Cloud Operations Center

Service Overview

Issue 01

Date 2025-07-07

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei Cloud and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Cloud Computing Technologies Co., Ltd.

Address: Huawei Cloud Data Center Jiaoxinggong Road
Qianzhong Avenue
Gui'an New District
Gui Zhou 550029
People's Republic of China

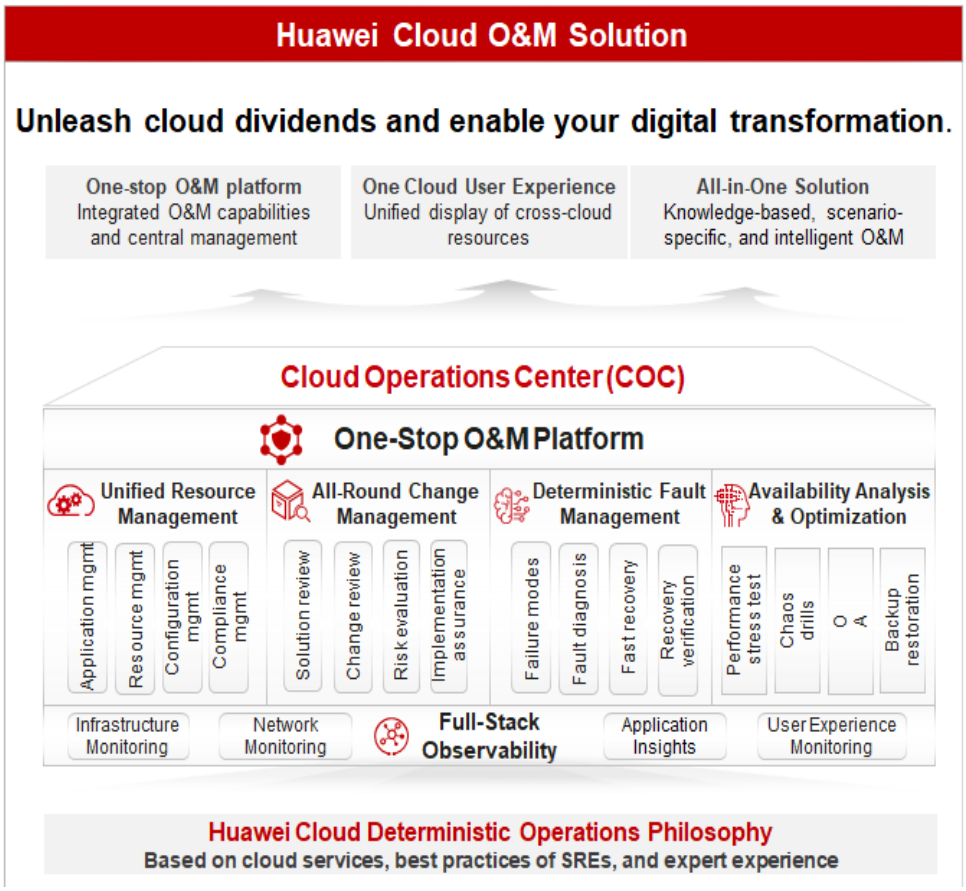
Website: https://www.huaweicloud.com/intl/en-us/

Contents

1 What Is COC?

Cloud Operations Center (COC) is a secure and efficient O&M platform, offering one-stop, AI-powered solutions for all your centralized O&M needs. It encompasses Huawei Cloud deterministic operations scenarios and features essential functionalities such as fault management, batch O&M, and chaos drills, to improve cloud O&M efficiency while ensuring security compliance.

Figure 1-1 COC service overview



Unified Resource Management

- Application management: provides the capability of modeling the association between applications and resources to fulfill your requirements in centralized cloud resource management and cost reduction management.
- Resource management: synchronizes and manages the resource instances used on various cloud platforms to build a resource O&M capability foundation.
- Configuration management: manages applications and resources, and centrally monitors their parameter configurations throughout their lifecycles.
- Compliance management: provides batch patch scanning and repair capabilities for resource O&M, ensuring both security compliance and efficiency.

Comprehensive Change Management

- Solution review: enables Standard Operating Procedure (SOP) for change solutions, clarifying and electronizing change solutions and archiving them after review. Rules and processes can be decoupled to ensure that a change execution process is correct and that the change solution can be accumulated.
- Change review: reviews change tickets according to the preset review process to ensure the reliability, efficiency, and process compliance of change solutions.
- Risk assessment: manages the changes based on scenario rules, process rules, and business rules to identify and prevent change risks. The change calendar is used to identify change conflicts and reduce change risks caused by change dependencies between services.
- Implementation assurance: presets change solutions, executes and standardizes change steps, enables change operation observation, and ensures timely handling of change exceptions, delivering controllable, visible, and manageable change processes.

Deterministic Fault Management

- Unified incident center: provides an E2E and standard incident handling mechanism, covering incident discovery, incident handling, recovery verification, and continuous improvement.
- War room and fault backtracking capabilities: triggers war room requests intelligently for live-network incidents, shortening troubleshooting time. In addition, you can observe the troubleshooting progress in real time from the command center. Fault backtracking facilitates issue summary and experience accumulation, preventing issues from recurring and shortening the MTTR.
- Response plans: enables you to develop response plans for known faults and handle deterministic issues using the contingency plan automation mechanism.
- Failure modes: leverages professional risk analysis methods and expert knowledge bases to accumulate a failure mode base, helping you analyze potential risks of cloud applications and pass on O&M experience.

Resilience Center Optimization

- Full-lifecycle risk management: encompasses risk management in both application deployment and running scenarios throughout the lifecycles of applications and resources, serving you based on years of dynamic risk management experience accumulated on Huawei Cloud.
- Proactive O&M: promotes the quality and resilience of your key services through proactive O&M methods, including performance pressure tests, emergency drills/chaotic engineering, and resilience evaluation.
- Rich fault drill tools: uses over 50 built-in drill attack tools based on Huawei Cloud best practices, enabling you to simulate complex and diversified service exception scenarios and develop countermeasures.
- Application HA improvement: The Production Readiness Review (PRR) feature leverages the SREs' best practices on cloud application rollout review and provides online review e-flows and review items, enhancing application High availability (HA).

Access Methods

You can access COC through the web-based management console or HTTPS-based application programming interfaces (APIs).

- APIs

  Use this method to access COC if you need to integrate COC into a third-party system for secondary development. For details, see ***Cloud Operations Center (COC) API Reference***.

- Management console

  Use the management console if you do not need to integrate COC with a third-party system.

  If you have registered an account, log in to the **management console** and choose COC on the home page. If you have not registered an account, register one by referring to **Signing Up for a HUAWEI ID and Enabling Huawei Cloud Services**.

