



Application Operations Management

User Guide

Date 2024-07-15

Contents

1 Service Overview	1
1.1 What Is AOM?	1
1.2 Advantages	1
1.3 Application Scenarios	2
1.4 Comparison Between AOM 1.0 and AOM 2.0	3
1.5 Relationships Between AOM and Other Services	4
1.6 Restrictions	8
1.7 Metric Overview	10
1.7.1 Introduction	10
1.7.2 Basic Metrics: VM Metrics	11
1.7.3 Basic Metrics: Container Metrics	23
1.7.4 Metric Dimensions	57
1.8 Basic Concepts	60
1.8.1 Resource Monitoring	60
1.8.2 Collection Management	62
1.9 Permissions Management	62
1.10 Privacy Statement	74
2 Getting Started	75
2.1 Subscribing to AOM 2.0	75
2.2 Managing Containers	75
3 Introduction	84
4 Access Center	88
5 Dashboard	90
5.1 Creating a Dashboard	90
5.2 Setting the Full-Screen Online Duration	96
5.3 Adding Variables	97
5.4 Graph Description	99
6 Alarm Management	103
6.1 Alarm Rules	103
6.1.1 Overview	103
6.1.2 Creating a Metric Alarm Rule	103

6.1.3 Creating an Event Alarm Rule.....	112
6.1.4 Managing Alarm Rules.....	115
6.2 Alarm Templates.....	116
6.3 Viewing Alarms.....	123
6.4 Viewing Events.....	124
6.5 Alarm Action Rules.....	125
6.5.1 Overview.....	125
6.5.2 Creating an Alarm Action Rule.....	125
6.5.3 Creating a Message Template.....	127
6.6 Alarm Noise Reduction.....	130
6.6.1 Overview.....	130
6.6.2 Creating a Grouping Rule.....	132
6.6.3 Creating a Suppression Rule.....	136
6.6.4 Creating a Silence Rule.....	139
7 Metric Analysis.....	143
7.1 Metric Browsing.....	143
7.2 Prometheus Monitoring.....	145
7.2.1 Creating Prometheus Instances.....	145
7.2.1.1 Prometheus Instance for Cloud Services.....	145
7.2.1.2 Prometheus Instance for CCE.....	146
7.2.1.3 Prometheus Instance for Remote Write.....	147
7.2.1.4 Prometheus Instance for Multi-Account Aggregation.....	148
7.2.2 Managing Prometheus Instances.....	150
7.2.3 Configuring a Recording Rule.....	152
7.2.4 Configuring Service Discovery.....	154
7.2.4.1 Configuring Metrics.....	154
7.2.4.2 Configuring Service Discovery for CCE Clusters.....	156
7.2.5 Obtaining the Service Address of a Prometheus Instance.....	158
7.2.6 Reporting Prometheus Data to AOM.....	159
7.2.7 Viewing Metric Data in AOM Using Grafana.....	161
7.3 Resource Usage Statistics.....	165
8 Log Analysis (Beta).....	167
8.1 Searching for and Viewing Logs.....	167
8.1.1 Searching for Logs.....	167
8.1.2 Quickly Analyzing Logs.....	171
8.1.3 Quickly Querying Logs.....	174
8.1.4 Viewing the Context.....	175
9 Container Insights.....	176
9.1 Workload Monitoring.....	176
9.2 Cluster Monitoring.....	177
10 Infrastructure Monitoring.....	181

10.1 Host Monitoring.....	181
11 Process Monitoring.....	184
11.1 Application Monitoring.....	184
11.2 Component Monitoring.....	185
11.3 Application Discovery.....	187
12 Collection Management.....	192
12.1 UniAgent Management.....	192
12.1.1 VM Access.....	192
12.1.1.1 Installing a UniAgent.....	192
12.1.1.2 Operating UniAgents in Batches.....	197
12.1.1.3 Operating ICAgents in Batches.....	198
12.1.1.4 Other Operations.....	200
12.1.2 CCE Access.....	201
12.1.3 Proxy Area Management.....	202
12.1.3.1 Proxy Area.....	202
12.1.3.2 Proxy.....	203
12.1.4 Historical Tasks.....	204
13 Configuration Management.....	207
13.1 Global Settings.....	207
13.1.1 Cloud Service Authorization.....	207
13.1.2 Access Management.....	207
13.1.3 Global Settings.....	208
14 Remarks.....	210
14.1 Alarm Tags and Annotations.....	210
14.2 Prometheus Statements.....	211
14.3 What Is the Relationship Between the Time Range and Statistical Period?.....	215
15 Permissions Management.....	217
15.1 Creating a User and Granting Permissions.....	217
15.2 Creating a Custom Policy.....	218
16 Auditing.....	220
16.1 Operations Logged by CTS.....	220
16.2 Querying Real-Time Traces.....	224
17 Upgrading to AOM 2.0.....	228
18 FAQs.....	230
18.1 Overview.....	230
18.2 Dashboard.....	230
18.2.1 Can I Import Grafana Views to AOM Dashboards?.....	230
18.3 Alarm Management.....	231
18.3.1 How Do I Distinguish Alarms from Events?.....	231

18.4 Log Analysis.....	231
18.4.1 Does AOM Display Logs in Real Time?.....	231
18.4.2 How Do I Check Which Application Generates Logs in AOM?.....	231
18.5 Prometheus Monitoring.....	232
18.5.1 How Do I Connect Prometheus Data to AOM?.....	232
18.5.2 How Do I Distinguish Basic Metrics from Custom Metrics When Using Prometheus Monitoring?.....	232
18.6 Container Insights.....	233
18.6.1 Why Can't AOM Detect Workloads After the Pod YAML File Is Deployed Using Helm?.....	233
18.7 Application Monitoring.....	234
18.7.1 What Are the Differences Between Application Monitoring Under Application Insights and that Under Process Monitoring?.....	234
18.8 Collection Management.....	234
18.8.1 Are ICAgent and UniAgent the Same?.....	234
18.8.2 What Can I Do If an ICAgent Is Offline?.....	235
18.8.3 Why Is an Installed ICAgent Displayed as "Abnormal" on the Agent Management Page?.....	236
18.8.4 Why Can't I View the ICAgent Status After It Is Installed?.....	236
18.8.5 Why Can't AOM Monitor CPU and Memory Usage After ICAgent Is Installed?.....	238
18.8.6 How Do I Obtain an AK/SK?.....	239
18.8.7 FAQs About ICAgent Installation.....	239
18.9 Other FAQs.....	240
18.9.1 Comparison Between AOM 1.0 and AOM 2.0.....	240
18.9.2 What Are the Differences Between AOM and APM?.....	240
18.9.3 What Are the Differences Between the Log Functions of AOM and LTS?.....	241
18.9.4 How Do I Create the apm_admin_trust Agency?.....	241
19 Change History.....	242

1 Service Overview

1.1 What Is AOM?

Application Operations Management (AOM) is a one-stop, multi-dimensional O&M management platform for cloud applications. It integrates observable data sources, such as Cloud Eye, Log Tank Service (LTS), Application Performance Management (APM), real user experience, and backend link data. It also provides one-stop observability analysis solutions. With AOM, you can detect faults in a timely manner, monitor applications, resources, and services in real time, and improve automated O&M capability and efficiency.

- **Hosting & Running**
AOM seamlessly interconnects with multiple upper-layer O&M services. It can quickly collect metric data from services such as ServiceStage, FunctionGraph, and Cloud Service Engine (CSE), and display them in real time.
- **Observability Analysis**
Provides observable analysis capabilities such as exception detection, historical data analysis, performance analysis, correlation analysis, and scenario-based analysis through container/Prometheus monitoring based on multi-scenario, -layer, and -dimensional metric data.
- **Collection Management**
Manages plug-ins centrally and issue instructions for operation such as script delivery and execution.
- **Openness**
Supports reporting of native Prometheus Query Language (PromQL) data, data reporting through APIs, data viewing through Grafana, and data dumping through Kafka.

1.2 Advantages

- **Compatibility and openness**
AOM supports various open-source protocols, opens O&M data query APIs and collection standards, and provides fully hosted, O&M-free, and cost-efficient cloud native monitoring capabilities.

- **Ready-to-use**
You can connect applications to AOM without changing code. Data can be collected in a non-intrusive way.
- **Abundant data sources**
AOM integrates multiple types of data (such as cloud monitoring, logs, real user experience, and backend connections) for observability analysis.
- **Full-stack integrated monitoring**
AOM monitors data of clients, servers, and cloud products. It supports data discovery and display, and reports alarms when there are exceptions. It implements integrated monitoring from top to bottom and from the frontend to the backend.
- **Association analysis**
AOM automatically associates applications and resources and displays data in a panorama view. AOM allows you to easily locate faults through drill-down analysis of metrics, logs, and alarms about applications, components, instances, hosts, and transactions.
- **Precise alarm reporting**
AOM has a unified alarm system, covering metric and event alarms. It provides alarm noise reduction policies, such as grouping, suppression, and silence. It also supports alarm notification and subscription, so that you can easily cope with alarm storms and detect and clear alarms.
- **Unified visualization**
Multiple data sources can be monitored and analyzed in the same dashboard. They are displayed in various graphs (such as line and digit graphs), helping you better monitor resources, learn about trends, and make decisions.

1.3 Application Scenarios

Maintaining Containers

Pain Points

Prometheus is ideal for monitoring containers. Since self-built Prometheus is costly for small- and medium-sized enterprises (SMEs) and insufficient for large enterprises, many are turning to hosted Prometheus.

Solutions

AOM fully interconnects with the open-source Prometheus ecosystem. With Kubernetes clusters connected to Prometheus, enterprises can monitor performance metrics of hosts and Kubernetes clusters through Grafana dashboards.

- Collect metrics through kube-prometheus-stack, self-built Kubernetes clusters, ServiceMonitor, and PodMonitor to monitor service data deployed in CCE clusters.
- Various alarm templates help you quickly detect and locate faults.

1.4 Comparison Between AOM 1.0 and AOM 2.0

Based on AOM 1.0 functions and common application monitoring, AOM 2.0 collects and monitors more metrics and logs, and displays monitoring results in a visualized manner.

This section compares AOM 1.0 with AOM 2.0.

Table 1-1 Comparison between AOM 1.0 and AOM 2.0

Function		Description	AOM 1.0	AOM 2.0
Resource monitoring	Access center	Infrastructure metrics can be quickly connected for monitoring.	Not supported.	Supported.
	Dashboard	Resource metrics and performance data are displayed in multiple graphs on the same screen.	Supported.	Supported.
	Alarm management	You can set event conditions for services or set threshold criteria for resource metrics. When an alarm is generated due to an exception in AOM or a related service, the alarm information is sent to the specified personnel by email or SMS.	Partially supported. During alarm rule creation, metrics can be selected by metric type or running Prometheus commands, but cannot be selected from full metrics.	Supported.
	Container insights	AOM monitors CCE resource usage, status, and alarms from workload and cluster dimensions for fast response and smooth workload running.	Supported.	Supported.
	Metric browsing	You can monitor metric data and trends of each resource in real time and create alarm rules for metrics to view services and analyze associated data in real time.	Supported.	Supported.
	Infrastructure monitoring	The running status of hosts, and VM CPU, memory, and disk information can be monitored in real time.	Supported.	Supported.

Function		Description	AOM 1.0	AOM 2.0
	Prometheus monitoring	AOM is fully interconnected with the open-source Prometheus ecosystem, monitors various components, provides multiple preset monitoring dashboards for out-of-the-box availability, and flexibly expands cloud native component metric plug-ins.	Not supported.	Supported.
	Log analysis	You can quickly search for required logs from massive quantities of logs. You can also quickly locate faults by analyzing the log source and context.	Supported.	Supported.
	Process monitoring	Rules can be set to discover deployed applications and collect associated metrics. Drill-down (from applications to components, instances, and containers) is also supported. Applications and components can be monitored from multiple dimensions.	Supported.	Supported.
Collection management	UniAgent	You can use UniAgents to schedule collection tasks to collect data. Currently, UniAgents can be installed manually or automatically.	Not supported.	Supported.

As functions of AOM 1.0 are gradually replaced by those of AOM 2.0, AOM 1.0 will be brought offline soon. You are advised to upgrade AOM 1.0 to AOM 2.0. For details, see [Upgrading to AOM 2.0](#).

1.5 Relationships Between AOM and Other Services

AOM can work with Simple Message Notification (SMN), Distributed Message Service (DMS), and Cloud Trace Service (CTS). For example, when you subscribe to SMN, AOM can inform related personnel of alarm rule status changes by email or Short Message Service (SMS) message. When AOM interconnects with middleware services such as Virtual Private Cloud (VPC) and Elastic Load Balance (ELB), you can monitor them in AOM. When AOM interconnects with Cloud Container Engine (CCE) or Cloud Container Instance (CCI), you can monitor their basic resources and applications, and view related logs and alarms.

SMN

SMN can push notifications based on requirements, and you can receive notifications by SMS message, email, or app. You can also integrate application functions through SMN to reduce system complexity.

AOM uses the message transmission mechanism of SMN. When it is inconvenient for you to query threshold rule status changes on site, AOM sends such changes to you by email or SMS messages. In this way, you can obtain resource status and other information in real time and take necessary measures to avoid service loss.

OBS

Object Storage Service (OBS) is a secure, reliable, and cost-effective cloud storage service. With OBS, you can easily create, modify, and delete buckets, as well as upload, download, and delete objects.

AOM allows you to dump logs to OBS buckets for long-term storage.

LTS

Log Tank Service (LTS) can collect, analyze, and store log data. You can use LTS for efficient device O&M, service trend analysis, security audits, and monitoring.

AOM is a unified entry for observability analysis. It does not provide log functions, but integrates them from LTS.

CTS

CTS records operations on cloud resources in your account. Based on the records, you can perform security analysis, trace resource changes, conduct compliance audits, and locate faults. To store operation records for a longer time, you can subscribe to OBS and synchronize operation records to OBS in real time.

With CTS, you can record operations associated with AOM for future query, audit, and tracing.

IAM

Identity and Access Management (IAM) provides identity authentication, permission management, and access control.

IAM can implement authentication and fine-grained authorization for AOM.

Cloud Eye

Cloud Eye provides a multi-dimensional monitoring platform for resources such as Elastic Cloud Server (ECS) and bandwidth. With Cloud Eye, you can view the resource usage and service running status in the cloud, and respond to exceptions in a timely manner to ensure smooth running of services.

AOM calls Cloud Eye APIs to obtain monitoring data of cloud services and displays them on the console so that you can monitor these services centrally.

APM

Application Performance Management (APM) monitors and manages the performance of cloud applications in real time. APM provides performance analysis of distributed applications, helping O&M personnel quickly locate and resolve faults and performance bottlenecks.

AOM integrates APM functions to better monitor and manage applications.

VPC

VPC is a logically isolated virtual network. It is created for ECS servers, and supports custom configuration and management, improving resource security and simplifying network deployment.

ELB

ELB distributes access traffic to multiple backend ECS servers based on forwarding policies. By distributing traffic, ELB expands the capabilities of application systems to provide services externally. By preventing single points of failures, ELB improves the availability of application systems.

RDS

RDS is a cloud-based web service which is reliable, scalable, easy to manage, and ready to use out-of-the-box.

DCS

DCS is an online, distributed, in-memory cache service compatible with Redis, Memcached, and In-Memory Data Grid (IMDG). It is reliable, scalable, ready to use out-of-the-box, and easy to manage, meeting your requirements for high read/write performance and fast data access.

CCE

CCE is a high-performance and scalable container service through which enterprises can build reliable containerized applications. It integrates network and storage capabilities, and is compatible with Kubernetes and Docker container ecosystems. CCE enables you to create and manage diverse containerized workloads easily. It also provides efficient O&M capabilities, such as container fault self-healing, monitoring log collection, and auto scaling.

You can monitor basic resources, applications, logs, and alarms about CCE on the AOM console.

ServiceStage

ServiceStage is a one-stop PaaS service that provides cloud-based application hosting, simplifying application lifecycle management, from deployment, monitoring, O&M, to governance. It provides a microservice framework compatible with mainstream open-source ecosystems and enables quick building of distributed applications.

You can monitor basic resources, applications, logs, and alarms about ServiceStage on the AOM console.

FunctionGraph

FunctionGraph hosts and computes functions in a serverless context. It automatically scales up/down resources during peaks and spikes without requiring the reservation of dedicated servers or capacities. Resources are billed on a pay-per-use basis.

You can monitor basic resources, applications, logs, and alarms about FunctionGraph on the AOM console.

