# Cloud Operations Center (COC)

# Service Overview

| | |
|---|---|
| **Issue** | 01 |
| **Date** | 2025-08-08 |

**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

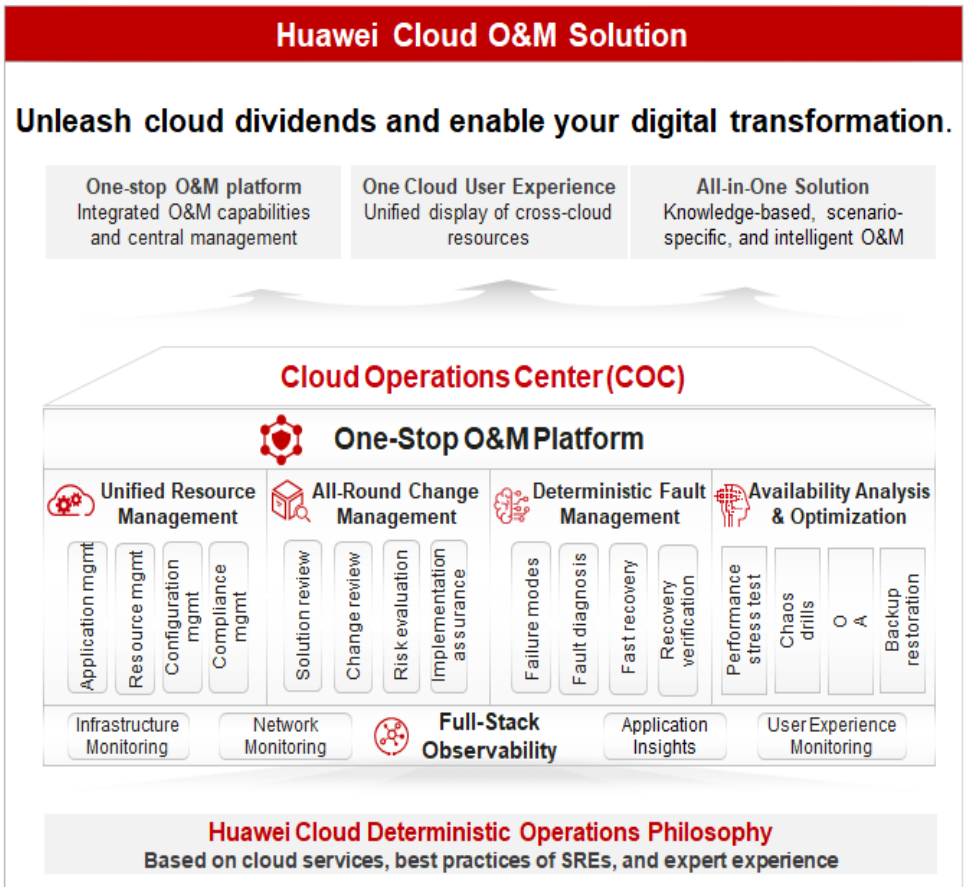


# 1 What Is COC?

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 changes based on scenario rules, process rules, and business rules to identify and prevent change risks in advance. 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 detailed operations, see the **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.

  Ensure that you have registered on Huawei Cloud. For details about how to register an account, see **Signing Up for a HUAWEI ID and Enabling Huawei Cloud Services**. Then, log in to the management console and click **Cloud Operations Center**.

