

Application Operations Management

User Guide

Issue 01
Date 2024-04-15



Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2024. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Cloud Computing Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI 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 Service Overview.....	1
1.1 What Is AOM?.....	1
1.2 Product Architecture.....	3
1.3 Functions.....	3
1.4 Scenarios.....	5
1.5 Metric Overview.....	5
1.5.1 Introduction.....	6
1.5.2 Network Metrics and Dimensions.....	6
1.5.3 Disk Metrics and Dimensions.....	7
1.5.4 File System Metrics and Dimensions.....	8
1.5.5 Host Metrics and Dimensions.....	9
1.5.6 Container Metrics and Dimensions.....	13
1.5.7 VM Metrics and Dimensions.....	17
1.5.8 Instance Metrics and Dimensions.....	18
1.5.9 Service Metrics and Dimensions.....	19
1.6 Restrictions.....	19
1.7 Privacy and Sensitive Information Protection Statement.....	24
1.8 Glossary.....	24
1.9 Permissions.....	26
2 Getting Started.....	31
2.1 Process of Using AOM.....	31
2.2 Installing an ICAgent.....	33
2.3 Creating Alarm Rules and Viewing Alarms.....	33
3 User Guide.....	38
3.1 Monitoring Overview.....	38
3.2 Dashboard.....	40
3.2.1 Creating a Dashboard.....	40
3.2.2 Setting the Full-Screen Online Duration.....	46
3.2.3 Graph Description.....	48
3.3 Alarm Management.....	52
3.3.1 Alarm Rules.....	52
3.3.1.1 Introduction.....	52

3.3.1.2 Creating a Metric Alarm Rule.....	52
3.3.1.3 Creating an Alarm Template.....	63
3.3.1.4 Creating an Event Alarm Rule.....	66
3.3.1.5 Managing Alarm Rules.....	68
3.3.2 Viewing Alarms.....	69
3.3.3 Viewing Events.....	70
3.3.4 Alarm Action Rules.....	71
3.3.4.1 Overview.....	71
3.3.4.2 Creating an Alarm Action Rule.....	71
3.3.4.3 Creating a Message Template.....	73
3.4 Metric Browsing.....	76
3.5 Infrastructure Monitoring.....	78
3.5.1 Application Monitoring.....	78
3.5.2 Component Monitoring.....	80
3.5.3 Host Monitoring.....	81
3.6 Prometheus Monitoring.....	84
3.7 Log Analysis.....	85
3.7.1 Searching for Logs.....	85
3.7.2 Viewing Log Files.....	87
3.7.3 Configuring VM Log Collection Paths.....	88
3.7.4 Adding Log Dumps.....	89
3.7.5 Accessing LTS.....	93
3.7.5.1 Introduction.....	93
3.7.5.2 Managing Access Rules.....	96
3.8 Configuration Management.....	98
3.8.1 Log Configuration.....	98
3.8.1.1 Viewing the Log Quota.....	98
3.8.1.2 Configuring Delimiters.....	98
3.8.2 Configuring Application Discovery.....	101
3.8.3 Access Management.....	106
3.8.3.1 Introduction.....	106
3.8.3.2 Reporting Prometheus Data to AOM.....	106
3.8.3.3 Viewing Metric Data in AOM Using Grafana.....	108
3.9 Collection Management.....	112
3.9.1 Installing an ICAgent.....	112
3.9.2 Upgrading the ICAgent.....	116
3.9.3 Uninstalling the ICAgent.....	117
3.10 Permissions Management.....	119
3.10.1 Creating a User and Granting Permissions.....	120
3.10.2 Creating a Custom Policy.....	121
3.11 Remarks.....	122
3.11.1 Prometheus Statements.....	122

3.11.2 What Is the Relationship Between the Time Range and Statistical Period?.....	123
4 FAQs.....	124
4.1 What Can I Do If an ICAgent Is Offline?.....	124
4.2 How Do I Obtain an AK/SK?.....	125
4.3 What Can I Do If Resources Are Not Running Properly?.....	125
4.4 How Can I Do If I Do Not Have the Permission to Access SMN?.....	127
4.5 How Do I Distinguish Alarms from Events?.....	127
4.6 Does AOM Display Logs in Real Time?.....	128
4.7 Why Is the Application Status Normal but the Component Status Abnormal?.....	128
5 Best Practices.....	129
5.1 Discovering Applications.....	129
A Change History.....	132

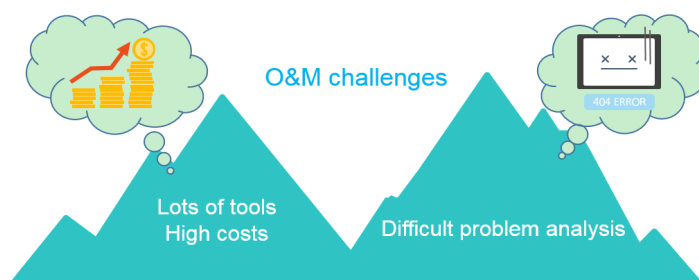
1 Service Overview

1.1 What Is AOM?

Challenges

With the popularization of container technologies, lots of enterprises develop applications using microservice frameworks. Because the number of cloud services increases, enterprises gradually turn to cloud O&M. However, they face the following O&M challenges:

Figure 1-1 Existing O&M issues



- Cloud O&M has high requirements on personnel skills. O&M tools are hard to configure. Multiple systems need to be maintained at the same time. Distributed tracing systems face high learning and usage costs, but have poor stability.
- Distributed applications face analysis difficulties such as how to visualize the dependency between microservices, improve user experience, associate scattered logs for analysis, and quickly trace problems.

Introduction to AOM

Figure 1-2 One-stop O&M platform



Application Operations Management (AOM) is a one-stop, multi-dimensional O&M management platform for cloud applications. It monitors your applications and related cloud resources, analyzes application health status in real time, and provides flexible data visualization functions, helping you monitor running status of applications, resources, and services in real time and detect faults in a timely manner.

Advantages

Figure 1-3 AOM advantage 1



Multi-Dimensional O&M

Provides one-stop multi-dimensional O&M platform for mobile apps, networks, services, middleware, and cloud resources.

Figure 1-4 AOM advantage 2



Health Check

Monitors service health in real time and detects exceptions or performance bottlenecks within minutes.



Ease of Use

Connects to applications without having to modify codes and collects data in a non-intrusive way.

- **Management over massive quantities of logs**

AOM supports log search and service analysis, automatically associates logs for cluster analysis, and filters logs by application, host, file, or instance.

- **Association analysis**

AOM automatically associates applications and resources and displays data in a panorama view. Through analysis of metrics and alarms about applications, components, instances, hosts, and transactions, AOM allows you to easily locate faults.

- **Open ecosystem**
O&M data query APIs are opened, collection standards are provided, and independent development is supported.

1.2 Product Architecture

AOM is a multi-dimensional O&M platform that focuses on resource data and associates log, metric, resource, alarm, and event data. It consists of the data collection and access layer, transmission and storage layer, and service computing layer.

Architecture Description

- **Data collection and access layer**
 - Collecting data by using ICAgent
You can install the ICAgent (a plug-in data collector) on a host and use it to report O&M data.
 - Connecting data by using APIs
You can connect service metrics to AOM as custom metrics using AOM open APIs or Exporter APIs.
- **Transmission and storage layer**
 - Data transmission: AOM Access is a proxy for receiving O&M data. After O&M data is received, such data will be placed in the Kafka queue. Kafka then transmits the data to the service computing layer in real time based on its high-throughput capability.
 - Data storage: After being processed by the AOM backend, O&M data is written into a database. Cassandra stores sequential data, Redis is used for cache query, etcd stores AOM configuration data, and Elasticsearch stores resources, logs, alarms, and events.
- **Service computing layer**
AOM provides basic O&M services such as alarm management, log management, and resource monitoring (such as metric monitoring).

1.3 Functions

Application Monitoring

Application monitoring allows you to view application resource usage, trends, and alarms in real time, so that you can make fast responses to ensure smooth running for applications.

This function adopts the hierarchical drill-down design. The hierarchy is as follows: Application list > Application details > Component details > Instance details > Process details. Applications, components, instances, and processes are visually associated with each other on the console.

Host Monitoring

Host monitoring allows you to view host resource usage, trends, and alarms in real time, so that you can make fast responses and ensure smooth running for hosts.

Like application monitoring, this function also adopts the hierarchical drill-down design. The hierarchy is as follows: Host list > Host details. The details page contains all the instances, GPUs, NICs, disks, and file systems of the current host.

Automatic Discovery of Applications

After you deploy applications on hosts, the ICAgent installed on the hosts automatically collects information, including names of processes, components, containers, and Kubernetes pods. Applications are automatically discovered and their graphs are displayed on the console. You can then set aliases and groups for better resource management.

Dashboards

With a dashboard, different graphs can be displayed on the same screen. Various graphs, such as line graphs, digit graphs, and top N resource graphs enable you to monitor data comprehensively.

For example, you can add key metrics to a dashboard for real-time monitoring. You can also compare the same metric of different resources on one screen. In addition, by adding common O&M metrics to a dashboard, you do not need to reselect them when re-opening the AOM console during routine O&M.

Alarm Management

The alarm list helps you manage alarms and events.

You can create alarm rules for key resource metrics. When the metric value reaches the threshold, AOM will generate alarms. An event alarm is generated when the resource data meets the event condition. A threshold-crossing alarm is generated when the metric data of a resource meets the threshold condition and an insufficient data event is generated when no metric data is reported, so that you can discover and handle exceptions at the earliest time. When an alarm is reported, alarm information will be sent to specified personnel by email or SMS based on alarm action rules. Therefore, such personnel can rectify faults in time to avoid service loss.

Log Management

AOM provides powerful log management capabilities. Log search enables you to quickly search for required logs from massive quantities of logs. Log dump enables you to store logs for a long period. By configuring delimiters, you can divide log content into multiple words and use these words to search for logs.

Metric Browsing

The **Metric Browsing** page displays metric data of each resource. You can monitor metric values and trends in real time, and create alarm rules for desired metrics. In

this way, you can monitor services in real time and perform data correlation analysis.

Prometheus Monitoring

AOM is fully connected with the open-source Prometheus ecosystem. It monitors many types of components, provides multiple ready-to-use dashboards, and supports flexible expansion of cloud-native component metric plug-ins.

1.4 Scenarios

Problem Inspection and Demarcation

During routine O&M, it is hard to locate faults and obtain logs. Therefore, a monitoring platform is required to monitor resources, logs, and application performance.

AOM interconnects with application services, and collects O&M data of infrastructures, middleware, and application instances in one stop. Through metric monitoring, log analysis, and alarm reporting, AOM enables you to monitor the application running status and resource usage easily, and detect and demarcate problems in a timely manner.

Advantages

- Automatic discovery: Collectors are deployed to proactively discover and monitor applications based on different runtime environments.
- Distributed application monitoring: AOM serves as a unified O&M platform that enables you to implement multi-dimensional monitoring over distributed applications with multiple cloud services.
- Alarm notification: Multiple exception detection policies, alarm trigger modes, and APIs are provided.

Multi-Dimensional O&M

You need to monitor comprehensive system running status and make fast response to various problems.

AOM provides multi-dimensional O&M capabilities from the cloud level to the resource level and from application monitoring to microservice tracing.

Advantages

- User experience assurance: Service health KPIs are monitored in real time and root causes of exceptions are analyzed.
- Fast fault diagnosis: Distributed tracing enables you to locate faults quickly.
- Resource running assurance: Hundreds of O&M metrics about resources such as containers, disks, and networks are monitored in real time, and clusters, VMs, applications, and containers are associated for analysis.

1.5 Metric Overview

1.5.1 Introduction

Metrics reflect resource performance data or status. A metric consists of a **namespace**, **dimension**, name, and unit. Metrics can be divided into:

Metric Namespaces

A namespace is an abstract collection of resources and objects. Metrics in different namespaces are independent of each other so that metrics of different applications will not be aggregated to the same statistics information.

- Namespaces of system metrics are fixed and started with **PAAS.**. For details, see [Table 1-1](#).

Table 1-1 Namespaces of system metrics

Namespace	Description
PAAS.NODE	Namespace of host, network, disk, and file system metrics
PAAS.CONTAINER	Namespace of component, instance, process, and container metrics

- Namespaces of custom metrics must be in the XX.XX format. Each namespace must be 3 to 32 characters long, starting with a letter (excluding **PAAS.**, **SYS.**, and **SRE.**). Only digits, letters, and underscores (_) are allowed.

Dimensions

Metric dimensions indicate the categories of metrics. Each metric has certain features, and a dimension may be considered as a category of such features.

- Dimensions of system metrics are fixed. Different types of metrics have different dimensions. For more details, see the following sections.
- Dimensions of custom metrics must be 1 to 32 characters long, which need to be customized.

1.5.2 Network Metrics and Dimensions

Table 1-2 Network metrics

Metric	Description	Value Range	Unit
Downlink rate (BPS) (aom_node_network_receive_bytes)	Inbound traffic rate of a measured object	≥ 0	Byte/s
Downlink rate (PPS) (aom_node_network_receive_packets)	Number of data packets received by an NIC per second	≥ 0	Packet/s

Metric	Description	Value Range	Unit
Downlink error rate (aom_node_network_receive_error_packets)	Number of error packets received by an NIC per second	≥ 0	Count/s
Uplink rate (BPS) (aom_node_network_transmit_bytes)	Outbound traffic rate of a measured object	≥ 0	Byte/s
Uplink error rate (aom_node_network_transmit_error_packets)	Number of error packets sent by an NIC per second	≥ 0	Count/s
Uplink rate (PPS) (aom_node_network_transmit_packets)	Number of data packets sent by an NIC per second	≥ 0	Packet/s
Total rate (BPS) (aom_node_network_total_bytes)	Total inbound and outbound traffic rate of a measured object	≥ 0	Byte/s

Table 1-3 Dimensions of network metrics

Dimension	Description
clusterId	Cluster ID
hostID	Host ID
nameSpace	Cluster namespace
netDevice	NIC name
nodeIP	Host IP address
nodeName	Host name

1.5.3 Disk Metrics and Dimensions

Table 1-4 Disk metrics

Metric	Description	Value Range	Unit
Disk read rate (aom_node_disk_read_kilobytes)	Volume of data read from a disk per second	≥ 0	KB/s

Metric	Description	Value Range	Unit
Disk write rate (aom_node_disk_write_kilobytes)	Volume of data written into a disk per second	≥ 0	KB/s

Table 1-5 Dimensions of disk metrics

Dimension	Description
clusterId	Cluster ID
diskDevice	Disk name
hostID	Host ID
nameSpace	Cluster namespace
nodeIP	Host IP address
nodeName	Host name

1.5.4 File System Metrics and Dimensions

Table 1-6 File system metrics

Metric	Description	Value Range	Unit
Available disk space (aom_node_disk_available_capacity_megabytes)	Disk space that has not been used	≥ 0	MB
Total disk space (aom_node_disk_capacity_megabytes)	Total disk space	≥ 0	MB
Disk read/write status (aom_node_disk_rw_status)	Read or write status of a disk	0 or 1 <ul style="list-style-type: none"> • 0: read / write • 1: read - only 	N/A

Metric	Description	Value Range	Unit
Disk usage (aom_node_disk_usage)	Percentage of the used disk space to the total disk space	0-100	%

Table 1-7 Dimensions of file system metrics

Dimension	Description
clusterId	Cluster ID
clusterName	Cluster name
fileSystem	File system
hostID	Host ID
mountPoint	Mount point
nameSpace	Cluster namespace
nodeIP	Host IP address
nodeName	Host name

1.5.5 Host Metrics and Dimensions

Table 1-8 Host metrics

Metric	Description	Value Range	Unit
Total CPU cores (aom_node_cpu_limit_core)	Total number of CPU cores that have been applied for a measured object	≥ 1	Cores
Used CPU cores (aom_node_cpu_used_core)	Number of CPU cores used by a measured object	≥ 0	Cores
CPU usage (aom_node_cpu_usage)	CPU usage of a measured object	0-100	%
Available physical memory (aom_node_memory_free_megabytes)	Available physical memory of a measured object	≥ 0	MB

Metric	Description	Value Range	Unit
Available virtual memory (aom_node_virtual_memory_free_megabytes)	Available virtual memory of a measured object	≥ 0	MB
Total GPU memory (aom_node_gpu_memory_free_megabytes)	Total GPU memory of a measured object	> 0	MB
GPU memory usage (aom_node_gpu_memory_usage)	Percentage of the used GPU memory to the total GPU memory	0-100	%
Used GPU memory (aom_node_gpu_memory_used_megabytes)	GPU memory used by a measured object	≥ 0	MB
GPU usage (aom_node_gpu_usage)	GPU usage of a measured object	0-100	%
Total NPU memory (aom_node_npu_memory_free_megabytes)	Total NPU memory of a measured object	> 0	MB
NPU memory usage (aom_node_npu_memory_usage)	Percentage of the used NPU memory to the total NPU memory	0-100	%
Used NPU memory (aom_node_npu_memory_used_megabytes)	NPU memory used by a measured object	≥ 0	MB
NPU usage (aom_node_npu_usage)	NPU usage of a measured object	0-100	%
NPU temperature (aom_node_npu_temperature_centrigrade)	NPU temperature of a measured object	-	°C
Physical memory usage (aom_node_memory_usage)	Percentage of the used physical memory to the total physical memory	0-100	%

Metric	Description	Value Range	Unit
Host status (aom_node_status)	Host status	<ul style="list-style-type: none"> 0: Normal 1: Abnormal 	N/A
NTP offset (aom_node_ntp_offset_ms)	Offset between the local time of the host and the NTP server time. The closer the NTP offset is to 0, the closer the local time of the host is to the time of the NTP server.	-	ms
NTP server status (aom_node_ntp_server_status)	Whether the host is connected to the NTP server	0 or 1 <ul style="list-style-type: none"> 0: Connected 1: Unconnected 	N/A
NTP synchronization status (aom_node_ntp_status)	Whether the local time of the host is synchronized with the NTP server time	0 or 1 <ul style="list-style-type: none"> 0: Synchronized 1: Not synchronized 	N/A
Processes (aom_node_process_number)	Number of processes on a measured object	≥ 0	N/A
GPU temperature (aom_node_gpu_temperature_centrigrade)	GPU temperature of a measured object	-	°C
Total physical memory (aom_node_memory_total_megabytes)	Total physical memory that has been applied for a measured object	≥ 0	MB

Metric	Description	Value Range	Unit
Total virtual memory (aom_node_virtual_memory_total_megabytes)	Total virtual memory that has been applied for a measured object	≥ 0	MB
Virtual memory usage (aom_node_virtual_memory_usage)	Percentage of the used virtual memory to the total virtual memory	0-100	%
Threads (aom_node_current_threads_num)	Number of threads created on a host	≥ 0	N/A
Max. threads (aom_node_sys_max_threads_num)	Maximum number of threads that can be created on a host	≥ 0	N/A
Total physical disk space (aom_node_phy_disk_total_capacity_megabytes)	Total disk space of a host	≥ 0	MB
Used disk space (aom_node_physical_disk_total_used_megabytes)	Used disk space of a host	≥ 0	MB
Hosts (aom_billing_hostUsed)	Number of hosts connected per day	≥ 0	N/A

 **NOTE**

- AOM can collect NPU metrics (total storage space, storage usage, used storage space, NPU usage, and temperature) of Ascend Snt9 and D710 hosts only.
- Memory usage = (Physical memory capacity - Available physical memory capacity) / Physical memory capacity; Virtual memory usage = ((Physical memory capacity + Total virtual memory capacity) - (Available physical memory capacity + Available virtual memory capacity)) / (Physical memory capacity + Total virtual memory capacity)
- The virtual memory of a VM is 0 MB by default. If no virtual memory is configured, the memory usage on the monitoring page is the same as the virtual memory usage.
- For the total and used physical disk space, only the space of the local disk partitions' file systems is counted. The file systems (such as JuiceFS, NFS, and SMB) mounted to the host through the network are not taken into account.

Table 1-9 Dimensions of host metrics

Dimension	Description
clusterId	Cluster ID
clusterName	Cluster name
gpuName	GPU name
gpuID	GPU ID
npuName	NPU name
npulD	NPU ID
hostID	Host ID
nameSpace	Cluster namespace
nodeIP	Host IP address
hostName	Host name

1.5.6 Container Metrics and Dimensions

Table 1-10 Container metrics

Metric	Description	Value Range	Unit
Total CPU cores (aom_container_cpu_limit_core)	Total number of CPU cores restricted for a measured object	≥ 1	Cores
Used CPU Cores (aom_container_cpu_used_core)	Number of CPU cores used by a measured object	≥ 0	Cores
CPU Usage (aom_container_cpu_usage)	CPU usage of a measured object. That is, the percentage of the used CPU cores to the total CPU cores restricted for a measured object.	0–100	%
Disk Read Rate (aom_container_disk_read_kilobytes)	Volume of data read from a disk per second	≥ 0	KB/s
Disk Write Rate (aom_container_disk_write_kilobytes)	Volume of data written into a disk per second	≥ 0	KB/s

Metric	Description	Value Range	Unit
Available File System Capacity (aom_container_filesystem_available_capacity_megabytes)	Available file system capacity of a measured object. This metric is available only for containers using the Device Mapper storage drive in the Kubernetes cluster of version 1.11 or later.	≥ 0	MB
Total File System Capacity (aom_container_filesystem_capacity_megabytes)	Total file system capacity of a measured object. This metric is available only for containers using the Device Mapper storage drive in the Kubernetes cluster of version 1.11 or later.	≥ 0	MB
File System Usage (aom_container_filesystem_usage)	File system usage of a measured object. That is, the percentage of the used file system to the total file system. This metric is available only for containers using the Device Mapper storage drive in the Kubernetes cluster of version 1.11 or later.	0–100	%
Total GPU Memory (aom_container_gpu_memory_free_megabytes)	Total GPU memory of a measured object	> 0	MB
GPU Memory Usage (aom_container_gpu_memory_usage)	Percentage of the used GPU memory to the total GPU memory	0–100	%
Used GPU Memory (aom_container_gpu_memory_used_megabytes)	GPU memory used by a measured object	≥ 0	MB
GPU Usage (aom_container_gpu_usage)	GPU usage of a measured object	0–100	%
Total NPU Memory (aom_container_npu_memory_free_megabytes)	Total NPU memory of a measured object	> 0	MB
NPU Memory Usage (aom_container_npu_memory_usage)	Percentage of the used NPU memory to the total NPU memory	0–100	%

Metric	Description	Value Range	Unit
Used NPU Memory (aom_container_npu_memory_used_megabytes)	NPU memory used by a measured object	≥ 0	MB
NPU Usage (aom_container_npu_usage)	NPU usage of a measured object	0–100	%
Total Physical Memory (aom_container_memory_request_megabytes)	Total physical memory restricted for a measured object	≥ 0	MB
Physical Memory Usage (aom_container_memory_usage)	Percentage of the used physical memory to the total physical memory restricted for a measured object	0–100	%
Used Physical Memory (aom_container_memory_used_megabytes)	Used physical memory of a measured object.	≥ 0	MB
Downlink Rate (BPS) (aom_container_network_receive_bytes)	Inbound traffic rate of a measured object	≥ 0	Bytes/s
Downlink Rate (PPS) (aom_container_network_receive_packets)	Number of data packets received by a NIC per second	≥ 0	Packet/s
Downlink Error Rate (aom_container_network_receive_error_packets)	Number of error packets received by a NIC per second	≥ 0	Count/s
Error Packets (aom_container_network_rx_error_packets)	Number of error packets received by a measured object	≥ 0	Count
Uplink Rate (BPS) (aom_container_network_transmit_bytes)	Outbound traffic rate of a measured object	≥ 0	Bytes/s
Uplink Error Rate (aom_container_network_transmit_error_packets)	Number of error packets sent by a NIC per second	≥ 0	Count/s
Uplink Rate (PPS) (aom_container_network_transmit_packets)	Number of data packets sent by a NIC per second	≥ 0	Packet/s

Metric	Description	Value Range	Unit
Status (aom_process_status)	Docker container status	0 or 1 <ul style="list-style-type: none"> • 0: Normal • 1: Abnormal 	None
Working Set Memory Usage (aom_container_memory_workingset_usage)	Usage of the working set memory	0–100	%
Used working set memory (aom_container_memory_workingset_used_megabytes)	Sum of resident set size (RSS) memory and cache	≥ 0	MB

Table 1-11 Dimensions of container metrics

Dimension	Description
appID	Service ID
appName	Service name
clusterId	Cluster ID
clusterName	Cluster name
containerID	Container ID
containerName	Container name
deploymentName	Kubernetes deployment name
kind	Application type
nameSpace	Cluster namespace
podID	Instance ID
podName	Instance name
serviceID	Inventory ID
gpuID	GPU ID
npuName	NPU name

Dimension	Description
npuid	NPU ID

1.5.7 VM Metrics and Dimensions

In AOM, VMs refer to processes, and VM metrics refer to process metrics.