IEF

Intelligent EdgeFabric (IEF) provides you a complete edge computing solution, in which cloud applications are extended to the edge. By leveraging edge-cloud synergy, you can manage edge nodes and applications remotely and process data nearby, to meet your requirements for remote management, data processing, analysis, decision-making, and intelligence of edge computing resources. In addition, you can perform O&M in the cloud, including edge node monitoring, application monitoring, and log collection.

You can monitor resources (such as edge nodes, applications, and functions), logs, and alarms about IEF on the AOM console without installing other plug-ins.

ECS

An ECS is a computing server consisting of CPU, memory, image, and Elastic Volume Service (EVS) disk. It supports on-demand allocation and auto scaling. ECSs integrate VPC, virtual firewall, and multi-data-copy capabilities to create an efficient, reliable, and secure computing environment. This ensures stable and uninterrupted running of services. After creating an ECS server, you can use it like using your local computer or physical server.

When purchasing an ECS, ensure that its OS meets the requirements in [Table 1-3](#). In addition, install a UniAgent on the ECS. Otherwise, the ECS cannot be monitored by AOM. You can monitor basic resources, applications, logs, and alarms about this ECS on the AOM console.

BMS

A Bare Metal Server (BMS) is a dedicated physical server in the cloud. It provides high-performance computing and ensures data security for core databases, key application systems, and big data. With the advantage of scalable cloud resources, you can apply for BMS servers flexibly and they are billed on a pay-per-use basis.

When purchasing a BMS server, ensure that its OS meets the requirements in [Table 1-3](#). In addition, install a UniAgent on the server. Otherwise, the server cannot be monitored by AOM. You can monitor basic resources, applications, logs, and alarms about this server on the AOM console.

1.6 Restrictions

Resource Monitoring Restrictions

Table 1-2 Resource monitoring restrictions

Category	Object	Restriction
Dashboard	Dashboard	A maximum of 1000 dashboards can be created in a region.
	Graph	A maximum of 30 graphs can be added to a dashboard.
	Resources in a 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.
Metric	Metric data	<ul style="list-style-type: none"> Basic edition: Metric data can be stored for up to 7 days. Professional edition: Metric data can be stored for up to 30 days.
	Metric item	After resources (such as clusters, components, and hosts) are deleted, their metric items can still be stored for up to 30 days.
	Dimension	A maximum of 20 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.
	Data points returned for a single query	A maximum of 1440 data points can be returned each time.
	Custom metric	No restrictions.
	Custom metric 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.

Category	Object	Restriction
	Application metric Job metric	<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. <p>A job automatically exits after it is completed. To monitor metrics of a job, ensure that its survival time is greater than 90s so that the ICAgent can collect its metric data.</p>
	Resources consumed by the ICAgent	When the ICAgent collects basic metrics, the resources consumed by the ICAgent are related to 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 fewer than 1000 containers run on a single node.
Alarm rule	Alarm rule	A maximum of 1,000 alarm rules (including metric alarm rules and event alarm rules) can be created.
	Alarm template	A maximum of 150 alarm templates can be created.
Alarm list	Alarms	You can query alarms generated within 31 days in the last year.
	Events	You can query events generated within 31 days in the last year.
Application discovery	Application discovery rules	A maximum of 100 application discovery rules can be created.

Collection Management restrictions

- OS Restrictions

Table 1-3 OSs and versions supported

OS	Version				
Euler OS	1.1 64-bit	2.0 64-bit			
Cent OS	7.1 64-bit	7.2 64-bit	7.3 64-bit	7.4 64-bit	7.5 64-bit
	7.6 64-bit	7.7 64-bit	7.8 64-bit	7.9 64-bit	8.0 64-bit
Ubuntu	16.04 server 64-bit	18.04 server 64-bit	20.04 server 64-bit	22.04 server 64-bit	

 **NOTE**

- For Linux x86_64 hosts, all the OSs and versions listed in the preceding table are supported.
- For Linux Arm hosts, CentOS 7.4/7.5/7.6, EulerOS 2.0, and Ubuntu 18.04 are supported.
- Resource Restrictions

Table 1-4 Resource restrictions

Object	Restriction
Agent client	When the average CPU usage is greater than 50% or the memory is greater than 100 MB for two minutes, the Agent client automatically restarts.
Agent installation, upgrade, or uninstallation	You can install, upgrade, or uninstall Agents for a maximum of 100 hosts at a time.
Host deletion	You can delete a maximum of 50 hosts with Agents uninstalled at a time.

1.7 Metric Overview

1.7.1 Introduction

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

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 1-5](#).

Table 1-5 Namespaces of system metrics

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

Metric 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 details, see [1.7.4 Metric Dimensions](#).
- Dimensions of custom metrics must be 1 to 32 characters long, which need to be customized.

1.7.2 Basic Metrics: VM Metrics

This section describes the types, names, and meanings of VM metrics reported by ICAgents to AOM.

Table 1-6 VM metrics

Category	Metric	Metric Name	Description	Value Range	Unit
Network metrics	aom_node_network_receive_bytes	Downlink Rate (BPS)	Inbound traffic rate of a measured object	≥ 0	Bytes/s
	aom_node_network_receive_packets	Downlink Rate (PPS)	Number of data packets received by a NIC per second	≥ 0	Packets/s

Category	Metric	Metric Name	Description	Value Range	Unit
	aom_node_network_receive_error_packets	Downlink Error Rate	Number of error packets received by a NIC per second	≥ 0	Count/s
	aom_node_network_transmit_bytes	Uplink Rate (BPS)	Outbound traffic rate of a measured object	≥ 0	Bytes/s
	aom_node_network_transmit_error_packets	Uplink Error Rate	Number of error packets sent by a NIC per second	≥ 0	Count/s
	aom_node_network_transmit_packets	Uplink Rate (PPS)	Number of data packets sent by a NIC per second	≥ 0	Packets/s
	aom_node_network_total_bytes	Total Rate (BPS)	Total inbound and outbound traffic rate of a measured object	≥ 0	Bytes/s
Disk metrics	aom_node_disk_read_kilobytes	Disk Read Rate	Volume of data read from a disk per second	≥ 0	KB/s
	aom_node_disk_write_kilobytes	Disk Write Rate	Volume of data written into a disk per second	≥ 0	KB/s
Disk partition metrics	aom_host_diskpartition_thinpool_metadata_percent	Thin Pool's Metadata Space Usage	Percentage of the thin pool's used metadata space to the total metadata space on a CCE node	0-100	%
	aom_host_diskpartition_thinpool_data_percent	Thin Pool's Data Space Usage	Percentage of the thin pool's used data space to the total data space on a CCE node	0-100	%
	aom_host_diskpartition_total_capacity_megabytes	Thin Pool's Disk Partition Space	Total thin pool's disk partition space on a CCE node	≥ 0	MB

Category	Metric	Metric Name	Description	Value Range	Unit
File system metrics	aom_node_disk_available_capacity_megabytes	Available Disk Space	Disk space that has not been used	≥ 0	MB
	aom_node_disk_capacity_megabytes	Total Disk Space	Total disk space	≥ 0	MB
	aom_node_disk_rw_status	Disk Read/Write 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
	aom_node_disk_usage	Disk Usage	Percentage of the used disk space to the total disk space	0-100	%
Host metrics	aom_node_cpu_limit_core	Total CPU Cores	Total number of CPU cores that have been applied for a measured object	≥ 1	Cores
	aom_node_cpu_used_core	Used CPU Cores	Number of CPU cores used by a measured object	≥ 0	Cores
	aom_node_cpu_usage	CPU Usage	CPU usage of a measured object	0-100	%
	aom_node_memory_free_megabytes	Available Physical Memory	Available physical memory of a measured object	≥ 0	MB
	aom_node_virtual_memory_free_megabytes	Available Virtual Memory	Available virtual memory of a measured object	≥ 0	MB
	aom_node_gpu_memory_free_megabytes	GPU Memory Capacity	Total GPU memory of a measured object	> 0	MB
	aom_node_gpu_memory_usage	GPU Memory Usage	Percentage of the used GPU memory to the total GPU memory	0-100	%

Category	Metric	Metric Name	Description	Value Range	Unit
	aom_node_gpu_memory_used_megabytes	Used GPU Memory	GPU memory used by a measured object	≥ 0	MB
	aom_node_gpu_usage	GPU Usage	GPU usage of a measured object	0-100	%
	aom_node_npu_memory_free_megabytes	Total NPU Memory	Total NPU memory of a measured object	> 0	MB
	aom_node_npu_memory_usage	NPU Memory Usage	Percentage of the used NPU memory to the total NPU memory	0-100	%
	aom_node_npu_memory_used_megabytes	Used NPU Memory	NPU memory used by a measured object	≥ 0	MB
	aom_node_npu_usage	NPU Usage	NPU usage of a measured object	0-100	%
	aom_node_npu_temperature_centigrade	NPU Temperature	NPU temperature of a measured object	-	°C
	aom_node_memory_usage	Physical Memory Usage	Percentage of the used physical memory to the total physical memory applied for a measured object	0-100	%
	aom_node_status	Host Status	Host status	<ul style="list-style-type: none"> • 0: Normal • 1: Abnormal 	N/A

Category	Metric	Metric Name	Description	Value Range	Unit
	aom_node_ntp_offset_ms	NTP Offset	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
	aom_node_ntp_server_status	NTP Server Status	Whether the host is connected to the NTP server	0 or 1 <ul style="list-style-type: none"> • 0: Connected • 1: Not connected 	N/A
	aom_node_ntp_status	NTP Synchronization 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: Synchronous • 1: Asynchronous 	N/A
	aom_node_process_number	Processes	Number of processes on a measured object	≥ 0	N/A
	aom_node_gpu_temperature_centigrade	GPU Temperature	GPU temperature of a measured object	-	°C
	aom_node_memory_total_megabytes	Total Physical Memory	Total physical memory that has been applied for a measured object	≥ 0	MB
	aom_node_virtual_memory_total_megabytes	Virtual Memory Size	Total virtual memory of a measured object	≥ 0	MB

Cate gory	Metric	Metric Name	Description	Value Range	Unit
	aom_node_virtu al_memory_usa ge	Virtual Memory Usage	Percentage of the used virtual memory to the total virtual memory	0-100	%
	aom_node_curr ent_threads_nu m	Current Threads	Number of threads created on a host	≥ 0	N/A
	aom_node_sys_ max_threads_n um	Max Threads	Maximum number of threads that can be created on a host	≥ 0	N/A
	aom_node_phy _disk_total_cap acity_megabyte s	Total Physical Disk Space	Total disk space of a host	≥ 0	MB
	aom_node_phys ical_disk_total_ used_megabyte s	Used Physical Disk Space	Used disk space of a host	≥ 0	MB
	aom_billing_ho stUsed	Hosts	Number of hosts connected per day	≥ 0	N/A
Clust er metr ics	aom_cluster_cp u_limit_core	Total CPU Cores	Total number of CPU cores that have been applied for a measured object	≥ 1	Cores
	aom_cluster_cp u_used_core	Used CPU Cores	Number of CPU cores used by a measured object	≥ 0	Cores
	aom_cluster_cp u_usage	CPU Usage	CPU usage of a measured object	0-100	%
	aom_cluster_dis k_available_cap acity_megabyte s	Available Disk Space	Disk space that has not been used	≥ 0	MB
	aom_cluster_dis k_capacity_meg abytes	Total Disk Space	Total disk space	≥ 0	MB

Category	Metric	Metric Name	Description	Value Range	Unit
	aom_cluster_disk_usage	Disk Usage	Percentage of the used disk space to the total disk space	0-100	%
	aom_cluster_memory_free_megabytes	Available Physical Memory	Available physical memory of a measured object	≥ 0	MB
	aom_cluster_virtual_memory_free_megabytes	Available Virtual Memory	Available virtual memory of a measured object	≥ 0	MB
	aom_cluster_gpu_memory_free_megabytes	Available GPU Memory	Available GPU memory of a measured object	> 0	MB
	aom_cluster_gpu_memory_usage	GPU Memory Usage	Percentage of the used GPU memory to the total GPU memory	0-100	%
	aom_cluster_gpu_memory_used_megabytes	Used GPU Memory	GPU memory used by a measured object	≥ 0	MB
	aom_cluster_gpu_usage	GPU Usage	GPU usage of a measured object	0-100	%
	aom_cluster_memory_usage	Physical Memory Usage	Percentage of the used physical memory to the total physical memory applied for a measured object	0-100	%
	aom_cluster_network_receive_bytes	Downlink Rate (BPS)	Inbound traffic rate of a measured object	≥ 0	Bytes/s
	aom_cluster_network_transmit_bytes	Uplink Rate (BPS)	Outbound traffic rate of a measured object	≥ 0	Bytes/s
	aom_cluster_memory_total_megabytes	Total Physical Memory	Total physical memory that has been applied for a measured object	≥ 0	MB

Category	Metric	Metric Name	Description	Value Range	Unit
	aom_cluster_virtual_memory_total_megabytes	Virtual Memory Size	Total virtual memory of a measured object	≥ 0	MB
	aom_cluster_virtual_memory_usage	Virtual Memory Usage	Percentage of the used virtual memory to the total virtual memory	0-100	%
Container metrics	aom_container_cpu_limit_core	Total CPU Cores	Total number of CPU cores restricted for a measured object	≥ 1	Cores
	aom_container_cpu_used_core	Used CPU Cores	Number of CPU cores used by a measured object	≥ 0	Cores
	aom_container_cpu_usage	CPU Usage	CPU usage of a measured object Percentage of the used CPU cores to the total CPU cores restricted for a measured object	0-100	%
	aom_container_disk_read_kilobytes	Disk Read Rate	Volume of data read from a disk per second	≥ 0	KB/s
	aom_container_disk_write_kilobytes	Disk Write Rate	Volume of data written into a disk per second	≥ 0	KB/s
	aom_container_filesystem_available_capacity_megabytes	Available File System Capacity	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

Category	Metric	Metric Name	Description	Value Range	Unit
	aom_container_filesystem_capacity_megabytes	Total File System Capacity	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
	aom_container_filesystem_usage	File System 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	%
	aom_container_gpu_memory_free_megabytes	GPU Memory Capacity	Total GPU memory of a measured object	> 0	MB
	aom_container_gpu_memory_usage	GPU Memory Usage	Percentage of the used GPU memory to the total GPU memory	0-100	%
	aom_container_gpu_memory_used_megabytes	Used GPU Memory	GPU memory used by a measured object	≥ 0	MB
	aom_container_gpu_usage	GPU Usage	GPU usage of a measured object	0-100	%
	aom_container_npu_memory_free_megabytes	Total NPU Memory	Total NPU memory of a measured object	> 0	MB

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

Category	Metric	Metric Name	Description	Value Range	Unit
	aom_container_network_transmit_error_packets	Uplink Error Rate	Number of error packets sent by a NIC per second	≥ 0	Count/s
	aom_container_network_transmit_packets	Uplink Rate (PPS)	Number of data packets sent by a NIC per second	≥ 0	Packets/s
	aom_process_status	Status	Docker container status	0 or 1 <ul style="list-style-type: none"> • 0: Normal • 1: Abnormal 	N/A
	aom_container_memory_workingset_usage	Working Set Memory Usage	Usage of the working set memory	0–100	%
	aom_container_memory_workingset_used_megabytes	Used Working Set Memory	Working set memory that has been used	≥ 0	MB
Process metrics	aom_process_cpu_limit_core	Total CPU Cores	Total number of CPU cores that have been applied for a measured object	≥ 1	Cores
	aom_process_cpu_used_core	Used CPU Cores	Number of CPU cores used by a measured object	≥ 0	Cores
	aom_process_cpu_usage	CPU Usage	CPU usage of a measured object Percentage of the used CPU cores to the CPU cores that have been applied	0–100	%
	aom_process_handle_count	Handles	Number of handles used by a measured object	≥ 0	N/A

Category	Metric	Metric Name	Description	Value Range	Unit
	aom_process_max_handle_count	Max Handles	Maximum number of handles used by a measured object	≥ 0	N/A
	aom_process_memory_request_megabytes	Total Physical Memory	Total physical memory that has been applied for a measured object	≥ 0	MB
	aom_process_memory_usage	Physical Memory Usage	Percentage of the used physical memory to the total physical memory applied for a measured object	0-100	%
	aom_process_memory_used_megabytes	Used Physical Memory	Used physical memory of a measured object	≥ 0	MB
	aom_process_status	Status	Process status	0 or 1 <ul style="list-style-type: none"> • 0: Normal • 1: Abnormal 	N/A
	aom_process_thread_count	Threads	Number of threads used by a measured object	≥ 0	N/A
	aom_process_virtual_memory_total_megabytes	Virtual Memory Size	Total virtual memory that has been applied for a measured object	≥ 0	MB

 **NOTE**

- If the host type is **CCE**, you can view disk partition metrics. The supported OSs are CentOS 7.6 and EulerOS 2.5.
- Log in to the CCE node as the **root** user and run the **docker info | grep 'Storage Driver'** command to check the Docker storage driver type. If the command output shows driver type **Device Mapper**, the thin pool metrics can be viewed. Otherwise, the thin pool metrics cannot be viewed.
- 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)
Currently, the virtual memory of a newly created 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.
- Cluster metrics are aggregated by AOM based on host metrics, and do not include the metrics of master hosts.

