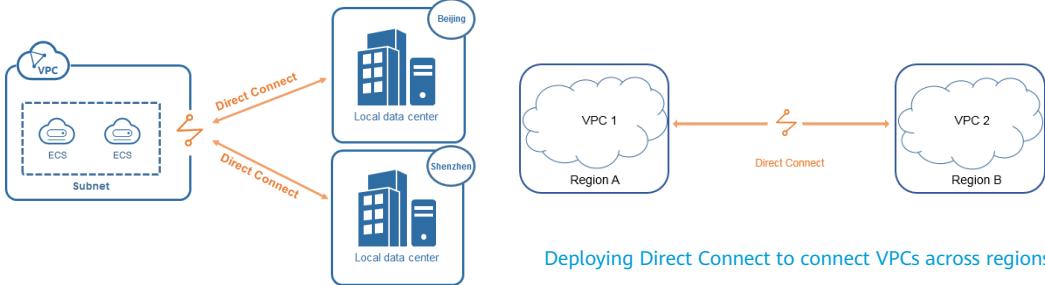


Connecting cloud servers to an on-premises data center through a dedicated high-speed line

With Direct Connect, you can connect your network, data center, and collocation environment to VPCs to enjoy a high-performance, low-latency, and secure network.

- You can connect your local facilities to a VPC in Huawei private cloud resources through a dedicated connection, such as an MSTP line or leased transmission line, bare optical fiber, and MPLS VPN.

Direct Connect Use Cases: Connecting a VPC to Multiple On-Premises Data Centers and Connecting VPCs Across Regions



Deploying Direct Connect to connect a VPC to multiple on-premises data centers

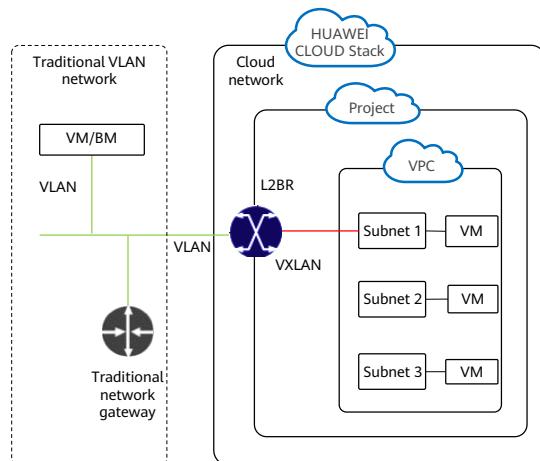
You can use Direct Connect to connect to the compute resources of VPCs in multiple regions to enjoy a high-performance, low latency network that is secure.

Deploying Direct Connect to connect VPCs across regions

You can use Direct Connect to connect VPCs in different regions so that they can communicate with each other.

Layer 2 Bridge

- Layer 2 Bridge (L2BR) is a dedicated high speed Layer 2 network connection that is fast, stable, and secure. During data center deployment, if there are some special functions that cannot be migrated from a physical server to a VM, you can use L2BR for Layer 2 communications between a VPC in the data center and a traditional VLAN network. In addition, multicast is supported to meet the requirements of urban rail cloud and media cloud.



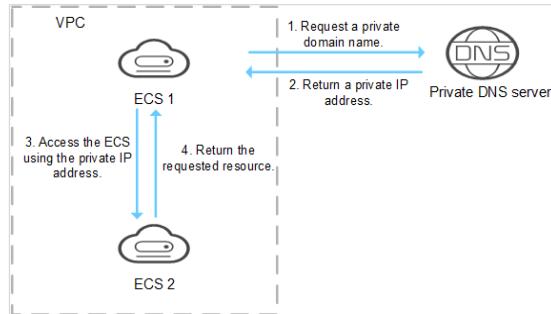
- Using L2BR, an extranet can communicate with private IP addresses of VPCs in the cloud at Layer 2 and Layer 3.
- VPC subnets that communicate with each other at Layer 2 must be in the same CIDR block as the extranet. Other subnets in the VPC can communicate with the extranet at Layer 3.
- IP addresses for both the internal and external networks need to be allocated or created to ensure that no IP address conflict occurs.
- Only one L2BR instance can be created in a VPC.

Contents

1. HUAWEI CLOUD Stack Network Services
2. General Network Services
3. Interworking Services
- 4. Value-Added Services**
5. Network Design

Cloud Domain Name Service

- Cloud Domain Name Service (CloudDNS) provides highly available and scalable authoritative DNS services that translate domain names into IP addresses required for network connection, reliably directing end users to your applications.



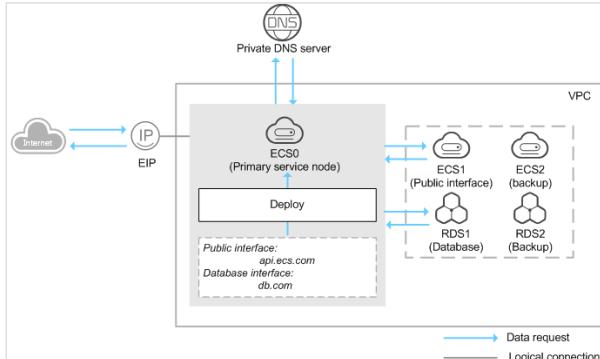
- CloudDNS associates private domain names that take effect only within VPCs with private IP addresses to facilitate access to cloud resources within the VPCs. You can also directly access cloud services through private DNS servers.
- Each domain name is unique on a network. It represents the logical address of a network access location.
- Computers can access the Internet only using domain names or IP addresses. Domain names are the key to Internet access.
- Domain name resolution maps domain names to IP addresses. It is an indispensable method for domain names to access desired websites.

CloudDNS Functions

- To facilitate access to cloud resources within the VPCs, CloudDNS associates private domain names that are only used within VPCs with private IP addresses.

- Associating a VPC with a private zone
- Disassociating a VPC from a private zone
- Viewing, modifying, and deleting a private DNS server and managing record sets

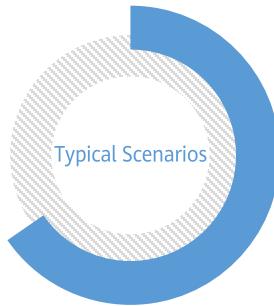
Please describe the domain name resolution process.



- Domain name resolution process (for details, see the trainee manual):
 - The client queries the local DNS server for www.abc.com (www.abc.com is used as an example).
 - If no domain name is found in the cache of the local DNS server, the local DNS server sends a query request to the root DNS server.
 - The root DNS server returns the IP address of the top-level DNS server that manages the .com to the local DNS server.
 - The local DNS server sends a query request to the top-level DNS server.
 - The top-level DNS server returns the address of the secondary DNS server that manages the .abc.com. (If .abc.com is a domain name registered or hosted on the platform, the returned address is the DNS server address of the platform ns1.hw.com or ns2.hw.com.)
 - The local DNS server sends a query request to ns1.hw.com or ns2.hw.com.
 - ns1.hw.com or ns2.hw.com finds the value x.x.x.x corresponding to www.abc.com and returns the value to the local DNS server.
 - The local DNS server returns the query result x.x.x.x to the client.

CloudDNS Use Cases

- CloudDNS provides private domain name resolution within a VPC. It can be used to manage the host names of cloud servers, switch cloud servers, and enable cloud servers to access cloud resources.



Managing the host names of cloud servers: internal development, testing, and production scenarios of enterprises

Switching cloud servers: website application deployment

Enabling cloud servers to access cloud resources: cloud server access to internal cloud services, such as SMN and OBS

Contents

1. HUAWEI CLOUD Stack Network Services
2. General Network Services
3. Interworking Services
4. Value-Added Services
- 5. Network Design**

Discussion of Network Design

Context: A provincial public security bureau needs to re-plan networks to migrate some workloads to the cloud. By default, networks of different departments cannot communicate with each other. The public security bureau wants to use certain cloud services to enable point-to-point communications between different departments after approval. The provincial public security bureau wants its cloud to interwork with other provincial clouds, and the provincial cloud provides a GUI for its citizens on the Internet.

- Which of the following network services do you recommend? Why?
- Key points:
 - Workloads need to be migrated.
 - Guests log in to the GUI and there is service traffic generated.
 - By default, networks of different departments cannot communicate with each other.
 - Networks of different departments can communicate with each other through certain cloud services.
 - Clouds need to communicate across provinces.

Quiz

1. (Single-answer question) Which of the following cloud services uses the VGW as the bearer NE?
 - A. VPC
 - B. EIP
 - C. ELB
 - D. VPN
2. (Multiple-answer question) Which of the following cloud services are optional for project deployment?
 - A. VPC
 - B. ELB
 - C. VPN
 - D. VPC Endpoint

- Answers:

- D
 - BCD

Summary

- In this course, we have learnt:
 - What HUAWEI CLOUD Stack network services are.
 - The functions, architectures, and use cases of VPC, SG, Network ACL, EIP, and ELB.
 - The network interworking solutions for different scenarios.

Recommendations

- Huawei Talent:
 - <https://e.huawei.com/en/talent/portal/#/>
- Huawei Certification:
 - <https://forum.huawei.com/enterprise/en/forum-813.html>

Acronyms

Acronym	Full Name	Description
BMS	Bare Metal Server	A BMS is a physical server dedicated for tenants.
CC	Cloud Connect	CC allows you to quickly build stable, high-speed, and high-quality networks between VPCs across regions.
DC	Direct Connect	Direct Connect enables you to set up a dedicated connection between your on-premises data center and a VPC. The connection features high security, high speed, low latency, stability, and reliability.
ECS	Elastic Cloud Server	An ECS is a cloud server that consists of vCPUs, memory, images, and EVS disks and allows on-demand allocation and elastic scaling.
EIP	Elastic IP	An EIP is a static IP address that can be directly accessed from an extranet. The extranet can be the Internet or an enterprise LAN.
ELB	Elastic Load Balance	ELB distributes incoming traffic across multiple backend servers based on specified forwarding policies.

Acronyms

Acronym	Full Name	Description
EVS	Elastic Volume Service	EVS is a virtual block storage service that provides storage for ECSS and BMSS.
OBS	Object Storage Service	OBS provides massive, secure, highly reliable, and low-cost data storage.
SG	Security Group	A security group is a collection of access control rules for cloud servers that have the same security requirements and are mutually trusted within a project.
VPC	Virtual Private Cloud	A VPC provides an isolated virtual network for cloud servers.
VPN	Virtual Private Network	VPN establishes encrypted communications tunnels between on-premises data centers and VPCs.

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and
organization for a fully connected,
intelligent world.

Copyright©2022 Huawei Technologies Co., Ltd.
All Rights Reserved.

The information in this document may contain predictive
statements including, without limitation, statements regarding
the future financial and operating results, future product
portfolio, new technology, etc. There are a number of factors that
could cause actual results and developments to differ materially
from those expressed or implied in the predictive statements.
Therefore, such information is provided for reference purpose
only and constitutes neither an offer nor an acceptance. Huawei
may change the information at any time without notice.



HUAWEI CLOUD Stack ManageOne ServiceCenter Introduction



Foreword

- This course teaches you about HUAWEI CLOUD Stack Operation Portal, including how to create a tenant model, bring services online, manage metering and pricing statistics, and perform tenant self-service maintenance and multi-cloud management on this portal. When covering how services on the cloud platform are provisioned, we will explain how users with different roles perform management operations.

Objectives

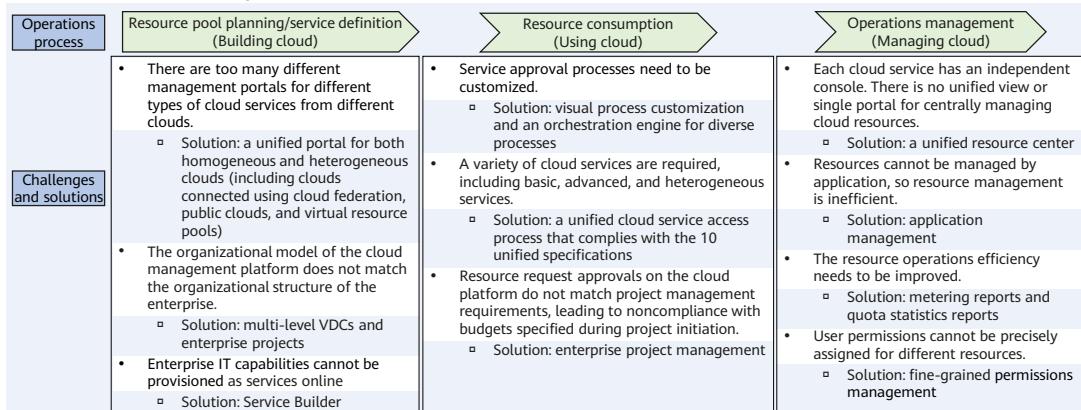
- Upon completion of this course, you will understand:
 - Basic functions of HUAWEI CLOUD Stack Operation Portal
 - How to provision services on HUAWEI CLOUD Stack
 - Basic concepts and tenant model creation process of HUAWEI CLOUD Stack
 - How to bring services online on HUAWEI CLOUD Stack
 - How to configure metering and pricing
 - How to perform tenant self-service maintenance
 - How to perform multi-cloud management

Contents

- 1. Operations Overview**
- 2. Resources and Organizations
- 3. Service Supply
- 4. Metering & Pricing
- 5. Tenant Maintenance
- 6. Multi-cloud Management

HUAWEI CLOUD Stack Operations Overview

- ManageOne ServiceCenter (Operation Portal) of HUAWEI CLOUD Stack provides a unified portal for tenants and operations management. It integrates a wide range of cloud service operations capabilities and supports connections to a variety of cloud services.

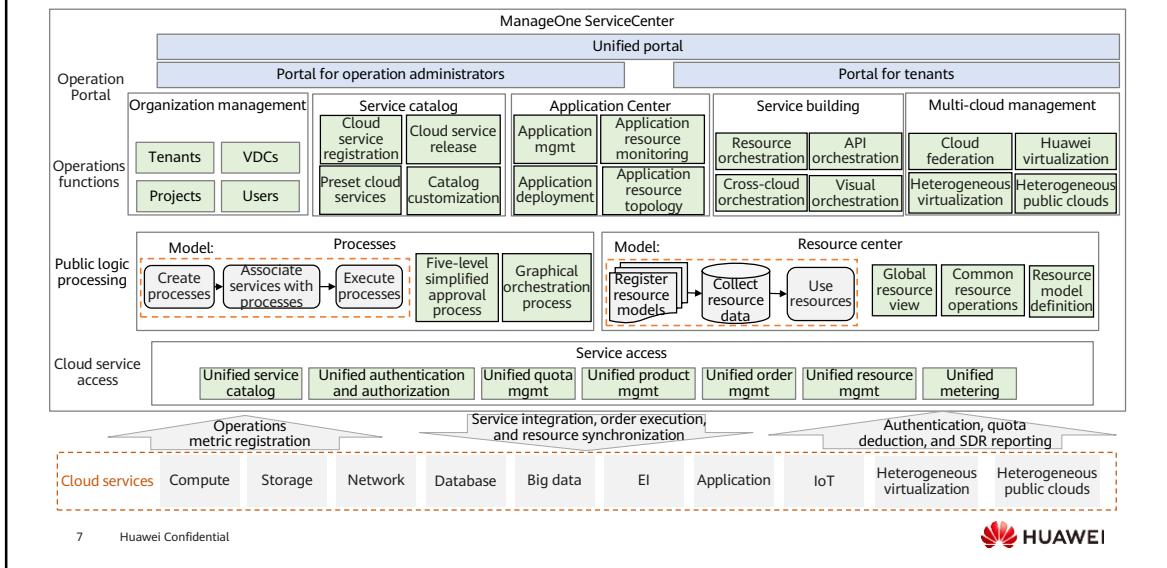


- ManageOne ServiceCenter (Operation Portal) provides a unified portal for tenants and operations management. It integrates a wide range of cloud service operations capabilities and supports connections to a variety of cloud services. Console Home integrates a range of cloud service consoles into a single unified portal. ServiceCenter allows you to orchestrate cloud service capabilities into cloud services available for users to request and add them to the service catalog.
- Another module of ManageOne, ManageOne Maintenance Portal, is used by HUAWEI CLOUD Stack for centralized maintenance on virtual and physical resources. ManageOne Maintenance Portal will be introduced in another course.
- In this course, we will focus on ManageOne Operation Portal. So, first, let's have a look at what cloud operations challenges have been haunting enterprises in building, using, and managing the cloud and how HUAWEI CLOUD Stack can help:
- When enterprises build clouds, there are three challenges on resource pool planning and service definition:
 - First, there are too many different management portals for different types of cloud services. To deal with this challenge, ServiceCenter provides multi-cloud management. It allows multiple clouds to be connected to one cloud using unified standards and support cloud connection using cloud federation.
 - Second, the organizational model of the cloud management platform does not match the organizational structure of the enterprise. ServiceCenter's multi-level VDC management capabilities can match organizational structures of enterprises.

- The third challenge is inability to provision enterprise IT capabilities as services online. ServiceCenter's Service Builder can tackle this challenge. It allows tenants to easily combine and orchestrate enterprise IT capabilities and cloud services of HUAWEI CLOUD Stack into new online services for diverse needs.
- When enterprises use clouds, there are three challenges on resource consumption:
 - First, enterprises require the cloud management platform to provide a customizable process engine to create different types of approval processes. ManageOne provides a visual process engine supporting online orchestration.
 - Second, a variety of cloud services are required, including basic services, container, big data, and third-party services. ManageOne supports connections to many kinds of cloud services based on "10 unified connection specifications."
 - The cloud services can come from HUAWEI CLOUD Stack, FusionCompute, VMware, AWS, Azure, Alibaba Cloud (connection plug-ins provided by ISVs, not included in the baseline version of ManageOne), and Tencent Cloud (connection plug-ins provided by ISVs, not included in the baseline version of ManageOne). ISVs can connect services from other platforms to ManageOne based on the 10 unified specifications.
 - The third challenge is that resource request approvals on the cloud platform do not match project management requirements, leading to noncompliance with budgets specified during project initiation. Enterprises can use enterprise projects of ManageOne to tackle this challenge.

- When it comes to cloud management, enterprises face four challenges on operations management:
 - The first challenge is lack of a unified resource management view. To manage cloud services in different regions, users have to access respective consoles of the services, which is inefficient. ManageOne provides a unified resource center to resolve this problem.
 - Second, resources cannot be managed by application, resulting in inefficient resource management. ManageOne provides application management to improve resource management efficiency.
 - Third, refined reports are needed to improve resource operations efficiency. To fit this need, ManageOne provides metering reports with customizable fields and quota statistics analysis.
 - The fourth challenge is lack of an effective mechanism that can precisely assign permissions for specific operations on different resources to users. ManageOne provides a fine-grained permissions management mechanism.

Functional Architecture of ServiceCenter



- ManageOne provides unified operations management, including unified access to cloud services, unified cloud service management, and unified organization management.
- Cloud service access: ManageOne provides unified cloud service access and allows operation administrators to centrally manage orders, services, and quotas of cloud services in all tenants.
- Public logic processing: Operation administrators can create processes or services that are globally visible.
- Operations functions: ManageOne provides tenants with a wide range of operations functions to match organizations of customers and deliver bespoke services.
- Operations portal: ManageOne provides a unified portal for operation administrators, VDC administrators, and other tenant users to access respective pages.

Contents

1. Operations Overview

2. Resources and Organizations

- Concepts

- User Roles

- Quotas and Approvals

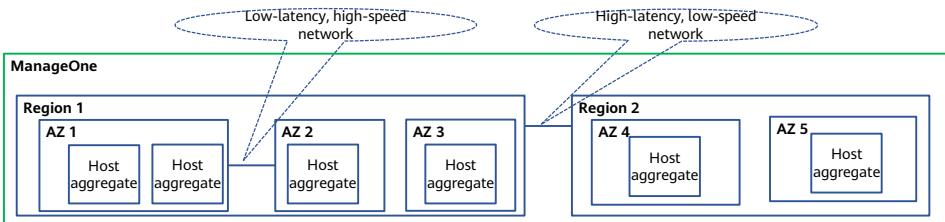
3. Service Supply

4. Metering & Pricing

5. Tenant Maintenance

6. Multi-cloud Management

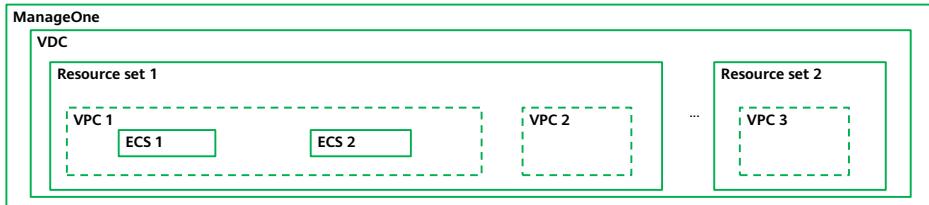
Physical Concepts



- Region: This is a geographical designation used by HUAWEI CLOUD. Generally, one region corresponds to one data center.
- Availability Zone (AZ): An AZ is an independent set of physical resources, including compute, storage, and network resources.
- Host aggregate: a group of physical hosts and related metadata.
- ManageOne: a unified cloud resource management platform

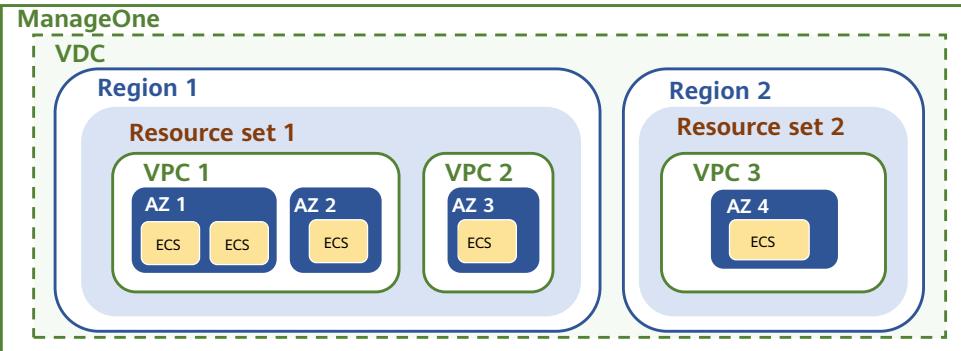
- The network latency within one region is low. There is no strict latency requirement for a network between different regions.
- Relationships between the physical concepts:
 - One region can contain multiple AZs.
 - One AZ cannot span multiple regions.
 - Each AZ contains one or multiple host aggregates.

Common Logical Concepts



- ManageOne is a unified cloud resource management platform that centrally manages on-premises cloud resources and public cloud resources.
- A Virtual Data Center (VDC) is a unit for resource allocation on ManageOne. A VDC matches a department of an enterprise or subsidiary. You can create up to five levels of VDCs.
- A resource set is the minimum unit of resource management on ManageOne. It can be used for resource isolation and user authorization.
- A Virtual Private Cloud (VPC) enables you to provision logically isolated, configurable, and manageable virtual networks for cloud servers, improving resource security and simplifying network deployment.
- An Elastic Cloud Server (ECS) is a computing server that consists of vCPUs, memory, images, and Elastic Volume Service (EVS) disks and allows on-demand allocation and elastic scaling. One ECS cannot use resources from different AZs.

Concept Relationships



- One VDC can contain resources from multiple regions. One region can provide resources for multiple VDCs.
- Multiple resource sets can be created in one region, and one resource set can contain resources from multiple AZs instead of multiple regions.
- A VPC can use resources in different AZs.

Other Concepts

Concept	Description
Global	ManageOne can be deployed in the Global zone to centrally manage multiple regions.
Project	A native OpenStack concept, used to group and isolate compute, storage, and network resources.
Enterprise project	Enterprise projects allow administrators to manage project budgets and control resource usage on a departmental basis. If you have such IT project needs, create enterprise projects.
Tenant	A tenant matches an enterprise or subsidiary. Data, operations, and networks of different tenants are isolated.

- In ManageOne 8.0.3 or later version, there are no projects, and all their functions are inherited by resource sets.

Contents

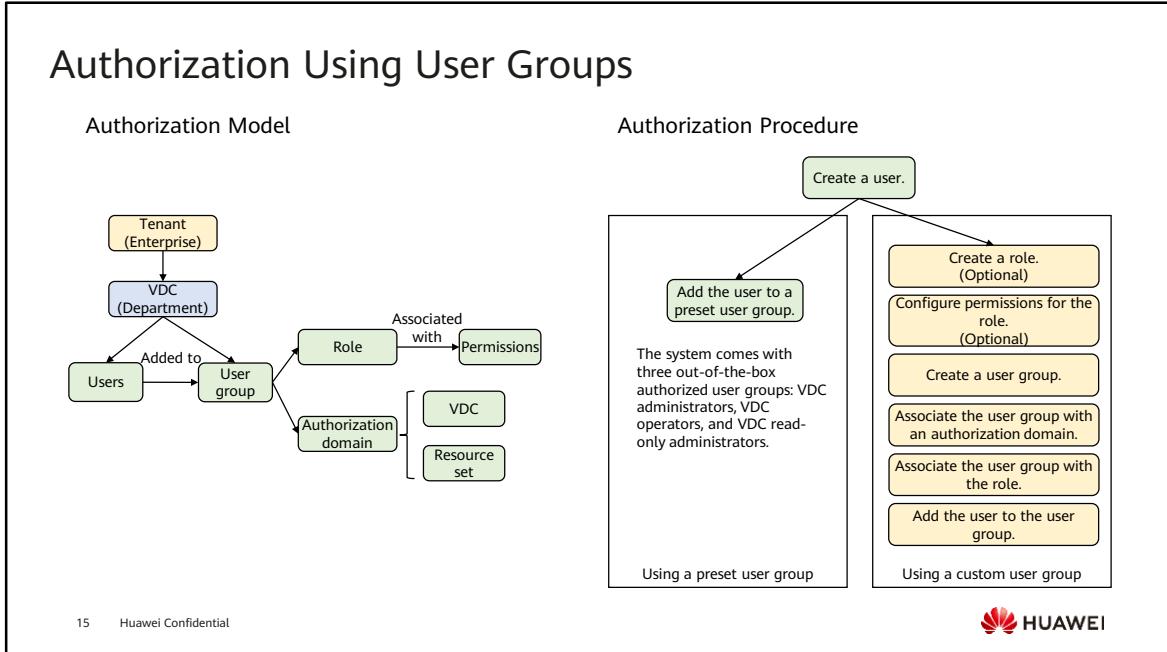
1. Operations Overview
2. **Resources and Organizations**
 - Concepts
 - User Roles
 - Quotas and Approvals
3. Service Supply
4. Metering & Pricing
5. Tenant Maintenance
6. Multi-cloud Management

User Roles

	Operation administrator	Has the highest-level operations management permissions. These administrators can manage rather than apply for all resources. bss_admin is the preset operation administrator.
	VDC administrator	Has management permissions for their own VDCs and lower-level VDCs, including all resources in those VDCs.
	VDC operator	Has management permissions for all resources in the resource sets associated with them.
	VDC read-only administrator	Has the permissions to view information about their own VDCs and lower-level VDCs, including resources, users, and self-service maintenance.
	Custom user groups	Has custom permissions
	Agent administrator	Has management permissions, same as those of first-level VDC administrators, for their own VDCs and lower-level VDCs, including all resource in those VDCs.

- Permissions of default user groups cannot be changed.
- Operation administrators and agent administrators have the following permissions without being associated with any user group:
 - Operation administrators have all operations management permissions, but they cannot request services.
 - Agent administrators have management permissions, same as those of first-level VDC administrators, for their own VDCs and lower-level VDCs, including all resources in those VDCs.
- Operation administrators can manage all user groups. VDC administrators or agent administrators can only manage user groups in the VDCs they belong to and their lower-level VDCs.

Authorization Using User Groups



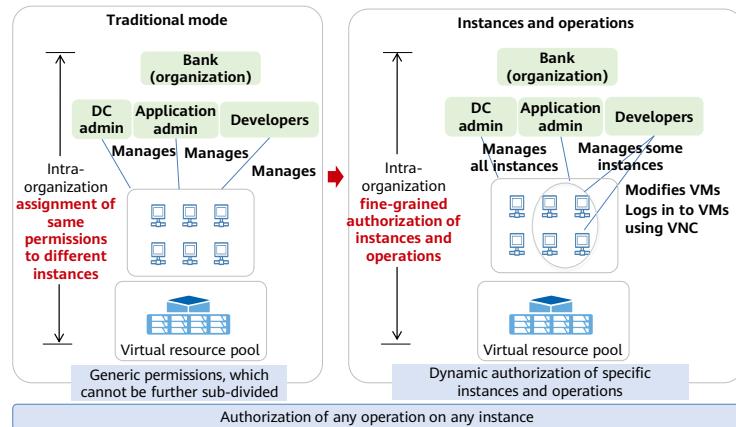
15 Huawei Confidential



- There are two authorization domains for user groups: VDCs and resource sets.
 - VDC authorization:
 - Permissions of default user groups (for example, the VDC administrator group) for VDCs have been defined and cannot be changed.
 - When a custom user group is created in a VDC, permissions for the VDC can be configured for the user group.
 - Resource set authorization: A user group can be associated with resource sets of other VDCs and configure permissions for the resource sets.
- The procedure for using user groups to manage and assign permissions is as follows:
 1. Create a resource set and associate it with a default user group.
 - If the default user groups can meet your requirements, go to step 4.
 - If the default user groups cannot meet your requirements, go to step 2.
 2. Create a custom user group or the default **VDC Admin** or **VDC Readonly Admin** user group. To create a custom user group, configure permissions for it.
 3. Add resource sets to the user group.
 4. Add users to the user group so that the users are assigned the operation permissions for resources in the resource set associated with the user group. If the users need to apply for resources, add the resource set to an enterprise project that has not been stopped.

Fine-grained User Authorization

- ManageOne enables fine-grained permissions control. It lets you control what resource management permissions are granted to which users in organizations at each level in an enterprise, achieving fine-grained user authorization.



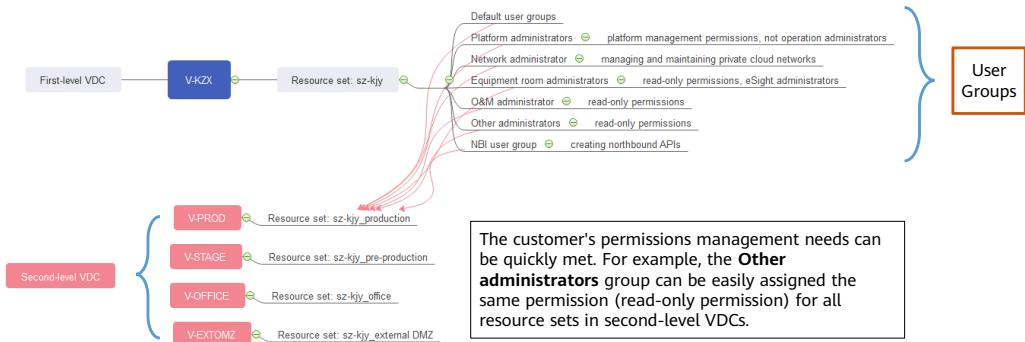
16 Huawei Confidential



- Customers can associate user groups with resource sets in other VDCs and configure permissions for the resource sets.
- When configuring resource set permissions, customers can select different cloud services and choose fine-grained permissions for specific cloud service operations, including creating, modifying, and deleting VMs, and logging in to VMs using VNC.

Organization Design Case

- A customer designed the following tenant model covering their production, pre-production, office, and external application domains. This tenant model fits their user permissions and organizational structure.



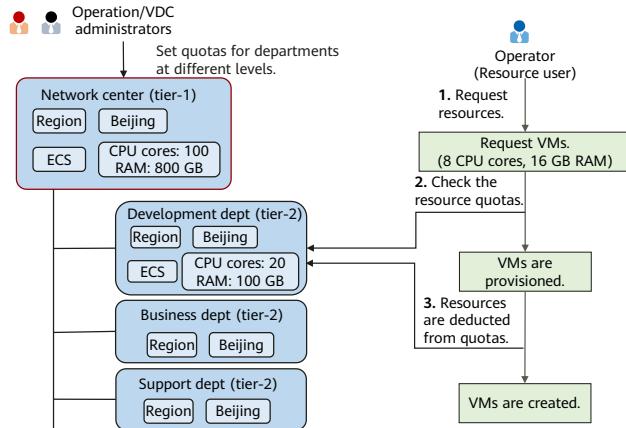
- Let's see this organization design case. The first-level VDC was used to manage all second-level VDCs. In the first-level VDC, in addition to preset user groups, six custom user groups were created. The figure shows respective permissions of the user groups on the VDC.
- The customer created four second-level VDCs for different domains: production, pre-production, office, and external use.
- Each VDC (at the first or second level) corresponds to a resource set.
- The customer requires that a user group in the first-level VDC be used to manage all second-level VDCs and be assigned the same permissions on the resource set of each second-level VDC. For example, the **Other administrators** group can be assigned the same permission (read-only permission) for all resource sets in second-level VDCs.
- This figure shows the final organization design, omitting associations between user groups and resource sets in other second-level VDCs.

Contents

1. Operations Overview
2. **Resources and Organizations**
 - Concepts
 - User Roles
 - Quotas and Approvals
3. Service Supply
4. Metering & Pricing
5. Tenant Maintenance
6. Multi-cloud Management

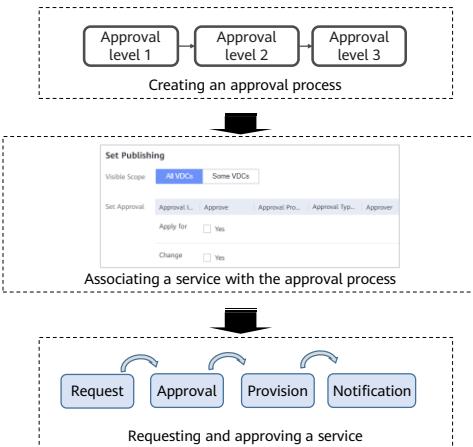
Quota Management for Enterprise Projects and VDCs

- IT departments can adjust quotas to control how many cloud resources can be used by each business department.



- Users can configure quotas for VDCs or enterprise projects to control budgets:
 - Operation administrators and VDC administrators can manage VDC quotas.
 - Enterprise project quotas control how many resources can be used by departments within their budgets.
- Quotas can be configured by VDC or enterprise project.
- Two quota types are supported: limited and unlimited.
- Approvals can be configured for quota changes.
- The CPU, memory, and storage metrics can be controlled based on the total number of resource pools.
- A quota usage overview is provided for audit.

Multi-level Approvals



1. A service can be associated with a published approval process when being brought online.
2. Specific operations on services, such as requesting, modifying, deleting, and renewing services, can be associated with different approval processes, or they can be configured to not require any approval.
3. After an upper-level VDC administrator publishes a service, a lower-level VDC administrator can bring the service online in the VDC the lower-level VDC administrator belongs to. They can also modify the approval process for the service.

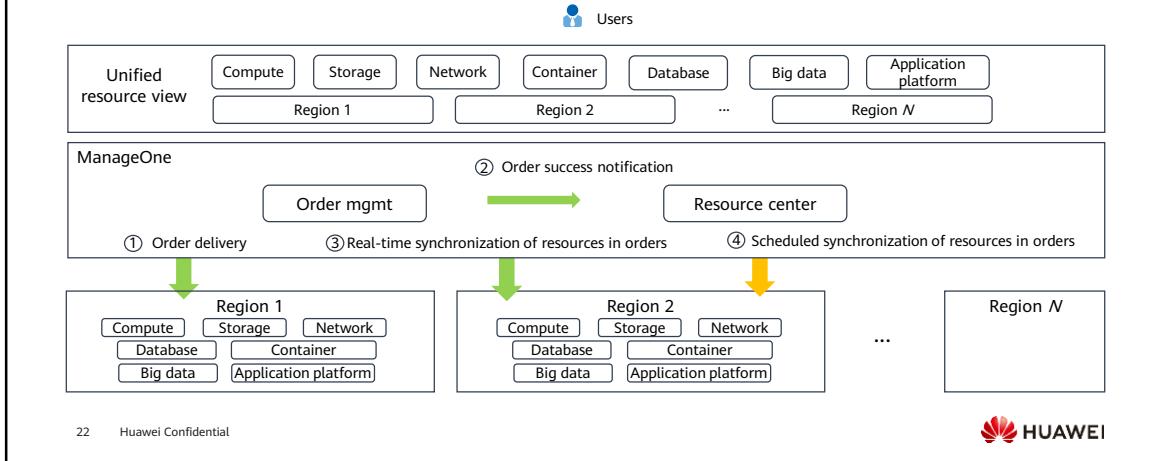
- ManageOne allows users to define independent approval processes. Operation administrators and VDC administrators can define approval processes. Approval processes published by operation administrators are globally visible, but those published by VDC administrators can be used only in the VDCs that the VDC administrators belong to and their lower-level VDCs.
- ServiceCenter supports up to five approval levels. Multiple users can be selected as approvers for each level. The approvers to be selected for an approval step must have the approval permission. Operation administrators and VDC administrators have the approval permission by default. VDC operators can participate in approvals by being assigned the approval permission or a new role.
- An approval process defined on ManageOne can be associated with a third-party service ticket system. After doing so, when an approval process is started, an approval request is sent to the third-party system.

Contents

1. Operations Overview
2. Resources and Organizations
- 3. Service Supply**
 - Service Management
 - Service Builder
 - Service Requests
4. Metering & Pricing
5. Tenant Maintenance
6. Multi-cloud Management

Unified Resource View

- Users can search for and manage resources by region, service type, resource set, or VDC. Read-only administrators can view global resources, VDC administrators can view resources in their own VDCs, and VDC operators can view resources they have requested.