Table 1-12 Process metrics

Metric	Description	Value Range	Unit
Total CPU cores (aom_process_cpu_limit_core)	Total number of CPU cores that have been applied for a measured object	≥ 1	Cores
Used CPU cores (aom_process_cpu_used_core)	Number of CPU cores used by a measured object	≥ 0	Cores
CPU usage (aom_process_cpu_usage)	CPU usage of a measured object. That is, the percentage of the used CPU cores to the total CPU cores.	0-100	%
Handles (aom_process_handle_count)	Number of handles used by a measured object	≥ 0	N/A
Max. handles (aom_process_max_handle_count)	Maximum number of handles used by a measured object	≥ 0	N/A
Total physical memory (aom_process_memory_request_megabytes)	Total physical memory that has been applied for a measured object	≥ 0	MB
Physical memory usage (aom_process_memory_usage)	Percentage of the used physical memory to the total physical memory	0-100	%
Used physical memory (aom_process_memory_used_megabytes)	Used physical memory of a measured object	≥ 0	MB

Metric	Description	Value Range	Unit
Status (aom_process_status)	Process status	0 or 1 <ul style="list-style-type: none"> • 0: Normal • 1: Abnormal 	N/A
Threads (aom_process_thread_count)	Number of threads used by a measured object	≥ 0	N/A
Total virtual memory (aom_process_virtual_memory_total_megabytes)	Total virtual memory that has been applied for a measured object	≥ 0	MB

Table 1-13 Dimensions of process metrics

Dimension	Description
appName	Service name
clusterId	Cluster ID
clusterName	Cluster name
nameSpace	Cluster namespace
processID	Process ID
processName	Process name
serviceID	Inventory ID
aomApplicationName	Application name
aomApplicationID	Application ID
processCmd	Process command ID

1.5.8 Instance Metrics and Dimensions

Instance metrics consist of container or process metrics. The dimensions of instance metrics are the same as those of container or process metrics. For details, see [Container Metrics and Dimensions](#) and [VM Metrics and Dimensions](#).

1.5.9 Service Metrics and Dimensions

Service metrics consist of instance metrics. The dimensions of service metrics are the same as those of instance metrics. For details, see [Instance Metrics and Dimensions](#).

1.6 Restrictions

OS Usage Restrictions

AOM supports multiple operating systems (OSs). When creating a host, ensure that its OS meets the requirements in [Table 1-14](#). Otherwise, the host cannot be monitored by AOM.

Table 1-14 OSs and versions supported by AOM

OS	Version					
SUSE	SUSE Enterprise 11 SP4 64-bit	SUSE Enterprise 12 SP1 64-bit	SUSE Enterprise 12 SP2 64-bit	SUSE Enterprise 12 SP3 64-bit		
openSUSE	13.2 64-bit	42.2 64-bit	15.0 64-bit (Currently, syslog logs cannot be collected.)			
EulerOS	2.2 64-bit	2.3 64-bit	2.5 64-bit	2.9 64-bit	2.10 64-bit	
CentOS	6.3 64-bit	6.5 64-bit	6.8 64-bit	6.9 64-bit	6.10 64-bit	
	7.1 64-bit	7.2 64-bit	7.3 64-bit	7.4 64-bit	7.5 64-bit	7.6 64-bit
Ubuntu	14.04 server 64-bit	16.04 server 64-bit	18.04 server 64-bit			
Fedora	24 64-bit	25 64-bit	29 64-bit			
Debian	7.5.0 32-bit	7.5.0 64-bit	8.2.0 64-bit	8.8.0 64-bit	9.0.0 64-bit	
Kylin	Kylin V10 SP1 64-bit					

 NOTE

- For Linux x86_64 servers, AOM supports all the OSs and versions listed in the preceding table.
- For Linux Arm servers, AOM only supports CentOS 7.4 and later versions, and other OSs and versions listed in the preceding table.

Resource Usage Restrictions

When using AOM, learn about the restrictions in [Table 1-15](#).

Table 1-15 Resource usage restrictions

Category	Object	Restriction
Dashboards	Dashboards	A maximum of 500 dashboards can be created in a region.
	Graphs in a dashboard	A maximum of 30 graphs can be added to a dashboard.
	Resources, threshold rules, components, or hosts in a graph	<ul style="list-style-type: none"> • A maximum of 12 resources across clusters can be added to a line graph. • A maximum of 12 resources can be added to a digit graph. Only one resource can be displayed. By default, the first resource is displayed. • A maximum of 10 threshold rules can be added to a threshold status graph. • A maximum of 10 hosts can be added to a host status graph. • A maximum of 10 components can be added to a component status graph.
Metrics	Metric data	Metric data can be stored in the database for up to 30 days.
	Total metrics	Up to 400,000 for a single account. Up to 100,000 for a small specification.
	Metric items	After resources (such as clusters, components, and hosts) are deleted, their metric items can be stored for up to 30 days.
	Dimensions	A maximum of 30 dimensions can be configured for a metric.
	Metric query API	A maximum of 20 metrics can be queried at a time.
	Statistical period	The maximum statistical period is 1 hour.

Category	Object	Restriction
	Data points returned for a single query	A maximum of 1440 data points can be returned each time.
	Custom metrics	Unlimited.
	Custom metrics reported	A single request cannot exceed 40 KB. The timestamp of a reported metric cannot be 10 minutes later than the standard UTC time. In addition, out-of-order metrics are not received. That is, if a metric is reported at a certain time point, the metrics of earlier time points cannot be reported.
	Application metrics	<ul style="list-style-type: none"> When the number of containers on a host exceeds 1000, the ICAgent stops collecting application metrics and sends the ICAgent Stopped Collecting Application Metrics alarm (ID: 34105). When the number of containers on a host within 1000, the ICAgent resumes the collection of application metrics and the ICAgent Stopped Collecting Application Metrics alarm is cleared.
	Resources consumed by the ICAgent	When the ICAgent collects basic metrics, the resources consumed by the ICAgent are greatly affected by the number of containers and processes. On a VM without any services, the ICAgent consumes 30 MB memory and records 1% CPU usage. To ensure collection reliability, ensure that the number of containers running on a single node must be less than 1000.
Logs	Size of a log	The maximum size of each log is 10 KB. If a log exceeds 10 KB, the ICAgent does not collect it. That is, the log will be discarded.
	Log traffic	A maximum of 10 MB/s is supported for each tenant in a region. If the log traffic exceeds 10 MB/s, logs may be lost.
	Log files	Text and binary log files can be collected.
The ICAgent can collect a maximum of 20 log files from a volume mounting directory.		
		The ICAgent can collect a maximum of 1000 standard container output log files. These files must be in JSON format.

Category	Object	Restriction
	Resources consumed during log file collection	The resources consumed during log file collection are closely related to the log volume, number of files, network bandwidth, and backend service processing capability.
	Log loss	<p>The collector uses multiple mechanisms to ensure log collection reliability and prevent data loss. However, logs may be lost in the following scenarios:</p> <ul style="list-style-type: none"> • The log rotation policy of CCE is not used. • Log files are rotated at a high speed, for example, once per second. • Logs cannot be forwarded due to improper system security settings or syslog itself. • The container running time, for example, shorter than 30s, is extremely short. • A single node generates logs at a speed greater than the allowed transmit bandwidth or log collection speed. Ensure that the log generation speed of a single node is lower than 5 MB/s.
	Log loss	When a single log line exceeds 10,240 bytes, the line will be discarded.
	Log repetition	When the ICAgent is restarted, identical data may be collected around the restart time.
Alarms	Alarms	You can query the alarms generated in the last 31 days.
	Events	You can query the events generated in the last 31 days.
-	Application discovery rules	You can create a maximum of 100 application discovery rules.

Data Capacity Restrictions

Table 1-16 Data capacity restrictions

Restriction Type	Small Scale	Medium Scale	Large Scale	Constraints	Usage Suggestion
Total number of metrics	500 vCPUs, about 100,000 metrics	1000 vCPUs, about 200,000 metrics	2500 vCPUs, about 600,000 metrics	When the total number of metrics exceeds the limit, system metrics can still be reported but customer metrics cannot. Reduce the number of customers to	If the total number of metrics exceeds the limit, expand the AOM scale or contact O&M personnel. AOM supports a maximum of 2500 vCPUs (about 600,000 metrics).
Maximum number of metrics for a single account	Unlimited	Unlimited	Unlimited		None
Total number of alarms	2 million	2 million	6 million		If the total number of alarms exceeds the limit, expand the AOM scale or contact O&M personnel. AOM supports a maximum of 6 million alarms.
Maximum number of alarms for a single account	Unlimited	Unlimited	Unlimited		None

Restriction Type	Small Scale	Medium Scale	Large Scale	Constraints	Usage Suggestion
				metrics.	

1.7 Privacy and Sensitive Information Protection Statement

All O&M data will be displayed on the AOM console. Therefore, do not upload your privacy or sensitive data to AOM. If necessary, encrypt such data.

Collector Deployment

When you manually install the ICAgent on an ECS, your AK/SK will be used as an input parameter in the installation command. To prevent privacy leakage, disable historical record collection before installing the ICAgent. After the ICAgent is installed, it will encrypt and store your AK/SK.

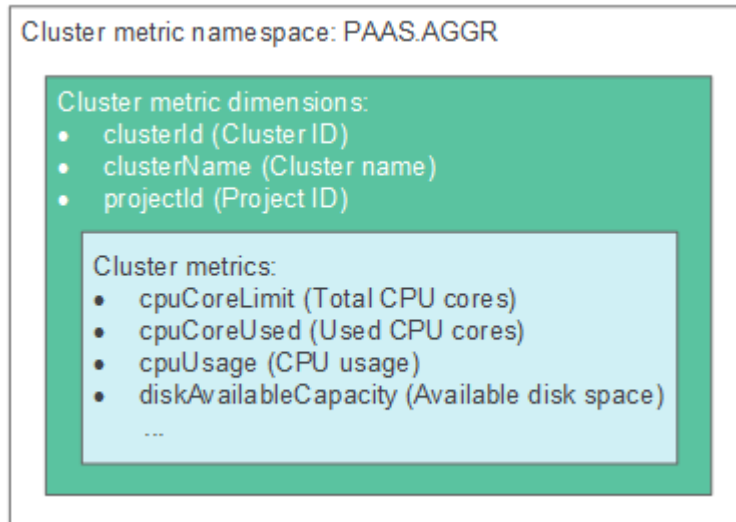
1.8 Glossary

Metrics

Metrics reflect resource performance data or status. A metric consists of a namespace, dimension, name, and unit.

Metric namespaces can be regarded as containers for storing metrics. Metrics in different namespaces are independent of each other so that metrics of different applications will not be aggregated to the same statistics information. Each metric has certain features, and a dimension may be considered as a category of such features. [Figure 1-5](#) describes the relationships among namespaces, dimensions, and cluster metrics.

Figure 1-5 Cluster metrics



Hosts

Each host of AOM corresponds to a VM or physical machine. A host can be your own VM or physical machine, or a VM (for example, an ECS) that you created. A host can only be connected to AOM for monitoring when its OS is supported by AOM and an ICAgent has been installed on the host.

ICAgent

ICAgent is a collector that runs on a host to collect metrics, logs, and application performance data in real time. Before using AOM, ensure that the ICAgent has been installed. Otherwise, AOM cannot be used.

Logs

AOM supports log collection, search, analysis, download, and dump. It also reports alarms based on keyword statistics and enables you to export reports, query SQL statements, and monitor data in real time.

Alarms

Alarms are reported when AOM or an external service (such as) is abnormal or may cause exceptions. Alarms will cause service exceptions and need to be handled.

There are two alarm clearance modes:

- Automatic clearance: After a fault is rectified, AOM automatically clears the corresponding alarm, for example, a threshold alarm.
- Manual clearance: After a fault is rectified, AOM does not automatically clear the corresponding alarm, for example, ICAgent installation failure alarm. In that case, manually clear the alarm.

Events

Events generally carry some important information. They are reported when AOM or an external service (such as) encounters some changes. Such changes do not necessarily cause service exceptions. Events do not need to be handled.

1.9 Permissions

AOM Permissions

[Table 1-17](#) lists all the system-defined permissions for AOM.

Table 1-17 System-defined permissions for AOM

Role/Policy Name	Description	Type	Dependency
AOM FullAccess	Administrator permissions for AOM. Users with these permissions can perform all operations on AOM.	System-defined policy	OBS Administrator, and LTS FullAccess
AOM ReadOnlyAccess	Read-only permissions for AOM. Users with these permissions can only view AOM data.	System-defined policy	

To use a custom fine-grained policy, log in to IAM as the administrator and select fine-grained permissions of AOM as required. For details, see [Table 1-18](#).

Table 1-18 AOM operations that support fine-grained permission control

Service	Operation	Fine-Grained Action	Usage Instruction
AOM (list)	Query metrics.	aom:metric:get	Recommended
	Query or count alarms/events.	aom:alarm:list	Recommended
	Query the event list.	aom:event:list	Recommended
	Query all PE scaling rules.	aom:autoScalingRule:list	Recommended
	Query logs.	aom:log:list	Recommended

Service	Operation	Fine-Grained Action	Usage Instruction
	Query the ICAgent list.	aom:icmgr:list	Recommended
	Query the message template list.	aom:notificationTemplate:list	Recommended
	Query the Prometheus instance list.	aom:prometheus:list	Recommended
AOM (read-only)	Query events.	aom:event:get	Recommended
	Query metrics.	aom:metric:list	Recommended
	Query the alarm rule list.	aom:alarmRule:list	Recommended
	Query an alarm rule.	aom:alarmRule:get	Recommended
	Query a dashboard or dashboard group.	aom:view:get	Recommended
	Query the resource list.	aom:inventory:list	Recommended
	Query or count resources.	aom:inventory:get	Recommended
	Query or count alarms.	aom:alarm:get	Recommended
	Query an access code.	aom:accessCode:get	Recommended
	Query the ICAgent version.	aom:icmgr:get	Recommended
	Query a PE scaling rule.	aom:autoScalingRule:get	Recommended
	Query logs.	aom:log:get	Recommended
	Query the subscription rule list.	aom:subscriberules:list	Recommended
	Query the alarm action rule list.	aom:actionRule:list	Recommended
Query an alarm action rule.	aom:actionRule:get	Recommended	

Service	Operation	Fine-Grained Action	Usage Instruction
	Query or preview a message template.	aom:notificationTemplate:get	Recommended
AOM (write)	Report an event.	aom:event:put	Use as required
	Report metrics.	aom:metric:put	Use as required
	Modify monitoring configuration.	aom:metric:set	Use as required
	Delete monitoring configuration.	aom:metric:delete	Use as required
	Add or modify a dashboard or dashboard group.	aom:view:create	Use as required
	Delete a dashboard or dashboard group.	aom:view:delete	Use as required
	Delete an application discovery rule.	aom:discoveryRule:delete	Use as required
	Add or modify a resource tag or alias.	aom:inventory:set	Use as required
	Report an event or alarm.	aom:alarm:put	Use as required
	Clear an alarm.	aom:alarm:delete	Use as required
	Register an alarm type.	aom:alarm:create	Use as required
	Delete an access code.	aom:accessCode:delete	Use as required
	Create an access code.	aom:accessCode:create	Use as required
	Add or modify an application discovery rule.	aom:discoveryRule:set	Use as required
	Deliver ICAgent configuration.	aom:icmgr:set	Use as required
Uninstall the ICAgent.	aom:icmgr:delete	Use as required	

Service	Operation	Fine-Grained Action	Usage Instruction
	Upgrade the ICAgent version.	aom:icmgr:update	Use as required
	Install the ICAgent.	aom:icmgr:create	Use as required
	Modify a PE scaling rule.	aom:autoScalingRule:update	Use as required
	Delete a PE scaling rule.	aom:autoScalingRule:delete	Use as required
	Stop a PE scaling rule.	aom:autoScalingRule:disable	Use as required
	Start a PE scaling rule.	aom:autoScalingRule:enable	Use as required
	Add or modify an alarm rule.	aom:alarmRule:create	Use as required
	Update an alarm rule.	aom:alarmRule:set	Use as required
	Delete an alarm rule.	aom:alarmRule:delete	Use as required
	Modify a subscription rule.	aom:subscriberules:update	Use as required
	Create a subscription rule.	aom:subscriberules:set	Use as required
	Delete a subscription rule.	aom:subscriberules:delete	Use as required
	Delete an alarm action rule.	aom:actionRule:delete	Use as required
	Update an alarm action rule.	aom:actionRule:update	Use as required
	Add an alarm action rule.	aom:actionRule:create	Use as required
	Delete a message template.	aom:notificationTemplate:delete	Use as required
	Modify a message template.	aom:notificationTemplate:update	Use as required
	Create a message template.	aom:notificationTemplate:create	Use as required

Service	Operation	Fine-Grained Action	Usage Instruction
	Delete a Prometheus instance.	aom:prometheus:delete	Use as required
	Create a Prometheus instance.	aom:prometheus:create	Use as required
	Modify a Prometheus instance.	aom:prometheus:update	Use as required

2 Getting Started

2.1 Process of Using AOM

AOM is a one-stop, multi-dimensional O&M management platform for cloud applications. It monitors applications and related cloud resources in real time, analyzes application health status, and provides flexible alarm reporting and data visualization functions. It helps you detect faults in a timely manner and monitor running status of applications, services, and other resources in real time. This section describes how to get started with AOM. The following figure shows the process.

Figure 2-1 Process of using AOM



1. **Creating a cloud host**
Each host corresponds to a VM on the cloud, for example, an Elastic Cloud Server (ECS). A host can be directly created on the ECS console.
2. **Installing an ICAgent**
An ICAgent is a data collector of AOM. It collects metrics, logs, and application performance data in real time. For the hosts created on the ECS console, manually install ICAgents.
3. **Configuring an alarm rule**
You can set threshold conditions for metrics by using alarm rules. If metric values meet threshold conditions, AOM generates threshold alarms. If no metric data is reported, AOM will report insufficient data events. In this way, you can identify and handle exceptions at the earliest time.
4. **Viewing alarms**
AOM provides the dashboard and alarm list for you to perform routine O&M.

2.2 Installing an ICAgent

This section describes how to install an ICAgent on an ECS.

Prerequisites

- An ECS has been created.
- An EIP has been bound to the ECS.
- The browser time is the same as the ECS time.

Procedure

Step 1 Obtain and use the AK/SK of a public account. Do not use the AK/SK of a personal account.

NOTICE

Ensure that the public account and AK/SK will not be deleted or disabled. If the AK/SK is deleted, the ICAgent cannot report data to AOM or LTS.

- If you have obtained the AK/SK, skip this step.
- If you do not have an AK/SK, [obtain them](#) first.

Step 2 On the menu bar, choose **Collection Management**. The **Agent Management** page is displayed.

Step 3 Select **Other: custom hosts** from the drop-down list on the right of the page and click **Install ICAgent**.

Step 4 Click **Copy Command**.

Step 5 Use a remote login tool, such as PuTTY, to log in as the **root** user to the server where the ICAgent is to be installed, run the command copied in [Step 4](#), and enter the AK/SK obtained in [Step 1](#) as prompted to install the ICAgent.

NOTE

- If the message **ICAgent install success** is displayed, the ICAgent is successfully installed in the `/opt/oss/servicemgr/` directory. After the ICAgent is successfully installed, choose **Other: custom hosts** on the **Agent Management** page to view the ICAgent status of the ECS.
- If the ICAgent fails to be installed, uninstall it according to [Uninstalling the ICAgent Through Logging In to the Server](#) and then install it again. If the problem persists, contact technical support.

----End

2.3 Creating Alarm Rules and Viewing Alarms

You can set threshold conditions for resource metrics by setting alarm rules. When the value of a metric reaches the threshold, an alarm is generated. If no metric

data is reported, an insufficient data event is generated so that you can detect and handle exceptions in a timely manner.

There are three modes for creating metric alarm rules: **Select by resource type**, **Select from all metrics**, and **Run Prometheus command**. The following uses **Select by resource type** as an example to describe how to add an alarm rule and view alarms.

Creating a Metric Alarm Rule

- Step 1** On the menu bar, choose **Monitoring Center**.
- Step 2** In the navigation pane, choose **Alarm Management > Alarm Rules**.
- Step 3** On the rule list page, click **Create Alarm Rule**.
- Step 4** Set basic information about the alarm rule by referring to [Table 2-1](#).

Table 2-1 Basic information

Parameter	Description
Rule Name	Name of a rule. Enter a maximum of 255 characters. The following special characters are not allowed: "\$# %&'<=>?\\"
Description	Description of the rule. Enter up to 1000 characters.

- Step 5** Set the detailed information about the alarm rule.
 1. Set **Rule Type** to **Metric alarm rule**.
 2. Set **Configuration Mode** to **Select by resource type** and specify **Resource Type** and **Monitored Object**.
 - **Resource Type**: Select a desired resource type from the drop-down list.
 - **Monitored Object**: Click **Select Monitored Object** to select a desired monitored object.

If you enable **Apply to All** when selecting monitored objects, an alarm rule will be created for all metrics of the type you select under an application or service.
 3. Set an alarm condition. Customize alarm conditions or create them by importing a template. The following describes how to customize an alarm condition.
 - **Custom**

Click **Custom** and set the statistical period, consecutive periods, and alarm condition. [Table 2-2](#) describes the parameters.

Table 2-2 Parameters for setting an alarm condition

Category	Parameter	Description
Alarm Condition	Metric	Metric to be monitored.
	Consecutive Periods	When the metric value meets the alarm condition for a specified number of consecutive periods, a metric alarm will be generated.
	Statistical Period	Metric data is aggregated based on the configured statistical period, which can be 1 minute, 5 minutes, 15 minutes, or 1 hour.
	Statistic	Method used to measure metrics. Options: Avg, Min, Max, Sum, and Samples.
	Alarm Condition	Trigger condition of a metric alarm. An alarm condition consists of two parts: operators (\geq , \leq , $>$, and $<$) and threshold value. For example, if the trigger condition is set to > 85 and an actual metric value exceeds 85, a metric alarm will be generated.
	Alarm Severity	Severity of a metric alarm. Options: Critical, Major, Minor, and Warning.
-	Check Interval	Interval at which metric query and analysis results are checked. <ul style="list-style-type: none"> ▪ Hourly: Query and analysis results are checked every hour. ▪ Daily: Query and analysis results are checked at a fixed time every day. ▪ Weekly: Query and analysis results are checked at a fixed time point on a specified day of a week. ▪ Custom interval: The query and analysis results are checked at a fixed interval. ▪ Cron: A cron expression is used to specify a time interval. Query and analysis results are checked at the specified interval. The time specified in the cron expression can be accurate to the minute and must be in the 24-hour notation. Example: 0/5 * * * *, which indicates that the check starts from 0th minute and is performed every 5 minutes.

Category	Parameter	Description
Advanced Settings	Alarm Clearance	An alarm will be cleared if the monitored object does not meet the trigger condition within the monitoring period. By default, metrics in only one period are monitored. You can set up to five monitoring periods.
	Action Taken for Insufficient Data	Action to be taken when no metric data is generated or metric data is insufficient within the monitoring period. You can set this option based on your requirements. By default, metrics in only one period are monitored. You can set up to five monitoring periods. The system supports the following actions: changing the status to exceeded and sending an alarm, changing the status to insufficient data and sending an event, maintaining the previous status, and changing the status to normal and sending an alarm clearance notification.

Step 6 Set an alarm notification policy. **Direct alarm reporting:** An alarm is directly sent when the alarm condition is met.

1. Specify whether to enable an alarm action rule. After an alarm action rule is enabled, the system sends notifications based on the associated SMN topic and message template. If the existing alarm action rules cannot meet your requirements, click **Create Rule** to create one. For details, see [Creating an Alarm Action Rule](#).
2. After an alarm action rule is selected, specify whether to enable alarm clearance notification. After alarm clearance notification is enabled, if the alarm clearance condition set in [Advanced Settings > Alarm Clearance](#) is met, alarm clearance notifications are sent based on the selected action rule.

Step 7 Click **Create Now**. Then, click **Back to Alarm Rule List** to view the created alarm rule.



In the expanded list, if a metric value meets the configured alarm condition, a metric alarm is generated on the alarm page. To view it, choose **Alarm Management > Alarm List** in the navigation pane.

----End

Viewing Alarms



Step 1 In the navigation pane, choose **Alarm Management > Alarm List**.

Step 2 Click the **Alarms** tab to view the alarm information.

1. Set a time range to view alarms. There are two methods to set a time range:
 Method 1: Use a predefined time label, such as **Last hour** or **Last 6 hours**. You can select a time range as required.
 Method 2: Specify the start time and end time (max. 31 days).
2. Set the interval for refreshing alarms. Click  and select a value from the drop-down list, such as **Refresh manually** or **1 minute auto refresh**.
3. Set filter criteria and click  to view the alarms generated in the period.

Step 3 Perform the operations listed in [Table 2-3](#) as required.

Table 2-3 Operations

Operation	Description
Viewing alarm statistics	Click  , and view alarm statistics that meet filter criteria within a specific time range on a bar graph.
Clearing alarms	<ul style="list-style-type: none"> • To clear an alarm, click  in the Operation column of the target alarm. • To clear one or more alarms, select them and click Clear in the displayed dialog box. <p>NOTE You can clear an alarm after the corresponding problem is resolved.</p>
Viewing alarm details	Click an alarm name to view the alarm details and handling suggestions.
Viewing cleared alarms	Click Active Alarms in the upper right corner and select Historical Alarms from the drop-down list to view alarms that have been cleared.

----End

3 User Guide

3.1 Monitoring Overview

The **O&M** page provides a full-link, multi-layer, and one-stop O&M page for resources, applications, and user experience. It displays the following cards: infrastructure monitoring, application monitoring, alarm statistics, component monitoring (CPU and memory), host monitoring (disk), host monitoring (CPU and memory), container instance monitoring (CPU and memory), and host monitoring (network).

Infrastructure Monitoring

This card mainly displays infrastructure metrics. You can select one cluster to view its information. When you select a cluster, the following information is displayed:

- Host running status, CPU usage, and physical memory usage.
- Trend graph of network traffic in the last 30 minutes. The values of each point in the graph respectively indicate the total downlink/uplink rates of selected clusters in one minute. The values displayed above the trend graph respectively indicate the total downlink/uplink rates of the cluster at the latest time point.
- Trend graph of CPU and memory usage in the last 30 minutes. The values of each point in the graph respectively indicate the average CPU and memory usage of the cluster in one minute. The values displayed above the trend graph respectively indicate the average CPU and memory usage of the cluster at the latest time point.