1.7.3 Basic Metrics: Container Metrics

This section describes the types, names, and meanings of metrics reported to AOM from CCE's kube-prometheus-stack add-on or on-premises Kubernetes clusters.

Table 1-7 Metrics of containers running in CCE or on-premises Kubernetes clusters

Target Name	Job Name	Metric	Description
<ul style="list-style-type: none"> • serviceMonitor/monitoring/coredns/0 • serviceMonitor/monitoring/node-local-dns/0 	coredns and node-local-dns	coredns_build_info	Information to build CoreDNS
		coredns_cache_entries	Number of entries in the cache
		coredns_cache_size	Cache size
		coredns_cache_hits_total	Number of cache hits total
		coredns_cache_misses_total	Number of cache misses
		coredns_cache_requests_total	Total number of DNS resolution requests in different dimensions
		coredns_dns_request_duration_seconds_bucket	Histogram of DNS request duration (bucket)
		coredns_dns_request_duration_seconds_count	Histogram of DNS request duration (count)

Target Name	Job Name	Metric	Description
		coredns_dns_request_duration_seconds_sum	Histogram of DNS request duration (sum)
		coredns_dns_request_size_bytes_bucket	Histogram of the size of DNS request (bucket)
		coredns_dns_request_size_bytes_count	Histogram of the size of DNS request (count)
		coredns_dns_request_size_bytes_sum	Histogram of the size of DNS request (sum)
		coredns_dns_requests_total	Number of DNS requests
		coredns_dns_response_size_bytes_bucket	Histogram of the size of DNS response (bucket)
		coredns_dns_response_size_bytes_count	Histogram of the size of DNS response (count)
		coredns_dns_response_size_bytes_sum	Histogram of the size of DNS response (sum)
		coredns_dns_responses_total	DNS response codes and number of DNS response codes
		coredns_forward_conn_cache_hits_total	Number of cache hits for each protocol and data flow
		coredns_forward_conn_cache_misses_total	Number of cache misses for each protocol and data flow
		coredns_forward_healthcheck_broken_total	Unhealthy upstream count
		coredns_forward_healthcheck_failures_total	Count of failed health checks per upstream
		coredns_forward_max_concurrent_rejects_total	Number of requests rejected due to excessive concurrent requests

Target Name	Job Name	Metric	Description
		coredns_forward_request_duration_seconds_bucket	Histogram of forward request duration (bucket)
		coredns_forward_request_duration_seconds_count	Histogram of forward request duration (count)
		coredns_forward_request_duration_seconds_sum	Histogram of forward request duration (sum)
		coredns_forward_requests_total	Number of requests for each data flow
		coredns_forward_responses_total	Number of responses to each data flow
		coredns_health_request_duration_seconds_bucket	Histogram of health request duration (bucket)
		coredns_health_request_duration_seconds_count	Histogram of health request duration (count)
		coredns_health_request_duration_seconds_sum	Histogram of health request duration (sum)
		coredns_health_request_failures_total	Number of health request failures
		coredns_hosts_reload_timestamp_seconds	Timestamp of the last reload of the host file
		coredns_kubernetes_dns_programming_duration_seconds_bucket	Histogram of DNS programming duration (bucket)
		coredns_kubernetes_dns_programming_duration_seconds_count	Histogram of DNS programming duration (count)
		coredns_kubernetes_dns_programming_duration_seconds_sum	Histogram of DNS programming duration (sum)
		coredns_local_localhost_requests_total	Number of localhost requests
		coredns_nodocache_setup_errors_total	Number of nodocache setup errors

Target Name	Job Name	Metric	Description
		coredns_dns_response_rcode_count_total	Number of responses for each Zone and Rcode
		coredns_dns_request_count_total	Number of DNS requests
		coredns_dns_request_do_count_total	Number of requests with the DNSSEC OK (DO) bit set
		coredns_dns_do_requests_total	Number of requests with the DO bit set
		coredns_dns_request_type_count_total	Number of requests for each Zone and Type
		coredns_panics_total	Total number of panics
		coredns_plugin_enabled	Whether a plugin is enabled
		coredns_reload_failed_total	Number of last reload failures
serviceMonitor/monitoring/kube-apiserver/0	apiserver	aggregator_unavailable_apiservice	Number of unavailable APIServices
		apiserver_admission_controller_admission_duration_seconds_bucket	Processing delay of an Admission Controller
		apiserver_admission_webhook_admission_duration_seconds_bucket	Processing delay of an Admission Webhook
		apiserver_admission_webhook_admission_duration_seconds_count	Number of Admission Webhook processing requests
		apiserver_client_certificate_expiration_seconds_bucket	Remaining validity period of the client certificate
		apiserver_client_certificate_expiration_seconds_count	Remaining validity period of the client certificate

Target Name	Job Name	Metric	Description
		apiserver_current_inflight_requests	Number of read requests in process
		apiserver_request_duration_seconds_bucket	Delay of the client's access to the APIServer
		apiserver_request_total	Number of different requests to the APIServer
		go_goroutines	Number of goroutines
		kubernetes_build_info	Information to build Kubernetes
		process_cpu_seconds_total	Total process CPU time
		process_resident_memory_bytes	Size of the resident memory set for a process
		rest_client_requests_total	Number of REST requests
		workqueue_adds_total	Number of adds handled by a work queue
		workqueue_depth	Depth of a work queue
		workqueue_queue_duration_seconds_bucket	Duration when a task exists in the work queue
		aggregator_unavailable_apiservice_total	Number of unavailable APIServices
rest_client_request_duration_seconds_bucket	Histogram of REST request duration		
serviceMonitor/monitoring/kubelet/0	kubelet	kubelet_certificate_manager_client_expiration_renew_errors	Number of certificate renewal errors
		kubelet_certificate_manager_client_ttl_seconds	Time-to-live (TTL) of the Kubelet client certificate
		kubelet_cgroup_manager_duration_seconds_bucket	Duration of the cgroup manager operations (bucket)

Target Name	Job Name	Metric	Description
		kubelet_cgroup_manager_duration_seconds_count	Duration of the cgroup manager operations (count)
		kubelet_node_config_error	If a configuration-related error occurs on a node, the value of this metric is true (1) . If there is no configuration-related error, the value is false (0) .
		kubelet_node_name	Node name. The value is always 1 .
		kubelet_pleg_relist_duration_seconds_bucket	Duration of relisting pods in PLEG (bucket)
		kubelet_pleg_relist_duration_seconds_count	Duration of relisting pods in PLEG (count)
		kubelet_pleg_relist_interval_seconds_bucket	Interval between relisting operations in PLEG (bucket)
		kubelet_pod_start_duration_seconds_count	Time required for starting a single pod (count)
		kubelet_pod_start_duration_seconds_bucket	Time required for starting a single pod (bucket)
		kubelet_pod_worker_duration_seconds_bucket	Duration for synchronizing a single pod. Operation type: create, update, or sync
		kubelet_running_containers	Number of running containers
		kubelet_running_pods	Number of running pods
		kubelet_runtime_operations_duration_seconds_bucket	Duration of the runtime operations (bucket)
		kubelet_runtime_operations_errors_total	Number of runtime operation errors listed by operation type

Target Name	Job Name	Metric	Description
		kubelet_runtime_operations_total	Number of runtime operations listed by operation type
		kubelet_volume_stats_available_bytes	Number of available bytes in a volume
		kubelet_volume_stats_capacity_bytes	Capacity of the volume in bytes
		kubelet_volume_stats_inodes	Total number of inodes in a volume
		kubelet_volume_stats_inodes_used	Number of used inodes in a volume
		kubelet_volume_stats_used_bytes	Number of used bytes in a volume
		storage_operation_duration_seconds_bucket	Duration of each storage operation (bucket)
		storage_operation_duration_seconds_count	Duration of each storage operation (count)
		storage_operation_errors_total	Number of storage operation errors
		volume_manager_total_volumes	Number of volumes in the Volume Manager
		rest_client_requests_total	Number of HTTP client requests partitioned by status code, method, and host
		rest_client_request_duration_seconds_bucket	Request delay (bucket)
		process_resident_memory_bytes	Size of the resident memory set for a process
		process_cpu_seconds_total	Total process CPU time
		go_goroutines	Number of goroutines
serviceMonitor/monitoring/kubelet/1	kubelet	container_cpu_cfs_periods_total	Number of elapsed enforcement period intervals

Target Name	Job Name	Metric	Description
		container_cpu_cfs_throttled_periods_total	Number of throttled period intervals
		container_cpu_cfs_throttled_seconds_total	Total time duration the container has been throttled
		container_cpu_load_average_10s	Value of container CPU load average over the last 10 seconds
		container_cpu_usage_seconds_total	Cumulative CPU time consumed by a container in core-seconds
		container_file_descriptors	Number of open file descriptors for a container
		container_fs_inodes_free	Number of available inodes in a file system
		container_fs_inodes_total	Number of inodes in a file system
		container_fs_io_time_seconds_total	Cumulative seconds spent on doing I/Os by the disk or file system
		container_fs_limit_bytes	Total disk or file system capacity that can be consumed by a container
		container_fs_read_seconds_total	Cumulative number of seconds the container spent on reading disk or file system data
		container_fs_reads_bytes_total	Cumulative amount of disk or file system data read by a container
		container_fs_reads_total	Cumulative number of disk or file system reads completed by a container
		container_fs_usage_bytes	File system usage bytes

Target Name	Job Name	Metric	Description
		container_fs_write_seconds_total	Cumulative number of seconds the container spent on writing data to the disk or file system
		container_fs_writes_bytes_total	Total amount of data written by a container to a disk or file system
		container_fs_writes_total	Cumulative number of disk or file system writes completed by a container
		container_memory_cache	Memory used for the page cache of a container
		container_memory_failcnt	Number of memory usage hits limits
		container_memory_max_usage_bytes	Maximum memory usage recorded for a container
		container_memory_rss	Size of the resident memory set for a container
		container_memory_swap	Container swap usage
		container_memory_usage_bytes	Current memory usage of a container
		container_memory_working_set_bytes	Memory usage of the working set of a container
		container_network_receive_bytes_total	Total volume of data received by the container network
		container_network_receive_errors_total	Cumulative number of errors encountered during reception
		container_network_receive_packets_dropped_total	Cumulative number of packets dropped during reception

Target Name	Job Name	Metric	Description
		container_network_receive_packets_total	Cumulative number of packets received
		container_network_transmit_bytes_total	Total volume of data transmitted on the container network
		container_network_transmit_errors_total	Cumulative number of errors encountered during transmission
		container_network_transmit_packets_dropped_total	Cumulative number of packets dropped during transmission
		container_network_transmit_packets_total	Cumulative number of packets transmitted
		container_spec_cpu_quota	CPU quota of the container
		container_spec_memory_limit_bytes	Memory limit for the container
		machine_cpu_cores	Number of logical CPU cores
		machine_memory_bytes	Amount of memory
serviceMonitor/monitoring/kube-state-metrics/0	kube-state-metrics-prom	kube_cronjob_status_active	Running cronjob
		kube_cronjob_info	Cronjob information
		kube_cronjob_labels	Label of a cronjob
		kube_configmap_info	ConfigMap information
		kube_daemonset_created	DaemonSet creation time
		kube_daemonset_status_current_number_scheduled	Number of DaemonSets that are being scheduled
		kube_daemonset_status_desired_number_scheduled	Number of DaemonSets expected to be scheduled

Target Name	Job Name	Metric	Description
		kube_daemonset_status_number_available	Number of nodes that should be running a DaemonSet pod and have at least one DaemonSet pod running and available
		kube_daemonset_status_number_misscheduled	Number of nodes that are not expected to run a DaemonSet pod
		kube_daemonset_status_number_ready	Number of nodes that should be running the DaemonSet pods and have one or more DaemonSet pods running and ready
		kube_daemonset_status_number_unavailable	Number of nodes that should be running the DaemonSet pods but have none of the DaemonSet pods running and available
		kube_daemonset_status_updated_number_scheduled	Number of nodes that are running an updated DaemonSet pod
		kube_deployment_created	Deployment creation timestamp
		kube_deployment_labels	Deployment labels
		kube_deployment_metadata_generation	Sequence number representing a specific generation of the desired state
		kube_deployment_spec_replicas	Number of desired replicas for a Deployment
		kube_deployment_spec_strategy_rollingupdate_max_unavailable	Maximum number of unavailable replicas during a rolling update of a Deployment

Target Name	Job Name	Metric	Description
		kube_deployment_status_observed_generation	The generation observed by the Deployment controller
		kube_deployment_status_replicas	Number of current replicas of a Deployment
		kube_deployment_status_replicas_available	Number of available replicas per Deployment
		kube_deployment_status_replicas_ready	Number of ready replicas per Deployment
		kube_deployment_status_replicas_unavailable	Number of unavailable replicas per Deployment
		kube_deployment_status_replicas_updated	Number of updated replicas per Deployment
		kube_job_info	Information about the job
		kube_namespace_labels	Namespace labels
		kube_node_labels	Node labels
		kube_node_info	Information about a node
		kube_node_spec_taint	Taint of a node
		kube_node_spec_unschedulable	Whether new pods can be scheduled to a node
		kube_node_status_allocatable	Allocatable resources on a node
		kube_node_status_capacity	Capacity for different resources on a node
		kube_node_status_condition	Condition of a node
		kube_node_volcano_oversubscription_status	Node oversubscription status
		kube_persistentvolume_status_phase	Phase of a PV status

Target Name	Job Name	Metric	Description
		kube_persistentvolumeclaim_status_phase	Phase of a PVC status
		kube_persistentvolume_info	Information about a PV
		kube_persistentvolumeclaim_info	Information about a PVC
		kube_pod_container_info	Information about a container running in the pod
		kube_pod_container_resource_limits	Number of container resource limits
		kube_pod_container_resource_requests	Number of container resource requests
		kube_pod_container_status_last_terminated_reason	Last reason the container was in a terminated state
		kube_pod_container_status_ready	Whether the container's readiness check succeeded
		kube_pod_container_status_restarts_total	Number of container restarts
		kube_pod_container_status_running	Whether the container is running.
		kube_pod_container_status_terminated	Whether the container is terminated
		kube_pod_container_status_terminated_reason	The reason why the container is in a terminated state
		kube_pod_container_status_waiting	Whether the container is waiting
		kube_pod_container_status_waiting_reason	The reason why the container is in the waiting state
		kube_pod_info	Information about a pod
		kube_pod_labels	Pod labels
		kube_pod_owner	Information about the pod's owner

Target Name	Job Name	Metric	Description
		kube_pod_status_phase	Current phase of a pod
		kube_pod_status_ready	Whether the pod is ready
		kube_secret_info	Information about a secret
		kube_statefulset_created	StatefulSet creation timestamp
		kube_statefulset_labels	Information about StatefulSet labels
		kube_statefulset_metadata_generation	Sequence number representing a specific generation of the desired state for a StatefulSet
		kube_statefulset_replicas	Number of desired pods for a StatefulSet
		kube_statefulset_status_observed_generation	The generation observed by the StatefulSet controller
		kube_statefulset_status_replicas	Number of replicas per StatefulSet
		kube_statefulset_status_replicas_ready	Number of ready replicas per StatefulSet
		kube_statefulset_status_replicas_updated	Number of updated replicas per StatefulSet
		kube_job_spec_completions	Desired number of successfully finished pods that should run with the job
		kube_job_status_failed	Failed jobs
		kube_job_status_succeeded	Successful jobs
		kube_node_status_allocatable_cpu_cores	Number of allocatable CPU cores of a node
		kube_node_status_allocatable_memory_bytes	Total allocatable memory of a node