# 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 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 dashboards

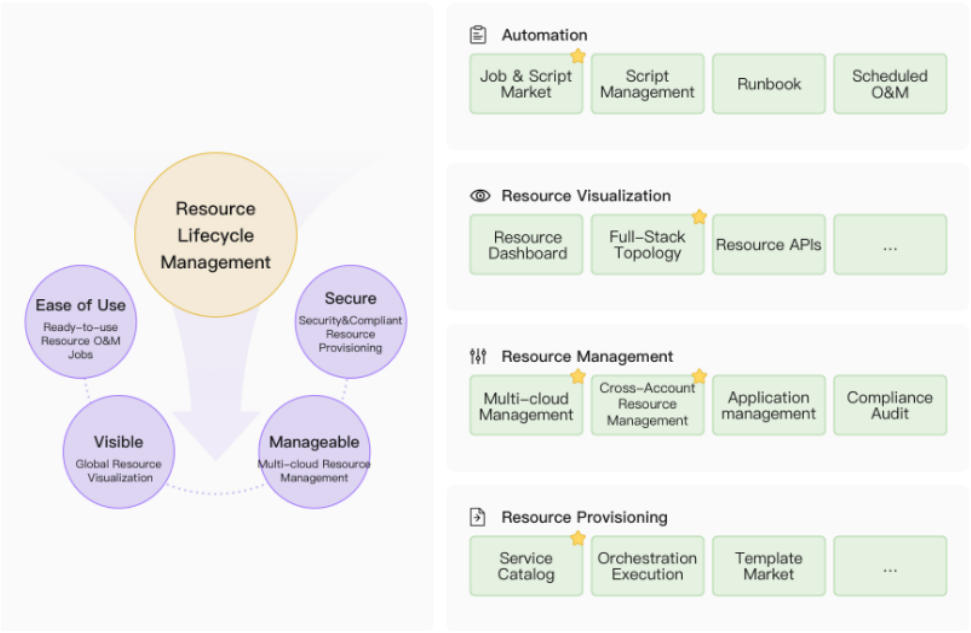

## Full-Lifecycle Resource Management

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



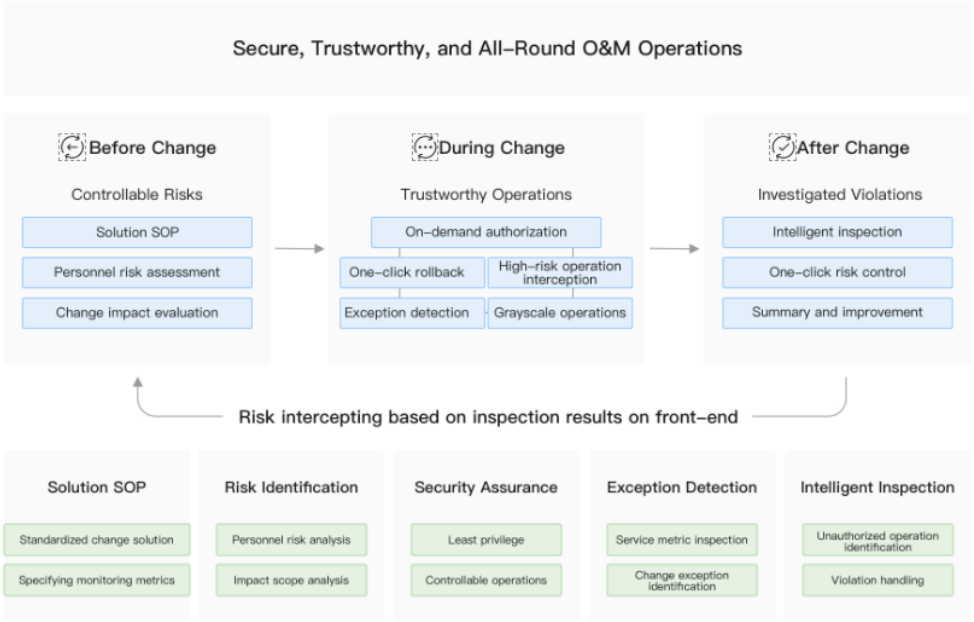

## Change Risk Control and Operations Trustworthiness

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



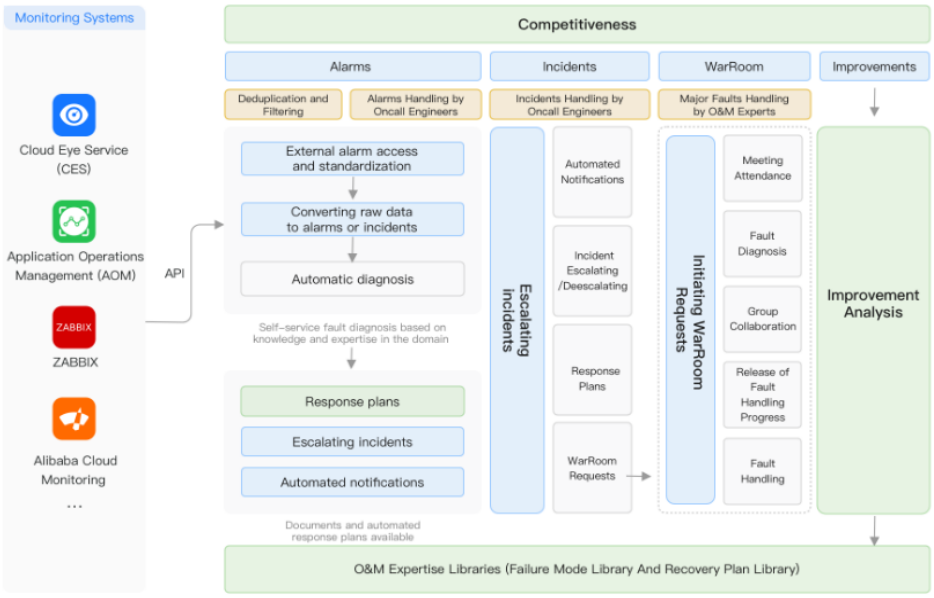

## Standardized Fault Management

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



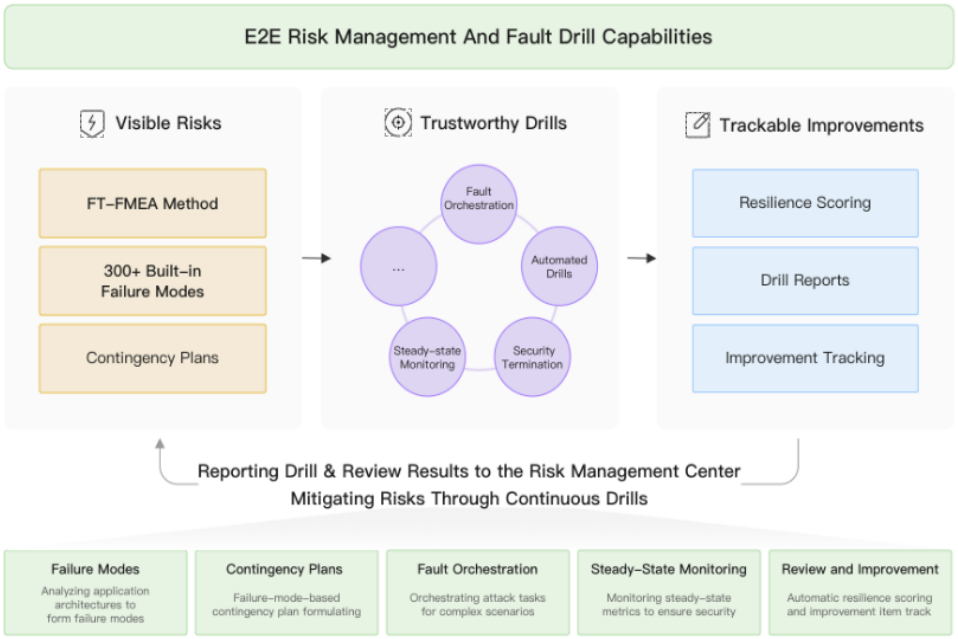

## Intelligent Chaos Drills

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 from the perspective of fault tolerance, and leverages Huawei Cloud SREs' years of accumulated experience in fault handling through the failure mode library.

**Figure 3-5** Intelligent chaos drills



# 4 Features

Table 4-1 describes the commonly used features of COC.

**Table 4-1** COC features

| Feature | Description | Region Availability |
| --- | --- | --- |
| Overview | The following feature modules are available on the COC overview page: resource overview, resource monitoring, application monitoring, security overview, quick entries, and more. You can view and perform operations on work items with ease on the overview page, enjoying simplified and highly efficient O&M. | Global |
| Resource management | COC provides a resource management view that is bolstered by management capabilities for various resources. By using this feature, you can create resource topologies, aggregate resources by resource type, query resources from the resource list by resource tag, and install the UniAgent components. | Global |
| 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. | Global |
| Patch management | Manage patches on ECSs, scan OS compliance, and repair OSs whose patches are non-compliant. | Global |
| Batch operations on ECSs | Batch manage ECSs, including batch starting, stopping, and restarting ECSs, and switching and reinstalling OSs for ECSs. | Global |
| Batch operations on RDS DB instances | Batch manage RDS DB instances, including starting, stopping, and restarting RDS DB instances in batches. | Global |