Application Monitoring

This card mainly displays application metrics:

1. Running status of applications and components.
2. The following information is displayed when you select an application:
 - Trend graph of network traffic in the last 30 minutes. The values of each point in the graph respectively indicate the receive rate (BPS) and send

- rate (BPS) of the selected application in one minute. The values above the graph respectively indicate the receive rate (BPS) and send rate (BPS) of the selected application at the latest time point.
- Trend graph of CPU and memory usage in the last 30 minutes. The values of each point in the graph respectively indicate the CPU and memory usage of the selected application in one minute. The values above the graph respectively indicate the CPU and memory usage of the selected application at the latest time point.

Alarm Statistics

This card mainly displays alarms, alarm rules, and trends of alarms and hosts.

Component Monitoring (CPU and Memory)

This card mainly displays:

- The top 5 components with high CPU and memory usage in the last minute.
- Trend graph of the CPU and memory usage of the selected component in the last hour. The values of each point in the graph respectively indicate the average CPU and memory usage of the component in one minute.
- CPU and memory usage of the selected component at the latest time point, which is displayed above the trend graph.
- Option **Hide system components**, which can be selected to hide system components.

Host Monitoring (Disk)

This card mainly displays:

- The top 5 hosts with high disk read/write rate in the last minute.
- Trend graph of the disk read/write rate of the selected host in the last hour. The values of each point in the graph respectively indicate the average disk read/write rate of the selected host in one minute.
- Disk read/write rate of the selected host at the latest time point, which is displayed above the trend graph.

Host Monitoring (CPU and Memory)

This card mainly displays:

- The top 5 hosts with high CPU and memory usage in the last minute.
- Trend graph of the CPU and memory usage of the selected host in the last hour. The values of each point in the graph respectively indicate the average CPU and memory usage of the host in one minute.
- CPU and memory usage of the selected host at the latest time point, which is displayed above the trend graph.

Container Instance Monitoring (CPU and Memory)

This card mainly displays:

- The top 5 container instances with high CPU and memory usage in the last minute.
- Trend graph of the CPU and memory usage of the selected container instance in the last hour. The values of each point in the graph respectively indicate the average CPU and memory usage of the container instance in one minute.
- CPU and memory usage of the selected container instance at the latest time point, which is displayed above the trend graph.
- **Hide system instances** option, which can be selected to hide system instances.

Host Monitoring (Network)



This card mainly displays:

- The top 5 hosts with high uplink/downlink network rate in the last minute.
- Trend graph of the uplink/downlink network rate of the selected host in the last hour. The values of each point in the graph respectively indicate the average uplink/downlink network rate of the selected host in one minute.
- Uplink/downlink network rate of the selected host at the latest time point, which is displayed above the trend graph.

More Operations

You can also perform the operations listed in [Table 3-1](#).

Table 3-1 Related operations

Operation	Description
Adding a card to favorites	To hide a card, click  in the upper right corner of the card and choose Add to Favorites . After a card is added to favorites, it is hidden from the O&M page. To view the card later, obtain it from favorites.
Enlarging a graph	Click  in the upper right corner of the metric graph.
Drilling down blue texts	Click the blue texts, such as Host , Application , or Component to drill down to the details page.

3.2 Dashboard

3.2.1 Creating a Dashboard

With a dashboard, different graphs (such as line graphs and digit graphs) are displayed on the same screen, so you can view metric data comprehensively.

You can add key resource metrics to a dashboard and monitor them in real time. You can also compare the same metric of different resources on one screen. In

In addition, by adding common O&M metrics to a dashboard, you do not need to reselect them when re-opening the monitoring center during routine O&M.

Precautions

- Preset dashboard templates are saved in the built-in group, including the cloud service and application templates. Preset dashboards cannot be deleted. Their groups cannot be changed. Dashboard templates cannot be created.
- Up to 50 dashboard groups can be created in a region.
- Up to 500 dashboards can be created in a region.
- A maximum of 30 graphs can be added to a dashboard.
- A maximum of 12 resources can be added to a digit graph. Only one resource can be displayed. By default, the first resource is displayed.
- A maximum of 10 threshold rules can be added to a threshold status graph.
- A maximum of 10 hosts can be added to a host status graph.
- A maximum of 10 components can be added to a component status graph.

Creating a Dashboard

Step 1 On the menu bar, choose **Monitoring Center**.

Step 2 In the navigation pane, choose **Dashboard**.

Step 3 Click  next to **Dashboard** to create a dashboard group.

Step 4 Click **Add Dashboard** in the upper left corner of the list.

Step 5 In the displayed dialog box, set parameters.

Table 3-2 Parameters for creating a dashboard

Parameter	Description
Dashboard Name	Name of a dashboard. Enter a maximum of 255 characters. The following special characters are not allowed: "\$# %&' +; <=>?\\"
Group Type	Options: Existing and New . <ul style="list-style-type: none"> • Existing: Select an existing dashboard group from the drop-down list. • New: Enter a dashboard group name to create one.

Step 6 Click **OK**.

----End

Adding a Graph to a Dashboard


- Step 1** In the navigation pane, choose **Dashboard**.
- Step 2** In the dashboard list, locate the target dashboard.
- Step 3** Go to the dashboard page, and select the Prometheus instance for which you want to add a graph from the drop-down list.
- Step 4** Go to the dashboard page. Click **Add Graph** or  in the upper right corner to add a graph to the dashboard. For details about the graphs that can be added to the dashboard, see [Graph Description](#). The data can be metric or system data. Select a graph as required.

Table 3-3 Parameters for adding a graph

Data Source	Adding Mode	Scenario
Metric Sources	See Add a metric graph .	Monitors infrastructure metrics.
System Graphs	See Add a system graph .	Monitors service alarms, or threshold, host, or component status.

- Add a metric graph. Set parameters by referring to [Table 3-4](#). Then, click **Add to Dashboard**.

Table 3-4 Adding a metric graph


Parameter	Description
Graph Title	Title of a graph to distinguish it from other graphs. Enter a maximum of 255 characters. The following special characters are not allowed: "\$# %&'<=>?\\"
Data Source	Click Metric Sources and select metric data as the source.
Graph Type	Options: line, digit, top N, table, bar, and digital line.

Parameter	Description
Metric List	<p>Add metrics as required. There are four modes to add metrics:</p> <ul style="list-style-type: none"> - Metric type: - All metrics: Select desired metrics from all metrics. When this mode is selected, enter keywords to search for metrics. - Resource type: Select your target resource from the resource tree and select a metric. In this mode, you can select the same metric of multiple resources at the same time. - Prometheus statement: Enter a Prometheus command and select your target metric. For details, see Prometheus Statements. <p>Click Add Metric to add up to 12 metric data records.</p> <p>NOTE</p> <ul style="list-style-type: none"> - When All metrics is selected, enter keywords to search for metrics. - Scope: Metric monitoring scope. The scope is in the key-value pair format. Directly select an option from the drop-down list or use AND, OR, and NOT to specify scopes for metrics. - Group Condition: Aggregate metric data by the specified field and calculate the aggregation result. Options: Not grouped, avg by, max by, min by, and sum by. For example, avg by clusterName indicates that metrics are grouped by cluster name, and the average value of the grouped metrics is calculated and displayed in the graph.
Graph Settings	Configure the graph settings by referring to Metric Data Graphs (Line/Digit/Top N/Table/Bar/Digital Line Graphs) .
Statistic	Method used to measure metrics. Options: Avg , Min , Max , Sum , and Samples .
Statistical Period	Interval at which metric data is collected. The available statistical period options vary according to the time range you select. For details, see What Is the Relationship Between the Time Range and Statistical Period? .
Time Range	Time range in which metric data is collected. Options: Last 30 minutes , Last hour , Last 6 hours , Last day , Last week , and Custom .
Refresh Frequency	Interval at which the metric data is refreshed. Options: Refresh manually , 30 seconds auto refresh , 1 minute auto refresh , and 5 minutes auto refresh .

- Add a system graph. Set parameters by referring to [Table 3-5](#). Then, click **Add to Dashboard**.

Table 3-5 Adding a system graph

Parameter	Description
Graph Title	Title of a graph, which is used to distinguish it from other graphs. Enter a maximum of 255 characters. The following special characters are not allowed: "\$# %&'<=>?\\"
Data Source	Click the System Graphs tab and then select Alarm Statistics , Threshold Status , Host Status , or Component Status as the data source.
Graph Settings	<ul style="list-style-type: none"> - Alarm Statistics: Set the graph by referring to Alarm Statistics Graphs (Ring). - Threshold Status: Select up to 10 threshold rules from the threshold rule list. The selected threshold data will be displayed in a table. NOTE Ensure that metric alarm rules have been created. Otherwise, threshold status graphs cannot be added. - If you select Host Status, select target hosts from the application tree. Up to 10 host monitoring data records can be added. - If you select Component Status, select target components from the application tree. Up to 10 component data records can be added.



Step 5 Click . The graph is successfully added to the dashboard.















----End










More Operations

After a dashboard is created, you can also perform the operations listed in [Table 3-6](#).

Table 3-6 Related operations

Operation	Description
Setting column display	Click  in the upper right corner of the dashboard list and select or deselect the columns to display.
Adding dashboards to favorites	Locate a dashboard and click  in the Operation column.

Operation	Description
Migrating dashboards to another group	<ul style="list-style-type: none"> Migrating a dashboard: Select a dashboard and click  in the Operation column. Migrating dashboards in batches: Select dashboards. In the displayed dialog box, click Migrate Group.
Deleting a dashboard	<ul style="list-style-type: none"> Deleting a dashboard: Select a dashboard and click  in the Operation column. Deleting dashboards in batches: Select dashboards. In the displayed dialog box, click Delete.
Changing a dashboard group name	<ol style="list-style-type: none"> In the dashboard list, click a dashboard name. Go to the dashboard page and click a dashboard name in the upper left corner. Move the cursor to the target dashboard group, click , and choose Modify to change the group name.
Deleting a dashboard group	<ol style="list-style-type: none"> In the dashboard list, click a dashboard name. Go to the dashboard page and click a dashboard name in the upper left corner. Move the cursor to the target dashboard group, click , and choose Delete. In the displayed dialog box, click OK.
Removing a graph from a dashboard	<ol style="list-style-type: none"> Select the target dashboard, click  in the upper right corner of the Dashboard page, move the cursor to the upper right corner of a graph, click , and select Remove from the drop-down list. Click  to delete the graph.
Relocating a graph on a dashboard	<ol style="list-style-type: none"> Select the target dashboard, click  in the upper right corner of the Dashboard page, move the cursor to the target graph, and move it to any position in the dashboard. Click  to adjust the current graph layout.
Full-screen display	Select the target dashboard and click  in the upper right corner of the Dashboard page to view the dashboard in full screen.
Exiting the full-screen mode	Move the cursor to the upper part of the screen and click  or  , or press Esc on the keyboard.
Manual refresh	Select the target dashboard and click  in the upper right corner of the Dashboard page and manually refresh the current page.
Auto refresh	Select the target dashboard and click the arrow next to  in the upper right corner of the Dashboard page and enable auto refresh.

Operation	Description
Manually refreshing a single graph	Select the target dashboard, move the cursor to the upper right corner of a graph, click  , and select Refresh from the drop-down list to manually refresh the current graph.
Modifying a graph	<ol style="list-style-type: none"> 1. Select the target dashboard, move the cursor to the upper right corner of a graph, click , and choose Modify to modify the graph. For details, see Adding a Graph to a Dashboard. 2. Modify parameters and click OK. 3. Click  in the upper right corner of the Dashboard page to save the modification.
Displaying a Graph in Full Screen	Select the target dashboard, move the cursor to the upper right corner of a graph, click  , and select Full Screen from the drop-down list.
Exiting the full-screen mode	Move the cursor to the upper part of the screen and click  , or click  and select Exit Full Screen from the drop-down list, or press Esc on the keyboard to exit the full-screen mode.
Rotating dashboards	Click a target dashboard and click  in the upper right corner of the Dashboard page. For details, see Setting the Full-Screen Online Duration .
Setting the query time	Select the target dashboard. In the upper right corner of the Dashboard page, click the drop-down list next to  and select Last 30 minutes , Last hour , Last 6 hours , Last day , Last week , or Custom from the drop-down list. If you select Custom , select the start time in the calendar that is displayed. The time can be accurate to seconds. Then click OK , so that you can query data in the dashboard based on the selected time range.
Exporting a monitoring report	Click a dashboard to go to its details page. Then click  in the upper right corner to export a CSV file to your local PC.

3.2.2 Setting the Full-Screen Online Duration

AOM provides an automatic logout mechanism to secure customer information. Specifically, after you access a page on the console but do not perform any operations within 1 hour, the console automatically logs you out.

When an AOM dashboard is used for monitoring in full-screen mode, the full-screen mode will exit when your account logs out. As a result, real-time monitoring cannot be performed. To prevent this, AOM allows you to customize full-screen online duration.

Precautions

- For security purposes, exit the full-screen view when it is not required.
- The full-screen online duration is irrelevant to operations. If the preset duration times out, the login page is automatically displayed.
- The full-screen online duration is subject to your latest setting.
For example, if full-screen monitoring is implemented on multiple screens, the online duration is subject to the latest setting.
- The full-screen online duration takes precedence over the automatic logout mechanism of the cloud.
For example, if you log in to the console, set the full-screen online duration to 2 hours on AOM pages, and then open other pages, your setting on the AOM pages also takes effect on other pages. That is, the login page will be automatically displayed 2 hours later.
- If you leave all full-screen views, the default automatic logout mechanism is used.
For example, if you log in to the console, set the full-screen online duration to 2 hours on AOM pages, open other pages, and then leave all full-screen views of AOM, the default logout mechanism will be used. That is, if you do not perform any operations within 1 hour, the login page will be automatically displayed.

Procedure


- Step 1** On the menu bar, choose **Monitoring Center**.
- Step 2** In the navigation pane, choose **Dashboard**.
- Step 3** Click a target dashboard and click  in the upper right corner of the **Dashboard** page.
- Step 4** In the dialogue box that is displayed, set the full-screen online duration. For details, see [Table 3-7](#).

Table 3-7 Online duration parameters

Parameter	Description
Online Setting	<p>Mode of setting the online duration. Options:</p> <ul style="list-style-type: none"> • Custom: After the specified duration expires, the login page will be automatically displayed. • Always online: The full-screen online duration is not restricted. That is, you can always implement full-screen monitoring and the login page will never be displayed.

Parameter	Description
Duration	Full-screen online duration. The duration varies according to the setting mode. <ul style="list-style-type: none"> • Custom: The default duration is 1 hour. Range: 1 to 24 hours. For example, if you enter 2 in the text box, the login page will be automatically displayed 2 hours later. • Always online: The default value is Always online and cannot be changed.
Dashboard Rotation	Specifies whether to enable dashboard rotation. If this function is enabled, you need to set Rotation Period and Dashboard .
Rotation Period	Period for rotating dashboards. Range: 10s to 120s. Default: 10s.
Dashboard	Dashboard to be rotated. Select one or more dashboards from the drop-down list.

Step 5 Click **OK** to enter the full-screen mode.

----End

3.2.3 Graph Description

The dashboard displays the query and analysis results of metric or system data in graphs (such as line/digit/status graphs).

Metric Data Graphs (Line/Digit/Top N/Table/Bar/Digital Line Graphs)

- **Line graph:** used to analyze the data change trend in a certain period. Use this type of graph when you need to monitor the metric data trend of one or more resources within a period.

You can use a line graph to compare the same metric of different resources.

Table 3-8 Line graph parameters

Category	Parameter	Description
-	X Axis Title	Title of the X axis.
	Y Axis Title	Title of the Y axis.
	Fit as Curve	Whether to fit a smooth curve.
	Hide X Axis Label	Whether to hide the X axis label.
	Hide Y Axis Label	Whether to hide the Y axis label.
	Y Axis Range	Value range of the Y axis.

Category	Parameter	Description
Advanced Settings	Left Margin	Distance between the axis and the left boundary of the graph.
	Right Margin	Distance between the axis and the right boundary of the graph.
	Top Margin	Distance between the axis and the upper boundary of the graph.
	Bottom Margin	Distance between the axis and the lower boundary of the graph.

- **Digit Graph:** used to highlight a single value. Use this type of graph to monitor the latest value of a metric in real time.

Table 3-9 Digit graph parameters

Parameter	Description
Show Miniature	After this function is enabled, the icon will be zoomed out based on a certain proportion. Also, a line graph is added.
Dimension	Select the desired metric from the drop-down list.

- **Top N:** The statistical unit is a cluster and statistical objects are resources such as hosts, components, or instances in the cluster. The top N graph displays top N resources in a cluster. By default, top 5 resources are displayed.

To view the top N resources, add a top N graph to the dashboard. You only need to select resources and metrics, for example, host CPU usage. AOM then automatically singles out top N hosts for display. If the number of resources is less than N, actual resources are displayed.

Table 3-10 Top N graph parameters

Category	Parameter	Description
-	Sorting Order	Sorting order of data. Default: Descending .
	Upper Limit	The maximum number of resources to be displayed in the top N graph. Default: 5 .
	Dimension	Metric dimensions to be displayed in the top N graph.
	Column Width	Column width. Options: auto (default), 16 , 22 , 32 , 48 , and 60 .
	Unit	Unit of the data to be displayed. Default: % .

Category	Parameter	Description
	Display X-Axis Scale	After this function is enabled, the scale of the X axis is displayed.
	Show Value	After this function is enabled, the value on the Y axis is displayed.
	Display Y-Axis Line	After this function is enabled, the line on the Y axis is displayed.
Advanced Settings	Left Margin	Distance between the axis and the left boundary of the graph.
	Right Margin	Distance between the axis and the right boundary of the graph.
	Top Margin	Distance between the axis and the upper boundary of the graph.
	Bottom Margin	Distance between the axis and the lower boundary of the graph.

- **Table:** A table lists content in a systematic, concise, centralized, and comparative manner, and intuitively shows the relationship between different categories or makes comparison, ensuring accurate display of data.

Table 3-11 Table parameters

Parameter	Description
Field Name	Name of a field.
Field Rename	Rename a table header field when necessary.

- **Bar graph:** A vertical or horizontal bar graph compares values between categories. It shows the data of different categories and counts the number of elements in each category. You can also draw multiple rectangles for the same type of attributes. Grouping and cascading modes are available so that you can analyze data from different dimensions.

Table 3-12 Bar graph parameters

Category	Parameter	Description
-	X Axis Title	Title of the X axis.
	Y Axis Title	Title of the Y axis.
	Y Axis Range	Value range of the Y axis.
	Hide X Axis Label	Whether to hide the X axis label.

Category	Parameter	Description
	Hide Y Axis Label	Whether to hide the Y axis label.
Advanced Settings	Top Margin	Distance between the axis and the upper boundary of the graph.
	Right Margin	Distance between the axis and the right boundary of the graph.
	Left Margin	Distance between the axis and the left boundary of the graph.
	Bottom Margin	Distance between the axis and the lower boundary of the graph.

- Digital line graph:** used to analyze the data change trend in a certain period and intuitively display related data. Use this type of graph when you need to monitor the metric data trend of one or more resources within a period.

Table 3-13 Parameters for setting a digital line graph

Parameter	Description
Fit as Curve	Whether to fit a smooth curve.
Show Legend	Whether to display legends.
Hide X Axis Label	Whether to hide the X axis label.
Hide Y-Axis Background Line	Whether to hide the Y axis background line.
Show Data Marker	Whether to display the connection points.
Dimension	Select the desired metric from the drop-down list.

Alarm Statistics Graphs (Ring)

The number and proportion of alarms of each severity are displayed in a ring.

Table 3-14 Ring graph parameters

Parameter	Description
Display Latest Alarms	If this function is enabled, the latest alarm will be displayed. This function is enabled by default.
Alarms to Display	Set the number of alarms to be displayed on a dashboard. Options: 4 , 10 , and 20 .

Health Status Graphs (Tables)

You can monitor the statuses of one or more threshold rules, hosts, or components in one health status graph. The graph can be a table.

- **Threshold status graph:** shows the status of threshold rules in real time. Threshold statuses can be displayed in a table. You can add up to 10 threshold data records.

NOTE

Before adding a threshold status graph, [create a metric alarm rule](#).

- **Host status graph:** shows the host status in real time. Host statuses can be displayed in a table. You can add up to 10 host data records.
- **Component status graph:** monitors the component status in real time. Component statuses can be displayed in a table. You can add up to 10 component data records.

3.3 Alarm Management

3.3.1 Alarm Rules

3.3.1.1 Introduction

The monitoring center is where you can set alarm rules. By setting alarm rules, you can define event conditions for services or threshold conditions for resource metrics. An event alarm is generated when the resource data meets the event condition. If a metric value meets a threshold condition, a threshold alarm will be reported. If there is no metric data, an insufficient data event will be reported.

Alarm rules are classified into metric alarm rules and event alarm rules. Generally, metric alarm rules monitor the usage of resources such as hosts and components in real time. When there are too many resource usage alarms and alarm notifications are sent too frequently, you can use event alarm rules to simplify alarm notifications, quickly identify a type of resource usage problems of a service, and resolve the problems in a timely manner.

The total number of metric alarm rules and event alarm rules is 1000. If the number of alarm rules has reached the upper limit, delete unnecessary rules and create new ones.

3.3.1.2 Creating a Metric Alarm Rule

You can set threshold conditions in metric alarm rules for resource metrics. If a metric value meets a threshold condition, a threshold alarm will be reported. If there is no metric data, an insufficient data event will be reported.

Functions

- You can set the consecutive periods, statistical period, and threshold condition. For details, see [Step 5.3](#).

- You can set whether to send a notification when an alarm is cleared. For details, see [Step 5.3](#).

Creation Mode

Metric alarm rules can be created in three modes: [Select by resource type](#), [Select from all metrics](#), and [Run Prometheus statement](#).

When creating metric alarm rules by resource type, you can set an alarm condition using two methods: [Custom](#) and [Template](#). If you select the second method, first create an alarm template by referring to [Creating an Alarm Template](#).

Precautions

If you need AOM to send email or SMS notifications when the metric alarm rule status (**Exceeded**, **Normal**, **Insufficient**, or **Disabled**) changes, set an alarm action rule according to [Creating an Alarm Action Rule](#).

Creating Metric Alarm Rules by Resource Type

- Step 1** On the menu bar, choose **Monitoring Center**.
- Step 2** In the navigation pane, choose **Alarm Management > Alarm Rules**.
- Step 3** On the **Alarm Rules** tab page, click **Create Alarm Rule**.
- Step 4** Set basic information about the alarm rule by referring to [Table 3-15](#).

Table 3-15 Basic information

Parameter	Description
Rule Name	Name of a rule. Enter a maximum of 255 characters. The following special characters are not allowed: "\$# %&'<=>?\\"
Description	Description of the rule. Enter up to 1000 characters.

- Step 5** Set the detailed information about the alarm rule.
 1. Set **Rule Type** to **Metric alarm rule**.
 2. Set **Configuration Mode** to **Select by resource type** and specify **Resource Type** and **Monitored Object**. [Table 3-16](#) describes the parameters.

Table 3-16 Parameter description

Parameter	Description
Resource Type	<p>Select a desired resource type from the drop-down list.</p> <ul style="list-style-type: none"> - When you click the Application Metrics tab, you can select resources based on the following dimensions: <ul style="list-style-type: none"> ▪ Host: Select resources by host, including host, host disk, host network, host file system, and host GPU. ▪ Application: Select resources by application. ▪ Component: Select resources by component. ▪ Process: Select resources by process. - When you click the Cloud Service Metrics tab, you can select resources by cloud service.
Monitored Object	<p>Click Select Monitored Object. All existing resources of the type you select will be displayed. Select target resources as required.</p> <p>If you enable Apply to All when selecting monitored objects, an alarm rule will be created for all resources of the type you select under an application or service. When this type of resources are added or modified, they will be automatically bound to the created alarm rule. When they are deleted, they will be automatically unbound from the alarm rule.</p>

3. Set an alarm condition. Customize an alarm condition or import an alarm condition from a template.
 - **Custom**
Click **Custom** and set the statistical period, consecutive periods, and alarm condition. [Table 3-17](#) describes the parameters.

Table 3-17 Alarm condition parameters

Category	Parameter	Description
Alarm Condition	Metric	Metric to be monitored.
	Consecutive Periods	When the metric value meets the alarm condition for a specified number of consecutive periods, a metric alarm will be generated.
	Statistical Period	Metric data is aggregated based on the configured statistical period, which can be 1 minute, 5 minutes, 15 minutes, or 1 hour.

Category	Parameter	Description
	Statistic	Method used to measure metrics. Options: Avg, Min, Max, Sum, and Samples.
	Alarm Condition	Trigger condition of a metric alarm. An alarm condition consists of two parts: operators (\geq , \leq , $>$, and $<$) and threshold value. For example, if the trigger condition is set to > 85 and an actual metric value exceeds 85, a metric alarm will be generated.
	Alarm Severity	Severity of a metric alarm. Options: Critical, Major, Minor, and Warning.
-	Check Interval	Interval at which metric query and analysis results are checked. <ul style="list-style-type: none"> ▪ Hourly: Query and analysis results are checked every hour. ▪ Daily: Query and analysis results are checked at a fixed time every day. ▪ Weekly: Query and analysis results are checked at a fixed time point on a specified day of a week. ▪ Custom interval: The query and analysis results are checked at a fixed interval. ▪ Cron: A cron expression is used to specify a time interval. Query and analysis results are checked at the specified interval. The time specified in the cron expression can be accurate to the minute and must be in the 24-hour notation. Example: 0/5 * * * *, which indicates that the check starts from 0th minute and is performed every 5 minutes.
Advanced Settings	Alarm Clearance	An alarm will be cleared if the monitored object does not meet the trigger condition within the monitoring period. By default, metrics in only one period are monitored. You can set up to five monitoring periods.