Target Name	Job Name	Metric	Description
		kube_replicaset_owner	Information about the ReplicaSet's owner
		kube_resourcequota	Information about resource quota
		kube_pod_spec_volumes_persistentvolumeclaims_info	Information about the PVC associated with the pod
serviceMonitor/monitoring/prometheus-lightweight/0	prometheus-lightweight	vm_persistentqueue_blocks_dropped_total	Number of dropped blocks in a send queue
		vm_persistentqueue_blocks_read_total	Number of blocks read by a send queue
		vm_persistentqueue_blocks_written_total	Number of blocks written to a send queue
		vm_persistentqueue_bytes_pending	Number of pending bytes in a send queue
		vm_persistentqueue_bytes_read_total	Number of bytes read by a send queue
		vm_persistentqueue_bytes_written_total	Number of bytes written to a send queue
		vm_promscrape_active_scrapers	Number of active scrapes
		vm_promscrape_connection_read_errors_total	Number of read errors during scrapes
		vm_promscrape_connection_write_errors_total	Number of write errors during scrapes
		vm_promscrape_max_scrape_size_exceeded_errors_total	Number of failed scrapes due to the exceeded response size
		vm_promscrape_scrape_duration_seconds_sum	Duration of scrapes (sum)
		vm_promscrape_scrape_duration_seconds_count	Duration of scrapes (count)
		vm_promscrape_scrapes_total	Number of scrapes

Target Name	Job Name	Metric	Description
		vmagent_remotewrite_bytes_sent_total	Number of bytes sent via a remote write
		vmagent_remotewrite_duration_seconds_sum	Time required for a remote write (sum)
		vmagent_remotewrite_duration_seconds_count	Time required for a remote write (count)
		vmagent_remotewrite_packets_dropped_total	Number of dropped packets during a remote write
		vmagent_remotewrite_pending_data_bytes	Number of pending bytes during a remote write
		vmagent_remotewrite_requests_total	Number of requests of the remote write
		vmagent_remotewrite_retries_count_total	Number of retries of the remote write
		go_goroutines	Number of goroutines
serviceMonitor/monitoring/node-exporter/0	node-exporter	node_boot_time_seconds	Node boot time
		node_context_switches_total	Number of context switches
		node_cpu_seconds_total	Seconds each CPU spent doing each type of work
		node_disk_io_now	Number of I/Os in progress
		node_disk_io_time_seconds_total	Total seconds spent doing I/Os
		node_disk_io_time_weighted_seconds_total	The weighted number of seconds spent doing I/Os
		node_disk_read_bytes_total	Number of bytes that are read
		node_disk_read_time_seconds_total	Number of seconds spent by all reads
		node_disk_reads_completed_total	Number of reads completed

Target Name	Job Name	Metric	Description
		node_disk_write_time_seconds_total	Number of seconds spent by all writes
		node_disk_writes_completed_total	Number of writes completed
		node_disk_written_bytes_total	Number of bytes that are written
		node_docker_thinpool_data_space_available	Available data space of a docker thin pool
		node_docker_thinpool_metadata_space_available	Available metadata space of a docker thin pool
		node_exporter_build_info	Node exporter build information
		node_filefd_allocated	Allocated file descriptors
		node_filefd_maximum	Maximum number of file descriptors
		node_filesystem_available_bytes	File system space that is available for use
		node_filesystem_device_error	Whether an error occurred while getting statistics for the given device
		node_filesystem_free_bytes	Remaining space of a file system
		node_filesystem_readonly	Read-only file system
		node_filesystem_size_bytes	Consumed space of a file system
		node_forks_total	Number of forks
		node_intr_total	Number of interruptions that occurred
		node_load1	1-minute average CPU load
		node_load15	15-minute average CPU load
		node_load5	5-minute average CPU load

Target Name	Job Name	Metric	Description
		node_memory_Buffers_bytes	Memory of the node buffer
		node_memory_Cached_bytes	Memory for the node page cache
		node_memory_MemAvailable_bytes	Available memory of a node
		node_memory_MemFree_bytes	Free memory of a node
		node_memory_MemTotal_bytes	Total memory of a node
		node_network_receive_bytes_total	Total amount of received data
		node_network_receive_drop_total	Cumulative number of packets dropped during reception
		node_network_receive_errs_total	Cumulative number of errors encountered during reception
		node_network_receive_packets_total	Cumulative number of packets received
		node_network_transmit_bytes_total	Total amount of transmitted data
		node_network_transmit_drop_total	Cumulative number of dropped packets during transmission
		node_network_transmit_errs_total	Cumulative number of errors encountered during transmission
		node_network_transmit_packets_total	Cumulative number of packets transmitted
		node_procs_blocked	Blocked processes
		node_procs_running	Running processes
		node_sockstat_sockets_used	Number of sockets in use
		node_sockstat_TCP_alloc	Number of allocated TCP sockets
		node_sockstat_TCP_inuse	Number of TCP sockets in use

Target Name	Job Name	Metric	Description
		node_sockstat_TCP_orphan	Number of orphaned TCP sockets
		node_sockstat_TCP_tw	Number of TCP sockets in the TIME_WAIT state
		node_sockstat_UDPLITE_inuse	Number of UDP-Lite sockets in use
		node_sockstat_UDP_inuse	Number of UDP sockets in use
		node_sockstat_UDP_memory	UDP socket buffer usage
		node_timex_offset_seconds	Time offset
		node_timex_sync_status	Synchronization status of node clocks
		node_uname_info	Labeled system information as provided by the uname system call
		node_vmstat_oom_kill	OOM kill in /proc/vmstat
		process_cpu_seconds_total	Total process CPU time
		process_max_fds	Maximum number of file descriptors of a process
		process_open_fds	Opened file descriptors by a process
		process_resident_memory_bytes	Size of the resident memory set for a process
		process_start_time_seconds	Process start time
		process_virtual_memory_bytes	Virtual memory size for a process
		process_virtual_memory_max_bytes	Maximum virtual memory size for a process

Target Name	Job Name	Metric	Description
		node_netstat_Tcp_ActiveOpens	Number of TCP connections that directly change from the CLOSED state to the SYN-SENT state
		node_netstat_Tcp_PassiveOpens	Number of TCP connections that directly change from the LISTEN state to the SYN-RCVD state
		node_netstat_Tcp_CurrEstab	Number of TCP connections in the ESTABLISHED or CLOSE-WAIT state
		node_vmstat_pgmajfault	Number of major faults per second in / proc/vmstat
		node_vmstat_pgpgout	Number of page out between main memory and block device in / proc/vmstat
		node_vmstat_pgfault	Number of page faults the system has made per second in / proc/vmstat
		node_vmstat_pgpgin	Number of page in between main memory and block device in / proc/vmstat
		node_processes_max_processes	PID limit value
		node_processes_pids	Number of PIDs
		node_nf_conntrack_entries	Number of currently allocated flow entries for connection tracking
		node_nf_conntrack_entries_limit	Maximum size of a connection tracking table
		promhttp_metric_handler_requests_in_flight	Number of metrics being processed

Target Name	Job Name	Metric	Description
		go_goroutines	Number of node exporter goroutines
podMonitor/ monitoring/ nvidia-gpu- device- plugin/0	monitoring/ nvidia-gpu- device-plugin	cce_gpu_utilization	GPU compute usage
		cce_gpu_memory_utilization	GPU memory usage
		cce_gpu_encoder_utilization	GPU encoding usage
		cce_gpu_decoder_utilization	GPU decoding usage
		cce_gpu_utilization_process	GPU compute usage of each process
		cce_gpu_memory_utilization_process	GPU memory usage of each process
		cce_gpu_encoder_utilization_process	GPU encoding usage of each process
		cce_gpu_decoder_utilization_process	GPU decoding usage of each process
		cce_gpu_memory_used	Used GPU memory
		cce_gpu_memory_total	Total GPU memory
		cce_gpu_memory_free	Free GPU memory
		cce_gpu_bar1_memory_used	Used GPU BAR1 memory
		cce_gpu_bar1_memory_total	Total GPU BAR1 memory
		cce_gpu_clock	GPU clock frequency
		cce_gpu_memory_clock	GPU memory frequency
		cce_gpu_graphics_clock	GPU frequency
		cce_gpu_video_clock	GPU video processor frequency
		cce_gpu_temperature	GPU temperature
		cce_gpu_power_usage	GPU power
		cce_gpu_total_energy_consumption	Total GPU energy consumption

Target Name	Job Name	Metric	Description
		cce_gpu_pcie_link_bandwidth	GPU PCIe bandwidth
		cce_gpu_nvlink_bandwidth	GPU NVLink bandwidth
		cce_gpu_pcie_throughput_rx	GPU PCIe RX bandwidth
		cce_gpu_pcie_throughput_tx	GPU PCIe TX bandwidth
		cce_gpu_nvlink_utilization_counter_rx	GPU NVLink RX bandwidth
		cce_gpu_nvlink_utilization_counter_tx	GPU NVLink TX bandwidth
		cce_gpu_retired_pages_sbe	Number of GPU single-bit error isolation pages
		cce_gpu_retired_pages_dbe	Number of GPU dual-bit error isolation pages
		xgpu_memory_total	Total xGPU memory
		xgpu_memory_used	Used xGPU memory
		xgpu_core_percentage_total	Total xGPU compute
		xgpu_core_percentage_used	Used xGPU compute
		gpu_schedule_policy	There are three GPU modes specified by three values. The value 0 indicates the GPU memory isolation, compute sharing mode. The value 1 indicates the GPU memory and compute isolation mode. The value 2 indicates the default mode, indicating that the GPU is not virtualized.

Target Name	Job Name	Metric	Description
		xgpu_device_health	Health status of xGPU. The value 0 indicates that the xGPU is healthy, and the value 1 indicates that the xGPU is unhealthy.
serviceMonitor/monitoring/prometheus-server/0	prometheus-server	prometheus_build_info	Information to build Prometheus
		prometheus_engine_query_duration_seconds	Query time
		prometheus_engine_query_duration_seconds_count	Number of queries
		prometheus_sd_discovered_targets	Number of targets discovered by each job
		prometheus_remote_storage_bytes_total	Number of bytes sent
		prometheus_remote_storage_enqueue_retries_total	Number of retries for entering a queue
		prometheus_remote_storage_highest_timestamp_in_seconds	Highest timestamp that has come into the remote storage via the Appender interface, in seconds since epoch
		prometheus_remote_storage_queue_highest_sent_timestamp_seconds	Highest timestamp successfully sent by a remote write
		prometheus_remote_storage_samples_dropped_total	Total number of samples read from the WAL but not sent to remote storage
		prometheus_remote_storage_samples_failed_total	Number of samples that failed to be sent to remote storage
prometheus_remote_storage_samples_in_total	Number of samples read into remote storage		

Target Name	Job Name	Metric	Description
		prometheus_remote_storage_samples_pending	Number of samples pending in shards to be sent to remote storage
		prometheus_remote_storage_samples_retrieved_total	Number of samples which failed to be sent to remote storage but were retried
		prometheus_remote_storage_samples_total	Total number of samples sent to remote storage
		prometheus_remote_storage_shard_capacity	Capacity of each shard of the queue used for parallel sending to the remote storage
		prometheus_remote_storage_shards	Number of shards used for parallel sending to the remote storage
		prometheus_remote_storage_shards_desired	Number of shards that the queues shard calculation wants to run based on the rate of samples in vs. samples out
		prometheus_remote_storage_shards_max	Maximum number of shards that the queue is allowed to run
		prometheus_remote_storage_shards_min	Minimum number of shards that the queue is allowed to run
		prometheus_tsdb_wal_segment_current	WAL segment index that TSDB is currently writing to
		prometheus_tsdb_head_chunks	Number of chunks in the head block
		prometheus_tsdb_head_series	Number of series in the head block
		prometheus_tsdb_head_samples_appended_total	Number of appended samples

Target Name	Job Name	Metric	Description
		prometheus_wal_watcher_current_segment	Current segment the WAL watcher is reading records from
		prometheus_target_interval_length_seconds	Actual intervals between scrapes
		prometheus_target_interval_length_seconds_count	Actual intervals between scrapes (count)
		prometheus_target_interval_length_seconds_sum	Actual intervals between scrapes (sum)
		prometheus_target_scrapes_exceeded_body_size_limit_total	Number of scrapes that hit the body size limit
		prometheus_target_scrapes_exceeded_sample_limit_total	Number of scrapes that hit the sample limit
		prometheus_target_scrapes_sample_duplicate_timestamp_total	Number scraped samples with duplicate timestamps
		prometheus_target_scrapes_sample_out_of_bounds_total	Number of samples rejected due to timestamp falling outside of the time bounds
		prometheus_target_scrapes_sample_out_of_order_total	Number of out-of-order samples
		prometheus_target_sync_length_seconds	Interval for synchronizing the scrape pool
		prometheus_target_sync_length_seconds_count	Interval for synchronizing the scrape pool (count)
		prometheus_target_sync_length_seconds_sum	Interval for synchronizing the scrape pool (sum)
		promhttp_metric_handler_requests_in_flight	Number of metrics being processed
		promhttp_metric_handler_requests_total	Number of metric processing times

Target Name	Job Name	Metric	Description
		go_goroutines	Number of goroutines
podMonitor/ monitoring/ virtual- kubelet- pods/0	monitoring/ virtual- kubelet-pods	container_cpu_load_ave- rage_10s	Value of container CPU load average over the last 10 seconds
		container_cpu_system_ seconds_total	Cumulative container CPU system time
		container_cpu_usage_ seconds_total	Cumulative CPU time consumed by a container in core-seconds
		container_cpu_user_se- conds_total	Usage of user CPU time
		container_cpu_cfs_peri- ods_total	Number of elapsed enforcement period intervals
		container_cpu_cfs_thr- ottled_periods_total	Number of throttled period intervals
		container_cpu_cfs_thr- ottled_seconds_total	Total time duration the container has been throttled
		container_fs_inodes_fr- ee	Number of available inodes in a file system
		container_fs_usage_by- tes	File system usage
		container_fs_inodes_to- tal	Number of inodes in a file system
		container_fs_io_curren- t	Number of I/Os currently in progress in a disk or file system
		container_fs_io_time_s- econds_total	Cumulative seconds spent on doing I/Os by the disk or file system
		container_fs_io_time_w- eighted_seconds_tot- al	Cumulative weighted I/O time of a disk or file system
container_fs_limit_byt- es	Total disk or file system capacity that can be consumed by a container		

Target Name	Job Name	Metric	Description
		container_fs_reads_bytes_total	Cumulative amount of disk or file system data read by a container
		container_fs_read_seconds_total	Cumulative number of seconds the container spent on reading disk or file system data
		container_fs_reads_merged_total	Cumulative number of merged disk or file system reads made by the container.
		container_fs_reads_total	Cumulative number of disk or file system reads completed by a container
		container_fs_sector_reads_total	Cumulative number of disk or file system sector reads completed by a container
		container_fs_sector_writes_total	Cumulative number of disk or file system sector writes completed by a container
		container_fs_writes_bytes_total	Total amount of data written by a container to a disk or file system
		container_fs_write_seconds_total	Cumulative number of seconds the container spent on writing data to the disk or file system
		container_fs_writes_merged_total	Cumulative number of merged container writes to the disk or file system
		container_fs_writes_total	Cumulative number of disk or file system writes completed by a container

Target Name	Job Name	Metric	Description
		container_blkio_device_usage_total	Blkio device bytes usage
		container_memory_failures_total	Cumulative number of container memory allocation failures
		container_memory_failcnt	Number of memory usage hits limits
		container_memory_cache	Memory used for the page cache of a container
		container_memory_mapped_file	Size of the container memory mapped file.
		container_memory_max_usage_bytes	Maximum memory usage recorded for a container
		container_memory_rss	Size of the resident memory set for a container
		container_memory_swap	Container swap usage
		container_memory_usage_bytes	Current memory usage of a container
		container_memory_working_set_bytes	Memory usage of the working set of a container
		container_network_receive_bytes_total	Total volume of data received by the container network
		container_network_receive_errors_total	Cumulative number of errors encountered during reception
		container_network_receive_packets_dropped_total	Cumulative number of packets dropped during reception
		container_network_receive_packets_total	Cumulative number of packets received
		container_network_transmit_bytes_total	Total volume of data transmitted on the container network

Target Name	Job Name	Metric	Description
		container_network_transmit_errors_total	Cumulative number of errors encountered during transmission
		container_network_transmit_packets_dropped_total	Cumulative number of packets dropped during transmission
		container_network_transmit_packets_total	Cumulative number of packets transmitted
		container_processes	Number of processes running inside the container
		container_sockets	Number of open sockets for the container
		container_file_descriptors	Number of open file descriptors for a container
		container_threads	Number of threads running inside the container
		container_threads_max	Maximum number of threads allowed inside the container
		container_ulimits_soft	Soft ulimit value of process 1 in the container. Unlimited if the value is -1, except priority and nice.
		container_tasks_state	Number of tasks in the specified state, such as sleeping, running, stopped, uninterruptible, or ioawaiting
		container_spec_cpu_period	CPU period of the container
		container_spec_cpu_shares	CPU share of the container
		container_spec_cpu_quota	CPU quota of the container