2 Benefits

One-Stop O&M Platform

- Centralized management and O&M
- Synergized ITSM, ITOM, and expert services
- Seamless operations without platform switching

All-in-One Solution

- Atomic O&M capabilities
- Tailored solutions based on the accumulated experience of Huawei Cloud O&M specialists
- Simplified O&M based on best practices derived from secure production, CloudOpsBrain, and fault management

"One Cloud" User Experience

- Full-spectrum resource management, covering Huawei Cloud and customer IDC scenarios
- Multi-perspective data displays for data value mining and informed decision-making
- Cloud-based O&M capabilities extend to customer IDCs and multi-cloud scenarios for high O&M efficiency

3 Application Scenarios

O&M BI Dashboard

The dedicated O&M BI dashboard caters to various O&M roles, aiding in optimization, insight generation, and decision-making.

Rich metrics: COC provides over 30 preset O&M metrics, delivering insights into your cloud resources across seven-perspective BI dashboards and a comprehensive enterprise-grade O&M sandbox. The O&M sandbox and the BI dashboards help you understand your service O&M situation from both bird's eye and ground level views in real time.

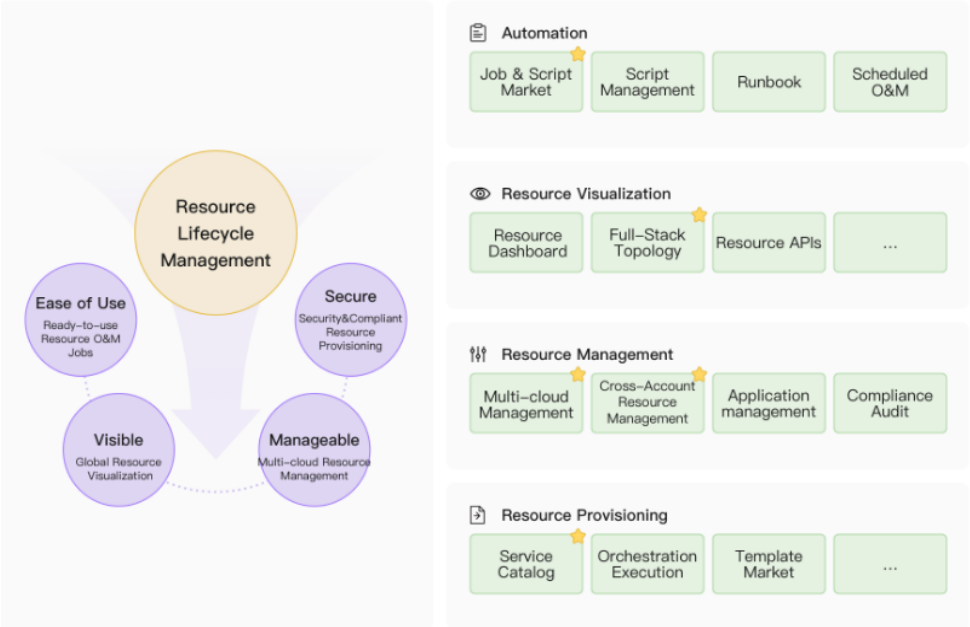
Figure 3-1 O&M BI dashboard

Full-Lifecycle Resource Management

Full-lifecycle resource management is available, and includes actions such as resource defining, requesting, provisioning, O&M, changing, configuration, renewal, and recycling; building a unified resource management center.

- Full-lifecycle management: eliminates breakpoints across the entire user resource management journey, ensuring smooth user resource management and efficient O&M.
- Resource management center: enables visualized management of your resources from a global perspective, and supports multi-cloud and cross-account centralized O&M.

Figure 3-2 Full-lifecycle resource management

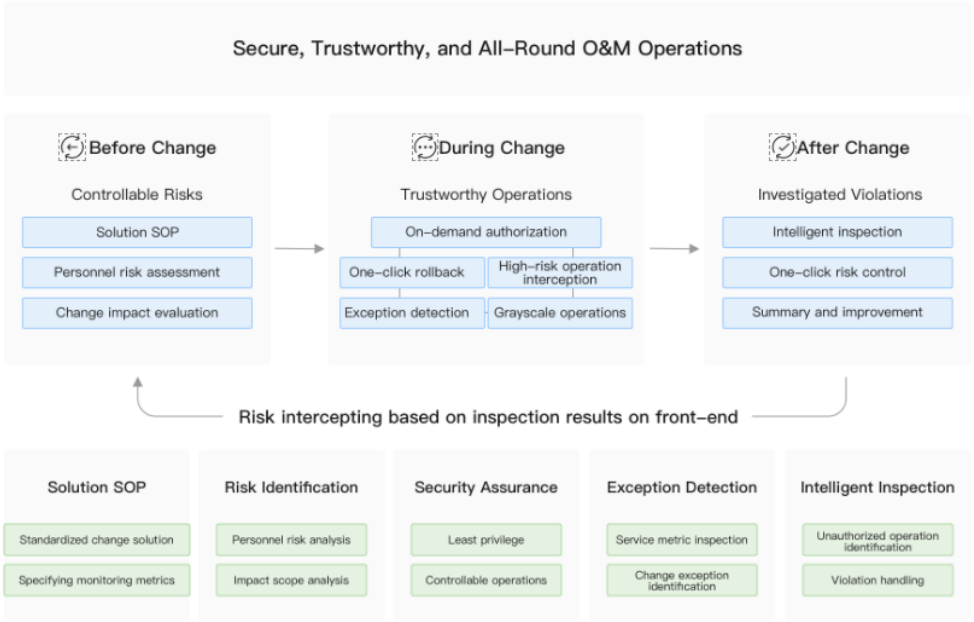


Change Risk Control and Operations Trustworthiness

Management and control models that integrate Huawei SRE best practices in secure production provide you with trustworthy, stable, and reliable O&M capabilities.

- All-round operations trustworthiness ensures operational security before, during, and after changes, is supported by personnel risk assessment capabilities, and offers high-risk command alerts, and automated inspection.
- AI-powered risk assessment: The intelligent interception algorithm for high-risk commands is used to mitigate operation risks.

Figure 3-3 Change risk control and operations trustworthiness

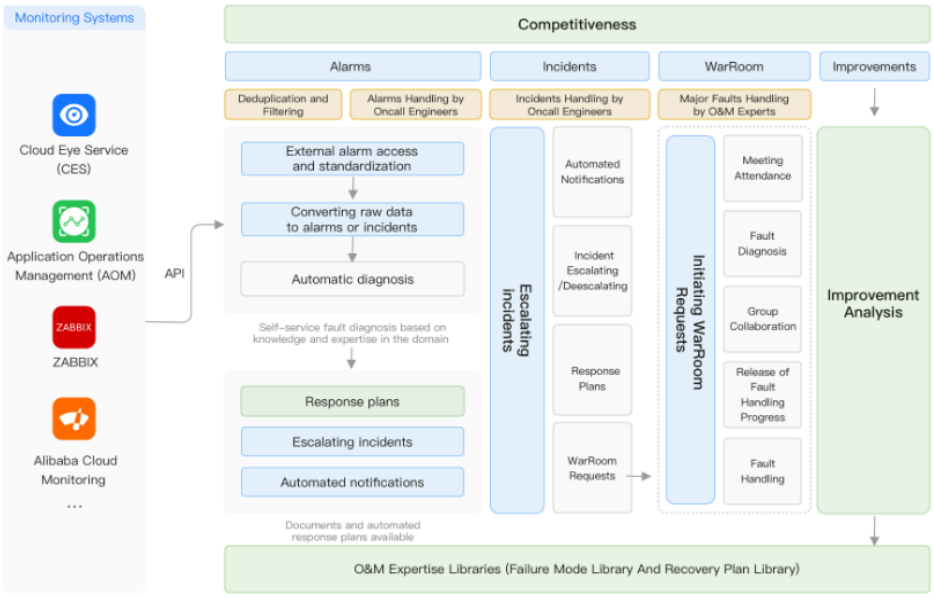


Standardized Fault Management

The standardized fault management process and war room enhance efficient fault synergy and rapid fault recovery.