Category	Parameter	Description
	Action Taken for Insufficient Data	<p>Action to be taken when no metric data is generated or metric data is insufficient within the monitoring period. You can set this option based on your requirements.</p> <p>By default, metrics in only one period are monitored. You can set up to five monitoring periods.</p> <p>The system supports the following actions: changing the status to exceeded and sending an alarm, changing the status to insufficient data and sending an event, maintaining the previous status, and changing the status to normal and sending an alarm clearance notification.</p>

– **Template**

Select **Template** and set related parameters. Ensure that you have created an alarm template. For details, see [Creating an Alarm Template](#).

Table 3-18 Alarm condition parameters

Parameter	Description
Bind Template	Specifies whether to bind an alarm profile.
Alarm Template	Select an alarm template. If the existing templates do not meet requirements, click Create Alarm Template to create one.
Alarm Condition	The system automatically imports the preset alarm condition in the template. Note that the condition cannot be modified.
Check Interval	The system automatically imports the check interval set in the template. Note that the check interval cannot be modified.
Alarm Clearance	The system automatically imports the alarm clearance setting in the template. Note that it cannot be modified.
Action Taken for Insufficient Data	The system automatically imports the action setting in the template. Note that it cannot be modified.

Step 6 Set an alarm notification policy.

- **Direct alarm reporting:** An alarm is directly sent when the alarm condition is met.

- a. Specify whether to enable an alarm action rule. After an alarm action rule is enabled, the system sends notifications based on the associated SMN topic and message template. If the existing alarm action rules cannot meet your requirements, click **Create Rule** to create one. For details, see [Creating an Alarm Action Rule](#).
- b. After an alarm action rule is selected, specify whether to enable alarm clearance notification. After alarm clearance notification is enabled, if the alarm clearance condition set in [Advanced Settings > Alarm Clearance](#) is met, alarm clearance notifications are sent based on the selected action rule.

Step 7 Click **Confirm**. Then, click **Back to Alarm Rule List** to view the created alarm rule.

In the expanded list, if a metric value meets the configured alarm condition, a metric alarm is generated on the alarm page. To view it, choose **Alarm Management > Alarm List** in the navigation pane. If a host meets the preset notification policy, the system sends an alarm notification to the specified personnel by email or SMS.

----End

Creating Metric Alarm Rules by Selecting Metrics from All Metrics

Step 1 On the menu bar, choose **Monitoring Center**.

Step 2 In the navigation pane, choose **Alarm Management > Alarm Rules**.

Step 3 On the **Alarm Rules** tab page, click **Create Alarm Rule**.

Step 4 Set basic information about the alarm rule by referring to [Table 3-19](#).

Table 3-19 Basic information

Parameter	Description
Rule Name	Name of a rule. Enter a maximum of 255 characters. The following special characters are not allowed: "\$# %&'<=>?\\"
Description	Description of the rule. Enter up to 1000 characters.

Step 5 Set the detailed information about the alarm rule.

1. Set **Rule Type** to **Metric alarm rule**.
2. Set **Configuration Mode** to **Select from all metrics**.

NOTE

- When **Select from all metrics** is selected, enter keywords to search for metrics.
- **Scope**: Metric monitoring scope. The scope is in the key-value pair format. Directly select an option from the drop-down list or use **AND**, **OR**, and **NOT** to specify scopes for metrics.
- **Group Condition**: Aggregate metric data by the specified field and calculate the aggregation result. Options: **Not grouped**, **avg by**, **max by**, **min by**, and **sum by**. For example, **avg by clusterName** indicates that metrics are grouped by cluster name, and the average value of the grouped metrics is calculated and displayed in the graph.

3. Select a target Prometheus instance from the drop-down list.
4. Set parameters such as the metric, environment, and check interval. [Table 3-20](#) describes the parameters.


After an alarm condition is set, the monitored metric data is displayed in a line graph above the alarm condition. You can click **Hide Graph**,  before a metric name, or the line icon before each metric data record to hide the metric data in the graph.

Table 3-20 Alarm condition parameters

Category	Parameter	Description
-	Add one by one	Calculation is performed based on the preset alarm conditions one by one. An alarm is triggered when one of the conditions is met. For example, if three alarm conditions are set, the system performs calculation respectively. If any of the conditions is met, an alarm will be triggered.
-	Combined operations	After calculation is performed based on the expression you set, an alarm is triggered when the condition is met. For example, if there is no metric showing the CPU core usage of a host, do as follows: <ul style="list-style-type: none"> - Set the metric of alarm condition "a" to aom_node_cpu_used_core and retain the default values for other parameters. This metric is used to count the number of CPU cores used by a measured object. - Set the metric of alarm condition "b" to aom_node_cpu_limit_core and retain the default values for other parameters. This metric is used to count the total number of CPU cores that have been applied for a measured object. - If the expression is set to "a/b", the CPU core usage of the host can be obtained. - Set the threshold condition to > 0.2. - Set Alarm Severity to Critical. A critical alarm will be generated when the CPU core usage of a host is greater than 0.2.
Alarm Condition	Metric	Select the metric to be monitored.

Category	Parameter	Description
	Scope	Metric monitoring scope. The scope is in the key-value pair format. Directly select an option from the drop-down list or use AND , OR , and NOT to specify scopes for metrics.
	Grouping Condition	Aggregate metric data by the specified field and calculate the aggregation result. Options: Not grouped , avg by , max by , min by , and sum by . For example, avg by clusterName indicates that metrics are grouped by cluster name, and the average value of the grouped metrics is calculated and displayed in the graph.
	Alarm Condition	Condition for triggering a metric alarm. It consists of the grouping condition (not grouped), judgment condition (\geq , \leq , $>$, and $<$), and threshold. For example, if the trigger condition is set to > 85 and an actual metric value exceeds 85, a metric alarm will be generated. Move the cursor to the graph area above the alarm condition. The ID, IP address, and unit of the current metric are displayed.
	Alarm Severity	Severity of a metric alarm. Options: Critical , Major , Minor , and Warning .
-	Check Interval	Interval at which metric query and analysis results are checked. <ul style="list-style-type: none"> - Hourly: Query and analysis results are checked every hour. - Daily: Query and analysis results are checked at a fixed time every day. - Weekly: Query and analysis results are checked at a fixed time point on a specified day of a week. - Custom interval: The query and analysis results are checked at a fixed interval. - Cron: A cron expression is used to specify a time interval. Query and analysis results are checked at the specified interval. The time specified in the cron expression can be accurate to the minute and must be in the 24-hour notation. Example: 0/5 * * * *, which indicates that the check starts from 0th minute and is performed every 5 minutes.

Category	Parameter	Description
-	Statistical Period	Metric data is aggregated based on the configured statistical period and statistical mode. If the threshold condition is met for a specified number of consecutive periods, a metric alarm is generated. By default, metrics in the last minute are collected.
Advanced Settings	Alarm Clearance	An alarm will be cleared if the monitored object does not meet the trigger condition within the monitoring period. By default, metrics in only one period are monitored. You can set up to five monitoring periods.
	Action Taken for Insufficient Data	Action to be taken when no metric data is generated or metric data is insufficient within the monitoring period. You can set this option based on your requirements. By default, metrics in only one period are monitored. You can set up to five monitoring periods. The system supports the following actions: changing the status to exceeded and sending an alarm, changing the status to insufficient data and sending an event, maintaining the previous status , and changing the status to normal and sending an alarm clearance notification.

Step 6 Set an alarm notification policy.

- **Direct alarm reporting:** An alarm is directly sent when the alarm condition is met.
 - a. Specify whether to enable an alarm action rule. After an alarm action rule is enabled, the system sends notifications based on the associated SMN topic and message template. If the existing alarm action rules cannot meet your requirements, click **Create Rule** to create one. For details, see [Creating an Alarm Action Rule](#).
 - b. After an alarm action rule is selected, specify whether to enable alarm clearance notification. After alarm clearance notification is enabled, if the alarm clearance condition set in [Advanced Settings > Alarm Clearance](#) is met, alarm clearance notifications are sent based on the selected action rule.

Step 7 Click **Confirm**. Then, click **Back to Alarm Rule List** to view the created alarm rule.

In the expanded list, if a metric value meets the configured alarm condition, a metric alarm is generated on the alarm page. To view it, choose **Alarm Management > Alarm List** in the navigation pane. If a host meets the preset

notification policy, the system sends an alarm notification to the specified personnel by email or SMS.

----End

Creating Metric Alarm Rules by Running Prometheus Statements

- Step 1** On the menu bar, choose **Monitoring Center**.
- Step 2** In the navigation pane, choose **Alarm Management > Alarm Rules**.
- Step 3** On the **Alarm Rules** tab page, click **Create Alarm Rule**.
- Step 4** Set basic information about the alarm rule by referring to [Table 3-19](#).

Table 3-21 Basic information

Parameter	Description
Rule Name	Name of a rule. Enter a maximum of 255 characters. The following special characters are not allowed: "\$# %&'<=>?\\"
Description	Description of the rule. Enter up to 1000 characters.



- Step 5** Set the detailed information about the alarm rule.
 1. Set **Rule Type** to **Metric alarm rule**.
 2. Set **Configuration Mode** to **Run Prometheus statement**.
 3. Select a target Prometheus instance from the drop-down list.
 4. Enter a Prometheus statement. There are two modes: manual input and auto input.
 - Manual input: used when you know the metric name and IP address, and you are familiar with Prometheus statement formats. Click . Related metric graphs are displayed in the lower part of the page in real time.
 - Auto input: used when you do not know the metric information or are unfamiliar with the Prometheus format. The command can only be automatically filled when you switch from the **Metric Browsing** page. Specifically, choose **Metric Browsing** in the navigation pane. Select the Prometheus instance to be monitored from the drop-down list. On the **Metric List** tab page, click **Metric type**, **All metrics**, or **Resource type** and then select up to 12 metrics from the resource tree. Next, click  above the metric list. The system automatically switches to the metric alarm rule creation page and autocompletes the Prometheus command.
 - You can click **View Example** to get more information. For details, see [Prometheus Statements](#).
 5. Set an alarm condition. Set alarm condition parameters, such as consecutive periods, statistical period, and threshold condition. [Table 3-22](#) describes the parameters.

Table 3-22 Alarm condition parameters

Category	Parameter	Description
Alarm Condition	Consecutive Periods	When the metric value meets the alarm condition for a specified number of consecutive periods, a metric alarm will be generated.
	Statistical Period	Metric data is aggregated based on the configured statistical period, which can be 1 minute, 5 minutes, 15 minutes, or 1 hour.
	Statistic	Method used to measure metrics. Options: Avg , Min , Max , Sum , and Samples .
	Alarm Condition	Trigger condition of a metric alarm. An alarm condition consists of two parts: operators (\geq , \leq , $>$, and $<$) and threshold value. For example, if the trigger condition is set to > 85 and an actual metric value exceeds 85, a metric alarm will be generated.
	Alarm Severity	Severity of a metric alarm. Options: Critical , Major , Minor , and Warning .
-	Check Interval	Interval at which metric query and analysis results are checked. <ul style="list-style-type: none"> - Hourly: Query and analysis results are checked every hour. - Daily: Query and analysis results are checked at a fixed time every day. - Weekly: Query and analysis results are checked at a fixed time point on a specified day of a week. - Custom interval: The query and analysis results are checked at a fixed interval. - Cron: A cron expression is used to specify a time interval. Query and analysis results are checked at the specified interval. The time specified in the cron expression can be accurate to the minute and must be in the 24-hour notation. Example: 0/5 * * * *, which indicates that the check starts from 0th minute and is performed every 5 minutes.
Advanced Settings	Alarm Clearance	An alarm will be cleared if the monitored object does not meet the trigger condition within the monitoring period. By default, metrics in only one period are monitored. You can set up to five monitoring periods.

Category	Parameter	Description
	Action Taken for Insufficient Data	<p>Action to be taken when no metric data is generated or metric data is insufficient within the monitoring period. You can set this option based on your requirements.</p> <p>By default, metrics in only one period are monitored. You can set up to five monitoring periods.</p> <p>The system supports the following actions: changing the status to exceeded and sending an alarm, changing the status to insufficient data and sending an event, maintaining the previous status, and changing the status to normal and sending an alarm clearance notification.</p>

Step 6 Set an alarm notification policy.

- **Direct alarm reporting:** An alarm is directly sent when the alarm condition is met.
 - a. Specify whether to enable an alarm action rule. After an alarm action rule is enabled, the system sends notifications based on the associated SMN topic and message template. If the existing alarm action rules cannot meet your requirements, click **Create Rule** to create one. For details, see [Creating an Alarm Action Rule](#).
 - b. After an alarm action rule is selected, specify whether to enable alarm clearance notification. After alarm clearance notification is enabled, if the alarm clearance condition set in [Advanced Settings > Alarm Clearance](#) is met, alarm clearance notifications are sent based on the selected action rule.

Step 7 Click **Confirm**. Then, click **Back to Alarm Rule List** to view the created alarm rule.

In the expanded list, if a metric value meets the configured alarm condition, a metric alarm is generated on the alarm page. To view it, choose **Alarm Management > Alarm List** in the navigation pane. If a host meets the preset notification policy, the system sends an alarm notification to the specified personnel by email or SMS.

----End

3.3.1.3 Creating an Alarm Template

An alarm template contains a group of alarm rules for a specific resource. You can use it to quickly create alarm rules for multiple metrics of a resource. Before creating a metric alarm rule by using a template, ensure that an alarm template has been created.

Precautions

You can create up to 150 alarm templates. If the number of alarm templates reaches 150, delete unnecessary templates and create new ones.

Procedure

- Step 1** On the menu bar, choose **Monitoring Center**.
- Step 2** In the navigation pane, choose **Alarm Management > Alarm Rules**.
- Step 3** On the **Alarm Templates** tab page, click **Create Alarm Template**.
- Step 4** Customize an alarm template. For details, see [Table 3-23](#).

Table 3-23 Alarm template parameters

Category	Parameter	Description
Template Info	Template Name	Name of the template. Enter a maximum of 64 characters. The following special characters are not allowed: "\$#%&'+';<=>?\\"
Template Info	Description	Description of the template. Enter up to 256 characters.
Alarm Rules	Monitored Object	Select a monitored object from the resource tree.
Alarm Rules > Alarm Condition	Metric	Metric to be monitored.
	Consecutive Periods	When the metric value meets the alarm condition for a specified number of consecutive periods, a metric alarm will be generated.
	Statistical Period	Metric data is aggregated based on the configured statistical period, which can be 1 minute, 5 minutes, 15 minutes, or 1 hour.
	Statistic	Method used to measure metrics. Options: Avg , Min , Max , Sum , and Samples .
	Alarm Condition	Trigger condition of a metric alarm. An alarm condition consists of two parts: operators (\geq , \leq , $>$, and $<$) and threshold value. For example, if the trigger condition is set to > 85 and an actual metric value exceeds 85, a metric alarm will be generated.
	Alarm Severity	Severity of a metric alarm. Options: Critical , Major , Minor , and Warning .

Category	Parameter	Description
Alarm Rules	Check Interval	<p>Interval at which metric query and analysis results are checked.</p> <ul style="list-style-type: none"> ● Hourly: Query and analysis results are checked every hour. ● Daily: Query and analysis results are checked at a fixed time every day. ● Weekly: Query and analysis results are checked at a fixed time point on a specified day of a week. ● Custom interval: The query and analysis results are checked at a fixed interval. ● Cron: A cron expression is used to specify a time interval. Query and analysis results are checked at the specified interval. The time specified in the cron expression can be accurate to the minute and must be in the 24-hour notation. Example: 0/5 * * * *, which indicates that the check starts from 0th minute and is performed every 5 minutes.
Alarm Rules > Advanced Settings	Alarm Clearance	An alarm will be cleared if the monitored object does not meet the trigger condition within the monitoring period. By default, metrics in only one period are monitored. You can set up to five monitoring periods.
	Action Taken for Insufficient Data	<p>Action to be taken when no metric data is generated or metric data is insufficient within the monitoring period. You can set this option based on your requirements.</p> <p>By default, metrics in only one period are monitored. You can set up to five monitoring periods.</p> <p>The system supports the following actions: changing the status to exceeded and sending an alarm, changing the status to insufficient data and sending an event, maintaining the previous status, and changing the status to normal and sending an alarm clearance notification.</p>







Step 5 Click **OK**.

----End

More Operations

After the alarm template is created, you can also perform the operations listed in [Table 3-24](#).

Table 3-24 Related operations

Operation	Description
Viewing an alarm template	In the template list, you can view information such as the template name, monitored object, and bound rules. Click  on the left of the template name. In the expanded list, you can view details about the bound rule and alarm condition.
Modifying an alarm template	Click  in the Operation column.
Copying an alarm template	Click  in the Operation column.
Deleting an alarm template	<ul style="list-style-type: none">• To delete an alarm template, click  in the Operation column.• To delete one or more alarm templates, select them and click Delete above the template list.
Unbinding an alarm rule	Click  next to the template name. On the Bound Rule tab page, click Unbind in the row that contains the desired rule to unbind it from the alarm template.
Searching for an alarm template	Enter a template name in the search box in the upper right corner and click  .

3.3.1.4 Creating an Event Alarm Rule

You can set event conditions for services by setting event alarm rules. When the resource data meets an event condition, an event alarm is generated.

Precautions

If you want to receive email or SMS notifications when the resource data meets the event condition, set an alarm action rule by referring to [Creating an Alarm Action Rule](#).

Procedure

- Step 1** On the menu bar, choose **Monitoring Center**.
- Step 2** In the navigation pane, choose **Alarm Management > Alarm Rules**.
- Step 3** on the **Alarm Rules** tab page.
- Step 4** Set basic information about the alarm rule by referring to [Table 3-25](#).

Table 3-25 Basic information

Parameter	Description
Rule Name	Name of a rule. Enter a maximum of 255 characters. The following special characters are not allowed: "\$# %&'<=>?\\"
Description	Description of the rule. Enter up to 1000 characters.

Step 5 Set the detailed information about the alarm rule.

1. Set **Rule Type** to **Event alarm rule**.
2. Set **Event Source**, **Monitored Object**, and **Alarm Condition**.

Table 3-26 Alarm rule parameters

Parameter	Description
Event Source	Name of the service for which an event alarm is reported. You can select a service from the service list.
Monitored Object	Select criteria to filter service events. You can select Notification Type , Event Name , Alarm Severity , Custom Attributes , Namespace , or Cluster Name as the filter criterion. One or more criteria can be selected. NOTE Set Event Name as the filter criterion. If no event name is selected, all events are selected by default.
Alarm Condition	Condition for triggering event alarms. In case of multiple events, click Batch Set to set alarm conditions for these events in batches. <ul style="list-style-type: none"> - Accumulated Trigger: When the trigger condition is met for a specified number of times in a monitoring period, the alarm action rule is triggered and an event alarm of the corresponding severity is sent. - Immediate Trigger: An alarm is generated immediately when the trigger condition is met.

Step 6 Set an alarm notification policy.

- **Direct alarm reporting**: An alarm is directly sent when the alarm condition is met.

For event alarm rules, the alarm action rule is enabled by default. The system sends alarm notifications based on the associated SMN topic and message template. If the existing alarm action rules cannot meet your requirements, click **Create Rule** to create one. For details about how to set an alarm action rule, see [Creating an Alarm Action Rule](#).

Step 7 Click **Confirm**. Then, click **Back to Alarm Rule List** to view the created alarm rule.

To view the alarm, choose **Alarm Management > Alarm List** in the navigation pane. The system also sends alarm notifications to specified personnel by email or SMS.

----End






3.3.1.5 Managing Alarm Rules


After an alarm rule is created, you can view the rule name, type, status, and monitored object of the alarm rule in the rule list. You can also modify, enable, or disable the alarm rule as required.

Procedure

- Step 1** On the menu bar, choose **Monitoring Center**.
- Step 2** In the navigation pane, choose **Alarm Management > Alarm Rules**.
- Step 3** On the **Alarm Rules** tab page, view all created alarm rules and perform the following operations as required. For details, see [Table 3-27](#).

Table 3-27 Operations related to alarm rules

Operation	Description
Filtering and displaying alarm rules	In the rule list, filter alarm rules by rule name, type, status, or other criteria.
Refreshing alarm rules	Click  in the upper right corner of the rule list to obtain the latest information about all alarm rules.
Customizing columns to display	Click  in the upper right corner of the rule list and select or deselect the columns to display.
Modifying alarm rules	Click  in the Operation column. For details, see Creating a Metric Alarm Rule and Creating an Event Alarm Rule .
Deleting alarm rules	<ul style="list-style-type: none"> • To delete an alarm rule, click  in the Operation column. • To delete one or more alarm rules, select them, click Batch Operation above the rule list, and select Delete from the drop-down list.
Enabling or disabling alarm rules	<ul style="list-style-type: none"> • Enable or disable an alarm rule in the Status column. • To enable or disable one or more alarm rules, select them, click Batch Operation above the rule list, and select Enable or Disable from the drop-down list.
Searching for alarm rules	You can search for alarm rules by rule names. Enter a keyword in the search box in the upper right corner and click  to search.

Operation	Description
Viewing detailed alarm information	Click  before a rule name to view rule details, including the basic information and alarm conditions. You can also view the monitored objects and the list of triggered alarms.
Viewing alarms	When the metric value of a resource meets threshold conditions during the configured consecutive periods, the system reports a threshold alarm. In the navigation pane, choose Alarm Management > Alarm List . On the Alarms tab page, view alarms. For details, see Viewing Alarms .
Viewing events	When no metric data of a resource is reported during the configured consecutive periods, the system reports an insufficient data event. In the navigation pane, choose Alarm Management > Alarm List . On the Events tab page, view events. For details, see Viewing Events .

----End

3.3.2 Viewing Alarms

Alarms are reported when AOM or an external service is abnormal or may cause exceptions. You need to take measures accordingly. Otherwise, service exceptions may occur. The **Alarms** tab page allows you to query and handle alarms, so that you can quickly detect, locate, and rectify faults.

Functions

The alarm list provides the following key functions:

- Alarm list: View alarm information by alarm severity in a graph.
- Advanced filtering: You can filter alarms by alarm severity, source, or keyword in the search box. By default, alarms are filtered by alarm severity.
- Alarm deletion: Delete alarms one by one or in batches.
- Alarm details: View the alarm object and handling suggestions in the alarm details. Handling suggestions are provided for all alarms.

Procedure



Step 1 On the menu bar, choose **Monitoring Center**.

Step 2 In the navigation pane, choose **Alarm Management > Alarm List**.

Step 3 Click the **Alarms** tab to view the alarm information.



1. Set a time range to view alarms. There are two methods to set a time range:
Method 1: Use the predefined time label, such as **Last hour** or **Last 6 hours**. You can select a time range as required.

Method 2: Specify the start time and end time to customize a time range. You can specify 31 days at most.

2. Set the interval for refreshing alarms. Click  and select a value from the drop-down list, such as **Refresh manually** or **1 minute auto refresh**.
3. Set filter criteria and click  to view the alarms generated in the period.

Step 4 Perform the operations listed in [Table 3-28](#) as required:

Table 3-28 Operations

Operation	Description
Viewing alarm statistics	Click  , and view alarm statistics that meet filter criteria within a specific time range on a bar graph.
Clearing alarms	<ul style="list-style-type: none"> • To clear an alarm, click  in the Operation column of the target alarm. • To clear one or more alarms, select them and click Clear in the displayed dialog box. <p>NOTE You can clear alarms after the problems that cause them are resolved.</p>
Viewing alarm details	Click an alarm name to view alarm details and handling suggestions.
Viewing cleared alarms	Click Active Alarms in the upper right corner and select Historical Alarms from the drop-down list to view alarms that have been cleared.

----End

3.3.3 Viewing Events



Events generally carry some important information, informing you of the changes of AOM or an external service. Such changes do not necessarily cause exceptions. You can handle events as required. The **Events** tab page allows you to quickly search for events and monitor your system.

Procedure

- Step 1** On the menu bar, choose **Monitoring Center**.
- Step 2** In the navigation pane, choose **Alarm Management > Alarm List**.
- Step 3** Click the **Events** tab to view the event information.
 1. Set a time range to view events. There are two methods to set a time range:


Method 1: Use the predefined time label, such as **Last hour** or **Last 6 hours**. You can select a time range as required.

Method 2: Specify the start time and end time to customize a time range. You can specify 31 days at most.

2. Set the event refresh interval. Click  and select a value from the drop-down list, such as **Refresh manually** or **1 minute auto refresh**.
3. Set filter criteria and click  to view the events generated in the period.

Step 4 Perform the operations listed in [Table 3-29](#) as required:

Table 3-29 Operations

Operation	Description
Viewing event statistics	Click  , and view event statistics that meet filter criteria within a specific time range on a bar graph.
Viewing event details	Click an event name to view event details and handling suggestions.

----End

3.3.4 Alarm Action Rules

3.3.4.1 Overview

The monitoring center allows you to customize alarm action rules. You can create an alarm action rule to associate an SMN topic with a message template. You can also customize notification content based on a message template.

3.3.4.2 Creating an Alarm Action Rule

You can create an alarm action rule and associate it with an SMN topic and a message template. When the resource or metric data meets the alarm condition, the system sends an alarm notification based on the associated SMN topic and message template.

Prerequisites

- A topic has been created.
- A topic policy has been set.
- A subscriber, that is, an email or SMS message recipient has been added for the topic.

Precautions

You can create a maximum of 1000 alarm action rules. If this number has been reached, delete unnecessary rules.

Procedure

Step 1 On the menu bar, choose **Monitoring Center**.

Step 2 In the navigation pane, choose **Alarm Management > Alarm Action Rules**.

Step 3 On the **Action Rules** tab page, click **Create**.