Target Name	Job Name	Metric	Description
		container_spec_memory_limit_bytes	Memory limit for the container
		container_spec_memory_reservation_limit_bytes	Memory reservation limit for the container
		container_spec_memory_swap_limit_bytes	Memory swap limit for the container
		container_start_time_seconds	Running time of the container.
		container_last_seen	Last time a container was seen by the exporter
		container_accelerator_memory_used_bytes	GPU accelerator memory that is being used by the container
		container_accelerator_memory_total_bytes	Total available memory of a GPU accelerator
		container_accelerator_duty_cycle	Percentage of time when a GPU accelerator is actually running
podMonitor/ monitoring/ everest-csi-controller/0	monitoring/ everest-csi-controller	everest_action_result_total	Number of action results
		everest_function_duration_seconds_bucket	Histogram of action duration (bucket)
		everest_function_duration_seconds_count	Histogram of action duration (count)
		everest_function_duration_seconds_sum	Histogram of action duration (sum)
		everest_function_duration_seconds_quantile	Time quantile required by the action
		node_volume_read_completed_total	Number of completed reads
		node_volume_read_merged_total	Number of merged reads
		node_volume_read_bytes_total	Total number of bytes read by a sector

Target Name	Job Name	Metric	Description
		node_volume_read_time_milliseconds_total	Total read duration
		node_volume_write_completed_total	Number of completed writes
		node_volume_write_merged_total	Number of merged writes
		node_volume_write_bytes_total	Total number of bytes written into a sector
		node_volume_write_time_milliseconds_total	Total write duration
		node_volume_io_now	Number of ongoing I/Os
		node_volume_io_time_seconds_total	Total I/O operation duration
		node_volume_capacity_bytes_available	Available capacity
		node_volume_capacity_bytes_total	Total capacity
		node_volume_capacity_bytes_used	Used capacity
		node_volume_inodes_available	Available inodes
		node_volume_inodes_total	Total number of inodes
		node_volume_inodes_used	Used inodes
		node_volume_read_transmissions_total	Number of read transmission times
		node_volume_read_timeouts_total	Number of read timeouts
		node_volume_read_sent_bytes_total	Number of bytes read
		node_volume_read_queue_time_milliseconds_total	Read queue waiting time
		node_volume_read_rtt_time_milliseconds_total	Read RTT

Target Name	Job Name	Metric	Description
		node_volume_write_transmissions_total	Number of write transmissions
		node_volume_write_timeouts_total	Number of write timeouts
		node_volume_write_queue_time_milliseconds_total	Write queue waiting time
		node_volume_write_rtt_time_milliseconds_total	Write RTT
		node_volume_localvolume_stats_capacity_bytes	Local storage capacity
		node_volume_localvolume_stats_available_bytes	Available local storage
		node_volume_localvolume_stats_used_bytes	Used local storage
		node_volume_localvolume_stats_inodes	Number of inodes for a local volume
		node_volume_localvolume_stats_inodes_used	Used inodes for a local volume
podMonitor/ monitoring/ nginx-ingress-controller/0	monitoring/ nginx-ingress-controller	nginx_ingress_controller_bytes_sent	Number of bytes sent to the client
		nginx_ingress_controller_connect_duration_seconds	Duration for connecting to the upstream server
		nginx_ingress_controller_header_duration_seconds	Time required for receiving the first header from the upstream server
		nginx_ingress_controller_ingress_upstream_latency_seconds	Upstream service latency
		nginx_ingress_controller_request_duration_seconds	Time required for processing a request, in milliseconds
		nginx_ingress_controller_request_size	Length of a request, including the request line, header, and body

Target Name	Job Name	Metric	Description
		nginx_ingress_controller_requests	Total number of HTTP requests processed by Nginx Ingress Controller since it starts
		nginx_ingress_controller_response_duration_seconds	Time required for receiving the response from the upstream server
		nginx_ingress_controller_response_size	Length of a response, including the request line, header, and body
		nginx_ingress_controller_nginx_process_connections	Number of client connections in the active, read, write, or wait state
		nginx_ingress_controller_nginx_process_connections_total	Total number of client connections in the accepted or handled state
		nginx_ingress_controller_nginx_process_cpu_seconds_total	Total CPU time consumed by the Nginx process (unit: second)
		nginx_ingress_controller_nginx_process_num_procs	Number of processes
		nginx_ingress_controller_nginx_process_oldest_start_time_seconds	Start time in seconds since January 1, 1970
		nginx_ingress_controller_nginx_process_read_bytes_total	Number of bytes read
		nginx_ingress_controller_nginx_process_requests_total	Total number of requests processed by Nginx since startup
		nginx_ingress_controller_nginx_process_resident_memory_bytes	Resident memory usage of a process, that is, the actual physical memory usage

Target Name	Job Name	Metric	Description
		nginx_ingress_controller_nginx_process_virtual_memory_bytes	Virtual memory usage of a process, that is, the total memory allocated to the process, including the actual physical memory and virtual swap space
		nginx_ingress_controller_nginx_process_write_bytes_total	Amount of data written by the Nginx process to disks or other devices for long-term storage
		nginx_ingress_controller_build_info	Build information of Nginx Ingress Controller, including the version and compilation time
		nginx_ingress_controller_check_success	Health check result of Nginx Ingress Controller. 1 : Normal. 0 : Abnormal
		nginx_ingress_controller_config_hash	Configured hash value
		nginx_ingress_controller_config_last_reload_successful	Whether the Nginx Ingress Controller configuration is successfully reloaded
		nginx_ingress_controller_config_last_reload_successful_timestamp_seconds	Last timestamp when the Nginx Ingress Controller configuration was successfully reloaded
		nginx_ingress_controller_ssl_certificate_info	Nginx Ingress Controller certificate information
		nginx_ingress_controller_success	Cumulative number of reload operations of Nginx Ingress Controller

Target Name	Job Name	Metric	Description
		nginx_ingress_controller_orphan_ingress	Whether the ingress is isolated. 1: Isolated. 0: Not isolated. namespace indicates the namespace where the ingress is located, ingress indicates the ingress name. type indicates that the isolation type (options: no-service and no-endpoint).
		nginx_ingress_controller_admission_config_size	Size of the admission controller configuration
		nginx_ingress_controller_admission_render_duration	Rendering duration of the admission controller
		nginx_ingress_controller_admission_render_ingresses	Length of ingresses rendered by the admission controller
		nginx_ingress_controller_admission_roundtrip_duration	Time spent by the admission controller to process new events
		nginx_ingress_controller_admission_tested_duration	Time spent on admission controller tests
		nginx_ingress_controller_admission_tested_ingresses	Length of ingresses processed by the admission controller

1.7.4 Metric Dimensions

Dimensions of VM Metrics Reported by ICAgents

Table 1-8 Dimensions of VM metrics reported by ICAgents

Category	Metric Dimension	Description
Network metrics	clusterId	Cluster ID
	hostID	Host ID

Category	Metric Dimension	Description
	nameSpace	Cluster namespace
	netDevice	NIC name
	nodeIP	Host IP address
	nodeName	Host name
Disk metrics	clusterId	Cluster ID
	diskDevice	Disk name
	hostID	Host ID
	nameSpace	Cluster namespace
	nodeIP	Host IP address
	nodeName	Host name
Disk partition metrics	diskPartition	Partition disk
	diskPartitionType	Disk partition type
File system metrics	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
Host metrics	clusterId	Cluster ID
	clusterName	Cluster name
	gpuName	GPU name
	gpuID	GPU ID
	npuName	NPU name
	npuID	NPU ID
	hostID	Host ID
	nameSpace	Cluster namespace
	nodeIP	Host IP address

Category	Metric Dimension	Description
	hostName	Host name
Cluster metrics	clusterId	Cluster ID
	clusterName	Cluster name
	projectId	Project ID
Container metrics	appID	Service ID
	appName	Service name
	clusterId	Cluster ID
	clusterName	Cluster name
	containerID	Container ID
	containerName	Container name
	deploymentName	Workload name
	kind	Application type
	nameSpace	Cluster namespace
	podID	Instance ID
	podIP	Pod IP address
	podName	Instance name
	serviceID	Inventory ID
	nodename	Host name
	nodeIP	Host IP address
	virtualServiceName	Istio virtual service name
	gpuID	GPU ID
	npuName	NPU name
npuID	NPU ID	
Process metrics	appName	Service name
	clusterId	Cluster ID
	clusterName	Cluster name
	nameSpace	Cluster namespace
	processID	Process ID
	processName	Process name

Category	Metric Dimension	Description
	serviceID	Inventory ID

1.8 Basic Concepts

1.8.1 Resource Monitoring

Table 1-9 Basic concepts

Terminology	Description
Metrics	<p>Metrics reflect resource performance data or status. A metric consists of a namespace, dimension, name, and unit.</p> <p>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.</p>
Host	<p>Each host of AOM corresponds to a VM or physical machine. A host can be your own VM or physical machine, or an Elastic Cloud Service (ECS) or Bare Metal Server (BMS) purchased. A host can be connected to AOM for monitoring only when its OS meets requirements and it is installed with an ICAgent.</p>
Logs	<p>You can quickly search for required logs from massive quantities of logs. You can also quickly locate faults by analyzing the log source and context.</p>
Log traffic	<p>Log traffic refers to the volume of logs reported per second. 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.</p>
Alarms	<p>Alarms are reported when AOM, ServiceStage, APM, or CCE is abnormal or may cause exceptions. Alarms will cause service exceptions and need to be handled.</p>
Events	<p>Events generally carry important information. They are reported when AOM, ServiceStage, APM, or CCE encounters some changes. Events do not necessarily cause service exceptions. Events do not need to be handled.</p>

Terminology	Description
Alarm clearance	<p>There are two alarm clearance modes:</p> <ul style="list-style-type: none"> • Automatic clearance: After a fault is rectified, AOM automatically clears the corresponding alarm. • Manual clearance: After a fault is rectified, AOM does not automatically clear the corresponding alarm. Instead, you need to manually clear the alarm.
Alarm rules	<p>Alarm rules are classified into metric alarm rules and event alarm rules.</p> <ul style="list-style-type: none"> • Metric alarm rules monitor the usage of resources (such as hosts and components) in the environment in real time. • If there are many resource alarms but you do not want to receive notifications too often, set event alarm rules to quickly identify specific types of resource usage problems.
Alarm notification	<p>There are two alarm notification modes:</p> <ul style="list-style-type: none"> • Direct alarm reporting: When setting alarm notification rules, specify alarm notification recipients so that they can take measures to rectify faults in a timely manner. Alarms can be sent through email and SMS. • Alarm noise reduction: Select a grouping rule to reduce alarm noise.
Alarm action rules	<p>An alarm action rule defines the action to be taken after an alarm is generated. It includes where the message is sent and in what form.</p>
Prometheus instances	<p>Logical units used to manage Prometheus data collection, storage, and analysis.</p>
Prometheus probes	<p>Deployed in the Kubernetes clusters on the user or cloud product side. Prometheus probes automatically discover targets, collect metrics, and remotely write data to databases.</p>
Exporters	<p>Collect monitoring data and regulate the data provided for external systems using the Prometheus monitoring function. Currently, hundreds of official or third-party exporters are available. For details, see Exporters.</p>
Jobs	<p>Configuration set for a group of targets. Jobs specify the capture interval, access limit, and other behavior for a group of targets.</p>

1.8.2 Collection Management

Table 1-10 Basic concepts of collection management

Terminology	Description
UniAgent	UniAgent manages the life cycle of plug-ins centrally and deliver instructions for operations such as script delivery or execution. It does not collect O&M data; instead, different plug-ins do so. Install, upgrade, and uninstall these plug-ins as required. More plug-ins (such as Cloud Eye and Host Security Service (HSS)) are coming soon.
AK/SK	Access key. You can install ICAgents using tenant-level AK/SK for easy log collection.
ICAgent	ICAgents collect metrics, logs, and application performance data. For the hosts created on the ECS or BMS console, manually install ICAgents. For the hosts that are created through CCE, ICAgents are automatically installed.
Installation host	You can deliver UniAgent installation instructions to hosts in batches through an installation host on AOM. After setting an installation host, you can remotely install UniAgents on other hosts in the same VPC.
Proxy area/ Proxy	To enable network communication between multiple clouds, create and configure an ECS as a proxy and bind an EIP to it. AOM delivers deployment and control instructions to remote hosts and receives O&M data through the proxy. A proxy area contains multiple proxies for high availability.

1.9 Permissions Management

If you need to assign different permissions to employees in your enterprise to access your AOM resources, Identity and Access Management (IAM) is a good choice for fine-grained permissions management. IAM provides identity authentication, permissions management, and access control, helping you secure access to your AOM resources.

With IAM, you can use your account to create IAM users for your employees, and assign permissions to the users to control their access to specific types of resources. For example, some software developers in your enterprise need to use AOM resources but are not allowed to delete them or perform any high-risk operations such as deleting application discovery rules. To achieve this result, you can create IAM users for the software developers and grant them only the permissions required for using AOM resources.

If your account does not need individual IAM users for permissions management, you may skip over this chapter.

IAM can be used free of charge. You pay only for the resources in your account. For more information, see IAM Service Overview.

AOM Permissions

By default, new IAM users do not have any permissions assigned. You need to add a user to one or more groups, and assign permissions policies or roles to these groups. The user then inherits permissions from the groups it is a member of. This process is called authorization. After authorization, the user can perform specified operations on AOM.

AOM is a project-level service deployed and accessed in specific physical regions. To assign AOM permissions to a user group, specify the scope as region-specific projects and select projects for the permissions to take effect. If **All projects** is selected, the permissions will take effect for the user group in all region-specific projects. When accessing AOM, the users need to switch to a region where they have been authorized to use this service.

You can grant users permissions by using roles and policies.

- **Roles:** A coarse-grained authorization mechanism provided by IAM to define permissions based on users' job responsibilities. This mechanism provides only a limited number of service-level roles for authorization. Cloud services depend on each other. When you grant permissions using roles, you may also need to attach dependent roles. However, roles are not an ideal choice for fine-grained authorization and secure access control.
- **Policies:** A type of fine-grained authorization mechanism that defines permissions required to perform operations on specific cloud resources under certain conditions. This mechanism allows for more flexible policy-based authorization, meeting requirements for secure access control. For example, you can grant Elastic Cloud Server (ECS) users only the permissions for managing a certain type of ECSs. Most policies define permissions based on APIs.

Table 1-11 lists all the system permissions supported by AOM.

Table 1-11 System permissions supported by AOM

Subservice Name	Policy Name	Description	Type	Dependent System Permissions
Monitoring center / collection management	AOM FullAccess	Administrator permissions for AOM 2.0. Users granted these permissions can operate and use AOM.	System-defined policy	CCE FullAccess and DMS ReadOnly Access
	AOM Viewer	Read-only permissions for AOM 2.0. Users granted these permissions can only view AOM data.	System-defined policy	CCE ReadOnly Access and DMS ReadOnly Access

Common Operations and System Permissions for Resource Monitoring

Table 1-12 lists the common operations supported by each system-defined policy of resource monitoring. Select policies as required.

Table 1-12 Common operations supported by each system-defined policy

Operation	AOM FullAccess	AOM Viewer
Creating an alarm rule	√	x
Modifying an alarm rule	√	x
Deleting an alarm rule	√	x
Creating an alarm template	√	x
Modifying an alarm template	√	x
Deleting an alarm template	√	x
Creating an alarm action rule	√	x
Modifying an alarm action rule	√	x
Deleting an alarm action rule	√	x
Creating a message template	√	x
Modifying a message template	√	x
Deleting a message template	√	x
Creating a grouping rule	√	x
Modifying a grouping rule	√	x
Deleting a grouping rule	√	x
Creating a suppression rule	√	x
Modifying a suppression rule	√	x
Deleting a suppression rule	√	x

Operation	AOM FullAccess	AOM Viewer
Creating a silence rule	√	x
Modifying a silence rule	√	x
Deleting a silence rule	√	x
Creating a dashboard	√	x
Modifying a dashboard	√	x
Deleting a dashboard	√	x
Creating a Prometheus instance	√	x
Modifying a Prometheus instance	√	x
Deleting a Prometheus instance	√	x
Creating an application discovery rule	√	x
Modifying an application discovery rule	√	x
Deleting an application discovery rule	√	x
Subscribing to threshold alarms	√	x
Configuring a VM log collection path	√	x

Common Operations Supported by Each System-defined Policy of Collection Management

Table 1-13 lists the common operations supported by each system-defined policy of collection management. Select policies as required.