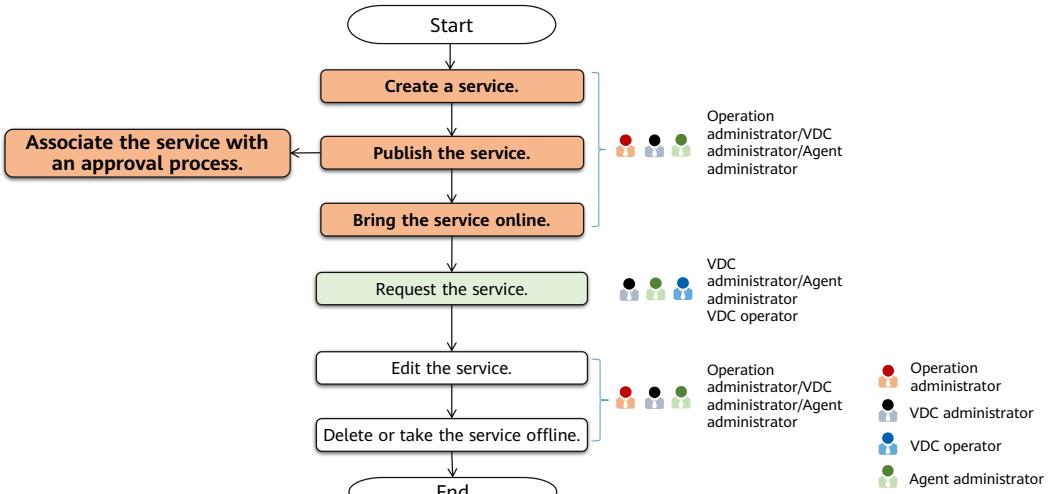


22 Huawei Confidential



- After cloud transformation of enterprises, many cloud resource pools in different regions and diverse services are deployed. Users need to open the console of each cloud service in each region or resource set to query services and perform related operations, which is inefficient. In addition, users cannot view resource statistics of global resources on a unified portal.
- ManageOne provides a unified resource view. Users can search for and manage resources by region, service type, resource set, and VDC. Read-only administrators can view all resources but cannot perform any operations on them. VDC administrators can view resources in their own VDCs. VDC operators can view resources requested by themselves.
- Region resource information can be updated to ManageOne in either of the following ways:
 - Real-time update: The resource center works with the order management module. After an order is created, the resource center is notified of data update in real time.
 - Scheduled update: The resource center verifies resources of each cloud service at a specified time every day to ensure data consistency between ManageOne and cloud services.

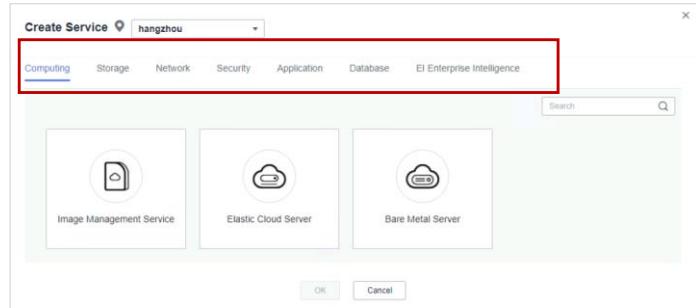
Process Overview of Bringing a Service Online



- Next, let's jump into how to create, publish, and bring online services, and associate services with approval processes.

Service Management: Creating a Service

- In addition to preset services, operation administrators can create services to suit different needs. VDC users can then request them.

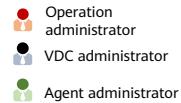
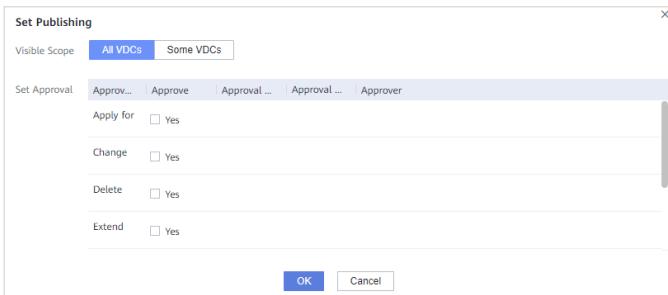


- Operation administrator
- VDC administrator
- Agent administrator



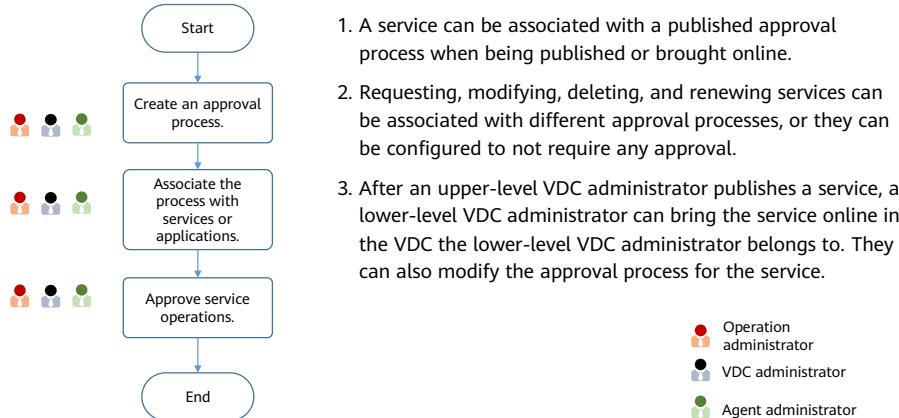
Service Management: Publishing a Service

- An unpublished service can be published, making it visible to specific VDC administrators.
- When a service is published, a visible scope and approval processes need to be configured for it.



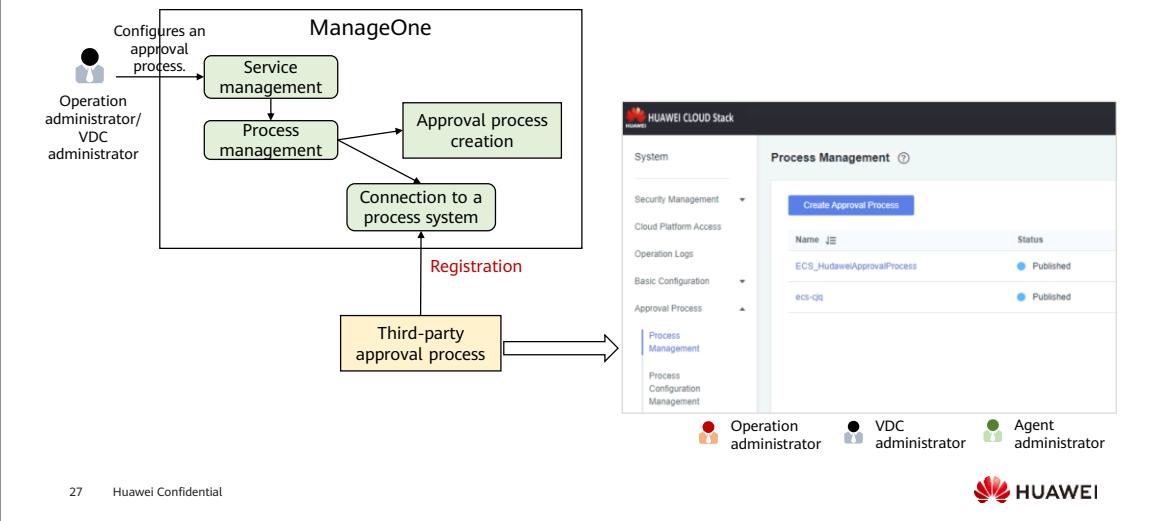
- An unpublished service can be published to become visible to specific VDC administrators. After an offline service is created by operation administrators, it is in the **Published** state and is globally visible.
- When an operation administrator selects the visible scope, the options are described as follows:
 - **All VDCs:** The service to be published is visible to all VDC administrators.
 - **Some VDCs:** The administrator can select tenants in which all VDC administrators can view the template.
- When a VDC administrator or an agent administrator selects the visible scope, the options are described as follows:
 - **All VDCs:** The service is visible to the VDC administrators of the VDCs the current VDC administrator or agent administrator belongs to and all its lower-level VDCs.
 - **Some VDCs:** The administrator can select VDCs in which all VDC administrators can view the service.

Approval Process Management



- ManageOne allows users to define independent approval processes. Operation administrators and VDC administrators can define approval processes. Approval processes published by operation administrators are globally visible, but those published by VDC administrators can be used only in the VDCs that the VDC administrators belong to and their lower-level VDCs.
- A single approval process supports up to five approval levels. Multiple users can be selected as approvers for each level. The approvers to be selected for an approval step must have the approval permission. Operation administrators and VDC administrators have the approval permission by default. VDC operators can participate in approvals by being assigned the approval permission or a new role.
- An approval process defined on ManageOne can be associated with a third-party service ticket system. After doing so, when an approval process is started, an approval request is sent to the third-party system.

Connection to a Third-party Approval System



- If users need to use approval processes of an external system, some customization must be made to interconnect with the external system first.

Service Management: Bringing a Service Online

- After a service is published, operation administrators, VDC administrators, or agent administrators can bring the service online, so users can request the service.



Operation administrator

An operation administrator can bring online preset services or services registered by other operation administrators. When bringing a service online, they can select online scopes and configure approvals for service operations. After the service is brought online, all users in the selected tenants can request the service.



VDC administrator

A VDC administrator can bring online services published by operation administrators or those published by upper-level VDC administrators and visible to VDCs that this VDC administrator belongs to. When bringing a service online, they can configure approvals for service operations. After the service is brought online, all users in the VDCs that the VDC administrator belongs to can request the service.



Agent administrator

An agent administrator can bring online services published by operation administrators. When bringing a service online, they can configure approvals for service operations. After the service is brought online, all users in the VDCs that the agent administrator can manage can request the service.



Operation administrator



VDC administrator



Agent administrator

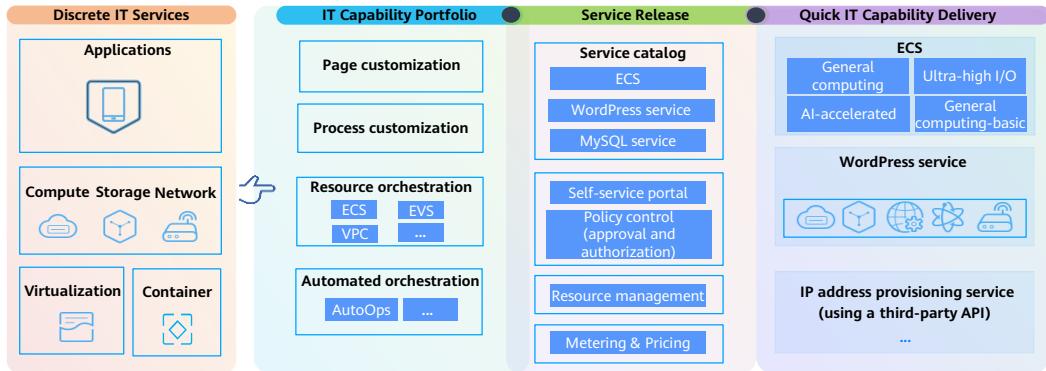
- When a service is brought online, an approval scope also needs to be configured. The approval settings are the same as those when a service is published.
- When bringing a service online, operation administrators not only can configure approvals but also set the visible scope, but VDC administrators or agent administrators can only configure approvals.

Contents

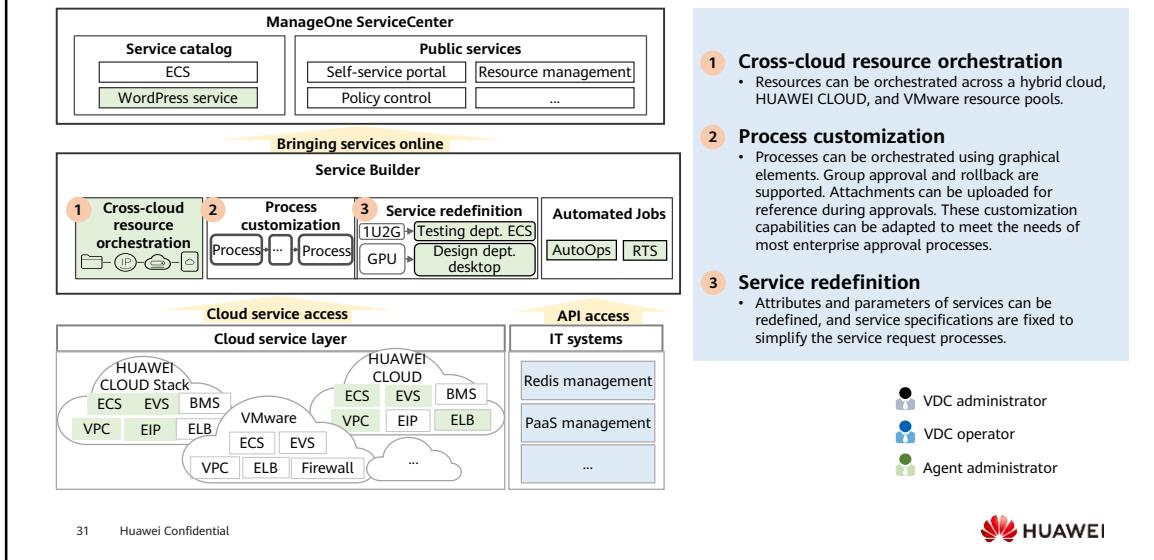
1. Operations Overview
2. Resources and Organizations
- 3. Service Supply**
 - Service Management
 - **Service Builder**
 - Service Requests
4. Metering & Pricing
5. Tenant Maintenance
6. Multi-cloud Management

Service Builder Overview

- Service Builder, backed by open service APIs, O&M automation capabilities, and a process engine adapted to enterprise needs, provides unified processes for provisioning IT capabilities as services. It helps cultivate a robust ecosystem. Users can quickly request, provision, configure, and deploy IT resources and capabilities online.



Service Builder Functions

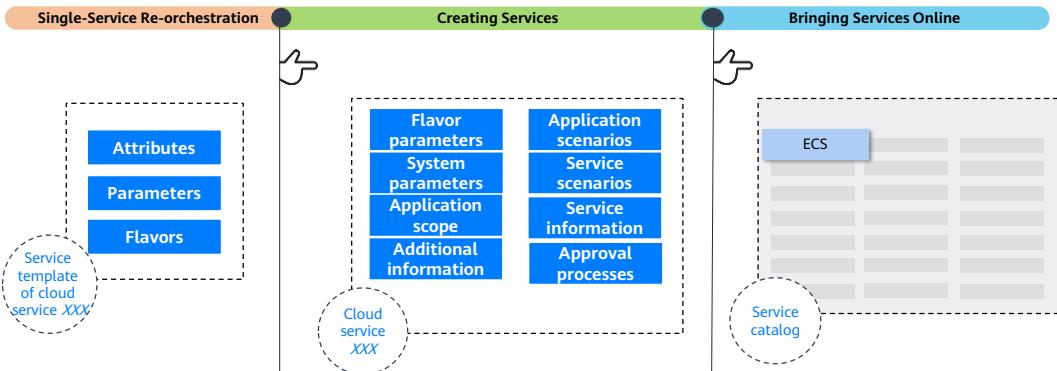


- Using the original orchestration mode of Service Builder, secondary development personnel need to develop resource orchestration plug-ins, which requires heavy development workload. In addition, some common operations (such as HTTPS links and database operations) need to be repeated.
- To resolve this problem, API orchestration was added for Service Builder since the ManageOne 8.1.0 version. API orchestration allows secondary development personnel to orchestrate atomic APIs on the visual orchestration UI without developing resource orchestration plug-ins. In addition, common operations can be performed using the orchestration engine. This greatly simplifies orchestration of cloud service resources.
- API orchestration of Service Builder combines enterprise legacy IT systems and orchestrates them into new cloud services. The new cloud services can be added to the service catalog and service marketplace. This boosts IT resource sharing and cultivates a robust IT service ecosystem.

Single-Service Re-orchestration

- Redefine how native cloud services are created and used and standardize service request processes to better suit IT governance needs of enterprises.

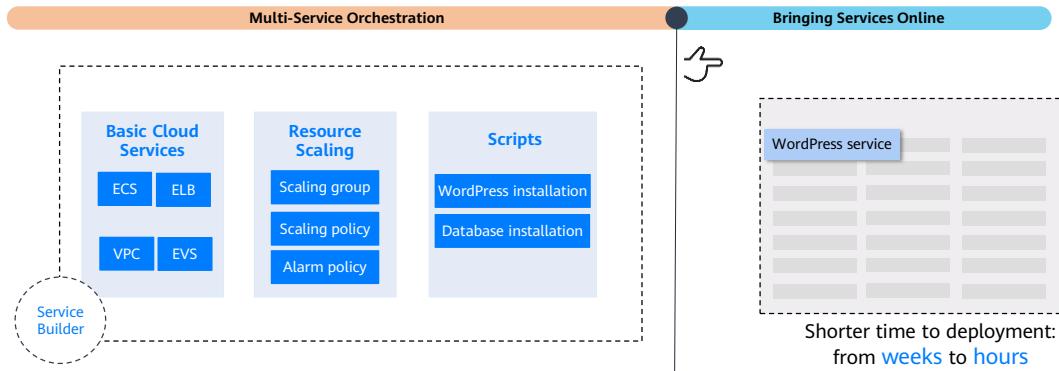
-Redefines cloud services using Service Builder.



Multi-Service Orchestration

- Service Builder allows you to orchestrate atomic capabilities of multiple cloud services into new scenario-specific services.

-----Combines cloud services using Service Builder-----

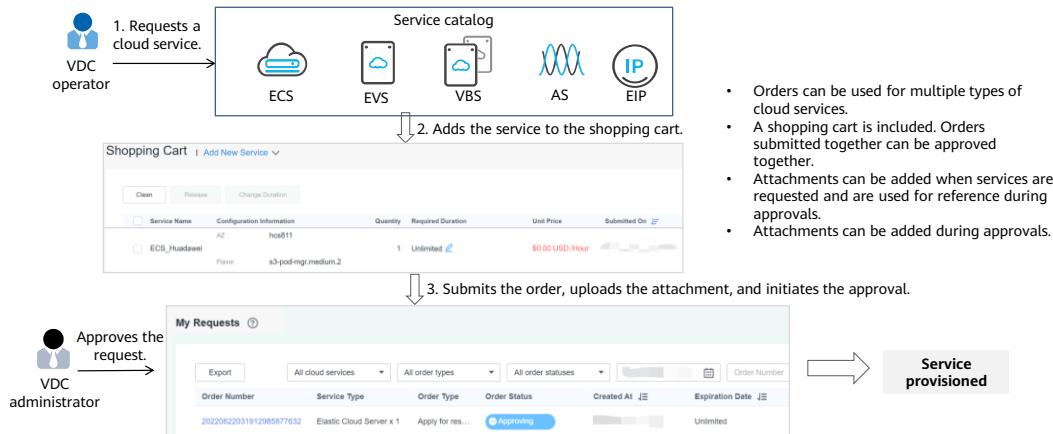


Contents

1. Operations Overview
2. Resources and Organizations
- 3. Service Supply**
 - Service Management
 - Service Builder
 - Service Requests**
4. Metering & Pricing
5. Tenant Maintenance
6. Multi-cloud Management

Requesting Services

- A user submits a service request. An administrator approves the request. Then, the system automatically creates resources required by the services and provisions them to the user.



35 Huawei Confidential



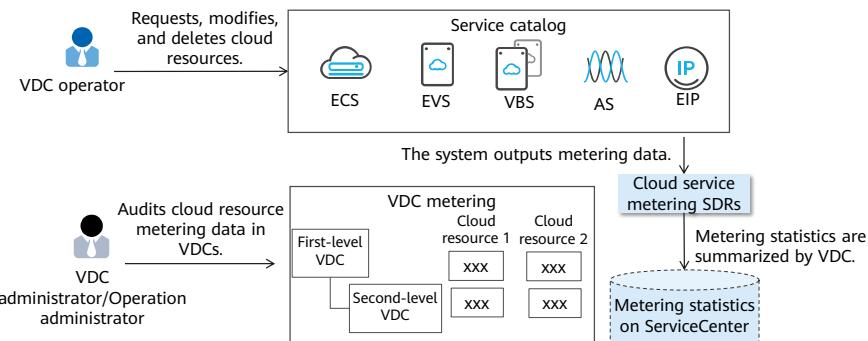
- In addition to service requesting, ManageOne also provides the recycle bin and shopping cart.
- Recycle bin:
 - VDC administrators, agent administrators, and VDC operators can view and delete resources in the recycle bin and restore resources from the recycle bin. Resources in the deleted state cannot be restored.
- Shopping cart:
 - You can add different types of services to the shopping cart and request the services at a time.
 - If you set parameters for requesting a service, but do not submit the request at that time, you can add the service to the shopping cart and submit the request later without selecting the service from the service list and setting the parameters again.
 - You can change durations of services, delete service, and submit service requests in the shopping cart.

Contents

1. Operations Overview
2. Resources and Organizations
3. Service Supply
- 4. Metering & Pricing**
5. Tenant Maintenance
6. Multi-cloud Management

Metering & Pricing

- ManageOne allows enterprise administrators to view resource usage statistics and track expenditures for each department.



- ManageOne allows enterprise administrators to view resource usage statistics and track expenditures for each department. The IT department can then review monthly, quarterly, and yearly metering reports and check the resource usage of each department against their budget.
 - Service pricing: An operation administrator can set a unit price for each service flavor.
 - Account management: An operation administrator can top up accounts each of which correspond to one VDC. If a service is priced and fee deduction is enabled for the service, the system deducts fees based on the quantity of used resources in the service. If the balance of an account is insufficient, the account cannot be used to apply for resources.
 - Metering reports: You can view metering results of each VDC in reports. There are different types of reports, including **Cloud Resource Details**, **Cloud Service Statistics**, **Tenant Statistics**, **Account Report**, **HUAWEI CLOUD Bill**, and **Custom Report**. You can select required types of reports to view metering data of cloud service resources.
 - Metering views: Metering views display metering results of each VDC and collect metering data of all cloud service resources in VDCs of a single tenant.
- Benefits of Metering & Pricing:
 - Services can be priced.
 - Resource usage of tenants can be metered and priced for easy business and fee settlement.
 - Detailed metering data of each VDC in a tenant is provided to facilitate operations analysis.

Tenant Report Analysis by VDC Administrators

The screenshot shows the Tenant Report Analysis interface. At the top, there are tabs for 'Cloud Resource Details', 'Cloud Service Statistics', 'Tenant Statistics', and 'Custom Report'. Below these are two main sections: a bar chart titled 'Usage' and a configuration panel.

Statistics are displayed in tables or charts.

Many statistics reports come preconfigured.

Filters can be customized.

Configuration Panel:

- After the configuration items are set, you can click the 'Save As' button at the bottom right of the page to update data. To save the configuration, you can click 'Save As'.
- Time: Absolute time
- Statistics Object: VDC
- Dimensions:
 - Region
 - Resource Type
 - Resource ID
 - Resource Name
 - Metering Metric
 - Metering Unit
 - Metering Value
 - Unit Price
 - Fee

VDC administrator (represented by a black dot)

Agent administrator (represented by a green dot)

38 Huawei Confidential



- This slide shows how VDC administrators view metering reports. Operation administrators can also view metering statistics of different VDCs on their own pages.
- You can view diverse metering statistics reports, such as monthly reports and reports in which data is collected by cloud service type, service instance, or custom conditions.
- You can configure statistics collection conditions, including the statistics period and whether tenant or VDC data is collected. The statistics period can be a relative or absolute time period.
- You can configure statistics collection fields, including the region, AZ, resource type, tag, project, resource name, resource ID, metering metric, metering unit, metering value, unit price, and fee.
- You can save reports with custom conditions so that you do not need to specify same conditions each time.
- You can export reports.
- You can subscribe to emails containing report data.

Viewing Metering Statistics by Operation Administrators

- To view metering statistics of a tenant, an operation administrator can log in to ManageOne Operation Management Portal, choose **Organization** from the top menu bar, click a tenant name, and then, choose **Metering** from the navigation pane.

The screenshot shows the ManageOne Operation Management Portal interface. The top navigation bar includes Home, Services, Resources, Organization (which is highlighted with a red box), Report, and System. Below the navigation is a tenant details card for "SZ_Huawei" with fields for Business Director, Mobile Number, Email, Description, and Synchronization Status. A "Check Detail" button is also present. The main content area has a sidebar with links like Summary, VDCs, Quota, Enterprise Projects, Resource Sets, **Metering** (highlighted with a red box), Users, User Groups, and Network Management. The "Metering Statistics" section displays a table titled "Top 5 Services by Fee" with four rows: EIP Bandwidth Monthly Bill (0.00000 USD), EVS Monthly Bill (0.00000 USD), ECS Monthly Bill (0.00000 USD), and EIP Monthly Bill (0.00000 USD). To the right is a chart titled "EIP Bandwidth Monthly Bill" showing usage in USD (0.0) over time (0 to 1000). The bottom section, "Service Statistics", lists Service Name (ECS, EIP, EIP-Bandwidth, EVS) and Total Fee (0.00000 USD). On the right side, there is a user icon labeled "Operation administrator". The HUAWEI logo is at the bottom right.

39 Huawei Confidential

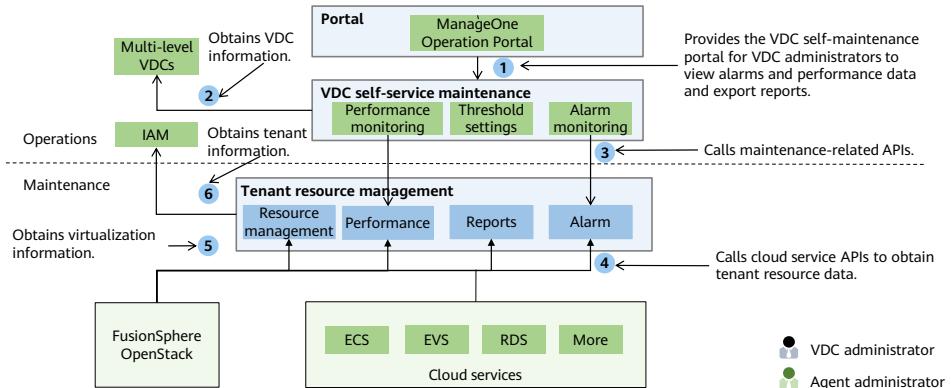
- Users can view monthly metering statistics or drill down into details.
- Operation administrators can view and export metering data of all tenants.

Contents

1. Operations Overview
2. Resources and Organizations
3. Service Supply
4. Metering & Pricing
- 5. Tenant Maintenance**
 - VDC Self-service Maintenance
 - Service, Order, and Resource Management
 - Application Management
6. Multi-cloud Management

VDC Self-service Maintenance

- Self-service Maintenance monitors resources, reports alarms, and sends notifications. VDC administrators can configure alarm thresholds, rules, and notification policies to get resource statuses of each service in real time.



41 Huawei Confidential



- VDC administrators at each level can perform the following management operations on VDCs that they belong to and their lower-level VDCs:
 - Create a lower-level VDC and configure its quotas.
 - Create and manage VDC administrators and VDC users.
 - Create and manage projects, and associate users with projects.
- ManageOne Maintenance Portal (OperationCenter) collects all maintenance data and monitors tenant resources.
- VDC self-service maintenance allows VDC administrators to set and monitor resources, alarms, and performance thresholds of VDCs that they belong to and their lower-level VDCs.
- The O&M data and basic functions are provided by ManageOne OperationCenter. The VDC self-maintenance service of ManageOne Operation Portal only displays self-maintenance data by VDC and provides the portal for performing operations on the self-maintenance data.

Contents

1. Operations Overview
2. Resources and Organizations
3. Service Supply
4. Metering & Pricing
- 5. Tenant Maintenance**
 - VDC Self-service Maintenance
 - **Service, Order, and Resource Management**
 - Application Management
6. Multi-cloud Management

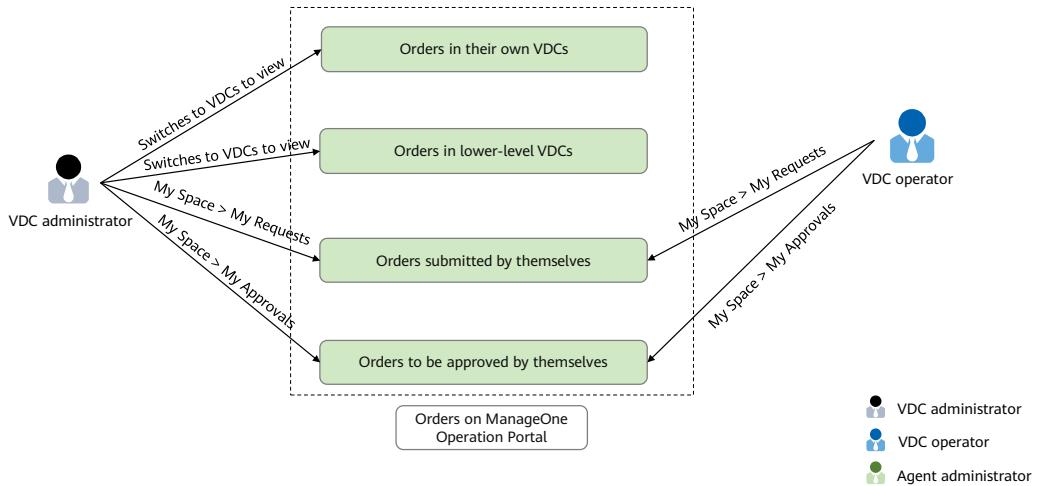
Service Management

- VDC administrators can manage:
 - Services published in upper-level VDCs
 - Services defined in their own VDCs
- VDC administrators can:
 - Bring services published in an upper-level VDC online in their own VDCs.
 - Publish services defined in their own VDCs.
 - Bring services defined in their own VDCs online in these VDCs.
- VDC operators can request:
 - Global services defined by operation administrators
 - Online services in their own VDCs

The screenshot displays two main windows. The top window is titled 'Service Management' and shows a service catalog with various categories like Computing, Storage, Network, Security, etc. A specific service entry for 'Elastic Cloud' is highlighted. The bottom window is titled 'Elastic Cloud Server' and shows a 'Select Service' dialog with two options: 'ecs_3husd01' and 'ECS'. Below the dialog, there's a list of users with their roles: 'user_Huawei' (VDC administrator), 'user_Huawei' (VDC operator), and 'user_Huawei' (Agent administrator). The HUAWEI logo is visible at the bottom right.

43 Huawei Confidential

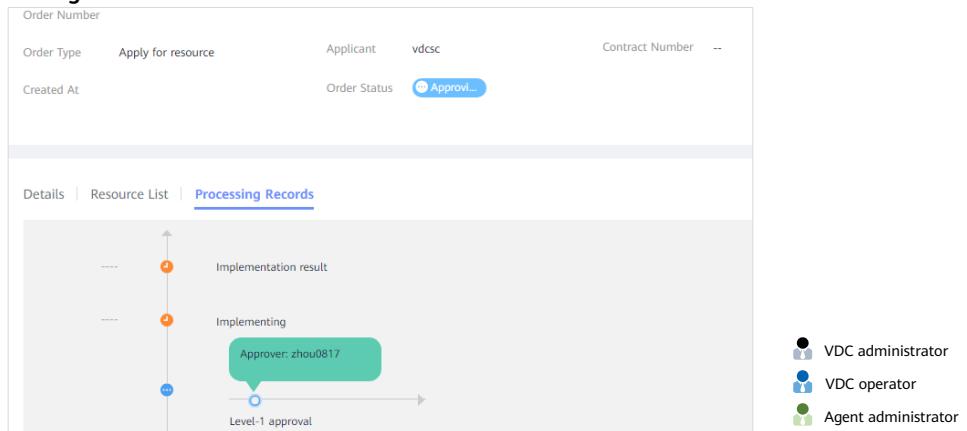
Order Management (1)



- A VDC administrator can submit or approve orders. They can view all orders in their own VDCs and lower-level VDCs.
- A VDC operator can submit orders. To enable a VDC operator to approve an order, the VDC operator must be added as an approver to the approval process associated with the order.

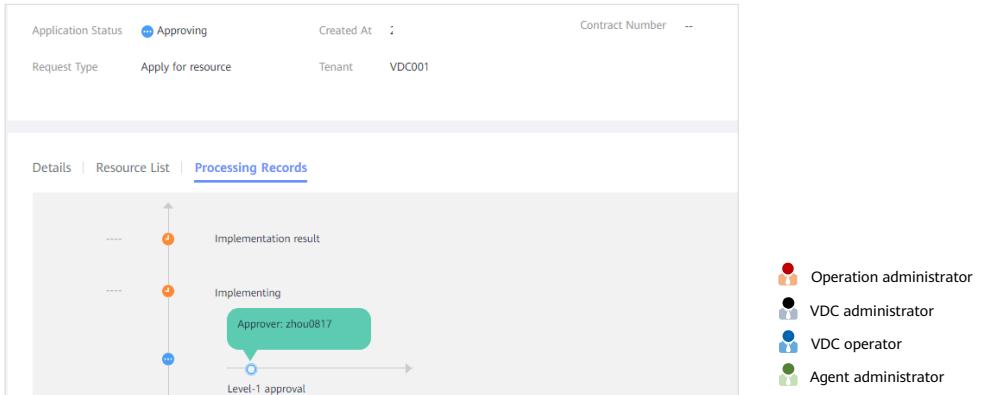
Order Management (2)

- VDC operators or order submitters can view order processing records, including approval records, on the **Processing Records** tab.



Order Management (3)

- In their approval records, VDC administrators or approval owners can view approvers, when approvals were completed, what approval comments there were, and how long it took for approvals for each completed approval phase.



Resource Overview

- To view an overview of the resources and their permissions scopes, VDC administrators or operation administrators can choose **Resources** from the menu bar at the top.



VDC administrator

The screenshot shows the HUAWEI CLOUD Stack interface. The top navigation bar includes Home, Resources (highlighted with a red box), Applications, Report, System, English, and Logout. Below the navigation is a search bar and a 'Switch Region' button. The main content area is titled 'Allocated Resources'. It features two tabs: 'Allocated Resources' (selected) and 'Allocated Quotas'. Under 'Allocated Resources', there are sections for Resource Type (with a toggle switch for 'Only display resource types that contain') and Region. A table lists resources: WordPress (2), Virtual Private Cloud (2), Elastic Volume Service (4), Elastic IP (1), and WordPress (2). Below the table are 'Selected' filters for Resource Type (All) and Region (All). At the bottom are 'Export' and 'Search' buttons.



Operation administrator

The screenshot shows the HUAWEI CLOUD Stack interface. The top navigation bar includes Home, Services, Resources (highlighted with a red box), Organization, Report, System, English, and Huawei. Below the navigation is a search bar and a 'Switch Region' button. The main content area is titled 'Overview'. It features a sidebar with 'Overview', 'Resource List', 'Applications', and 'Onboarding'. The main area displays resource counts: Image Management (6), Elastic Cloud Server (25), and Elastic Volume Service (25).

- VDC administrators and operation administrators can only view resources on this page. They cannot manage resources on this page.

Resource Management

- VDC operators or VDC administrators can select a cloud service, go to the cloud service console, and manage the resources displayed there.

The screenshot shows the HUAWEI CLOUD Stack interface. At the top, there's a navigation bar with tabs: Home, Resources, Application, Report, and System. The Resources tab is currently selected. Below the navigation bar, there's a search bar with 'Region' set to 'hangzhou' and 'Resource Set' set to 'zj-hz-1_Res_Huadawei'. Underneath the search bar is a text input field with placeholder text 'Enter a name to search for a service.' The main content area is organized into several sections:

- Basic cloud services**:
 - Computing**: WordPress, Service_154c, Image Management Service, Cloud Container Engine, Auto Scaling, Elastic Cloud Server, Bare Metal Server.
 - Storage**: Cloud Server Backup Service, Volume Backup Service, Elastic Volume Service, Object Storage Service 3.0.
 - Network**: Virtual Private Cloud, Elastic Load Balance, Elastic IP, Network ACL, Virtual Private Network, Direct Connect, VPC Endpoint, Cloud Domain Name Service, Cloud Firewall.
- Database**:
 - Database**: GaussDB SQL, Data Replication Service.

On the right side of the interface, there's a legend for user roles:

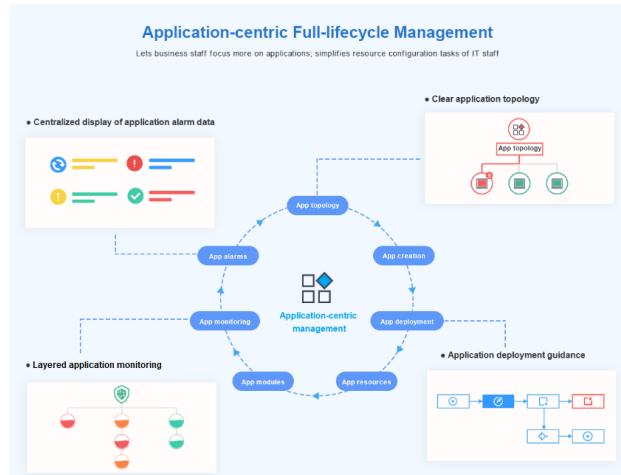
- VDC administrator (Icon: person with a crown)
- VDC operator (Icon: person with a blue circle)
- Agent administrator (Icon: person with a green circle)

Contents

1. Operations Overview
2. Resources and Organizations
3. Service Supply
4. Metering & Pricing
- 5. Tenant Maintenance**
 - VDC Self-service Maintenance
 - Service, Order, and Resource Management
 - Application Management**
6. Multi-cloud Management

Application Overview

- An application corresponds to a customer's business system. Users can manage resources and create modules in applications, or use the UI to install and manage application software.
- ManageOne also provides application-based monitoring and alarm views to facilitate resource management.



50 Huawei Confidential

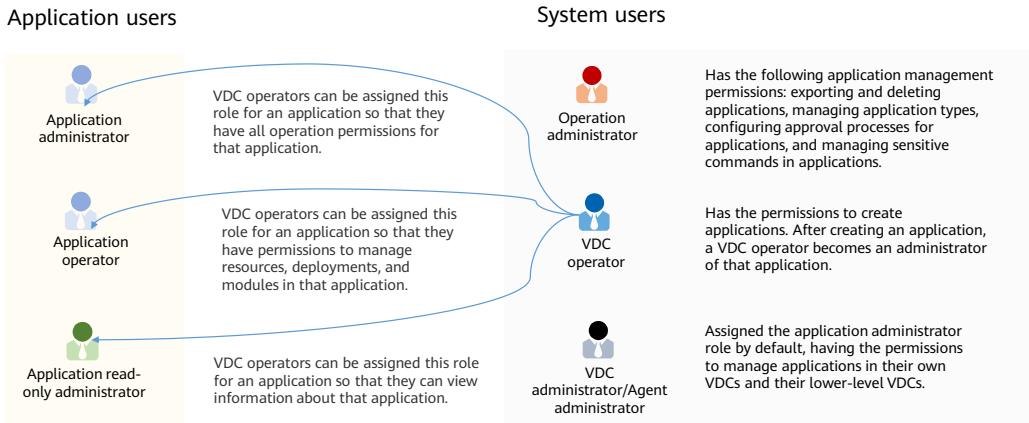


- Application Management has the following features:
 - Easy to build
 - The UI makes it easy to create diverse applications on demand. For instance, you can use the UI to configure application details, add resources, and create modules and deployment tasks.
 - Easy to deploy
 - You can use graphically designed deployment processes to install, upgrade, and maintain application software.
 - Easy to manage
 - You can view application topologies and all-round application monitoring data, perform UI-based operations to manage applications, resources, modules, deployments, users, and alarms, as well as start and stop resources and manage processes with a few clicks.

