HUAWEI CLOUD O&M Basics

HUAWEI

Foreword

- HUAWEI CLOUD not only provides resource services to meet enterprise needs to migrate their service systems to the cloud, but also ensures the normal running of the service systems on the cloud to meet the enterprise governance requirements.
- This section will help you understand HUAWEI CLOUD O&M.

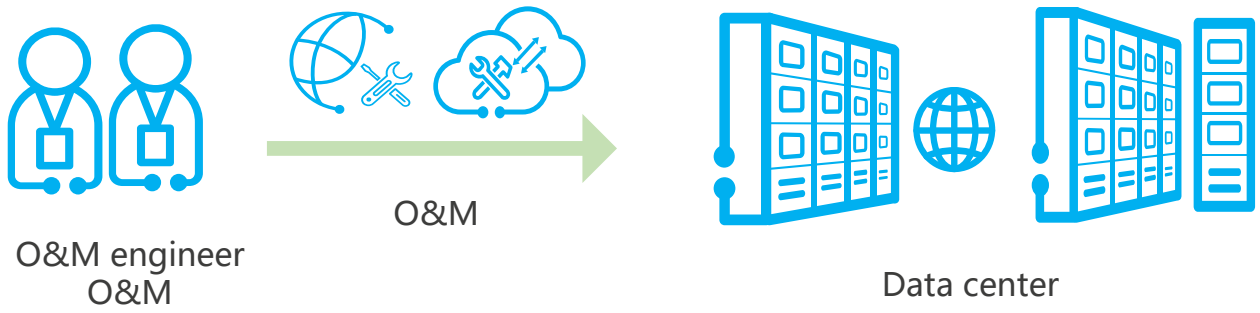
Objectives

- Upon completion of this course, you will:
  - Gain basic knowledge about O&M, monitoring, and auditing.
  - Understand the positioning, principles, and usage of common governance services on HUAWEI CLOUD.

Contents

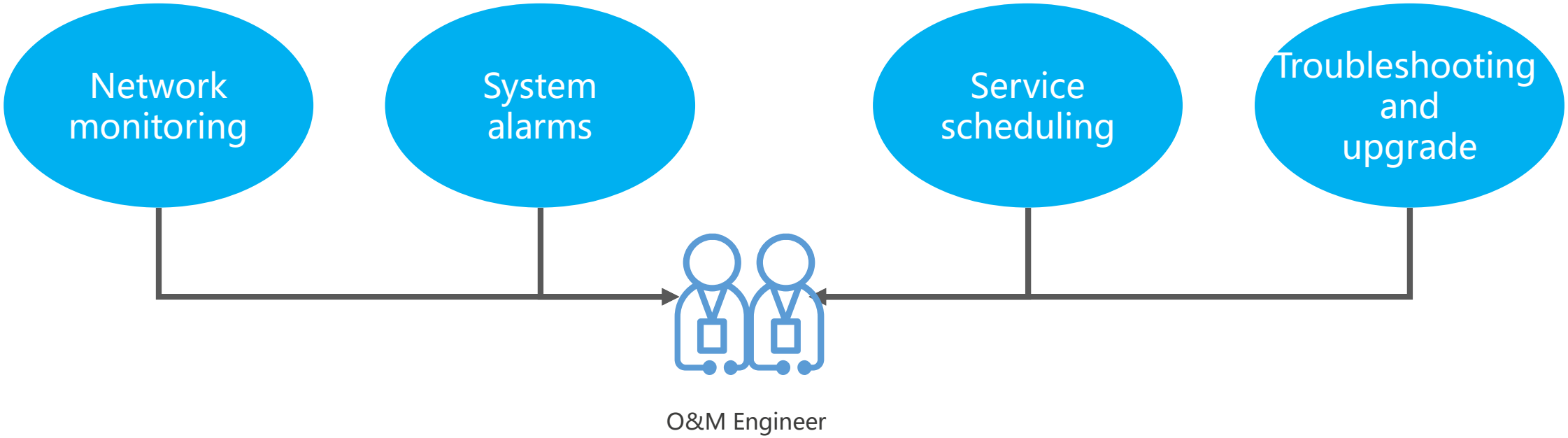
What Is O&M?

- O&M refers to operations and maintenance. It includes monitoring and managing devices and service systems to ensure services run normally. O&M also includes handling various problems and summarizing maintenance experiences to improve O&M efficiency and quality.
- O&M is essentially the operations and maintenance of devices and services such as servers and networks in each phase of their lifecycles, to achieve an optimum level of cost, stability, and efficiency.



Responsibilities of O&M Personnel

- O&M personnel are responsible for planning information, networks, and services based on service requirements and ensuring the long-term stability and availability of services by using various means, including but not limited to the following:

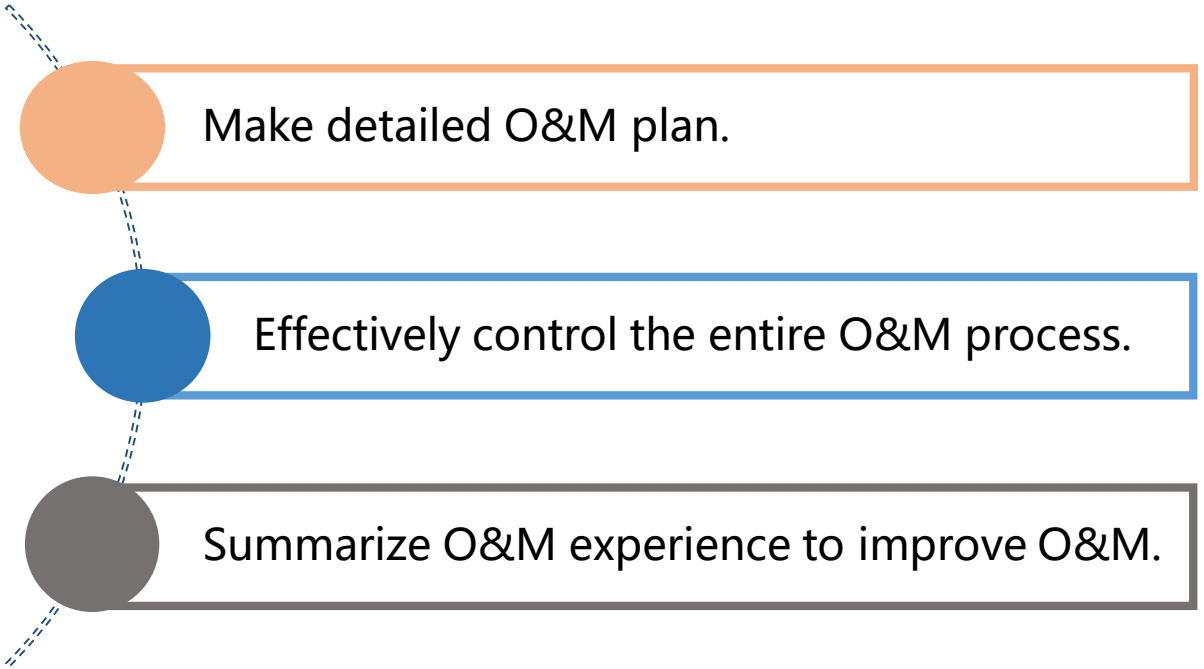


Classification of O&M Personnel

- As the number and complexity of devices, operating systems, and applications deployed in ICT data centers increase, enterprises have higher requirements on O&M. This calls for specialized O&M. Common O&M positions are as follows:

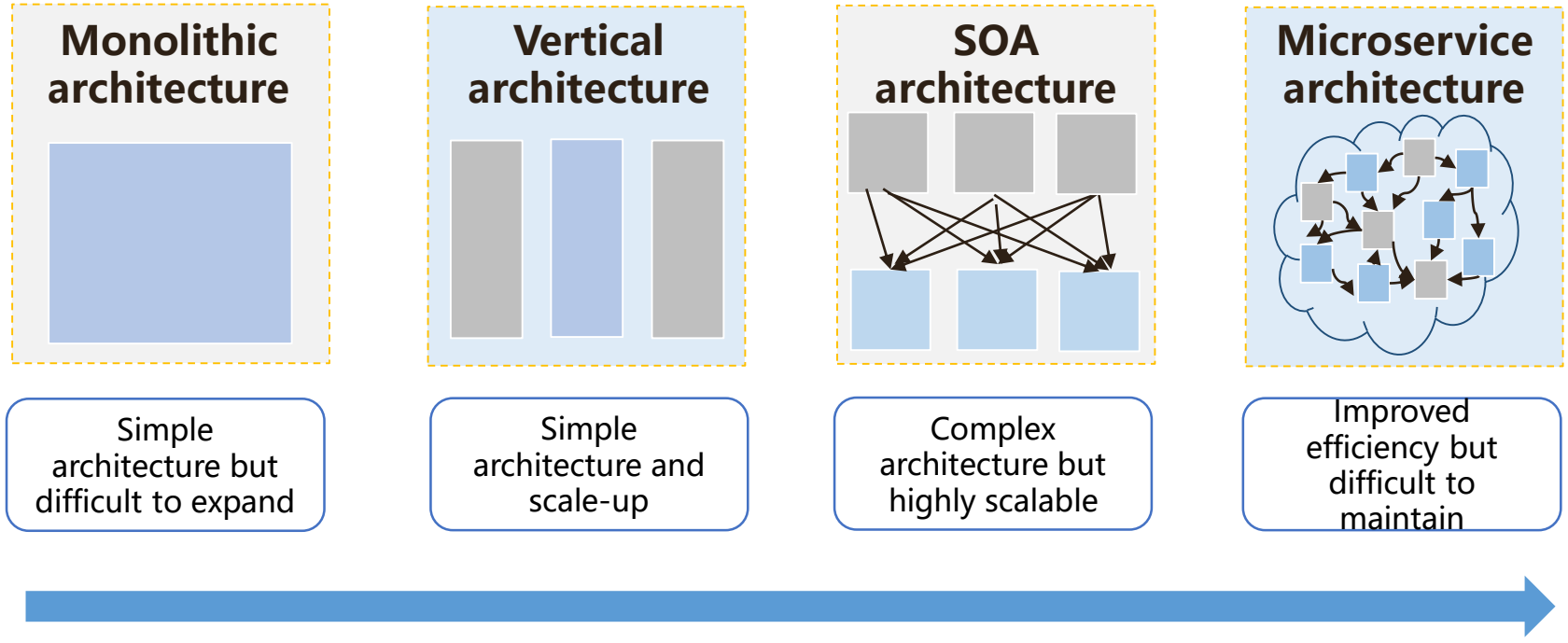
ICT O&M Principles

- We have learned about various O&M positions. How should ICT O&M personnel go about their jobs? O&M seems simple. However, to better serve enterprise business systems, we must first understand the overall principles of ICT O&M.



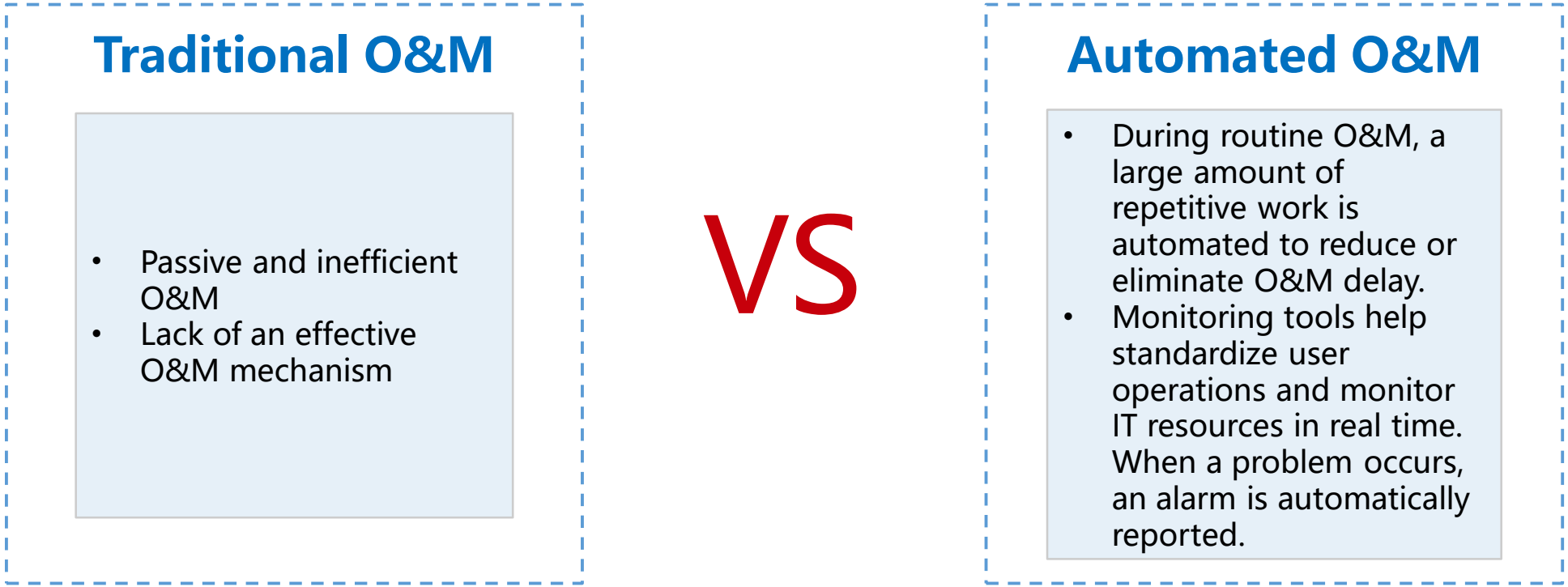
O&M Challenges Brought About by Evolution of IT Architecture

- The IT architecture becomes more and more complex, and O&M personnel face many challenges.