Step 4 Set parameters such as **Rule Name** and **Action Type** by referring to [Table 3-30](#).

Table 3-30 Parameters of an alarm action rule

Parameter	Description
Rule Name	Action rule name. Enter up to 100 characters. Only digits, letters, and underscores (_) are allowed. Do not start or end with an underscore.
Description	Description of the action rule. Enter up to 1024 characters.
Action Type	Type of action that is associated with the SMN topic and message template. Select your desired action from the drop-down list. Currently, only Notification is supported.
Topic	SMN topic. Select your desired topic from the drop-down list. If there is no topic you want to select, create one on the SMN console.
Message Template	Notification message template. Select your desired template from the drop-down list. If there is no message template you want to select, create one by referring to Creating a Message Template .

Step 5 Click **OK**.


----End

More Operations

After an alarm action rule is created, you can perform operations described in [Table 3-31](#).

Table 3-31 Related operations

Operation	Description
Modifying an alarm action rule	Click Modify in the Operation column.

Operation	Description
Deleting an alarm action rule	<ul style="list-style-type: none">To delete a single rule, click Delete in the Operation column in the row that contains the rule, and then click Yes on the displayed page.To delete one or more rules, select them, click Delete above the rule list, and then click Yes on the displayed page. <p>NOTE Before deleting an alarm action rule, you need to delete the alarm rule bound to the action rule.</p>
Searching for an alarm action rule	Enter a rule name in the search box in the upper right corner and click  .

3.3.4.3 Creating a Message Template

You can create message templates to customize notifications. When a preset notification rule is triggered, notifications can be sent to specified personnel by emails or SMS. If no message template is created, the default message template will be used.

Functions

- Message templates for emails and SMS are supported.
- Message templates can be customized. For details, see [Step 3.3](#).

Precautions

- You can create up to 100 message templates. If the number of templates exceeds the upper limit, delete unnecessary templates and create new ones.
- By default, one message template is preset and cannot be deleted or edited. If there is no custom message template, notifications are sent based on a preset message template by default.

Creating a Message Template

Step 1 On the menu bar, choose **Monitoring Center**.

Step 2 In the navigation pane, choose **Alarm Management > Alarm Action Rules**.

Step 3 On the **Message Templates** tab page, click **Create**.

1. Enter a template name and description.

Table 3-32 Parameter description

Parameter	Description
Template Name	Name of a message template. Enter up to 100 characters and do not start or end with an underscore (_) or hyphen (-). Only digits, letters, underscores, and hyphens are allowed.
Description	Description of the template. Enter up to 1024 characters.

2. Select a language (for example, English).
3. Customize the template content (default fields are automatically filled in when a message template is created). There are templates for emails and SMS. For details, see [Table 3-33](#).

 **NOTE**

- In addition to the message fields in the default template, the message template also supports custom fields. You need to specify the fields when reporting event alarms. For details, see the alarm reporting structs in the following message template.
- Custom fields support the JSONPath format. Example: `$event.metadata.case1` or `$event.metadata.case[0]`.
- In the upper right corner of the **Body** area, click **Add Variables** to add required variables.
- If you select **Emails**, you can click **Preview** to view the final effect. On the **Preview** page, change the message topic if necessary.

Table 3-33 Variables in the default message template

Variable	Description	Definition
Account	Account used to log in to the management console.	<code>\${domain_name}</code>
Notification Type	Type selected when an alarm rule is created, which can be Alarm or Event .	<code>\${event_type}</code>
Severity	Alarm or event severity, which can be Critical , Major , Minor , or Warning .	<code>\${event_severity}</code>
Name	Name of the alarm rule that is triggered.	<code>\${event_name}</code>
Occurred	Time when the alarm or event is triggered.	<code>\${starts_at}</code>
Source	Name of the service that triggers the alarm or event.	<code>\${resource_provider}</code>

Variable	Description	Definition
Resource Type	Type of the resource selected when you customize an alarm rule or define alarm reporting.	\${resource_type}
Resource Identifier	Resource that triggers the alarm or event.	\${resources}
Possible Cause	Cause of the alarm. For non-custom reporting, "NA" is displayed.	\${alarm_probableCause_zh}
Additional Info	Additional alarm description, such as the metric name and alarm rule status change.	\${message}
Suggestion	Suggestion on how to handle the alarm. For non-custom reporting, "NA" is displayed.	\${alarm_fix_suggestion_zh}

Alarm reporting structs corresponding to the message template

```
{
  "events": [{
    "starts_at": 1579420868000,    // ${starts_at}
    "ends_at": 1579420868000,
    "timeout": 60000,
    "resource_group_id": "5680587ab6*****755c543c1f",
    "metadata": {
      "event_name": "test",        // ${metadata.event_name}
      "event_severity": "Major",  // ${metadata.event_severity}
      "event_type": "alarm",      // ${metadata.event_type}
      "resource_provider": "ecs",  // ${metadata.resource_provider}
      "resource_type": "vm",      // ${metadata.resource_type}
      "resource_id": "ecs123",
      "key1": "Custom field"      // ${event.metadata.key1}
    },
    "annotations": {
      "alarm_probableCause_zh_cn": "possible cause", // ${annotations.alarm_probableCause_zh}
      "alarm_fix_suggestion_zh_cn": "fix suggestion", // ${annotations.alarm_fix_suggestion_zh}
      "key2": "Custom field"      // ${event.annotations.key2}
    }
  ]
}
```


4. Click **Confirm**. The message template is created.

----End

More Operations

After creating a message template, you can perform the operations listed in [Table 3-34](#).

Table 3-34 Related operations

Operation	Description
Editing a message template	Click Edit in the Operation column.
Copying a message template	Click Copy in the Operation column.
Deleting a message template	<ul style="list-style-type: none"> To delete a single message template, click Delete in the Operation column in the row that contains the template, and then click Yes on the displayed page. To delete one or more message templates, select them, click Delete above the template list, and then click Yes on the displayed page. <p>NOTE Before deleting a message template, delete the alarm action rules bound to it.</p>
Searching for a message template	Enter a template name in the search box in the upper right corner and click  .

3.4 Metric Browsing

The **Metric Browsing** page displays metric data of each resource. You can monitor metric values and trends in real time, and create alarm rules for real-time service data monitoring and analysis.

Monitoring Metrics

- Step 1** On the menu bar, choose **Monitoring Center**.
- Step 2** In the navigation pane, choose **Metric Browsing**.
- Step 3** Select a target Prometheus instance from the drop-down list.
- Step 4** Choose **Metric Sources > Metric List**.
- Step 5** Click **Metric type**, **All metrics**, or **Resource type** and then select one or more metrics from the resource tree. You can also add metrics by running a Prometheus statement. For details, see [Prometheus Statements](#).

 NOTE

- When **All metrics** is selected, enter keywords to search for metrics.
- **Scope:** Metric monitoring scope. The scope is in the key-value pair format. Directly select an option from the drop-down list or use **AND**, **OR**, and **NOT** to specify scopes for metrics.
- **Group Condition:** Aggregate metric data by the specified field and calculate the aggregation result. Options: **Not grouped**, **avg by**, **max by**, **min by**, and **sum by**. For example, **avg by clusterName** indicates that metrics are grouped by cluster name, and the average value of the grouped metrics is calculated and displayed in the graph.

Step 6 Click **Add Metric** to add up to 12 metrics.

 NOTE

If more than 1000 resource metrics are queried, you are advised to use the following methods to monitor metric data so that accurate and comprehensive metric data can be displayed:

1. Adjust the metric query mode to query metric data of a specified resource.
2. Select a top N graph.

Step 7 Set metric parameters by referring to [Table 3-35](#), view the metric graph in the upper part of the page, and analyze metric data from multiple perspectives.

Table 3-35 Metric parameter description

Parameter	Description
Statistic	Method used to measure metrics. Options: Avg , Min , Max , Sum , and Samples . NOTE Samples indicates the number of data points.
Statistical Period	Interval at which metric data is collected. The available statistical period options vary according to the time range you select. For details, see What Is the Relationship Between the Time Range and Statistical Period? .
Time Range	Time range in which metric data is collected. Options: Last 30 minutes , Last hour , Last 6 hours , Last day , Last week , and Custom .
Refresh Frequency	Interval at which the metric data is refreshed. Options: Refresh manually , 30 seconds auto refresh , 1 minute auto refresh , and 5 minutes auto refresh .
Graph Type	Options: line, digit, top N, table, digital line, and bar graphs








Step 8 (Optional) Choose **Metric Sources > Graph Settings** to modify the display settings (such as X/Y axis titles and values) of the metric graph. For details, see [Metric Data Graphs \(Line/Digit/Top N/Table/Bar/Digital Line Graphs\)](#).

----End

More Operations

You can also perform the operations listed in [Table 3-36](#).

Table 3-36 Related operations

Operation	Description
Hiding metric data	After selecting a metric, click  next to the metric to hide the metric data in the current graph. To show the metric data again, click  next to the metric.  or  indicate the status of metric data.
Adding an alarm rule for a metric	After selecting a metric, click  in the upper right corner of the metric list to create an alarm rule for the metric.
Deleting a metric	Click  next to the target metric.
Adding a metric graph to a dashboard	After selecting a metric, click  in the upper right corner of the metric list.
Viewing early metrics	If there was metric data generated within 30 days before the version upgrade, click View Early Metric in the upper right corner of the Metric Browsing page to view and analyze the historical data and graphs.

3.5 Infrastructure Monitoring

3.5.1 Application Monitoring

An application is a group of identical or similar components divided based on business requirements. Applications are classified into system applications and custom applications. System applications are discovered based on built-in discovery rules, and custom applications are discovered based on custom rules.



NOTE

The ICAgent reports resource information every ten minutes. The following describes the resource status changes:

- If the ICAgent on a host does not report resource information **for three consecutive times**, the system determines that the resource has been deleted. Therefore, the host status is displayed as **Deleted** within 30 minutes after the ICAgent is uninstalled or the resource is deleted.
- When the ICAgent on a host reports resource information **for one time**, the system determines that the resource exists. The host status is displayed as **Normal** ten minutes after the resource is created or the ICAgent is installed.



Step 1 On the menu bar, choose **Monitoring Center**.

Step 2 In the navigation pane, choose **Infrastructure Monitoring > Application Monitoring**.

- The application list displays parameters such as the application name, deployment mode, application discovery rule, and number of components.
- To view target applications, set filter criteria (such as the deployment mode, running status, and application name) above the application list.
- In the upper right corner of the page, set application filter criteria.
 - a. Set a time range to view the applications reported. There are two methods to set a time range:
Method 1: Use a predefined time label, such as **Last 30 minutes** or **Last hour**. You can select a time range as required.
Method 2: Specify the start time and end time (max. 15 days).
 - b. Set the interval for refreshing information. Click  in the upper right corner and select a value from the drop-down list, such as **Refresh manually** or **1 minute auto refresh**.
 - c. Click  in the upper right corner, select or deselect the check boxes to show or hide columns.
- Click **Create Application**. On the page that is displayed, configure an application discovery rule. Applications that meet the rule can be automatically discovered and related metrics can be monitored. For details, see [Configuring Application Discovery](#).

Step 3 Set filter criteria to search for the desired application.

Step 4 Click the application name. The **Application Details** page is displayed.

- On the **Application Details** page, view the running status, ID, and creation time of the application.
- In the upper right corner of the page, set a time range and refresh frequency.
- On the **Component List** tab page, view the name, status, and resource usage of components. You can click a component name to view its metrics on the **Component Details** page.
- Enter an instance name in the search box in the upper right corner and click  to search.
- Click  to refresh the component list.
- On the **Host List** tab page, view the name, IP address, status, and resource usage of hosts. You can click a host name to view its metrics on the **Host Details** page.
- On the **Monitoring View** tab page, view key metrics of the target application, such as the CPU usage.
- On the **Alarms** tab page, view the alarm details of the application. For details, see [Viewing Alarms](#).

----End

3.5.2 Component Monitoring

Components refer to the services that you deploy, including containers and common processes.

The component list displays information such as type, CPU usage, and memory usage of each component. You can click a component name to learn more information about the component. AOM supports drill-down from a component to an instance, and then to a container. You can implement multi-dimensional monitoring.



NOTE

The ICAgent reports resource information every ten minutes. The following describes the resource status changes:

- If the ICAgent on a host does not report resource information **for three consecutive times**, the system determines that the resource has been deleted. Therefore, the host status is displayed as **Deleted** within 30 minutes after the ICAgent is uninstalled or the resource is deleted.
- When the ICAgent on a host reports resource information **for one time**, the system determines that the resource exists. The host status is displayed as **Normal** ten minutes after the resource is created or the ICAgent is installed.

Step 1 On the menu bar, choose **Monitoring Center**.


Step 2 In the navigation pane, choose **Infrastructure Monitoring > Component Monitoring**.

- The component list displays information such as **Component Name**, **Application**, **Deployment Mode**, and **Application Discovery Rules**.
- To view target components, you can set filter criteria (such as the running status, application, cluster name, deployment mode, and component name) above the component list.
- Enable or disable **Hide System Components** to hide or show system components. By default, system components are hidden.
- In the upper right corner of the page, set component filter criteria.
 - a. Set a time range to view the components reported. There are two methods to set a time range:
Method 1: Use the predefined time label, such as **Last 30 minutes**, **Last hour**, **Last 6 hours**, **Last day**, or **Last week**. Select one as required.
Method 2: Specify the start time and end time (max. 15 days).
 - b. Set the interval for refreshing information. Click  and select a value from the drop-down list as required, such as **Refresh manually**, **30 seconds auto refresh**, **1 minute auto refresh**, or **5 minutes auto refresh**.
 - c. Click  in the upper right corner, select or deselect the check boxes to show or hide columns.

Step 3 Perform the following operations as required:

- **Adding an alias**

If a component name is complex and difficult to identify, you can add an alias for the component.



In the component list, click  in the **Operation** column of the target component, enter an alias, and click **OK**. The added alias can be modified but cannot be deleted.

Step 4 Set filter criteria to search for the desired component.

 **NOTE**

Components cannot be searched by alias.

Step 5 Click the component name to go to the **Component Details** page.

- On the **Component Details** page, view the running status, ID, creation time, application, cluster, and namespace of the component.
- In the upper right corner of the page, set a time range and refresh frequency.
- On the **Instance List** tab page, view basic information such as the instance type, status, node IP address, usage, and creation time. Click an instance name to view its metrics on the **Instance Details** page.
- Enter an instance name in the search box in the upper right corner and click  to search.
- Click  to refresh the instance list.
- On the **Host List** tab page, view the name, IP address, status, and resource usage of the host where the component is located. Click a host name to view its metrics on the **Host Details** page.
- On **Monitoring View** tab page, monitor key metrics of the component, such as the total number of CPU cores, used CPU cores, and CPU core usage.
- On the **Events** tab page, view the event details of the component. For details, see [Viewing Events](#).
- On the **Alarms** tab page, view the alarm details of the component. For details, see [Viewing Alarms](#).

----End

3.5.3 Host Monitoring

Hosts include Elastic Cloud Servers (ECSs). Both IPv4 and IPv6 addresses are supported.

AOM monitors the resource usage and health status of hosts, common system devices such as disks and file systems of hosts, and service processes or instances running on hosts.

 **NOTE**

The ICAgent reports resource information every ten minutes. The following describes the resource status changes:

- If the ICAgent on a host does not report resource information **for three consecutive times**, the system determines that the resource has been deleted. Therefore, the host status is displayed as **Deleted** within 30 minutes after the host is stopped or the ICAgent is uninstalled.
- When the ICAgent on a host reports resource information **for one time**, the system determines that the resource exists. The host status is displayed as **Normal** ten minutes after the host is started or the ICAgent is installed.


Precautions

- The host status can be **Normal**, **Abnormal**, **Warning**, **Silent**, or **Deleted**. The running status of a host is displayed as **Abnormal** when the host is faulty due to network failures or host power-off or shut-down, or when a threshold alarm is reported on the host. For more information, see [What Can I Do If Resources Are Not Running Properly?](#)



Procedure

Step 1 On the menu bar, choose **Monitoring Center**.

Step 2 In the navigation pane, choose **Infrastructure Monitoring > Host Monitoring**.

- To view desired hosts, set filter criteria (such as the running status, host type, host name, and IP address) above the host list.
- You can select or deselect **Hide master host** as required. By default, master hosts are hidden.
- Click  next to **Hide master host** to synchronize host information.
- In the upper right corner of the page, set host filter criteria.
 - a. Set a time range to view the hosts reported. There are two methods to set a time range:


Method 1: Use the predefined time label, such as **Last 30 minutes**, **Last hour**, **Last 6 hours**, **Last day**, or **Last week**. Select one as required.

Method 2: Specify the start time and end time (max. 15 days).
 - b. Set the interval for refreshing information. Click  and select a value from the drop-down list as required, such as **Refresh manually**, **30 seconds auto refresh**, **1 minute auto refresh**, or **5 minutes auto refresh**.
 - c. Click  in the upper right corner and select or deselect **Tags**.


Step 3 Perform the following operations as required:

- **Adding an alias**

If a host name is too complex to identify, you can add an alias, which makes it easy to identify a host as required.

In the host list, click  in the **Operation** column of the target host, enter an alias, and click **OK**. The added alias can be modified but cannot be deleted.

- **Synchronizing host data**



In the host list, locate the target host and click  in the **Operation** column to synchronize host information.

Step 4 Set filter criteria to search for the desired host.

 **NOTE**

Hosts cannot be searched by alias.

Step 5 Click a host name. The **Host Details** page is displayed.

- On the **Host Details** page, view the running status and ID of the host.
- In the upper right corner of the page, set a time range and refresh frequency.
- Click the **Instance List** tab to view the basic information (such as the instance name and IP address). Click an instance to view its metrics on the details page.
- Enter an instance name in the search box in the upper right corner and click  to search.
- Click  to refresh the instance list.
- On **Monitoring View** tab page, monitor key metrics of the host, such as the total number of CPU cores, used CPU cores, and CPU core usage.
- On the **Events** tab page, view the event details of the host. For details, see [Viewing Events](#).
- On the **Alarms** tab page, view the alarm details of the host. For details, see [Viewing Alarms](#).
- On the **File Systems** tab page, view the basic information about the file system of the host. Click a disk file partition to monitor its metrics on the **Monitoring View** page.
- On the **Disk** tab page, view the basic information about the disks of the host. Click a disk to monitor its metrics on the **Monitoring View** page.
- On the **Disk Partition** tab page, view the disk partition information about the host. Click a disk partition to monitor its metrics on the **Monitoring View** page.
- On the **NIC** tab page, view the basic information about the NICs of the host. Click a NIC to monitor its metrics on the **Monitoring View** page.
- On the **GPU** tab page, view the basic information about the GPUs of the host. Click a GPU to monitor its metrics on the **Monitoring View** page.

----End

3.6 Prometheus Monitoring

AOM is fully connected with the open-source Prometheus ecosystem. It monitors many types of components, provides multiple ready-to-use dashboards, and supports flexible expansion of cloud-native component metric plug-ins.

Precaution

System instances cannot be deleted.

Creating a Prometheus Instance

- Step 1** On the menu bar, choose **Monitoring Center**.
- Step 2** In the navigation pane on the left, choose **Prometheus Monitoring**. In the right pane, click **Add Prometheus Instance**.
- Step 3** Set information such as the instance name and instance type.

Table 3-37 Parameters for creating a Prometheus instance






Parameter	Description
Instance Name	Prometheus instance name. Enter a maximum of 100 characters and do not start or end with an underscore (_) or hyphen (-). Only letters, digits, underscores, and hyphens are allowed.
Instance Type	Type of the Prometheus instance. Currently, only Prometheus for Remote Write is supported.

- Step 4** Click **OK**.

----End

More Operations

Table 3-38 Related operations

Operation	Description
Viewing a Prometheus instance	<p>The Prometheus instance list displays information such as the instance name, instance type, and creation time in real time. Click the instance name to go to the instance details page and view the basic information and credential of the instance.</p> <ul style="list-style-type: none"> By default, the AppKey is hidden. To show it, click  or  reflects the status of the AppKey. Click  on the right of the Prometheus configuration code to copy it to the corresponding file.
Searching for a Prometheus instance	Enter an instance name in the search box and click  .
Deleting a Prometheus instance	Click  in the Operation column of the target Prometheus instance.

3.7 Log Analysis

3.7.1 Searching for Logs





AOM enables you to quickly query logs, and use log source information and context to locate faults.

- Step 1** On the menu bar, choose **Monitoring Center**.
- Step 2** In the navigation pane, choose **Log Analysis > Log Search**.
- Step 3** On the **Log Search** page, click the **System**, or **Host** tab and set filter criteria as prompted.

 **NOTE**

1. You can search for logs by system, or host.
 - For system logs, you can set filter criteria such as **Host**.
 - For host logs, you can set filter criteria such as **Host**.
2. Enter a keyword in the search box. Rules are as follows:
 - Enter a case-sensitive keyword.
 - Enter a keyword for exact search. A keyword refers to a word between two adjacent delimiters.
 - Enter a keyword containing an asterisk (*) or a question mark (?) for fuzzy search. For example, enter **ER?OR**, ***ROR**, or **ER*R**.
 - Enter a phrase for exact search. For example, enter **Start to refresh** or **Start-to-refresh**. Note that hyphens (-) are **delimiters**.
 - Enter a keyword containing AND (&&) or OR (||) for search. For example, enter **query logs&&error*** or **query logs||error**.
 - If no log is found, you are advised to narrow down the search scope and add an asterisk (*) before and after the keyword for fuzzy match.

Step 4 View the search results of logs.

The search results are sorted based on the log collection time. The keywords in the search results are highlighted. You can click  in the **Time** column to switch the sorting order.  indicates the default order.  indicates the ascending order by time (the earliest log is displayed at the top).  indicates the descending order by time (the latest log is displayed at the top).

1. AOM allows you to view context. Click **Context** in the **Operation** column to view the previous or next logs of a log for fault locating.
 - In the **Display Rows** drop-down list, set the number of rows that display raw context data of the log.

 **NOTE**


For example, select **200** from the **Display Rows** drop-down list.

- If there are more than or equal to 100 logs printed before a log and more than or equal to 99 logs printed following the log, the preceding 100 logs and following 99 logs are displayed as the context.
 - If there are fewer than 100 logs (for example, 90) printed before a log and fewer than 99 logs (for example, 80) printed following the log, the preceding 90 logs and following 80 logs are displayed as the context.
- Click **Export Current Page** to export displayed raw context data of the log to a local PC.

 **NOTE**

To ensure that tenant hosts and services run properly, some components (for example, kube-dns) provided by the system will run on the tenant hosts. The logs of these components are also queried during tenant log query.

2. Click **View Details** on the left of the log list to view details such as host IP address and source.

Step 5 (Optional) Click  on the right of the **Log Search** page, select an export format, and export the search result to a local PC.

Logs are sorted according to the order set in [Step 4](#) and a maximum of 5000 logs can be exported. For example, when 6000 logs in the search result are sorted in the descending order, only the first 5000 logs can be exported.

Logs can be exported in CSV or TXT format. You can select a format as required. If you select the CSV format, detailed information (such as the log content, host IP address, and source) can be exported. Only log content will be exported when you select the TXT format. Each line indicates a log.

Step 6 (Optional) Click **Configure Dumps** to dump the searched logs to the same log file in the OBS bucket at a time. For details, see [Adding One-Off Dumps](#).

----End

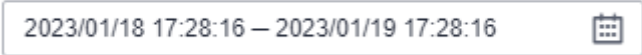
3.7.2 Viewing Log Files

You can quickly view log files of component instances or hosts to locate faults.

Viewing Log Files

- Step 1** On the menu bar, choose **Monitoring Center**.
- Step 2** In the navigation pane, choose **Log Analysis > Log Files**.
- Step 3** On the page that is displayed, click the **Host** tab and click a name. Information such as the log file name and latest written time is displayed on the right of the page.
- Step 4** Click **View** in the **Operation** column of the desired instance. [Table 3-39](#) shows how to view log file details.

Table 3-39 Operations

Operation	Setup	Description
Setting a time range	Date	Click  to select the date and time.
Viewing log files	Clear	Click Clear to clear the logs displayed on the screen. This operation clears only the logs displayed on the screen but does not delete them.
	Viewing real-time logs	The function of real-time monitoring is disabled by default. To enable it, click Enable Real-Time Viewing . After this function is enabled, the latest written logs can be viewed. For real-time log viewing, AOM automatically highlights exception keywords in logs, facilitating fault locating. Such keywords are case-sensitive. For example, when you enter format to search, format in logs will be highlighted, but Format and FORMAT will not.

Step 5 (Optional) Click **Configure Dumps** in the **Operation** column of the target instance to dump its logs to the same log file in the OBS bucket at a time. For details, see [Adding One-Off Dumps](#).

----End

3.7.3 Configuring VM Log Collection Paths

AOM can collect and display VM logs. VM refers to an Elastic Cloud Server (ECS) running Linux. Before collecting logs, ensure that you have set a log collection path.

Prerequisites

You have installed an ICAgent on a VM. For details, see [Installing an ICAgent](#). About five minutes after the ICAgent is installed, you can view your VM in the VM list on the **Path Configuration** page.

Precautions

- An ICAgent collects ***.log**, ***.trace**, and ***.out** log files only. For example, **/opt/yilu/work/xig/debug_cpu.log**.
- Ensure that an absolute path of the log directory or file is configured and the path exists. For example, **/opt/yilu/work/xig** or **/opt/yilu/work/xig/debug_cpu.log**.
- An ICAgent does not collect log files from subdirectories. For example, the ICAgent does not collect log files from the **/opt/yilu/work/xig/debug** subdirectory of **/opt/yilu/work/xig**.
- A maximum of 20 log collection paths can be configured for a VM.
- For ECSs in the same resource space, only the latest log collection configuration in the system will be used. AOM and LTS log collection configurations cannot take effect at the same time. For example, if you configure log collection paths in AOM for ECSs, the previous collection configurations you made in LTS for these ECSs become invalid.