- Standard process: provides a standardized troubleshooting process on Huawei Cloud. Bolstered by response plans and the war room-based synergy of O&M engineers, R&D teams, and other personnel, this standardized process helps you handle faults encountered with ease.
- O&M knowledge base: enables the swift handling of faults. A rich repository of O&M knowledge, derived from handling historical faults and the accumulation of experience in handling unknown faults, increases efficiency during fault handling process.

Figure 3-4 Standardized fault management

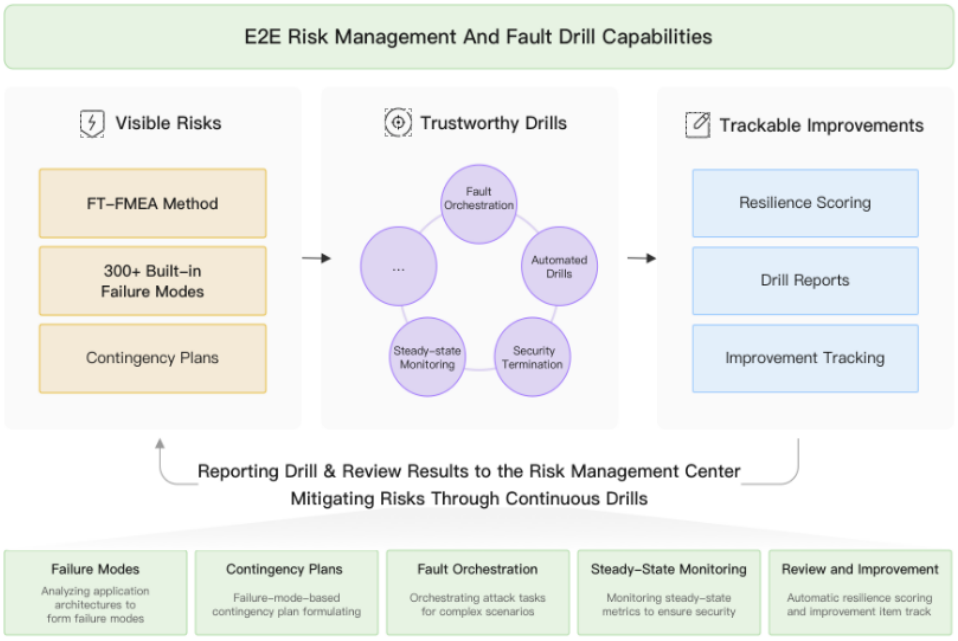


Intelligent Chaos Drills

Full-stack chaos engineering solutions enable you to quickly evaluate the potential resilience risks of applications and continuously monitor application architectures.

- E2E chaos engineering solutions: provide E2E chaos drill capabilities based on your service scenarios from four dimensions: risk analysis, contingency plans, drill execution, and drill review.
- Failure mode library: introduces the methodology of analyzing fault scenarios for DR, and leverages Huawei Cloud SREs' years of accumulated experience in fault handling through the failure mode library.

Figure 3-5 Intelligent chaos drills



4 Functions

This section describes the main functions of Cloud Operations Center (COC).

Overview

The COC overview page contains multiple modules, including the O&M probability, resource dashboard, resource monitoring, security overview, quick configuration center, and O&M BI. You can view and perform operations on work items with ease on the overview page, enjoying simplified and highly efficient O&M. For more information, see **Overview**.

Resource Management

In the Information Technology Infrastructure Library (ITIL) process, the infrastructure resource-oriented management approach can cause problems such as data isolation and information inconsistency between O&M services. The resource management module of COC can centrally manage core resources of Huawei Cloud and other clouds and offline IDC resources, quickly providing accurate and consistent resource configuration data for features such as change management and batch O&M. COC leverages the following mechanisms to implement unified resource management:

- Resource discovery and identification: COC can automatically discover and identify offline resources of Huawei Cloud, peer vendor clouds, and IDCs, and manage them centrally.
- Resource monitoring and management: Through a unified monitoring page, O&M engineers monitor resource usage in real time and dynamically adjust resource usage.
- Data synchronization and consistency: COC supports data synchronization to ensure data consistency and accuracy between O&M services.

  For more information, see **Resource Management Overview**.

Application Management

COC provides an application-centric resource management view that is bolstered by the capability of modeling the association between applications and resources. By using this feature, you can manage your resources by application, region, resource group, or resource model, query resources in a resource list by tag, and

install the UniAgent components. You can use the application management function of COC to manage resources by group and manage the relationship between cloud service objects and applications. The management scope includes core resources of Huawei Cloud, other clouds (currently, Alibaba Cloud, AWS, and Azure are supported), and on-premises IDC resources, provides unified and reliable resource group information for functions such as chaos drills, change management, and account management.

For more information, see **Application Management Overview**.

Batch Resource Processing

COC delivers the batch resource operation capability that allows you to centrally manage multiple types of resources, such as Elastic Cloud Servers (ECSs), Relational Database Service (RDS) DB instances, FlexusL instances, and Bare Metal Servers (BMSs). It supports a variety of operation scenarios, including batch start, stop, and restart, OS reinstallation, and OS change, meeting resource operation requirements in different O&M phases. For more information, see **Batch Resource Processing Overview**.

Script Management

The script management function of COC is a core tool that helps you implement O&M automation. It provides efficient and accurate solutions for complex or repetitive O&M tasks. With script execution tools, you do not need to perform a large number of complex manual operations, configure devices one by one, and repeatedly execute tasks. Instead, you can create scripts to complete tasks at a time. This greatly shortens the task handling time and effectively avoids human misoperations, fundamentally improves the efficiency and accuracy of O&M. Create, modify, and delete scripts, and execute your own and public scripts on VMs For more information, see **Script Management Overview**.

Job Management

Job management is a core tool for operation automation. It orchestrates atomic actions (such as restarting instances and executing scripts) in a structured process to form a reusable, manageable, and standard operation set, which is called a job. The core capabilities include job lifecycle management and cross-instance batch execution. It aims to help you efficiently complete repeated operations, reduce manual error risks, and implement standardized and version-based management of operation processes.