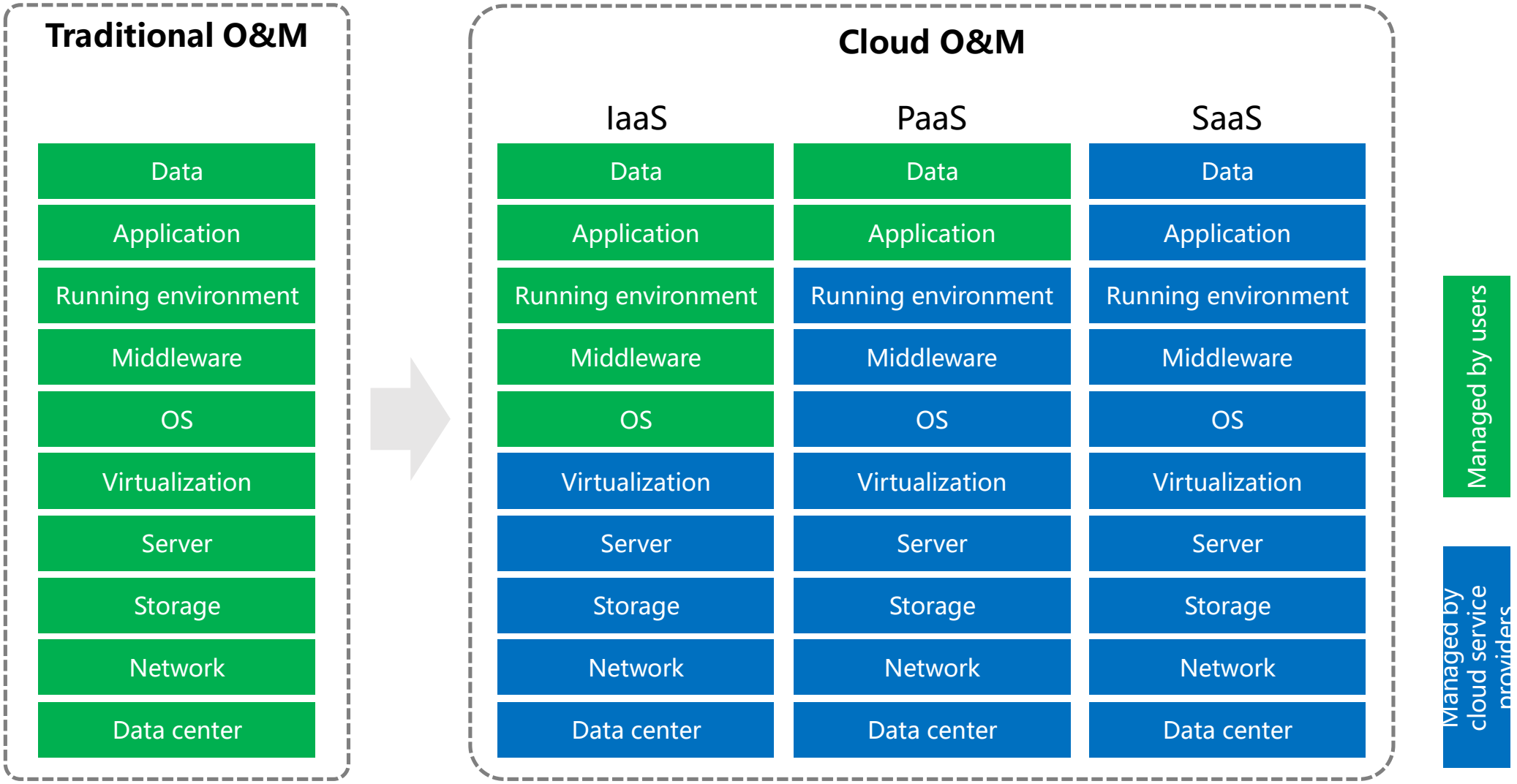


Era of Automated O&M

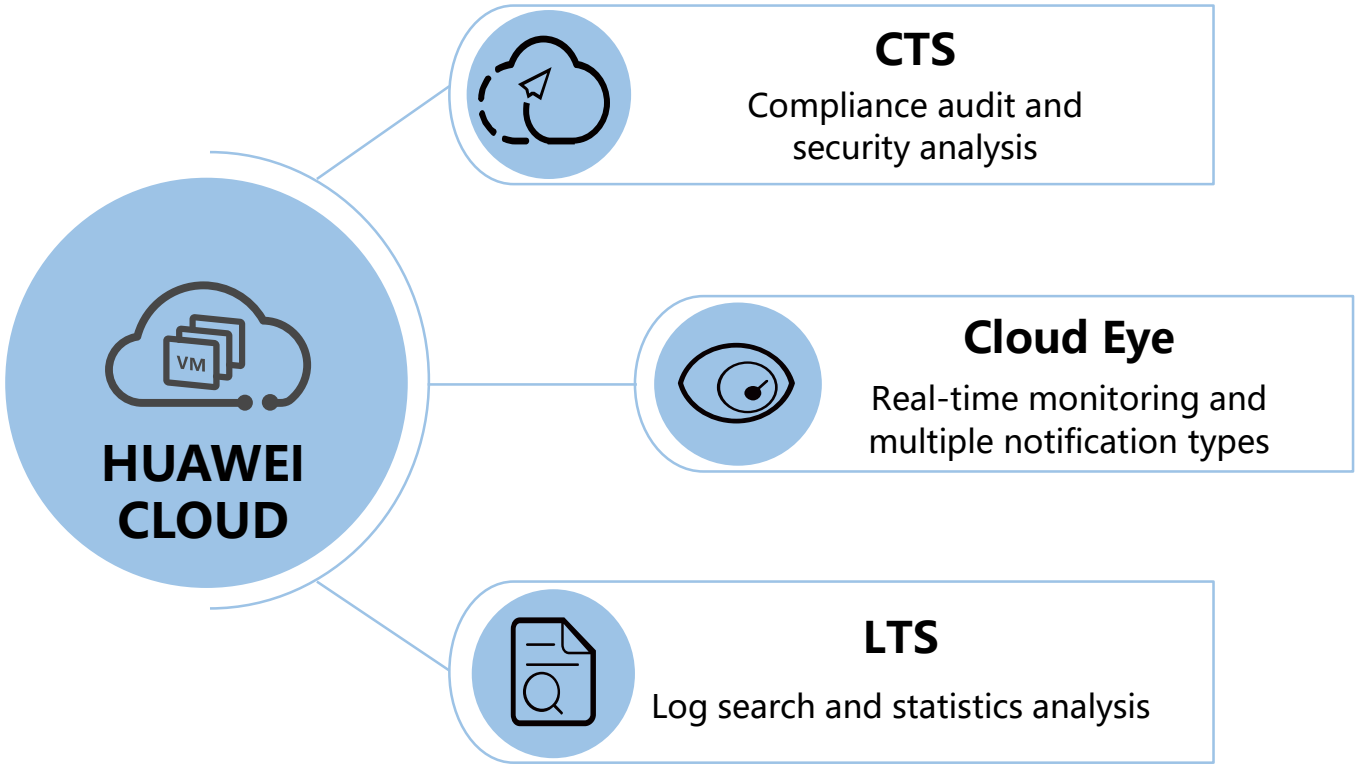
- Traditional manual O&M is being gradually replaced by automated O&M platforms. Responsibilities of O&M personnel and development personnel are converging. The concept of integrated O&M and development (DevOps) is becoming more and more popular and is being used by most enterprises.



O&M Changes in the Cloud Era



Common O&M Services on HUAWEI CLOUD



Contents

Why Is Monitoring Required?

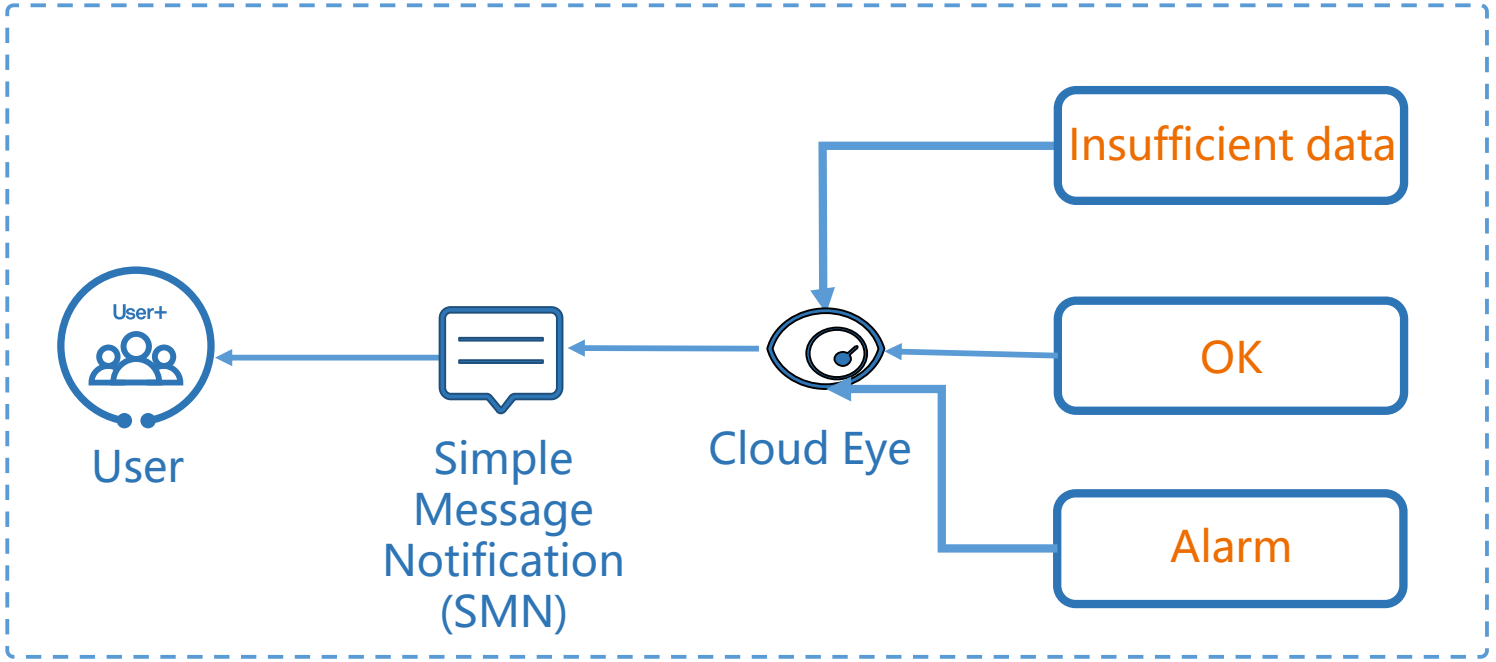
- Monitoring helps identify potential risks. Through monitoring, we can learn about the running status of the enterprise network. Once a security risk is detected, O&M personnel can be informed of the risk in a timely manner, so that they have time to mitigate the risk. This prevents the service system from being affected and resolves issues at the earliest.

What Is Cloud Eye?

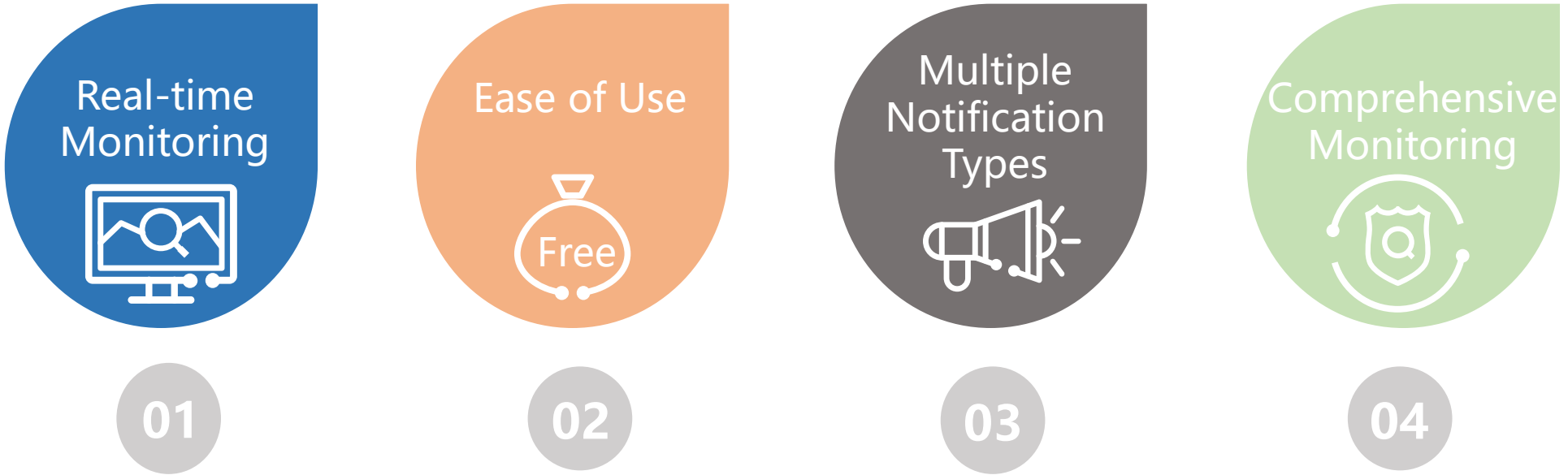
- **Cloud Eye** is a multi-dimensional monitoring service. You can use Cloud Eye to monitor resources, set alarm rules, identify resource exceptions, and quickly respond to resource changes.