Configuring Log Collection Paths

Step 1 On the menu bar, choose **Monitoring Center**.


Step 2 In the navigation pane, choose **Log Analysis > Path Configuration**.

Step 3 In the VM list, click  in the **Operation** column to configure one or more log collection paths for a VM.

You can use the paths automatically identified by the ICAgent or manually configure paths.

- **Using the paths automatically identified by the ICAgent**

The ICAgent automatically scans the log files of your VM, and displays all the log files that have file handles and are suffixed with **.log**, **.trace**, or **.out** on the page.

You can click  in the **Operation** column to add a path automatically identified by the ICAgent to the log collection path list. To configure multiple paths, repeat this operation.

- **Manually configuring log collection paths**

If the paths automatically identified by the ICAgent cannot meet your requirements, enter a log directory or file (for example, **/usr/local/uniagentd/log/agent.log**) in the **Log Collection Path** text box, and then add the path to the log collection path list. To configure multiple paths, repeat this operation.

Step 4 Click **OK**.

----End

Viewing VM Logs

After a log collection path is configured, the ICAgent collects log files from the configured path. The collection takes about 1 minute. After the collection is complete, you can perform the following operations:

- **Viewing VM log files**

In the navigation pane, choose **Log Analysis > Log Files**. Click the **Host** tab to view the collected log files. For details, see [Viewing Log Files](#).

- **Viewing and analyzing VM logs**

In the navigation pane, choose **Log Analysis > Log Search**. Click the **Host** tab to view and analyze the collected logs by time range, keyword, and context. For details, see [Searching for Logs](#).

3.7.4 Adding Log Dumps

AOM dumps logs to Object Storage Service (OBS) buckets for long-term storage. To store logs for a long period, add log dumps.

AOM offers both periodic and one-off dump modes. You can choose one of them as required.

- **Periodic dump:** Current logs are dumped in real time into an OBS bucket and 1-day logs are divided based on the dump cycle.

To periodically store logs for a long period, add periodic dumps. For details, see [Adding Periodic Dumps](#).

- **One-off dump:** Historical logs are dumped to a log file of an OBS bucket at a time.

One-off dump is similar to the export function on the **Log Search** page. You can export up to 5000 logs on that page. When you need to export more logs but the export function cannot meet your needs, dump the logs at a time according to [Adding One-Off Dumps](#).

NOTE

- To add a log dump, you must have OBS administrator permissions in addition to AOM and LTS permissions.
- If you need to dump logs to OBS buckets in real time for long-term storage, use the log dump function of LTS.

Adding Periodic Dumps

For example, when you need to dump the logs of the **als0320a** component into corresponding files in the **/home/Periodical Dump** directory of the **obs-store-test** OBS bucket in real time, and the dump cycle is 3 hours, do as follows:

- Step 1** On the menu bar, choose **Monitoring Center**.
- Step 2** In the navigation pane, choose **Log Analysis > Log Dumps**.
- Step 3** Click **Add Log Dump** in the upper right corner of the page. Then, set parameters according to [Table 3-40](#) and click **OK**.

Table 3-40 Periodic dump parameters

Parameter	Description	Example
Dump Mode	Select Periodic dump .	Periodic dump
Filter Criteria	Logs can be filtered by multiple criteria such as log type, cluster, or namespace, so that you can dump the logs that meet specific criteria.	Set Log Type to Host , Cluster Name to All custom clusters , and Host to 192.168.0.170 .
Log Group	Logs can be categorized into logical groups, so that you can dump them based on groups.	log-group1
Dump Cycle	You can divide 1-day logs based on the dump cycle. There are "N" time segments in a day (Number of time segments = 24 hours/Dump cycle). The logs of the same time segment are dumped into the same log file. For example, if the dump cycle is set to 3 hours, there are 8 time segments in a day. The logs generated at 00:00–03:00 in a day are dumped to the log file in the Log collection date (format: YYYY-MM-DD) > 00 path, and the logs generated at 03:00–06:00 in a day are dumped to the log file in the Log collection date (format: YYYY-MM-DD) > 03 path. Other time segments can be deduced by analogy.	3 hours
Target OBS Bucket	OBS bucket that stores logs. NOTE Before storing logs, ensure that an OBS bucket has been created. You can click View OBS and create a bucket on the OBS console.	obs-store-test

Parameter	Description	Example
OBS Bucket Directory	OBS bucket directory for storing logs.	/home/ Periodical Dump

After the periodic dump is added, the new logs of the specified resource will be dumped into the OBS bucket in real time.

In the preceding example, the logs of host **192.168.0.170** will be dumped into corresponding log files in the **/home/Periodical Dump** directory of the **obs-store-test** bucket in real time, and the dump cycle is 3 hours.

 **NOTE**

Periodic dump is a near-real-time dump but has latency in minutes. The latency varies depending on log quantity and size. Details are as follows:

- If the number of logs generated within 5 minutes exceeds 1000 or the log size exceeds 2 MB, the logs are dumped in real time.
- If the number of logs generated within 5 minutes is less than 1000 or the log size is less than 2 MB, the logs are dumped every 5 minutes.

Step 4 Download the log files in the OBS bucket to a local host for locating faults.

1. In the periodic dump list, click the target OBS bucket to go to the **Objects** page on the OBS console.
2. On the **Objects** tab page, find the log files stored in OBS, such as **192.168.0.74_var-paas-sys-log-apm-count_warn.log** and **192.168.0.74_var-paas-sys-log-apm-debug_erro.trace**.

Paths of the log files dumped to the OBS bucket: Log file paths are related to the selected log types, as shown in the following table.

Table 3-41 Paths of the log files dumped to the OBS bucket

Log Type	Log File Path
Component	Belong bucket directory > Log group name > Cluster name > Component name > Log collection date (format: YYYY-MM-DD) > File ID (format: 0X) For example, obs-store-test > home > Periodical Dump > log-group1 > zhqtest0112n > als0320a > 2019-03-22 > 03 .
Host	Belong bucket directory > Log group name > CONFIG_FILE > default_appname > Log collection date (format: YYYY-MM-DD) > File ID (format: 0X)
System	Belong bucket directory > Log group name > Cluster name > Log collection date (format: YYYY-MM-DD) > File ID (format: 0X)

Names of the log files dumped to the OBS bucket: Host IPv4 address_Log file source_Log file name. Note that slashes (/) in a log file source must be replaced with hyphens (-). For example, **192.168.0.74_var-paas-sys-log-apm-count_warn.log** or **192.168.0.74_var-paas-sys-log-apm-debug_erro.trace**.

3. Select the required log file and click **Download** to download it to the default download path. To save the log file to a custom path, choose **More > Download As**.

----End

Adding One-Off Dumps

For example, to dump the logs that contain the **warn** keyword in the last 30 minutes of **als0320a** to the **/home/One-off Dump** directory of the **obs-store-test** OBS bucket, do as follows:

- Step 1** On the menu bar, choose **Monitoring Center**.
- Step 2** In the navigation pane, choose **Log Analysis > Log Dumps**.
- Step 3** Click **Add Log Dump** in the upper right corner of the page. Then, set parameters according to [Table 3-42](#) and click **OK**.

Table 3-42 One-off dump parameters

Parameter	Description	Example
Dump Mode	Select One-off dump .	One-off dump
Filter Criteria	Logs can be filtered by multiple criteria such as log collection time, cluster, or namespace, so that you can dump the logs that meet specific criteria.	Set Log Collection Time to Last 30 minutes . Set Log Type to Host , Cluster Name to All custom clusters , Host to 192.168.0.170 , and Keyword to warn .
Log Group	Logs can be categorized into logical groups, so that you can dump them based on groups. NOTE After a dump task is deleted, log groups will also be deleted.	log-group2
Target OBS Bucket	OBS bucket that stores logs. NOTE If no OBS bucket is available, click View OBS to create a bucket on the OBS console.	obs-store-test

Parameter	Description	Example
OBS Bucket Directory	OBS bucket directory for storing logs. NOTE By default, logs are stored in the root directory of the OBS bucket.	/home/One-off Dump

After the one-off dump is added and the dump status changes to **Dumped**, the historical logs that meet criteria are dumped into the same log file of the OBS bucket at a time.

For example, the historical logs that contain the **warn** keyword in the last 30 minutes of host **192.168.0.170** will be dumped to the **log-group2_shard_0(custom).log** file in the **/home/One-off Dump** directory of the **obs-store-test** bucket at a time.

Step 4 Download the log files in the OBS bucket to a local host for locating faults.

1. In the one-off dump list, click the target OBS bucket to go to the **Objects** page on the OBS console.
2. On the **Objects** tab page, find the log file stored in OBS, for example, **/home/One-off Dump/log-group2_shard_0(custom).log**.

Paths of the log files dumped to the OBS bucket: **OBS bucket > Belong bucket directory**. For example, **obs-store-test/home/One-off Dump**.

Names of the log files dumped to the OBS bucket: Log file names are related to dump file formats, as shown in the following table.

Table 3-43 Names of the log files dumped to the OBS bucket

Name of Log File
- Log group name _shard_0(custom) , for example, log-group2_shard_0(custom).log
- Log group name _shard_1(custom)

3. Select the required log file and click **Download** to download it to the default download path. To save the log file to a custom path, choose **More > Download As**.

----End

3.7.5 Accessing LTS

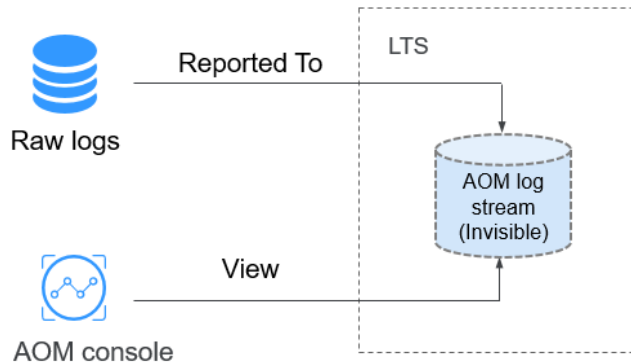
3.7.5.1 Introduction

Log Tank Service (LTS) allows you to search for and dump logs. By setting access rules, you can map the logs of workloads from AOM to LTS for analysis.

What Is Mapping?

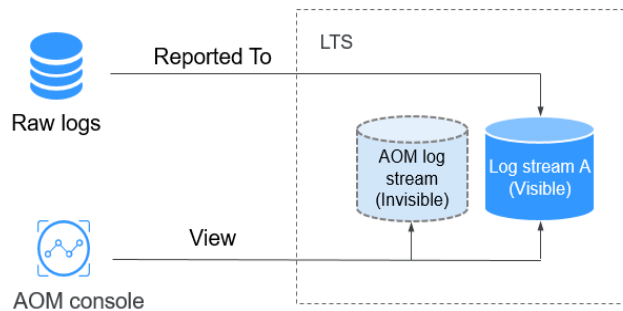
AOM logs exist in LTS in the form of a log stream, as shown in [Figure 3-1](#). You can view raw logs in configured log collection paths on AOM, but cannot view the AOM log stream on LTS. You can create a mapping by adding an access rule on AOM. After the mapping is created, you can view and analyze AOM logs on LTS.

Figure 3-1 Before mapping



After you create log stream A and an access rule, the mapping from AOM to LTS is created. New AOM logs will be reported to log stream A. You can view all logs on AOM before and after the mapping. Historical logs in the AOM log stream will not be copied or migrated to log stream A, as shown in [Figure 3-2](#).

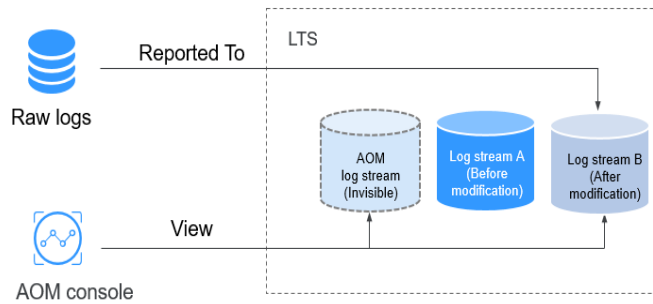
Figure 3-2 After mapping



Modifying a Mapping

If you modify a mapping, for example, change log stream A to log stream B, new logs will be reported to log stream B. You can view the content of AOM log stream and log stream B on AOM, but cannot view the content of log stream A, as shown in [Figure 3-3](#).

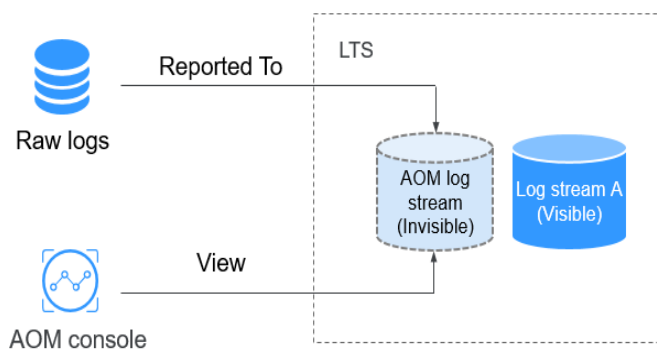
Figure 3-3 Modifying a mapping



Deleting a Mapping

When you delete an access rule or a mapped log stream, the corresponding mapping is deleted. New logs are reported only to the AOM log stream. In this case, you cannot view the content of log stream A, as shown in [Figure 3-4](#). If the access rule is deleted but log stream A is not, you can still view the logs that have already been mapped on LTS.

Figure 3-4 Deleting a mapping

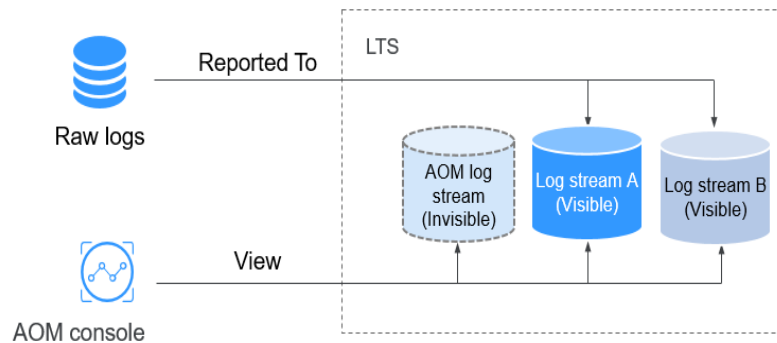


NOTE

Deleted access rules or mapped log streams cannot be recovered. Exercise caution when performing this operation.

Duplicate Mapping

If a workload or file is mapped to both log streams A and B, new logs will be reported to both of them. Duplicate logs exist on AOM. Therefore, duplicate mapping is not recommended.

Figure 3-5 Duplicate mapping

3.7.5.2 Managing Access Rules

This section describes how to add, view, and delete access rules.

Prerequisites

- A log group and log stream have been created. You can also create them on the **Add Access Rule** page.
- A cluster, namespace, and workload are available.

Adding Access Rules

To map the logs of workloads from AOM to LTS, perform the following steps:

Step 1 On the menu bar, choose **Monitoring Center**.

Step 2 In the navigation pane, choose **Log Analysis > LTS Access**.

Step 3 Click **Add Access Rule**.

Step 4 Select an access type. **Access by Namespace**, **Access by Workload**, or **Automatic Mapping** are available.

- **Access by Namespace:** All logs of the selected namespace are connected to the specified log stream.
 - a. **Rule Name:** Enter a rule name. Only letters, digits, hyphens (-), underscores (_), and periods (.) are allowed.
 - b. **Cluster:** Select a cluster from the drop-down list.
 - c. **Namespace:** Select a namespace from the drop-down list.
 - d. **Workload:** Retain the default value **All**.
 - e. **Container Name:** Select a container from the drop-down list.
 - f. Set an access rule.
 - **Access all logs:** If you select this option, select a log group and log stream.
 - **Specify log paths:** If you select this option, specify a log path and then select a log group and log stream.
- **Access by Workload:** Logs of the selected workload are connected to the specified log stream.

- a. **Rule Name:** Enter a rule name. Only letters, digits, hyphens (-), underscores (_), and periods (.) are allowed.
 - b. **Cluster:** Select a cluster from the drop-down list.
 - c. **Namespace:** Select a namespace from the drop-down list.
 - d. **Workload:** Select one or more workloads from the drop-down list.
 - e. **Container Name:** Select a container from the drop-down list.
 - f. Set an access rule.
 - **Access all logs:** If you select this option, select a log group and log stream.
 - **Specify log paths:** If you select this option, specify a log path and then select a log group and log stream.
- **Automatic Mapping:** Workload logs are automatically connected to the generated log streams with the same names as the workloads.
 - a. **Rule Name:** Enter a rule name. Only letters, digits, hyphens (-), underscores (_), and periods (.) are allowed.
 - b. **Cluster:** Select a cluster from the drop-down list.
 - c. **Namespace:** Select a namespace from the drop-down list.
 - d. **Workload:** Select one or more workloads from the drop-down list.

If you select one workload, the rule name is changed to **Custom rule name_0** after the rule is created, for example, **test_0**. If you select multiple workloads, the rule names are changed to **Custom rule name_0**, **Custom rule name_1**, and so on, such as **test_0** and **test_1**.
 - e. Set an access rule: Select a log group and specify a log stream prefix. A log stream will be generated based on the log stream prefix and workload name. By default, all logs of the selected workload are connected.

----End


Managing Access Rules

On the **LTS Access** page, you can search for, view, edit, and delete access rules.

- Search

Click the search box, select a filter criterion, for example, **Workload**, and then select options under it. You can also directly enter a keyword in the search box. In this case, the system searches for information based on access rule names by default.
- View

In the rule list, view the cluster name and namespace of the created rule.

Click  in the upper right corner of the search box to customize the display of columns. Click a log group name in the **Log Group** column to go to the log group details page on the LTS console.
- Modify

On the **LTS Access** page, click **Edit** in the **Operation** column to edit an access rule. For details about the impact of modifying an access rule, see [Modifying a Mapping](#).

- Delete

On the **LTS Access** page, click **Delete** in the **Operation** column to delete an access rule. Select one or more access rules and click **Delete** above the rule list.

NOTE

Deleted access rules or mapped log streams cannot be recovered. Exercise caution when performing this operation. For details about the impact of deleting an access rule, see [Deleting a Mapping](#).

Other Operations

On the **Access LTS** page, click **Go to LTS Console** to go to the LTS console and create a log group and log stream for mapping.

3.8 Configuration Management

3.8.1 Log Configuration

3.8.1.1 Viewing the Log Quota

Step 1 On the menu bar, choose **Monitoring Center**.

Step 2 Log in to the AOM console. In the navigation pane, choose **Configuration Management > Log Configuration**.

Step 3 On the **Quota Details** tab page, view the log size and retention period.

Log Retention Period: 7 days (default), which cannot be changed.

----End

3.8.1.2 Configuring Delimiters

AOM enables you to divide the log content into multiple words for search by configuring delimiters. By default, AOM provides the following delimiters:

```
",";=()[]{}@&<>/\n\t\r
```

If default delimiters cannot meet requirements, customize delimiters according to the following procedure.

Precautions

Delimiters are applicable only to the logs generated after the delimiters are configured. Earlier logs are processed based on earlier delimiters.




Procedure

Step 1 On the menu bar, choose **Monitoring Center**.

Step 2 In the navigation pane, choose **Configuration Management > Log Configuration**, and click the **Delimiter Configuration** tab.

Step 3 Configure delimiters.

You can configure delimiters using the following methods: If you use both methods at the same time, the union set will be selected.

- Custom delimiters: Click , enter a delimiter in the text box, and click .
- Use ASCII code: Click **Add Special Delimiters**, enter the ASCII value according to [ASCII Comparison Table](#), and click .

Step 4 Preview the log content.

Enter the log content to preview in the text box and click **Preview**.

Step 5 Confirm the configuration and click **OK**.

NOTE

Click **Reset** to restore the default configuration. Default delimiters are as follows:

```
,";=()[]{}@&<>/:\n\t\r
```

----End

ASCII Comparison Table

Table 3-44 ASCII comparison table

ASCII Value	Control Character	ASCII Value	Control Character	ASCII Value	Control Character	ASCII Value	Control Character
0	NUL (Null)	32	Space	64	@	96	`
1	SOH (Start of heading)	33	!	65	A	97	a
2	STX (Start of text)	34	"	66	B	98	b
3	ETX (End of text)	35	#	67	C	99	c
4	EOT (End of transmission)	36	\$	68	D	100	d
5	ENQ (Enquiry)	37	%	69	E	101	e

ASCII Value	Control Character	ASCII Value	Control Character	ASCII Value	Control Character	ASCII Value	Control Character
6	ACK (Acknowledge)	38	&	70	F	102	f
7	BEL (Bell)	39	'	71	G	103	g
8	BS (Backspace)	40	(72	H	104	h
9	HT (Horizontal tab)	41)	73	I	105	i
10	LF (Line feed)	42	*	74	J	106	j
11	VT (Vertical tab)	43	+	75	K	107	k
12	FF (Form feed)	44	,	76	L	108	l
13	CR (Carriage return)	45	-	77	M	109	m
14	SO (Shift out)	46	.	78	N	110	n
15	SI (Shift in)	47	/	79	O	111	o
16	DLE (Data link escape)	48	0	80	P	112	p
17	DC1 (Device control 1)	49	1	81	Q	113	q
18	DC2 (Device control 2)	50	2	82	R	114	r
19	DC3 (Device control 3)	51	3	83	S	115	s
20	DC4 (Device control 4)	52	4	84	T	116	t

ASCII Value	Control Character	ASCII Value	Control Character	ASCII Value	Control Character	ASCII Value	Control Character
21	NAK (Negative acknowledge)	53	5	85	U	117	u
22	SYN (Synchronous suspension)	54	6	86	V	118	v
23	ETB (End of transmission block)	55	7	87	W	119	w
24	CAN (Cancel)	56	8	88	X	120	x
25	EM (End of medium)	57	9	89	Y	121	y
26	SUB (Substitute)	58	:	90	Z	122	z
27	ESC (Escape)	59	;	91	[123	{
28	FS (File separator)	60	<	92	/	124	
29	GS (Group separator)	61	=	93]	125	}
30	RS (Record separator)	62	>	94	^	126	~
31	US (Unit separator)	63	?	95	_	127	DEL (Delete)

3.8.2 Configuring Application Discovery

AOM can discover applications and collect their metrics based on configured rules. Application discovery supports both automatic and manual configuration. This section focuses on manual configuration.

- **Automatic configuration**

After you install the ICAgent on a host according to [Installing an ICAgent](#), the ICAgent automatically discovers applications on the host based on [Built-in Service Discovery Rules](#) and displays them on the **Application Monitoring** page.

- **Manual configuration**

After you add a custom application discovery rule on the application discovery page and apply it to the host where the ICAgent is installed (for details, see [Installing an ICAgent](#)), the ICAgent discovers applications on the host based on the configured service discovery rule and displays them on the **Application Monitoring** page.

Filtering Rules

The ICAgent will periodically detect processes on the target host. The effect is similar to that of running the `ps -e -o pid,comm,lstart,cmd | grep -v defunct` command. Then, the ICAgent checks whether processes match the filtering rules in [Table 3-45](#). If a process meets a filtering rule, the process is filtered out and is not discovered by AOM. If a process does not meet any filtering rules, the process is not filtered and is discovered by AOM.

ICAgent detection results may as follows:

PID	COMMAND	STARTED	CMD
1	systemd	Tue Oct 2 21:12:06 2018	/usr/lib/systemd/systemd --switched-root --system --deserialize 20
2	kthreadd	Tue Oct 2 21:12:06 2018	[kthreadd]
3	ksoftirqd/0	Tue Oct 2 21:12:06 2018	(ksoftirqd/0)
1140	tuned	Tue Oct 2 21:12:27 2018	/usr/bin/python -Es /usr/sbin/tuned -l -P
1144	sshd	Tue Oct 2 21:12:27 2018	/usr/sbin/sshd -D
1148	agetty	Tue Oct 2 21:12:27 2018	/sbin/agetty --keep-baud 115200 38400 9600 hvc0 vt220
1154	docker-containe	Tue Oct 2 21:12:29 2018	docker-containerd -l unix:///var/run/docker/libcontainerd/docker-containerd.sock --shim docker-containerd-shim --start-timeout 2m --state-dir /var/run/docker/libcontainerd/containerd --runtime docker-runc --metrics-interval=0

Table 3-45 Filtering rules

Filtering Rule	Example
If the COMMAND value of a process is docker-containe , vi , vim , pause , sshd , ps , sleep , grep , tailf , tail , or systemd-udevd , and the process is not running in the container, the process is filtered out and is not discovered by AOM.	In the preceding information, the process whose PID is 1154 is not discovered by AOM because its COMMAND value is docker-containe .
If the CMD value of a process starts with [and ends with] , the process is filtered out and is not discovered by AOM.	In the preceding information, the process whose PID is 2 is not discovered by AOM because its CMD value is [kthreadd] .
If the CMD value of a process starts with (and ends with) , the process is filtered out and is not discovered by AOM.	In the preceding information, the process whose PID is 3 is not discovered by AOM because its CMD value is (ksoftirqd/0) .

Filtering Rule	Example
If the CMD value of a process starts with /sbin/ , the process is filtered out and is not discovered by AOM.	In the preceding information, the process whose PID is 1148 is not discovered by AOM because its CMD value starts with /sbin/ .