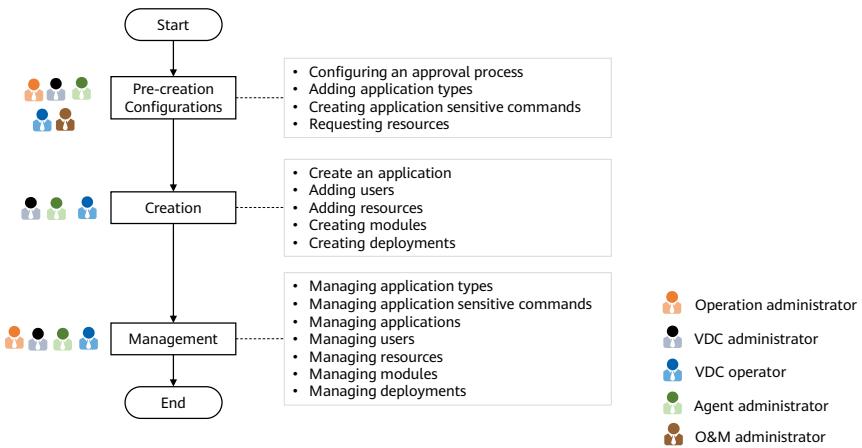
Application Users

Application users	 Application administrator	Has all operation permissions for an application: managing applications, resources, users, modules, and deployments.
	 Application operator	Has the permissions to manage resources, modules, and deployments in applications. However, they cannot add or remove resources from applications.
	 Application read-only administrator	Has the permission to view application information.
System users	 Operation administrator	Has the highest-level operations management permissions. bss_admin is the preconfigured operation administrator.
	 VDC administrator/Agent administrator	Has management permissions for their own VDCs and lower-level VDCs, including all resources in those VDCs.
	 VDC operator	Has management permissions for all resources in the resource sets associated with them.

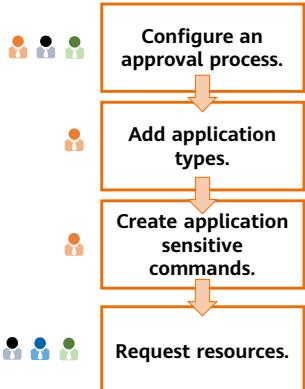
Relationships Between System Users and Application Users



Application Management Process



Configurations Before Application Creation



An approval process can be associated with applications. After doing so, when a VDC user creates or modifies an application, the request needs to be approved based on the approval process.

An operation administrator can add application types, so when creating applications, VDC users can select desired types based on how the applications will be used.

Certain commands can be configured as sensitive commands in applications, and the system will identify them in a timely manner. This ensures that operations for applications are secure and controllable.

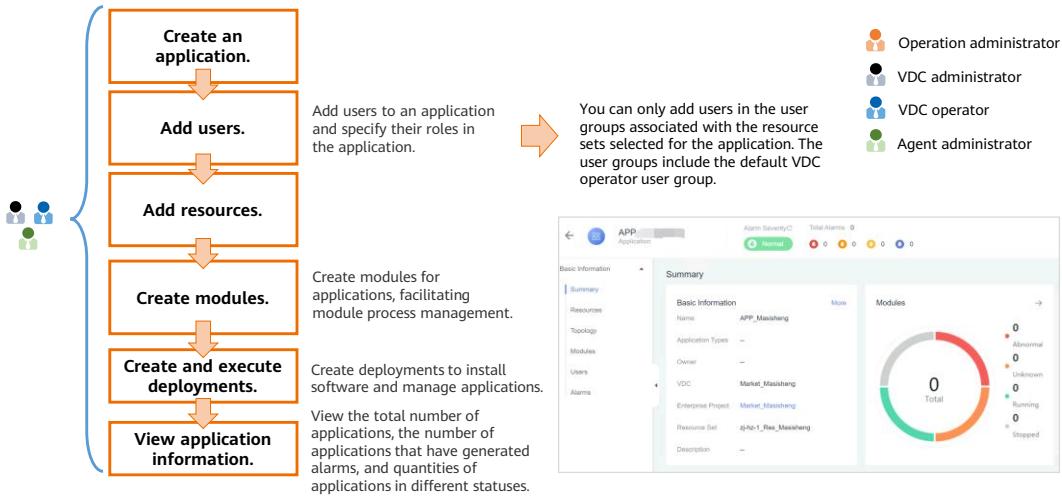
VDC users request ECs and BMs.



- Operation administrator
- VDC administrator
- VDC operator
- Agent administrator



Creating an Application

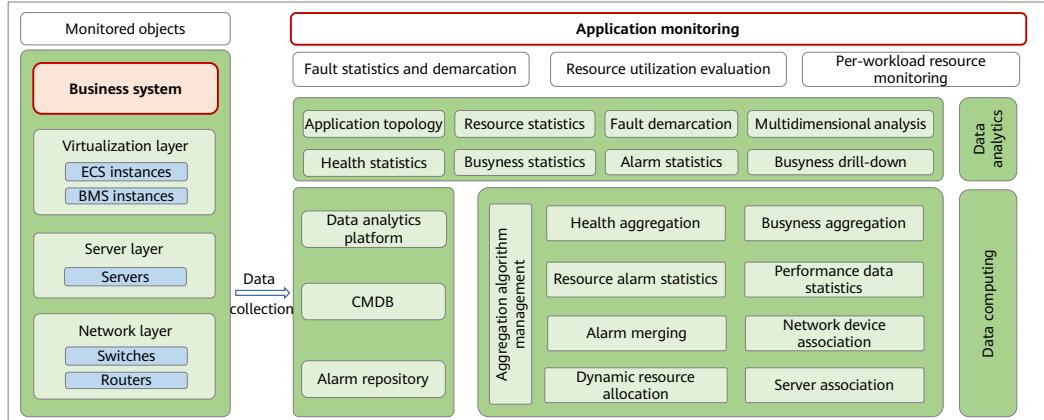


55 Huawei Confidential

- Adding an application user:
 - You can only add users in the user groups associated with the resource sets selected for the application. The user groups include: The default VDC operator user group
 - Custom user groups not assigned the **VDC Admin** or **VDC Readonly** permission
- Viewing application information:
 - Operation administrators can view all applications. VDC administrators can view applications in their own VDCs and lower-level VDCs. VDC operators can only view their own applications.
 - On the **Basic Information** page, view the application details, including the **Summary**, **Resources**, **Topology**, **Modules**, **Users**, **Deployments**, and **Alarms** information. Only VDC users can view deployment information.
 - Before viewing the busyness of application resources in the topology, ensure that the OperationInsight license has been imported and the resource pool has been updated. You can use an operation administrator account to update the resource pool on the **System > System Integration > Private Cloud Access** page.

Application Resource Monitoring

- **Positioning and value:** Compared with conventional resource-centric monitoring, application-centric monitoring is more helpful in ensuring service continuity and stability.



56 Huawei Confidential



- ManageOne comprehensively evaluates the status of application resources at the virtualization, server, and network layers.
 - When O&M personnel detect an application fault through fault reports, alarm notifications, or routine health checks, they can leverage the fault demarcation capability of Application Resource Monitoring to quickly determine whether the fault occurs at the virtualization layer, server layer, or network layer, specify the owner, and rectify the fault as soon as possible.
 - When evaluating resource utilization by application, O&M personnel can leverage the busyness evaluation capability of Application Resource Monitoring to quickly identify applications with low resource utilization. In addition, they can also assess resource utilization at the virtualization layer, server layer, and network layer to quickly obtain the evaluation result.
 - The resource utilization of applications is monitored in real time to help O&M personnel detect and avoid service interruption or faults caused by insufficient resources in a timely manner. In addition, O&M personnel can quickly determine what performance metrics of what resources at which layer among the virtualization layer, server layer, and network layer has high resource utilization, providing data support for customers' capacity expansion decisions.

Application Analysis on Operation Portal: Health Evaluation

- VDC administrators can quantitatively evaluate health and busyness.

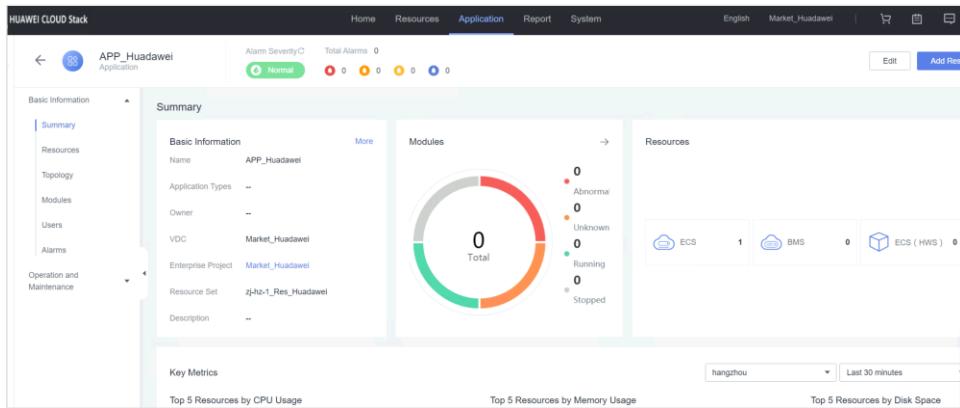
The screenshot shows the HUAWEI CLOUD Stack Application interface. At the top, there are tabs for Home, Resources, Application (which is selected), Report, and System. Below the tabs, there's a summary section with counts for Total Applications (1), Application Alarms (0 Critical, 0 Major, 0 Minor, 0 Warning), Application Statuses (1 Running, 0 Approving, 0 To be submitted, 0 To be deleted), and Application Types (1 OtherCategory). There are also Create and Export buttons. A search bar allows entering an application name. The main table lists one application: APP_Huawei, which is running and has normal alarms. It also shows details like Owner (--), Operator (--), VDC (Market_Huawei), Enterprise Project (Market_Huawei), Application Types (zj-hz-1_Res_Hua...), and Resource Set (Edit Delete).

Application Name	Status	Alarms	Owner	Operator	VDC	Enterprise Project	Application Types	Resource Set	Operation
APP_Huawei	Running	Normal	--	--	Market_Huawei	Market_Huawei	--	zj-hz-1_Res_Hua...	Edit Delete

- Application Analysis provides the following functions:
- Application health and busyness can be quantitatively evaluated.
- Basic information, performance data, alarms, and topologies of each resource can be displayed on one page.
- An application topology shows you resources and resource associations at different layers. It also shows resource health, busyness, alarms, and performance data so you can demarcate faults faster.

Application Analysis on Operation Portal: Aggregated Analysis

- VDC administrators can view basic information, performance data, alarms, and topologies of many kinds of resources on the same page.



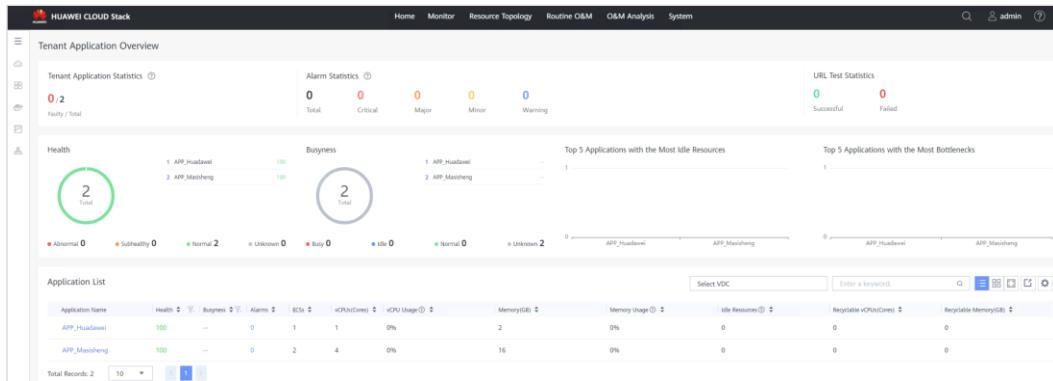
58 Huawei Confidential



- VDC administrators or operation administrators can view accurate statuses of allocated resources in the monitoring view on the resource management page.

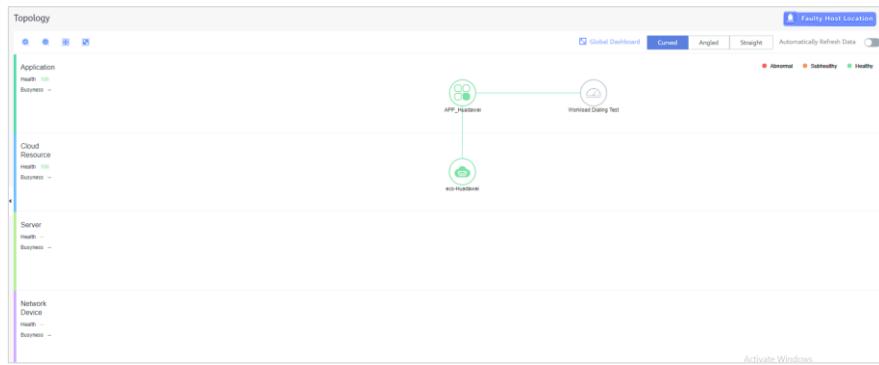
Application Analysis on Maintenance Portal: Application Maintenance

- O&M administrators can view information for all tenant applications on ManageOne, including the quantity, health, busyness, risks, and exceptions.



Application Analysis on Maintenance Portal: Association Topology

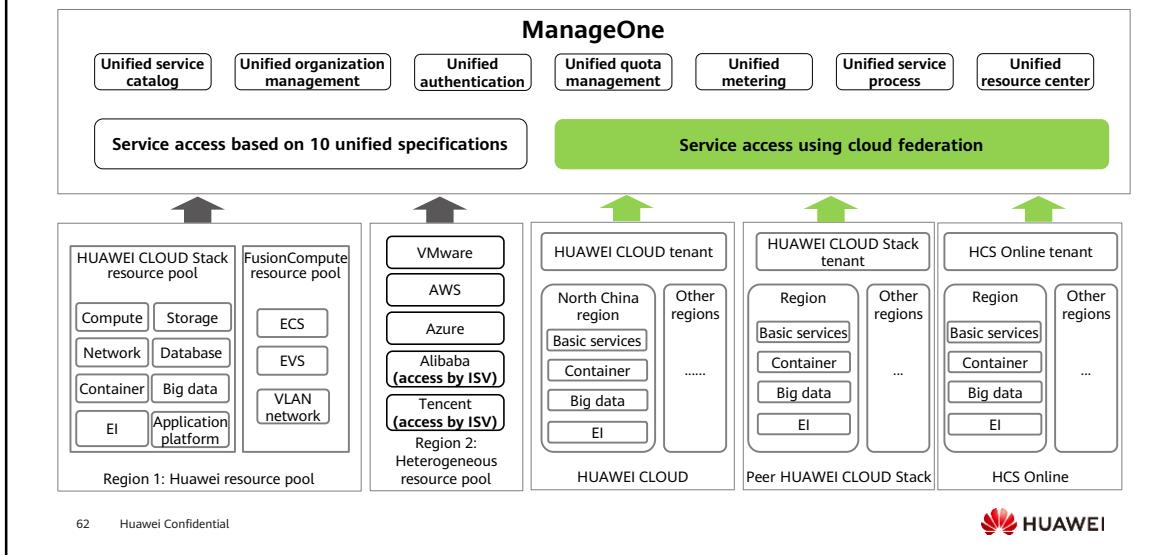
- ManageOne Maintenance Portal uses application topologies to display application resources and their associations as well as other application data including health, busyness, alarms, and performance data, so users can locate faults faster.



Contents

1. Operations Overview
2. Resources and Organizations
3. Service Supply
4. Metering & Pricing
5. Tenant Maintenance
- 6. Multi-cloud Management**

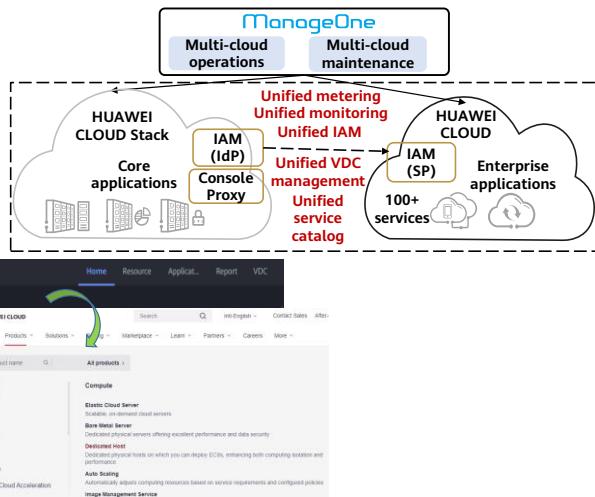
Multi-cloud Management Overview



- Multiple clouds are connected to ManageOne of HUAWEI CLOUD Stack in either of the following ways:
- One cloud access: The following clouds can be connected to ManageOne based on 10 unified specifications: HUAWEI CLOUD Stack, FusionCompute, VMware, AWS, Azure, Alibaba Cloud (connection plug-ins provided by ISVs, not included in the baseline version), and Tencent Cloud (connection plug-ins provided by ISVs, not included in the baseline version). ISVs can connect services from other platforms to ManageOne based on the 10 unified specifications.
- Cloud federation: HUAWEI CLOUD, HUAWEI CLOUD Stack, and HCS Online (in Huawei edge regions and DeC scenarios) are supported. You can request cloud service resources in these resource pools on ManageOne as a tenant through federated authentication. Note that:
 - The connection to HCS Online does not support unified quota management, metering, service process, and resource center.
 - When HCS Online is deployed in the customer's equipment room, ManageOne manages HCS Online using the 10 unified specifications.

Cloud Federation Overview

- Cloud Federation is a new approach to hybrid clouds. It is provided by ManageOne based on the same architecture plus Identity and Access Management (IAM) shared between HUAWEI CLOUD Stack and HUAWEI CLOUD.

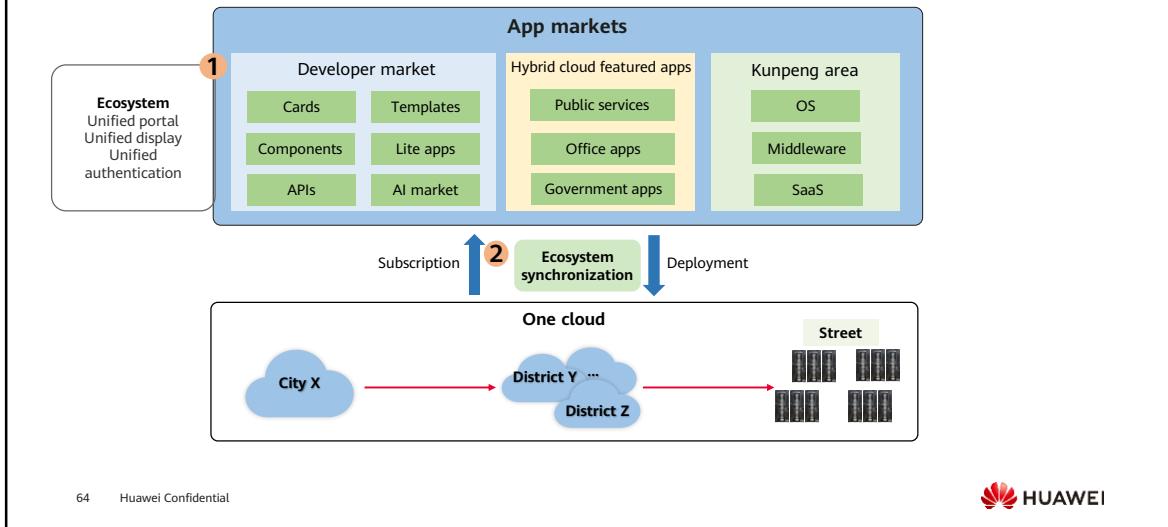


63 Huawei Confidential



- In a traditional hybrid cloud, the API interconnection approach is used. A private cloud needs to connect to the API of each public cloud service required by private cloud users and implements the logic of requesting the public cloud service. The workload is equivalent to developing the console and requesting process of the public cloud service on the private cloud. If many public cloud services are required, the workload is huge. To make things worse, the private cloud needs to adapt to fast changes to public cloud services such as containers, big data, and EI.
- To overcome the disadvantages of traditional API interconnection, ManageOne provides cloud federation. Cloud federation enables federation between HUAWEI CLOUD Stack IAM and HUAWEI CLOUD IAM, so VDC users of HUAWEI CLOUD Stack ManageOne can request and use a wide range of HUAWEI CLOUD services within their permissions scopes. Just one connection is enough. HUAWEI CLOUD Stack does not need to connect to HUAWEI CLOUD services one by one.
- Identity provider (IdP): a system that authenticates user identities. For example, IAM is the identity provider of the public cloud system. In federated identity authentication, the identity system of your organization is the identity provider.
- Service provider (SP): a system that provides services. In federated identity authentication, the public cloud system is the service provider.

Cloud Federation Marketplace

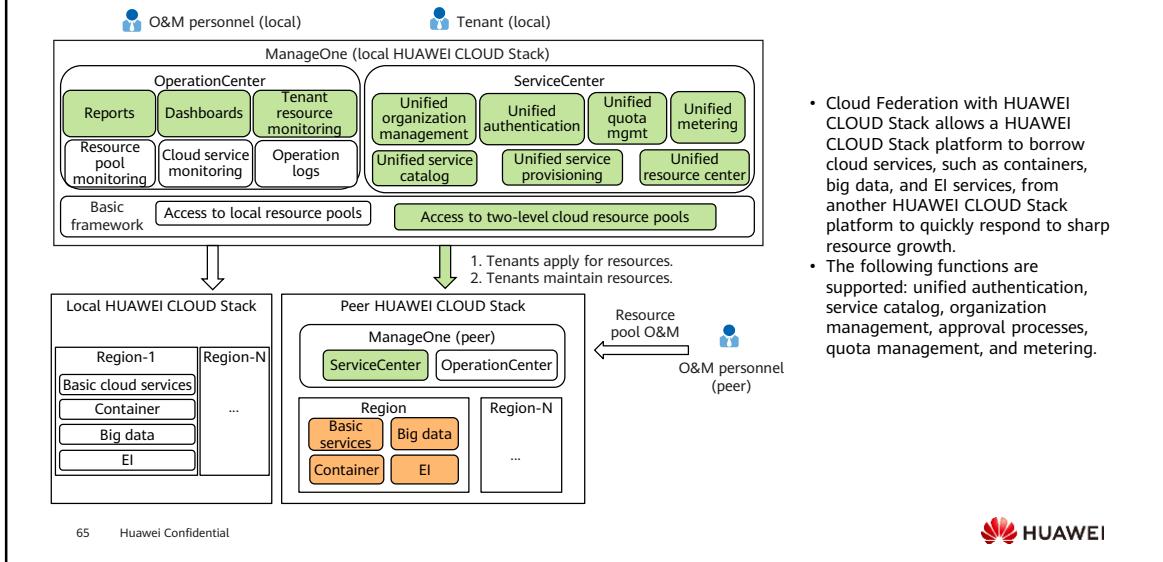


64 Huawei Confidential



- The hybrid cloud marketplace is like an online store. It presents cloud or offline applications provided by third-party service providers to users. It helps customers quickly, easily, securely migrate workloads to the cloud.
- The hybrid cloud marketplace integrates on-cloud and off-cloud offerings in marketplaces of both HUAWEI CLOUD and HUAWEI CLOUD Stack.
 - HUAWEI CLOUD marketplace: HUAWEI CLOUD cooperates with ISVs to provide users with various application offerings, including applications, operating environment, bandwidth, and cloud server resources. You can quickly purchase suitable application offerings on the marketplace (including the complete environment for running the application software), and use the purchased application software and services to release your own products.
 - HUAWEI CLOUD Stack marketplace: HUAWEI CLOUD Stack cooperates with ISVs to provide an entry for requesting consulting-related offerings. The HUAWEI CLOUD Stack marketplace allows customers to view and consult about the offerings that cannot be provisioned on the HUAWEI CLOUD marketplace or automatically orchestrated and provisioned on ManageOne.

Cloud Federation with HUAWEI CLOUD Stack



- Cloud Federation with HUAWEI CLOUD Stack allows a HUAWEI CLOUD Stack platform to borrow cloud services, such as containers, big data, and EI services, from another HUAWEI CLOUD Stack platform to quickly respond to sharp resource growth.

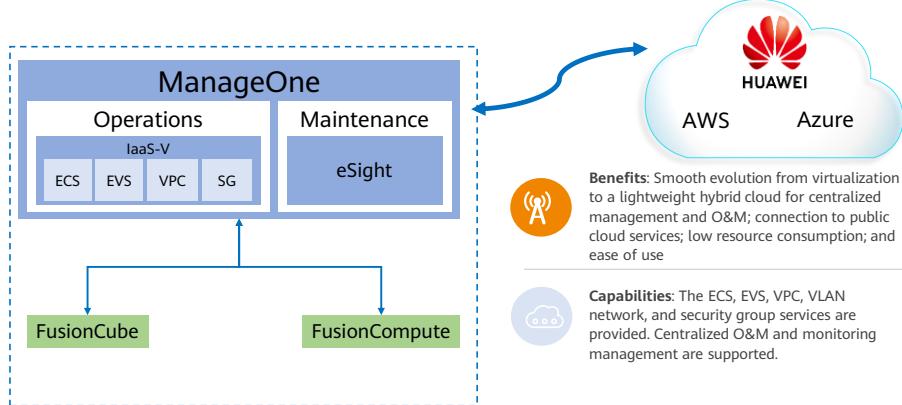
- The following functions are supported: unified authentication, service catalog, organization management, approval processes, quota management, and metering.



- The traditional multi-cloud integration solution requires heavy workload. Cloud federation with HUAWEI CLOUD Stack is a lightweight solution for multi-cloud integration.
- In this slide, the peer HUAWEI CLOUD Stack that provides big data services serves as the resource provider, and the local HUAWEI CLOUD Stack that uses big data services serves as the resource user. The cloud federation process is as follows:
 - Negotiate and determine how many resources can be used by local HUAWEI CLOUD Stack.
 - Create a tenant on peer HUAWEI CLOUD Stack and set the quota to the resource quantity specified in step 1. The tenant is used by local HUAWEI CLOUD Stack to request resources.
 - Interconnect local HUAWEI CLOUD Stack with peer HUAWEI CLOUD Stack on the **Two-Level Cloud Access** page of local ManageOne. The interconnection account is the tenant created in step 2.
 - Associate the VDC of local HUAWEI CLOUD Stack with the resource pool of peer HUAWEI CLOUD Stack on demand. Then, users in the VDC can request resources of peer HUAWEI CLOUD Stack in federated authentication mode.

Onboarding Virtual Resource Pools to Cloud

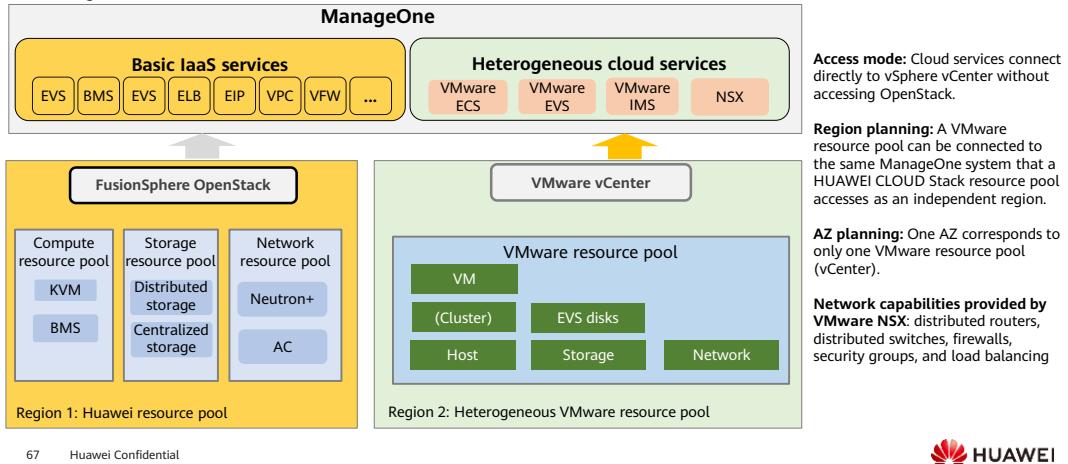
- HUAWEI CLOUD Stack supports smooth evolution from virtualization to a lightweight easy-to-use cloud with low resource consumption that is inexpensive and provides multi-cloud management capabilities.



- Take FusionCompute as an example. ManageOne centrally manages virtual resource pools managed by FusionCompute and synchronizes cloud service resources, such as ECSs and EVS disks, in virtual resource pools managed by FusionCompute. ManageOne provides a unified portal to centrally manage diverse resource pools of FusionCompute.

Onboarding VMware Virtual Resource Pools

- HUAWEI CLOUD Stack can use VMware Services to onboard VMware resources and provide them for tenants. The VMware Services include VMware ECS, VMware EVS, VMware IMS, and VMware snapshot. This helps customers centrally manage their new and existing VMware resources.

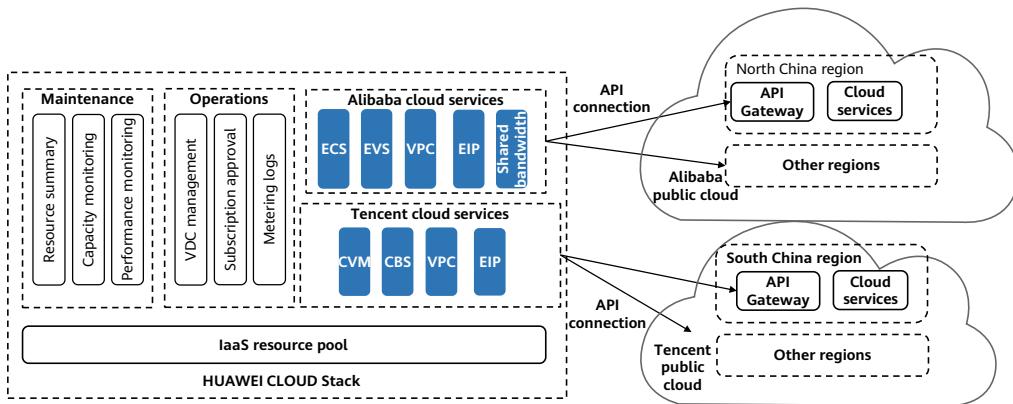


67 Huawei Confidential



- HUAWEI CLOUD Stack can use virtual resource pool onboarding to centrally manage existing VMware resource pools to meet different service requirements. As such, HUAWEI CLOUD Stack can centrally manage resource pools of both HUAWEI CLOUD Stack and VMware.

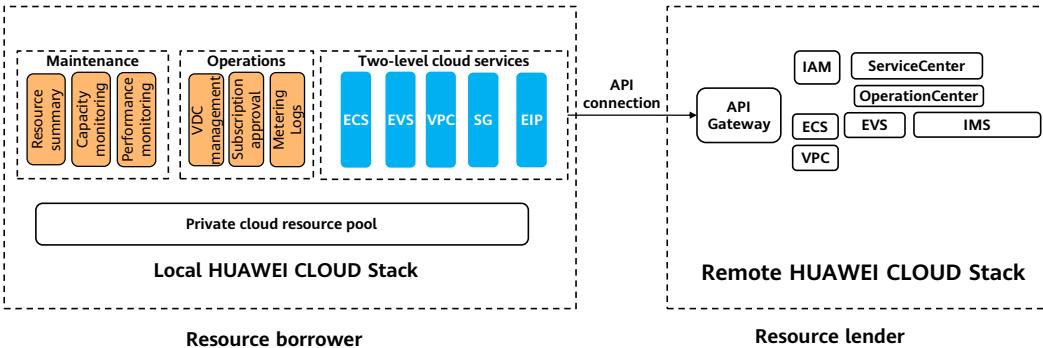
Onboarding Heterogeneous Third-party Clouds



- Prerequisites:
 - Guanghua-CA has developed the Alibaba Cloud service layer based on the 10 unified specifications of HUAWEI CLOUD Stack and interconnected this service layer with Alibaba Cloud APIs to provide ECS, EVS, VPC, EIP, and shared bandwidth services.
 - Guanghua-CA has developed the Tencent Cloud service layer based on the 10 unified specifications of HUAWEI CLOUD Stack and interconnected this service layer with Tencent Cloud APIs to provide CVM (cloud server), CBS (cloud volume), VPC, and EIP services.
- A customer wanted to use ManageOne to centrally manage services of HUAWEI CLOUD Stack and Alibaba Cloud (or Tencent Cloud) deployed at their local site to cut management costs.
- Onboarding process:
 - Deploy the Alibaba Cloud service components of Guanghua-CA on ManageOne, use the customer's Alibaba Cloud account to access Alibaba Cloud, and synchronize information about the Alibaba Cloud region to ManageOne.
 - When creating a tenant, an operation administrator associates the tenant with an Alibaba Cloud region and configures quotas for the tenant.
 - Users of the tenant log in to ManageOne, select the Alibaba Cloud region in the service catalog, and apply for Alibaba Cloud services.

Two-level cloud services

- A two-level cloud allows a local HUAWEI CLOUD Stack resource pool with insufficient resources to borrow resources from another cloud.



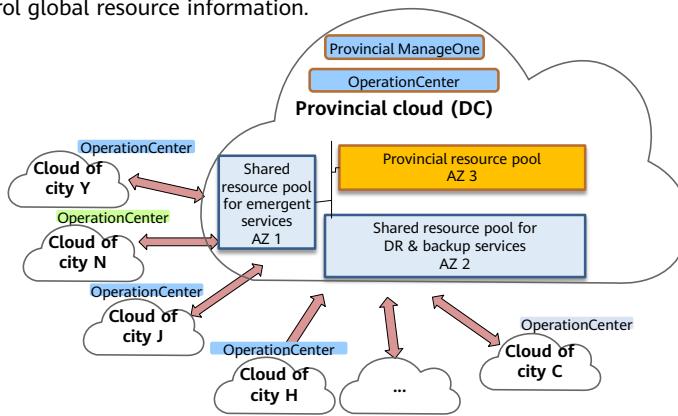
69 Huawei Confidential



- Currently, the two-level cloud takes less priority in HUAWEI CLOUD Stack.
- Two-level Cloud allows a local HUAWEI CLOUD Stack resource pool with insufficient resources to borrow resources from another one.
- Before resources are borrowed, a first-level VDC and administrator account need to be created on ManageOne of peer HUAWEI CLOUD Stack. The local HUAWEI CLOUD Stack uses this account to request resources from the peer HUAWEI CLOUD Stack.
- Two-level cloud supports ECS, EVS, VPC, EIP, SG, and IMS. IMS supports image query only. If private images are required, use the first-level VDC administrator account to log in to the IMS console of the peer HUAWEI CLOUD Stack and create a private image.
- The two-level cloud is co-deployed with ManageOne. No additional resources need to be deployed.

Multi-cloud Monitoring

- Multi-cloud Monitoring supports centralized monitoring of resources from multiple clouds at different levels and provides comprehensive cloud resource usage information, helping organizational leaders easily control global resource information.



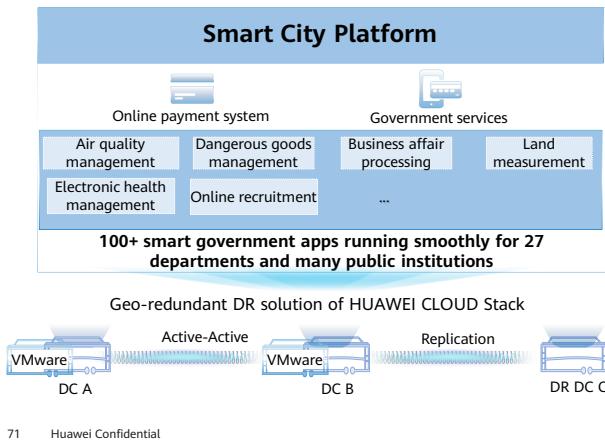
70 Huawei Confidential



- To meet intensive monitoring requirements of group customers, the HQ DC centrally monitors resources in multiple clouds at two levels of peripheral site DCs and supports query and statistics collection for global cloud resources.
- Key technologies:
 - The municipal cloud NBI provides the API for summarizing data, including alarm statistics data, resource statistics, and resource pool capacity data.
 - Municipal cloud data is synchronized to the provincial cloud and multi-cloud management is supported.
- Key specifications (scope):
 - Rights- and domain-based control can be implemented cloud by cloud.
 - Resource pool capacity information, resource quantities, alarm statistics, and resource pool load information can be displayed cloud by cloud.
 - Data reports can be generated cloud by cloud.

Case - Geo-Redundant DR Solution for a City

- Huawei used a HUAWEI CLOUD Stack geo-redundant DR solution to provide multi-level protection for the customer to ensure service continuity. ManageOne, a centralized cloud management platform, was used to centrally manage and maintain multiple data centers and vendors, including VMware. Huawei helped the customer deploy 258 nodes, migrated over 100 business systems to the cloud, and launched smart city applications.



71 Huawei Confidential



Solutions

- Huawei's geo-redundant DR solution provides intra-city active-active replication and remote asynchronous replication to ensure zero data loss in core systems.
- BCManager provides visual DR management using DR views and supports one-click automated failover for seamless service switchover.
- ManageOne, a centralized management platform, allows the customer to centrally, visually manage resources from different vendors and across multiple DCs, improving O&M efficiency by 65%.