For more information, see **Job Management Overview**.

Scheduled O&M

Scheduled O&M is an important module of COC for automatic scheduling of O&M tasks. This module clearly displays scheduled task details (such as the task name, type, execution time, and status) and task execution records (including the execution time, result, and logs). You can create scheduled tasks and manage them, such as modifying, pausing, enabling, and deleting tasks.

For more information, see **Scheduled O&M Overview**.

Account Management

You can centrally manage human-machine accounts of Huawei Cloud ECSs, RDS DB instances, GaussDB instances, and middleware. We collect multiple accounts in one place to avoid risks like forgetting passwords or having them leaked. You can get host passwords using account management. With security controls, you can log in to Linux hosts and run commands without entering passwords.

For more information, see **Account Management Overview**.

Parameter Center

The parameter center is developed to provide you with secure and reliable parameter storage and full-lifecycle management and control capabilities through centralized and standardized management, resolving pain points such as scattered data, security risks, and complex reference. Manage parameters throughout the whole service lifecycle in regions to continuously monitor parameter correctness and consistency. You can quickly reference O&M scenarios such as job orchestration.

For more information, see **Parameter Center Overview**.

OS Version Change

OS version change is a functional module that focuses on host OS upgrade management in COC. It provides convenient and efficient OS version change capabilities for hosts. With this function, you can easily create an OS version change task to upgrade multiple hosts in batches, greatly improving the OS upgrade efficiency.

For more information, see **OS Version Change Overview**.

Fault Management

COC fault management provides you with the capabilities of quick fault demarcation, locating, and recovery. It supports ingestion of alarms from multiple sources. COC aggregates raw alarms and performs noise reduction on the alarms, and then convert corresponding alarms to incidents or aggregated alarms. Faults reported by the alarms or incidents will be quickly demarcated through the application topology diagnosis tool, or war rooms, and then be swiftly rectified based on online response plans with the MTTR shortened. All faults and their handling processes will be reviewed for service improvement. In addition, it continuously accumulates the fault management O&M knowledge base and improves the risk resistance capability.

Table 4-1 Fault management functions

Module	Description	Operation Guide
Alarm Management	You can use collect, aggregate, and convert alarm data, and configure and manage alarm rules.	**Alarm Management**
Incident Management	The incident management module manages all incidents of applications, including incident acceptance and rejection, ticket conversion, processing, and closing. Incidents can be generated based on alarm conversion rules, or created by users or based on alarms.	**Incident Management**
War Room	When there is a major or critical fault, a war room can be set up to quickly convene experts such as fault analysis members and application SRE engineers to rectify the fault. This improves the efficiency of collaborative communication, fault diagnosis and demarcation, and fault handling. War rooms also enable you to quickly detect and respond to incidents, shortening the MTTR.	**War Room**
Improvement Ticket Management	Improvement ticket management is the process of tracking and closing improvement tickets for product, O&M, or management issues found during incident or war room handling, or during drills.	**Improvement Management**
Issue Ticket Management	Issue management is the process of first discovering issues such as product function defects and poor performance issues during the use of software products, and then recording the fault root causes and resolving the issues during the application. Setting up war rooms is mainly used to reduce the number of product or service faults on the live network. This improves the overall service quality, promote the continuous improvement of product or application quality, and prevent issues from recurring.	**Problem Management**
Alarm Conversion Rules	Alarm conversion rules suppress, reduce noise, deduplicate, and distribute routes for all received raw alarms. Vertical suppression and horizontal convergence of multiple monitoring sources are supported for multi-dimensional noise reduction. When configuring an incident forwarding rule, you can specify default objects for assigning incidents and configure notification policy for precise accurate notification.	**Conversion Rules**

Module	Description	Operation Guide
Data Source Management	Data source management aims to provide you with an easy and quick way to interconnect COC with existing and third-party monitoring systems, such as Huawei Cloud Eye, AOM, and other monitoring tools. The core value is to collect alarm information scattered in different monitoring systems of the same service centrally to implement centralized management, preventing monitoring blind spots and complex management caused by scattered alarm data on different platforms.	Access Integration

Change Management

Change management is the core module for ensuring secure and orderly O&M operations. Its core function is to build safe production capabilities covering the entire lifecycle of O&M operations. This module uses systematic process design and multi-level risk control mechanisms to accurately identify potential risks and develop countermeasures in advance, effectively reducing risks during change operations, provides solid assurance for the stable running of the O&M system. This module manages the core services of the change process. It integrates key capabilities such as change calendar, change center, change configuration, and change control. These capabilities work together to form a closed-loop change management system including planning, execution, configuration, and monitoring.

For more information, see **Change Management Overview**.

Chaos Drills

COC allows you to perform automatic chaos drills covering from risk identification, emergency plan management, fault injection, and review and improvement. Based on years of best practices of Huawei Cloud SRE in chaos drills, customers can proactively identify, mitigate, and verify risks of cloud applications, improving the resilience of cloud applications.

For more information, see **Chaos Drill Overview**.

To-Do Center

The to-do center is used to record and track daily to-do tasks to remind you of the tasks.

In the COC to-do center, you can create a to-do task and assign it to a specified engineer for processing. You can set the deadline and enter the recommended solution for the to-do task. After the to-do task is created, the owner can be notified by SMS messages or emails.

For more information, see **To-Do Center Overview**.

Personnel Management

You can centrally manage O&M engineers on COC using this feature. On the page, you can manage users who log in through different login methods, including IAM

users, IAM federated users, and IAM Identity Center users. Data on the target page is the basic user data of COC and is available for authorized users to use the basic functional modules such as to-do task creation, scheduled O&M, notification management, and incident center.

For more information, see **Personnel Management Overview**.

Shift Management

You can customize a unified, multi-dimensional, and multi-form personnel management system on COC. This function is widely used in scenarios where owners are involved, such as service review and service ticket transfer. You can manage shift scenarios on the shift schedule management page and add personnel on the **O&M Personnel Management** page to shift schedules. Manage O&M personnel centrally, from multiple dimensions, in different forms, or based on your other custom requirements. You can also create shift scenarios and roles and add personnel managed on the **Personnel Management** page to the scenarios and roles as required.

- When you need to configure or obtain O&M engineers in a shift, go to the shift management page to configure or query a shift.
- Created shifts can be directly used to configure personnel parameters when using O&M service modules such as alarm conversion rules, incident center, automated O&M, notification management, and change ticket management.

  For more information, see **Shift Management Overview**.

Notification Management

You can use notification templates for changes, incidents, issues, and alarms with various notification modes in different service scenarios and process phases. You can subscribe to notifications as required to avoid missing important information. When an incident ticket, issue ticket, alarm ticket, or change ticket is generated, the corresponding notification rules match the information about the incident, issue, alarm, or change are matched. Then, the system parses and obtains the recipients, the notification content, and notification method, and finally send the corresponding notifications. Notification modes are classified into incident, issue, change, and alarm notifications.