Built-in Service Discovery Rules

AOM provides **Default_Rule**, and ICAgent has the built-in **Sys_Rule**. These rules are executed on all hosts, including those added later. The priorities of the built-in discovery rules are as follows: **Sys_Rule** > **Default_Rule**. Rule details are as follows:

Sys_Rule (cannot be disabled)

When **Sys_Rule** is used, both the component name and application name must be set. The names are determined according to the following priorities:

- Priorities for determining the application name:
 - a. Use the value of the **Dapm_application** field in the process startup command.
 - b. If the value in **a** is empty, use the value of the **Dapm_application** field in the **JAVA_TOOL_OPTIONS** variable.
 - c. If the value in **b** is empty, use the value of the **PAAS_MONITORING_GROUP** variable.
 - d. If the value in **c** is empty, use the value of the **DAOM.APPN** field in the process startup command.
- Priorities for determining the component name:
 - a. Use the value of the **DAOM.PROCN** field in the process startup command. If the value is empty, use the value of the **Dapm_tier** field.
 - b. If the value in **a** is empty, use the value of the **Dapm_tier** field in the **JAVA_TOOL_OPTIONS** variable.
 - c. If the value in **b** is empty, use the value of the **PAAS_APP_NAME** variable.

In the following example, the component name is **atps-demo** and the application name is **atpd-test**.

```
PAAS_MONITORING_GROUP=atpd-test
PAAS_APP_NAME=atps-demo
JAVA_TOOL_OPTIONS=-javaagent:/opt/oss/servicemgr/ICAgent/pinpoint/pinpoint-bootstrap.jar -
Dapm_application=atpd-test -Dapm_tier=atps-demo
```

Default_Rule (can be disabled)

- If the **COMMAND** value of a process is **java**, obtain the name of the JAR package in the command, the main class name in the command, and the first keyword that does not start with a hyphen (-) in the command based on the priorities in descending order as the component name, and use the default value **unknownapplicationname** as the application name.
- If the **COMMAND** value of a process is **python**, obtain the name of the first **.py/.pyc** script in the command as the component name, and use the default value **unknownapplicationname** as the application name.

- If the **COMMAND** value of a process is **node**, obtain the name of the first .js script in the command as the component name, and use the default value **unknownapplicationname** as the application name.

Custom Discovery Rules

The priorities of discovery rules are as follows: **Sys_Rule** > **Custom discovery rules** > **Default_Rule**.

Step 1 On the menu bar, choose **Monitoring Center**.

Step 2 In the navigation pane, choose **Configuration Management** > **Application Discovery**.

Step 3 Click **Add Custom Application Discovery Rule** and configure an application discovery rule.

Step 4 Select a host for pre-detection.

1. Customize a rule name, for example, **rule-test**.
2. Select a typical host, for example, **host-test**, to check whether the application discovery rule is valid. The hosts that execute the rule will be configured in [Step 7](#). Then, click **Next**.

Step 5 Set an application discovery rule.

1. Click **Add Check Items**. AOM can discover processes that meet the conditions of check items.

For example, AOM can detect the processes whose command parameters contain **ovs-vsitchd unix:** and environment variables contain **SUDO_USER=paas**.

NOTE

- To precisely detect processes, you are advised to add check items about unique features of the processes.
 - You need to add one check item at least and can add five check items at most. If there are multiple check items, AOM only discovers the processes that meet the conditions of all check items.
2. After adding check items, click **Detect** to search for the processes that meet the conditions.

If no process is detected within 10s, modify the application discovery rule and detect processes again. Go to the next step only when at least one process is detected.

Step 6 Set a component name.

1. Set an application name.

In the **Application Name Settings** area, click **Add Naming Rule** to set an application name for the discovered process.

NOTE

- If you do not set an application name, **unknownapplicationname** is used by default.
- When you add multiple naming rules, all the naming rules are combined as the application name of the process. Metrics with the same application name are aggregated.

2. Set a component name.

In the **Component Name Settings** area, click **Add Naming Rule** to set a component name for the discovered process.

 **NOTE**

- The component name cannot be left blank.
 - When you add multiple naming rules, all the naming rules are combined as the component name of the process. Metrics with the same component name are aggregated.
3. Preview the component name.
If the application or component name does not meet your requirements, locate the name in the **Preview Component Name** table and rename it.

Step 7 Set a priority and detection range.

1. Set a priority: When there are multiple rules, set priorities. Enter 1 to 9999. The default value is **9999**. The smaller value, the higher priority. For example, **1** indicates the highest priority and **9999** indicates the lowest priority.

 **NOTE**

- Do not use multiple custom discovery rules with the same priority for the same process.
2. Set a detection range: Select a host to be detected. That is, select the host to which the configured rule is applied. If no host is selected, this rule will be executed on all hosts, including those added later.

Step 8 Click **Add** to complete the configuration. AOM collects metrics of the process.

Step 9 Wait for about two minutes, choose **Infrastructure Monitoring > Component Monitoring** in the navigation pane, select the target host (for example, **host-test**) from the cluster drop-down list, and find the target component (for example, / **openswitch/**) that has been monitored.

----End

More Operations

After creating an application discovery rule, you can also perform the operations described in [Table 3-46](#).

Table 3-46 Related operations

Operation	Description
Viewing rule details	In the Name column, click the name of an application discovery rule.
Enabling or disabling a rule	<ul style="list-style-type: none"> • Click Enable in the Operation column. • Click Disable in the Operation column. After a rule is disabled, AOM does not collect process metrics.

Operation	Description
Deleting a rule	<ul style="list-style-type: none">To delete a discovery rule, click Delete in the Operation column. NOTE Built-in application discovery rules cannot be deleted.
Modifying a rule	Click Modify in the Operation column. NOTE Built-in application discovery rules cannot be modified.

3.8.3 Access Management

3.8.3.1 Introduction

Access Management allows you to quickly connect monitoring data to AOM. This function determines whether to establish or delete network channels, and generate or revoke authentication credentials for reporting monitoring data.

By using the generated access code as an authentication credential, you can remotely report native Prometheus metrics to AOM according to [Reporting Prometheus Data to AOM](#) and store time series data for a long time. You can also use the access code to query data in AOM according to [Viewing Metric Data in AOM Using Grafana](#). AOM supports the following native Prometheus APIs:

APIs for querying Prometheus data:

- GET /v1/:project_id/aom/api/v1/query
- GET /v1/:project_id/aom/api/v1/labels
- GET /v1/:project_id/aom/api/v1/label/:label_name/values
- POST /v1/:project_id/aom/api/v1/query
- POST /v1/:project_id/aom/api/v1/query_range
- POST /v1/:project_id/aom/api/v1/labels

When calling the preceding APIs, add **access_code** to the **Authorization** field in the request header.

Example: "Authorization: Bearer {access_code}" or "Authorization: Basic base64Encode("aom_access_code:{access_code}")"

API for reporting time series data: **POST /v1/:project_id/push**

NOTE

base64Encode means that parameters are encoded using Base64.

3.8.3.2 Reporting Prometheus Data to AOM

If you have deployed the open-source Prometheus, go to [Step 4](#).

This section describes how to configure the **access code** in the Prometheus configuration file and make the configuration effective.

Prerequisites

You have created an ECS.


Procedure

Step 1 Install and start Prometheus. For details, see [Prometheus official documentation](#).

Step 2 Add an access code.

1. Log in to the AOM console and choose **Monitoring Center** in the menu bar.
2. In the navigation pane on the left, choose **Global Configuration**.
3. In the right pane, click **Add Access Code**.
4. In the dialog box that is displayed, click **OK**. The system automatically generates an access code.

NOTE

- You can create up to two access codes for each project.
 - An access code is an identity credential for calling APIs. Keep your access code secure.
5. After the access code is added, click  to view it. To delete the access code, click **Delete** in the **Operation** column. Deleted access codes cannot be recovered. Exercise caution when performing this operation.

Step 3 Obtain the configuration code for Prometheus remote write.

1. Log in to the AOM console and choose **Monitoring Center** in the menu bar.
2. In the navigation pane on the left, choose **Prometheus Monitoring**. In the instance list, click the name of the target Prometheus instance.
3. Obtain the configuration code for Prometheus remote write.

Step 4 Log in to the ECS and locate the Prometheus configuration file.

Run the following command:

```
./prometheus --config.file=prometheus.yml
```

Open **prometheus.yml** and add the configuration code obtained in [Step 3](#) to the end.

The following shows an example. You need to configure the italic part.

```
# my global config
global:
  scrape_interval: 15s # Set the scrape interval to every 15 seconds. Default is every 1 minute.
  evaluation_interval: 15s # Evaluate rules every 15 seconds. The default is every 1 minute.
  # scrape_timeout is set to the global default (10s).

# Alertmanager configuration
alerting:
  alertmanagers:
    - static_configs:
      - targets:
        # - alertmanager:9093

# Load rules once and periodically evaluate them according to the global 'evaluation_interval'.
rule_files:
  # - "first_rules.yml"
  # - "second_rules.yml"
```



```
# A scrape configuration containing exactly one endpoint to scrape:
# Here it's Prometheus itself.
scrape_configs:
# The job name is added as a label `job=<job_name>` to any timeseries scraped from this config.
- job_name: 'prometheus'

# metrics_path defaults to '/metrics'
# scheme defaults to 'http'.

static_configs:
- targets: ['localhost:9090']
remote_write:
- url: 'https://${POD_LB_IP}:8149/v1/{project_id}/{prometheus_instance}/push'
  tls_config:
    insecure_skip_verify: true
    bearer_token: 'SE**iH'
```

Step 5 Check the private domain name.

In the preceding example, data is reported through the intranet. Ensure that the host where Prometheus is located can resolve private domain names.

Step 6 Restart Prometheus.

Step 7 You can [use Grafana to query metric data in AOM](#) to check whether data is successfully reported after the preceding configuration is modified.

----End

3.8.3.3 Viewing Metric Data in AOM Using Grafana

Prerequisites

- You have created an ECS.
- An EIP has been created and bound to the ECS.


Procedure

Step 1 Install and start Grafana. For details, see the [Grafana official documentation](#).

Step 2 Add an access code.

1. Log in to the AOM console and choose **Monitoring Center** in the menu bar.
2. In the navigation pane on the left, choose **Global Configuration**.
3. In the right pane, click **Add Access Code**.
4. In the dialog box that is displayed, click **OK**. The system automatically generates an access code.

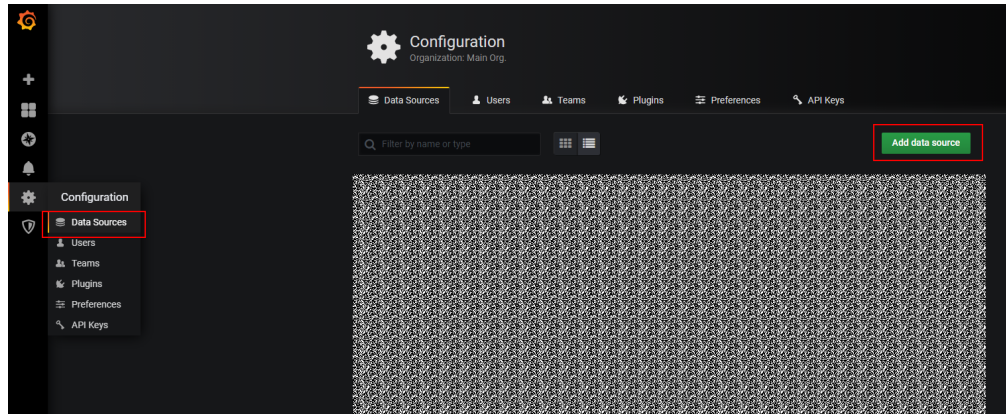
NOTE

- You can create up to two access codes for each project.
 - An access code is an identity credential for calling APIs. Keep your access code secure.
5. After the access code is added, click  to view it. To delete the access code, click **Delete** in the **Operation** column. Deleted access codes cannot be recovered. Exercise caution when performing this operation.

Step 3 Configure Grafana.

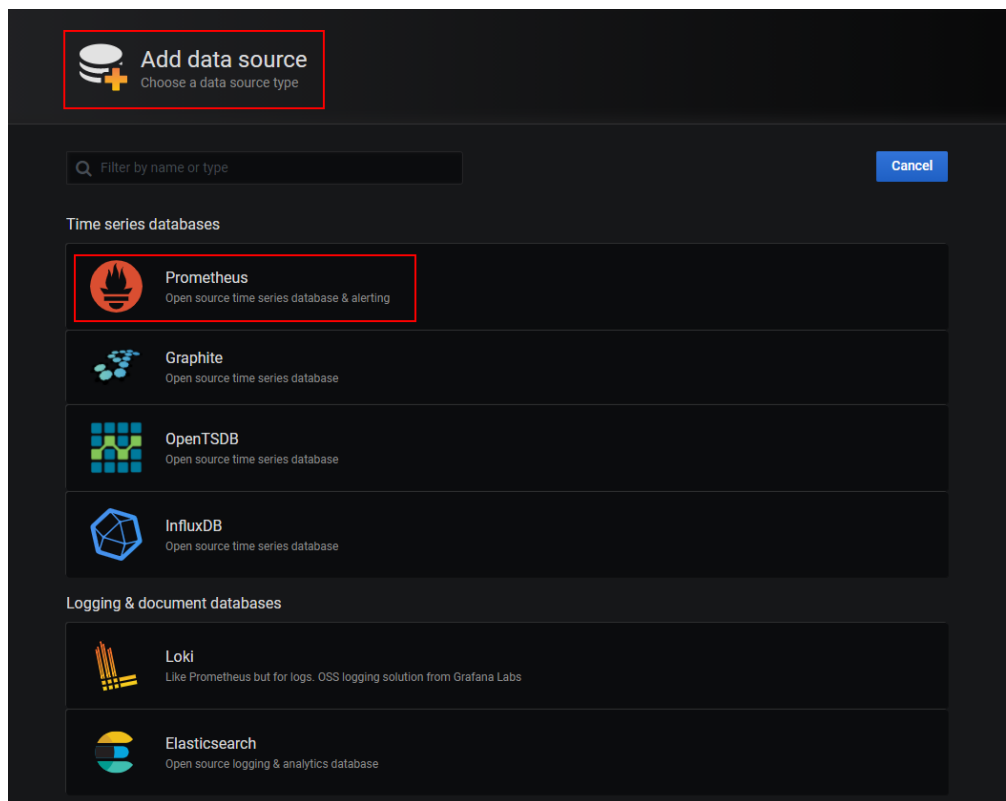
1. Log in to Grafana.
2. In the navigation pane, choose **Configuration > Data Sources**. Then, click **Add data source**.

Figure 3-6 Configuring Grafana



3. Click **Prometheus** to access the configuration page.

Figure 3-7 Entering the Prometheus configuration page



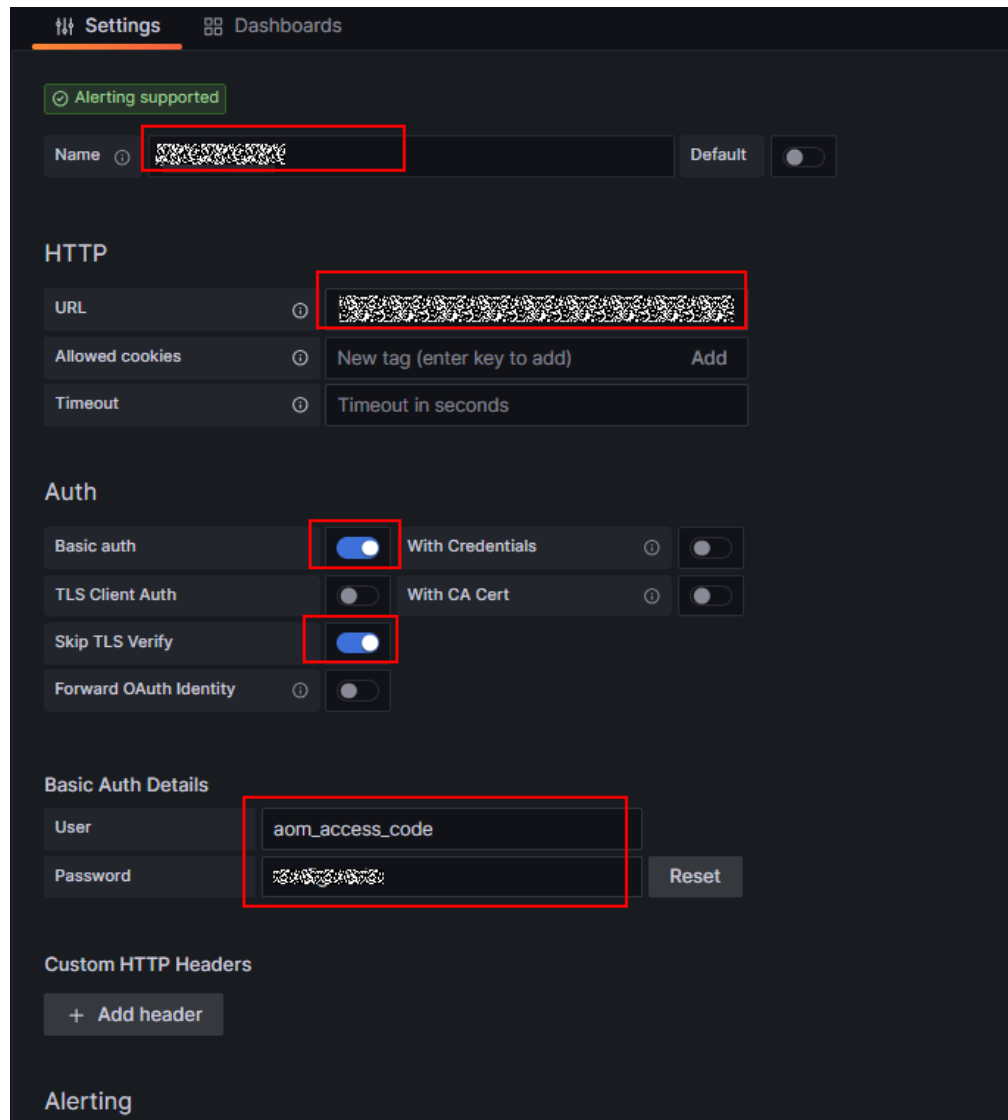
4. Set parameters according to the following figure.
 - **Password:** access code generated in [Step 2](#)
 - **User:** aom_access_code
 - **URL:** `{URI-scheme}://{Endpoint}/v1/{project_id}/{prometheus_instance}/aom`

- **URI-scheme:** protocol used to transmit requests. Currently, all APIs use HTTPS.
- **Endpoint:** Domain name or IP address of the server where the REST service is deployed. The endpoint varies depending on services and regions.
- **project_id:** project ID.
- **prometheus_instance:** Prometheus instance ID. This parameter is optional. To obtain the value, go to the **Prometheus Monitoring** page, click an instance name, and obtain the instance ID from the URL in **Prometheus Configuration Code** on the instance details page. By default, the Prometheus configuration code does not contain the Prometheus instance ID.

 **NOTE**

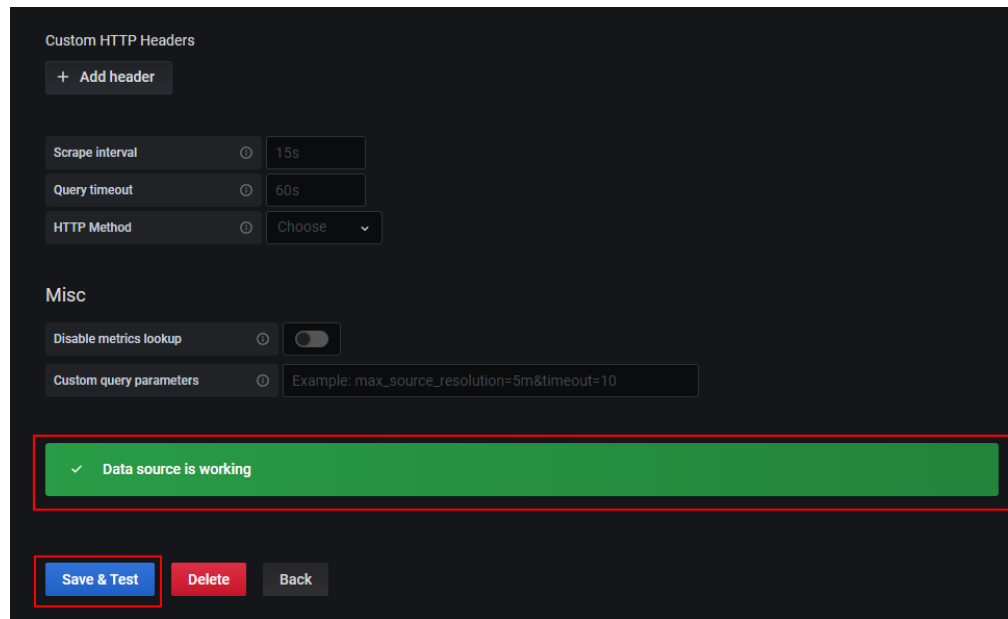
- The **Basic auth** and **Skip TLS Verify** options under **Auth** must be enabled.
- Access codes correspond to project IDs. Confirm their mapping when entering information.

Figure 3-8 Setting parameters



5. Click **Save&Test** to check whether the configuration is successful. If the configuration is successful, you can use Grafana to configure dashboards and view metric data.

Figure 3-9 Checking whether the configuration is successful



----End

3.9 Collection Management

3.9.1 Installing an ICAgent

The following table describes the ICAgent status.

Table 3-47 ICAgent status

Status	Description
Running	The ICAgent is running properly.
Uninstalled	The ICAgent is not installed. For details about how to install the ICAgent, see Installing an ICAgent .
Installing	The ICAgent is being installed. This operation takes about 1 minute to complete.
Installation failed	Failed to install the ICAgent. Uninstall the ICAgent according to Uninstalling the ICAgent Through Logging In to the Server and then install it again.
Upgrading	The ICAgent is being upgraded. This operation takes about 1 minute to complete.
Upgrade failed	Failed to upgrade the ICAgent. Uninstall the ICAgent according to Uninstalling the ICAgent Through Logging In to the Server and then install it again.

Status	Description
Offline	The Access Key ID/Secret Access Key (AK/SK) are incorrect. Obtain the correct AK/SK and install the ICAgent again.
Abnormal	The ICAgent is abnormal. Contact technical support.
Restricted	The AOM license is restricted. Check the license and update it in a timely manner.

Prerequisites

Before installing the ICAgent, ensure that the time and time zone of the local browser are consistent with those of the server. If multiple servers are deployed, ensure that the local browser and multiple servers use the same time zone and time. Otherwise, metric data of applications and servers displayed on the console may be inaccurate.

Installation Methods

There are two methods to install the ICAgent.

For details, see [Table 3-48](#).

Table 3-48 Installation methods

Method	Application Scenario
Initial installation	This method is used when the following conditions are met: 1. An elastic IP address (EIP) has been bound to the server. 2. The ICAgent has never been installed on the server.
Inherited installation	This method is used when the following conditions are met: You have multiple servers on which the ICAgent is to be installed. One server is bound to an EIP, but others are not bound to an EIP. You have installed the ICAgent on the server bound with an EIP. For the servers that are not bound with an EIP, perform inherited installation.

Initial Installation

After you apply for a server and install the ICAgent for the first time, perform the following operations:

- Step 1** Obtain and use the AK/SK of a public account. Do not use the AK/SK of a personal account.

NOTICE

Ensure that the public account and AK/SK will not be deleted or disabled. If the AK/SK is deleted, the ICAgent cannot report data to AOM or LTS.

- If you have obtained the AK/SK, skip this step.
- If you do not have an AK/SK, **obtain them** first.

Step 2 On the menu bar, choose **Collection Management**. The **Agent Management** page is displayed.

Step 3 Select **Other: custom hosts** from the drop-down list on the right of the page and click **Install ICAgent**.

Step 4 Click **Copy Command**.

Step 5 Use a remote login tool, such as PuTTY, to log in as user **root** to the server where the ICAgent is to be installed, and run the following command to disable history recording before ICAgent installation:

set +o history

Step 6 Run the installation command copied in **Step 4** and enter the obtained AK/SK obtained in **Step 1** as prompted.

Step 7 After the ICAgent is installed, run the following command to enable historical record collection:

set -o history

----End

 **NOTE**

- If the message "ICAgent install success." is displayed, the ICAgent is successfully installed in the **/opt/oss/servicemgr/** directory. After the ICAgent is successfully installed, choose **Other: custom hosts** on the **Agent Management** page to view the ICAgent status of the ECS.
- If the ICAgent fails to be installed, uninstall it according to **Uninstalling the ICAgent Through Logging In to the Server** and then install it again. If the problem persists, contact technical support.

Inherited Installation

If the ICAgent has been installed on a server and the **ICProbeAgent.tar.gz** installation package exists in the **/opt/ICAgent/** directory of this server, use this method to install the ICAgent on a remote server with a few clicks.

NOTICE

After the ICAgent is upgraded, the **/opt/ICAgent/** directory and the files stored in it will be deleted. Therefore, reinstall the ICAgent and then perform inherited installation.

Step 1 Run the following command (*x.x.x.x* indicates the server IP address) on the server where the ICAgent has been installed:

```
bash /opt/oss/servicemgr/ICAgent/bin/remotelInstall/remote_install.sh -ip  
x.x.x.x
```

Step 2 Enter the password of the **root** user of the server where the ICAgent is to be installed as prompted.

 **NOTE**

- If both the Expect tool and the ICAgent have been installed on the server, the ICAgent will be installed on the remote server after the preceding command is executed. If the ICAgent has been installed on the server, but the Expect tool has not, enter the information as prompted.
- Ensure that the **root** user can run the **SSH** or **SCP** command on the server where the ICAgent has been installed to remotely communicate with the server where the ICAgent is to be installed.
- Ensure that the **ICProbeAgent.tar.gz** installation package is transmitted to the server to be installed.
- If the message **ICAgent install success** is displayed, the ICAgent is successfully installed in the **/opt/oss/servicemgr/** directory. After the ICAgent is successfully installed, choose **Other: custom hosts** on the **Agent Management** page to view the ICAgent status of the ECS.
- If the ICAgent fails to be installed, uninstall it according to [Uninstalling the ICAgent Through Logging In to the Server](#) and then install it again. If the problem persists, contact technical support.