Highlights

- Active-active architecture, ensuring zero data loss
- Automated failover for seamless service switchover
- Per-tenant DR protection for core services



- Pain points:
 - The customer has deployed over 100 government applications for 27 departments and many public institutions. However, there is no complete disaster recovery system in the data center to protect the services. Once a disaster occurs, services may be interrupted and data loss will occur. The customer requires that their 30 core applications and database systems among the applications keep no data loss in disasters.
 - Manually locating and troubleshooting faults causes long downtime. The customer requires automated fault detection and failover for fast service switchover in the event of faulty databases and VM services and requires no labor increase.
 - It is hard for the customer to demarcate system faults across multiple vendors (IBM, VMware, and EMC).
- Solution
 - Huawei used the HUAWEI CLOUD Stack geo-redundant DR solution to provide multi-level protection for the customer to ensure service continuity. ManageOne, a centralized cloud management platform, was used to centrally manage and maintain multiple data centers and vendors including VMware. Huawei helped the customer deploy 258 nodes, migrated over 100 business systems to the cloud, and launched smart city applications.

- Highlights
 - Huawei's geo-redundant DR solution provides DR as a service. Tenants can apply for DR protection for more than 30 core applications on demands. The solution uses industry-leading storage replication technology to quickly protect any types of applications and databases. Plus, the solution provides intra-city active-active replication and remote asynchronous replication to ensure zero data loss in core systems.
 - BCManager provides visual DR management using DR views and supports one-click automated failover for seamless service switchover.
 - ManageOne allows the customer to centrally, visually manage resources from different vendors and across multiple DCs, improving O&M efficiency by 65%.
- Summary
 - With this solution, over 100 smart government apps can stably run for 27 departments and many public institutions of the customer. The customer-developed apps provide one-stop government services. The services are made available 24/7. The e-health system reduces patient waiting time. The online recruitment system saves paper and improves efficiency.

Quiz

1. (True or false) A VDC administrator can be assigned the application administrator role.
2. (True or false) VDC operators can configure quotas for VDCs or enterprise projects.
3. (Multiple-answer question) Which of the following roles can configure the visible scope for a service when it is published?
 - A. Operation administrator
 - B. VDC administrator
 - C. VDC operator
 - D. Agent administrator

- 1. False
- 2. False
- 3. ABD

Summary

- This course has introduced and covered the main steps of provisioning services as well as tenant maintenance and multi-cloud management on HUAWEI CLOUD Stack. You have also learned some common concepts, their relationships, user roles, and resource sets in HUAWEI CLOUD Stack. When bringing a service online, administrators need to create, publish, and bring the service online, and associate the service with related approval processes. Operation administrators can configure metering and pricing for services.

Recommendations

- Huawei Talent:
 - <https://e.huawei.com/en/talent/portal/#/>
- Huawei Certification:
 - <https://forum.huawei.com/enterprise/en/forum-813.html>

Acronyms (1)

Acronym	Full Name	Description
AZ	Availability Zone	Used to isolate physical resources.
VPC	Virtual Private Cloud	A VPC provides an isolated virtual network for cloud servers. You can configure and manage the virtual network.
VDC	Virtual Data Center	A VDC is a new type of data center that applies cloud computing to Internet data center (IDC).
HCS	HUAWEI CLOUD Stack	HUAWEI CLOUD Stack is a data center solution that manages physically distributed, logically unified resources, coordinates cloud management, and provides insights into services.
VNC	Virtual Network Console	VNC is open-source software based on UNIX and Linux OSs. It can serve as an auxiliary desktop login method used when desktop login fails due to network faults.
CPU	Central Processing Unit	A central processing unit used to interpret computer instructions and process data in computer software.
ECS	Elastic Cloud Server	An ECS is a computing server that consists of CPUs, memory, images, and Elastic Volume Service (EVS) disks and allows on-demand allocation and elastic scaling.

Acronyms (2)

Acronym	Full Name	Description
ELB	Elastic Load Balance	ELB is a service that automatically distributes access traffic to multiple ECSSs to balance the load. It provides greater fault tolerance in applications and expands application service capabilities.
BMS	Bare Metal Server	A BMS is a physical server dedicated for a single tenant.
RAM	Random-access memory	Random-access memory is a form of computer memory that can be read and changed in any order, typically used to store working data and machine code.
RTS	Resource Template Service	Resource Template Service (RTS) helps users model and set up public cloud resources.
EIP	Elastic IP Address	EIP enables your cloud resources to communicate with the Internet using static public IP addresses and scalable bandwidths.
VM	Virtual Machine	Virtual machine
EVS	Elastic Volume Service	An EVS disk is a virtual block storage that is based on distributed architecture and can elastically scale up and down.
API	Application Programming Interface	An API is a particular set of rules and specifications used to facilitate communication between software programs.

Thank you.

把数字世界带入每个人、每个家庭、

每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.

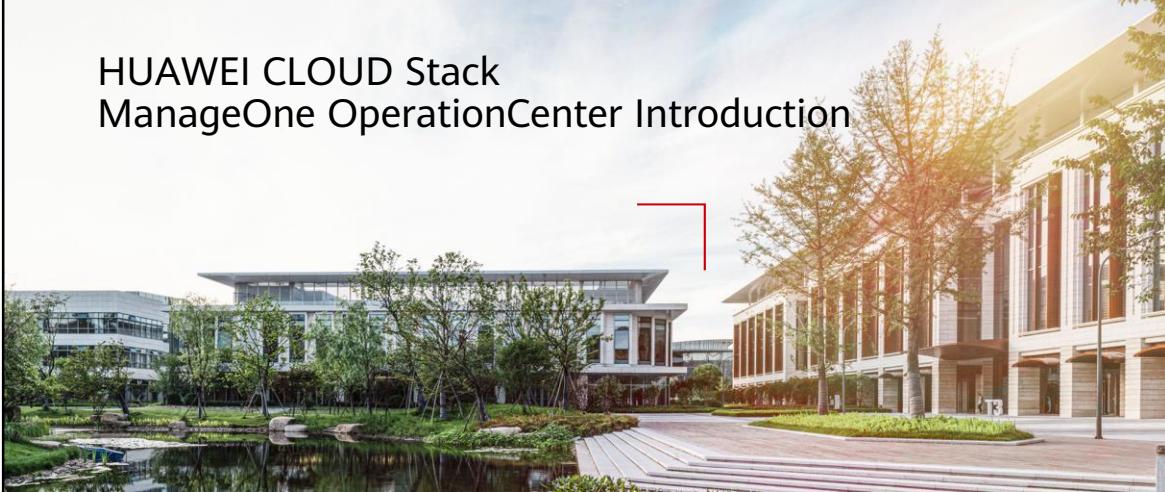
Copyright©2022 Huawei Technologies Co., Ltd.
All Rights Reserved.

The information in this document may contain predictive statements including, without limitation, statements regarding the future financial and operating results, future product portfolio, new technology, etc. There are a number of factors that could cause actual results and developments to differ materially from those expressed or implied in the predictive statements. Therefore, such information is provided for reference purpose only and constitutes neither an offer nor an acceptance. Huawei may change the information at any time without notice.



HUAWEI CLOUD Stack

ManageOne OperationCenter Introduction



Foreword

- This course describes the logical architecture and core capabilities of HUAWEI CLOUD Stack ManageOne OperationCenter as well as HUAWEI CLOUD Stack maintenance capabilities in different scenarios.

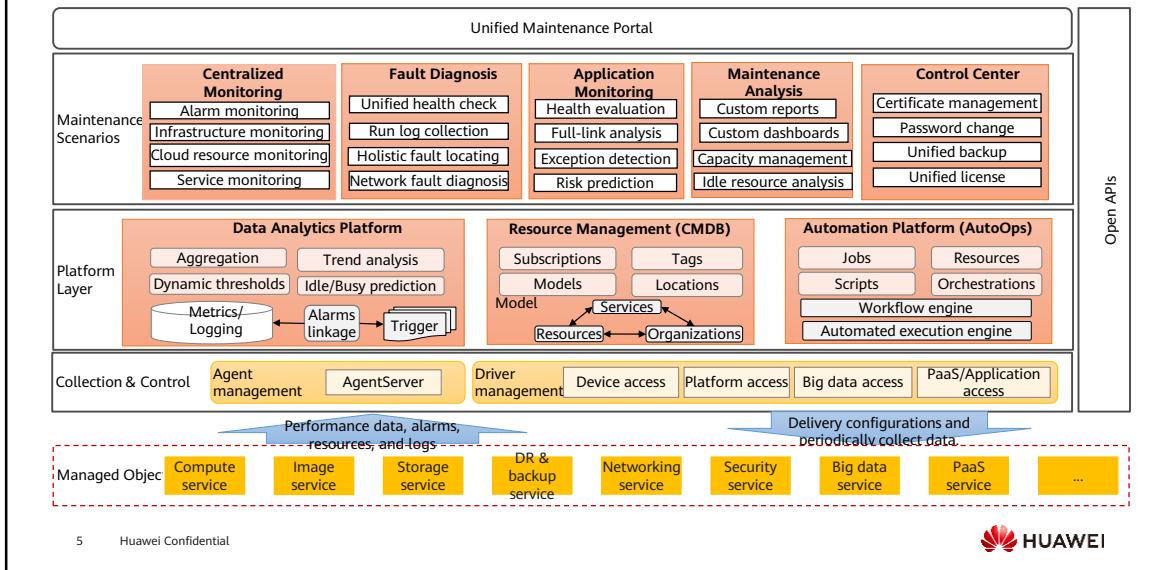
Objectives

- Upon completion of this course, you will understand:
 - The logical architecture and core capabilities of ManageOne Maintenance Portal.
 - The data collection and control principles of ManageOne at the data collection and control layer.
 - The basic principles of the ManageOne platform layer.
 - The functions and configurations of ManageOne in different maintenance scenarios.
 - How to use ManageOne maintenance tools.
 - How to analyze data using ManageOne reports.

Contents

- 1. Maintenance Overview**
2. Maintenance Functions at the Collection and Control Layer
3. Maintenance Functions at the Platform Layer
4. Maintenance Functions in Different Scenarios

Maintenance Overview: Function Overview

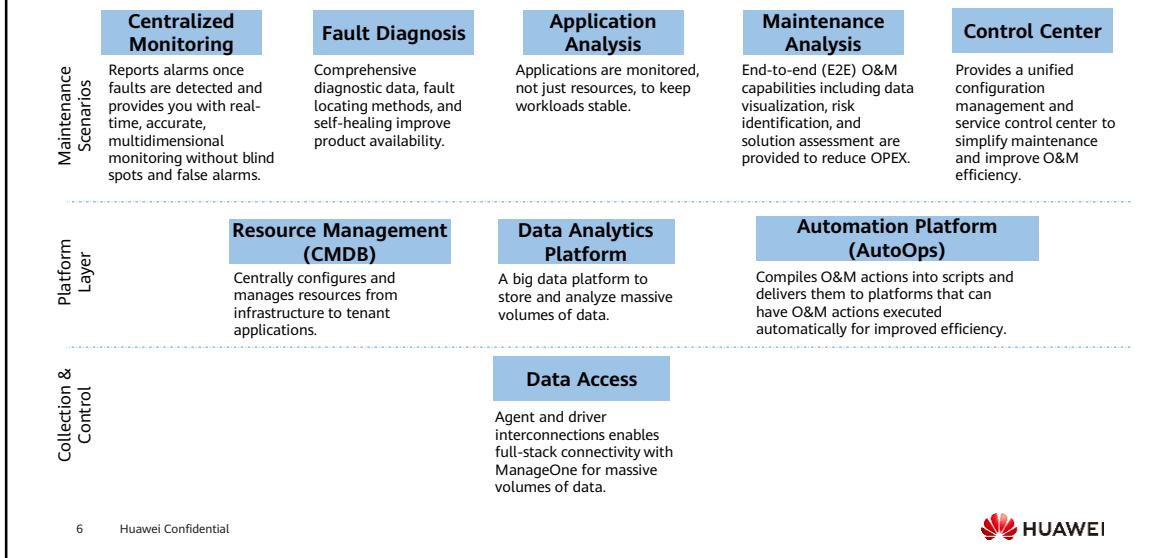


5 Huawei Confidential



- HUAWEI CLOUD Stack resources are managed by ManageOne OperationCenter, which is divided into the collection and control layer, platform layer, and maintenance scenario layer from bottom to top.
- Maintenance Portal allows you to centrally monitor physical resources, virtual resources, cloud services as well as applications, and view their topologies, alarms, logs, capacity data, and performance data. Maintenance Portal helps you centrally manage cloud and non-cloud resources, identify system vulnerabilities, quickly locate faults, and recover key services. ManageOne dashboards, reports, and automation are provided for you to achieve visual and automated maintenance.

Maintenance Functions



6 Huawei Confidential



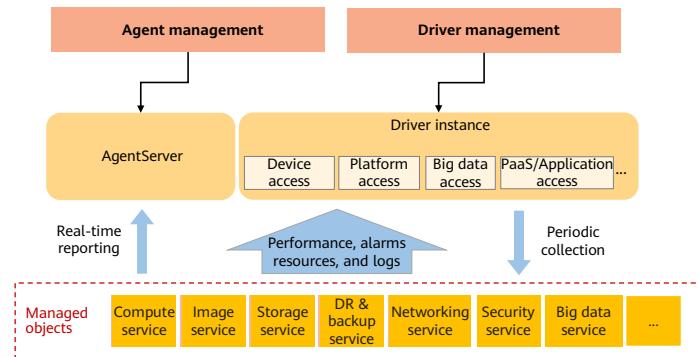
- HUAWEI CLOUD Stack resources are managed by ManageOne OperationCenter, which is divided into the collection and control layer, platform layer, and maintenance scenario layer from bottom to top.
- Based on the hierarchical decoupling architecture, ManageOne OperationCenter is classified into the following parts:
 - Collection & Control: Agent and driver interconnections enables full-stack connectivity with ManageOne for massive volumes of data.
 - Platform layer: The CMDB, data analytics platform, and automated O&M platform form the O&M foundation. The three platforms accumulate O&M data and provide open O&M capabilities.
 - Maintenance scenarios: Focusing on customer values and business scenarios, ManageOne builds one-stop, scenario-based maintenance capabilities that cover monitoring, management, and control to match customer maintenance organizations.
 - Open APIs: ManageOne offers standard data access capabilities and provides maintenance data to third parties through northbound APIs.

Contents

1. Maintenance Overview
- 2. Maintenance Functions at the Collection and Control Layer**
3. Maintenance Functions at the Platform Layer
4. Maintenance Functions in Different Scenarios

Maintenance Device Access Management (1)

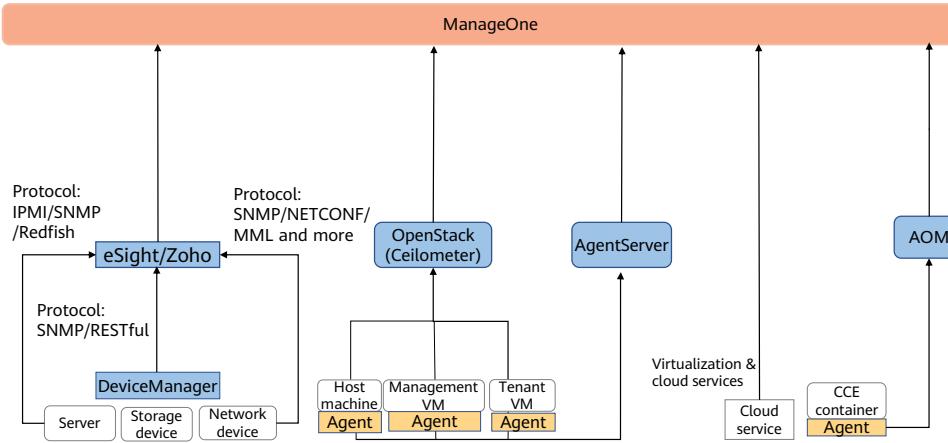
- The data collection and control layer fetches global data through agents and drivers.
 - For general-purpose OSs, data of managed objects is obtained by the agent and is reported to the AgentServer in real time.
 - For third-party systems or embedded systems, drivers are used for their connections. Data of managed objects is periodically collected by driver instances.



- Full-stack data access: Based on the agent and driver interconnection technologies, data of full-stack objects from infrastructure to tenant applications can be collected at a low cost.
- Agents are used to access NEs running general-purpose OSs. This is a reliable, secure, and flexible way to deliver upstream and downstream maintenance capabilities. Drivers are used to access third-party, embedded, and legacy systems. In this way, ManageOne can manage objects of these systems without intruding into their systems.

Maintenance Device Access Management (2)

- The relationships are as follows:



9 Huawei Confidential



- The data collection and control layer provides the following core capabilities:
 - Hardware monitoring metrics: ManageOne connects to eSight or Zoho to obtain hardware-related alarms and metrics.
 - Virtualization channel: ManageOne obtains metrics of host machines and VMs through FusionSphere OpenStack Ceilometer.
 - Agent channel: An agent is deployed on the host OS to collect data.
 - Open APIs: ManageOne provides APIs for cloud services to proactively report monitoring data.
 - AOM channel: ManageOne interconnects with AOM to synchronize monitoring data of containers.

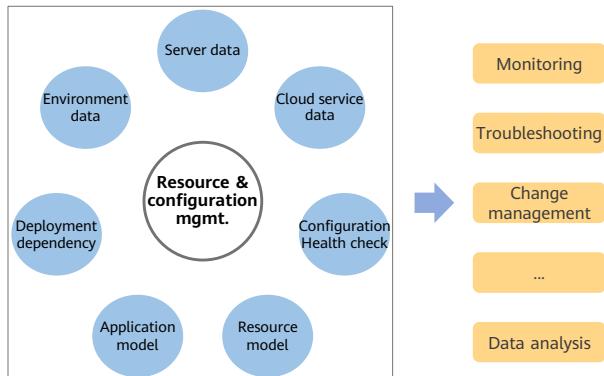
- API description:
 - Hardware monitoring metrics: ManageOne obtains performance data files through the SFTP channel provided by eSight.
 - VM out-of-band performance metrics (OS agent not required): FusionSphere OpenStack Ceilometer collects related metrics through virtualization resource management (VRM) and then reports these metrics to ManageOne.
 - VM in-band (OS) performance metrics and call chain logs: The agent deployed on the host machine and management VM collects and reports related performance metrics and call chain logs. (Note: Only call chain logs are collected. Run logs are not collected in real time.)
 - Cloud service tenant instance metrics: Cloud services report tenant instance performance metrics to ManageOne through the RESTful API. (Tenant instances refer to the instance objects, such as EIP, RDS, and ECS, provisioned to tenants.)
 - Cloud service tenant audit logs: Cloud services report tenant audit logs to ManageOne through the RESTful API.
 - CCE container metrics: AOM collects the metrics through an agent and then reports them to ManageOne.

Contents

1. Maintenance Overview
2. Maintenance Functions at the Collection and Control Layer
- 3. Maintenance Functions at the Platform Layer**
 - Resource Management (CMDB)
 - Data Analytics Platform
 - Automation Platform (AutoOps)
4. Maintenance Functions in Different Scenarios

What Is CMDB?

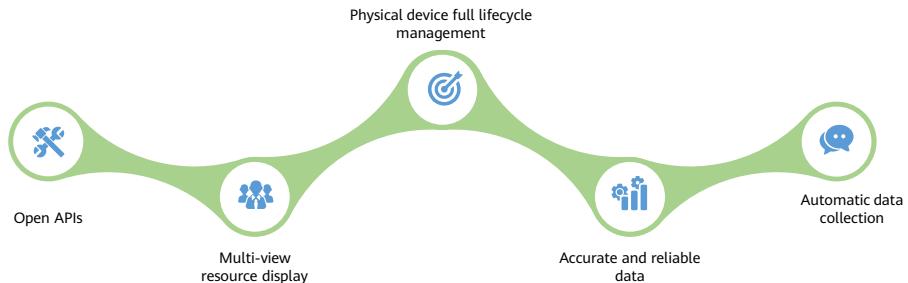
- Configuration Management Database (CMDB) is used to store and manage massive amounts of data related to devices and systems in an enterprise's IT architecture. It ensures data accuracy, timeliness, and effectiveness based on relevant processes, and it provides an organized view of configuration data and sharing information. CMDB helps maximize the value of configuration data.



- During the current Data Center (DC) O&M, the following problems exist in asset management and control: independent data management of each department, scattered data, manual maintenance, and lack of an effective review mechanism. A CMDB can solve these problems to some extent.
- A CMDB is short for configuration management database. Specifically, a CMDB can automatically discover and store data in the entire IT system, for example, the number of servers and storage devices in the entire IT system, device brand, asset code, maintenance personnel, department, OS running on the server, OS version, applications running on the OS, and application version. Moreover, a CMDB can store relationships between different resources and provide a centralized view of IT systems.
- In HUAWEI CLOUD Stack, CMDB, as the cornerstone and data bus of O&M, builds a globally unified resource model, unifies siloed data, and efficiently integrates scattered tools to build an automated O&M system throughout the entire process.
- In HUAWEI CLOUD Stack, the core capabilities of CMDBs include: resource full lifecycle management, including data production, reconciliation, and verification as well as synchronization with O&M tools. All O&M functions (including monitoring, change, troubleshooting, and data analysis) are developed based on CMDBs.

CMDB Benefits

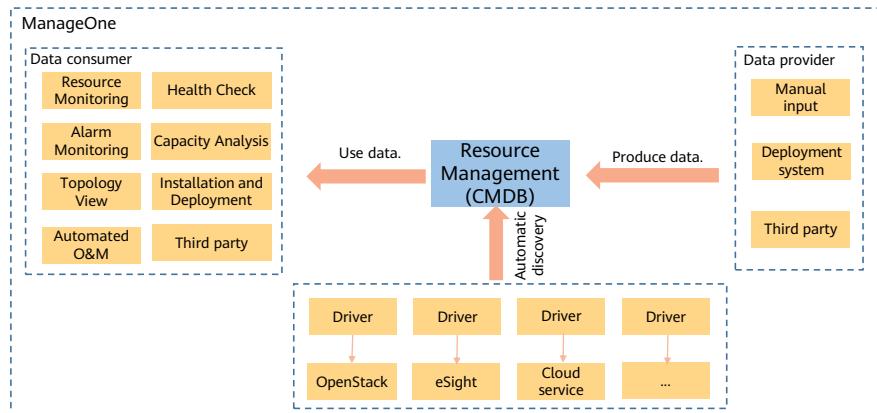
- A CMDB automatically discovers objects and collects data and uses related rules to ensure the accuracy and reliability of that data. It helps you centrally manage resource data collected from multiple sources, gives you a comprehensive overview of the data and helps you maintain resources. It improves O&M efficiency.



- **Open APIs:** A CMDB provides a variety of APIs for you to flexibly query resource data and manage resource instances.
- **Multi-view resource display:** You can view the resource list and resource data in the dimensions of all resources, resource pools, DCs, and VDCs.
- **Full-lifecycle management of physical devices:** Devices can be directly connected to ManageOne, simplifying the way to manage devices. eSight is associated with ManageOne to realize device full-process management, including device adding, monitoring, maintenance, and removal, allowing you to gradually build the lifecycle management capability of physical devices.
- **Accurate and reliable data:** Resource Management standardizes data collected from multiple sources so that the data can be maintained in a simple, unified way to improve the accuracy of resource configuration. In addition, only the data that meets preset rules and is from trusted sources can be collected to avoid data conflicts and improve data accuracy.
- **Automatic data collection:** A CMDB works with other tools to automatically discover objects and collect data, reducing manual workloads, improving data collection efficiency, reducing O&M risks caused by manual misoperations, and ensuring data timeliness and effectiveness.

Implementation Logic of CMDB

- Resource Management obtains data about system and tenant resources using System Access and manages those resources using a unified model. It also provides data for resource monitoring and automated O&M.



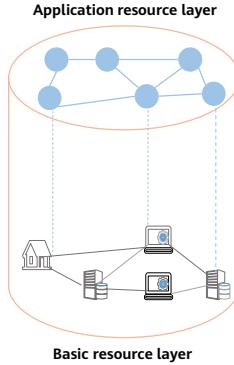
14 Huawei Confidential



- Resource Management obtains data from deployment systems and third-party systems, or manually entered by O&M administrators.
- Resource Management also obtains data of system resources and tenant resources from interconnected systems.
- Resource Management provides data sources for O&M services.
 - Resource Management provides data of monitored objects for Resource Monitoring, helping O&M personnel obtain the running status of resources in a timely manner.
 - Resource Management provides data of objects to be checked for Health Check.
 - Resource Management provides a fault root cause tree for Alarm Monitoring, helping administrators quickly locate and rectify faults.
 - Resource Management provides data such as capacity usage and thresholds for Capacity Analysis, helping O&M personnel predict and analyze capacity.
 - Resource Management provides relationships between resources for Topology View, helping O&M personnel quickly and intuitively locate faults.
 - Resource Management provides data for installation and deployment.
 - Resource Management provides data for Automated O&M, allowing for operation execution in one click and improving O&M efficiency and satisfaction.
 - Resource Management provides data for third-party systems through northbound APIs (NBIs).

CMDB Models and Functions

- A CMDB model consists of a basic resource layer and an application resource layer. Resources at the application layer are integrated based on applications to build a complete profile of a DC.
- A CMDB can clarify the relationships between application resources and basic resources for subsequent service analysis and troubleshooting.

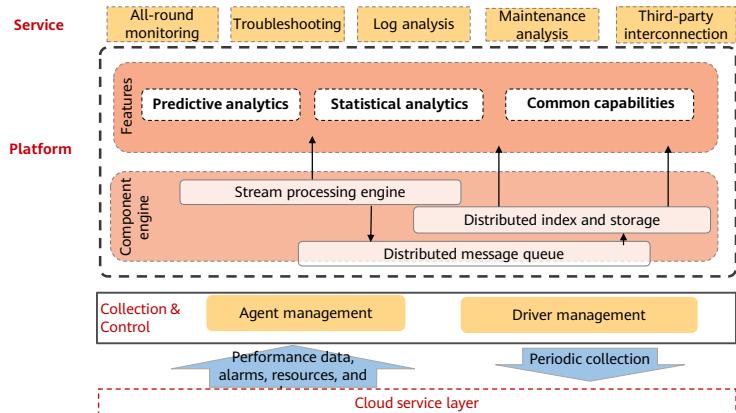


Contents

1. Maintenance Overview
2. Maintenance Functions at the Collection and Control Layer
- 3. Maintenance Functions at the Platform Layer**
 - Resource Management (CMDB)
 - **Data Analytics Platform**
 - Automation Platform (AutoOps)
4. Maintenance Functions in Different Scenarios

What Is Data Analytics Platform?

- The data analytics platform provides comprehensive data analysis capabilities based on big data technologies such as distributed message queues (DMQs), distributed index/storage, and stream processing engines.

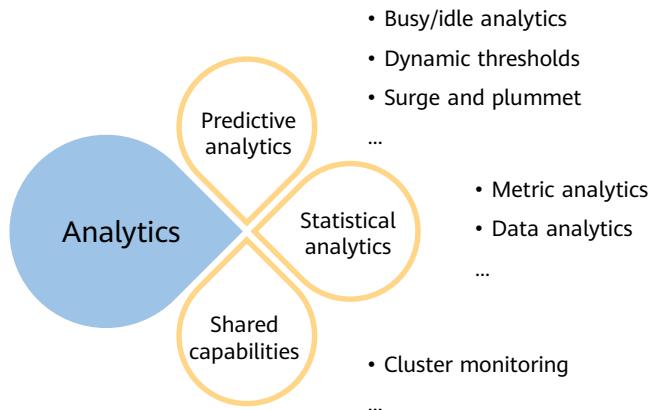


17 Huawei Confidential



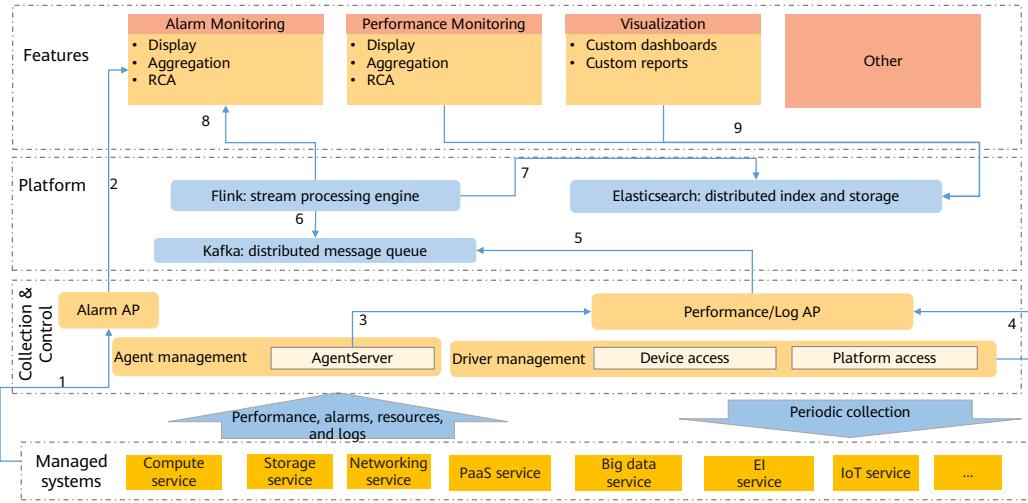
- Digital transformation of enterprises has seen the surging value of data. The ManageOne data analytics platform uses big data technologies to preset unified O&M models (data sets) and related algorithms to develop O&M data asset capabilities. With the data analytics platform, O&M services such as all-round monitoring, call chain-based fault analysis, log analysis, capacity analysis, reports/dashboards, and idle resource analysis are developed.
- Workload: High-value services are created based on the data platform.
- Platform: Based on the big data technology, enhanced features, such as metric data search, aggregation, and association, Top Percentile (TP), exception detection, stream processing, trend prediction, dynamic threshold, and multidimensional detection, are supported. O&M data is gradually aggregated as needed.
- Access: Standard southbound data access specifications and APIs are provided.

Data Analytics Capabilities



- Based on big data technologies, the data analytics platform develops predictive analytics, statistical analytics, and common capabilities. It includes the following functions:
 - Busy/idle analytics: analyzes the busy/idle status of each service to provide reference for O&M personnel.
 - Dynamic threshold: A dynamic threshold can prevent heavy workloads of static threshold configurations and reduce the number of false negatives and false positives.
 - Sharp increase and decrease: For traditional fixed, static thresholds, the system may fail to report alarms when the service volume increases or decreases sharply but does not reach the threshold. After the sensitivity is set for a dynamic threshold, the system can automatically identify services that increase or decrease sharply and report alarms to reduce the probability of false negatives.
 - Statistical analytics: The data analytics platform analyzes system and metrics data collected by the collection and control layer, and displays the data based on different rules, for example, the total number of current alarms, CPU usage, and top 5 physical devices by disk usage.
 - Cluster monitoring: The cluster running status can be monitored.

Key Data Flows of the Data Analytics Platform



- The core process of the data analytics platform is as follows:
 - External systems report alarms over REST or SNMP.
 - Alarms are processed (resource data added) and reported to the alarm module.
 - Performance and metric data collected by an agent is sent to the performance or metric AP.
 - Metric data of cloud services is reported through drivers (conversion) or APIs opened by the performance AP.
 - Preprocessed data (structured logs) is reported to Kafka.
 - Flink consumes data obtained from Kafka for streaming computing.
 - Preprocessed metric data (aggregation calculation/dimension adding) is reported to Elasticsearch.
 - Threshold alarms are reported to the alarm module.
 - The upper-layer service module queries data in Elasticsearch.

- Agent management: Agents and data channels on hosts where agents can be deployed are managed.
- Driver management: In scenarios where external system APIs need to be called, drivers can be used to call APIs and convert formats and protocols.
- Alarm AP: adds alarm data (resource related).
- Kafka: Metrics reported by external systems and structured logs are sent to the message middleware first.
- Flink: pre-processes metrics (dimensions added), calculates thresholds, and performs aggregation calculation.
- Elasticsearch: stores raw and aggregation metrics for upper-layer applications to query. The aggregation capability of Elasticsearch is used during the query.
- Alarm monitoring: Alarms are stored in the alarm monitoring module, which provides capabilities such as alarm display, aggregation, toggling/intermittent disconnection, masking, notification, and RCA.
- Performance monitoring: provides functions such as metrics visualization and monitoring configuration.
- Visualization: Data queried from Elasticsearch is visualized to custom reports and dashboards.

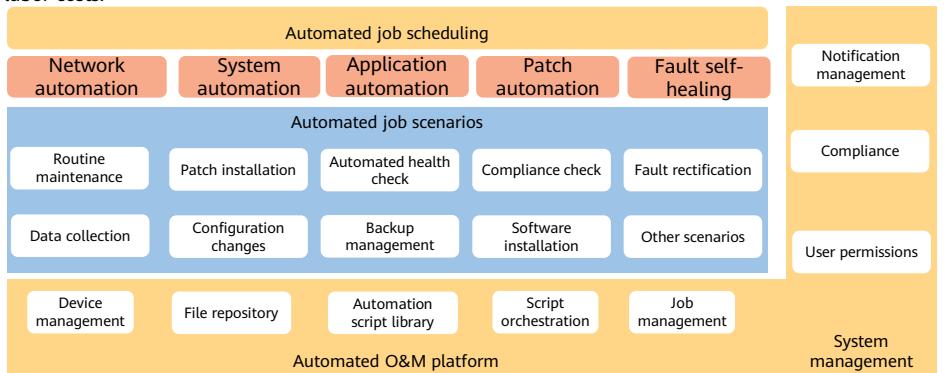
- Other: capacity management, resource analysis, and NBI management

Contents

1. Maintenance Overview
2. Maintenance Functions at the Collection and Control Layer
- 3. Maintenance Functions at the Platform Layer**
 - Resource Management (CMDB)
 - Data Analytics Platform
 - **Automation Platform (AutoOps)**
4. Maintenance Functions in Different Scenarios

What Is AutoOps?

- AutoOps provides agile and automated full-stack O&M automation capabilities from infrastructure to applications. AutoOps gives you an O&M operation library that you can use to flexibly orchestrate O&M processes and standardize O&M scenarios. It supports scheduled and immediate execution of O&M tasks in batches and can expand to meet growing business demands. By deploying AutoOps, you can improve efficiency and reduce your labor costs.



Basic Concepts of AutoOps (1)



Device management

- The list of devices to be maintained is obtained from the CMDB and the agent is deployed on the devices online or offline. A maintenance channel is established between devices in the management system.



Operation management

- A single atomic O&M script is encapsulated into a specific O&M operation to be executed. The system provides preset operation libraries for a diverse range of preset routine O&M operations, but if they do not suit your needs, you can also create your own custom O&M scripts and then add them to the custom operation library.



Orchestration management

- Atomic operations or sub-orchestration can be orchestrated by a unified workflow engine to flexibly assemble a variety of O&M scenarios.



Scenario management

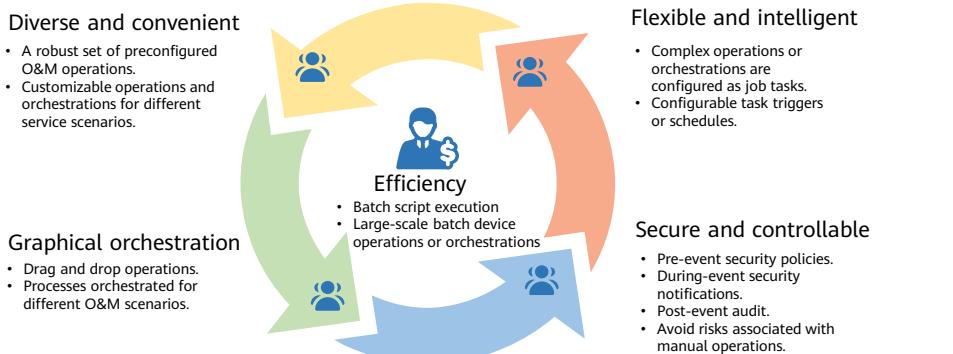
- Orchestrations are classified by scenario so that O&M administrators can search for and execute orchestration processes based on specific scenarios.

Basic Concepts of AutoOps (2)

-  **Job management**
 - You can create jobs for operations or orchestrations, schedule and execute operations or orchestrations on specified devices. Job parameters can be saved and reused. Jobs can be executed immediately, periodically, or once at a scheduled time.
-  **Job history**
 - The execution history of all jobs is recorded to make it easier for you to query execution results or to audit operations. The job history includes the executor, execution time, execution duration, job status, script content, and execution status of each node (script output and execution logs).
-  **Security policy**
 - To control the automated O&M platform, AutoOps provides the security policy function. An administrator can define the time, person, device set, and operations or orchestrations that can be performed. In this way, sensitive operations can be controlled.
-  **Sensitive command**
 - An automated O&M script may contain sensitive commands, which can result in a system breakdown or severe service problems. This function can help O&M personnel scan scripts containing specified sensitive commands, confirm the scripts, and identify the impact of sensitive commands on services.

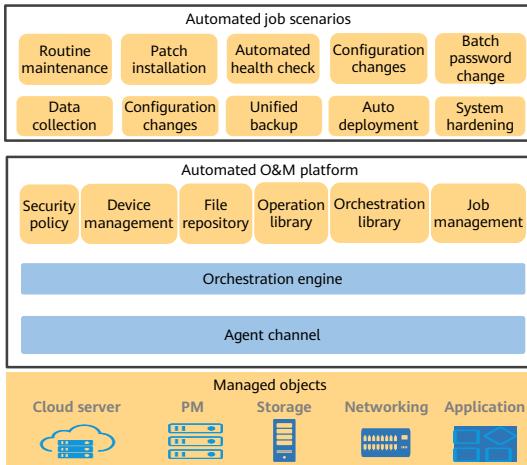
AutoOps Benefits

- AutoOps allows you to execute scripts on resources in batches to simplify routine O&M. O&M operations are orchestrated for different scenarios using the orchestration engine to accommodate different O&M scenarios, like patch installation and periodic health checks, improving O&M efficiency.



- Rich and convenient: ManageOne has a preset O&M operations library to meet daily O&M requirements. Users can also customize operations and orchestrations suitable for their business scenarios.
- Flexible and intelligent: Complex operations or orchestrations are configured into many tasks and can be automatically executed after you set the trigger conditions and time period. For example, for a scheduled health check task, you only need to select devices and set the execution time. The task will be automatically executed.
- Batch and efficient: Script tasks containing operations or orchestrations are executed in batches on a large number of devices.
- Graphical orchestration: Users can use an orchestration engine to orchestrate atomic O&M operations or orchestrations by dragging and dropping them into O&M processes to accommodate diverse O&M scenarios. In this way, O&M operations can be standardized and reused.
- Secure and controllable: AutoOps provides a complete security control mechanism, including pre-event security policy creation, during-event security alarm notification, and post-event auditing, to avoid security risks caused by manual operations.