| Feature | Description | Region Availability |
| --- | --- | --- |
| Batch operations on FlexusL instances | Manage FlexusL instances, including starting, stopping, and restarting instances, and reinstalling OSs in batches. | Global |
| Script management | Create, modify, and delete scripts, and execute your own and public scripts on VMs (Script management is only allowed on ECSs currently.) | Global |
| Job management | Create, modify, and delete jobs, and execute jobs on VMs (Job management is only allowed on ECSs currently.) | Global |
| Scheduled O&M | You can either select job or script execution tasks from existing tasks or create such tasks. There are two task execution methods available: one-time execution and periodic execution. Periodic task execution includes execution using Cron expressions and simple periodic execution. | Global |
| Parameter center | 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. | Global |
| Incident center | You can check all incidents on the incident dashboard in the COC incident center. You can also manually handle incidents, associate incidents with jobs, escalate or de-escalate incidents, forward incidents to their owners, check handling records of incidents, and initiate war room requests with just a few clicks. | Global |
| Alarm center | Clean raw alarms based on alarm conversion rules and then create alarms. Alarms can be allocated to O&M engineer shifts or individuals so that alarm owners are clear. You can manually clear alarms, convert alarms to incident tickets, or use the automated alarm handling feature. | Global |
| War rooms | 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. | Global |
| 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. | Global |

| Feature | Description | Region Availability |
| --- | --- | --- |
| Issue 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. | Global |
| 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. | Global |
| Data source management | Quickly integrate with existing or external monitoring systems with ease for centralized alarm management. Each monitoring system employs distinct integration access keys for seamless interconnectivity. | Global |
| Change management | The change center provides a unified platform for engineers to manage change tasks. With the change center, engineers can submit tickets to manage change requests, review, and execution. | Global |
| Chaos drills | Configure fault drill templates and attack templates and perform fault drills on physical machines, VMs, or Cloud Container Engine (CCE) containers using the templates. You can also manage failure modes. | Global |
| To-do center | On the to-do task dashboard, you can view the handling status of to-do tasks, historical to-do task statistics, and overview of all to-do tasks. You can also manually create to-do tasks. | Global |
| Execution records | On the execution record page, you can query service ticket records of operations on patches, scripts, jobs, and ECSs, and view service ticket details. | Global |
| Personnel management | Centrally manage O&M engineers on COC using this feature. You can manage users of the current tenant on the **O&M Engineer Management** page. The basic user data on the **O&M Engineer Management** page is synchronized from Identity and Access Management (IAM) and is used by multiple basic functional modules in creating to-do tasks, performing scheduled O&M, managing notifications, managing incidents, and more. | Global |

| Feature | Description | Region Availability |
| --- | --- | --- |
| Shift schedule management | 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. | Global |
| Notification management | The notification management module allows you to create notification subscription instances that contain notification scenarios and matching rules. When a change ticket is generated, the notification module first matches the ticket with notification rules and scenarios, then parses the O&M engineers to be notified, the notification content, and notification method, and finally sends the notification messages. | Global |
| Mobile application management | Bind or modify mobile apps. (Currently, only WeCom is supported.) | Global |
| SLA management | Service Level Agreement (SLA) provides ticket timeliness management for you. When a ticket triggers a rule, the SLA notifies you to follow up and handle the ticket in a timely manner, and it records details about the ticket SLA triggering. In SLA management, you can use public SLA rules or user-defined rules, and can configure notifications for SLA violation and warning. | Global |
| Account management | Manage and host ECS accounts and periodically change passwords of ECS accounts. | Global |