Main functions:

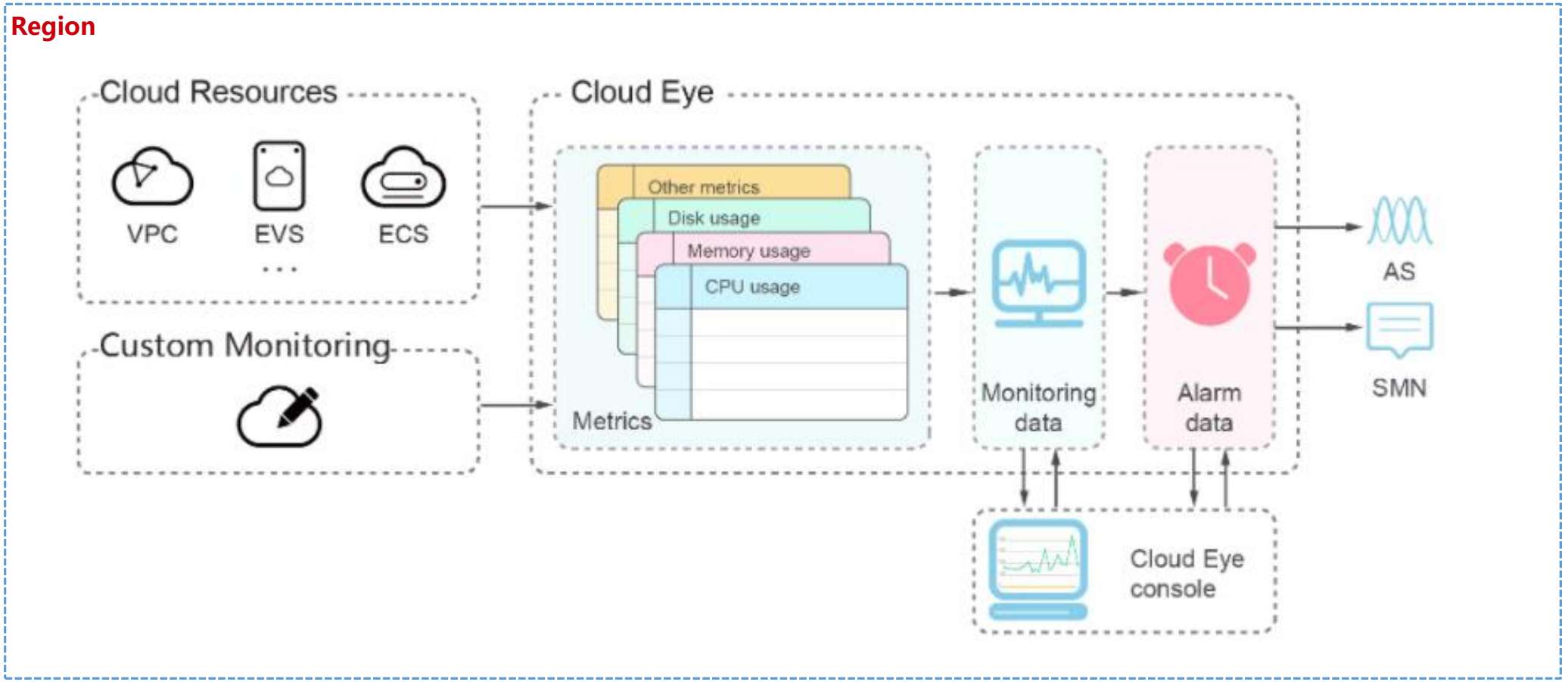
- Automatic monitoring
- Real-time Notifications
- Panels
- Resource groups
- Monitoring data transfer to OBS



Cloud Eye Advantages



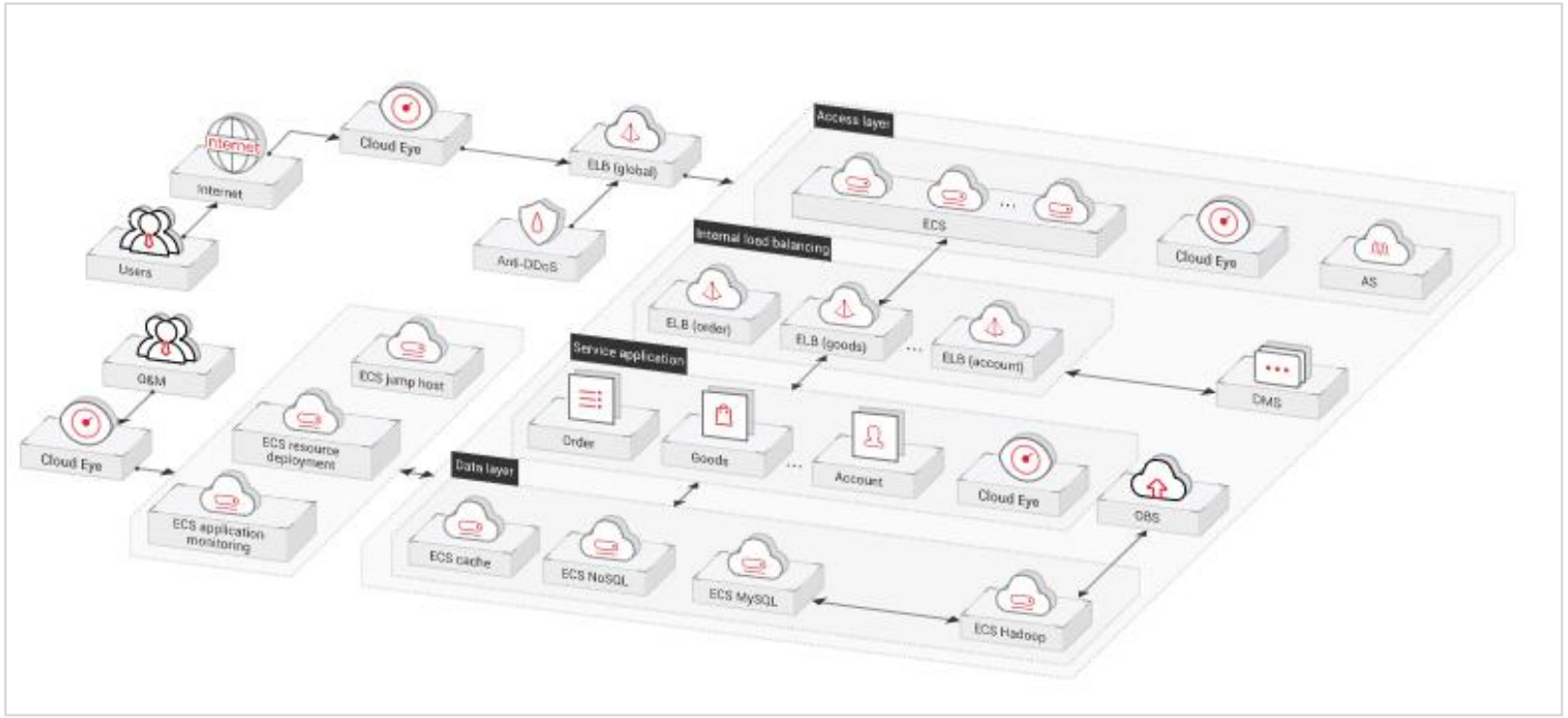
Cloud Eye Architecture



Application Scenario - E-Commerce Websites

Characteristics of E-Commerce Websites

- Editable Monitoring Panel
  Provides you with a comprehensive view of key system monitoring information.
- Alarm-Triggered Scaling
  The system automatically expands or reduces capacity based on the service traffic volume and configured alarm rules.
- Comprehensive Server Monitoring
  Enables monitoring of customized network traffic metrics to prevent network bottlenecks.

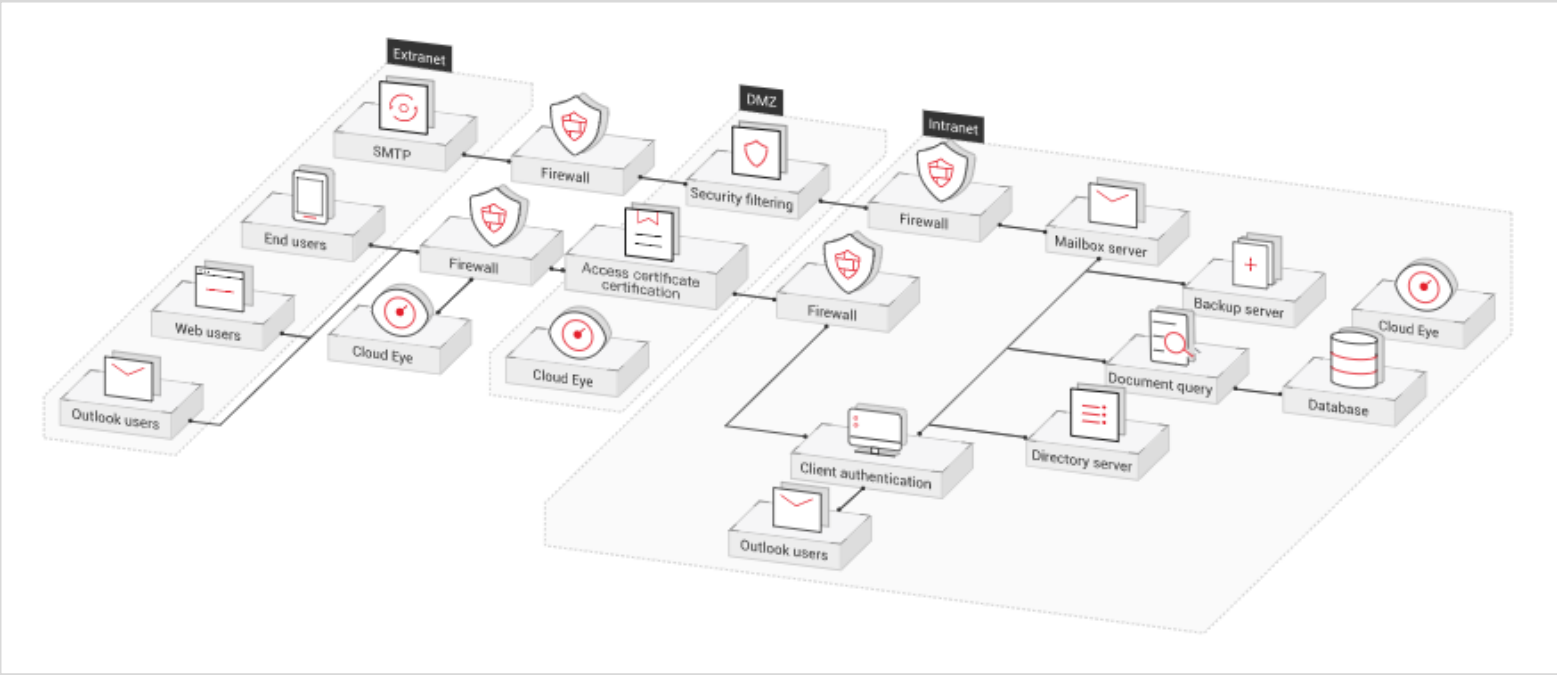


HUAWEI

Application Scenario - Enterprise Offices

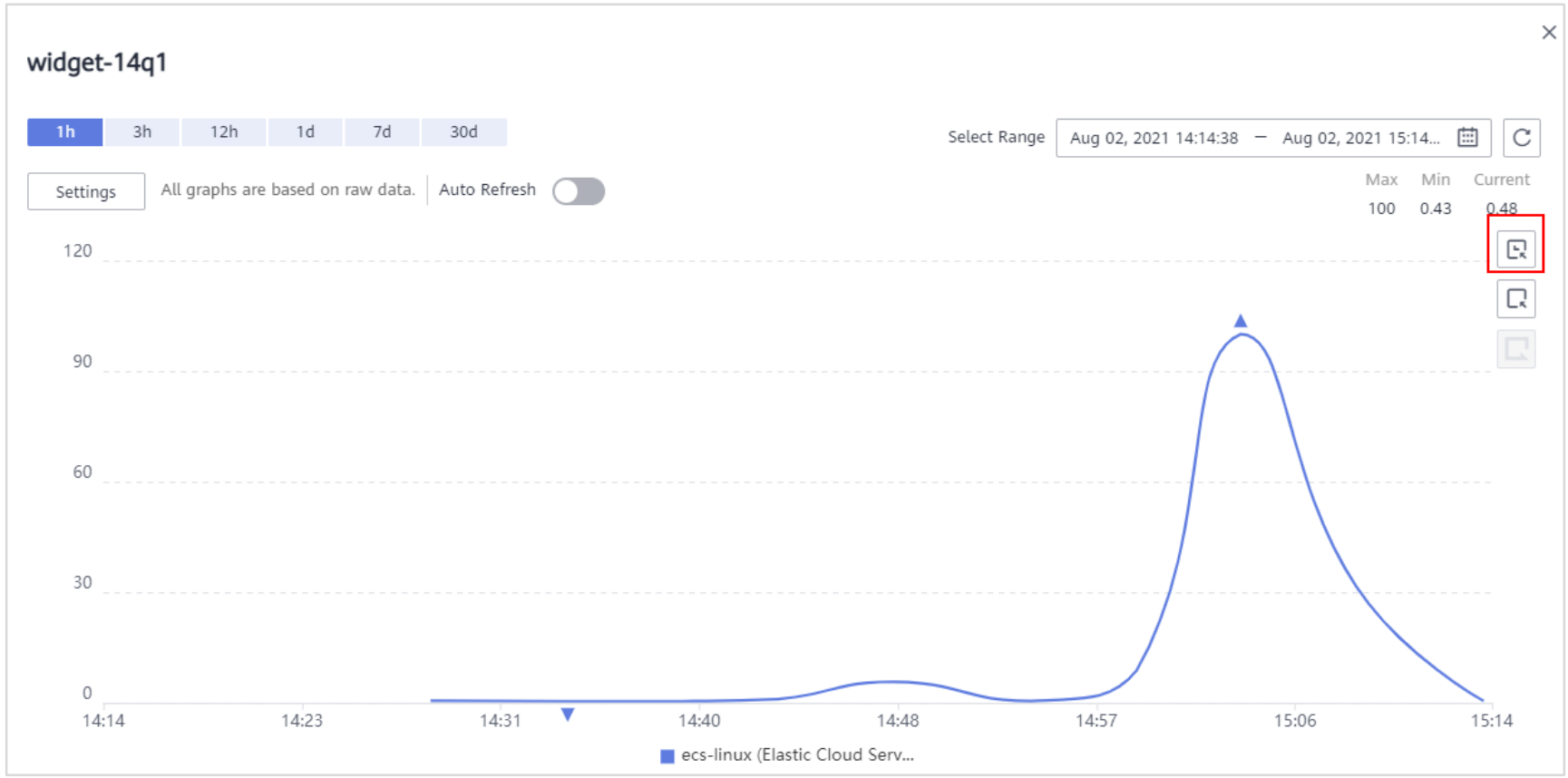
Characteristics of Enterprise Offices

- Alarm-Triggered Expansion
  ECS expansion is automatically triggered by alarms that are generated if ECS usage reaches the configured threshold.
- Log Monitoring
  Logins are monitored in real time and malicious login requests are rejected to ensure security.
- Comprehensive Server Monitoring
  Enables monitoring of customized network traffic metrics to prevent network bottlenecks.