Implementation Logic of AutoOps

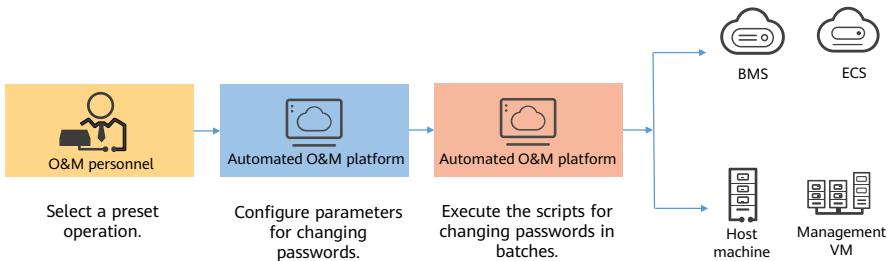


- **Managed objects:** Automated Jobs obtains a list of managed objects from Resource Management (CMDB) and remotely executes scripts through the Agent.
- **Platform capabilities:** Atomic operations can be orchestrated into standard O&M actions using the orchestration engine, and can then be executed based on different policies.
- **O&M scenarios:** Routine O&M operations are designed based on different scenarios.

- AutoOps consists of managed objects, the automated O&M platform, and automated job scenarios.
- Managed objects: Automated Jobs obtains a list of managed objects from Resource Management (CMDB) and remotely executes scripts through the Agent.
- Platform capabilities: Atomic operations can be orchestrated into standard O&M actions using the orchestration engine, and can then be executed based on different policies.
- Automated Jobs provides you with a wide variety of operation scenarios, such as automated health checks, batch password change, and routine maintenance.

AutoOps Application Scenario - Password Change

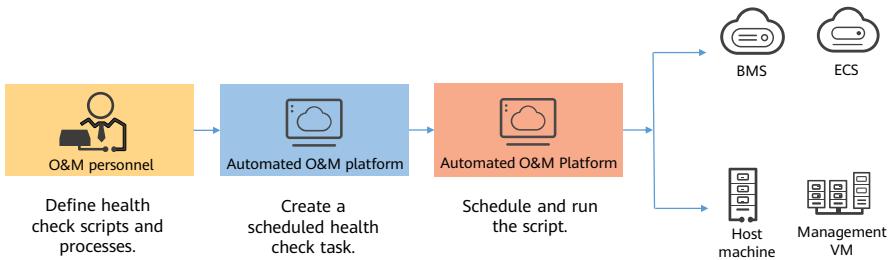
- On the automated O&M platform, you can quickly change passwords of multiple managed objects.



- For security purposes, enterprises need to periodically change system passwords. However, O&M personnel are likely to make mistakes when changing passwords for a large number of VM OSs in a cloud data center one by one. On the automated O&M platform, you can change passwords in batches in one click. This greatly boosts password change efficiency and frees O&M personnel from work burdens.

AutoOps Application Scenario - Scheduled Health Checks

- O&M personnel can create custom health check scripts and processes, configure periodic health checks, and schedule script execution.



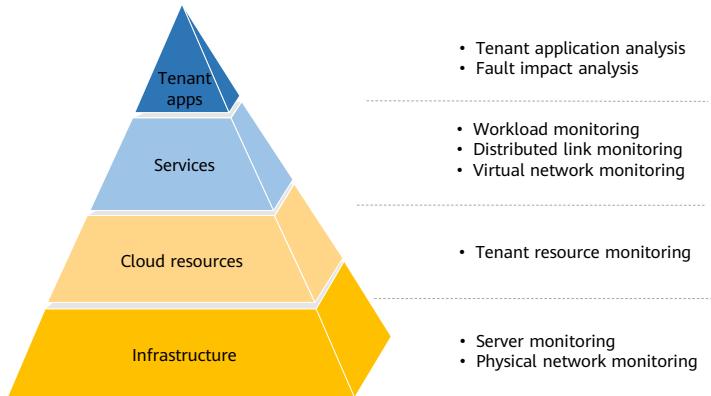
- Customers need to perform system health checks daily or weekly and adjust the health check process on demand. However, manual operations are error-prone and easy to forget, and are complex when massive volumes of devices need to be checked. With the O&M automation platform, customers can flexibly orchestrate the health check process and set scheduled tasks.

Contents

1. Maintenance Overview
 2. Maintenance Functions at the Collection and Control Layer
 3. Maintenance Functions at the Platform Layer
- 4. Maintenance Functions in Different Scenarios**
- Centralized Monitoring
 - Application Analysis
 - Maintenance Analysis
 - Deployment Change
 - Fault Diagnosis

Comprehensive Monitoring

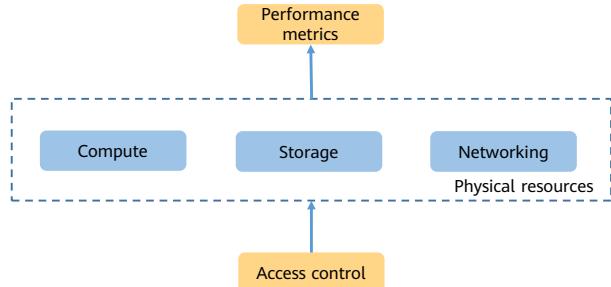
- Comprehensive Monitoring covers the infrastructure, cloud resources, services, and tenant applications.



- ManageOne proactively monitors the running status of cloud data centers, helping enterprises reduce IT costs and improve O&M efficiency.
- All-round Monitoring provides the following functions:
 - Infrastructure, cloud resources, services, and tenant applications are monitored.
 - The agent-based massive metric collection, ultra-large-scale data storage, real-time metric aggregation and calculation, and service call chain analysis are realized.
 - Key objects, such as cloud services, VMs, and containers, are monitored from all aspects.

Physical Resource Monitoring

- Physical Resource Monitoring allows you to see the performance of your compute, networking, and storage resources in real time, along with historical and real-time performance data in graphs. The performance metrics of physical resources are monitored. This feature helps O&M personnel track resource performance in real time, detect risks, provide warnings, locate and analyze problems, make better informed decisions, and provide more robust O&M assurance.



Physical Resource Monitoring

- This feature includes central monitoring and management of alarms, topologies, and performance data of hardware devices such as data center servers, storage devices, and network devices, so you can quickly locate and rectify hardware faults.

Monitoring details of a physical resource

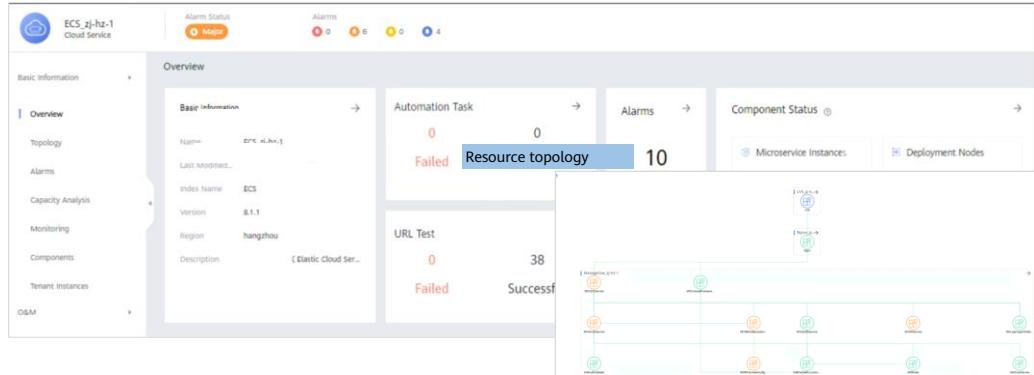
The screenshot displays the monitoring details for a physical resource named 'eBackup Server01'. The interface is divided into several sections:

- Basic Information:** Shows the server's name, running status (Unknown), and various identifiers like BMC IP Address and Model.
- Summary:** A central panel showing basic information, alarms, and component status.
- Alarms:** A section showing 0 total alarms, categorized by severity: Critical (0), Major (0), Minor (0), and Warning (0).
- Component Status:** A grid showing the status of Mainboard, CPU, Memory, Hard Disk, Power Supply, and Fan components across Normal, Faulty, and Total categories.

Cloud Resource Monitoring

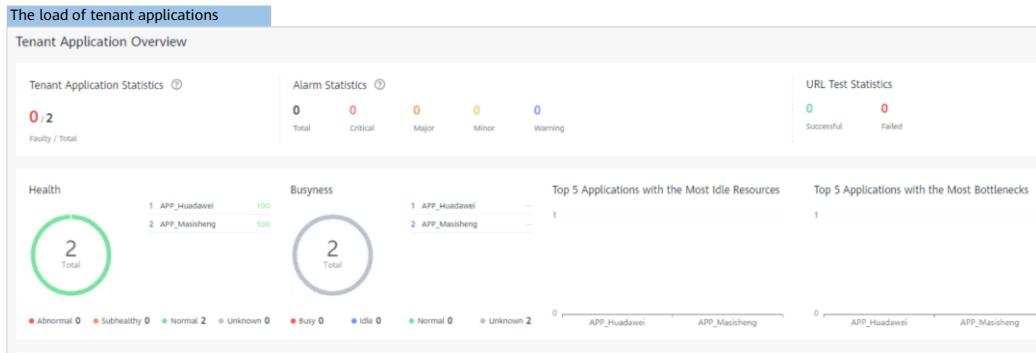
- Cloud Resource Monitoring allows you to view automation tasks, alarms, and component running status, and collect statistics on key metrics, such as CPU usage, memory usage, and disk usage.

Monitoring details of a cloud resource

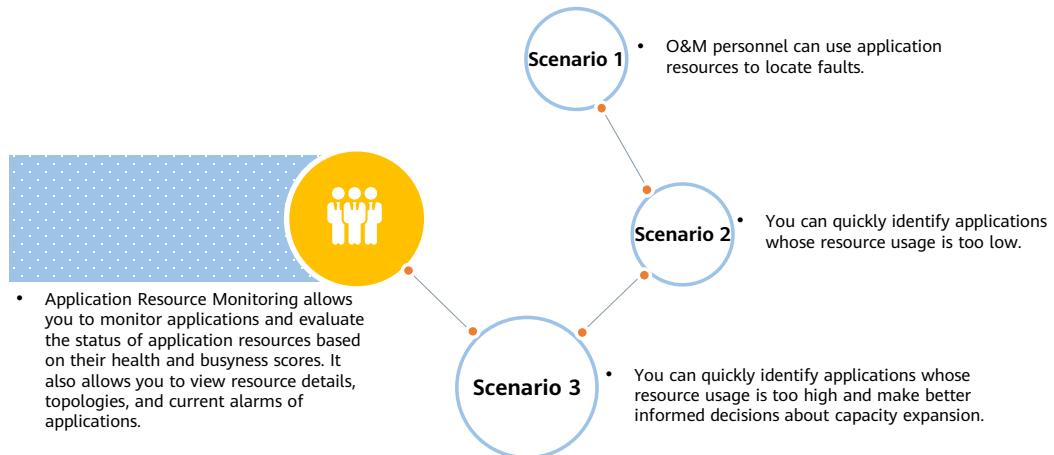


Application Resource Monitoring

- Application Resource Monitoring allows you to monitor resources from the perspective of the applications. This feature continuously evaluates the resource usage of each application in terms of their capacity and load, and provides comprehensive assurance for key workloads.



Application Resource Monitoring



- Scenario 1: When O&M personnel detect an application fault from alarm notifications or routine health checks, they can use application resources to demarcate the fault, quickly determine whether the fault occurs at the virtualization layer, server layer, or network layer, specify the owner, and rectify the fault as soon as possible.
- Scenario 2: O&M personnel can evaluate resource busyness of each application to quickly identify applications with low resource usage. Meanwhile, O&M personnel can also evaluate resource usage at the virtualization layer, server layer, and network layer.
- Scenario 3: O&M personnel can view the resource usage of each application in real time to detect and prevent service interruption or faults caused by insufficient resources. Moreover, O&M personnel can quickly determine what performance metrics of what resources at which layer among the virtualization layer, server layer, and network layer has high resource utilization, providing data support for customers' capacity expansion decisions.

Monitoring Configuration - Performance Monitoring Task Management

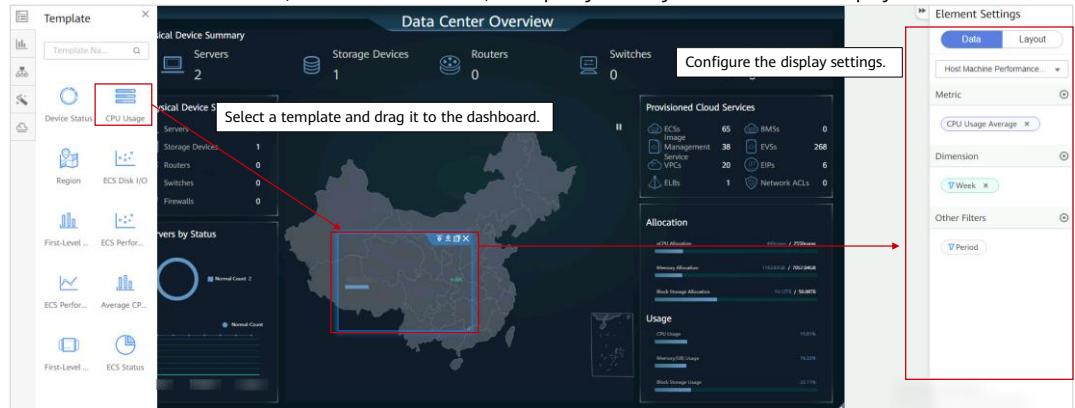
- You can view performance monitoring tasks. You can also add resources to be collected, specify collection metrics and collection periods as required to customize a monitoring task.

Default monitoring task overview, including the monitoring scope, metrics, and collection task status.

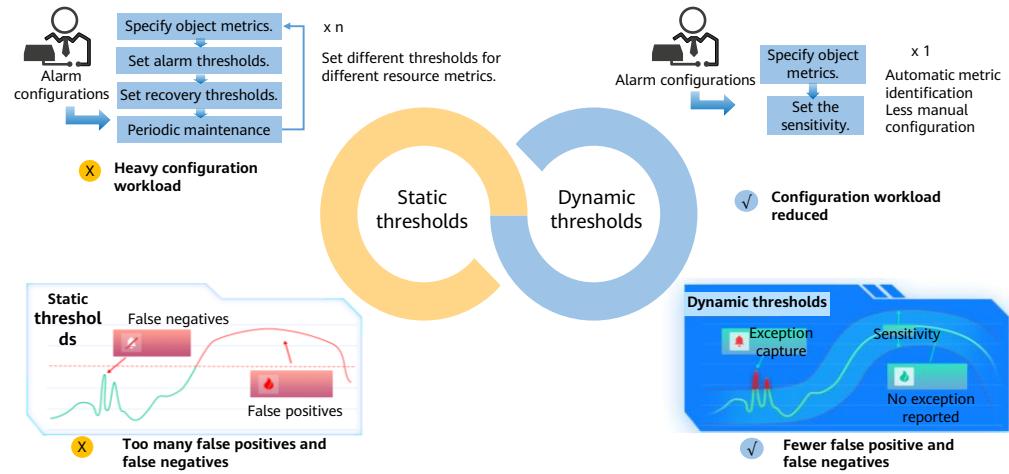
The screenshot shows the 'Performance Monitoring Task Management' interface. On the left, there's a sidebar with options like 'Monitoring Config...', 'Performance Monitoring ...', 'Performance Threshold ...', 'Agent Management', 'Monitoring Tasks', 'Application Scoring System', and 'Cloud Service Configuration'. The main area has tabs for 'Default Monitoring' and 'Custom Monitoring', with 'Default Monitoring' selected. Below this is a table titled 'Operation Records' showing three entries: 'Power Supply-G3 psu-D...', 'Elastic Load Balancing-I...', and 'Port-eSight Storage-Def...'. To the right, a large window is open for 'Create Monitoring Task'. It has sections for 'Basic Information' (Task Name: 'test'), 'Task Configuration' (Resource Type: 'Network Resource-Interface', Resource Subtype: 'eSight'), and 'Select Objects' (with radio buttons for 'Select all objects', 'Select objects by scope', and 'Select by object'). A note at the bottom says 'Ensure that a performance monitoring task has been created on eSight and its status is Started.' There are also 'Start' and 'Stop' buttons for each task entry.

Dashboard Monitoring

- A dashboard shows you monitoring details in a way that lets you intuitively and conveniently monitor the system in real time.
- You can create a dashboard, customize its content, and specify the way the dashboard is displayed.



Monitoring Configuration - Dynamic Thresholds



38 Huawei Confidential



- Conventional static thresholds have the following problems: It is time-consuming to manually set different thresholds for resource metrics. When service volumes surge but metrics do not reach the thresholds, exceptions may not be reported. When service volumes are stable but metrics exceed the thresholds, alarms are falsely reported.
- Exception detection: The Gaussian Mixture Model (GMM) is used to detect exceptions. For metrics that are difficult to predict and change irregularly, the abnormal outlier detection method is used.
- Metric prediction: The LSTM, XGBoost, and EWMA algorithms are used to predict specific metrics and show strong periodic changes to fit metric curves.
- Error detection: The boxplot method is used to detect the prediction error of metrics.

Alarm Monitoring - Viewing Current, Historical, and Masked Alarms

- You can view current, historical, and masked alarms and display alarms by source, severity, and time of occurrence.

Current and historical alarms of the system

Default template | Filter | 11 21 32 19

Auto Refresh | Quick Filter

Combo Sorting | Export | Comment | Clear | Acknowledge | ...

Operation	Alarm Serial Nu...	Severity	Name	Alarm Source	Last Occurred	Region	Type	Cleared On	Possible Causes	Other Information
<input type="checkbox"/>	24964777	Warning	Incoming Network Dropped	elbv3_cvs_vm...	Cloud...	GuAn	Integrity alarm		Nic=brcps, I	
<input type="checkbox"/>	24964756	Warning	Incoming Network Dropped	elbv3_nginx_vm...	Cloud...	GuAn	Integrity alarm		Nic=brcps, I	
<input type="checkbox"/>	24964426	Major	Incorrect Metering SDRs	ManageOne-Ser...	Cloud...		Processing error		ErrorSDR=[{"err...	CloudService
<input type="checkbox"/>	24959765	Major	Incorrect Metering SDRs	ManageOne-Ser...	Cloud...		Processing error		ErrorSDR=[{"err...	CloudService
<input type="checkbox"/>	24964233	Major	CPU Usage Threshold Alarm	br_vm_az0_dc0...	Cloud...	GuAn	Integrity alarm		Monitor Unit	
<input type="checkbox"/>	24964180	Major	Physical Memory Used Rate	ManageOne-Ser...	Cloud...	GuAn	Integrity alarm		Monitor Unit	
<input type="checkbox"/>	24953536	Warning	Incoming Network Dropped	122B388E-2A8C...	Cloud...	GuAn	Integrity alarm		Nic=brcps, N	
<input type="checkbox"/>	24963498	Warning	Incoming Network Dropped	br_vm_az0_dc0...	Cloud...	GuAn	Integrity alarm		Nic=brcps, N	
<input type="checkbox"/>	24958346	Warning	Incoming Network Dropped	vrouter_vm_az0...	Cloud...	GuAn	Integrity alarm		Nic=brcps, N	
<input type="checkbox"/>	24962401	Major	CPU Usage Threshold Alarm	br_vm_az0_dc0...	Cloud...	GuAn	Integrity alarm		Monitor Unit	
<input type="checkbox"/>	24948081	Major	GaussdbHA_upload_to_rem	SMN_DB_SMNA...	Cloud...	GuAn	Integrity alarm		Monitor Unit	
<input type="checkbox"/>	24939942	Warning	Incoming Network Dropped	vrouter_vm_az0...	Cloud...	GuAn	Integrity alarm		Nic=brcps, N	
<input type="checkbox"/>	24939319	Warning	Outgoing Network Dropped	elbv3_nginx_vm...	Cloud...	GuAn	Integrity alarm		Nic=listen_17	
<input type="checkbox"/>	24937966	Warning	Incoming Network Dropped	8134388E-2A8C...	Cloud...	GuAn	Integrity alarm		Nic=brcps, N	
<input type="checkbox"/>	24942515	Warning	Incoming Network Dropped	br_vm_az0_dc0...	Cloud...	GuAn	Integrity alarm		Nic=brcps, N	
<input type="checkbox"/>	24937366	Warning	Outgoing Network Dropped	elbv3_nginx_vm...	Cloud...	GuAn	Integrity alarm		Nic=v049361	

Alarm Monitoring - Alarm Handling

- O&M personnel can handle alarms themselves or specify alarm handlers.

Manually handling alarms										
Default template		Filter								
<input checked="" type="checkbox"/> Auto Refresh		<input type="checkbox"/> Quick Filter		Combo Sorting			Export		Comment	
Operation	Alarm Serial No.	Severity	Name	Alarm Source	L...	Last Occurred	Region	Type	Cleared On	Priority
<input checked="" type="checkbox"/>	24964777	Warning	Incoming Network Dropped	elbv3_cvx_vmx_...	Cloud	GuAn	Integrity alarm	Myself	Specify Handler	Nic=brcps, h
<input checked="" type="checkbox"/>	24964756	Warning	Incoming Network Dropped	elbv3_nginx_vmx_...	Cloud	GuAn	Integrity alarm	Other Users	Change Severity	Nic=brcps, h
<input checked="" type="checkbox"/>	24964426	Major	Incorrect Metering SDRs	ManageOne-Ser...	Cloud	GuAn	Processing error	...	Set as Invalid	Nic=brcps, h
<input checked="" type="checkbox"/>	24959765	Major	Incorrect Metering SDRs	ManageOne-Ser...	Cloud	GuAn	Processing error	...	Set as Valid	Nic=brcps, h
<input checked="" type="checkbox"/>	24964233	Major	CPU Usage Threshold Alarm	br_vmx_az0_dc0...	Cloud	GuAn	Integrity alarm	...	Set as Under Maintenance	Nic=brcps, h
<input checked="" type="checkbox"/>	24964180	Major	Physical Memory Usage Rate	ManageOne-Ser...	Cloud	GuAn	Integrity alarm	...	Set as Normal	Nic=brcps, h
<input checked="" type="checkbox"/>	24963536	Warning	Incoming Network Dropped	1228388E-2ABC...	Cloud	GuAn	Integrity alarm	...	Send Email Notification	Nic=brcps, h
<input checked="" type="checkbox"/>	24963498	Warning	Incoming Network Dropped	br_vmx_az0_dc0...	Cloud	GuAn	Integrity alarm	...	Send SMS Message Notification	Nic=brcps, h
<input checked="" type="checkbox"/>	24958346	Warning	Incoming Network Dropped	routervm_az0_az0...	Cloud	GuAn	Integrity alarm	...		
<input checked="" type="checkbox"/>	24948081	Major	GaussDB10A_upload_to_ren...	SMN_DB_SMNA...	Cloud	GuAn	Integrity alarm	...		
<input checked="" type="checkbox"/>	24939942	Warning	Incoming Network Dropped	routervm_az0_az0...	Cloud	GuAn	Integrity alarm	...		
<input checked="" type="checkbox"/>	24939319	Warning	Outgoing Network Dropped	elbv3_cvx_vmx_...	Cloud	GuAn	Integrity alarm	...		
<input checked="" type="checkbox"/>	24937966	Warning	Incoming Network Dropped	8134388E-2ABC...	Cloud	GuAn	Integrity alarm	...		
<input checked="" type="checkbox"/>	24942515	Warning	Incoming Network Dropped	br_vmx_az0_dc0...	Cloud	GuAn	Integrity alarm	...		
<input checked="" type="checkbox"/>	24937366	Warning	Outgoing Network Dropped	elbv3_nginx_vmx_...	Cloud	GuAn	Integrity alarm	...		
<input checked="" type="checkbox"/>	24937252	Warning	Incoming Network Dropped	4A2B288E-2ABC...	Cloud	GuAn	Integrity alarm	...		

Alarm Monitoring - Alarm Extension

- You can register, import, export, or dump alarm information for future query and analysis. CloudMonitorAlarm alarm information can also be synchronized to Maintenance Portal.

The image displays three screenshots of the Alarm Extension interface:

- Export alarm information.**: Shows a dialog for importing alarm information from an Excel file. It includes fields for "Download Template" and "Import File".
- Synchronize CMA alarms.**: Shows a dialog for synchronizing CloudMonitorAlarm (CMA) alarms. A note states: "CloudMonitorAlarm (CMA) alarms can only be manually synchronized. The next alarm synchronization can be performed 10 minutes later." It includes a "Synchronize CMA Alarms" button.
- Dump alarm information.**: Shows a task progress dialog for a "Manual Alarm/Event Dump". The progress bar is at 100% and labeled "Successful". Task details include:

Task Name	Progress	Status	Execution Type	Task Type	Task Category
Manual Alarm/Event Dump	100%	Successful	One-time	Manual Alarm/Event Dump	System task
				Start Time	
				End Time	

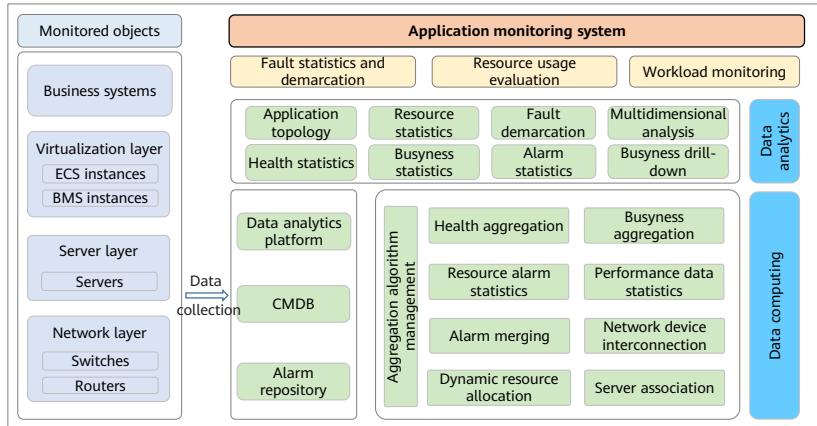
A "Dump" button is located in the bottom right corner.

Contents

1. Maintenance Overview
 2. Maintenance Functions at the Collection and Control Layer
 3. Maintenance Functions at the Platform Layer
- 4. Maintenance Functions in Different Scenarios**
- Centralized Monitoring
 - **Application Analysis**
 - Maintenance Analysis
 - Deployment Change
 - Troubleshooting

Application Analysis

- **Positioning and value:** Applications, not just resources, are monitored to keep workloads stable.



43 Huawei Confidential



- The health status of resources can be monitored for service needs. Quantitative assessment, KPI exception detection, and assistance in fault demarcation and locating can be used to shorten the Mean Time to Repair (MTTR) and improve service continuity. Applications, not just resources, are monitored to keep workloads stable.
- Application Analysis provides the following functions:
 - Comprehensively evaluates the status of application resources at the virtualization, server, and network layers.
 - Monitors application resources, supports application fault statistics and demarcation, and assesses application resource utilization.
- Application scenarios:
 - When administrators receive an alarm notification or a fault from a user, or an application fault is detected during routine health checks, you can use the fault demarcation capability to quickly locate and demarcate the fault and rectify the fault as soon as possible.
 - When evaluating resource utilization by application, O&M personnel can leverage the busyness evaluation capability of Application Resource Monitoring to quickly identify applications that are not fully used. In addition, they can also assess resource utilization at the virtualization layer, server layer, and network layer to quickly obtain the evaluation result.
 - Real-time monitoring of resource utilization helps O&M personnel detect and avoid service interruption or faults caused by insufficient resources in a timely manner. O&M personnel can also quickly identify the resources with high utilization at the virtualization layer, server layer, and network layer and make better decisions on capacity expansion.

Application Analysis: Health Evaluation

- Quantitative evaluation of application health and busyness.

Application List						
Application Name	Health	Business	Application Level	Project	User	Alarms
APP_Huawei	100	--	Common	zl-Az-1, Ren_Huawei	--	0
APP_Masheng	100	--	Common	zl-Az-1, Ren_Masheng	--	0

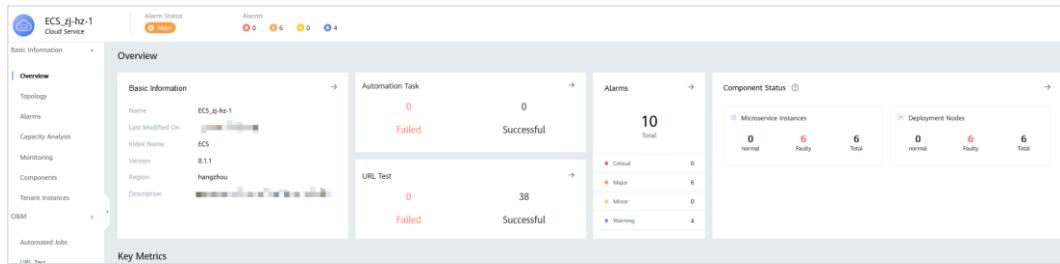
44 Huawei Confidential



- Application Analysis provides the following functions:
 - Application health and busyness can be quantitatively evaluated.
 - Basic information, performance data, alarms, and topologies of each resource can be displayed on one page.
 - An application topology shows you resource allocation and association at different layers. It also shows resource health, busyness, alarms, and performance data so you can demarcate faults faster.

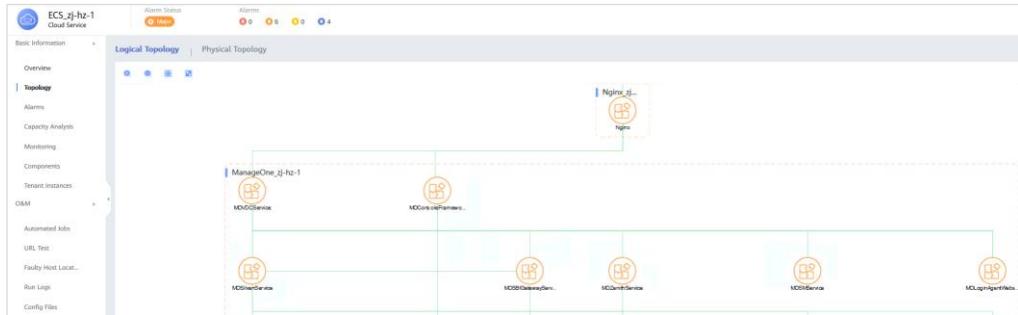
Application Analysis: Aggregation Analysis

- Basic information, performance data, alarms, and topologies of each resource can be displayed on one page.



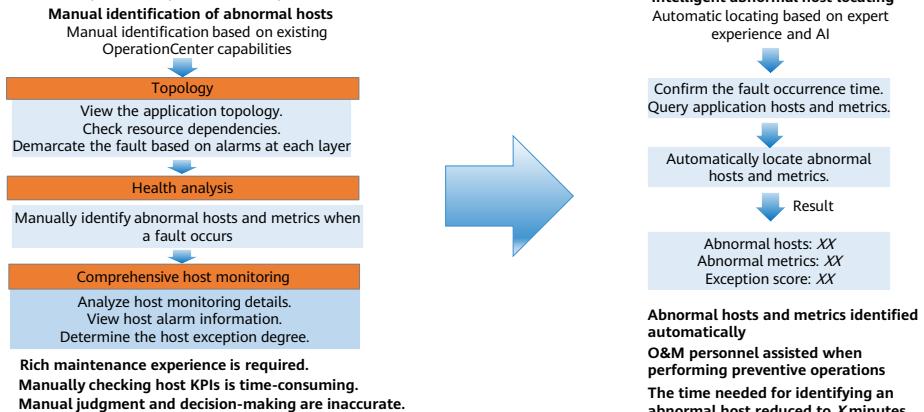
Application Analysis: Associated Topology

- An application topology shows you resource allocation and association at different layers. It also shows resource health, busyness, alarms, and performance data so you can demarcate faults faster.



Application Analysis: Intelligent Identification of Abnormal Hosts

- Positioning and value: Abnormal hosts and metrics can be identified automatically. Guidance is provided for O&M personnel to perform preventive operations, and shorten the MTTR.



47 Huawei Confidential

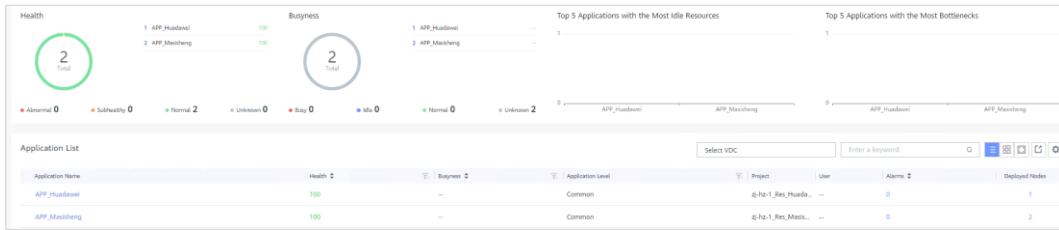


- Core capabilities:**

- Abnormal hosts and metrics can be automatically located.
- Clustering abnormal hosts helps improve the explainability of location results.
- Abnormal hosts are sorted to help O&M personnel perform required workarounds.

Application Scoring System Management

- Applications are analyzed based on health and busyness calculations which are preconfigured on ManageOne. Alternatively, the two calculation methods can also be configured by administrators for different applications, layers, and nodes as required.



- Note: Modifying parameters in a calculation method affects overall application health and busyness. Exercise caution when performing this operation.

Busyness Score Calculation

- The busyness threshold is configured when ManageOne manages application resources.

Calculation Method and Parameters

Busyness Threshold	[0,20]	Idle	[20,90]	Normal	[90,100]	Busy
--------------------	----------	------	-----------	--------	------------	------

① Node Busyness Score

- Node busyness score = $\sum(\text{Each indicator value of the node} \times \text{Weight of each indicator}) / \text{Total weight} \times 100$
- Weight of each indicator: If an indicator value is within the range of [0, 30%), the weight is 1; If an indicator value is within the range of [30%, 90%), the weight is 3; If an indicator value is within the range of [90%, 100%), the weight is 10

② Resource Layer Busyness Score

- Busyness score of a resource layer = $\sum(\text{Busyness score of a node} \times \text{Weight of a node}) / \text{Total weight}$
- Weight of each node: If the value of its busyness is within the range of [0, 30], the weight is 1; If the value of its busyness is within the range of [30, 90], the weight is 3; If the value of its busyness is within the range of [90, 100], the weight is 10

③ Application Busyness Score

- No busy resource layers exist Application busyness score = $\sum(\text{Busyness score of a resource layer} \times \text{Weight of a resource layer}) / \text{Total weight}$
- Busy resource layer exists Application busyness score = $\text{Max(Busyness score of a resource layer)}$

- When the busyness threshold of an application reaches a certain level, a busyness status (idle, normal, or busy) is reported.

• Node Busyness Score

- The busyness score of a node is determined by the indicator value and weight of each indicator. $\text{Node busyness score} = \sum(\text{Each indicator value of the node} \times \text{Weight of each indicator}) / \text{Total weight} \times 100$ The weight is dynamically adjusted based on the indicator value. For example, if the value of **CPU Usage** ranges from 0 to 30% (exclusive), the weight is 1.

• Resource Layer Busyness Score

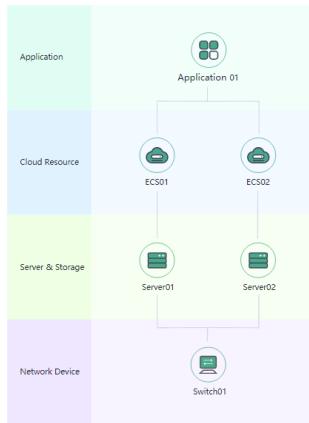
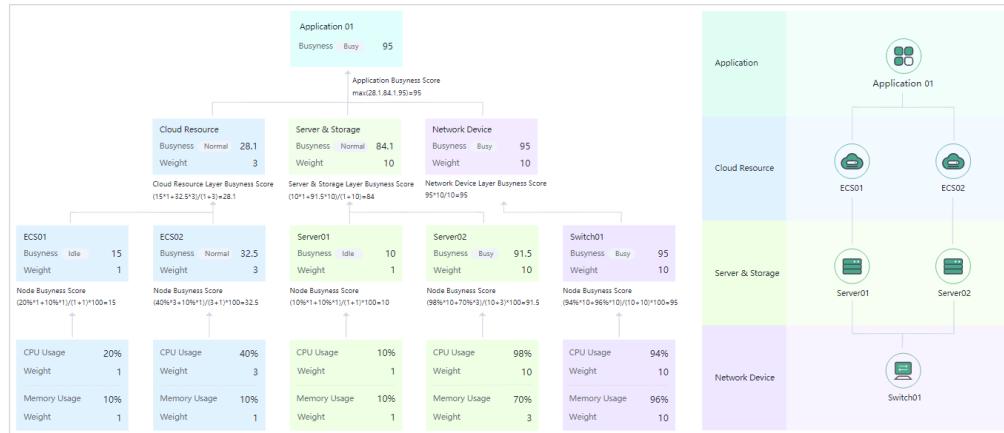
- The busyness score of a resource layer is determined by the busyness score and weight of a node at the layer. $\text{Busyness score of a layer} = \sum(\text{Busyness score of a node} \times \text{Weight of a node}) / \text{Total weight}$ The weight is dynamically adjusted based on the node busyness. For example, if the value of busyness of the ECS01 node ranges from 0 to 30 (exclusive), the weight is 1.

• Application Busyness Score

- When no busy resource layers exist, the busyness score of an application is determined by the busyness and weight of a resource layer. $\text{Application busyness score} = \sum(\text{Busyness score of a resource layer} \times \text{Weight of a resource layer}) / \text{Total weight}$
- When there is a busy resource layer, the busyness score of an application is determined by the maximum busyness score of the resource layer.

Busyness Example

- If the busyness score is not a percentage (%), the formula is as follows: Value for a node = Actual indicator value/Reference value.



50 Huawei Confidential



- The layers of container resources are displayed only for containerized applications.

Health Score Calculation

- The health threshold is configured when ManageOne manages application resources.

Calculation Method and Parameters

1 Health Threshold [0,30) **Abnormal** [30,85) **Subhealthy** [85,100) **Healthy**

1 Node/URL Test Health Score

- No critical alarm is generated
Node/URL Test health score = 100 – Number of major alarms x 5 – Number of minor alarms x 3 – Number of warning alarms x 1
- Critical alarm exists
Node/URL Test health score = 45 – Number of critical alarms x 15 – Number of major alarms x 5 – Number of minor alarms x 3 – Number of warning alarms x 1 (If the calculation result is less than 0, use value 0.)