# 5 Security

## 5.1 Shared Responsibilities

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

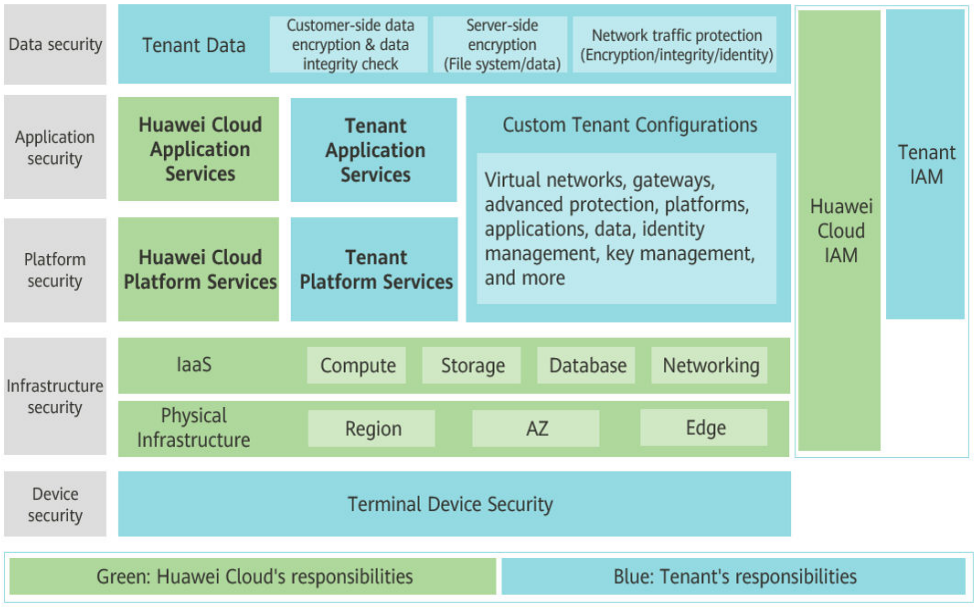
**Figure 1** illustrates the responsibilities shared by Huawei Cloud and you.

- Huawei Cloud: ensures the security of cloud services and provides secure clouds. Huawei Cloud's security responsibilities include ensuring the security of its IaaS, PaaS, and SaaS services, as well as the physical environments of the Huawei Cloud data centers that power these services. Huawei Cloud is responsible for not only the security functions and performance of our infrastructure, cloud services, and technologies, but also for the overall cloud O&M security and, in the broader sense, the security and compliance of our infrastructure and services.
- Tenants: Ensure secure use of cloud services. Huawei Cloud's security responsibilities include ensuring the security of its IaaS, PaaS, and SaaS services, as well as the physical environments of the Huawei Cloud data centers that power these services.

**Huawei Cloud Security White Paper** elaborates on the ideas and measures for building Huawei Cloud security, including cloud security strategies, the shared responsibility model, compliance and privacy, security organizations and personnel, infrastructure security, tenant service and security, engineering security, O&M security, and ecosystem security.

**Figure 5-1** Shared responsibility model of Huawei Cloud




# 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 more information about access keys and how to obtain them, see **Access Keys/ Secret Keys**.

## 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.

If you want to enable and configure CTS, refer to **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. |