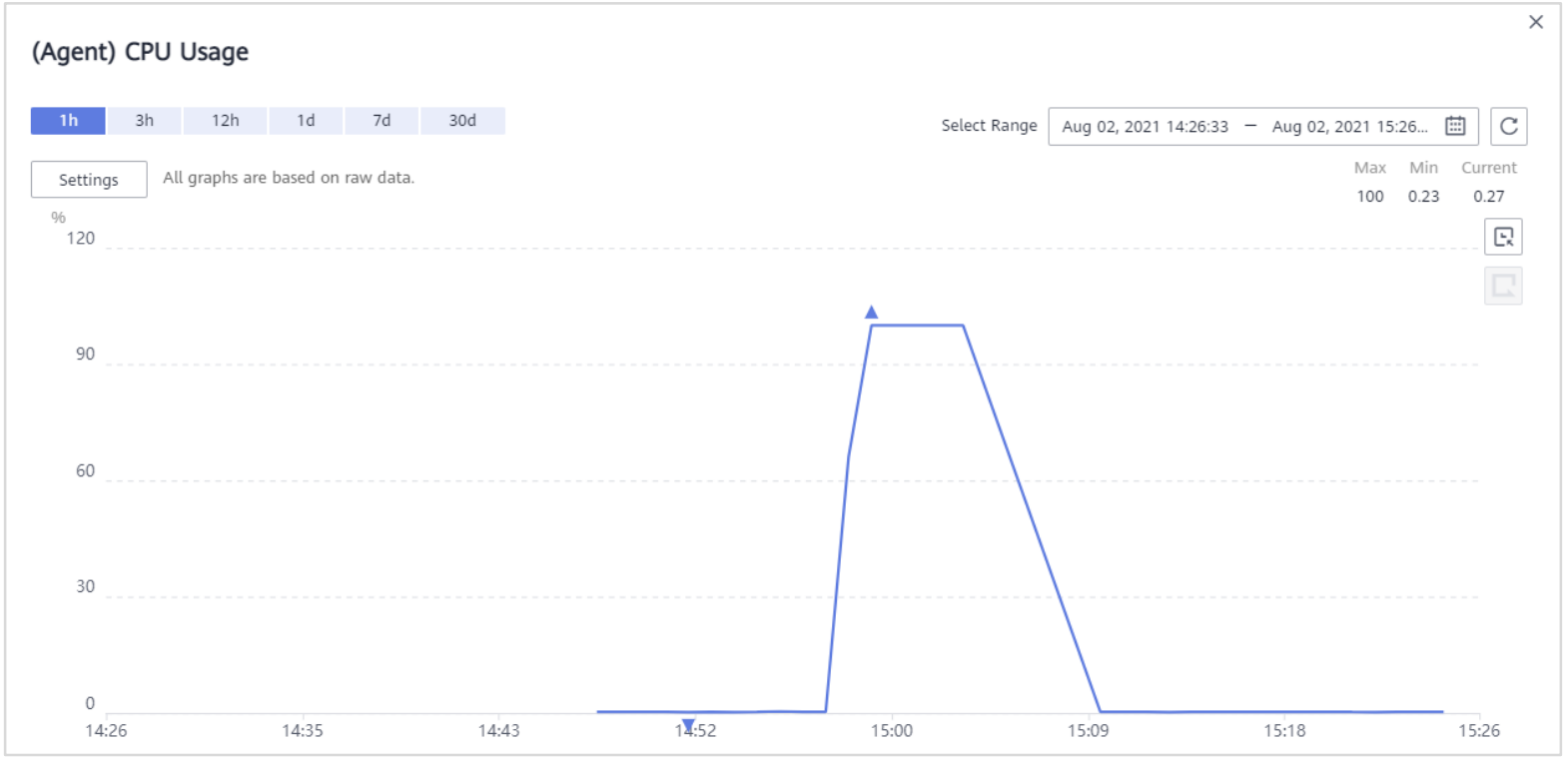
Panels

- You can use panels to view core metrics and compare the performance data of different services.



Metrics

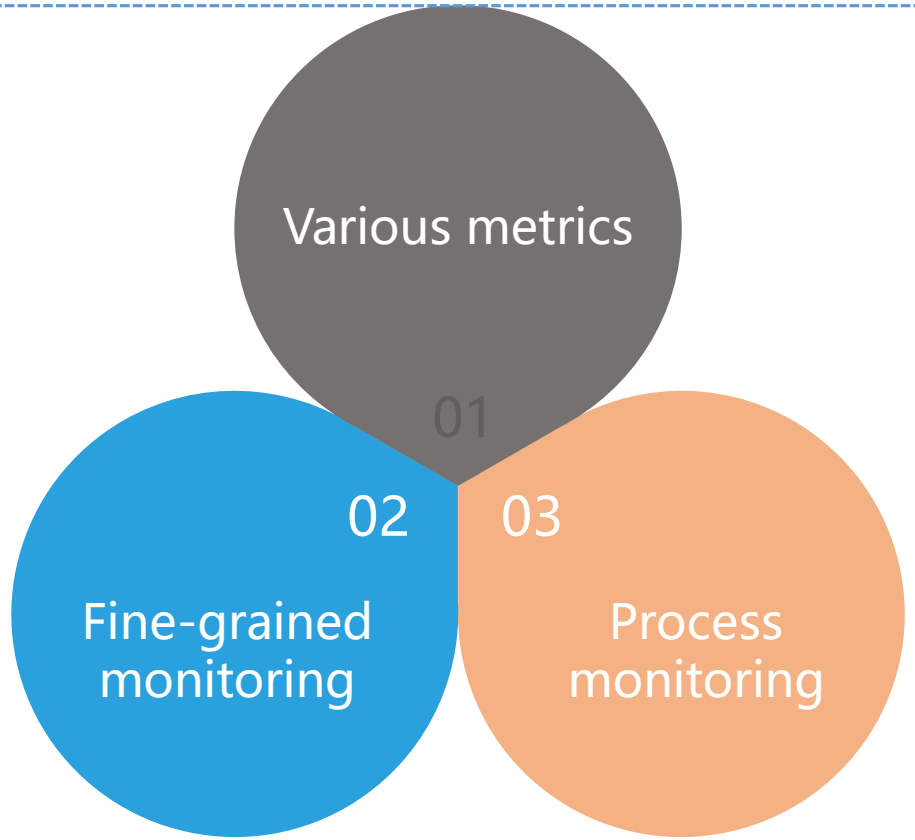
- This is the core concept of Cloud Eye. A metric refers to a quantitative value of a resource dimension on the cloud platform, such as the ECS CPU usage and memory usage. A metric is a time-dependent variable that generates a certain amount of monitoring data over time. It helps you understand the changes over a specific period of time.



Server Monitoring

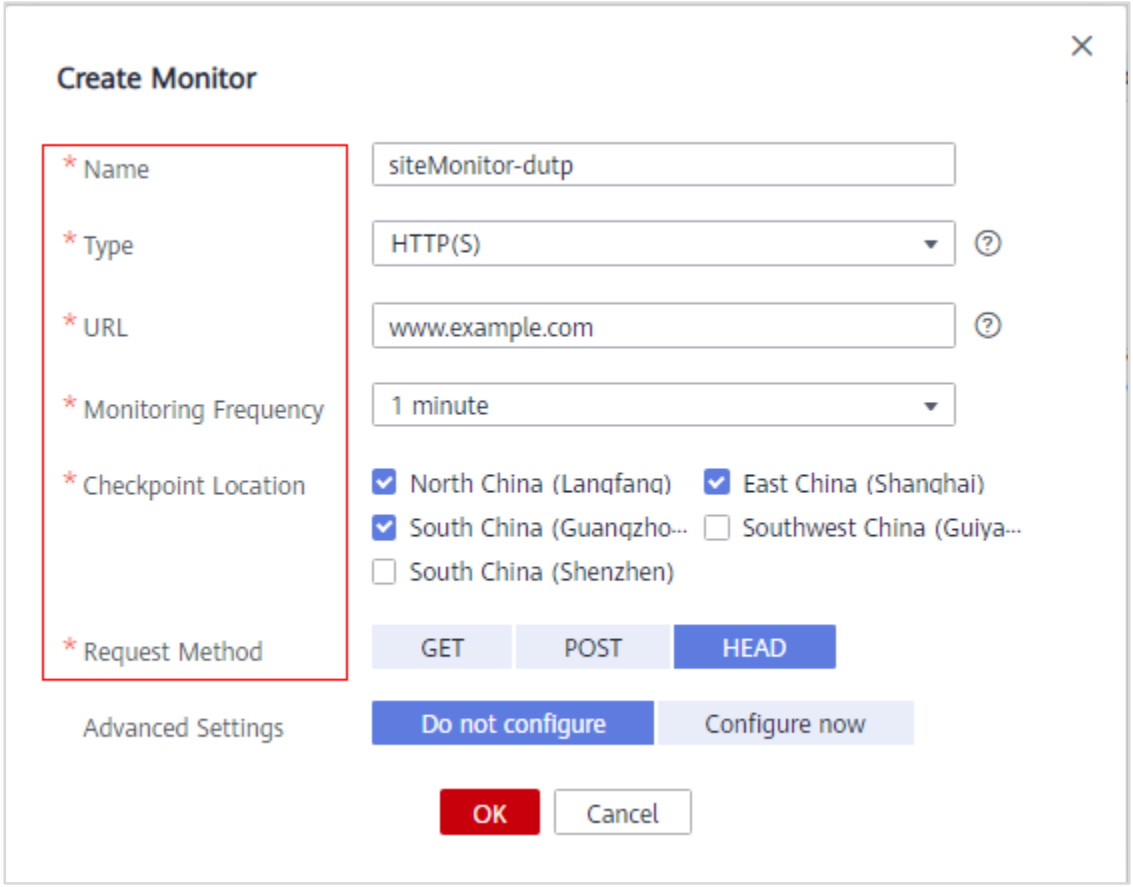
- Server monitoring comprises basic monitoring, OS monitoring, and process monitoring for servers.

Functions



Website Monitoring

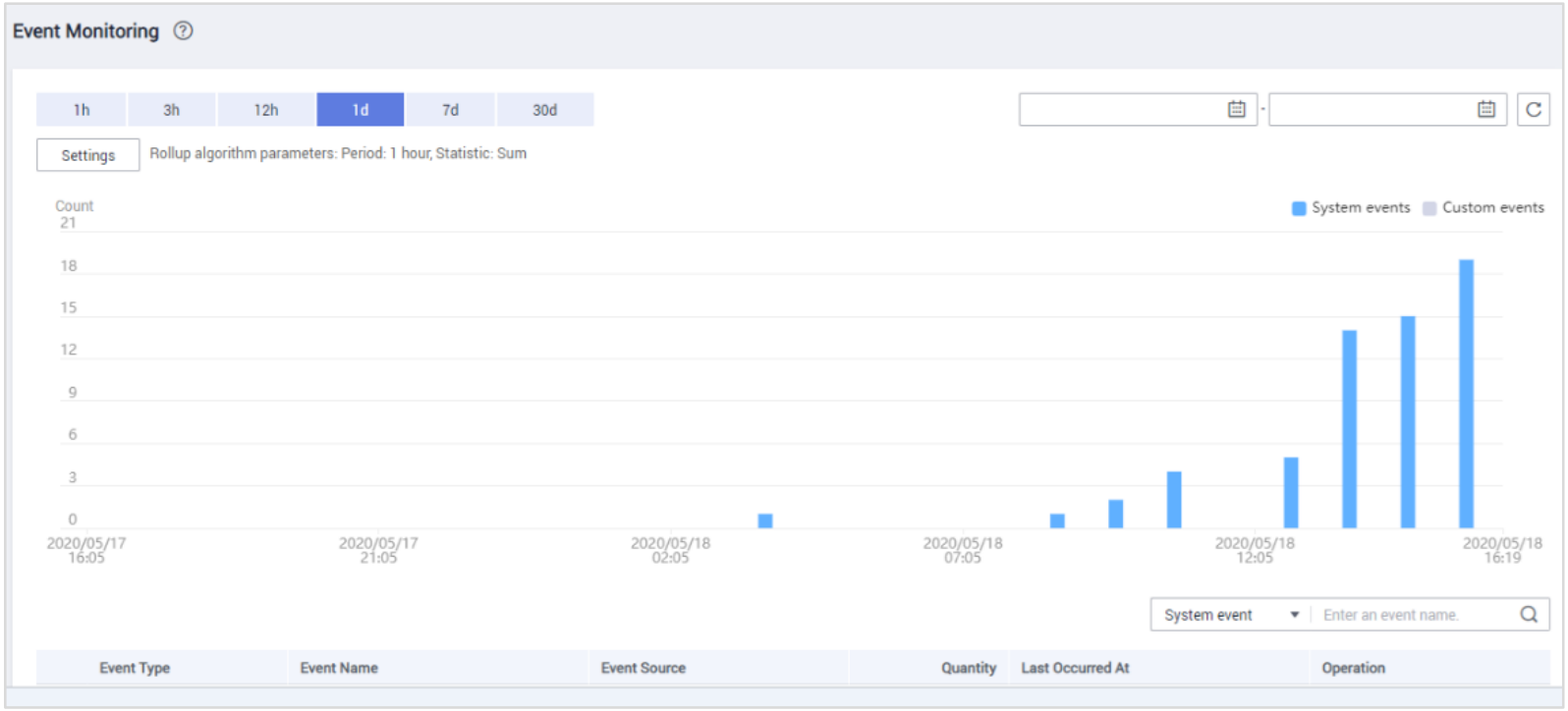
- Website monitoring is to continuously monitor remote server statuses, such as availability and connectivity, by simulating real users' access to remote servers.
- Website monitoring can detect availabilities of domain names and IP addresses, access response time, and packet loss rate, and generate alarms based on monitoring results.



HUAWEI

Event Monitoring

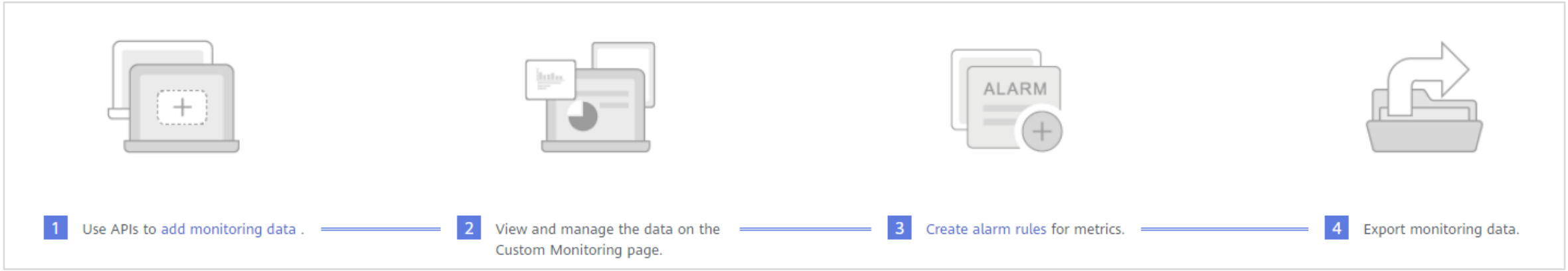
- In event monitoring, you can query system and custom events reported to Cloud Eye through the API. You can create alarm rules for both system and custom events. When specific events occur, Cloud Eye generates alarms for them.