For more information, see **Notification Management**.

Mobile Application Management

You can manage configurations of third-party mobile apps and configure parameters for a war room when an incident requires the war room on a third-party mobile app. For more information, see **Mobile App Management**.

SLA Management

Service Level Agreement (SLA) is generally used to measure the service quality in the industry. It defines the quality standard, delivery method, and acceptable performance level of a service. The SLA management function of COC provides the service ticket validity period management capability. When a service ticket triggers an SLA rule, COC records the SLA trigger details for the service ticket and notifies

the corresponding users to follow up and handle the service ticket in a timely manner.

For more information, see **SLA Management**.

SLO Management

As a core performance metric widely recognized in the industry, service level objective (SLO) is a key quantitative standard for measuring the quality of services and applications. The core value of the SLO is to provide a unified and measurable service quality evaluation benchmark for service and technical teams, ensuring that service capabilities are aligned with service requirements.

For more information, see **SLO Management**.

Process Management

You can customize the incident process, issue process, and change scenario. You can use the customized process management configuration for the fault management and change management modules as needed.

For more information, see **Process Management**.

Report Subscription

The report subscription function is used by O&M personnel to collect O&M data and report service statuses. It provides automatic and periodic O&M data statistics reports. This feature addresses the issues of inefficiency in traditional manual collection and sorting of O&M data, as well as the high labor costs associated with statistical analysis.

The report data comes from the O&M BI dashboards delivered by COC. When creating a subscription report, you can set subscription parameters such as the report sending frequency, report content, and recipients. Then, recipients can periodically receive the subscribed report in their email addresses. You can also view and download historical reports on the report subscription page.

For more information, see **Subscribing to a Report**.

5 Security

5.1 Shared Responsibilities

Huawei guarantees that its commitment to cyber security will never be outweighed by the consideration of commercial interests. To cope with emerging cloud security challenges and pervasive cloud security threats and attacks, Huawei Cloud builds a comprehensive cloud service security assurance system for different regions and industries based on Huawei's unique software and hardware advantages, laws, regulations, industry standards, and security ecosystem.

Unlike traditional on-premises data centers, cloud computing separates operators from users. This approach not only enhances flexibility and control for users but also greatly reduces their operational workload. For this reason, cloud security cannot be fully ensured by one party. Cloud security requires joint efforts of Huawei Cloud and you, as shown in **Figure 5-1**.

- **Huawei Cloud**: Huawei Cloud is responsible for infrastructure security, including security and compliance, regardless of cloud service categories. The infrastructure consists of physical data centers, which house compute, storage, and network resources, virtualization platforms, and cloud services Huawei Cloud provides for you. In PaaS and SaaS scenarios, Huawei Cloud is responsible for security settings, vulnerability remediation, security controls, and detecting any intrusions into the network where your services or Huawei Cloud components are deployed.
- **Customer**: As our customer, your ownership of and control over your data assets will not be transferred under any cloud service category. Without your explicit authorization, Huawei Cloud will not use or monetize your data, but you are responsible for protecting your data and managing identities and access. This includes ensuring the legal compliance of your data on the cloud, using secure credentials (such as strong passwords and multi-factor authentication), and properly managing those credentials, as well as monitoring and managing content security, looking out for abnormal account behavior, and responding to it, when discovered, in a timely manner.

Figure 5-1 Huawei Cloud shared security responsibility model

Cloud security responsibilities are determined by control, visibility, and availability. When you migrate services to the cloud, assets, such as devices, hardware, software, media, VMs, OSs, and data, are controlled by both you and Huawei Cloud. This means that your responsibilities depend on the cloud services you select. As shown in **Figure 5-1**, customers can select different cloud service types (such as IaaS, PaaS, and SaaS services) based on their service requirements. As control over components varies across different cloud service categories, the responsibilities are shared differently.

- In on-premises scenarios, customers have full control over assets such as hardware, software, and data, so tenants are responsible for the security of all components.
- In IaaS scenarios, customers have control over all components except the underlying infrastructure. So, customers are responsible for securing these components. This includes ensuring the legal compliance of the applications, maintaining development and design security, and managing vulnerability remediation, configuration security, and security controls for related components such as middleware, databases, and operating systems.
- In PaaS scenarios, customers are responsible for the applications they deploy, as well as the security settings and policies of the middleware, database, and network access under their control.
- In SaaS scenarios, customers have control over their content, accounts, and permissions. They need to protect their content, and properly configure and protect their accounts and permissions in compliance with laws and regulations.

5.2 Identity Authentication and Access Control

Identity Authentication

You can access COC through the COC console, application programming interfaces (APIs), and software development kits (SDKs). No matter which method you choose, you actually use REST APIs to access COC.

COC APIs can authenticate requests. An authenticated request must contain a signature value. The signature value is calculated based on the access key (AK/SK) of the requester and the information carried in the request body. COC supports authentication using an Access Key ID (AK)/Secret Access Key (SK) pair. This means it can use AK/SK-based encryption to authenticate a request sender. For details about access keys and how to obtain them, see **Access Keys (AK/SK)**.

Access Control

You can use IAM to securely control access to your COC resources. For more information about IAM and COC permissions management, see **Permissions Management**.

5.3 Auditing and Logging

Auditing

Cloud Trace Service (CTS) is a log audit service intended for Huawei Cloud security. It allows you to collect, store, and query cloud resource operation records. You can use these records to monitor resource changes, analyze security, audit compliance, and locate faults.

After you enable CTS and configure a tracker, CTS can record management and data traces of COC for auditing.

To learn how to enable CTS, see **Enabling CTS**.

Logging

After you enable CTS and configure a tracker for COC, CTS can record operations performed on COC.

For more information, see **Viewing Logs**.

5.4 Service Resilience

COC provides a three-level reliability architecture and uses intra-AZ instance disaster recovery (DR), dual-AZ DR, and periodic backups to ensure service durability and reliability.

Table 5-1 COC service reliability architecture

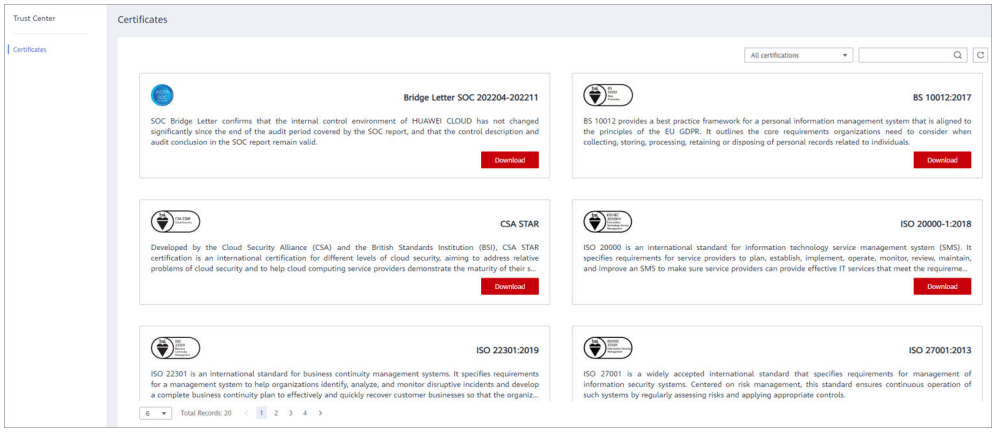
Reliability Solution	Brief
Intra-AZ instance DR	In a single AZ, COC implements instance DR in multi-instance mode and quickly rectifies faults to continuously provide services.
Multi-AZ DR	COC supports cross-AZ DR. If an AZ is faulty, COC services are not interrupted.
Data DR	Data is periodically backed up for data DR.