2 Resource Layer Health Score

- Non-key nodes exist
Health score of a resource layer = $\prod(\text{Health score of a key node}/100) \times 100$ (Π indicates the product operation)
- Non-key node exists
Health score of a resource layer = $\prod(\text{Health score of a key node}/100) \times \text{Average health score of non-key nodes}$ (Π indicates the product operation)

3 URL Test Health Score

- Overall health score of an url test = $\prod(\text{Health score of an url test}/100) \times 100$ (Π indicates the product operation)

4 Application Health Score

- No abnormal resource layers exist
Application health score = $\sum(\text{Health score of a resource layer} \times \text{Weight of a resource layer})/\text{Total weight} \times (\text{Health score of a URL test}/100)$
- Abnormal resource layer exists
Application health score = $\min(\text{Health score of a resource layer}) \times (\text{Health score of a URL test}/100)$

• Node/URL Test Health Score

- When no critical alarm is generated, administrators specify a total score for a node or URL test task and a score for each alarm severity. Health score of a node or a URL test task = Total score – Number of major alarms x Score for each major alarm – Number of minor alarms x Score for each minor alarm – Number of warning alarms x Score for each warning alarm.
- When any critical alarm is generated, administrators specify a total score for a node or URL test task and a score for each alarm severity. Health score of a node or a URL test task = Total score – Number of major alarms x Score for each major alarm – Number of minor alarms x Score for each minor alarm – Number of warning alarms x Score for each warning alarm.

• Resource Layer Health Score

- When there is no non-key node, the formula is as follows: Health score of a resource layer = $\prod(\text{Health score of a key node}/100) \times 100$.
- When there are non-key nodes, the formula is as follows: Health score of a resource layer = $\prod(\text{Health score of a key node}/100) \times \text{Average health score of non-key nodes}$.

• URL Test Health Score

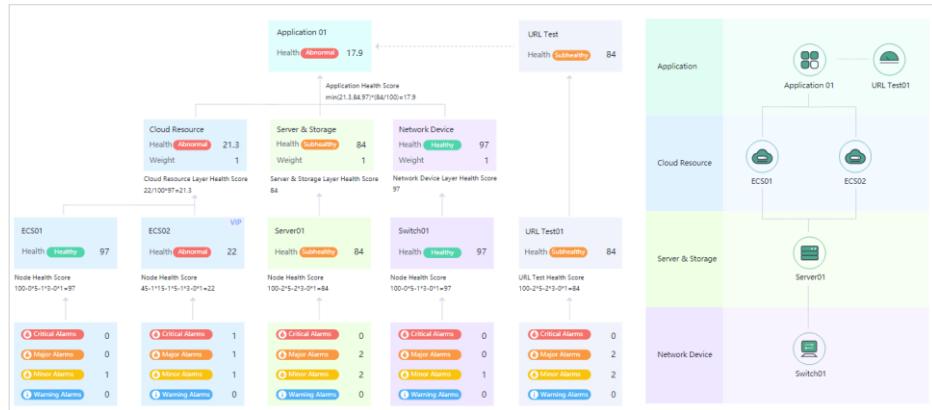
- Overall health score of a URL test = $\prod(\text{Health score of a URL test}/100) \times 100$.

• Application Health Score

- When there is no abnormal resource layer, the formula is as follows:
Application health score = $\sum(\text{Health score of a resource layer} \times \text{Weight of a resource layer})/\text{Total weight} \times (\text{Health score of a URL test}/100)$.
- When an abnormal resource layer exists, the formula is as follows:
Application health score = $\min(\text{Health score of a resource layer}) \times (\text{Health score of a URL test}/100)$.

Health Example

- If there are no non-key nodes, the health score of a resource layer is determined by the health score of the key node. Health score of a resource layer = $\prod(\text{Health score of a key node}/100) \times 100$



Contents

1. Maintenance Overview
 2. Maintenance Functions at the Collection and Control Layer
 3. Maintenance Functions at the Platform Layer
- 4. Maintenance Functions in Different Scenarios**
- Centralized Monitoring
 - Application Analysis
 - **Maintenance Analysis**
 - Deployment Change
 - Troubleshooting

Maintenance Analysis

- Maintenance Analysis features maintenance dashboards, report management, resource management and forecast, and data set management. These functions help reduce OPEX, and provide end-to-end maintenance capabilities such as data visualization and risk identification. They make it easier to design and execute maintenance plans.

Maintenance Dashboard

- On a dashboard, O&M personnel get a comprehensive view of their O&M data. They can see application details and track resource utilization, quickly identifying idle resources and bottlenecks so as to scale resources as needed.

Report Management

- There are preconfigured reports for routine monitoring, capacity optimization, resource optimization, and risk analysis. These reports provide quick insights and predictions, and warn O&M personnel of potential issues. They let you analyze services faster.



Data Set Management

- You can view data sets, customize data sets, and perform secondary data processing and analysis to provide effective data set support for custom dashboards, reports, and monitoring dashboards.

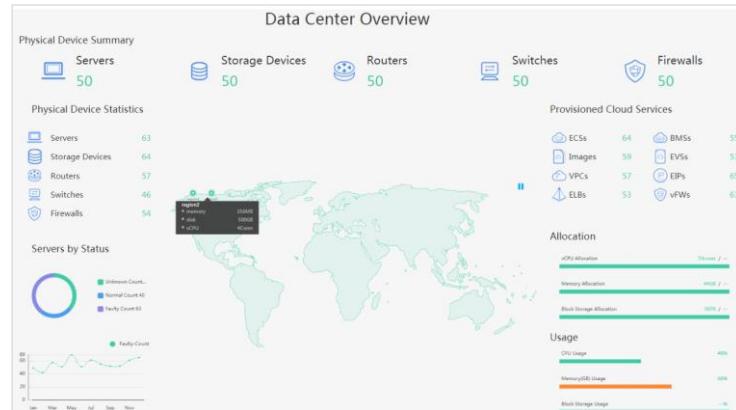
Resource Management and Forecast

- Resource capacity, idleness, and bottlenecks are analyzed to fit scenario-specific analysis requirements and help improve resource utilization.



Maintenance Analysis: Dashboard Monitoring

- Positioning and value: You can use a unified data set model to flexibly customize dashboards for visual maintenance analysis. Resource statistics are displayed on a dashboard for you to clearly monitor resources and ensure stable running of workloads.



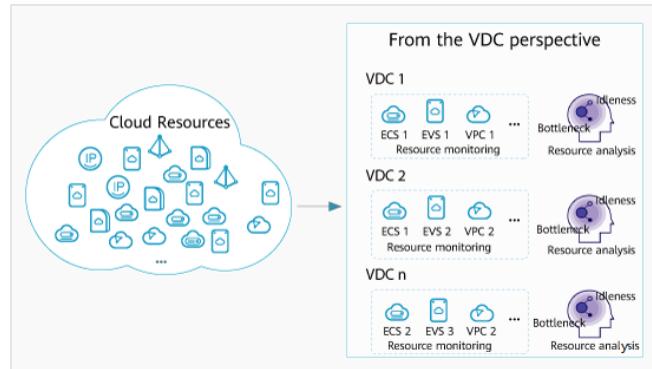
55 Huawei Confidential



- You can customize dashboards based on the unified data set model to facilitate self-service data analysis and visualization.
- Dashboards provide the following functions:**
 - Graphic elements can be dragged and dropped to form a dashboard online and suit diverse demonstration needs.
 - All mainstream diagram elements, including column charts, pie charts, line charts, area charts, and hot spot charts, are supported.
 - Diverse styles provided enable you to flexibly design dashboard layouts to accommodate different presentation needs.
 - Data can be dynamically updated and associated with diagram elements, allowing for real-time monitoring.

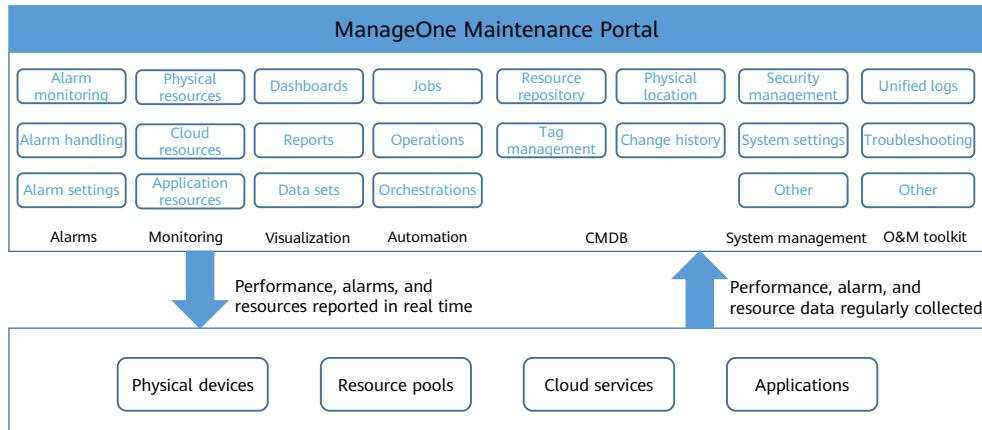
Maintenance Analysis: Dashboard Monitoring

- Applications, not just resource pools, are monitored, providing data support for service scaling.



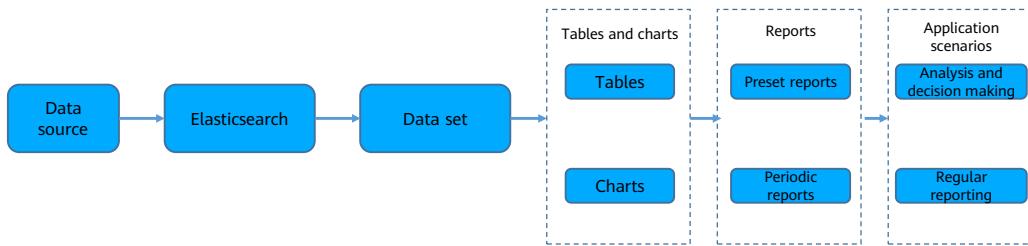
Maintenance Analysis: Report Management

- Application scenarios: decision making, analysis, and scheduled reports.



- O&M personnel can combine multiple dimensions and indicators based on service requirements on Maintenance Portal. They can flexibly filter data to quickly locate key data and perform self-service analysis and periodic reporting.

Data Report Logic



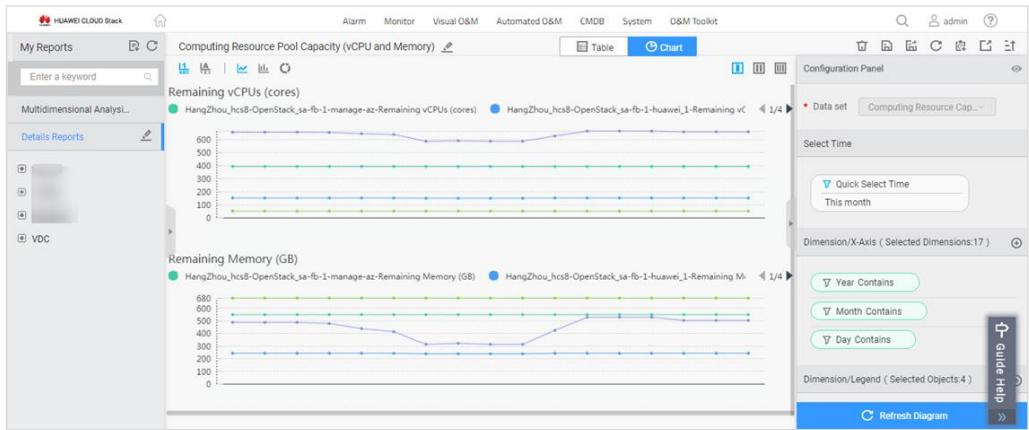
- Data source: Reports provide open data access.
- Elasticsearch: Data sources are distributively stored on an Elasticsearch server.
- Data set: Data obtained from the Elasticsearch server is divided into different data sets based on data types, such as alarms, performance, capacity, services, and resources.
- Table and chart: Maintenance Portal provides preset, custom, and periodic reports.
- Preset reports include multidimensional analysis reports and details reports.
- Custom reports: Administrators can customize reports by combining dimensions and indicators. Custom reports facilitate self-service analysis and calculation and can obtain specific service data.
- Periodic reports: Administrators can define periodic tasks to generate report data at regular intervals. The system sends the data to specific personnel by email to support service analysis and appraisal.
- Application scenarios: The application scenarios of reports include analysis, decision making, and regular reporting.

Indicators and Data Storage

- The values of specific indicators stored in data sets change over time.
 - For example, the CPU usage of an ECS instance is an indicator provided by HUAWEI CLOUD ECS. This indicator is aggregated based on raw data and supports multiple aggregation modes, such as Avg, Max, Sum, and Count.
- Custom indicator: A new indicator can be generated based on the selected or entered preset indicators and four arithmetic operations (addition, subtraction, multiplication, and division). For example, if selected preset indicators are **Sum of Total CPUs** and **Average Value of CPU Usage**, and the indicator to be generated is **Used CPUs**, the formula is as follows: **Used CPU = Sum of Total CPUs x Average Value of CPU Usage**
- The performance indicator data is reported to the data analytics platform (Elasticsearch) every 5 minutes. The indicator data in the report comes from Elasticsearch. Elasticsearch data is stored as follows:
 - Within 7 days: The performance indicator data is generated every 5 minutes.
 - 7 days to 6 months: The performance indicator data is generated every 30 minutes. Elasticsearch processes data generated every 30 minutes. The data can be the maximum, minimum, average value, or other value types of the indicator within that period.
 - More than 6 months: The performance indicator data is generated daily. The data record value is calculated by taking the average value of all performance indicator data records generated every 30 minutes in one day. For example, to obtain the maximum value of a performance indicator, calculate the maximum values collected within every 30 minutes and calculate the average of these maximum values.
- The maximum, minimum, average, and peak values of each performance indicator displayed in the report are calculated based on the performance indicator data stored in Elasticsearch.

Preset Reports: Multidimensional Analysis Reports

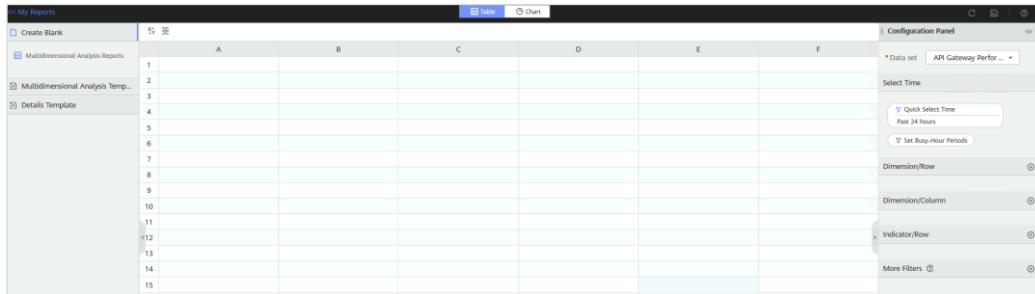
- Multidimensional analysis reports and details reports for typical service scenarios have been preset on ManageOne.



- You can select a specific report by capacity or by resource to view analysis results. You can also learn the indicators, be aware of service health status, and proactively identify problems.

Custom Reports

- Positioning and value: You can use a unified data set model to flexibly customize reports for visual maintenance analysis.



- Based on a unified data set model, a wide variety of preset reports are provided. If preset reports cannot meet your requirements on obtaining required data, you can drag and drop elements and combine multiple dimensions and indicators to obtain valid data for quick analysis and calculation. Custom reports can be tables and charts.
- Custom reports provide the following functions:
 - Graphic elements can be dragged and dropped to design reports online to gain insight into O&M data.
 - Online roll-up and drill-down in different dimensions are supported.
 - Diverse preset reports, such as device quantity statistics, capacity analysis, resource usage analysis, and alarm statistics, are provided.
 - Data can be displayed in cross tabulations.
 - You can switch between tables and charts online.
 - Report data displayed in both tables and charts can be exported in many file formats.
 - Diverse report tasks can be scheduled.

Periodic Reports

- You can create a periodic report task and associate the task with a specific report as needed to analyze how the data is changing each hour, day, week, month, or quarter. After a task is executed successfully, you can periodically view generated reports or have them emailed to you.

The screenshot shows the 'Periodic Report Task Management > Edit Periodic Task' interface. It includes the following sections:

- Basic Information:** Task Name: task, Report: Select (maximum 10 reports), Report Format: EXCEL (selected), Report Export Type: Compressed(*.zip).
- Task Configuration:** One-time (disabled) / Periodic (selected). A note states: "If there are many concurrent tasks, task execution is likely to fail. Select execution time different from that of existing tasks. It is recommended that a maximum of 5 tasks are executed at an interval of 10 minutes in an hour."
- Execution Policy of Periodic Task:** First Execution Time: 2023-09-18 10:00:00, Execution Frequency: 1 Hour.
- Task Validity Period:** Permanently Executed: On (selected), Expiration Date: 2023-09-18 10:00:00.
- Notification:** Notify by email (unchecked), two notes about mail server configuration, Recipients: [REDACTED], Subject: [REDACTED].

62 Huawei Confidential



- When you need to obtain and view data through a periodic report, you can create a periodic report task and manage it.

Execution Policy of Periodic Task

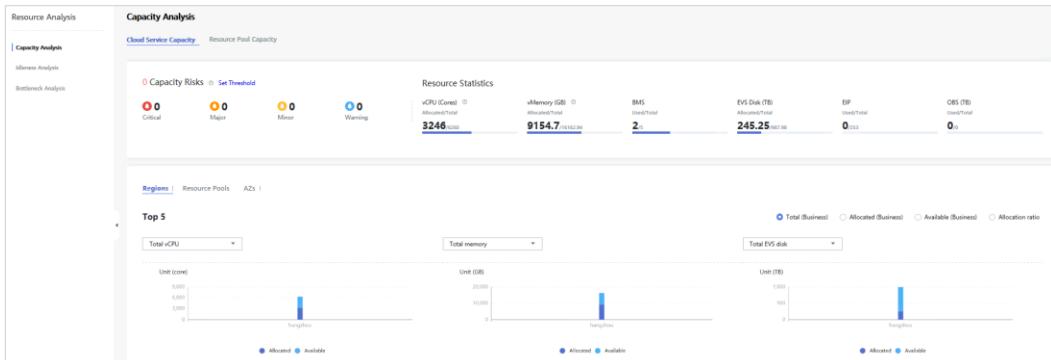
- First Execution Time:** indicates the time when the period task was executed for the first time.
- Execution Frequency:** indicates the frequency of executing a periodic task, including hour, day, week, month, and quarter.

Task Validity Period

- Permanently Executed:** If this switch is turned on, the periodic task will be permanently executed.
- Expiration Date:** indicates the time when a periodic task is stopped. If **Permanently Executed** is turned on, you cannot set this parameter.

Maintenance Analysis: Capacity Management and Forecast

- Positioning and value: Capacities of resource pools and cloud services can be centrally managed and predicted to help customers scale resources, improve resource utilization, and improve the turnover rate.

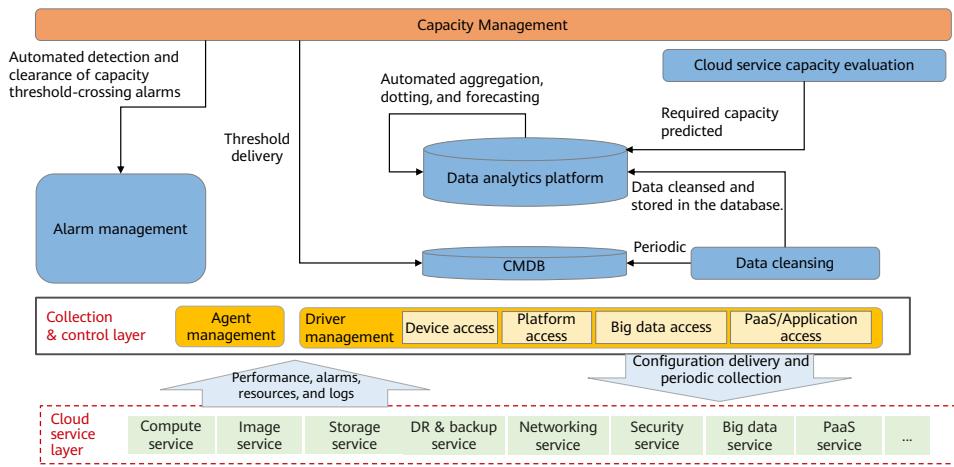


63 Huawei Confidential



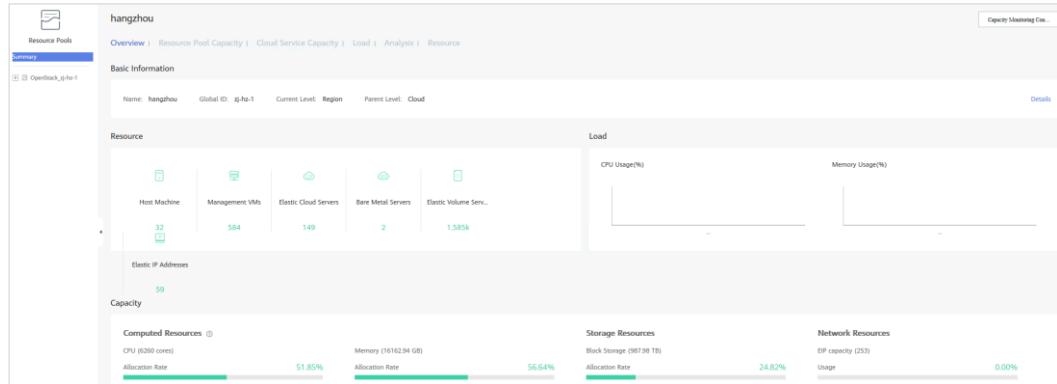
- Capacities of resource pools and cloud services can be centrally managed and predicted to help customers scale resources, improve resource utilization, and improve the turnover rate.
- Capacity Management provides the following functions:**
 - Capacities of different resources pools (including heterogeneous resource pools) in different clouds can be managed.
 - Capacity thresholds can be set and capacities can be predicted to detect risks in a timely manner.
 - Capacities of cloud services can be managed and predicted for customers to scale capacities and adjust policies.

Implementation Logic of Capacity Management and Forecast



Resource Pool Capacity Analysis

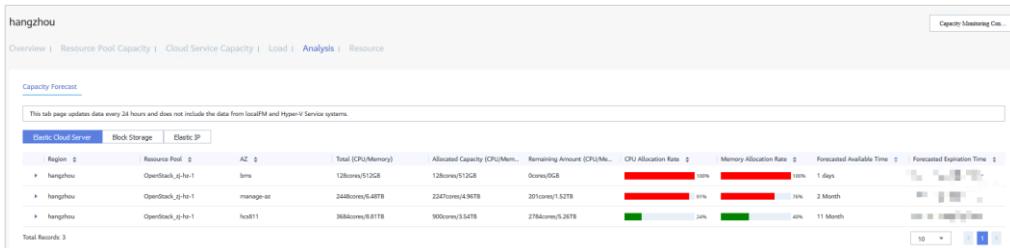
- You can query the capacities of basic resources requiring attention based on selected dimensions.



- In Huawei virtual resource pools, the unit of CPU capacity is GHz. In Huawei OpenStack resource pools, the unit of CPU capacity is core.
- In the one cloud with one pool scenario, resource capacities in the region or resource pool dimension are not displayed separately.
- Capacity data with the **After Overcommitment** identifier displayed in the list is obtained after overcommitment. The capacity data of some resources that are irrelevant to overcommitment is displayed as --.
- Object-based Storage** is not displayed if Object Storage Service (OBS) is not connected to ManageOne.
- You can query the capacities of following resources:
 - Private cloud: resource pool list, AZ list, host group list, host machine list, compute resources, storage resources, and networking resources.
 - Two-level cloud: compute, storage, and network resources.
 - Public cloud: compute, storage, and network resources as well as databases.

Resource Capacity Forecast

- You can view historical capacity usage and usage forecasts in the local cloud in real time and scale resources based on this data.



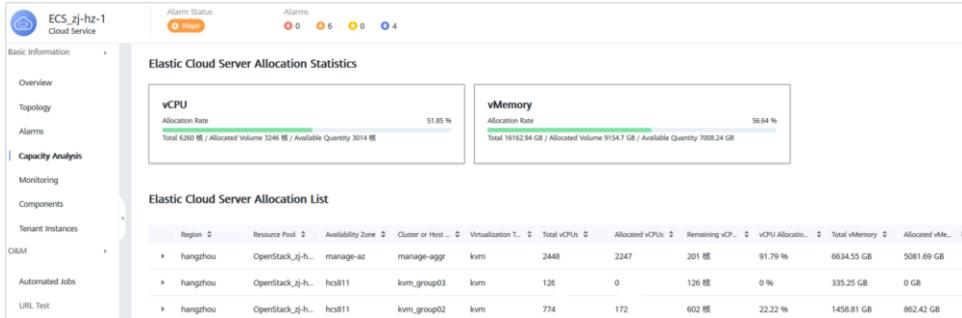
66 Huawei Confidential



- On ManageOne Maintenance Portal, you can forecast resource capacities and analyze cloud service capacities to customize a proper operations plan and capacity expansion policy, maximizing return on investment (ROI).
- The **Analysis** tab page is not displayed for independently interconnected FusionCompute resource pools.
- When a BMS is provisioned in an AZ, the **Capacity Forecast** tab page is unavailable for this AZ.
- In the one cloud with one pool scenario, resource capacities in the region or resource pool dimension are not displayed separately.
- Capacities of ECSs, block storage, and EIPs can be forecasted.

Cloud Service Capacity Analysis

- You can view capacity statistics and cloud service risks in a cloud data center.



Configuring Capacity Alarm Thresholds

- You can set capacity thresholds for different alarm severity levels. When a capacity metric reaches a specified threshold, the system sends the alarm to customers and provides necessary measures.

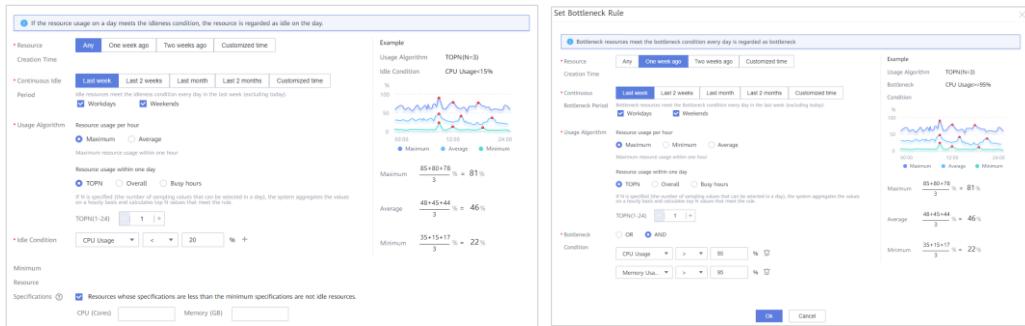
The screenshot shows the 'Capacity Monitoring' section of the ManageOne interface. It includes a navigation bar at the top with tabs for Dashboard, Monitoring, Report Management, Resource Management and Forecast, and Data Set Management. Below the navigation bar, there is a main content area with several sections:

- Capacity Monitor...**: A summary section with a table showing resource pool capacity usage across various services like Cloud Service Capacity, Cloud Service Host Aggregate, and Elastic IP Collection Settings.
- Capacity Threshold Maintenance**: A detailed table showing default threshold rules for different capacity metrics. The columns include Cloud Service, Capacity Metric, Warning (%), Minor (%), Major (%), Critical (%), Remarks, and Operation. Rules listed include vCPU allocation rate, vMemory allocation rate, Usage, and Block storage allocation rate, all set to 90% critical level.
- Default Threshold Rule**: A table showing customized threshold rules. It includes a header row with columns: Cloud Service, Capacity Metric, Applicable Scope, Warning (%), Minor (%), Major (%), Critical (%), Remarks, and Operation. A single row is shown under 'Add'.
- Customized Threshold Rule**: A table showing a single customized threshold rule for 'Cloud Service' with 'Capacity Metric' as 'vCPU allocation rate', 'Applicable Scope' as 'Host', 'Warning (%)' as '90', 'Minor (%)' as '90', 'Major (%)' as '90', 'Critical (%)' as '90', 'Remarks' as '...', and 'Operation' as 'Modify'.

- You can set capacity thresholds in different alarm severity levels and collect elastic IP addresses.
- You can configure and add capacity threshold rules.
- vCPU allocation rate** and **vMemory allocation rate** alarms on only host groups can be reported. **Datastore usage rate** alarms on resource pools can be reported. **Storage usage rate** and **Storage allocation rate** alarms on AZs can be reported. **Elastic IP usage rate** alarms on resource pools can be reported.
- The default threshold rules are recommended. You can also customize thresholds corresponding to the alarm severity as required.
- A virtual resource pool does not support such capacity metrics as the **vCPU allocation rate**, **Storage usage rate**, **Storage allocation rate**, and **Elastic IP usage rate**.
- In new installation scenarios, the warning, minor, and major thresholds of capacity metrics are not set by default. You can set them as required. In upgrade scenarios (upgrade to ManageOne 8.0.0 or later), the warning, minor, and major thresholds of new capacity metrics are not set by default. You can set them as required. The configured capacity metrics are the same as those configured before the upgrade.

Maintenance Analysis: Resource Idleness/Bottleneck Analysis

- Positioning and value: O&M administrators can identify idle resources in a timely manner and enjoy a clear understanding of their VDCs, resource pools, and tenants that the resources belong to. In addition, bottlenecks can be quickly detected.

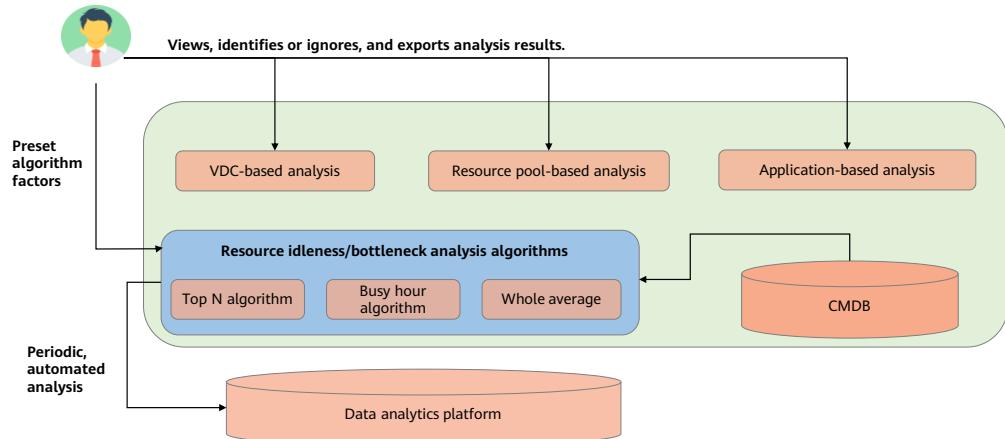


69 Huawei Confidential



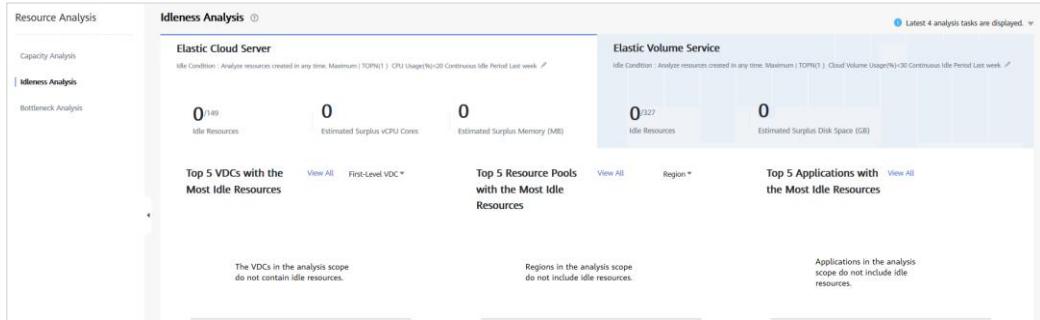
- Resource Idleness/Bottleneck Analysis:** O&M administrators can identify idle resources in a timely manner and enjoy a clear understanding of their VDCs, resource pools, and tenants that the resources belong to. In addition, bottlenecks can be quickly detected. In this way, O&M administrators can know whether cloud resources are properly allocated and whether current resources are affordable for service running.
- Resource Idleness/Bottleneck Analysis provides the following functions:**
 - Resources can be analyzed from multiple dimensions, such as VDCs, applications, and resource pools. Many calculation methods are preset and can be customized to accommodate different scenario requirements.
 - Resource Idleness/Bottleneck Analysis helps customers identify idle resources in a timely manner and instructs administrators to reclaim and reasonably reallocate resources, maximizing resource utilization and minimizing enterprise costs.
 - It also helps customers identify resources with performance or capacity bottlenecks in a timely manner and instructs administrators to scale resources, ensuring secure and stable service running.

Implementation Logic of Resource Idleness/Bottleneck Analysis



Idleness Analysis

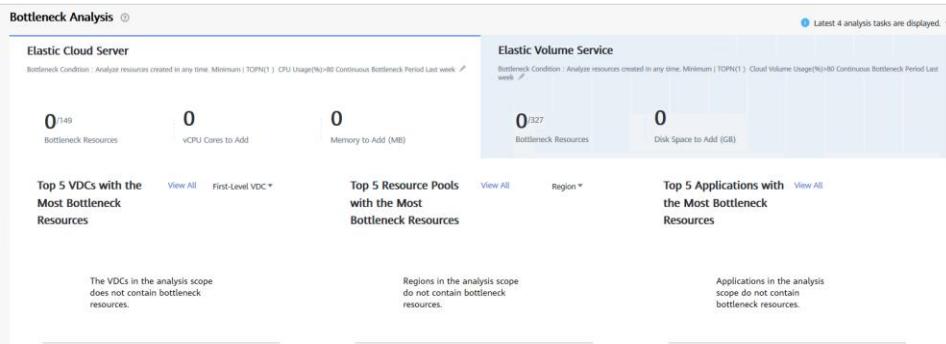
- By setting idleness rules, you can calculate and collect statistics on which resources have had low resource utilization for a long time, either globally, or by VDC, resource pool, or application.



- By detecting idle resources, the global resources can be flexibly scaled down and the utilization is improved.
 - Algorithms of resource idleness rules can be flexibly configured, and the thresholds for determining whether a resource is idle can be customized.
 - The system can analyze global idle resources and centrally display the identified idle resources by VDC, resource pool, and application.
 - The recommended specifications of each detected idle resource are provided for you to flexibly scale down the resource.

Bottleneck Analysis

- Resources with high usage for a long time are bottlenecks. You can configure the rules for determining whether a resource is a bottleneck as required. By setting bottleneck rules, you can summarize and collect global statistics on resources with high resource utilization, and discover and analyze bottlenecks by VDC, resource pool, or application.



- By detecting bottlenecks, the global resources can be flexibly scaled up and the utilization is improved.
 - Algorithms of bottleneck rules can be flexibly configured, and the thresholds for determining whether a resource is a bottleneck can be customized.
 - The system can analyze global bottleneck resources and centrally display the identified resources by VDC, resource pool, and application.
 - The recommended specifications of each detected bottleneck are provided for you to flexibly scale up the resource.

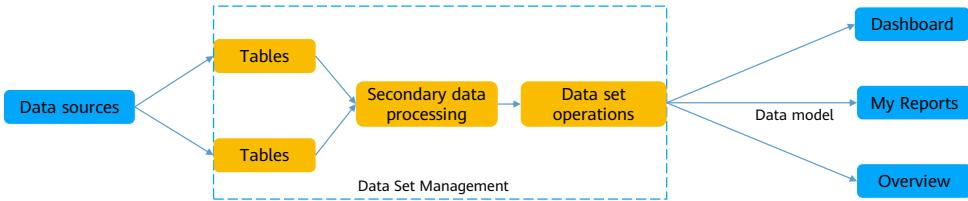
Data Set Management

- Positioning and value: Global dataset metrics are created based on the data obtained from different data sources. These metrics provide data for dashboards and reports for data visualization and processing.

Data Set Management			
Multidimensional Analysis Data Sets	Details Data Sets	Enter a data set: <input type="text"/>	
All			
Name	Group	Type	Remarks
Big Data Host Details	Big Data	Preset data set	Displays big data host details.
Server Details	Physical Resource	Preset data set	Displays x86server details, performance, and performance trend.
FC Switch Port Details	Physical Resource	Preset data set	Displays details, performance, and performance trend of fiber ...
Host Details	Physical Resource	Preset data set	Displays physical host details, performance, and performance trend.
ECS Details	Cloud Resource	Preset data set	Displays ECS details, performance, and performance trend.
Controller Details	Physical Resource	Preset data set	Displays details, performance, and performance trend of storag...
EVS Details	Cloud Resource	Preset data set	Displays EVS disk details, performance, and performance trend.
RDS 6.5 details	Cloud Resource	Preset data set	Displays RDS details, performance, and performance trend.
Big Data Cluster Details	Big Data	Preset data set	Displays big data cluster details.
LUN Details	Physical Resource	Preset data set	Displays details, performance, and performance trend of LUN.

- Data Set Management:** A unified model is built for all O&M data. Diverse data sets are provided to suit different analysis needs.
- 80+ data sets of 6 categories, including alarms, capacity, and performance domains are preconfigured.
 - Data can be flexibly analyzed online using analytic data sets.
 - Massive volumes of data in a details data set can be exported and queried.
 - Dimensions and metrics can be customized online.
 - Dimensions can be extended by tag synchronization.

Data Set Management



- Data sets bridge the gap between data sources and visual display, receiving data from data sources and providing data models for visual display (dashboards, reports, and overview).
- Generally, data sets are used by IT engineers, data R&D engineers, and data analysts to process data.
- A wide variety of data sets are preconfigured in the system for you to directly use. If the preset data sets cannot meet your requirements, for example, when you need to collect statistics on physical and virtual resources in the same report, you can customize a data set and combine multiple existing data sets into a new one. The intersection of dimensions and the union of indicators are used.

Creating or Modifying a Data Set

- During routine maintenance, if the preset data set does not include the data you are concerned with, you can create or modify data sets on the **Data Set Management** page.