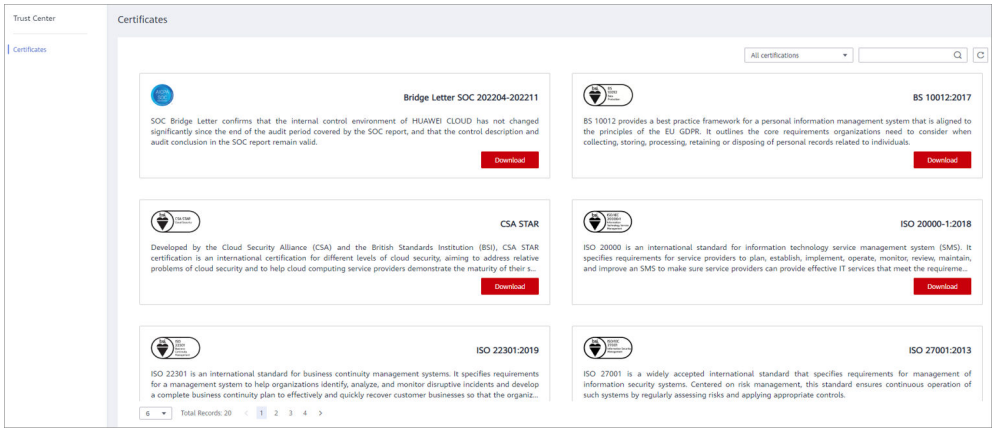
## 5.5 Certificates

### 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.

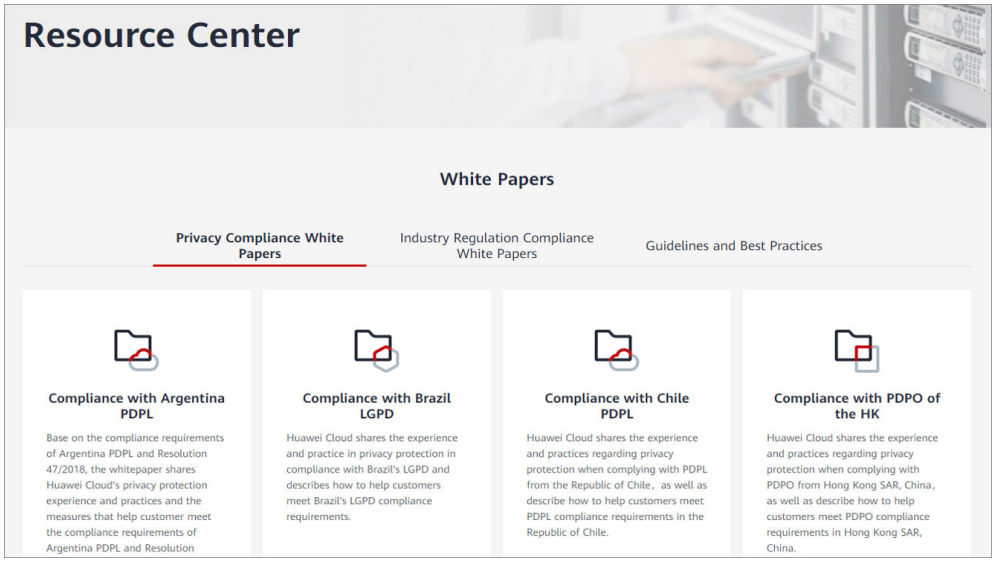
**Figure 5-2** Downloading compliance certificates




## Resource Center

Huawei Cloud also provides the related resources to help you 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 resources purchased on Huawei Cloud, Identity and Access Management (IAM) is a good choice for fine-grained permissions management. IAM provides identity authentication, permissions management, and access control, helping you to securely access your Huawei Cloud resources. If your HUAWEI ID does not require IAM for permissions management, you can skip this section.

IAM can be used on Huawei Cloud for free. You pay only for the resources purchased using your account.

With IAM, you can control access to specific Huawei Cloud resources. For example, you can create IAM users for software developers and grant them the permissions required for using COC resources but not the permissions needed for performing any other operations.

You can grant permissions using roles and policies.

- Roles: A coarse-grained authorization method provided by IAM to define permissions by job responsibility. Only a limited number of service-level roles are available for authorization. Cloud Services depend on each other. When you grant permissions using roles, you also need to attach dependent roles. However, roles are not an ideal choice for fine-grained authorization and secure access control.
- Policies: A fine-grained authorization strategy provided by IAM to define permissions required to perform operations on specific cloud resources under certain conditions. This type of authorization is more flexible and is ideal for least secure access control. For example, you can grant IAM users only permissions to manage ECSs of a certain type.

IAM supports both role-based access control (RBAC) and attribute-based access control (ABAC).

RBAC is a role-based authorization model. By default, a new principal does not have any permissions. You need to assign a system-defined role, system-defined policy, or custom policy to the principal and select the authorization scope so that the principal can have the specified permissions.

The other is a new model based on ABAC, which is also called policy authorization. An administrator can tailor access control policies based on service

requirements and then attach or grant the policies to a principal so that the principal can have the specified permissions. The principal can then perform operations on specified cloud services.

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

**Table 6-1** Differences between RBAC and ABAC

| Authorization Model | Core Relationship | Permission | Authorization Method | Application Scenario |
| --- | --- | --- | --- | --- |
| RBAC | Roles | • System-defined roles<br>• System-defined policies<br>• Custom policies | Granting roles or policies to principals | It offers a simple approach to access management but is not always flexible enough. For more granular permissions control, administrators need to constantly add more roles, which may lead to role explosion. This model can work well for small- and medium-sized enterprises where there is not too much work involved in maintaining roles and permissions. |
| ABAC | Policies | • System-defined policies<br>• Custom policies | • Granting policies to principals<br>• Attaching policies to principals | It gives you more granular, more flexible control of your resources. There is no need to modify existing rules to accommodate new users. All administrators need to do is assign relevant attributes to the new users. However, the construction of a policy-based authorization model is more complex and has higher requirements on the professional capabilities. Therefore, this model is more suitable for medium- and large-sized enterprises. |

COC supports only RBAC. For details about supported system-defined permissions, see **System-defined Permissions in RBAC**.