HUAWEI

Custom Monitoring

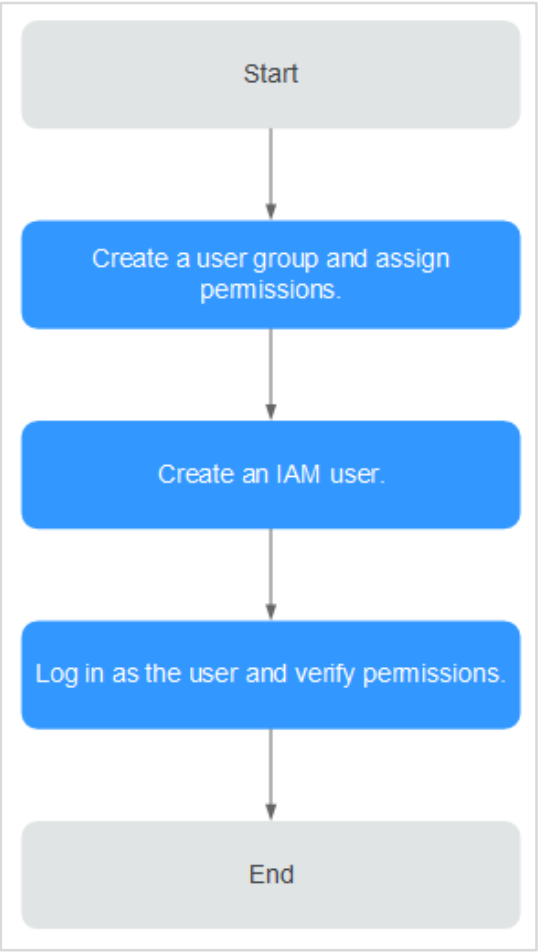
- The Custom Monitoring page displays all custom metrics reported by users. You can use simple API requests to publish collected monitoring data of those metrics to Cloud Eye for processing and display.



Permissions Management

Configuration:

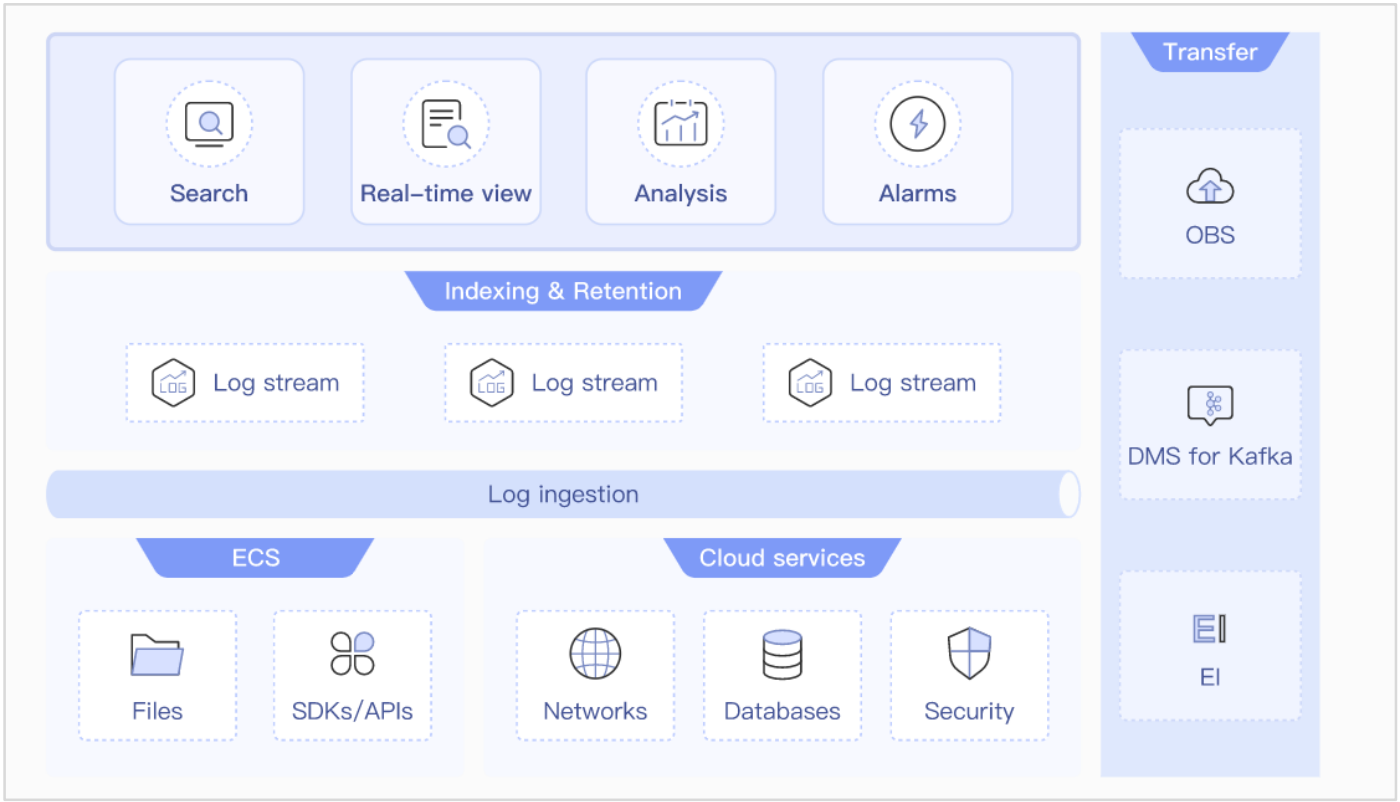
- Create a user group on the IAM console, and assign the **CES Administrator**, **Tenant Guest**, and **Server Administrator** policies to the group.
- Create a user on the IAM console and add the user to the created group.
- Log in to the Cloud Eye console as the created user, and verify that the user only has the **CES Administrator** permission.



Contents

Why Logs Matter?

- Logs are files generated by system processes and record important system information. They provide useful details for fault location and program commissioning.

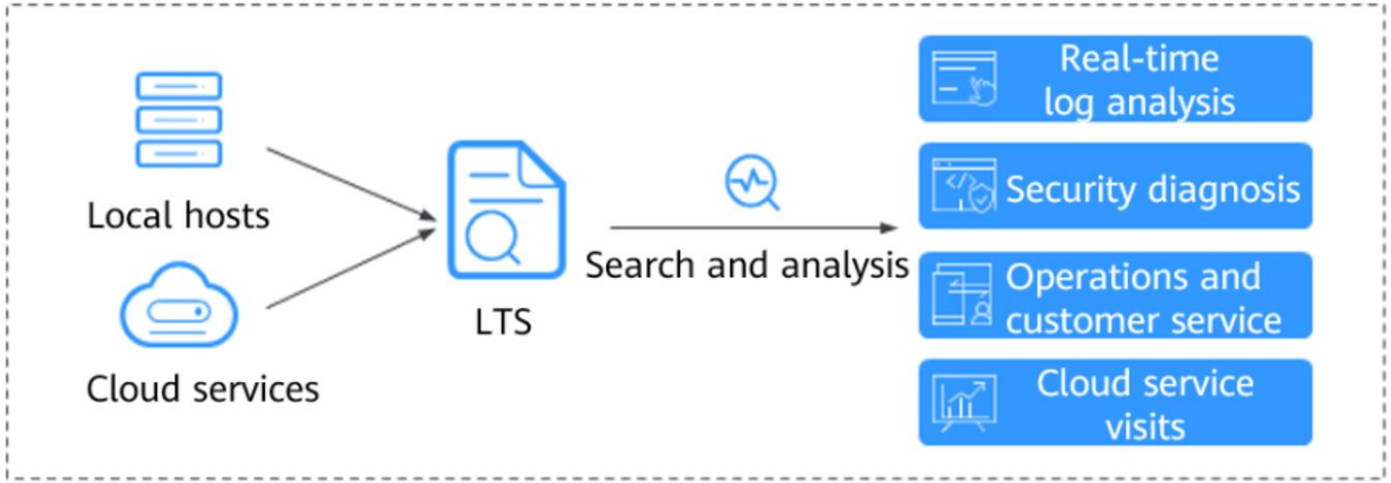


What Is Log Tank Service?

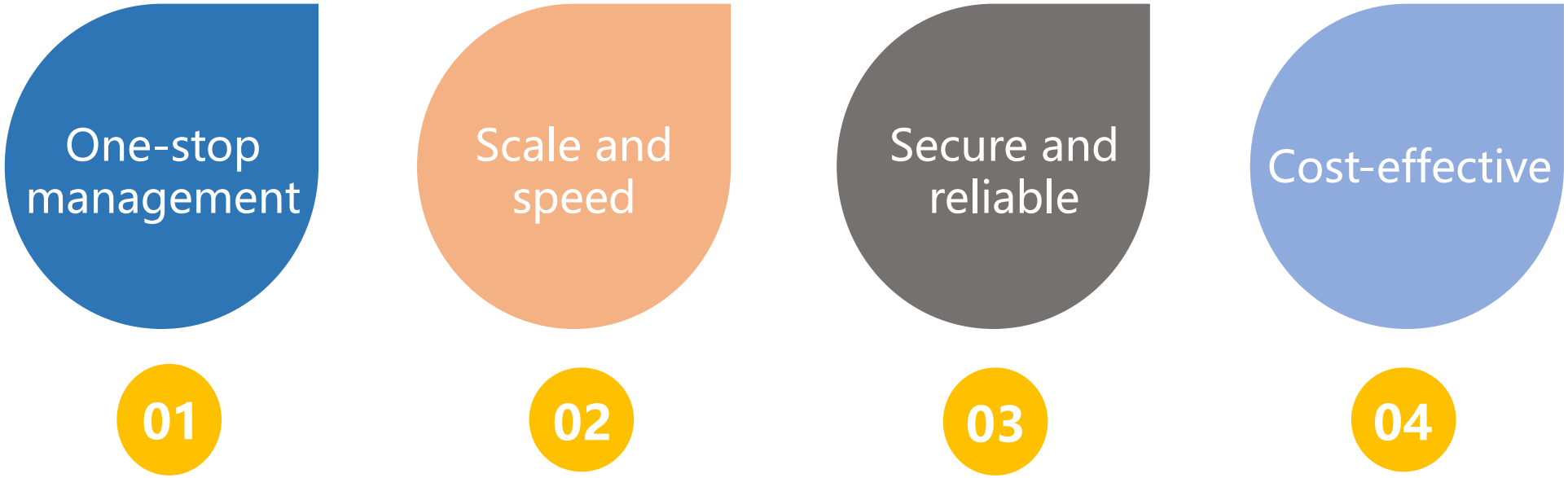
- Log Tank Service (LTS) collects logs from hosts and cloud services for centralized management, and processes large volumes of logs efficiently, securely, and in real-time. LTS provides you with the insights needed for optimizing availability and performance of cloud services and applications. It allows you to make faster data-driven decisions, perform device O&M easily, and analyze service trends.

Major functions:

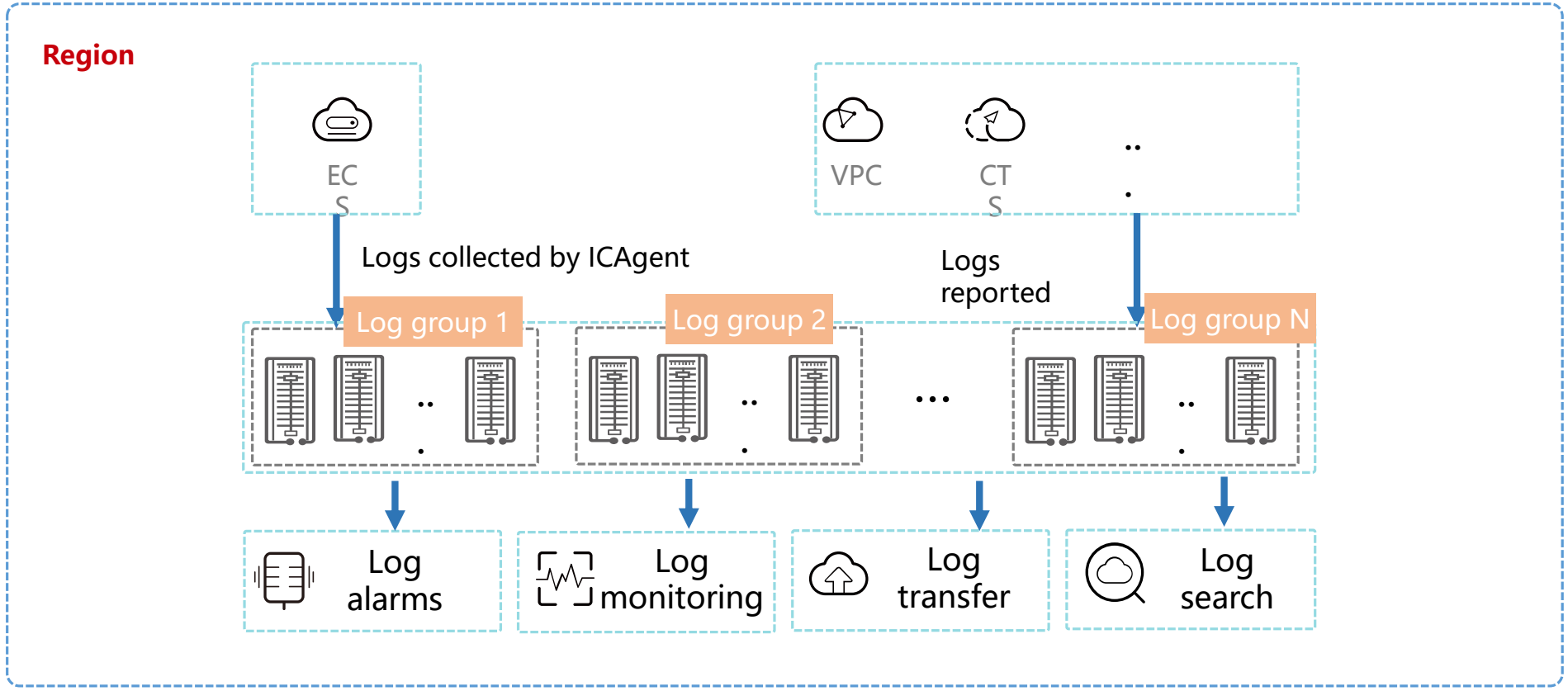
- Real-time log collection
- Log query and real-time analysis
- Log monitoring and alarms
- Log transfer