----End

Inherited Batch Installation

If the ICAgent has been installed on a server and the **ICProbeAgent.zip** installation package exists in the **/opt/ICAgent/** directory of this server, use this method to install the ICAgent on multiple remote servers in batches with a few clicks.

NOTICE

1. Ensure that you can run the **SSH** and **SCP** commands on the ECS where the ICAgent has been installed to communicate with the remote ECSs where the ICAgent is to be installed.
2. If you have installed the ICAgent in a server through an agency, you also need to set an agency for other servers where the ICAgent is to be installed.
3. Batch installation scripts depend on Python versions. You are advised to implement batch installation on hosts running Python 2.x. Python 3.x does not support batch installation.
4. You need to press **Enter** at the end of each line in the **iplist.cfg** file.
5. After the ICAgent is upgraded, the **/opt/ICAgent/** directory and the files stored in it will be deleted. Therefore, reinstall the ICAgent and then perform inherited batch installation.

Prerequisites

The IP addresses and passwords of all servers for which the ICAgent is to be installed have been collected, sorted in the **iplist.cfg** file, and uploaded to the **/opt/ICAgent/** directory on the server where the ICAgent has been installed. The following is an example of the **iplist.cfg** file, where IP addresses and passwords are separated by spaces.

192.168.0.109 password (Set the password as required.)

192.168.0.39 password (Set the password as required.)

NOTE

- Because the **iplist.cfg** file contains sensitive information, you are advised to clear the information after use.
- If the passwords of all servers are the same, only list IP addresses in the **iplist.cfg** file and enter the password once during execution. If the password of an IP address is different from those of the other ones, list both passwords and IP addresses in the **iplist.cfg** file.
- The batch installation function depends on Python 2.7.*. If the system displays a message indicating that Python cannot be found during the installation, install Python 2.7.* and try again.

Procedure

Step 1 Run the following command on the server where the ICAgent has been installed:

```
bash /opt/oss/servicemgr/ICAgent/bin/remoteInstall/remote_install.sh -  
batchModeConfig /opt/ICAgent/iplist.cfg
```

Enter the default password of the **root** user as prompted. If the passwords of all IP addresses have been configured in the **iplist.cfg** file, press **Enter** to skip this step. Otherwise, enter the default password.

```
batch install begin  
start to install python pexpect module  
use local pyexpect package  
Please input default passwd:  
send cmd to 192.168.0.109  
send cmd to 192.168.0.39  
2 tasks running, please wait...  
2 tasks running, please wait...  
2 tasks running, please wait...  
End of install agent: 192.168.0.39  
End of install agent: 192.168.0.109  
All hosts install icagent finish.
```

Wait for a while. When the message "All hosts install icagent finish." is displayed, the ICAgent is successfully installed on all the hosts listed in the configuration file.

Step 2 After the ICAgent is successfully installed, choose **Other: custom hosts** on the **Agent Management** page to view the ICAgent status of the ECS.

----End

3.9.2 Upgrading the ICAgent

To ensure better collection experience, AOM will continuously upgrade ICAgent versions. When the system displays a message indicating that a new ICAgent version is available, perform the following operations:

 **NOTE**

If the ICAgent has a critical bug, the system will upgrade the ICAgent version.

- Step 1** On the menu bar, choose **Collection Management**. The **Agent Management** page is displayed.
- Step 2** Select **Cluster: XXX** or **Other: custom hosts** from the drop-down list on the right of the page.
- Step 3** Upgrade the ICAgent. If you select **Cluster: xxx** in **Step 2**, directly click **Upgrade ICAgent**. In this way, the ICAgent on all hosts in the cluster can be upgraded at a time. If you select **Other: custom hosts** in **Step 2**, select a desired host and then click **Upgrade ICAgent**.
- Step 4** Wait for about 1 minute to complete the upgrade. When the ICAgent status changes from **Updating** to **Running**, the ICAgent is successfully upgraded.

 **NOTE**

If the upgrade fails, log in to the node and run the installation command to reinstall the ICAgent. The overwrite installation is supported. Therefore, you can reinstall the ICAgent without uninstallation.

----End

3.9.3 Uninstalling the ICAgent

If the ICAgent on a server is uninstalled, server O&M will be affected, making Application Operations Management (AOM) functions unavailable. Exercise caution when performing this operation.

You can uninstall the ICAgent using either of the following methods:

- **Uninstalling the ICAgent Through the AOM Console:** Applies to the scenario where the ICAgent has been successfully installed and needs to be uninstalled.
- **Uninstalling the ICAgent Through Logging In to the Server:** Applies to the scenario where the ICAgent fails to be installed and needs to be uninstalled for reinstallation.
- **Remotely Uninstalling the ICAgent:** Applies to the scenario where the ICAgent has been successfully installed and needs to be remotely uninstalled.
- **Uninstalling the ICAgent in Batches:** Applies to the scenario where the ICAgent has been successfully installed and needs to be uninstalled in batches.

Uninstalling the ICAgent Through the AOM Console

- Step 1** On the menu bar, choose **Collection Management**. The **Agent Management** page is displayed.
- Step 2** Select **Other: custom hosts** from the drop-down list on the right of the page.
- Step 3** Select one or more servers where the ICAgent is to be uninstalled, and click **Uninstall ICAgent**. In the **Uninstall ICAgent** dialog box, click **Yes**.

The ICAgent begins to be uninstalled. This operation takes about 1 minute to complete. If the involved server is removed from the node list, the ICAgent is successfully uninstalled.

----End

Uninstalling the ICAgent Through Logging In to the Server

Step 1 Log in to the server where the ICAgent is to be uninstalled as the **root** user.

Step 2 Run the following command to uninstall the ICAgent:

```
bash /opt/oss/servicemgr/ICAgent/bin/manual/uninstall.sh;
```

If the message **ICAgent uninstall success.** is displayed, the ICAgent is successfully uninstalled.

Wait for five minutes. On the **Agent Management** page, choose **Other: custom hosts**. The target host is removed from the displayed list.

----End

Remotely Uninstalling the ICAgent

Step 1 Run the following command (*x.x.x.x* indicates the server IP address) on the server where the ICAgent has been installed:

```
bash /opt/oss/servicemgr/ICAgent/bin/remoteUninstall/remote_uninstall.sh -  
ip x.x.x.x
```

Step 2 Enter the password of the **root** user of the server where the ICAgent is to be uninstalled as prompted.

NOTE

- If both the Expect tool and the ICAgent have been installed on the server, the ICAgent will be uninstalled from the remote server after the preceding command is executed. If the ICAgent has been installed on the server, but the Expect tool has not, enter the information as prompted.
- Ensure that the **root** user can run the **SSH** or **SCP** command on the server where the ICAgent has been installed to remotely communicate with the server where the ICAgent is to be uninstalled.
- If the message **ICAgent uninstall success** is displayed, the ICAgent is successfully uninstalled. After the ICAgent is successfully uninstalled, choose **Other: custom hosts** on the **Agent Management** page to view the ICAgent status of the ECS.

----End

Uninstalling the ICAgent in Batches

If the ICAgent has been installed on a server and the **ICProbeAgent.zip** installation package exists in the **/opt/ICAgent/** directory of this server, use this method to uninstall the ICAgent from multiple remote servers in batches with a few clicks.

NOTICE

The servers must belong to the same Virtual Private Cloud (VPC) and network segment.

Prerequisites

The IP addresses and passwords of all servers from which the ICAgent is to be uninstalled have been collected, sorted in the **iplist.cfg** file, and uploaded to the **/opt/ICAgent/** directory on the server where the ICAgent has been installed. The following is an example of the **iplist.cfg** file, where IP addresses and passwords are separated by spaces.

192.168.0.109 password (Set the password as required.)

192.168.0.39 password (Set the password as required.)

 **NOTE**

- Because the **iplist.cfg** file contains sensitive information, you are advised to clear the information after use.
- If the passwords of all servers are the same, only list IP addresses in the **iplist.cfg** file and enter the password once during execution. If the password of an IP address is different from those of the other ones, list both passwords and IP addresses in the **iplist.cfg** file.
- You need to press **Enter** at the end of each line in the **iplist.cfg** file.

Procedure

Step 1 Run the following command on the server where the ICAgent has been installed:

```
bash /opt/oss/servicemgr/ICAgent/bin/remoteUninstall/remote_uninstall.sh -  
batchModeConfig /opt/ICAgent/iplist.cfg
```

Enter the default password of the **root** user as prompted. If the passwords of all IP addresses have been configured in the **iplist.cfg** file, press **Enter** to skip this step. Otherwise, enter the default password.

```
batch uninstall begin  
Please input default passwd:  
send cmd to 192.168.0.109  
send cmd to 192.168.0.39  
2 tasks running, please wait...  
End of uninstall agent: 192.168.0.109  
End of uninstall agent: 192.168.0.39  
All hosts uninstall icagent finish.
```

Wait until the message **All hosts uninstall icagent finish.** is displayed, which indicates that the ICAgent is successfully uninstalled from all the hosts listed in the configuration file.

Step 2 After the ICAgent is successfully uninstalled, choose **Other: custom hosts** on the **Agent Management** page to view the ICAgent status of the ECS.

----End

3.10 Permissions Management

3.10.1 Creating a User and Granting Permissions

This chapter describes how to use Identity and Access Management (IAM) for fine-grained permissions control for your Application Operations Management (AOM) resources. With IAM, you can:

- Create IAM users for personnel based on your enterprise's organizational structure. Each IAM user has their own identity credentials for accessing AOM resources.
- Grant only the permissions required for users to perform a task.
- Entrust an account or a cloud service to perform efficient O&M on your AOM resources.

If your account meets your permissions requirements, you can skip this section.

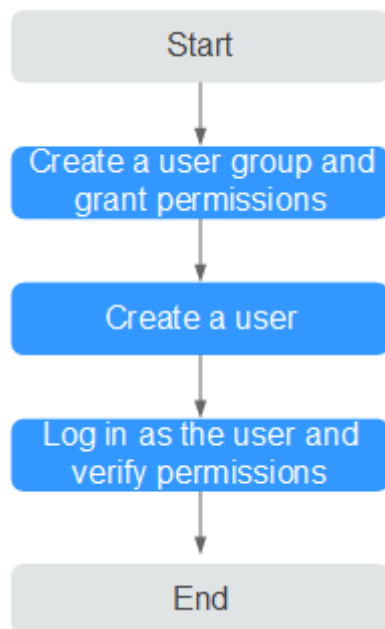
This section describes the procedure for granting permissions (see [Figure 3-10](#)).

Prerequisites

Learn about the permissions (see section "Permissions Management" in *AOM Service Overview*) supported by AOM and choose policies or roles according to your requirements. For the permissions of other services, see section "Permission Description" in the help center.

Process

Figure 3-10 Process for granting AOM permissions



1. Create a user group and assign permissions.
Create a user group on the IAM console, and assign the **AOM ReadOnlyAccess** policy to the group.
2. Create an IAM user.
Create a user on the IAM console and add the user to the group created in **1**.

3. Log in and verify permissions.
Log in to the AOM console as the created user, and verify that it only has read permissions for AOM.

3.10.2 Creating a Custom Policy

Custom policies can be created as a supplement to the system policies of AOM.

You can create custom policies in either of the following two ways:

- Visual editor: Select cloud services, actions, resources, and request conditions. This does not require knowledge of policy syntax.
- JSON: Edit JSON policies from scratch or based on an existing policy.

For example custom policies, see the following description.

Example Custom Policies

- Example 1: Allowing a user to create threshold rules

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "aom:alarmRule:create"
      ]
    }
  ]
}
```

- Example 2: Forbidding a user to delete application discovery rules

A deny policy must be used in conjunction with other policies to take effect. If the permissions assigned to a user contain both Allow and Deny actions, the Deny actions take precedence over the Allow actions.

To grant a user the **AOM FullAccess** system policy but forbid the user to delete application discovery rules, create a custom policy that denies the deletion of application discovery rules, and grant both the **AOM FullAccess** and deny policies to the user. Because the Deny action takes precedence, the user can perform all operations except deleting application discovery rules. The following is an example deny policy:

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "aom:discoveryRule:delete"
      ]
    }
  ]
}
```

- Example 3: Defining permissions for multiple services in a policy

A custom policy can contain actions of multiple services that are all of the project-level type. The following is an example policy containing actions of multiple services:

```
{
  "Version": "1.1",
  "Statement": [
```

```

{
  "Effect": "Allow",
  "Action": [
    "aom:*:list",
    "aom:*:get",
    "apm:*:list",
    "apm:*:get"
  ]
},
{
  "Effect": "Allow",
  "Action": [
    "cce:cluster:get",
    "cce:cluster:list",
    "cce:node:get",
    "cce:node:list"
  ]
}
]
}

```

3.11 Remarks

3.11.1 Prometheus Statements

AOM is interconnected with Prometheus Query Language (PromQL), which provides various built-in functions. These functions can be used to filter and aggregate metric data. You can run Prometheus statements to add metrics.

Prometheus Statement Syntax

For details about the Prometheus statement syntax, go to the [Prometheus official website](#).

Common Prometheus Commands

Table 3-49 lists the common Prometheus commands for querying metrics. You can modify parameters such as the IP address and ID based on site requirements.

Table 3-49 Common Prometheus commands

Metric	Tag Definition	PromQL
Host CPU usage	{nodeIP="", hostID=""}	aom_node_cpu_usage{nodeIP="192.168.57.93",hostID="ca76b63f-dbf8-4b60-9c71-7b9f13f5ad61"}
Host application request throughput	{aomApplicationID="",aomApplicationName=""}	http_requests_throughput{aomApplicationID="06dc9f3b0d8cb867453ecd273416ce2a",aomApplicationName="root"}

Metric	Tag Definition	PromQL
Success rate of host application requests	{appName="",serviceID="",clusterId=""}	http_requests_success_rate{aomApplicationID="06dc9f3b0d8cb867453ecd273416ce2a",aomApplicationName="root"}
Host component CPU usage	{appName="",serviceID="",clusterId=""}	aom_process_cpu_usage{appName="icagent",serviceID="2d29673a69cd82fabe345be5f0f7dc5f",clusterId="00000000-0000-0000-0000-00000000"}
Host process threads	{processCmd=""} {processID=""} {processName=""}	aom_process_thread_count{processCmd="cdb06c2c05b58d598e9430fa133aff7_b14ee84c-2b78-4f71-9ecc-2d06e053172c_ca4d29a846e9ad46a187ade88048825e",processName="icwatchdog"}

3.11.2 What Is the Relationship Between the Time Range and Statistical Period?

In AOM, a maximum of 1440 data points can be returned for a single metric query. The relationship between the time range and statistical period is as follows:

$$\text{Maximum time range} = \text{Statistical period} \times 1440$$

If you select a time range shorter than or equal to the maximum time range, all the statistical periods that meet the preceding formula can be selected. For example, if you want to query metrics in the last hour, the available statistical periods are 1 minute and 5 minutes.

For a [dashboard](#), the relationship between the time range and statistical period is shown in the following table.

Table 3-50 Relationship between the time range and statistical period

Time Range	Statistical Period
Last 30 minutes	1 minute or 5 minutes
Last hour	
Latest 6 hours	1 minute, 5 minutes, 15 minutes, or 1 hour
Last day	
Last week	1 hour
Custom	1 minute, 5 minutes, 15 minutes, or 1 hour

4 FAQs

4.1 What Can I Do If an ICAgent Is Offline?

After an ICAgent is installed, its status is offline.

Problem Analysis

- **Cause:** The AK/SK are incorrect or ports 30200 and 30201 are disconnected.
- **Impact:** The ICAgent cannot work.

Solution

Step 1 Log in to the server where the ICAgent is installed as the **root** user.

Step 2 Run the following command to check whether the AK/SK configuration is correct:
`cat /var/ICAgent/oss.icAgent.trace | grep proxyworkflow.go`

- If no command output is displayed, the AK/SK configuration is incorrect. Go to [Step 3](#).
- If a command output is displayed, the AK/SK configuration is correct. Go to [Step 4](#).

Step 3 After configuring the AK/SK, reinstall the ICAgent. For details, see [Installing an ICAgent](#). If the installation still fails, go to [Step 4](#).

Step 4 Check port connectivity.

1. Run the following command to obtain the access IP address:
`cat /opt/oss/servicemgr/ICAgent/envs/ICProbeAgent.properties | grep ACCESS_IP`
2. Run the following command to respectively check the connectivity of ports 30200 and 30201:
`curl -k https://ACCESS_IP:30200`
`curl -k https://ACCESS_IP:30201`
 - If **404** is displayed, the port is connected. In this case, contact technical support.

- If the command output is not **404**, the port is not connected. Contact the network administrator to open the port and reinstall ICAgent. If the installation still fails, contact technical support.

----End

4.2 How Do I Obtain an AK/SK?

NOTICE

- Obtain and use the AK/SK of a public account. Ensure that the public account and AK/SK will not be deleted or disabled.
 - Each account can create a maximum of two AK/SK pairs. They are permanently valid.
-
- AK: unique ID associated with the SK. It is used together with the SK to sign requests.
 - SK: secret access key used in conjunction with an AK to sign requests cryptographically. It identifies a request sender and prevents the request from being modified.

Procedure

1. Log in to the management console, hover the mouse pointer over the username in the upper right corner, and select **My Credentials** from the drop-down list.
2. On the **My Credentials** page, click the **Access Keys** tab.
3. Click **Add Access Key**, enter the key description, and click **OK**.
4. Click **Download**.

Obtain the AK and SK from the **credentials** file.

NOTE

Keep the AK/SK secure.

4.3 What Can I Do If Resources Are Not Running Properly?

Resource statuses include **Normal**, **Warning**, **Abnormal**, **Silent**, and **Deleted**. **Warning**, **Abnormal**, and **Silent** indicate improper resource running. Analyze and rectify faults according to the following instructions.

Warning

If a minor alarm or warning exists, the resource status is **Warning**.

Suggestion: Handle the alarm based on alarm details.

Abnormal

If a critical or major alarm exists, the resource status is **Abnormal**.

Suggestion: Handle the alarm based on alarm details.

Silent

If the ICAgent fails to collect resource metrics, the resource status is **Silent**. The causes include but are not limited to:

- **Cause 1: The ICAgent is abnormal.**

Suggestion: On the menu bar, choose **Collection Management**. The **Agent Management** page is displayed. Check the ICAgent status in the **ICAgent Status** column. If the status is not **Running**, the ICAgent is not installed or does not work. For details about how to rectify the fault, see [Table 4-1](#).

Table 4-1 ICAgent troubleshooting suggestions

Status	Suggestion
Uninstalled	Install the ICAgent according to Installing an ICAgent .
Installing	Wait for about 1 minute to complete the ICAgent installation.
Installation failed	Uninstall the ICAgent according to Uninstalling the ICAgent Through Logging In to the Server and then install it again.
Upgrading	Wait for about 1 minute to complete the ICAgent upgrade.
Upgrade failed	Uninstall the ICAgent according to Uninstalling the ICAgent Through Logging In to the Server and then install it again.
Offline	Ensure that the Access Key ID/Secret Access Key (AK/SK) or Elastic Cloud Server (ECS) agency configuration is correct.
Faulty	Contact technical support.

- **Cause 2: AOM cannot monitor the current resource.**

Suggestion: Check whether your resources can be monitored by AOM. AOM can monitor hosts, Kubernetes containers, and user processes, but does not monitor system processes.

- **Cause 3: The local time of the host is not synchronized with the NTP server time.**

 **NOTE**

NTP Sync Status: indicates whether the local time of the host is synchronized with the NTP server time. The value can be **0** or **1**. **0** indicates the synchronized status while **1** indicates the asynchronized status.

Suggestion: On the **Metric Browsing** page, check the **NTP Sync Status** metric of the host. If the value of **NTP Sync Status** is **1**, the local time of the host is

not synchronized with that of the NTP server. To solve the problem, perform synchronization.

- **Cause 4: The resource is deleted or stopped.**

Suggestions:

- On the ECS page, check whether the host is restarted, stopped, or deleted.
- If an application discovery rule is stopped or deleted, the component discovered based on the rule will also be stopped or deleted. On the AOM page, check whether the application discovery rule is stopped or deleted.

4.4 How Can I Do If I Do Not Have the Permission to Access SMN?

When you log in to AOM as an IAM user and try to create an alarm action rule, the message "Sorry, you do not have the permission to access Simple Message Notification (SMN)" is displayed.

Problem Analysis

- **Cause:** The IAM user does not have the permission to access Simple Message Notification (SMN).
- **Impact:** Email or message notifications cannot be received.

Solution

Contact the administrator (account to which the IAM user belongs) to add the SMN access permission. To add the permission, do as follows:

Log in to IAM as the administrator, and add the SMN access permission to the IAM user.

4.5 How Do I Distinguish Alarms from Events?

Similarities Between Alarms and Events

Both alarms and events are the information reported to AOM when the status of AOM or an external service (such as) changes.

Differences Between Alarms and Events

- Alarms are reported when AOM or an external service (such as) is abnormal or may cause exceptions. Alarms must be handled. Otherwise, service exceptions may occur.
- Events generally carry some important information. They are reported when AOM or an external service (such as) encounters some changes. Such changes do not necessarily cause service exceptions. Events do not need to be handled.

4.6 Does AOM Display Logs in Real Time?

The logs displayed on Application Operations Management (AOM) are near real-time logs, of which the latency is in seconds.

There is a time interval between log collection and processing. If the number of logs is small, the latency is about 10s. If the number of logs is large, the latency is much longer.

4.7 Why Is the Application Status Normal but the Component Status Abnormal?

On the application monitoring or details page, the application status is normal, but its component status is abnormal.

Possible Cause

An alarm associated with the component exists. Therefore, the component status is abnormal. However, the component alarm is not associated with the application. Therefore, the application status is still normal.

Suggestion

On the component list or details page, view the component status and associated alarms.

5 Best Practices

5.1 Discovering Applications

Application Discovery Overview

AOM can discover applications and collect their metrics based on configured rules. You can view the discovered applications on the **Application Monitoring** page and their metrics on the **O&M** page.

The relationship between applications and components is as follows:

- **Component:** the smallest unit for completing a task. It can be a microservice, container process, or common process.
- **Application:** a complete service module consisting of multiple components.

After application discovery is configured, you can use AOM to monitor application metrics and associate related alarms. Mainly, AOM can:

1. Provide association relationships between applications and components, between components and component instances, and between applications and hosts.
2. Enable you to search for associated components and logs.
3. Aggregate component metrics (so that you can obtain aggregated results of all component instances).

Procedure

- Step 1** On the menu bar, choose **Monitoring Center**.
- Step 2** In the navigation pane, choose **Configuration Management > Application Discovery**.
- Step 3** Click **Add Custom Application Discovery Rule** and configure an application discovery rule.
- Step 4** Select a host for pre-detection.
 1. Customize a rule name, for example, **ruletest**.

2. Select a typical host, for example, **host-test**, to check whether the application discovery rule is valid. The hosts that execute the rule will be configured in **Step 7**. Then, click **Next**.

Step 5 Set an application discovery rule.

1. Click **Add Check Items**. AOM can discover processes that meet the conditions of check items.

For example, AOM can detect the processes whose command parameters contain **ovs-vsitchd unix:** and environment variables contain **SUDO_USER=paas**.

 **NOTE**

- To precisely detect processes, you are advised to add check items about unique features of the processes.
 - You need to add one check item at least and can add five check items at most. If there are multiple check items, AOM only discovers the processes that meet the conditions of all check items.
2. After adding check items, click **Detect** to search for the processes that meet the conditions.
If no process is detected within 10s, modify the application discovery rule and detect processes again. Go to the next step only when at least one process is detected.

Step 6 Set a component name.

1. Set an application name.

In the **Application Name Settings** area, click **Add Naming Rule** to set an application name for the discovered process.

 **NOTE**

- If you do not set an application name, **unknownapplicationname** is used by default.
 - When you add multiple naming rules, all the naming rules are combined as the application name of the process. Metrics with the same application name are aggregated.
2. Set a component name.
In the **Component Name Settings** area, click **Add Naming Rule** to set a component name for the discovered process.

 **NOTE**

- The component name cannot be left blank.
 - When you add multiple naming rules, all the naming rules are combined as the component name of the process. Metrics with the same component name are aggregated.
3. Preview the component name.
If the application or component name does not meet your requirements, locate the name in the **Preview Component Name** table and rename it.

Step 7 Set a priority and detection range.

1. Set a priority: When there are multiple rules, set priorities. Enter 1 to 9999. The default value is **9999**. The smaller value, the higher priority. For example, **1** indicates the highest priority and **9999** indicates the lowest priority.

 **NOTE**

Do not use multiple custom discovery rules with the same priority for the same process.

2. Set a detection range: Select a host to be detected. That is, select the host to which the configured rule is applied. If no host is selected, this rule will be executed on all hosts, including those added later.

Step 8 Click **Add** to complete the configuration. AOM collects metrics of the process.

Step 9 Wait for about two minutes, choose **Infrastructure Monitoring > Component Monitoring** in the navigation pane, select the target host (for example, **host-test**) from the cluster drop-down list, and find the target component (for example, / **openswitch/**) that has been monitored.

Step 10 View the application status.

1. In the navigation pane, choose **Infrastructure Monitoring > Application Monitoring**.
2. Click an application to view its components and other resources.
3. Click the **Component List** tab and view the component information.
4. Click the **Host List** tab to view the host information.
5. Click the **Alarms** tab to view alarms.

----**End**

A Change History

Table A-1 Change history

Release On	Description
2024-04-15	This issue is the first official release.