For more information about IAM, see **What Is IAM?**

## System-defined Permissions in RBAC

COC supports RBAC. 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 in RBAC and ABAC 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 supported by system-defined permissions for 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 | √ |

## System-defined Permissions in ABAC

COC supports ABAC. Table 6-4 lists all the system-defined policies for COC with ABAC System-defined policies in RBAC and ABAC are not interoperable.

**Table 6-4** System-defined policies for COC

| Policy | Description | Policy Type |
| --- | --- | --- |
| COCReadOnlyPolicy | Read-only permissions of COC | System-defined policies |
| COCFullAccessPolicy | Administrator permissions of COC | System-defined policies |

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

**Table 6-5** Common operations supported by each system-defined policy

| Operation | COCReadOnlyPolicy | 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 | √ | √ |

| Operation | COCReadOnlyPolicy | COCFullAccessPolicy |
| --- | --- | --- |
| Adding, deleting, modifying, and executing scheduled O&M jobs | 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 | √ |
| Viewing chaos drill plans | √ | √ |
| Executing drill tasks | x | √ |
| Viewing shift schedules | √ | √ |
| Creating a shift schedule | x | √ |
| Viewing account baselines | √ | √ |
| Creating account baselines | x | √ |

## 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 |
| Latin America-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:<br>• EulerOS 2.2 (64-bit) for Tenant 20210227<br>• EulerOS 2.3 (64-bit)<br>• EulerOS 2.5 (64-bit) for Tenant 20210229<br>• CentOS 7.2 (64-bit)<br>• CentOS 7.3 (64-bit)<br>• CentOS 7.4 (64-bit)<br>• CentOS 7.5 (64-bit)<br>• CentOS 7.6 (64-bit) for Tenant 20200925 (for resource image creation)<br>• CentOS 7.6 (64-bit) for Tenant 20210227<br>• 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 user-defined script cannot exceed 4096 bytes. |
| Job management | Global parameters | The number of global parameters of a user-defined job cannot exceed 30. |
| War rooms | 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.<br>Currently, account hosting (account import) is supported for the following types of resources:<br>• ECSs<br>• DCS instances<br>• RDS instances<br>• 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 **Personnel Management**.

# 8 COC and Other Services

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

**Figure 8-1** COC and other services

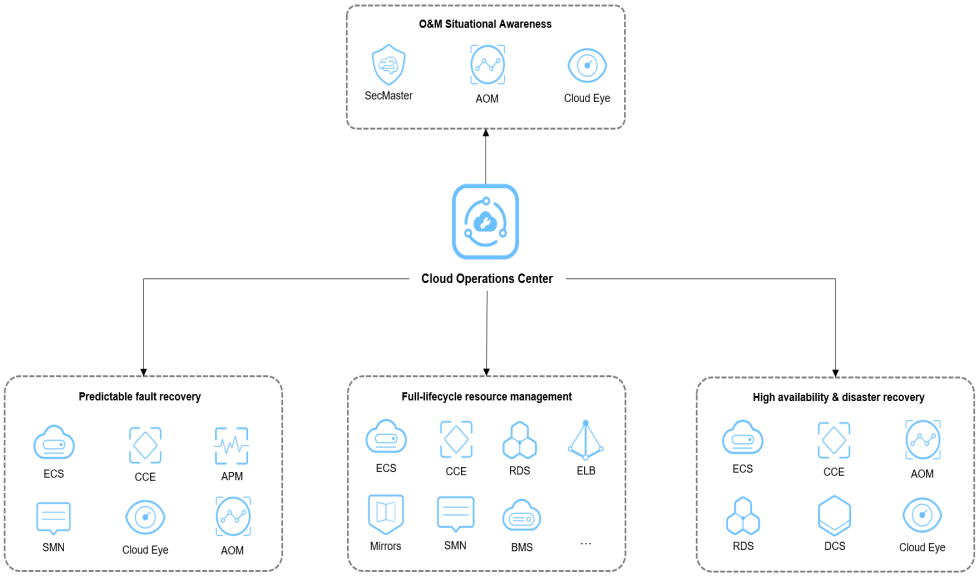



**Table 8-1** COC and other services

| 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**<br>**Integrating Cloud Eye**<br>**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**<br>**Integrating AOM**<br>**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**<br>**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**<br>**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**<br>**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**<br>**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 Baseline

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 Rule

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.

## incident

An IT Operations (ITOps) concept. COC incidents are either manually created 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 Alarm

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.

## Issue

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

## War room

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%).