Table 1-13 Common operations supported by each system-defined policy of collection management

Operation	AOM FullAccess	AOM Viewer
Querying a proxy area	√	√
Editing a proxy area	√	x

Operation	AOM FullAccess	AOM Viewer
Deleting a proxy area	√	x
Creating a proxy area	√	x
Querying all proxies in a proxy area	√	√
Querying all proxy areas	√	√
Querying the Agent installation result	√	√
Obtaining the Agent installation command of a host	√	√
Obtaining the host heartbeat and checking whether the host is connected with the server	√	√
Uninstalling running Agents in batches	√	x
Querying the Agent home page	√	√
Testing the connectivity between the installation host and the target host	√	x
Installing Agents in batches	√	x
Obtaining the latest operation log of the Agent	√	√

Operation	AOM FullAccess	AOM Viewer
Obtaining the list of versions that can be selected during Agent installation	√	√
Obtaining the list of all Agent versions under the current project ID	√	√
Deleting hosts with Agents installed	√	x
Querying Agent information based on the ECS ID	√	√
Deleting a host with an Agent installed	√	x
Setting an installation host	√	x
Resetting installation host parameters	√	x
Querying the list of hosts that can be set to installation hosts	√	√
Querying the list of Agent installation hosts	√	√
Deleting an installation host	√	x
Upgrading Agents in batches	√	x
Querying historical task logs	√	√
Querying historical task details	√	√

Operation	AOM FullAccess	AOM Viewer
Querying all historical tasks	√	√
Querying all execution statuses and task types	√	√
Querying the Agent execution statuses in historical task details	√	√
Modifying a proxy	√	x
Deleting a proxy	√	x
Setting a proxy	√	x
Querying the list of hosts that can be set to proxies	√	√
Updating plug-ins in batches	√	x
Uninstalling plug-ins in batches	√	x
Installing plug-ins in batches	√	x
Querying historical task logs of a plug-in	√	√
Querying all plug-in execution records	√	√
Querying plug-in execution records based on the task ID	√	√
Querying the plug-in execution statuses in historical task details	√	√
Obtaining the plug-in list	√	√

Operation	AOM FullAccess	AOM Viewer
Querying the plug-in version	√	√
Querying the list of supported plug-ins	√	√
Obtaining the CCE cluster list	√	√
Obtaining the Agent list of a CCE cluster	√	√
Installing ICAgent on a CCE cluster	√	x
Upgrading ICAgent for a CCE cluster	√	x
Uninstalling ICAgent from a CCE cluster	√	x
Obtaining the CCE cluster list	√	√
Obtaining the list of hosts where the ICAgent has been installed	√	√
Installing ICAgent on CCE cluster hosts	√	x
Upgrading ICAgent on CCE cluster hosts	√	x
Uninstalling ICAgent from CCE cluster hosts	√	x

Fine-grained Permissions

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 about fine-grained permissions of AOM, see [Table 1-14](#).

Table 1-14 Fine-grained permissions of AOM

Permission	Description	Permission Dependency	Application Scenario
aom:cmdbApplication:get	Obtaining the details of an application	N/A	Obtaining the details of an application based on the application ID or name
aom:cmdbApplication:update	Modifying an application		Modifying an application
aom:cmdbApplication:delete	Deleting an application		Deleting an application
aom:cmdbApplication:get	Obtaining the details of an application		Obtaining the details of an application
aom:cmdbComponent:get	Querying the details of a component		Querying the details of a component based on the component ID or name
aom:cmdbComponent:create	Adding a component		Adding a component
aom:cmdbComponent:update	Updating a component		Updating a component
aom:cmdbComponent:delete	Deleting a component		Deleting a component
aom:cmdbComponent:move	Transferring a component		Transferring a component
aom:cmdbComponent:list	Querying the component list		Querying the component list
aom:cmdbEnvironment:create	Creating an environment		Creating an environment
aom:cmdbEnvironment:update	Modifying an environment		Modifying an environment
aom:cmdbEnvironment:get	Obtaining the details of an environment		Obtaining the details of an environment based on the environment name+region +component ID, or environment ID
aom:cmdbEnvironment:delete	Deleting an environment		Deleting an environment

Permission	Description	Permission Dependency	Application Scenario
aom:cmdbSubApplication:get	Querying the details of a sub-application		Querying the details of a sub-application
aom:cmdbSubApplication:update	Modifying a sub-application		Modifying a sub-application
aom:cmdbSubApplication:move	Transferring a sub-application		Transferring a sub-application
aom:cmdbSubApplication:delete	Deleting a sub-application		Deleting a sub-application
aom:cmdbSubApplication:create	Adding a sub-application		Adding a sub-application
aom:cmdbSubApplication:list	Querying the sub-application list		Querying the sub-application list
aom:cmdbResources:unbind	Unbinding a resource		Unbinding a resource
aom:cmdbResources:bind	Binding a resource		Binding a resource
aom:cmdbResources:move	Transferring a resource		Transferring a resource
aom:cmdbResources:get	Querying the details of a resource		Querying the details of a resource
aom:alarm:put	Reporting an alarm		Reporting a custom alarm
aom:event2AlarmRule:create	Adding an event alarm rule		Adding an event alarm rule
aom:event2AlarmRule:set	Modifying an event alarm rule		Modifying an event alarm rule
aom:event2AlarmRule:delete	Deleting an event alarm rule		Deleting an event alarm rule

Permission	Description	Permission Dependency	Application Scenario
aom:event2AlarmRule:list	Querying all event alarm rules		Querying all event alarm rules
aom:actionRule:create	Adding an alarm action rule		Adding an alarm action rule
aom:actionRule:delete	Deleting an alarm action rule		Deleting an alarm action rule
aom:actionRule:list	Querying the alarm action rule list		Querying the alarm action rule list
aom:actionRule:update	Modifying an alarm action rule		Modifying an alarm action rule
aom:actionRule:get	Querying an alarm action rule by name		Querying an alarm action rule by name
aom:alarm:list	Obtaining the sent alarm content		Obtaining the sent alarm content
aom:alarmRule:create	Creating a threshold rule		Creating a threshold rule
aom:alarmRule:set	Modifying a threshold rule		Modifying a threshold rule
aom:alarmRule:get	Querying threshold rules		Querying all threshold rules or a single threshold rule by rule ID
aom:alarmRule:delete	Deleting a threshold rule		Deleting threshold rules in batches or a single threshold rule by rule ID
aom:discoveryRule:list	Querying application discovery rules		Querying existing application discovery rules
aom:discoveryRule:delete	Deleting an application discovery rule		Deleting an application discovery rule
aom:discoveryRule:set	Adding an application discovery rule		Adding an application discovery rule

Permission	Description	Permission Dependency	Application Scenario
aom:metric:list	Querying time series objects		Querying time series objects
aom:metric:list	Querying time series data		Querying time series data
aom:metric:get	Querying metrics		Querying metrics
aom:metric:get	Querying monitoring data		Querying monitoring data
aom:muteRule:delete	Deleting a silence rule	N/A	Deleting a silence rule
aom:muteRule:create	Adding a silence rule		Adding a silence rule
aom:muteRule:update	Modifying a silence rule		Modifying a silence rule
aom:muteRule:list	Querying the silence rule list		Querying the silence rule list

Roles/Policies Required by AOM Dependent Services

If an IAM user needs to view data or use functions on the AOM console, grant the **AOM FullAccess** or **AOM ReadOnlyAccess** policy to the user group to which the user belongs and then add the roles or policies required by AOM dependent services by referring to [Table 1-15](#).

 **NOTE**

When a user subscribes to AOM for the first time, AOM will automatically create a service agency. In addition to the **AOM FullAccess** permission, the user must be granted the **Security Administrator** permission.

Table 1-15 Roles/Policies required by AOM dependent services

Console Function	Dependent Service	Policy/Role Required
<ul style="list-style-type: none"> Workload monitoring Cluster monitoring Prometheus for CCE 	CCE	<ul style="list-style-type: none"> To use workload and cluster monitoring, you need to set the CCE ReadOnlyAccess permission. To use Prometheus for CCE, you need to set the CCE FullAccess permission.

1.10 Privacy 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 Elastic Cloud Server (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.

Container Monitoring

For Cloud Container Engine (CCE) container monitoring, the AOM collector (ICAgent) must run as a privileged container. Evaluate the security risks of the privileged container and identify your container service scenarios. For example, for a node that provides services through logical multi-tenant container sharing, use open-source tools such as Prometheus to monitor the services and do not use ICAgent.

2 Getting Started

2.1 Subscribing to AOM 2.0

- Step 1** Log in to the management console.
 - Step 2** Click  in the upper left corner and select your desired region from the drop-down list.
 - Step 3** Click  on the left and choose **Management & Deployment > Application Operations Management**.
 - Step 4** In the navigation pane on the left, choose **AOM 2.0**. The AOM 2.0 page is displayed.
 - Step 5** On the notice dialog box that is displayed, read the billing changes for switching AOM 1.0 to AOM 2.0.
 - Step 6** Click **Authorize**. On the **Service Authorization** page that is displayed, read the *Authorization Statement* and select "I have read and agreed to the *Authorization Statement*".
 - Step 7** Click **Subscribe and Authorize for Free** for AOM 2.0.
 - Step 8** In the navigation tree on the left, click a function, for example, **Dashboard**.
- End

2.2 Managing Containers

This section describes how to use AOM to quickly manage containers on the **Overview** page, including container monitoring and alarm rule creation. The procedure is as follows:

1. **Monitoring Containers:** AOM is compatible with Kubernetes and automatically collects and reports container information.
2. **Setting an Alarm Rule:** Create metric alarm rules to ensure that notifications are sent when containers are abnormal.
3. **Setting an Alarm Action Rule:** Configure alarm action rules, for example, containers automatically restart when they become abnormal.

Monitoring Containers

Step 1 Log in to the AOM 2.0 console.

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

Step 3 Go to the **By Container** page.


Step 4 In the **Getting Started** area, click **Monitor Container**. The **Workload Monitoring** page is displayed.

Step 5 In the upper right corner of the page, set filter criteria.



1. Set a time range to view the workloads reported. There are two methods to set a time range:

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

Method 2: Specify the start time and end time (max. 30 days).

2. Set the interval for refreshing information. Click  and select a desired value from the drop-down list.

Step 6 Click any workload tab to view information, such as workload name, status, cluster, and namespace.

- In the upper part of the workload list, filter workloads by cluster, namespace, or pod name.
- Click  in the upper right corner to obtain the latest workload information.
- Click  in the upper right corner and select or deselect the columns to display.
- Click the name of a workload to view its details.
 - On the **Pods** tab page, view all pod conditions of the workload. Click a pod name to view the resource usage and health status of the pod's containers.
 - On the **Monitoring Views** tab page, view the resource usage of the workload.
 - On the **Alarms** tab page, view the alarm details of the workload.
 - On the **Events** tab page, view the event details of the workload.

----End

Setting an Alarm Rule

Metric alarm rules can be created in three modes: **Select by resource type**, **Select from all metrics**, and **PromQL**.

The following uses **Select from all metrics** as an example.

Step 1 On the **Overview** page, switch to **By Container**.

Step 2 In the **Getting Started** area, click **Set Alarm Rule**. The **Alarm Rules** page is displayed.

Step 3 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 256 characters and do not start or end with any special character. Only letters, digits, underscores (_), and hyphens (-) are allowed.
Enterprise Project	Enterprise project. <ul style="list-style-type: none"> If you have selected All for Enterprise Project on the global settings page, select one from the drop-down list here. If you have already selected an enterprise project on the global settings page, this option will be grayed and cannot be changed. <p>NOTE To use the enterprise project function, contact engineers.</p>
Description	Description of the rule. Enter up to 1,024 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**.
3. Select a target Prometheus instance from the drop-down list.
4. Set alarm rule details. [Table 2-2](#) describes the parameters.

After the setting is complete, the monitored metric data is displayed in a line graph above the alarm condition. Click the line icon before each metric data record to hide the metric data in the graph. You can click **Add Metric** to add metrics and set the statistical period and detection rules for the metrics.

After moving the cursor to the metric data and the corresponding alarm condition, you can perform the following operations as required:






- Click  next to an alarm condition to hide the corresponding metric data record in the graph.
- Click  next to an alarm condition to convert the metric data and alarm condition into a Prometheus command.
- Click  next to an alarm condition to quickly copy the metric data and alarm condition and modify them as required.
- Click  next to an alarm condition to remove a metric data record from monitoring.

Table 2-2 Alarm rule details

Parameter	Description
Multiple Metrics	<p>Calculation is performed based on the preset alarm conditions one by one. An alarm is triggered when one of the conditions is met.</p> <p>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.</p>
Combined Operations	<p>The system performs calculation based on the expression you set. If the condition is met, an alarm will be triggered.</p> <p>For example, if there is no metric showing the CPU core usage of a host, do as follows:</p> <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 Rule to Max > 0.2. - In the trigger condition, set Consecutive Periods to 3. - Set Alarm Severity to Critical. <p>If the maximum CPU core usage of a host is greater than 0.2 for three consecutive periods, a critical alarm will be generated.</p>
Metric	<p>Metric to be monitored. When Select from all metrics is selected, enter keywords to search for metrics.</p> <p>Click the Metric text box. In the resource tree on the right, you can also select a target metric by resource type.</p>
Statistical Period	<p>Metric data is aggregated based on the configured statistical period, which can be 1 minute, 5 minutes, 15 minutes, or 1 hour.</p>



Parameter	Description
Condition	<p>Metric monitoring scope. If this parameter is left blank, all resources are covered.</p> <p>Each condition is in a key-value pair. You can select a dimension name from the drop-down list. The dimension value varies according to the matching mode.</p> <ul style="list-style-type: none"> - =: Select a dimension value from the drop-down list. For example, if Dimension Name is set to Host name and Dimension Value is set to 192.168.16.4, only host 192.168.16.4 will be monitored. - !=: Select a dimension value from the drop-down list. For example, if Dimension Name is set to Host name and Dimension Value is set to 192.168.16.4, all hosts excluding host 192.168.16.4 will be monitored. - =~: The dimension value is determined based on one or more regular expressions. Separate regular expressions by vertical bar (). For example, if Dimension Name is set to Host name and Regular Expression is set to 192.* 172.*, only hosts whose names are 192.* and 172.* will be monitored. - !~: The dimension value is determined based on one or more regular expressions. Separate regular expressions by vertical bar (). For example, if Dimension Name is set to Host name and Regular Expression is set to 192.* 172.*, all hosts excluding hosts 192.* and 172.* will be monitored. <p>For details about how to enter a regular expression, see Regular Expression Examples.</p> <p>You can also click  and select AND or OR to add more conditions for the metric.</p>
Grouping Condition	<p>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.</p>
Rule	<p>Detection rule of a metric alarm, which consists of the statistical mode (Avg, Min, Max, Sum, and Samples), determination criterion (\geq, \leq, $>$, and $<$), and threshold value. For example, if the detection rule is set to Avg >10, a metric alarm will be generated if the average metric value is greater than 10.</p>

Parameter	Description
Trigger Condition	When the metric value meets the alarm condition for a specified number of consecutive periods, a metric alarm will be generated. Range: 1 to 30. For example, if Consecutive Periods is set to 2 , a metric alarm will be triggered if the trigger condition is met for two consecutive periods.
Alarm Severity	Severity of a metric alarm. Options: Critical , Major , Minor , and Warning .

Step 6 Click **Advanced Settings** and set information such as **Check Interval** and **Alarm Clearance**. For details about the parameters, see [Table 2-3](#).

Table 2-3 Advanced settings

Parameter	Description
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.
Alarm Clearance	The alarm will be cleared when the alarm condition is not met for a specified number of consecutive periods. By default, metrics in only one period are monitored. You can set up to 30 consecutive monitoring periods. For example, if Consecutive Periods is set to 2 , the alarm will be cleared when the alarm condition is not met for two consecutive periods.