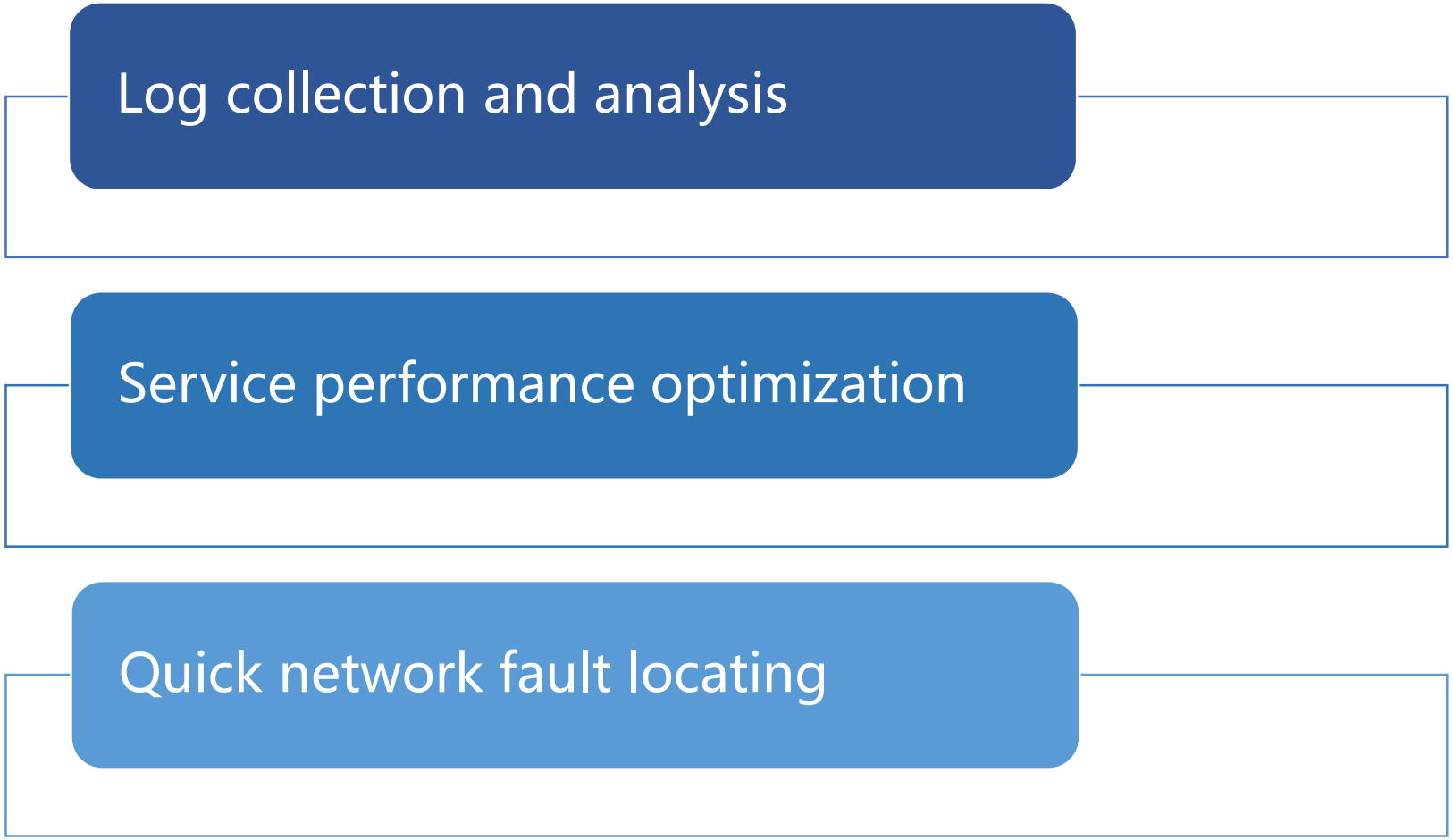
LTS Advantages



LTS Architecture

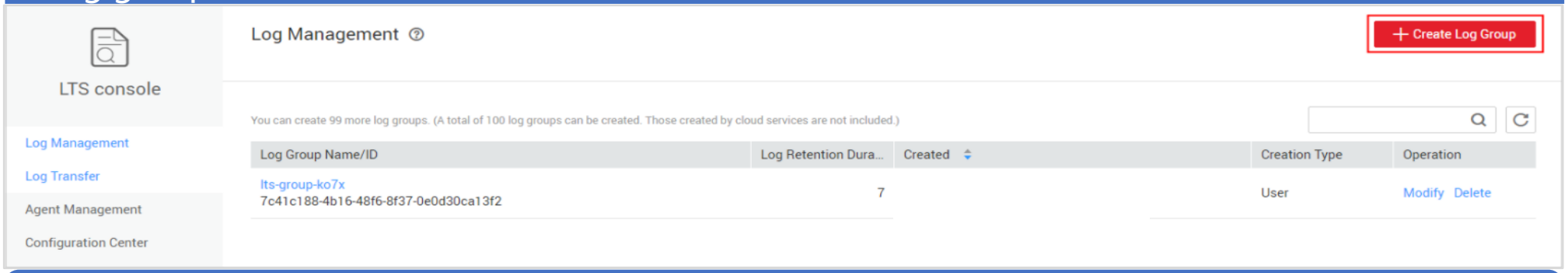


LTS Scenarios

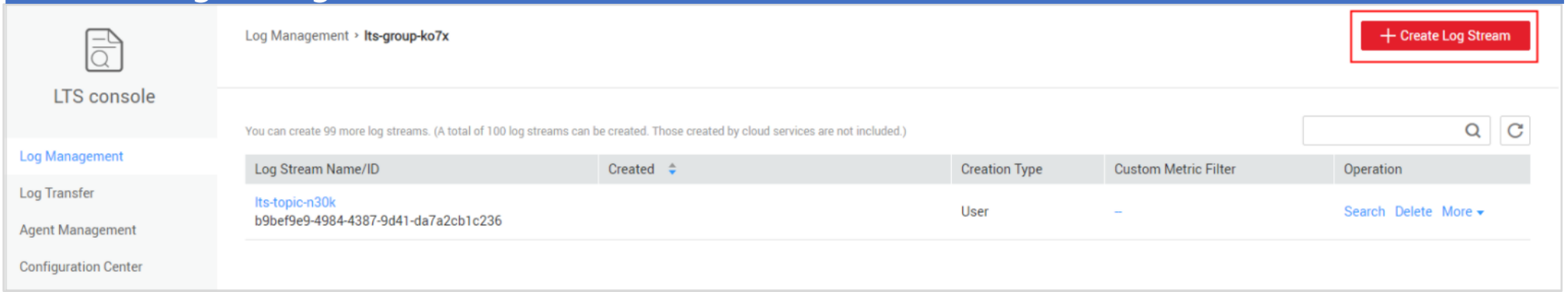


Using LTS: Basic Concepts

A log group is the basic unit in LTS for log management. You can set log retention duration for a log group.

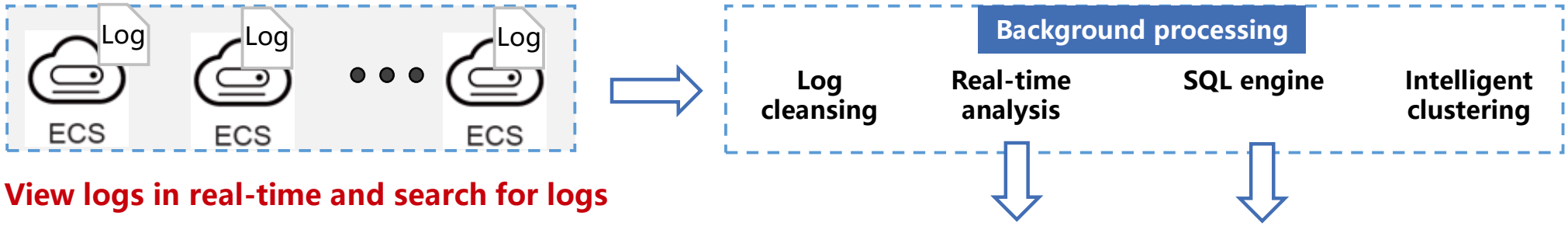


A log stream is the basic unit for log read and write. You can create log streams in a log group for finer log management.

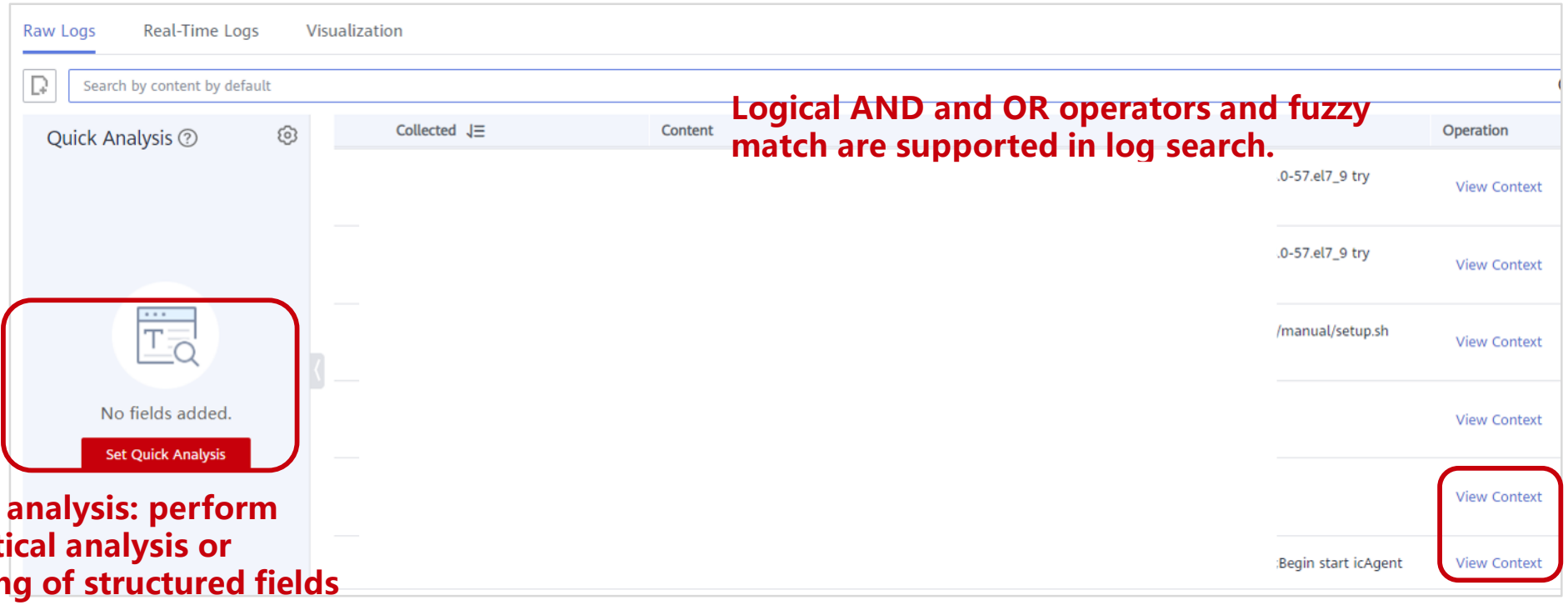


ICAgent is the log collection tool of LTS. If you want to collect logs from hosts, install ICAgent on the hosts.

Using LTS: Querying Logs



View logs in real-time and search for logs



Logical AND and OR operators and fuzzy match are supported in log search.

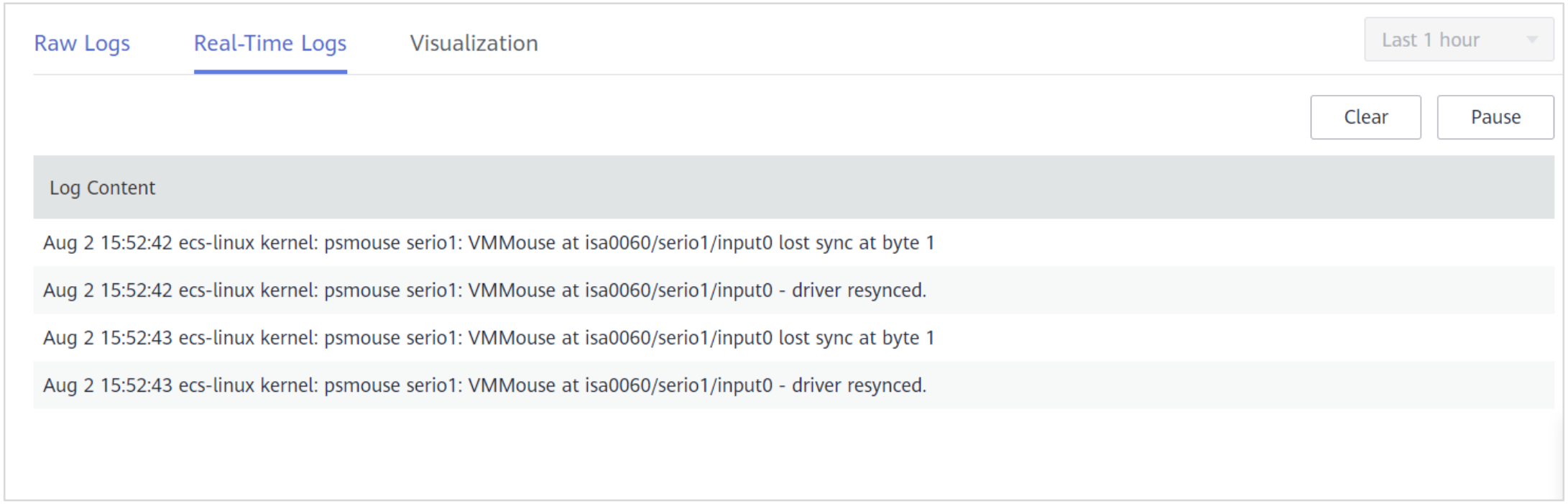
Quick analysis: perform statistical analysis or filtering of structured fields

View log contexts for more accurate analysis

HUAWEI

Using LTS: Viewing Real-Time Logs

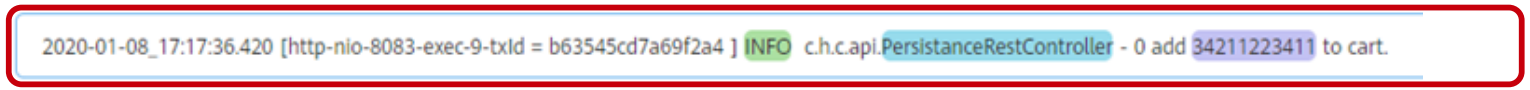
- You can view logs in real time on the Real-Time Logs tab, where the logs are updated every five seconds.



Using LTS: Structuring Logs

- After you add extraction rules, LTS uses these rules to convert raw logs to a structured format, facilitating execution of SQL queries.

Select a log event as a sample and extract fields.



You can extract fields from log texts in any format and easily generate regular expressions for log parsing on the UI.