5.5 Certificates

Compliance Certificates

Huawei Cloud services and platforms have obtained various security and compliance certifications from authoritative organizations, such as International Organization for Standardization (ISO), system and organization controls (SOC), and Payment card industry (PCI) compliance standards. You can **download** them from the console.

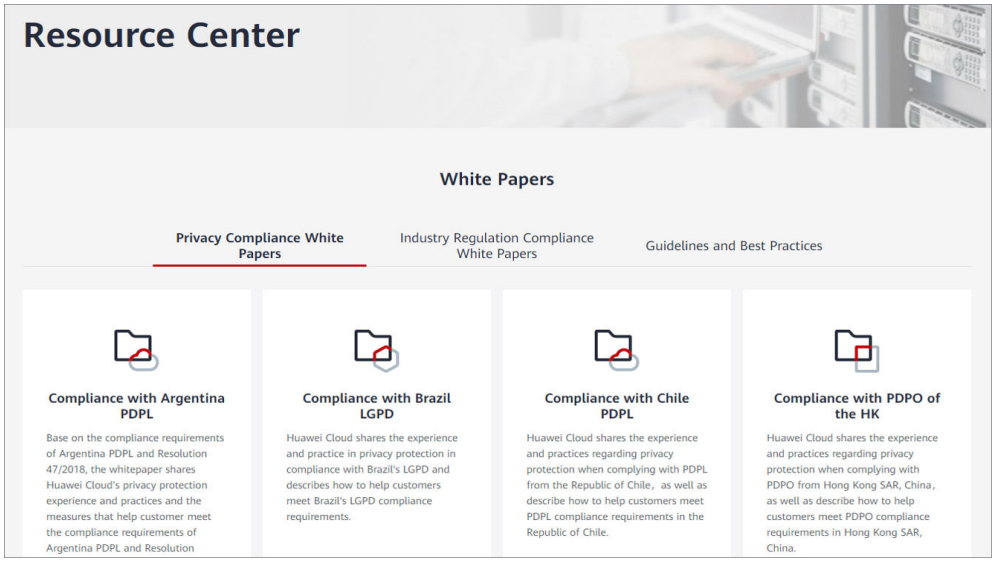
Figure 5-2 Downloading compliance certificates



Resource Center

Huawei Cloud also provides the following resources to help users meet compliance requirements. For details, see **Resource Center**.

Figure 5-3 Resource center



6 Permissions Management

If you need to assign different permissions to employees in your enterprise to access your COC resources, IAM is a good choice for fine-grained permissions management. IAM provides identity authentication, permissions management, and access control, helping you secure access to your Huawei Cloud resources. If your HUAWEI ID does not require IAM for permissions management, you can skip this section.

IAM is a free service. You only pay for the resources in your account.

With IAM, you can control access to specific Huawei Cloud resources. For example, if you want some software developers in your enterprise to use COC resources but do not want them to delete COC resources or perform any other high-risk operations, you can grant the permission to use COC resources but not the permission to delete them.

IAM supports role/policy-based authorization and identity policy-based authorization.

The following table describes the differences between the two authorization models.

Table 6-1 Differences between role/policy-based and identity policy-based authorization

Authorization Model	Core Relationship	Permission	Authorization Method	Application Scenario
Role/Policy-based authorization	User-permissions-authorization scope	• System-defined roles • System-defined policies • Custom policies	Granting roles or policies to principals	To authorize a user, you need to add it to a user group first and then specify the scope of authorization. It provides a limited number of condition keys and cannot meet the requirements of fine-grained permissions control. This method is suitable for small- and medium-sized enterprises.
Identity policy-based authorization	Policies	• System-defined identity policies • Custom identity policies	• Assigning identity policies to principals • Attaching identity policies to principals	You can authorize a user by attaching an identity policy to it. User-specific authorization and a variety of key conditions allow for more fine-grained permissions control. However, this model can be hard to set up. It requires a certain amount of expertise and is suitable for medium- and large-sized enterprises.

Assume that you want to grant IAM users permission to create ECSs in CN North-Beijing4 and OBS buckets in CN South-Guangzhou . With role/policy-based authorization, the administrator needs to create two custom policies and assign both to the IAM users. With identity policy-based authorization, the administrator only needs to create one custom identity policy and configure the condition key **g:RequestedRegion** for the policy, and then attach the policy to the users or grant the users the access permissions to the specified regions. Identity policy-based authorization is more flexible than role/policy-based authorization.

Policies/Identity policies and actions in the two authorization scenarios are not interoperable. You are advised to use the identity policy-based authorization model. For details about system-defined permissions in the two authorization models, see **Policies/Roles Permission Management** and **Identity Policy-based Authorization**.

For details about IAM, see **What Is IAM?**

Policies/Roles Permission Management

COC supports authorization with roles and policies. By default, new IAM users do not have any permissions assigned. You need to add them to one or more groups and attach policies or roles to these groups. The users then inherit permissions from the groups and can perform specified operations on cloud services based on the permissions they have been assigned.

COC is a global service deployed and accessed without specifying any physical region. When the authorization scope is set to **Global services**, you have the permission to access COC resources in all regions.

Table 6-2 lists all the system-defined permissions for COC. System-defined policies and system-defined identity policies in the two authorization models are not interoperable.

Table 6-2 COC system-defined permissions

System-defined Role/ Policy Name	Description	Type	Dependency
COC ReadOnlyAccess	Read-only permissions of COC	System-defined policies	None
COC FullAccess	Administrator permissions of COC	System-defined policies	None

Table 6-3 lists the common operations and permissions supported by each system-defined policy of COC.

Table 6-3 Common operations supported by each system-defined policy

Operation	COC ReadOnlyAccess	COC FullAccess
Viewing to-do tasks	√	√
Creating and handling to-do tasks	x	√
Viewing the resource list	√	√
Managing resources	x	√
Viewing the script list	√	√
Adding, deleting, modifying, and executing scripts	x	√

Operation	COC ReadOnlyAccess	COC FullAccess
Viewing the job list	√	√
Adding, deleting, modifying, and executing jobs	x	√
Performing operations on ECSs	x	√
Viewing scheduled O&M tasks	√	√
Adding, deleting, modifying, and executing scheduled O&M tasks	x	√
Viewing the parameter center	√	√
Adding, deleting, and modifying parameters	x	√
Viewing incident tickets	√	√
Creating and handling incidents	x	√
Viewing alarm records	√	√
Handling alarms	x	√
View chaos drill plans	√	√
Executing drill tasks	x	√
Viewing shift schedules	√	√
Creating a shift schedule	x	√
Viewing account baselines	√	√
Creating account baselines	x	√

Identity Policy-based Authorization

COC supports authorization with identity policies. **Table 6-4** lists all the system-defined identity policies for COC. System-defined policies in identity policy-based authorization are not interoperable with those in role/policy-based authorization.