The screenshot shows the 'Data Set Management' page with the following details:

- Multidimensional Analysis Data Sets** tab is selected.
- Create** button is highlighted.
- Name**: ECS Performance Analysis
- Group**: Resource Performance Analysis
- Type**: Preset data set
- Remarks**: Collects statistics on and analyzes trends of ECS p...
- Operation**: ECS
- Indicator List** section is expanded, showing various metrics like Weight Average CPU Usage(%) and Peak Memory Usage(%).
- Add Indicator** button is highlighted with a red box.
- Dimensions** section includes Date (Year, Month, Week, Day, Week Day, Hour), Logical Location (Region, Resource Pool, Availability Zone, Cluster or Host Aggregate, Host Name), and VDC (VDC Name, VDC Level, Project, User ID, User Name, Resource Type, UUID, Name, Created On).
- VDC** section includes First-Level VDC, Level-2 VDC, Level-3 VDC, Level-4 VDC, and Level-5 VDC.
- Preset data set**: ECS Performance Analysis (Multi-Cloud)
- Details**: Collects statistics on and analyzes trends of ECS p...

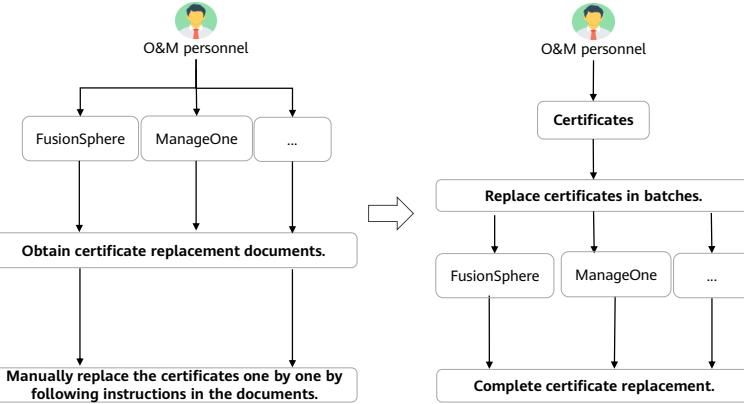
- You can create multidimensional analysis data sets and modify data sets by adding dimensions and indicators.
- Details data sets can be modified only by adding attributes (tag attributes) and indicators (custom indicators).

Contents

1. Maintenance Overview
 2. Maintenance Functions at the Collection and Control Layer
 3. Maintenance Functions at the Platform Layer
- 4. Maintenance Functions in Different Scenarios**
- Centralized Monitoring
 - Application Analysis
 - Maintenance Analysis
 - Deployment Change
 - Troubleshooting

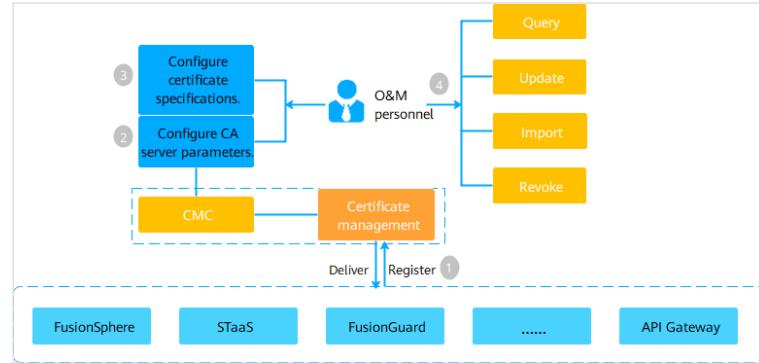
Certificates

- Positioning and value: A unified certificate management page is provided for you to request certificates online and replace multiple certificates at a time.



- A unified certificate management page is provided for you to request certificates online and replace multiple certificates at a time.
- Certificates provides the following functions:**
 - After interconnecting with customer's CA server, Certificates allows you to request and replace certificates in batches.
 - Customers can purchase certificates and manually import them to replace the portal certificate.

Logical Architecture of Certificates



- Certificates of each solution component are registered with Certificates and can be managed by O&M personnel on the **Certificates** page.
- Before maintaining certificates, you need to set parameters of the CA server to be connected to the system.
- Configure the certificate parameters, including the certificate format, key pair generation algorithm, key pair length, and certificate validity period.
- During maintenance, O&M personnel can view, update, import, and revoke certificates.

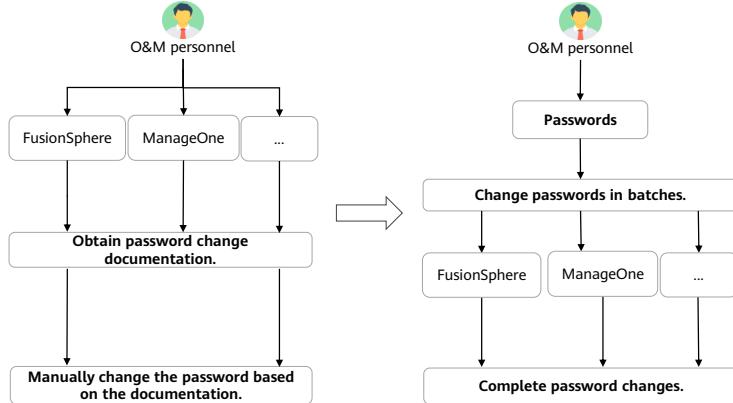
Certificate Update

The screenshot shows the 'Certificates' section of the Huawei Cloud interface. At the top, there's a 'Configure CRL Information' panel with instructions and buttons for 'Configure' and 'Import CRL'. Below it, a table lists certificates. The table has columns for Name, Component, Region, Subject Name, CA, End Time, Type, Usage, Update Time, Update Status, and Operation. The 'Operation' column contains links labeled 'Update'.

Name	Component	Region	Subject Name	CA	End Time	Type	Usage	Update Time	Update Status	Operation
ManageOne-L...	ManageOne	Global	C=CN, O=Huawei, ...			Internal certificate	SSL certificate	--	Update	Update
ManageOne-L...	ManageOne	Global	C=CN, O=Huawei, ...			Internal certificate	SSL certificate	--	Update	Update
ManageOne-E...	ManageOne	Global	C=CN, O=Huawei, ...			Internal certificate	SSL certificate	--	Update	Update
ManageOne-E...	ManageOne	Global	C=CN, O=Huawei, ...			Internal certificate	SSL certificate	--	Update	Update
ManageOne-A...	ManageOne	Global	CN=Platform Cert, ...			Internal certificate	SSL certificate	--	Update	Update
ManageOne-L...	ManageOne	Global	C=CNL0=PMS,CN=...			Internal certificate	SSL certificate	--	Update	Update
ManageOne-P...	ManageOne	Global	CN=Platform Cert, ...			Portal certificate	SSL server certificate	--		Update Import Export CSR

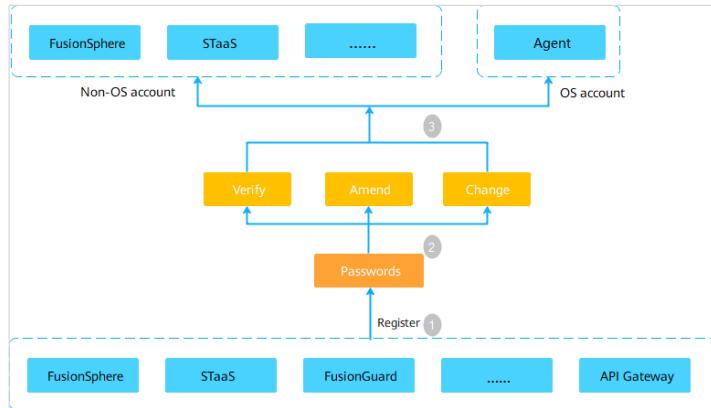
Passwords

- Positioning and value: A unified password management page makes it easier to quickly change passwords.



- A unified password management page makes it easier to quickly change passwords.
- Passwords** provides the following functions:
 - OS accounts can be automatically managed with the help of a CMDB.
 - You can proactively change passwords, change the expiration time, verify and amend passwords.
 - You can quickly change passwords in batches when passwords are about to expire or have expired.

Logical Architecture of Passwords



81 Huawei Confidential



- Accounts of each cloud service are registered with Passwords for unified management.
- **Passwords** allows you to verify, amend, and change account passwords.
 - Passwords can be amended on the **Passwords** page.
 - Password verification and management tasks need to be delivered to the cloud service or the Agent on the VM to which the account belongs.
- A password maintenance task is delivered.
 - If an OS account is used, the operation command will be delivered to the Agent on the VM to which the account belongs. Operation commands related to FusionSphere OS accounts will be delivered to FusionSphere for execution.
 - If a non-OS account is used, the operation command is delivered to each cloud service.

Passwords

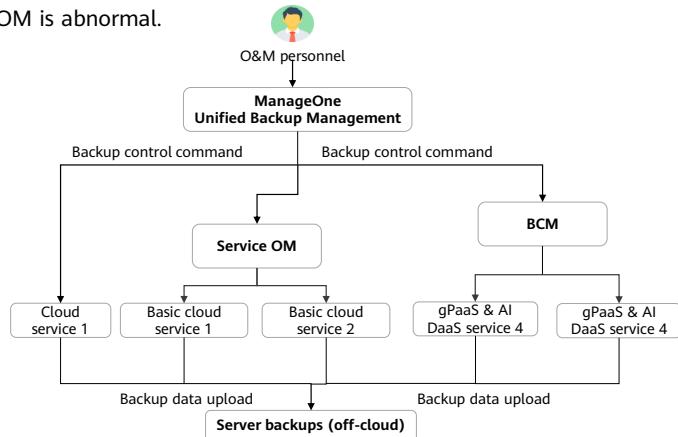
- **Passwords** allows O&M personnel to view basic account information, verify, amend, and change passwords, so less time needs to be spent maintaining passwords.

The screenshot shows the 'Passwords' module interface. At the top, it displays 'Account Statistics': 1394 Accounts, 163 Expired Passwords, and 0 About-to-Expire Passwords. Below this are several filter sections: Account Type (Portal, Application, OS, Database), Account Status (Normal, About to expire, Expired), Previous Change Result (Running, Successful, Failed, Timed out, Queuing, Extending), Verification Result (Running, Successful, Failed, Timed out, Queuing), and a 'Show' dropdown. A note at the bottom states: 'Note: Passwords of gIaaS and AI Daas services are not managed by the Passwords module. You can manage account passwords of these services by referring to operation guides related to them.' The main area is a table listing accounts with columns: Accounts, IP, Device Name, Account Type, Component, Region, Account Status, Previous Change Result, Verification Result, Description, and Operation. The table lists five accounts:

Accounts	IP	Device Name	Account Type	Component	Region	Account Status	Previous Change Result	Verification Result	Description	Operation
opsadmin	10.200.16.45	CDK-Server02	OS	CloudCDK	Hangzhou	Normal	Successful	Successful	logon administrator...	Extend Change Verify
opsadmin	10.200.18.36	AOM-Redis05	OS	CloudFiddleWare	Hangzhou	Normal	Successful	Successful	OS login account, ...	Extend Change Verify
root	10.200.45.125	isap-inst-ingest-gro...	ISAP	hangzhou	Normal	Normal	Successful	Successful	Password of OS acc...	Extend Change Verify
filetpadm	10.200.16.10	ManageOne-Servic...	OS	ManageOne	hangzhou	Normal	Successful	Successful	SFTP user of the Fu...	Extend Change Verify

Backup Management

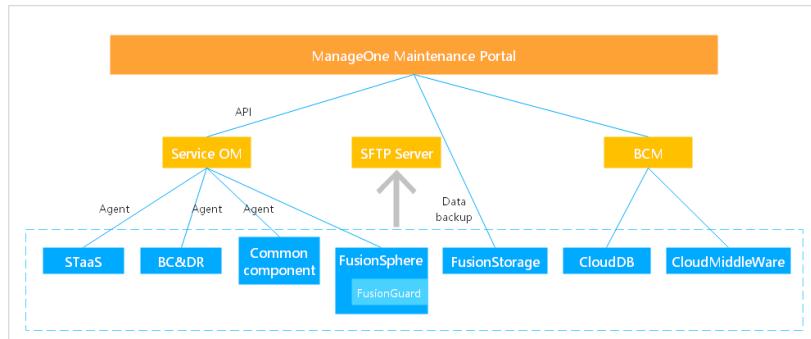
- Positioning and value: Management data is backed up in a unified manner to minimize the impact on workloads if Service OM is abnormal.



- Unified Backup Management:** Management data is backed up in a unified manner to minimize the impact on workloads if exceptions occur.
- Unified Backup Management provides the following functions:**
 - Data can be manually or periodically backed up. Full backup and incremental backup are supported.
 - Backup tasks can be uniformly managed.
 - Backup server addresses, backup protocols, and backup paths can be uniformly managed.

Logical Architecture of Backup Management

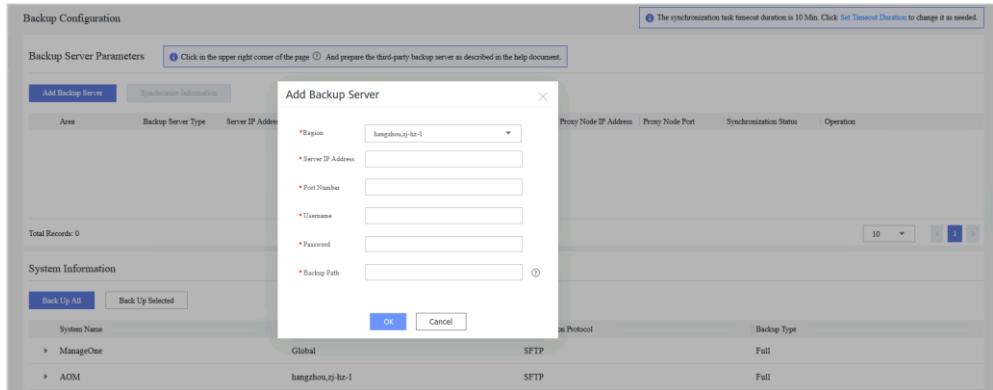
- If a third-party SFTP backup server is available, data from resource pools, ManageOne, ModelArts, and EI is backed up to the third-party SFTP backup server. After gPaaS & AI DaaS services are connected, the CloudDB and CloudMiddleWare backup policies must be configured. Otherwise, data is backed up every 30 days by default.



- STaaS, BC&DR, common components, and FusionSphere connect to ManageOne Maintenance Portal through Service OM.
- FusionStorage directly connects to ManageOne Maintenance Portal.
- CloudDB and CloudMiddleWare connect to ManageOne Maintenance Portal through BCM.
- Data of STaaS, BC&DR, common components, FusionSphere, FusionStorage, CloudDB, and CloudMiddleWare is backed up to an SFTP server.

Manual Backup (1)

- You need to add a backup server.



Manual Backup (2)

- On the **System Information** page, you can click **Back Up All** or **Back Up Selected** to back up the objects as needed.

System Information			
	Area	Transmission Protocol	Backup Type
ManageOne	Global	SFTP	Full
AOM	hangzhou,zj-hz-1	SFTP	Full
CCE	hangzhou,zj-hz-1	SFTP	Full
CSBS-VBS	hangzhou,zj-hz-1	SFTP	Full
CSP-DB	hangzhou,zj-hz-1	SFTP	Full
CloudDB	hangzhou,zj-hz-1	SFTP	Full,Incremental
CloudMiddleWare	hangzhou,zj-hz-1	SFTP	Full

Periodic Backup

- You can create a backup policy to perform periodic backup. Incremental backup or full backup is performed by hour or day.

Basic Details

- Name: 11
- Period: 24 Day
- First Execution Time: [dropdown]
- Backup Type: Full backup Incremental backup
- Description: Enter a brief description.

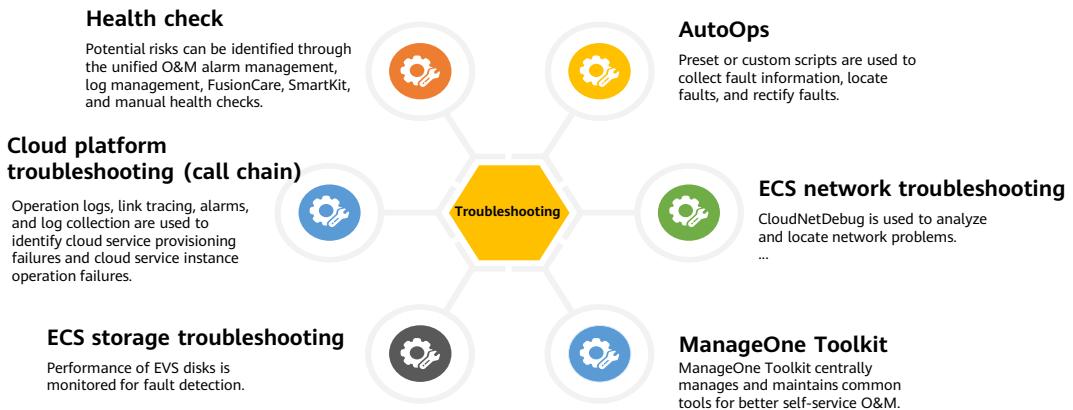
Systems to Back Up

Available	Selected
<input checked="" type="checkbox"/> hangzhouj-hz-1 <ul style="list-style-type: none"><input checked="" type="checkbox"/> FusionSphere<input checked="" type="checkbox"/> eBackup-10.200.17.234<input checked="" type="checkbox"/> eBackup-10.200.16.158<input checked="" type="checkbox"/> CSBS-VBS<input checked="" type="checkbox"/> CSP-DB<input checked="" type="checkbox"/> CCE<input checked="" type="checkbox"/> AOM...	<input type="checkbox"/> hangzhouj-hz-1_FusionSphere <input type="checkbox"/> hangzhouj-hz-1_eBackup-10.200.17.234 <input type="checkbox"/> hangzhouj-hz-1_eBackup-10.200.16.158 <input type="checkbox"/> hangzhouj-hz-1_CSBS-VBS <input type="checkbox"/> hangzhouj-hz-1_CSP-DB <input type="checkbox"/> hangzhouj-hz-1_CCE <input type="checkbox"/> hangzhouj-hz-1_AOM <input type="checkbox"/> hangzhouj-hz-1_LTS

Contents

1. Maintenance Overview
 2. Maintenance Functions at the Collection and Control Layer
 3. Maintenance Functions at the Platform Layer
- 4. Maintenance Functions in Different Scenarios**
- Centralized Monitoring
 - Application Analysis
 - Maintenance Analysis
 - Deployment Change
 - Troubleshooting

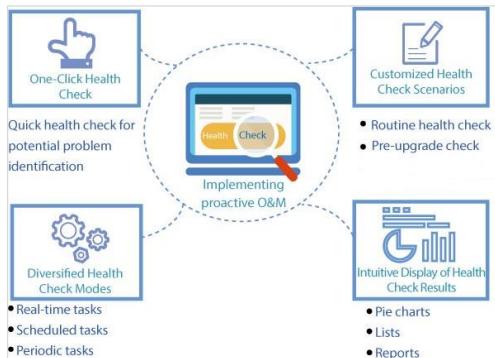
Troubleshooting Types



- Troubleshooting includes cloud platform troubleshooting (call chain), ECS network troubleshooting, ECS storage troubleshooting, and ManageOne toolkit. Before a fault occurs, a health check is also a way to identify potential risks or prevent faults.
- What are O&M? Many people believe that the responsibility of O&M is to handle faults and maintain system stability. However, an excellent O&M operation is to prevent, reduce, or even avoid faults. How can we prevent and reduce faults? Currently, one of the most common ways for many companies is to perform routine health checks to identify potential risks in advance. However, there are thousands of devices in a large data center and O&M requires more than manpower. Therefore, Huawei has developed a set of health check tools to improve devices, systems, processes, and personnel capabilities.

Health Check

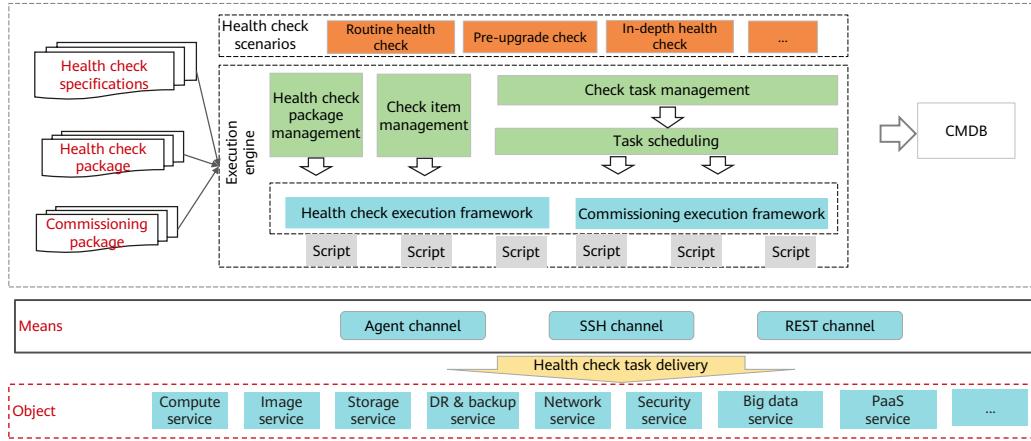
- A health check tool is provided for both technical support and maintenance engineers to check systems and services periodically and rectify faults based on the check results. This tool leverages the long-term, stable running of cloud platforms and services.



- One-click health check
 - The ManageOne health check tool can quickly check the node health status and identify potential system problems, achieving proactive O&M.
- Custom health check scenarios
 - You can select a health check task based on site requirements. Currently, you can select routine health check and pre-upgrade health check tasks.
- Diversified health check modes
 - Health check tasks can be performed in real time, on schedule, or periodically. You can configure tasks based on environment requirements.
- Intuitive display of health check results
 - Check results are displayed in pie charts, lists, and health check reports, helping O&M personnel intuitively obtain the health status of products.

Health Check Architecture

- Positioning and value: Standard, visualized, and automated health check actions help avoid risks caused by manual operations and improve the work efficiency of onsite personnel.

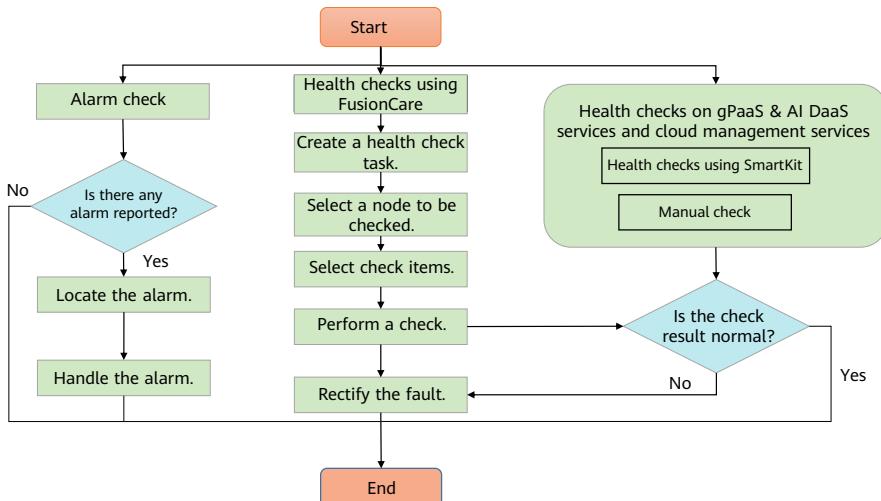


91 Huawei Confidential



- The health check tool provides the following functions:
 - It can perform health checks on objects of both management plane and tenant plane.
 - Infrastructure services, gPaaS & AI DaaS service, and cloud management platforms can be checked.
 - The development state, release state, and running state are decoupled to facilitate the development, deployment, and execution of health check tasks.
 - A variety of health check scenarios, such as pre-upgrade check and routine health check, are supported.
 - Local scripts, remote protocols, and other methods are used for health checks.

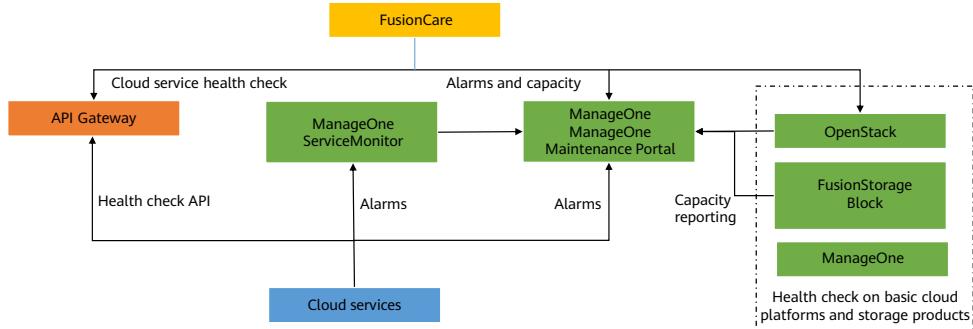
Health Check Process



- Alarm checks and FusionCare health checks are usually used for routine health checks of HUAWEI CLOUD Stack. For gPaaS & AI DaaS services that cannot be checked using FusionCare, you can perform manual health checks or use SmartKit for health checks. Currently, the HCIP course of HUAWEI CLOUD Stack 8.1.1 does not involve the health checks on DR services and on storage devices using SmartKit.
 - Checking alarms: Alarms are checked on ManageOne Maintenance Portal.
 - FusionCare health check: Perform health check using FusionCare from the **Health Check** entry on ManageOne Maintenance Portal. Basic cloud platforms and infrastructure cloud services can be checked using FusionCare from the **Health Check** entry on ManageOne Maintenance Portal.
 - SmartKit is a service tool for products in the storage, server, and cloud computing fields.

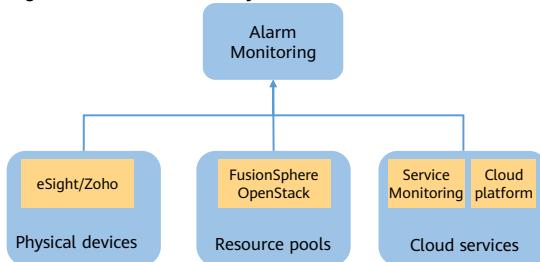
FusionCare Health Check Principles

- Cloud service health check: Each cloud service registers a health check API with API Gateway so that FusionCare can check basic cloud platforms, infrastructure cloud services, and gPaaS & AI DaaS services.
- Health check on basic cloud platforms and storage products: FusionCare calls the API of each product to perform health checks.



Collecting Alarm Information on ManageOne Maintenance Portal

- Alarm Monitoring on HUAWEI CLOUD Stack ManageOne Maintenance Portal centrally monitors alarms that are reported by services or third-party systems. It helps O&M administrators quickly locate faults and troubleshoot them, ensuring an uninterrupted service. Alarm Monitoring is dedicated to monitoring and O&M for continuously-evolving complex networks. It monitors faults on traditional and next-generation networks, reducing Mean Time to Repair (MTTR) and improving network O&M efficiency.



- Alarms on Maintenance Portal can be identified through routine health checks.
 - eSight: monitors Huawei physical devices. For example, eSight can check the status of RH2288H servers and FusionStorage storage devices.
 - Zoho: monitors third-party physical devices.
 - Cloud platform: monitors FusionSphere OpenStack resource pools and cloud services, such as compute, storage, network, and cloud services as well as tenant instances.

Health Checks Using FusionCare

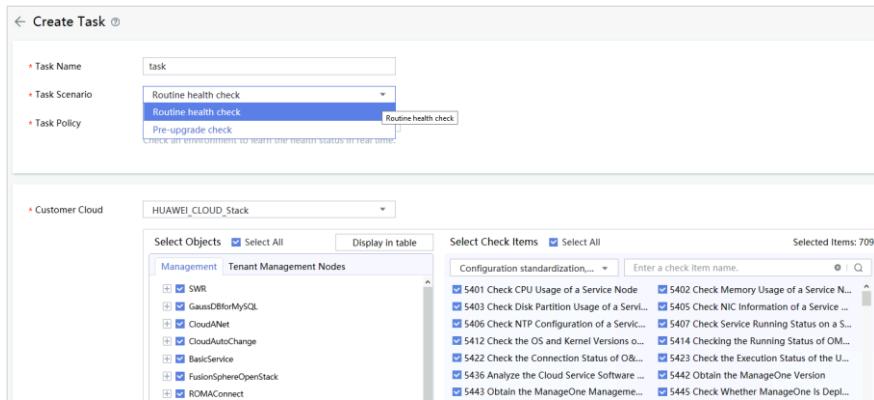
- On ManageOne Maintenance Portal, choose **Routine O&M > Health Check**. You can create, modify, and delete health check tasks and export health check reports.

The screenshot shows the 'Health Check Tasks' page. At the top, there are four status counts: All Task (2), Executing (0), Finished (2), and Not started (0). Below this is a search bar with placeholder text 'Enter a task name.' and a 'Create' button. A table lists two tasks: 'CCE' and 'test'. The 'CCE' task was finished 14m45s ago with 100% progress, a routine health check, and a real-time task. It has a pass rate of 93.75% and was created by admin. The 'test' task was finished 31m3s ago with 100% progress, a routine health check, and a real-time task. It has a pass rate of 91.91% and was created by admin. There are buttons for 'Modify' and 'Export Report' next to each task row. At the bottom left, it says 'Total Records: 2' and there are navigation buttons for page 1 of 1.

Name	Start Time	Execution Durat...	Status	Progress	Task Scenario	Task Policy	Object Check Pa...	Check Item Pass...	Created	Operation
CCE	14m45s		Finished	100%	Routine health...	Real-time task	50%	93.75%	admin	Modify Export Report
test		31m3s	Finished	100%	Routine health...	Real-time task	91.91%	99.09%	admin	Modify Export Report

Health Checks Using FusionCare: Creating Health Check Tasks

- Health checks can be used for routine health checks and pre-upgrade checks.



- FusionCare check tasks can be executed immediately, periodically, and as scheduled. This page uses immediate execution as an example to describe how to create a health check task and export a check report to a local PC.
- Routine health check
 - In scenarios such as routine maintenance, service quality assurances during big events, quarterly health checks, and checks after fault recovery, O&M personnel use the health check function to periodically check projects or sites to identify issues and potential risks, reduce and prevent accidents, and handle potential risks before they spread.
- Pre-upgrade check
 - You can perform pre-upgrade checks and handle the risks before the upgrade.

Health Checks Using FusionCare: Exporting a Health Check Report

- After a health check is complete, you can export the health check report for the health check object.

The screenshot shows the 'Health Check Tasks' page with two tasks listed:

Name	Start Time	Execution Durat...	Status	Progress	Task Scenario	Task Policy	Object Check Pa...	Check Item Pass...	Created	Operation
CCE	[REDACTED]	14m45s	Finished	100%	Routine health...	Real-time task	50%	99.75%	admin	Modify Export Report
test	[REDACTED]	31m3s	Finished	100%	Routine health...	Real-time task	91.91%	99.09%	admin	Modify Export Report

A modal window titled 'Export Report' is displayed, showing the 'Report Type' section with 'Basic Report' selected. It also contains a note: 'A basic report contains the health check results of all products supported by FusionCare. The report file is in .xlsx and .html format.' There are 'Cancel' and 'OK' buttons at the bottom.

- A basic report covers all products that can be checked by FusionCare. The report is an XLSX or HTML file.
- A synthesis report contains health check results of FusionCompute, FusionSphere OpenStack, ManageOne, and IaaS Service. The report is in .docx format.

Manual Health Check

- Check the running status of OMMHAService.
 - Log in to the node where OMMHAService is deployed, go to the `/opt/oss/Tenant name/apps/OMMHAService/bin/` directory, and run the `status.sh` script to check whether the service is normal.

```
[ossadm@MOC-ManageOne-Service01 bin]$ sh status.sh
HAMode
double

HostName          HostName           HAVersion        StartTime       HAAActive      HAAllResOK      HARunPhase
ha1              MOC-ManageOne-Service01  V100R001C01    2023-06-20 10:00:00  active         normal        Active
ha2              MOC-ManageOne-Service02  V100R001C01    2023-06-20 10:00:00  standby        normal        Inactive

ResName          ResStatus        ResHASatus      ResType
ha1             RMICritical    Active_normal    Active_standby
ha1             RMfloatip      Normal          Single_active
ha1             RMRnic        Normal          Double_active
ha1             SwitchStatus   Normal          Double_active
ha2             RMICritical    Stopped         Active_standby
ha2             RMfloatip      Normal          Single_active
ha2             RMRnic        Normal          Double_active
ha2             SwitchStatus   Normal          Double_active

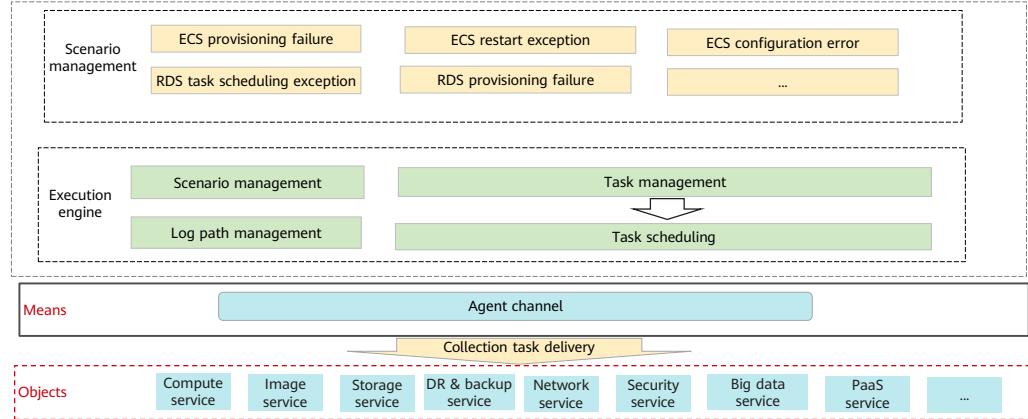
[ossadm@MOC-ManageOne-Service01 bin]$
```

- HAAActive:** indicates the node role. The value can be **active**, **standby**, or **NULL**.
 - Generally, **NULL** indicates that OMMHA on the node is abnormal. In normal cases, the two nodes are in the **active** and **standby** statuses respectively.
- HAAllResOK:** indicates the status of all resources. The value can be **normal**, **exception**, or **abnormal**.
 - Note: In normal cases, the status of all resources is **normal**.
 - If the resource status is **exception**, the system attempts to automatically restore the resources. After multiple automatic recovery failures, the resource status changes from **exception** to **abnormal**. In this case, the system stops automatically rectifying the fault.
- HARunPhase:** indicates the HA running period.
 - Note: **Activing** indicates that the standby node is being promoted to active. **Actived** indicates that the standby node has been promoted to active. **Deactivating** indicates that the active node is being demoted to standby. **Deactived** indicates that the active node has been demoted to standby.
- ResStatus** indicates the resource status.
 - Status of the active and standby nodes:
 - Standby_normal** indicates that the standby node is running properly.
 - Active_normal** indicates that the active node is running properly.
 - Raising_active** indicates that the standby node is being promoted to active.
 - Lowng_standby** indicates that the active node is being demoted to standby.

- Note: In normal cases, one node is in the **Active_normal** status and the other is in the **Standby_normal** status.
- Resource status of nodes deployed in single-active mode:
 - **Normal** indicates that the resource is normal.
 - **Stopped** indicates that the resource is no longer used.
- Note: In normal cases, one node is in the **Normal** status and the other is in the **Stopped** status.
- **ResHAStatus** indicates the resource status. The value can be **Normal** or **Abnormal**.
 - Note: In normal cases, all resources are in the **Normal** status.
- **ResType** indicates the resource type. The value can be **Active_standby** or **Single_active**.

Log Management

- Positioning and value: Run logs can be precisely collected based on different fault scenarios, facilitating system fault demarcation and locating.



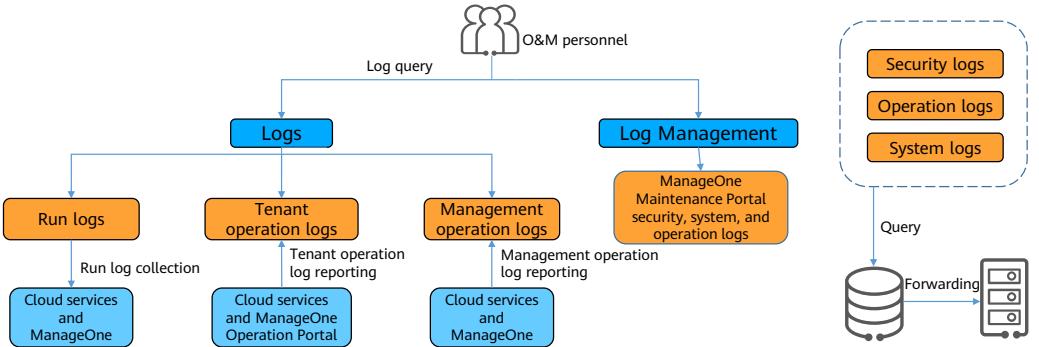
100 Huawei Confidential

HUAWEI

- Run logs can be precisely collected based on different fault scenarios, facilitating system fault demarcation and locating.
- Log Management provides the following functions:**
 - Fault scenarios:** More than 200 common fault scenarios are provided, covering mainstream fault scenarios.
 - One-click collection:** Run logs of different services, components, and devices distributed on each node can be centrally collected and exported for R&D engineers to analyze.
 - Powerful filtering:** If a fault occurs, you can set filtering conditions, such as the time, service, node, and keyword, to search for run logs, and export and send them to R&D engineers.

Log Category

- O&M personnel store and manage security logs, system logs, and operation logs on the **Logs** page of ManageOne Maintenance Portal.