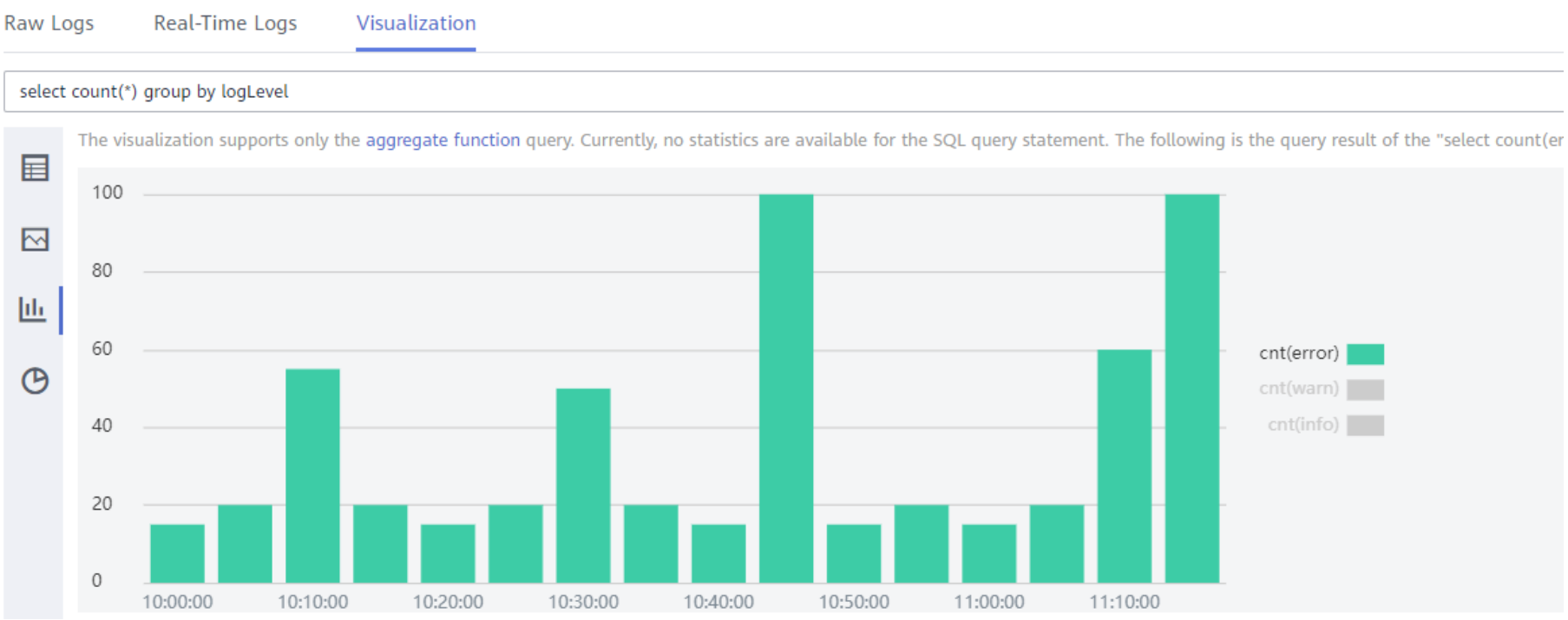
Statement	Description	Example
GROUP BY	Group results of one or more columns (generally used with aggregate functions).	select * group by (year),(month)
LIKE	Search for the specified pattern in a column in the WHERE clause.	
WHERE	Specify the selection condition.	

Common SQL syntax and aggregate functions are supported.

Function	Description	Example
count(*)	Calculate the number of tuples.	select count(*)
count (<column name>)	Calculate the number of values in a column.	select count(num)
min (<column name>)	Calculate the minimum value in a column.	select min(num)
max (<column name>)	Calculate the maximum value in a column.	select max(num)
avg (<column name>)	Calculate the average value in a column.	select avg(num)
sum (<column name>)	Calculate the sum of values in a column.	select sum(num)

Using LTS: Visualizing Logs

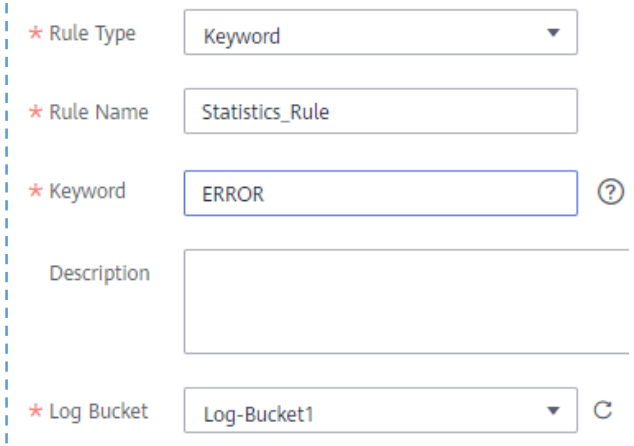
- You can visualize SQL query results in tables, trend charts, bar charts, or pie charts.



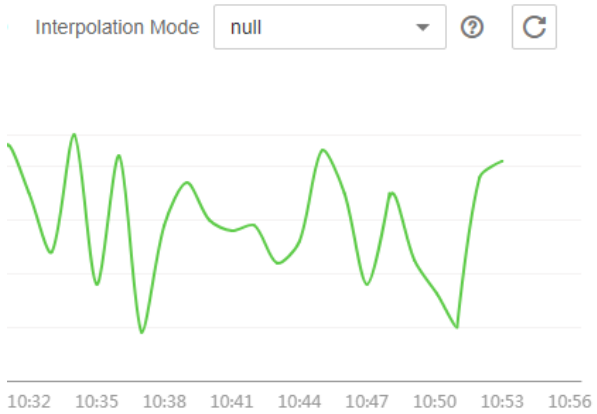
HUAWEI

Using LTS: Collecting Statistics and Configuring Alarms

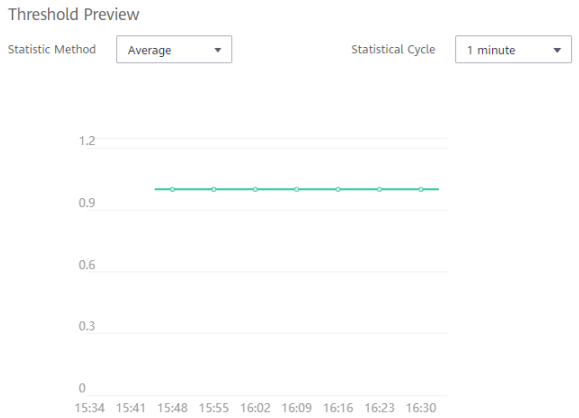
Step 1 Create a statistical rule



Step 2 Check the curve chart of keyword statistics



Step 3 Set a threshold



Step 4 Connect to the alarm center

Rule Name	Log Bucket	Rule Type	Keywords	Metric
count-error	count-error	Keywords	error	--

Keyword alarms support HTTP, email, and SMS notifications.

HUAWEI

Contents

What Is Auditing?

- Auditing is the process of gathering and analyzing evidence to evaluate an enterprise's financial statements, drawing conclusions and producing reports on the compliance of the statements to generally accepted standards, and communicating the audit results to stakeholders. An audit in the information and communications technology (ICT) industry is mainly an examination of the entire lifecycle of information systems.

Audits on enterprises will usually compare the following two aspects:

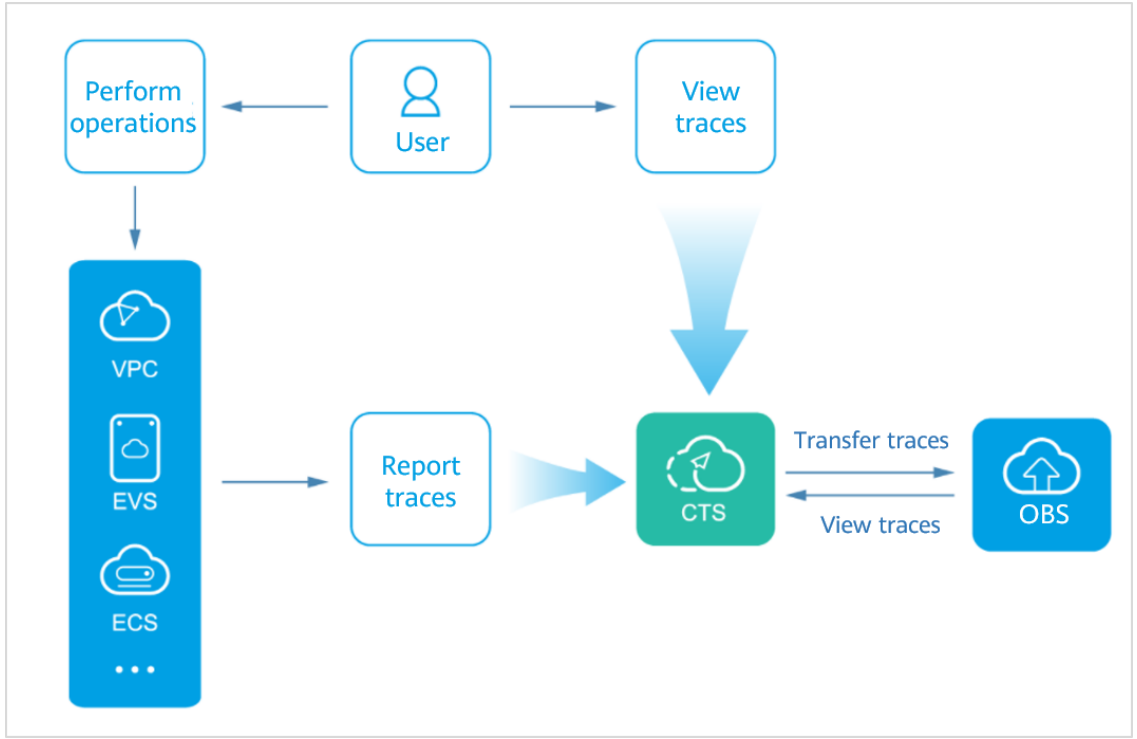
Purpose of Auditing

- Auditing is to check whether the information presented in an enterprise's financial statements is fair and accurate, helping the enterprise operate in a healthy manner. In the ICT industry, audits usually aim to examine whether information systems are running healthily.

HUAWEI

What Is Cloud Trace Service?

- Cloud Trace Service (CTS) records operations on cloud resources in your account. You can use the operation records (called traces in CTS) to perform security analysis, track resource changes, conduct compliance audits, and locate faults. You can also transfer the traces to Object Storage Service (OBS) in real time to store them for a longer period of time.



CTS Advantages

Traditional auditing

- Standardized audit processes cannot be carried out in traditional IT environments. Unauthorized API calls and console operations on servers, databases, OSs, and other resources cannot be systematically recorded in real time. System configuration changes are manually documented by IT staff.
- Audit records are manually documented. They do not have copies and cannot be stored for a long time.

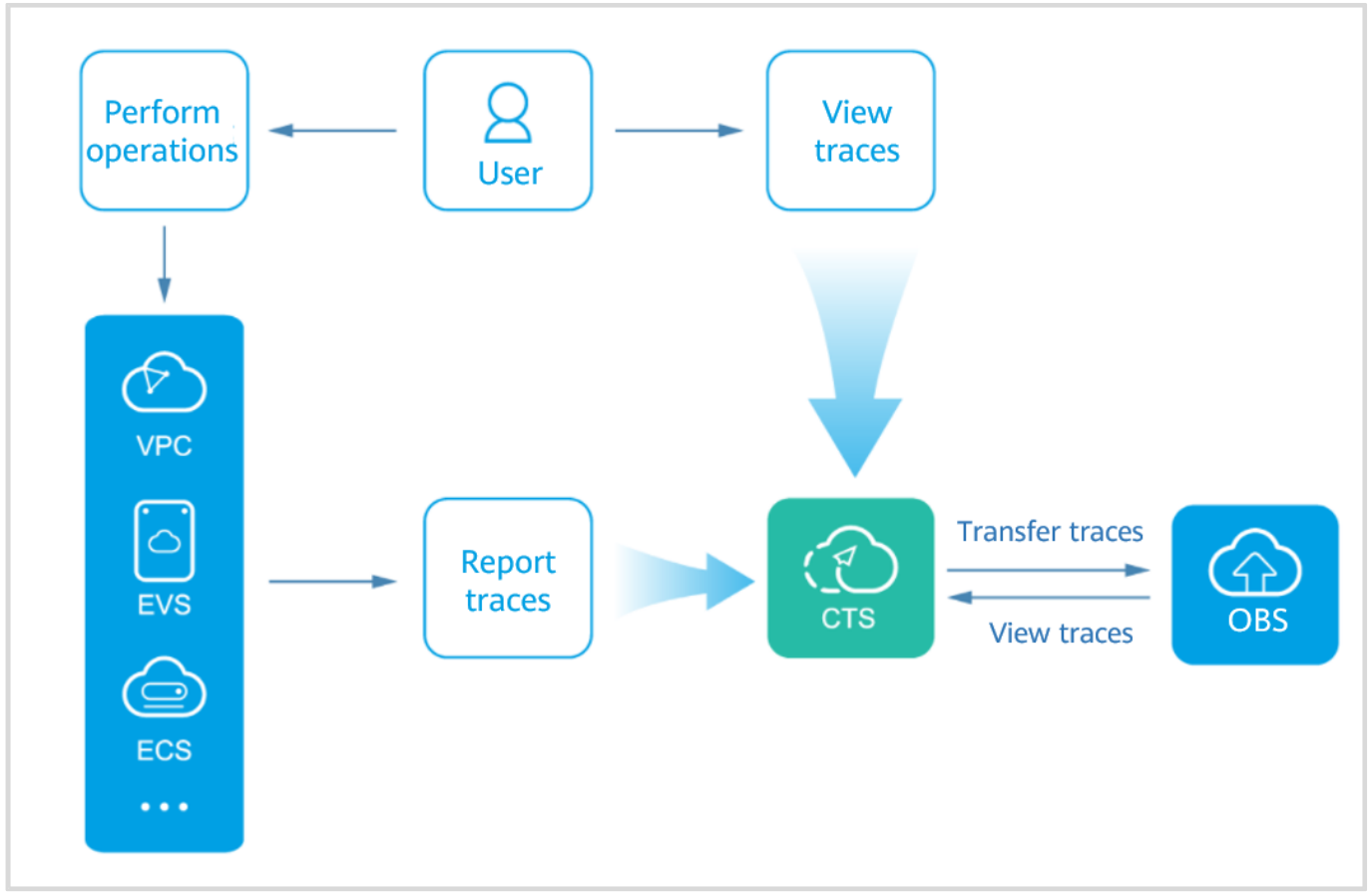
VS.

CTS

- All operations on cloud resources can be systematically recorded in real time. Manual efforts are not required.
- CTS can regularly merge traces into time-stamped files and transfer the files to OBS buckets for highly available and cost-effective long-term storage.