Table 6-4 COC system-defined identity policies

Identity Policy Name	Description	Type
COCReadOnlyPolicy	Read-only permissions of COC	System-defined identity policies
COCFullAccessPolicy	Administrator permissions of COC	System-defined identity policies

Table 6-5 lists the common operations supported by system-defined identity policies of COC.

Table 6-5 Common operations supported by system-defined identity policies

Operation	COCReadOnlyAccess	COCFullAccessPolicy
Viewing to-do tasks	√	√
Creating and handling to-do tasks	x	√
Viewing the resource list	√	√
Managing resources	x	√
Viewing the script list	√	√
Adding, deleting, modifying, and executing scripts	x	√
Viewing the job list	√	√
Adding, deleting, modifying, and executing jobs	x	√
Performing operations on ECSs	x	√
Viewing scheduled O&M tasks	√	√
Adding, deleting, modifying, and executing scheduled O&M tasks	x	√
Viewing the parameter center	√	√
Adding, deleting, and modifying parameters	x	√
Viewing incident tickets	√	√

Operation	COCReadOnlyAccess	COCFullAccessPolicy
Creating and handling incidents	x	√
Viewing alarm records	√	√
Handling alarms	x	√
View chaos drill plans	√	√
Executing drill tasks	x	√
Viewing shift schedules	√	√
Creating a shift schedule	x	√
Viewing account baselines	√	√
Creating account baselines	x	√

Identity Policies On Which the COC Console Depends

Table 6-6 Identity policy dependencies of the COC console

Console Function	Dependent Cloud Service/Resource	Identity Policy Required
Executing the script	ECS	After an IAM user is assigned the **COCFullAccessPolicy** permission, the user needs to be assigned the **ECSFullPolicy** permission to execute scripts on ECSs.
Executing a Job	ECS	After an IAM user is assigned the **COCFullAccessPolicy** permission, the user needs to be assigned the **ECSFullPolicy** permission to execute jobs on ECSs.
Performing operations on ECSs	ECS	After an IAM user is assigned the **COCFullAccessPolicy** permission, the user needs to be assigned the **ECSFullPolicy** permission to execute operations on ECSs.
Executing scheduled O&M tasks	ECS	After an IAM user is assigned the **COCFullAccessPolicy** permission, the user needs to be assigned the **ECSFullPolicy** permission to execute scheduled O&M tasks on ECSs.

Related Links

- What Is IAM?

7 Constraints and Limitations

NOTE

Cloud Operations Center (COC) is universally applicable. However, it is not supported in some special regions and scenarios (such as dedicated regions). If you have any requirements, contact COC service personnel.

By June 2025, COC supports the following Huawei Cloud regions:

Table 7-1 Huawei Cloud regions supported by Cloud Operations Center (COC)

Region
ME-Riyadh
CN-Hong Kong
AP-Singapore
AP-Bangkok
AP-Jakarta
CN East-Shanghai 1
CN East-Shanghai2
CN East2
CN North-Ulanqab1
CN East-Qingdao
CN North-Beijing1
CN North-Beijing4
CN South-Guangzhou
CN South-Shenzhen
TR-Istanbul

Region
LA-Sao Paulo1
LA-Santiago
LA-Mexico City
LA-Mexico City2
CN Southwest-Guiyang1
AF-Cairo
AF-Johannesburg

When using COC, pay attention to the restrictions listed in **Table 7-2**.

Table 7-2 Restrictions on COC

Functional Module	Object	Restriction
Public	Managing patches, scripts, jobs, or ECSs	A maximum of 200 instances can be selected for a single operation task.
	Managing patches, scripts, jobs, or ECSs	The timeout interval for executing a service ticket must be less than or equal to 86,400 seconds (24 hours).
Resource management	Installing OSs supported by UniAgent	Currently, the following Linux OS versions are supported: • EulerOS 2.2 (64-bit) for Tenant 20210227 • EulerOS 2.3 (64-bit) • EulerOS 2.5 (64-bit) for Tenant 20210229 • CentOS 7.2 (64-bit) • CentOS 7.3 (64-bit) • CentOS 7.4 (64-bit) • CentOS 7.5 (64-bit) • CentOS 7.6 (64-bit) for Tenant 20200925 (for resource image creation) • CentOS 7.6 (64-bit) for Tenant 20210227 • CentOS 7.6 (64-bit) for Tenant 20210525

Functional Module	Object	Restriction
	UniAgent client	If the CPU usage is greater than 10% or the memory is greater than 200 MB, the UniAgent client automatically restarts.
	Installing a UniAgent	A maximum of 100 UniAgent hosts can be installed at a time.
Application management	Applications	An application must be within 5 layers.
Patch management	Patch baselines	A tenant can create a maximum of 50 (public baselines excluded) patch baselines.
Script management	Script content	The content of a custom script cannot exceed 100 KB.
Job management	Global parameters	The number of global parameters of a user-defined job cannot exceed 30.
War Room	War room initiation rules	A maximum of 50 war room initiation rules can be created by a tenant.
Alarm conversion rules	Alarm conversion rules	A tenant can create a maximum of 50 alarm conversion rules
Data source management	Data records	COC retains only the latest 10 records of integrated data source.
Personnel management	Number of engineers	The number of personnel created by a tenant cannot exceed 50.
Shift schedule management	Roles	A maximum of 10 roles are allowed in a single shift scheduling scenario.

Functional Module	Object	Restriction
Account management	Resource types	Currently, ECSs can be managed. Currently, account hosting (account import) is supported for the following types of resources: • ECSs • DCS instances • RDS instances • DMS instances
	Account baselines	The number of baseline accounts is less than or equal to 30, and the number of components associated with the accounts is less than or equal to 100.

Currently, COC supports IAM login, IAM federated user login (including IAM user SSO and virtual user SSO), and login via IAM Identity Center. Login via IAM agencies is not supported. You can select one from these supported login methods to use COC features, such as ticket creation and review. For details about each login method, see **Managing O&M Engineers**.

8 COC and Other Services

Figure 8-1 shows the relationships between COC and other services.