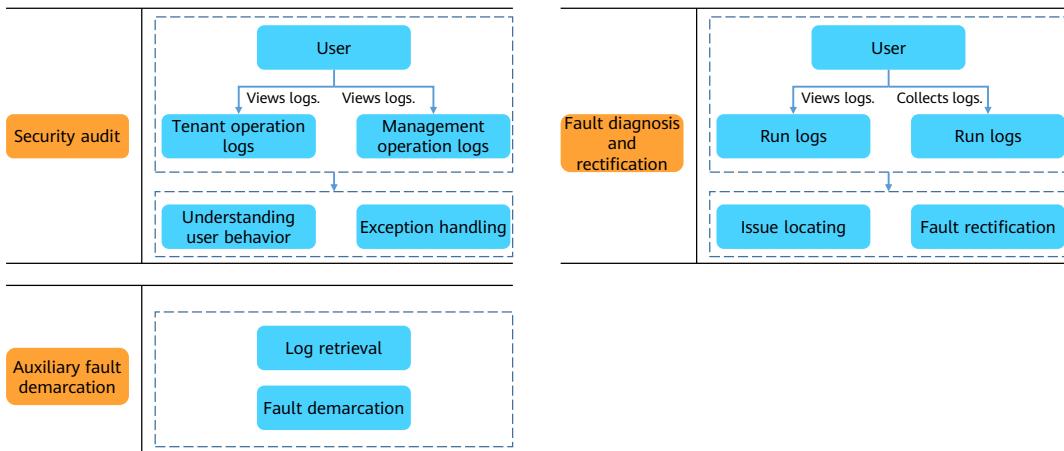


101 Huawei Confidential



- Log Management consists of Logs and Log Management on ManageOne Maintenance Portal.
- Logs are classified into run logs, management operation logs, and tenant operation logs.
 - Run logs
 - Logs generated during the running of cloud services and ManageOne are collected.
 - Tenant operation logs
 - Logs of operations performed by users on ManageOne Operation Portal and operation logs reported by cloud services are collected.
 - Management operation logs
 - Operation logs of cloud platform management systems or devices that support the Syslog or RESTful protocol can be collected and forwarded.

Application Scenarios of Logs



- **Security audit:** By viewing management operation logs and tenant operation logs, you can understand user behavior and detect suspicious activities. The system records logs for important service operations (including system parameter configuration, and resource configuration and release) to ensure that the system running information can be traced. If any exception log is found, you can report it to the upper-level department and handle it in a timely manner.
- **Fault diagnosis and rectification:** By viewing and collecting run logs, you can understand the real-time running status of processes in the system to locate and rectify faults.
- **Auxiliary fault demarcation:** Call chain logs can be collected and log search capabilities are provided for call chains to facilitate call chain fault demarcation.

Run Logs - Log Template

- Log template

- The Logs function combines the common fault scenarios of cloud services to generate log templates and preset these templates in the software. Administrators can collect log information as required.
- If the preset templates cannot accommodate the service needs, administrators can add templates, combine related cloud service logs, and quickly collect valid log data.

The screenshot shows a 'Template Details' interface with the following fields:

- Name:** MO_0009_Failed to Report Device Performance Data
- Cloud Service:** ManageOne
- Description:** The device performance data fails to be reported.

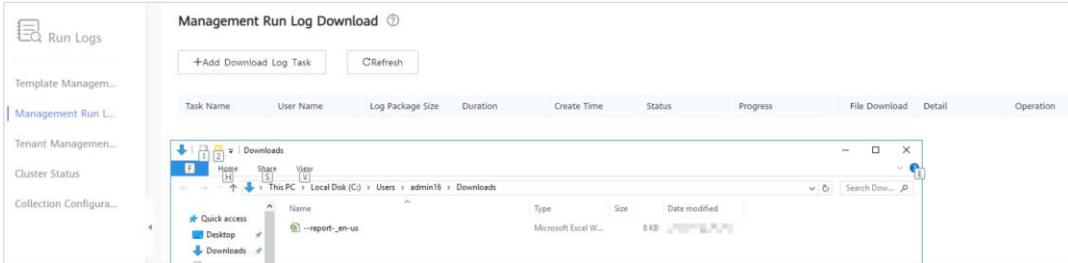
The 'Add' section lists five entries:

No.	Cloud Service	Service/Microservice	Path
1	ManageOne	HIBORService	/var/log/oss/HIBORService/
2	ManageOne	MODataStrategyEngineService	/var/log/oss/MODataPipelineService/modatapipelineengine*/*log/ /var/log/oss/MODataPipelineService/modatapipelineengine*/*log/ /var/log/oss/MODataStrategyEngineService/ /var/log/oss/MODataStrategyEngineService/modatstrategyneser
3	ManageOne	MORCSAPService	/var/log/oss/MOCommonDriverService/mocommondrive*/*log/
4	ManageOne	MOSMSService	/var/log/oss/MOPerfMonitorService/mopernmonitor*/*log/ /var/log/oss/MOPerfMonitorWebsite/moperfmonitorwebsite-*/*log/
5	ManageOne	MOPmAcessService	/var/log/oss/MOPmAcessService/mopmaccessservice-*/*log/

- Preset templates cannot be modified.
- Preset templates cannot be deleted.
- Preset templates cannot be downloaded.

Run Logs - Management Run Logs

- Run logs are classified into management run logs and tenant management node run logs. You can collect logs based on the log template.



- Typical templates of run logs are preset based on common cloud service fault scenarios. Run logs can be downloaded based on these templates. If the preset templates cannot meet the current service needs, you can combine related cloud service log paths to customize log templates.
- Scenario of management run logs: To locate faults, O&M personnel need to view the run logs of management VMs and download the log files of cloud services to the local PC for analysis.

Run Logs - Tenant Operation Logs

Task Name	Username	Log Package Size	Duration	Creation Time	Status	Progress	Operation
No data found							

- Scenario of tenant management node run logs: Management logs of some cloud services are stored on VMs on Tenant Portal. During fault locating, O&M personnel need to view run logs of VMs or VM containers and download log files generated during cloud service running to a local PC for analysis.
- Management run logs in the IaaS OpenStack resource pool cannot be collected on the **Logs > Run Logs** page.

Management Operation Logs

Management Operation Logs

Protocol type: Syslog

Time: Last 15 minutes Last hour Last day Last 3 days Last week Last 30 days Custom

Host Name:

Keyword:

Search Export

- Management Operation Logs collects and forwards operation logs of management systems or devices, such as eSight, servers, storage devices, DR and backup services, CloudAuditLog, and FusionStorage Block management system using the Syslog or RESTful protocol. In this way, factors that affect normal running of the system can be detected in a timely manner, and corresponding measures can be taken quickly.

Tenant Operation Logs

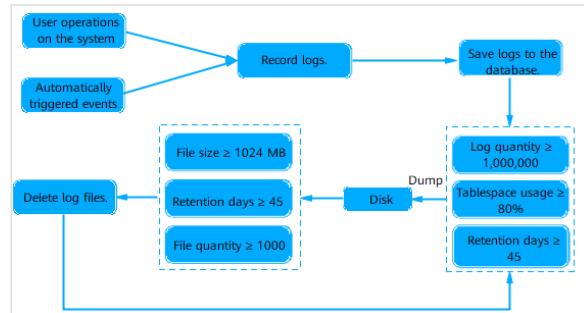
- On the **Tenant Operation Logs** page, locate the fault and click its call chain link.

The screenshot shows the 'Tenant Operation Logs' interface. At the top, there are filters for 'Operation Time' (Last 3 months), 'Service Name' (All Service Name), 'Event' (All Event), 'Request ID' (Enter a request ID), 'Resource Type' (All Resource Type), 'Log Level' (All log levels), 'Resource Set ID' (Enter a Resource Set ID), 'Operation Result' (All Operation Result), and 'Operation ID' (Enter an operation ID). Below the filters is a search bar with 'Search by: Event Name'. A 'Export' button is available. The main area displays a table of events:

Event	Resource Name	Log Level	Operation Result	Operation User	Operation IP	Operation Time	Call Chain Link
user.logout	CSIC_admin	Minor	Successful	CSIC_admin	-	2023-09-15 10:00:00	Call Chain Link
user.logout	CSIC_admin2	Minor	Successful	CSIC_admin2	-	2023-09-15 10:00:00	Call Chain Link
batchRenameInstances	an-100-gray	Warning	Failed	CSIC_admin	192.168.1.100	2023-09-15 10:00:00	Call Chain Link

Principles of Log Overflow Dump

- When users perform operations on ManageOne Maintenance Portal or the system automatically triggers operations or tasks, the generated logs will be saved to a log management database. To ensure sufficient database space, the system provides the log dump function and automatically saves the logs that meet the conditions to the disks of the server, and deletes them from the database.



Log Storage (1)

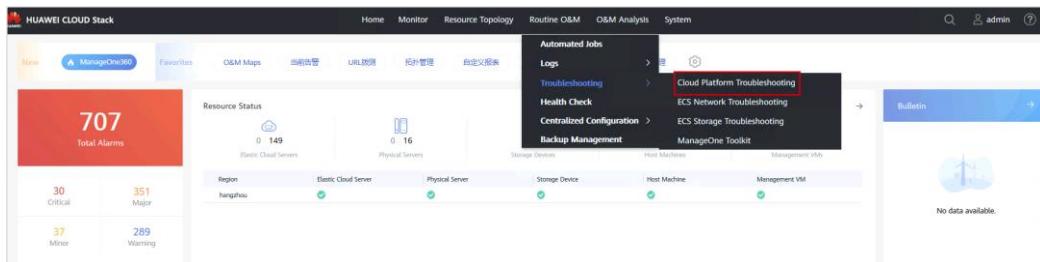
Log Type	Storage Mode	Default Storage Duration	Dump Mechanism	Forwarding Mechanism
Run logs	SFTP server	Log files on the SFTP server are stored for two days and will be automatically deleted two days later.	Run logs cannot be dumped.	Run logs cannot be forwarded.
Tenant operation logs	Elasticsearch server	365 days	<p>Dump conditions:</p> <ol style="list-style-type: none"> 1. The number of logs stored in the database exceeds 80% of the preset value. 2. Logs are stored for more than 365 days. <p>Trigger mechanism: The system checks logs at 01:30 every day and automatically saves logs that meet requirements as files to <code>/opt/share/Product/MOICAgent/dumpFile/tenantdbsvr/motenan</code> <code>ttracedb</code> on a hard disk of a server.</p> <p>The system dumps 10,000 logs each time, after which, the system checks whether either of the preceding conditions is met. If the conditions are not met, the system stops dumping logs.</p>	Tenant operation logs can be forwarded to the Syslog server.

Log Storage (2)

Log Type	Storage Mode	Default Storage Duration	Dump Mechanism	Forwarding Mechanism
Management operation logs	Elasticsearch server	14 days by default. The duration can be set to 1 month, 3 months, or 6 months.	Management operation logs cannot be dumped.	Management operation logs can be forwarded to the Syslog server.
Log management (security, system, and operation logs)	Log management database	45 days	<p>Dump conditions: Too many logs may result in insufficient database storage space. When more than one million logs have been stored, or the stored logs have occupied over 80% of database storage space, or if the logs have been stored for more than 45 days, the logs will be dumped.</p> <p>Trigger mechanism: The system checks database logs every hour and automatically saves logs that meet requirements in .csv or .zip format to the /var/share/oss/Product/SMLogLicService/dump directory on the hard disk of a server.</p>	When the space occupied by log files on the hard disk of the server exceeds 1024 MB, the storage duration exceeds 45 days, or the total number of log files exceeds 1000, you can forward logs to the Syslog server. Entry: System > Logs > Log Configuration > Forwarding Configuration.

Viewing Logs by Call Chains

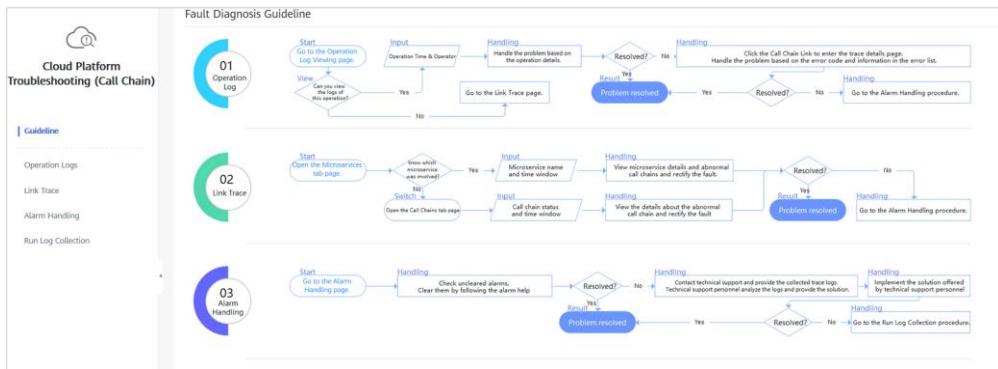
- If no alarm is generated on the management plane, then the fault can be found on the service plane. Log in to ManageOne Maintenance Portal as an administrator and choose **Routine O&M > Troubleshooting > Cloud Platform Troubleshooting**.



- Elasticsearch is used to store data, including mainly call chain data and run logs.

Call Chain

- Application scenarios: troubleshooting on cloud service provisioning failure and cloud service instance operation failure.



Exception Analysis

- Faults can be located and rectified based on the exception information.

- Question:

According to the screenshot on the right, if no fault occurs at the system management layer, list the causes of the error "Volume xxx could not be found".

```

Details
Service Name: cinder-api
Details | Exception Analysis | Raw | Overview

Call Type          function
Call Label         rpc
Name               cinder.proxy.volume.manager.VolumeManager.create_volume
Call Parameter     (<cinder.proxy.volume.manager.VolumeManager object at
                   0x7b3fb1b10>, <cinder.context.RequestContext object at
                   0x7b3fb1b10>).lu volume'
Volume_name_id=None.admin.metadata=>
>attach_status='detached',availability_zone='kvm.type1.bootable'=False.consistencygroup_id=None.created_at=None.deleted_at=None.display_descripti
on=None.display_name='ecs-9ded-volume-0000'.ec2_id=None.encryption_key_id=None.glance_metadata=>
>.host='kvm.type1.hypervisor.global_business.01'.id=147c0622-test-49d3d4f3-4928-21launched_at=None.metadata=[{'tenant': '0'}].migration_status='None.multilatash=False,os_v
endor_volumes_extend=>
>.previous_status=None.project_id=273cb2927e94becb187bcc
cf03f90e.provider_auth=None.provider_geometry='None.prov
ider_id=None.provider_location=None.replication_driver_data=
None.replication_extended_status=None.replication_status='dis
abled.scheduled_at=>

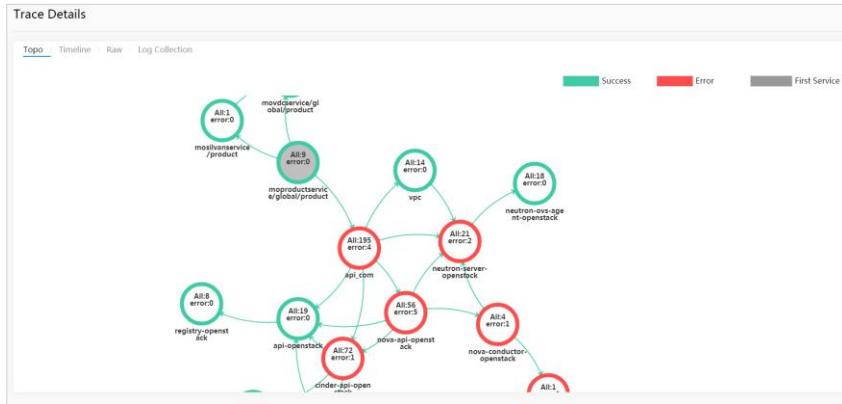
```

OK

- There are many answers to this question. You can check the ECS provisioning process or provision VMs of other images and flavors for comparison.
- Possible fault types:
 - The EVS disk type is incorrect.
 - The CPU model of the associated host group is incorrect.
 - The boot mode of the image is incorrect.
 - The disk format of the image is incorrect.

Viewing Trace Details

- On the displayed **Trace Details** page, locate the faulty node in the call chain.



Viewing Operations or URLs

- Click the link in the **Operation/URL** column of the specified service to view its details.

The screenshot shows a "Trace Details" interface with a "Timeline" tab selected. It displays two entries:

ID	URL	Method	Response Code	Duration	Generate Time
1f8d863e47291fc78c97695c78f5de	http://10.200.16.10.32018/vdc/v3.0/system/operation-log	POST	200	1 ms	

Below this, under "Details", there is a table:

Service Name	Status	Operation/URL	Time Axis
modbservice	●	post http://10.200.16.10.32018/vdc/v3.0/system/operation-log	1 ms
modbservice	●	post http://10.200.16.10.32018/v1.0/MO/system/trace	...

Automated O&M with AutoOps

- AutoOps provides a preset O&M script library for you to perform daily O&M. If the preset library does not meet your requirements, you can customize scripts on a case-by-case basis. The following table lists the top ten common issues compiled by the HUAWEI CLOUD Stack solution maintenance team and second-line engineers. The solution maintenance team has worked out these issues using AutoOps.

Fault Scenario Name	Extreme Scenario Code
FS-01013 Failed to cold migrate a VM	FS-01013
FS-05004 Abnormal Host Status	FS-05004
FS-05006 VM HA Failure	FS-05006
FS-01006 Failed to migrate a VM	FS-01006
FS-01002 Failed to delete a VM	FS-01002
FS-01003 Failed to start a VM	FS-01003
FS-01004 Failed to stop a VM	FS-01004
FS-01005 Failed to restart a VM	FS-01005
FS-01007 Failed to clone a VM	FS-01007
FS-01009 Failed to log in with VNC window	FS-01009

- AutoOps provides preset automated O&M script packages based on scenarios. You can visit <http://support.huawei.com> and download the script packages and then import them to the **Routine O&M > Automated Jobs** page of ManageOne Maintenance Portal. Then, this feature helps O&M personnel automatically collect cloud information and perform common troubleshooting operations, such as fault diagnosis and preliminary demarcation and locating, improving troubleshooting efficiency.
- ManageOne AutomationScripts 8.X.X provides automated O&M script packages of different versions at <http://support.huawei.com> for enterprises and carriers.
 - Enterprise users: <https://support.huawei.com/enterprise/en/cloud-computing/manageone-automationscripts-pid-250623328/software>.
 - Carrier users: <https://support.huawei.com/carrier/productNewOffering?col=product&path=PBI1-21430725/PBI1-23710112/PBI1-21431666/PBI1-21782552/PBI1-250623328&resTab=SW>.
- Note: The following conditions must be met before administrators customize operations if the operations provided on the **Preset Operations** tab page cannot meet the administrator's requirements: AutoOps has been deployed. The product license mode is used. The OperationCenter advanced edition license is available.
- To use AutoOps on the ECS and BMS nodes on the tenant plane, you must have the OperationCenter advanced edition license and AutoOps must be deployed, that is, the ManageOne-Auto node exists.

Importing Preset Scripts to AutoOps

- O&M processes are flexibly orchestrated to standardize O&M scenarios. O&M tasks can be executed immediately or as scheduled and can be expanded to meet growing demands. AutoOps helps O&M administrators effectively reduce labor costs while improving O&M efficiency.

The screenshot shows the 'Orchestration Management' section of the AutoOps interface. On the left, there's a sidebar with 'Automated Jobs' and 'Job Management' sections. The main area is titled 'Orchestration Management' and contains tabs for 'Custom Orchestrations' and 'Preset Orchestrations'. Below these are buttons for 'Create Orchestration', 'Import', 'Export', 'Publish', 'Unpublish', and 'Delete'. A search bar at the top right allows filtering by 'Orchestration Name' and 'Enter a keyword'. The central part of the screen displays a table of 'Preset Orchestrations' with columns: 'Orchestration Name', 'Last Modified', 'Publishing Status', 'Execution Dimension', 'Cloud Service Version', 'Cloud Service ID', 'Last Modified By', and 'Operation'. There are three rows visible in the table, each representing a different preset orchestration.

Orchestration Name	Last Modified	Publishing Status	Execution Dimension	Cloud Service Version	Cloud Service ID	Last Modified By	Operation
[Redacted]	[Redacted]	Published	Task	--	--	admin	Execute View Execution History More
[Redacted]	[Redacted]	Unpublished	Task	--	--	admin	Execute View Execution History More
[Redacted]	[Redacted]	Published	Task	--	--	admin	Execute View Execution History More

- Preset orchestrations are automation scripts provided by the system by default. O&M administrators can select scripts of different scenarios to collect information as required. They can also customize orchestration scripts.

Automatically Collecting HUAWEI CLOUD Stack Information Using AutoOps

- After automation software packages are imported to AutoOps, you can collect information for O&M with a few clicks. For example, to collect the HUAWEI CLOUD Stack overview, locate the HUAWEI CLOUD Stack overview orchestration and click **Execute**.

The screenshot shows the AutoOps interface under the 'Orchestration Management' tab. On the left sidebar, 'Orchestration Management' is selected. The main area displays a table of imported orchestrations:

Orchestration Name	ID	Publishing Status	Execution Dimension	Cloud Service ID	System	Package Name	Package Version	Operation
obs_autoops_region...	Published	Task	OBS	--	--	--	--	Execute View Execution History
obs_autoops_ls_takeo...	Published	Task	OBS	--	--	--	--	Execute View Execution History
obs_autoops_region...	Published	Task	OBS	--	--	--	--	Execute View Execution History
obs_autoops_ls_takeo...	Published	Task	OBS	--	--	--	--	Execute View Execution History

- After the software package for automatically collecting HUAWEI CLOUD Stack overview information is imported, you can run the automation script on the **Orchestration Management** page to collect HUAWEI CLOUD Stack information. The following basic information about all regions managed by ManageOne can be collected: the ESN, region list, deployment model, cloud service usage, resource usage, and compute and storage device list (anonymized). You are advised to collect overview information about the cloud environment to help you understand the environment deployment and service scale.
- Note: The collection result may contain the device list and configuration information, but does not contain any tenant account, password, or internal service information of the instance. Keep the collection result secure to prevent sensitive information leakage.

Automatically Collecting HUAWEI CLOUD Stack Information Using AutoOps

- Collection results can be downloaded to a local PC for you to view the collection details.

Job Name	Orchestration/Operation	Execution Policy	Start Time	Time Required	Job Status	Execution Dimension	Operation
[REDACTED]	[REDACTED]	Periodic	[REDACTED]	16.52s	Successful	—	Download Report Stop
[REDACTED]	[REDACTED]	Periodic	[REDACTED]	44.03s	Failed	Task	Download Report Stop
[REDACTED]	[REDACTED]	Periodic	[REDACTED]	43.77s	Failed	Task	Download Report Stop

- After the execution is successful and the collection is complete, AutoOps provides a compressed package containing the collection results. If the collection fails, you can view the failure cause in the execution details for analysis.

ECS Network Troubleshooting - CloudNetDebug

- Log in to ManageOne Maintenance Portal as an administrator and choose **Routine O&M > Troubleshooting > ECS Network Troubleshooting**.

The screenshot shows the HUAWEI CLOUD Stack Maintenance Portal. The top navigation bar includes links for Home, Monitor, Resource Topology, Routine O&M, O&M Analysis, and System. A user icon and a help symbol are also present. Below the navigation is a search bar and a 'Diagnosis Procedure' link. The main content area is titled 'ECS Network Troubleshooting' with the sub-instruction 'Diagnoses ECS communication problems within the cloud platform.' A table lists two ECS instances: 'ais-config-001_ZDQ283TO' and 'ecs-test01', both marked as 'Running'. To the right of the table is a vertical sidebar with options: Automated Jobs, Logs, Troubleshooting (which is selected and highlighted in blue), Health Check, Centralized Configuration, Backup Management, Cloud Platform Troubleshooting, ECS Network Troubleshooting (selected and highlighted in blue), ECS Storage Troubleshooting, and ManageOne Toolkit.

120 Huawei Confidential



- ECS network disconnection on the cloud platform can be identified by performing a probe task and capturing service flow packets.
- Symptom**
 - Tenant service and network traffic is interrupted.
 - Tenant service traffic is intermittently interrupted, and packet loss occurs on the network.
- Notes:**
 - The ECS network troubleshooting is unavailable for HCS Online.
 - The ECS network troubleshooting in the HUAWEI CLOUD Stack scenario supports only FusionSphere OpenStack resource pools.

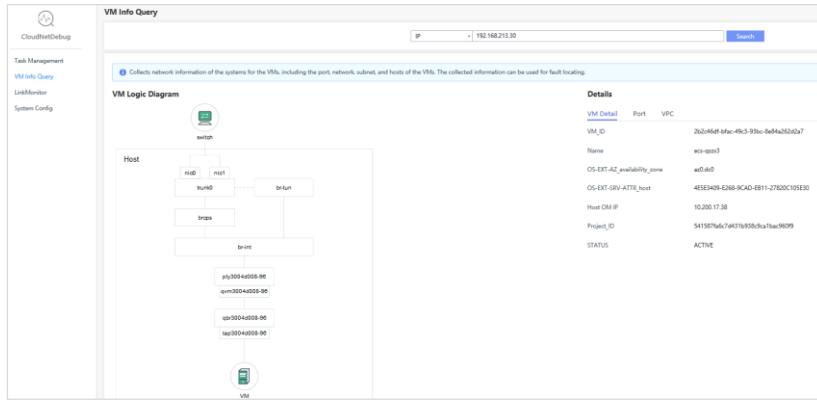
Abnormal Communication Between Two VMs

- A customer reported that the traffic between two service VMs in the cloud data center was abnormal. The SCP file transmission between VM1 and VM2 was unstable. The IP address of VM1 was 192.168.10.221, the name of VM1 was vm_yc, the IP address of VM2 was 192.168.20.31, and the name of VM2 was vm_test2. The source port of VM1 was 5339, the destination port of VM2 was 22, and the protocol type was TCP.
- **How do I use CloudNetDebug for troubleshooting?**



Step 1: Query the VM Status

- In CloudNetDebug, you can use the VM IP address or ID to query VM information for fault locating.



Step 2: Perform Probe Tests to Check Links

- Create a probe task.

The screenshot shows the 'Task Management' interface with the following details:

- Task Name:** test
- Protocol Type:** TCP
- Source IP:** 192.168.213.30
- Source Port:** 21
- Destination IP:** 192.168.213.49
- Destination Port:** 21
- Probe Rate (PPS):** 2
- Probe Count:** 100

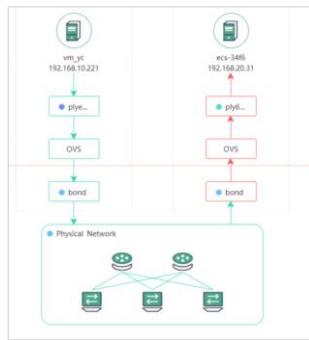
123 Huawei Confidential



- After the probe information is specified, click **Next** to check the scenario. The possible causes are as follows:
 - 1. The probe traffic belongs to the VPC L2 or L3.
 - 2. The probe traffic belongs to the VPC peering.
 - 3. If the source and destination IP addresses belong to different VPCs but no VPC peering connection is configured between them, the traffic is invalid.
- If result 3 is obtained, the traffic between the two VMs is invalid and cannot be forwarded. In this case, you can determine the cause and do not need to perform the following steps.
- If result 1 or result 2 is obtained, create a probe task for VPC L3 traffic.

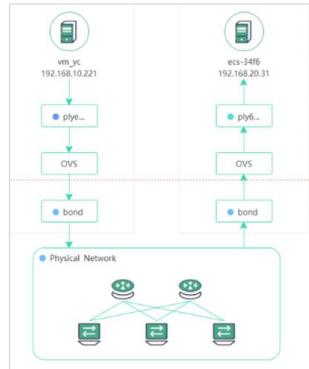
Step 3: Analyze Probe Test Results If a Fault Occurs

- As shown in the figure, packet loss occurred on a host. Its bond port received packets, but its Ply bridge did not receive packets. It was suspected that the OVS was faulty. In this case, collect both OVS and flow table information of br-int and br-tun bridges for further fault locating.



Step 4: Analyze Probe Test Results If No Fault Occurs

- If no problem is found during the probe test, you need to capture packets to further check whether applications are normal.



Step 5: Capture Packets to Locate Application Faults

- Create a packet capture task.

The screenshot shows the 'Task Management' interface with the 'Basic Information' tab selected. A task named 'task' is being configured. The 'Protocol Type' is set to 'ANY'. Under 'Packet Details', the 'Internal IP' is checked and set to '192.168.213.10'. The 'Source IP' is set to '192.168.213.10' and the 'Source ID' is set to '2601dead-beef-c000-4'. The 'Destination IP' is set to '100.200.17.43' and the 'Destination Port' is set to 'Enter an integer from 1 to 65535'. The 'Bidirectional' option is selected. The 'Packet Capture Duration' is set to '1 minute', 'Maximum Number Of Packets' is set to '10000', and 'Packet Capture File Size (MB)' is set to '50'. A note at the bottom states: 'Tip: The CPU usage of the packet capture tool at the packet capture point is limited by the qgroup. When the packet transmission rate is 20,000 pps, the maximum CPU usage of the packet capture tool is referenced the CPU usage of the EulerOS system is less than 20%, and the CPU usage of the OSSE system is less than 2%.' There are 'Next' and 'Cancel' buttons at the bottom.

Step 6: Capture Packets to Locate Application Faults

- Analyze the scenario and select the packet capture point.

The screenshot shows the 'Task Management' interface with the 'CloudNetDebug' tab selected. In the 'Scenario Analysis' section, the task scenario is set to 'Network Service Capture'. Under 'Capture Point Selection', there is a note: 'The number of points that user selected in a task cannot be greater than 10.' Below this, a table lists five potential capture points:

ID	IP
1	Virtual Network Node
2	Virtual Network Node
3	Virtual Network Node
4	Virtual Network Node
5	Virtual Network Node

At the bottom of the interface are 'Previous', 'Delete', and 'Cancel' buttons.

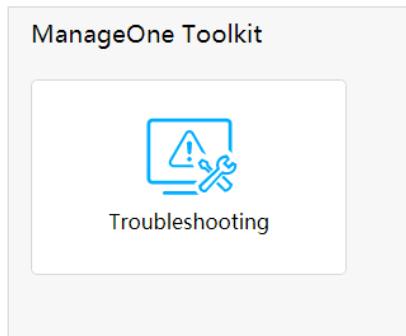
Step 7: Capture Packets to Locate Application Faults

- Download the packet capture file, use Wireshark to open the file, and perform the following operations:
 - Check whether packets are captured on the tap port of the source host. If this happens, the packets are sent from the source VM.
 - Check whether packets are captured on the tap port of the destination host. If this happens, the packets have been sent to the destination VM.
 - If the fault persists, use the packet capture file to analyze the application interaction packets and check whether the service interaction between the source and destination VMs is normal.

HOST(6.24.53.169)	<input type="checkbox"/> trunk2_C10B42C1-EFD0-D8A7-E811-C6ACF6AFDFAD_6fb9f6d-75b8-43f3-9990-007ab7eaefc0_24	
	<input type="checkbox"/> tapeBf9d0b6-4a_C10B42C1-EFD0-D8A7-E811-C6ACF6AFDFAD_6fb9f6d-75b8-43f3-9990-007ab7eaefc0_24	
	<input type="checkbox"/> tunnel_B2598981-A719-E811-B65C-785860655392_d4bac3d-2a99-4c73-8290-265b22a8751c_bearing_24	
HOST(6.24.53.137)	<input type="checkbox"/> tap6ca9cb5-69_B2598981-A719-E811-B65C-785860655392_d4bac3d-2a99-4c73-8290-265b22a8751c_24	

ManageOne Toolkit

- ManageOne Toolkit centrally manages and maintains common tools to improve self-service O&M capabilities. Common tools are used to start and stop one or more application instances and rectify common faults.



- In HUAWEI CLOUD Stack 8.1.1, start and stop operations are not supported.

ManageOne Toolkit - Troubleshooting

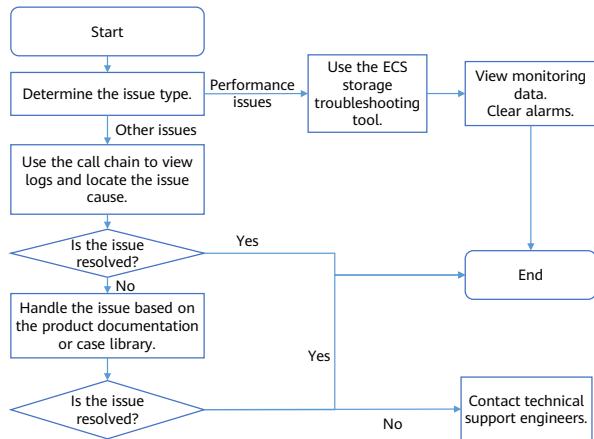
- During routine maintenance, if maintenance operations (such as data query, index deletion, index configuration query, full index query, cluster information query, abnormal index query, forcible shard recovery, and unassigned shard query) on the Elasticsearch data platform and third-party system access user authentication need to be performed, administrators can use the troubleshooting tool of the ManageOne toolkit to search for cases by the case name, and execute the cases to handle faults quickly.

The screenshot shows the 'ManageOne Toolkit > Troubleshooting' page. At the top left are 'Import Case' and 'Refresh' buttons. On the right is a search bar with placeholder text 'Enter a case name.' and a magnifying glass icon. Below the search bar is a table with columns: 'Case Name', 'Description', 'Execution Status', 'Last Execution Time', and 'Operation'. The table contains four rows of data. The 'Operation' column for each row has three buttons: 'Execute', 'Delete', and 'View Details'.

Case Name	Description	Execution Status	Last Execution Time	Operation
elasticsearch_index_recover	Recover index	--	--	Execute Delete View Details
elasticsearch_index_delete	Delete index	--	--	Execute Delete View Details
elasticsearch_index_query	Query index	--	--	Execute Delete View Details

ECS Storage Troubleshooting

- Symptom
 - The I/O read/write speed of EVS disks attached to ECSs was slow, and VM services were affected.
- Possible causes
 - The ECS was incorrectly configured.
 - The storage device was faulty or the performance of the storage device was insufficient.
 - The storage link was faulty.



- For details about how to use the call chain to view logs, see the log management part in this course. This part describes how to use the ECS storage troubleshooting tool to analyze ECS performance problems.

ECS Storage Troubleshooting: Performance Issues (1)

- Log in to ManageOne Maintenance Portal as an administrator and choose **Routine O&M > Troubleshooting > ECS Storage Troubleshooting**.

Name	Status	OS Version	Created	Elastic IP Address	Region	VDC Name	Operation
as-config-001_20Q081370	Running	EulerOS 2.5 64bit	2023-08-10 10:00:00	10.0.0.10	hangzhou	mostest	Diagnose
ecs-test01	Running	CentOS 7.8 64bit	2023-08-10 10:00:00	10.0.0.11	hangzhou	HCI-E-Anhui	Diagnose

ECS Storage Troubleshooting: Performance Issues (2)

- View ECS details and alarm information.

ECS Storage Troubleshooting [Back to ECS List](#) Diagnosis Procedure

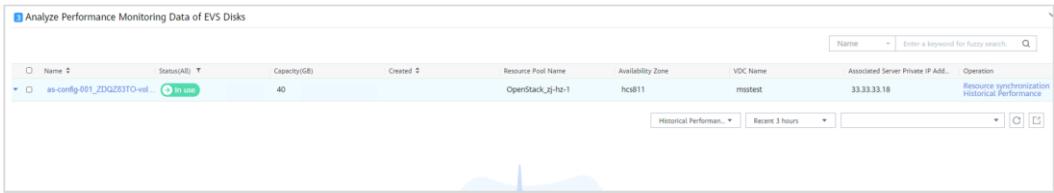
Check ECS Status

as-config-001_ZDQZ83TO Running

Original ID: c3f1191a-b755-4077-be07-7cde... | Created: 2023-07-10T10:00:00 | Private IP Address: 33.33.33.18 | Elastic IP Address: -- | Region: hangzhou
Resource Pool: OpenStack_zj-hs-1 | Availability Zone: hcs811 | Host Aggregator: kvm_group02 | Host Machine: Computer10 | Virtual Private Cloud: vpc-7db8

ECS Storage Troubleshooting: Performance Issues (3)

- Analyze the EVS disk performance monitoring data for fault diagnosis.



Quiz

1. (Multiple-answer question) Which of the following items are parts of ManageOne Maintenance Portal?
 - A. The collection & control layer
 - B. The platform layer
 - C. Maintenance scenarios
 - D. The application layer
2. (Multiple-answer question) If the HUAWEI CLOUD Stack platform needs to be upgraded, which of the following tools can be used to perform a comprehensive pre-upgrade check on the platform, including the storage backend system?
 - A. FusionCare
 - B. SmartKit
 - C. ManageOne toolkit
 - D. CloudNetDebug

- Answers:

- 1. ABC
 - 2. AB

Summary

- This course described the core capabilities of HUAWEI CLOUD Stack OperationCenter and the principles and capabilities of the collection and control layer, platform layer, and O&M scenarios.

Recommendations

- Huawei Talent:
 - <https://e.huawei.com/en/talent/portal/#/>
- Huawei Certification:
 - <https://forum.huawei.com/enterprise/en/forum-813.html>

Acronyms

Acronym	Full Name	Description
OC	OperationCenter	OperationCenter is the only entry for ManageOne O&M management. It can manage and monitor cloud services, tenant resources, and infrastructures (compute, storage, and network devices) that the cloud services depend on.
CMDB	Configuration Management Database	Resource Management (CMDB) is used to store and manage a multitude of data about devices and systems in the enterprise IT architecture. It ensures data accuracy, timeliness, and effectiveness based on relevant processes, and provides unified O&M resource configuration data, implementing information sharing and maximizing the value of configuration information.
VM	Virtual Machine	A virtual machine (VM) is the virtualization/emulation of a computer system, which runs in an independent environment and provides functionality of a physical computer.
ECS	Elastic Cloud Server	Elastic Cloud Servers (ECSs) provide scalable, on-demand compute resources, which can be obtained by yourself at any time on the cloud.
VPC	Virtual Private Cloud	A Virtual Private Cloud (VPC) provisions logically isolated sections of a public cloud in order to provide a secure virtual private environment.
VDC	Virtual Data Center	A Virtual Data Center (VDC) is a set of cloud resources that support a business with cloud computing capabilities. A VDC can abstract resources from physical resources using virtualization, dynamically allocate and schedule resources, and implement the automatic deployment of data centers.
EIP	Elastic IP Address	An Elastic IP Address (EIP) enables your cloud resources to communicate with the Internet using static public IP addresses and scalable bandwidths.

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and
organization for a fully connected,
intelligent world.

Copyright©2022 Huawei Technologies Co., Ltd.
All Rights Reserved.

The information in this document may contain predictive
statements including, without limitation, statements regarding
the future financial and operating results, future product
portfolio, new technology, etc. There are a number of factors that
could cause actual results and developments to differ materially
from those expressed or implied in the predictive statements.
Therefore, such information is provided for reference purpose
only and constitutes neither an offer nor an acceptance. Huawei
may change the information at any time without notice.