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 consecutive 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 Previous status, and changing the status to Normal and sending an alarm clearance notification.</p>
Alarm Tag	<p>Click  to add an alarm tag. It is an alarm identification attribute in the format of "key:value". It is used in alarm noise reduction scenarios.</p> <p>For details, see Alarm Tags and Annotations.</p>
Alarm Annotation	<p>Click  to add an alarm annotation. Alarm non-identification attribute in the format of "key:value". It is used in alarm notification and message template scenarios.</p> <p>For details, see Alarm Tags and Annotations.</p>

Step 7 Set an alarm notification policy. For details, see [Table 2-4](#).

Table 2-4 Parameters for setting an alarm notification policy

Parameter	Description
Notify When	<p>Set the scenario for sending alarm notifications.</p> <ul style="list-style-type: none"> ● Alarm triggered: If the alarm trigger condition is met, the system sends an alarm notification to the specified personnel by email or SMS. ● Alarm cleared: If the alarm clearance condition is met, the system sends an alarm notification to the specified personnel by email or SMS.

Parameter	Description
Alarm Mode	<ul style="list-style-type: none"> Direct alarm reporting: An alarm is directly sent when the alarm condition is met. If you select this mode, set an interval for notification and specify whether to enable an action rule. Frequency: frequency for sending alarm notifications. Select a desired value from the drop-down list. If you enable this function, 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 in the drop-down list to create one. For details about how to set alarm action rules, see Setting an Alarm Action Rule. Alarm noise reduction: Alarms are sent only after being processed based on noise reduction rules, preventing alarm storms. If you select this mode, the silence rule is enabled by default. You can determine whether to enable Grouping Rule as required. If you enable this function, select a grouping rule from the drop-down list. If the existing grouping rules cannot meet your requirements, click Create Rule in the drop-down list to create one.

Step 8 Click **Confirm**. Then click **View Rule** 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 metric value meets the preset notification policy, the system sends an alarm notification to the specified personnel by email or SMS.

----End

Setting an Alarm Action Rule

Step 1 Go to the **By Container** page.

Step 2 In the **Getting Started** area, click **Set Alarm Action Rule**. The **Alarm Action Rules** page is displayed.

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 2-5](#).

Table 2-5 Parameters for creating an alarm action rule

Parameter	Description
Rule Name	Name of an action rule. Enter up to 100 characters and do not start or end with an underscore (_) or hyphen (-). Only digits, letters, underscores, and hyphens are allowed.

Parameter	Description
Enterprise Project	<p>Enterprise project.</p> <ul style="list-style-type: none"> If you have selected All for Enterprise Project on the global settings page, select one from the drop-down list here. If you have already selected an enterprise project on the global settings page, this option will be grayed and cannot be changed. <p>NOTE To use the enterprise project function, contact engineers.</p>
Description	Description of the action rule. Enter up to 1,024 characters.
Action Type	Type of an alarm action rule. Only Metric/Event is supported.
Action	Type of action that is associated with the SMN topic and message template. Select one from the drop-down list. 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 no proper message template is available, click Create Template to create a message template.

Step 5 Click **OK**.

----End

3 Introduction

Application Operations Management (AOM) is a one-stop, multi-dimensional O&M management platform for cloud applications. It provides one-stop observability analysis and automated O&M solutions. By collecting metrics, logs, and performance data from the cloud and local devices, AOM enables you to monitor real-time running status of applications, resources, and services and detect faults in a timely manner, improving O&M automation capability and efficiency.

Table 3-1 Function description

Category	Description
Overview	Provides quick entries to common services or functions from the container perspective, and monitors and displays key resource or application data in real time.
Access center	At the access center, you can quickly connect multi-dimensional metrics at different layers in various scenarios. After the connection is complete, you can view the usage of metrics and status of related resources or applications on the Metric Browsing page.
Dashboard	With a dashboard, different resource data graphs can be displayed on the same screen. Various graphs (such as line graphs, digit graphs, and status graphs) help you monitor data comprehensively.

Category	Description
Alarm management	<p>Provides the alarm list, event list, alarm rules, alarm templates, and alarm notifications.</p> <ul style="list-style-type: none"> ● Alarm list 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 alarm list displays the alarms generated within a specified time range. ● Event list Events generally carry some important information, informing you of the changes of AOM or an external service. Such changes do not necessarily cause exceptions. The event list displays the events generated within a specified time range. ● Alarm rules By setting alarms 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. 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. ● Alarm templates An alarm template is a combination of alarm rules based on cloud services. You can use an alarm template to create threshold alarm rules, event alarm rules, or PromQL alarm rules for multiple metrics of one cloud service in batches. ● Alarm notification AOM supports alarm notification. You can configure alarm notification by creating alarm action rules and noise reduction rules. When an alarm is generated due to an exception in AOM or an external service, the alarm information is sent to specified personnel by email or Short Message Service (SMS). In this way, related personnel can take measures to rectify faults in a timely manner to avoid service loss.

Category	Description
Metric analysis	<p>Provides metric browsing, Prometheus monitoring, and resource usage.</p> <ul style="list-style-type: none"> 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. Resource usage After metric data is reported to AOM through Prometheus monitoring, you can view the number of reported basic and custom metric samples on the Resource Usage page.
Log analysis (beta)	<p>Supports log search.</p> <p>AOM enables you to quickly query logs, and locate faults based on log sources and contexts.</p>
Container insights	<p>Monitors workloads and clusters.</p> <ul style="list-style-type: none"> Workload monitoring Workloads deployed on CCE are monitored. Therefore, you can understand the resource usage, status, and alarms of workloads in a timely manner. Cluster monitoring Clusters deployed using CCE are monitored. The Cluster Monitoring page displays the pod status and CPU usage of the clusters in real time.
Infrastructure monitoring	<p>Provides host monitoring.</p> <ul style="list-style-type: none"> Host monitoring Host monitoring displays resource usage, trends, and alarms, so that you can quickly respond to malfunctioning hosts and handle errors to ensure smooth host running.

Category	Description
Process monitoring	<p>Provides application and component monitoring, and application discovery.</p> <ul style="list-style-type: none"> • Application monitoring An application groups identical or similar components based on service requirements. • Component monitoring Components refer to the services that you deploy, including containers and common processes. • Application discovery AOM can discover applications and collect their metrics based on configured rules.
Collection management	<p>Centrally manages the life cycle of collection plug-ins and delivers instructions (such as script delivery and execution). UniAgent does not collect data; instead, collection plug-ins do that.</p>
Management	<p>Provides global configuration.</p> <ul style="list-style-type: none"> • Global configuration Includes cloud service authorization, access management, and global settings.

Going Back to AOM 1.0

On any page of AOM 2.0, click **Back to 1.0** in the navigation pane to go back to AOM 1.0. For details about AOM 1.0, see [AOM 1.0 User Guide](#).

Enterprise Project

An enterprise project can contain one or more applications.

Log in to the AOM 2.0 console. In the enterprise project drop-down list in the navigation pane, select a desired enterprise project.

NOTE

To use the enterprise project function, contact engineers.

4 Access Center

At the access center, you can quickly connect metrics to monitor. After the connection is complete, you can view the usage of metrics and status of related resources or applications on the [Metric Browsing](#) page.

Environment Access

This function enables CCE and CCI container metrics, and ECS metrics to be reported to AOM.

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Access Center**.

Step 3 In the **Environments** panel, click a target card.

- Click the **Cloud Container Engine (CCE) (Prometheus) (New)** card. On the displayed page, connect the metric data collected using the Prometheus add-on installed on the CCE cluster to AOM. For details, see [7.2.1.2 Prometheus Instance for CCE](#).
- By default, an ICAgent is installed when you purchase a CCE cluster. The ICAgent automatically reports CCE cluster metrics to AOM.
Click the **Cloud Container Engine (CCE) (ICAgent) (Old)** card to view the connected CCE cluster metrics.
- CCI automatically reports metrics to AOM as ready-to-use data. No manual configuration is required.
Click the **Cloud Container Instance (CCI)** card to view the connected CCI metrics.
- Click the **ECS ICAgent (Old)** card. On the **Collection Management** page, click [Install UniAgent](#) to install the UniAgent on the ECS.
After the UniAgent is installed, ECS metrics are automatically reported to AOM.

----End

Connecting Cloud Services

Connect cloud service metrics, such as the CPU usage, memory usage, and health status.

- Step 1** Log in to the AOM 2.0 console.
 - Step 2** In the navigation pane, choose **Access Center**.
 - Step 3** In the **Cloud Services** panel, click a target cloud service card.
 - Step 4** In the displayed dialog box, select a target cloud service and click **Confirm** to connect the cloud service metrics to the created **Prometheus instance for cloud services**.
- End

Open-Source Monitoring System Access

This function is suitable for customers who have self-built Prometheus servers, but need Prometheus storage availability and scalability through remote write.

- Step 1** Log in to the AOM 2.0 console.
 - Step 2** In the navigation pane, choose **Access Center**.
 - Step 3** In the **Open Source Monitoring** panel, click the **Prometheus for Remote Write** card.
 - Step 4** In the displayed dialog box, **create a Prometheus instance for remote write**.
- End

API/SDK Access

Connect metric data using APIs.

5 Dashboard

5.1 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 addition, you can add routine O&M metrics to a dashboard so that you can perform routine checks without re-selecting metrics when you open AOM again.

Precautions

- Preset dashboard templates are listed under **System**, including the container, cloud service, native middleware, and application templates. Preset dashboards cannot be deleted. Their groups cannot be changed. Dashboard templates cannot be created.
- Up to 1,000 dashboard groups can be created in a region.
- Up to 1,000 dashboards can be created in a region.
- A maximum of 30 graphs can be added to a dashboard.
- A maximum of 200 metric data records can be displayed in 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.

Creating a Dashboard

Step 1 Log in to the AOM 2.0 console.

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 5-1 Parameters for creating a dashboard

Parameter	Description
Dashboard Name	Name of a dashboard.
Enterprise Project	Enterprise project. <ul style="list-style-type: none"> If you have selected All for Enterprise Project on the global settings page, select one from the drop-down list here. If you have already selected an enterprise project on the global settings page, this option will be grayed and cannot be changed. <p>NOTE To use the enterprise project function, contact engineers.</p>
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

After a dashboard is created, you can add graphs to the dashboard:

Step 1 In the dashboard list, locate the target dashboard.

Step 2 Go to the dashboard page, and select the Prometheus instance for which you want to add a graph from the drop-down list.

Step 3 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 [5.4 Graph Description](#). The data can be metric. Select a graph as required.

- Add a metric graph. Set parameters by referring to [Table 5-2](#). Then click **Save**.

Table 5-2 Adding a metric graph

Parameter	Description
Graph Name	Name of a graph to distinguish it from other graphs.

Parameter	Description
Data Source	Click Metric Sources and select metric data as the source.
Graph Type	Options: line, digit, top N, table, bar, and digital line.
Metric List	<p>Add metrics as required. There are two ways to add metrics:</p> <ul style="list-style-type: none"> – All metrics: Select desired metrics from all metrics. When you select metrics in this mode, you can only enter English keywords to search and only English content is displayed. – Prometheus statement: Enter a Prometheus command and select your target metric. For details, see 14.2 Prometheus Statements. <p>Click Add Metric to add up to 100 metric data records.</p> <p>NOTE</p> <ul style="list-style-type: none"> – When All metrics is selected, enter keywords to search for metrics. – Condition: Metric monitoring scope. The condition is in the key-value pair format. Directly select an option from the drop-down list or use AND and OR to specify conditions 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	On the right of the page, click the down arrow, select a desired graph type from the drop-down list, and set graph parameters (such as the X axis title, Y axis title, and displayed value). For details about the parameters, see 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 .





Step 4 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 5-3](#).

Table 5-3 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.
Moving dashboards to another group	<ul style="list-style-type: none"> • Moving a dashboard: Locate a dashboard and choose ... > Move Group in the Operation column. • Moving dashboards in batches: Select dashboards to move. In the displayed dialog box, click Move Group.
Deleting a dashboard	<ul style="list-style-type: none"> • Deleting a dashboard: Locate a dashboard and choose ... > Delete in the Operation column. • Deleting dashboards in batches: Select dashboards to delete. In the displayed dialog box, click Delete.
Changing a dashboard group name	<ol style="list-style-type: none"> 1. In the dashboard list, click a dashboard name. 2. Go to the dashboard page and click a dashboard name in the upper left corner. 3. Move the cursor to the target dashboard group and choose ⋮ > Modify to change the group name.
Deleting a dashboard group	<p>You can delete a dashboard using either of the following methods:</p> <p>Method 1:</p> <ol style="list-style-type: none"> 1. In the dashboard list, click a dashboard name. 2. Go to the dashboard page and click a dashboard name in the upper left corner. 3. Move the cursor to the target dashboard group and choose ⋮ > Delete. 4. In the displayed dialog box, click OK. <p>Method 2: In the dashboard group list, locate the target dashboard group and choose ... > Delete. In the displayed dialog box, click Yes to delete the dashboard group.</p>
Deleting a graph from a dashboard	<ol style="list-style-type: none"> 1. Click the target dashboard, click  in the upper right corner of the dashboard page, move the cursor to the upper right corner of a graph, and choose ⋮ > Delete. 2. Click  to save the setting.

Operation	Description
Relocating a graph on a dashboard	<ol style="list-style-type: none"> 1. Click 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. 2. Click  to save the setting.
Full-screen display	Click 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	Click the target dashboard and click  in the upper right corner of the dashboard page and manually refresh the current page.
Auto refresh	Click the target dashboard and click the arrow next to  in the upper right corner of the dashboard page and enable auto refresh.
Manually refreshing a graph	Click the target dashboard, move the cursor to the upper right corner of a graph, and choose  > Refresh to manually refresh the graph.
Modifying a graph	<ol style="list-style-type: none"> 1. Click the target dashboard, move the cursor to the upper right corner of a graph, 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 setting.
Adding alarm rules	<ul style="list-style-type: none"> • Adding an alarm rule when adding a graph <ol style="list-style-type: none"> 1. Click Add Graph on the page or click  in the upper right corner of the page. 2. After selecting a metric, click  in the upper right corner of the metric list to add an alarm rule for the metric. For details, see 6.1.2 Creating a Metric Alarm Rule. • Adding an alarm rule when modifying a graph <ol style="list-style-type: none"> 1. Locate a target dashboard, move the cursor to the upper right corner of a graph, and choose  > Modify. 2. After selecting a metric, click  in the upper right corner of the metric list to add an alarm rule for the metric. For details, see 6.1.2 Creating a Metric Alarm Rule.
Displaying a graph in full screen	Click the target dashboard, move the cursor to the upper right corner of a graph, and choose  > Full Screen .

Operation	Description
Exiting the full-screen mode	Move the cursor to the upper part of the screen and click  , or choose  > Exit Full Screen , 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 details page. Set full-screen display by referring to 5.2 Setting the Full-Screen Online Duration .
Setting a dashboard	Click a target dashboard and click  in the upper right corner of the dashboard details page. For details, see 5.3 Adding Variables .
Setting the query time	Select the target dashboard. In the upper right corner of the dashboard page, click the time range 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 a time range 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 dashboard	Export the metric graph data of a dashboard in JSON format and save it to your local PC for further analysis. You can export a dashboard using either of the following methods: Method 1: In the dashboard list, locate a dashboard, and choose  > Export Dashboard in the Operation column. Method 2: Click a dashboard to go to its details page and choose  > Export Dashboard in the upper right corner.
Importing a dashboard	Import the dashboard data in JSON format from a local PC to AOM for analysis. You can import a dashboard using either of the following methods: Method 1: On the Dashboard page, click Import Dashboard . Method 2: In the dashboard group list, locate the group to which the dashboard is to be imported, and choose  > Import Dashboard . Procedure: 1. Select the JSON dashboard file to be imported, upload it or drag it to the upload area in the Import Dashboard dialog box, and then click OK . 2. In the dialog box that is displayed, set information such as the dashboard name by referring to Table 5-1 . 3. Click OK .
Exporting a monitoring report	Click a dashboard to go to its details page. Then click  in the upper right corner, and choose Export Line Graph Report to export a CSV file to your local PC.

5.2 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 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** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane, choose **Dashboard**.
- Step 3** Click a target dashboard and click  in the upper right corner of the dashboard details page.
- Step 4** In the dialogue box that is displayed, set the full-screen online duration. For details, see [Table 5-4](#).

Table 5-4 Online duration parameters

Parameter	Description
Online Setting	Mode of setting the online duration. Options: <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.
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


5.3 Adding Variables

You can add variables to customize filters when viewing or adding graphs on the **Dashboard** page.

Procedure

Step 1 Log in to the AOM 2.0 console.

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

Step 3 Select a desired dashboard and click  in the upper right corner of the **Dashboard** page. The **Variable Settings** page is displayed.