Figure 8-1 COC and other services

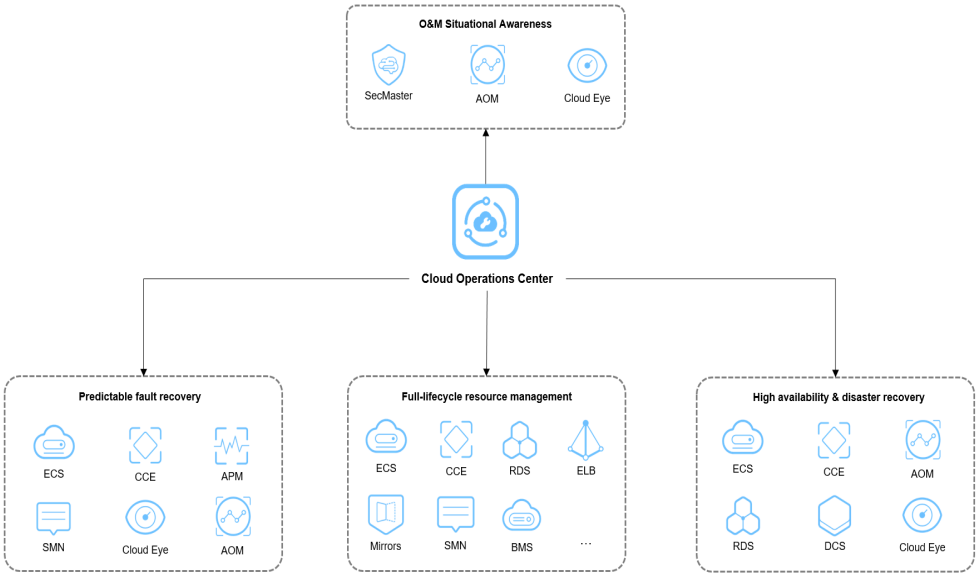


Table 8-1 COC and other services

Service	Interaction with Other Services	Related Feature
SecMaster	Provides security monitoring information for you on the **Overview** page. Presents a comprehensive security overview from three perspectives: security score, security monitoring data, and security trend. It also allows for the creation of personalized security monitoring dashboards.	Security Score

Service	Interaction with Other Services	Related Feature
Cloud Eye	Represents a resource monitoring data overview and also provides the resource alarm details. After Cloud Eye is integrated into COC, you can obtain and handle alarms generated on Cloud Eye in the fault management module of COC. You can also view metric data on Cloud Eye during chaos drills. To use these functions, enable Cloud Eye first.	**Resource Monitoring** **Integrating Cloud Eye** **Chaos Drills**
Application Operations Management (AOM)	Provides application monitoring dashboards. The dashboards configured on AOM can be displayed in COC. After AOM is integrated into COC, you can obtain and handle alarms generated on AOM in the fault management module of COC. You can also view metric data on AOM during chaos drills.	**Viewing Application Monitoring** **Integrating AOM** **Chaos Drills**
Elastic Cloud Server (ECS)	Provides ECSs for your operations like batch ECS management, script execution, job execution, and scheduled task management. You can also execute chaos drill tasks on ECSs.	**Batch Operations on ECS Instances** **Chaos Drills**
Cloud Container Engine (CCE)	Provides CCE instances, so that you can execute chaos drills on these instances.	**Chaos Drills**
Application Performance Management (APM)	Enables you to obtain and handle alarms generated on APM, and transfer alarms to incidents as required in the fault management module of COC.	**Integrating APM**
Simple Message Notification (SMN)	Enables you to send notifications by SMS messages, emails, voice calls, WeCom, and DingTalk in scenarios like fault management and resource O&M in COC. To use these functions, enable the SMN service first.	**Notification Management**
RDS	Enables you to perform batch operations on RDS DB instances. You can also execute chaos drills on these RDS DB instances.	**Batch Operations on RDS DB Instances** **Chaos Drills**
Bare Metal Server (BMS)	Provides BMSs for your operations like batch BMS management, script execution, job execution, and scheduled task management.	**Batch Operations on BMSs**

Service	Interaction with Other Services	Related Feature
Object Storage Service (OBS)	Enables you to distribute and upload files to ECSs during resource O&M. To use these functions, purchase buckets on OBS first.	**Executing Common Scripts**
Huawei Cloud Flexus	Provides FlexusL instances for your operations like batch FlexusL instance management, script execution, job execution, and scheduled task management. You can also execute chaos drill tasks on FlexusL instances.	**Batch Operations on FlexusL Instances** **Chaos Drills**
Data Encryption Workshop (DEW)	Enables you to create encrypted parameters during resource O&M. To use this function, purchase keys on DEW first. During account management, you can use keys to protect your account passwords.	**Encrypting Parameters** **Account Management**

9 Product Concepts

IDC

Internet data center (IDC): a professional physical facility that provides infrastructure services for centralized data storage, processing, and transmission.

Patch Baselines

A collection of preset patch management rules, including the OS type, patch category, and compliance level. Generally, patches are scanned and installed on instances based on the patch baseline.

Alarm Conversion Rules

Raw alarm information ingested to COC is converted to incidents or aggregated alarms based on a variety of triggering types and conditions, implementing alarm aggregation and noise reduction.

Incidents

An IT Operations (ITOps) concept. COC incidents are manually created, converted from alarms, or automatically generated based on alarm conversion rules. Incidents are abnormal statuses or service interruptions in an application and need to be quickly responded to and handled through a standard process. There are five standard incident levels: P1, P2, P3, P4, and P5.

Aggregated Alarms

Content automatically generated after the COC alarm conversion rules are triggered. You can use COC to clear aggregated alarms, convert alarms to incidents, and execute response plans.

Issues

An ITOps concept. Issues generally refer to the deep causes of incidents. The causes are determined through systematic investigations.

War Rooms

In COC, a war room is a meeting set up to quickly recover services when a group fault or major fault occurs. It enables joint operations of the O&M, R&D, and operations teams, and ensure quick service recovery. In a war room, you can use application diagnosis and response plans to quickly recover applications. In addition, you can start up DingTalk, WeCom, and Lark war room groups.

Improvement

An ITOps concept. Based on incident analysis and alarm handling, the architecture, configuration, and process are systematically optimized to continuously improve application quality and efficiency.

Change

An ITOps concept. It is a general term for a series of operations, such as adding, deleting, modifying, and querying applications, resources, architectures, and configurations.

PRR

A Production readiness review (PRR) in the O&M domain refers to a standardized process that systematically evaluates and verifies whether a service or application meets production environment requirements such as high availability, maintainability, and disaster recovery capabilities before it is rolled out.

SLI

SLI is short for Service level Indicator, which is a basic metric of the SLA and SLO. It directly reflects the key quality dimensions, such as delay and error rate, of services.

SLO

SLO is short for Service level objective, which is used to measure the system stability and reliability based on the SLI. It is the core basis of the SLA. Its core value lies in transforming the vague system stability into a quantifiable commitment (for example, "monthly availability ≥ 99.999%).

SLA

SLA is short for service level agreement, which is a service quality commitment that clearly defines the performance metrics, availability standards, and liability clauses that the service provider must meet. The core is to balance user requirements and service capabilities through quantitative objectives (for example, availability ≥ 99.999%).