CTS Architecture

- **Major functions:**
  - Trace collection
  - Trace query
  - Trace transfer
  - Trace file encryption



CTS Basic Concepts

Tracker

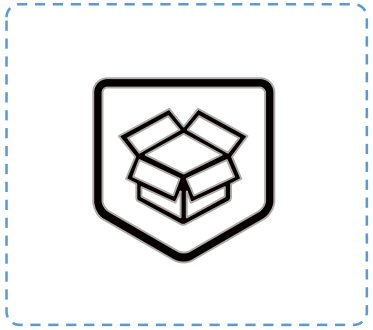
You need to enable CTS before using it. A tracker is automatically created when CTS is enabled. The tracker automatically identifies all cloud services you are using and records all operations performed on the services.

Trace

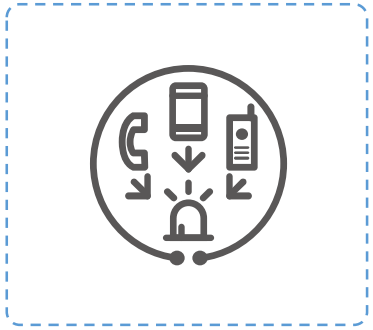
Traces are operation records captured and stored by CTS. Traces help you identify when a specific operation was performed by a specific user on a specific resource.

- Management traces
  - Traces reported by cloud services
- Data traces
  - Traces of read and write operations reported by OBS

CTS Scenarios



Resource tracking



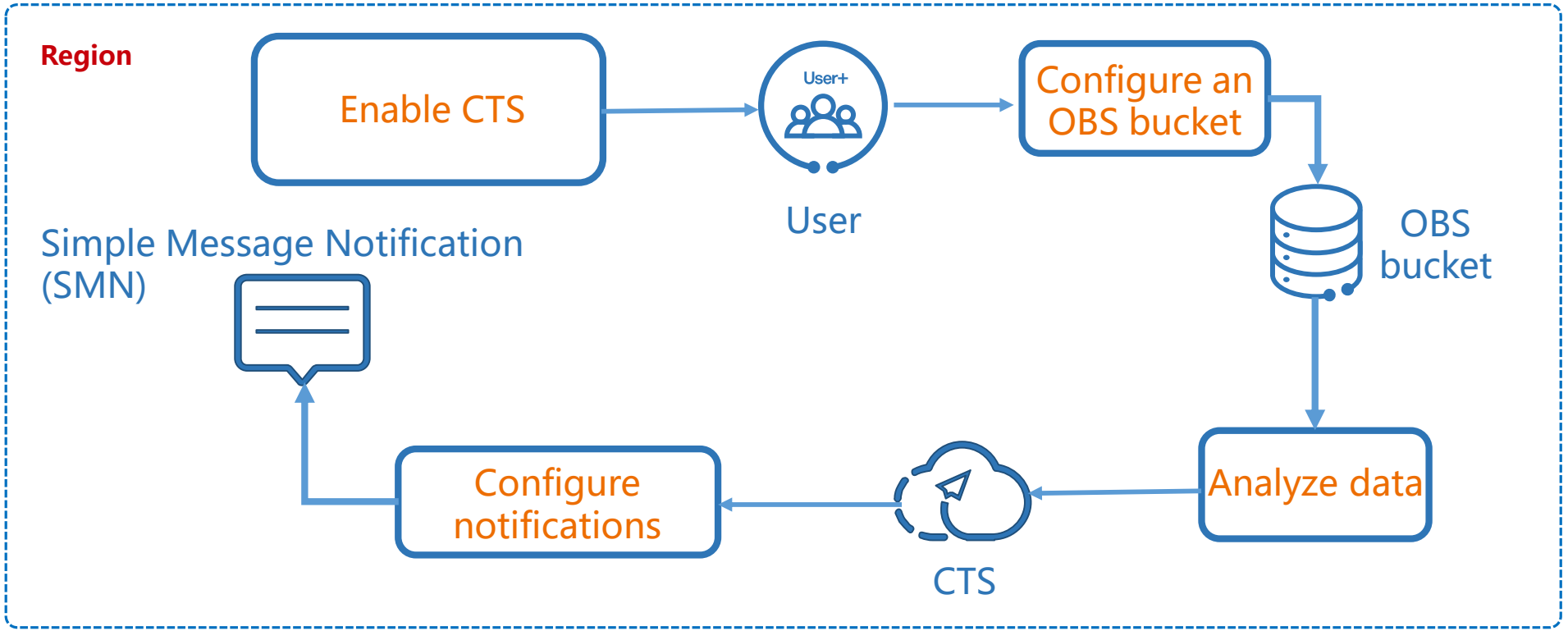
Compliance auditing

Fault locating

Security analysis

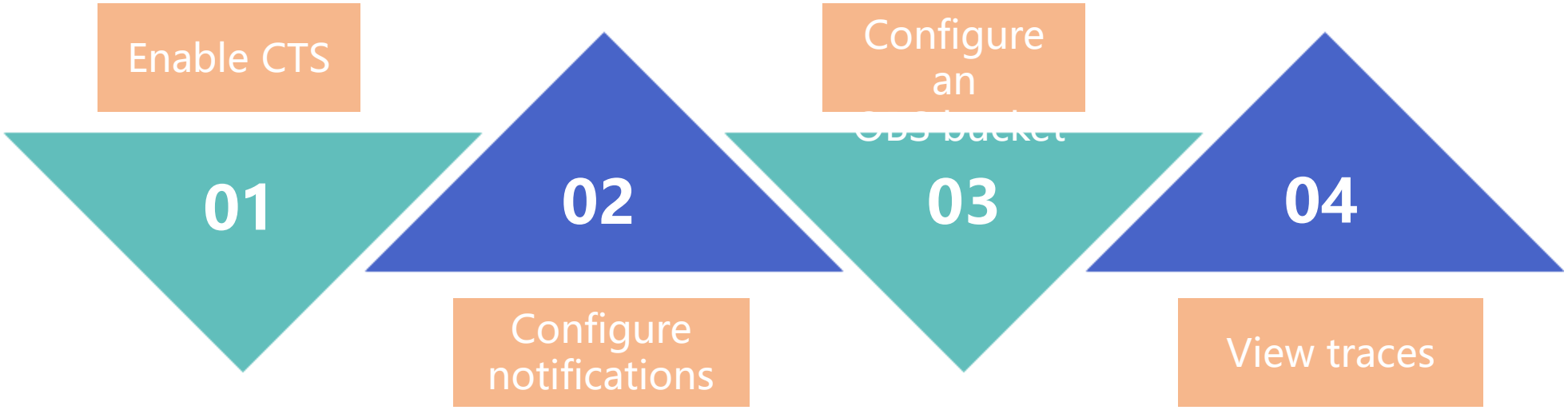
Using CTS: Security Analysis

- Each trace records details of an operation. You can identify when an operation was performed by a specific user and the IP address from which the operation was performed. You can perform security analysis and user behavior pattern analysis based on traces and configure notifications for key operations.



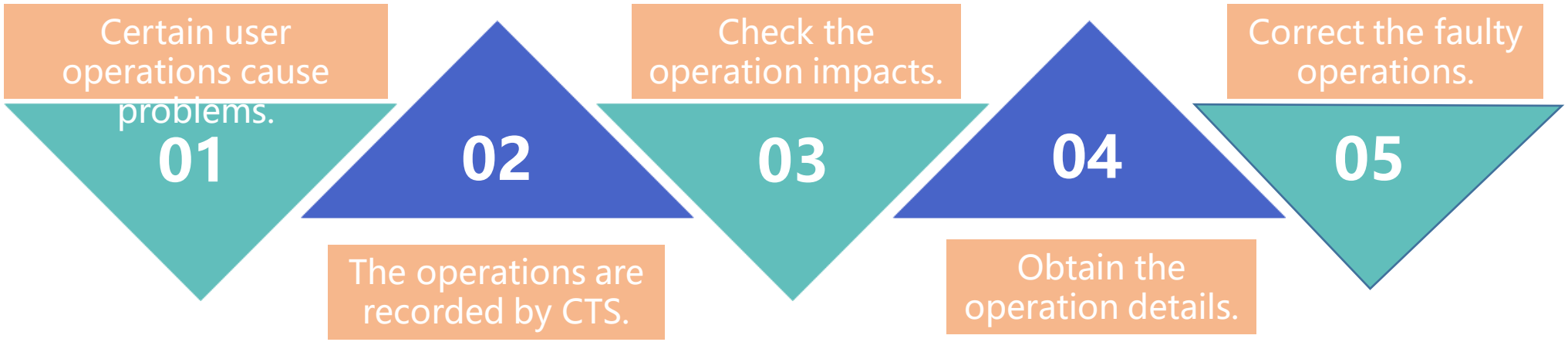
Using CTS: Resource Change Tracking

- CTS records resource changes and the change results, allowing you to track and analyze resource usage statistics.



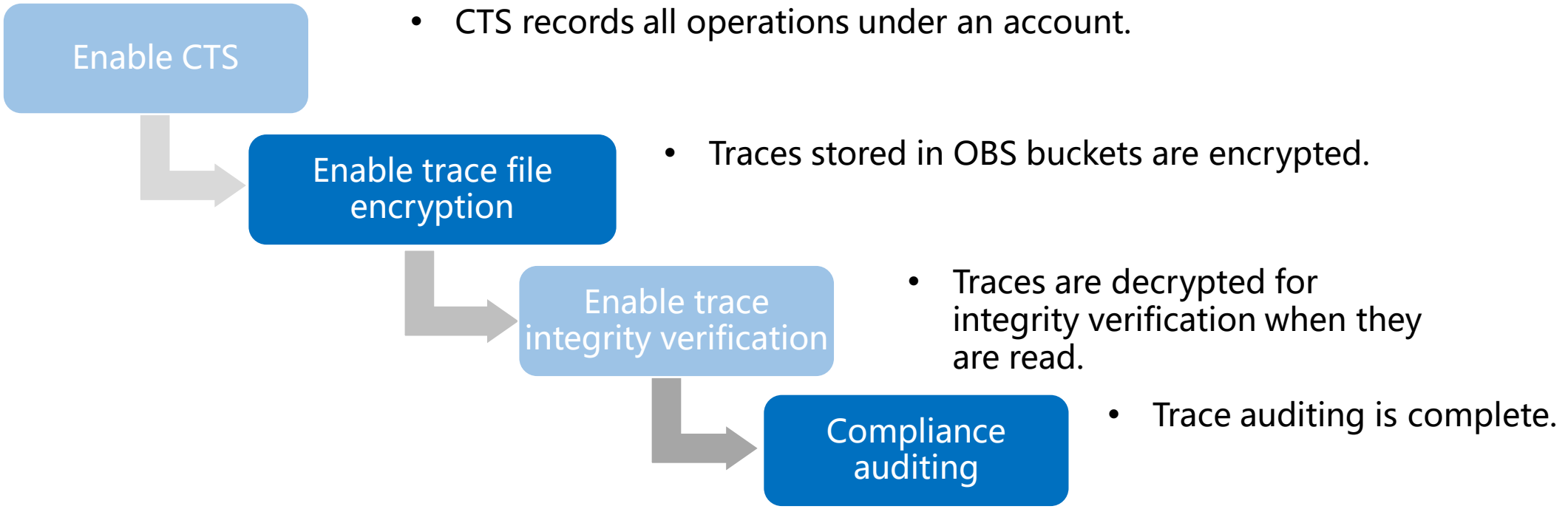
Using CTS: Fault Locating

- If a fault occurs, you can view CTS traces to figure out the cause and rectify the fault quickly. For example, you can quickly determine that the deletion of a system volume during configuration led to a failure in ECS capacity expansion.



Using CTS: Compliance Auditing

- CTS records operations and allows you to query operation records, making it easy to comply with internal policies and regulatory standards. This helps you meet the requirements of IT compliance certifications (for example, certifications for financial cloud and trusted cloud).

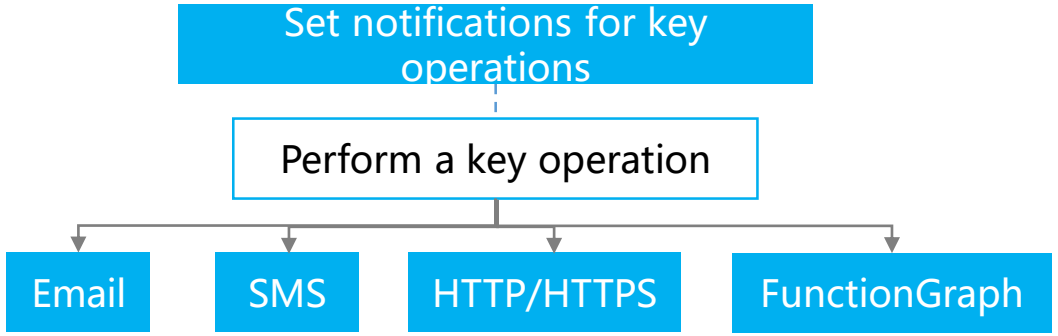


Using CTS: Key Event Notifications

- Traces can be set as triggers for notifications sent to emails, mobile phones, and system interfaces or as triggers to invoke FunctionGraph functions.

  Major functions:

  - You can be alerted of changes to core system components, networking, and security configurations so that risks can be detected and mitigated as soon as possible.
  - Traces collected by CTS can be synchronized to your own audit systems through HTTP/HTTPS notifications for independent auditing.
  - FunctionGraph can be triggered by traces to execute specific functions.



Quiz

1. Cloud Eye is a free cloud service.

   True

   False

2. Which of the following are scenarios of CTS?

   A. Resource tracking

   B. Compliance auditing

   C. Fault locating

   D. Security analysis

Summary

- O&M services play an important role in ensuring that platforms are secure and operate normally. We can use CTS to better manage platforms, and use Cloud Eye to monitor platforms in real time. With LTS, we can obtain logs in real time and evaluate and eliminate potential risks.

Recommendations

- Huawei Learning
  - https://e.huawei.com/en/talent/#/
- HUAWEI CLOUD Help Center
  - https://support.huaweicloud.com/intl/en-us/help-novice.html

Acronyms and Abbreviations

CTS: Cloud Trace Service

ECS: Elastic Cloud Server

IT: Internet technology

ICT: Information and communications technology

IAM: Identity and Access Management

LTS: Log Tank Service

OBS: Object Storage Service

SOA: Service-oriented architecture

Acronyms and Abbreviations

SQL: Structured query language

VPC: Virtual Private Cloud

Thank you.

把数字世界带入每个人、每个家庭、
每个组织,构建万物互联的智能世界.

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

HUAWEI