Step 4 Click **Add Variable** and set parameters by referring to [Table 5-5](#).

Table 5-5 Parameters for adding variables

Parameter	Description
Variable Name	Name of a variable. Enter up to 255 characters and do not start or end with an underscore (_). Only digits, letters, and underscores are allowed.
Type	Type of the variable. Only Query is supported.
Alias	Alias of the variable. Enter up to 255 characters and do not start or end with an underscore (_) or hyphens (-). Only digits, letters, hyphens, and underscores are allowed. If you set an alias, it will be preferentially displayed.
Description	Description of the variable.
Data Source	Source of the data. Select a data source on the Dashboard page. It is dimmed here and cannot be selected. You can select a default or custom Prometheus instance. By default, the default Prometheus instance is selected. Options: Prometheus instance for cloud services, ECS, CCE, remote write, or multi-account aggregation, or the default Prometheus instance.
Refresh Mode	Filter refresh mode. Only On dashboard load is supported, which means refreshing filters when your dashboard is refreshed.
Metric	Name of a metric. You can select metrics of the selected Prometheus instance.
Display Field	Displayed in a filter drop-down list on a dashboard.
Value	Value of the display field.
Conditions	Dimension name and value. You can set multiple conditions for the same metric.
Allow multiple values	Whether multiple values can be selected. By default, this function is disabled. If it is enabled, you can select multiple values for your custom filter.
Include "All"	Whether the All option is available. By default, this function is disabled. If it is enabled, the All option will be added for your custom filter.

Step 5 Click **Save** to add the variable.




The new variable will be displayed as a filter on the dashboard page and the page for adding a graph. You can click the filter and select a desired value from the drop-down list.

----End

More Operations

After the variable is added, you can perform the operations listed in [Table 5-6](#) if needed.

Table 5-6 Related operations

Parameter	Description
Searching for a variable	You can search for variables by name. Enter a keyword in the search box above the variable list and click  to search.
Editing a variable	Click  in the Operation column of the target variable. For details, see Table 5-5 .
Deleting a variable	Click  in the Operation column of the target variable. In the displayed dialog box, click Yes .

5.4 Graph Description

The dashboard displays the query and analysis results of metric 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 5-7 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.
Advanced Settings	Left Margin	Distance between the axis and the left boundary of the graph.

Category	Parameter	Description
	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 5-8 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.

- **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 5-9 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: % .
-	Display X-Axis Scale	After this function is enabled, the scale of the X axis is displayed.

Category	Parameter	Description
-	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 5-10 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.

In the following figure, you can view the CPU usage of different hosts.

Table 5-11 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 5-12 Digital line graph parameters

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 Markers	Whether to display the connection points.

6 Alarm Management

6.1 Alarm Rules

6.1.1 Overview

AOM allows you to set alarm rules. With alarm rules, you can set event conditions for services, or set 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 the environment 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 1,000. If the number of alarm rules has reached the upper limit, delete unnecessary rules and create new ones.

6.1.2 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 statistical period, detection rules, and trigger conditions for alarm rules. For details, see [Step 5](#).
- You can configure alarm notifications. For details, see [Step 7](#).

Creation Mode

There are the following configuration modes for you to create metric alarm rules: [Select from all metrics](#) and [PromQL](#).

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 [6.5.2 Creating an Alarm Action Rule](#).

Creating Metric Alarm Rules by Selecting Metrics from All Metrics

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane, choose **Alarm Management** > **Alarm Rules**.
- Step 3** Click **Create Alarm Rule**.
- Step 4** Set basic information about the alarm rule by referring to [Table 6-1](#).

Table 6-1 Basic information



Parameter	Description
Rule Name	Name of a rule. Enter a maximum of 256 characters and do not start or end with any special character. Only letters, digits, underscores (_), and hyphens (-) are allowed.
Enterprise Project	Enterprise project. <ul style="list-style-type: none"> • If you have selected All for Enterprise Project on the global settings page, select one from the drop-down list here. • If you have already selected an enterprise project on the global settings page, this option will be grayed and cannot be changed. <p>NOTE To use the enterprise project function, contact engineers.</p>
Description	Description of the rule. Enter up to 1,024 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**.
3. Select a target Prometheus instance from the drop-down list.
4. Set alarm rule details. [Table 6-2](#) describes the parameters.

After the setting is complete, the monitored metric data is displayed in a line graph above the alarm condition. Click the line icon before each metric data record to hide the metric data in the graph. You can click **Add Metric** to add metrics and set the statistical period and detection rules for the metrics.

After moving the cursor to the metric data and the corresponding alarm condition, you can perform the following operations as required:

- Click  next to an alarm condition to hide the corresponding metric data record in the graph.
- Click  next to an alarm condition to convert the metric data and alarm condition into a Prometheus command.




- Click  next to an alarm condition to quickly copy the metric data and alarm condition and modify them as required.
- Click  next to an alarm condition to remove a metric data record from monitoring.

Table 6-2 Alarm rule details

Parameter	Description
Multiple Metrics	<p>Calculation is performed based on the preset alarm conditions one by one. An alarm is triggered when one of the conditions is met.</p> <p>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.</p>
Combined Operations	<p>The system performs calculation based on the expression you set. If the condition is met, an alarm will be triggered.</p> <p>For example, if there is no metric showing the CPU core usage of a host, do as follows:</p> <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 Rule to Max > 0.2. - In the trigger condition, set Consecutive Periods to 3. - Set Alarm Severity to Critical. <p>If the maximum CPU core usage of a host is greater than 0.2 for three consecutive periods, a critical alarm will be generated.</p>
Metric	<p>Metric to be monitored. When Select from all metrics is selected, enter keywords to search for metrics.</p> <p>Click the Metric text box. In the resource tree on the right, you can also select a target metric by resource type.</p>
Statistical Period	<p>Metric data is aggregated based on the configured statistical period, which can be 1 minute, 5 minutes, 15 minutes, or 1 hour.</p>



Parameter	Description
Condition	<p>Metric monitoring scope. If this parameter is left blank, all resources are covered.</p> <p>Each condition is in a key-value pair. You can select a dimension name from the drop-down list. The dimension value varies according to the matching mode.</p> <ul style="list-style-type: none"> - =: Select a dimension value from the drop-down list. For example, if Dimension Name is set to Host name and Dimension Value is set to 192.168.16.4, only host 192.168.16.4 will be monitored. - !=: Select a dimension value from the drop-down list. For example, if Dimension Name is set to Host name and Dimension Value is set to 192.168.16.4, all hosts excluding host 192.168.16.4 will be monitored. - =~: The dimension value is determined based on one or more regular expressions. Separate regular expressions by vertical bar (). For example, if Dimension Name is set to Host name and Regular Expression is set to 192.* 172.*, only hosts whose names are 192.* and 172.* will be monitored. - !~: The dimension value is determined based on one or more regular expressions. Separate regular expressions by vertical bar (). For example, if Dimension Name is set to Host name and Regular Expression is set to 192.* 172.*, all hosts excluding hosts 192.* and 172.* will be monitored. <p>For details about how to enter a regular expression, see Regular Expression Examples.</p> <p>You can also click  and select AND or OR to add more conditions for the metric.</p>
Grouping Condition	<p>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.</p>
Rule	<p>Detection rule of a metric alarm, which consists of the statistical mode (Avg, Min, Max, Sum, and Samples), determination criterion (\geq, \leq, $>$, and $<$), and threshold value. For example, if the detection rule is set to Avg >10, a metric alarm will be generated if the average metric value is greater than 10.</p>

Parameter	Description
Trigger Condition	When the metric value meets the alarm condition for a specified number of consecutive periods, a metric alarm will be generated. Range: 1 to 30. For example, if Consecutive Periods is set to 2 , a metric alarm will be triggered if the trigger condition is met for two consecutive periods.
Alarm Severity	Severity of a metric alarm. Options: Critical , Major , Minor , and Warning .

Step 6 Click **Advanced Settings** and set information such as **Check Interval** and **Alarm Clearance**. For details about the parameters, see [Table 6-3](#).

Table 6-3 Advanced settings

Parameter	Description
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.
Alarm Clearance	The alarm will be cleared when the alarm condition is not met for a specified number of consecutive periods. By default, metrics in only one period are monitored. You can set up to 30 consecutive monitoring periods. For example, if Consecutive Periods is set to 2 , the alarm will be cleared when the alarm condition is not met for two consecutive periods.

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 consecutive 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 Previous status, and changing the status to Normal and sending an alarm clearance notification.</p>
Alarm Tag	<p>Click  to add an alarm tag. It is an alarm identification attribute in the format of "key:value". It is used in alarm noise reduction scenarios.</p> <p>For details, see Alarm Tags and Annotations.</p>
Alarm Annotation	<p>Click  to add an alarm annotation. Alarm non-identification attribute in the format of "key:value". It is used in alarm notification and message template scenarios.</p> <p>For details, see Alarm Tags and Annotations.</p>

Step 7 Set an alarm notification policy. For details, see [Table 6-4](#).

Table 6-4 Parameters for setting an alarm notification policy

Parameter	Description
Notify When	<p>Set the scenario for sending alarm notifications.</p> <ul style="list-style-type: none"> ● Alarm triggered: If the alarm trigger condition is met, the system sends an alarm notification to the specified personnel by email or SMS. ● Alarm cleared: If the alarm clearance condition is met, the system sends an alarm notification to the specified personnel by email or SMS.

Parameter	Description
Alarm Mode	<ul style="list-style-type: none"> Direct alarm reporting: An alarm is directly sent when the alarm condition is met. If you select this mode, set an interval for notification and specify whether to enable an action rule. Frequency: interval for sending alarm notifications. Select a desired value from the drop-down list. <p>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 in the drop-down list to create one. For details, see Creating an Alarm Action Rule.</p> <ul style="list-style-type: none"> Alarm noise reduction: Alarms are sent only after being processed based on noise reduction rules, preventing alarm storms. <p>If you select this mode, the silence rule is enabled by default. You can determine whether to enable Grouping Rule as required. After this function is enabled, select a grouping rule from the drop-down list. If existing grouping rules cannot meet your requirements, click Create Rule in the drop-down list to create one. For details, see 6.6.2 Creating a Grouping Rule.</p>

Step 8 Click **Confirm**. Then click **View Rule** 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 metric value 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 Log in to the AOM 2.0 console.

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

Step 3 Click **Create Alarm Rule**.

Step 4 Set basic information about the alarm rule by referring to [Table 6-5](#).

Table 6-5 Basic information

Parameter	Description
Rule Name	Name of a rule. Enter a maximum of 256 characters and do not start or end with any special character. Only letters, digits, underscores (_), and hyphens (-) are allowed.


Parameter	Description
Enterprise Project	<p>Enterprise project.</p> <ul style="list-style-type: none"> If you have selected All for Enterprise Project on the global settings page, select one from the drop-down list here. If you have already selected an enterprise project on the global settings page, this option will be grayed and cannot be changed. <p>NOTE To use the enterprise project function, contact engineers.</p>
Description	Description of the rule. Enter up to 1,024 characters.

Step 5 Set the detailed information about the alarm rule.

- Set **Rule Type** to **Metric alarm rule**.
- Set **Configuration Mode** to **PromQL**.
- Select a target Prometheus instance from the drop-down list.
- Set alarm rule details. [Table 6-6](#) describes the parameters.

After the setting is complete, the monitored metric data is displayed in a line graph above the alarm condition. Click the line icon before each metric data record to hide the metric data in the graph.



Table 6-6 Alarm rule details

Parameter	Description
Default Rule	<p>Detection rule generated based on Prometheus statements. The system provides two input modes: Custom and CCEFromProm. After the input is complete, click Query. The corresponding graph will be displayed in the lower part of the page in real time.</p> <ul style="list-style-type: none"> Custom: If you have known the metric name and IP address and are familiar with the Prometheus statement format, select Custom from the drop-down list and manually enter a Prometheus command. CCEFromProm: used when you do not know the metric information or are unfamiliar with the Prometheus format. Select CCEFromProm from the drop-down list and then select a desired template from the CCE templates. The system then automatically fills in the Prometheus command based on the selected template. <p>You can click  to view examples. For details, see 14.2 Prometheus Statements.</p>
Alarm Severity	Severity of a metric alarm. Options: Critical , Major , Minor , and Warning .

Parameter	Description
Dimensions	Metric monitoring dimension, which is automatically generated based on the Prometheus statement you set.
Duration	A metric alarm will be triggered when the alarm condition is met for the specified duration. For example, if Duration is set to 2 minutes , a metric alarm will be triggered when the alarm condition is met for two minutes.

Step 6 Click **Advanced Settings** and set information such as **Check Interval** and **Alarm Clearance**. For details about the parameters, see [Table 6-7](#).

Table 6-7 Advanced settings

Parameter	Description
Check Interval	Interval at which metric query and analysis results are checked. <ul style="list-style-type: none"> • XX hours: Check the query and analysis results every XX hours. • XX minutes: Check the query and analysis results every XX minutes.
Alarm Tag	Alarm identification attribute in the format of "key:value". It is used in alarm noise reduction scenarios. It is automatically generated based on the Prometheus statement you set. You can modify it as required. To add more alarm tags, click  . For details, see 14.1 Alarm Tags and Annotations .
Alarm Annotation	Click  to add an alarm annotation. Alarm non-identification attribute in the format of "key:value". It is used in alarm notification and message template scenarios. For details, see 14.1 Alarm Tags and Annotations .

Step 7 Set an alarm notification policy. For details, see [Table 6-8](#).

Table 6-8 Parameters for setting an alarm notification policy

Parameter	Description
Notify When	<p>Set the scenario for sending alarm notifications.</p> <ul style="list-style-type: none"> • Alarm triggered: If the alarm trigger condition is met, the system sends an alarm notification to the specified personnel by email or SMS. • Alarm cleared: If the alarm clearance condition is met, the system sends an alarm notification to the specified personnel by email or SMS.
Alarm Mode	<ul style="list-style-type: none"> • Direct alarm reporting: An alarm is directly sent when the alarm condition is met. If you select this mode, set an interval for notification and specify whether to enable an action rule. Frequency: interval for sending alarm notifications. Select a desired value from the drop-down list. 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 in the drop-down list to create one. For details, see Creating an Alarm Action Rule. • Alarm noise reduction: Alarms are sent only after being processed based on noise reduction rules, preventing alarm storms. If you select this mode, the silence rule is enabled by default. You can determine whether to enable Grouping Rule as required. After this function is enabled, select a grouping rule from the drop-down list. If existing grouping rules cannot meet your requirements, click Create Rule in the drop-down list to create one. For details, see 6.6.2 Creating a Grouping Rule.
Notification Template	<p>Template for sending alarm notifications. It is automatically generated based on the Prometheus statement you set.</p>

Step 8 Click **Confirm**. Then click **View Rule** 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 metric value meets the preset notification policy, the system sends an alarm notification to the specified personnel by email or SMS.

----End

6.1.3 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 [6.5.2 Creating an Alarm Action Rule](#).

Procedure

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane, choose **Alarm Management > Alarm Rules**.
- Step 3** Click **Create Alarm Rule**.
- Step 4** Set basic information about the alarm rule by referring to [Table 6-9](#).

Table 6-9 Basic information

Parameter	Description
Rule Name	Name of a rule. Enter a maximum of 256 characters and do not start or end with any special character. Only letters, digits, underscores (_), and hyphens (-) are allowed.
Enterprise Project	Enterprise project. <ul style="list-style-type: none"> • If you have selected All for Enterprise Project on the global settings page, select one from the drop-down list here. • If you have already selected an enterprise project on the global settings page, this option will be grayed and cannot be changed. <p>NOTE To use the enterprise project function, contact engineers.</p>
Description	Description of the rule. Enter up to 1,024 characters.

- Step 5** Set the detailed information about the alarm rule.
 1. Set **Rule Type** to **Event alarm rule**.
 2. Specify an event type and source.
 - If **Event Type** is set to **System**, **Event Source** can only be **CCE** or **ModelArts**.
 - If **Event Type** to set to **Custom**, select an event source from the existing service list.
 3. Set alarm rule details.

Table 6-10 Alarm rule parameters

Parameter	Description
Monitored Object	<p>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.</p> <p>NOTE Set Event Name as the filter criterion. If no event name is selected, all events are selected by default.</p>
Alarm Condition	<p>Condition for triggering event alarms. It contains:</p> <ul style="list-style-type: none"> - Event Name: The value varies depending on Monitored Object. If you do not specify any event for Monitored Object, all events are displayed here and cannot be changed. - Trigger Mode: trigger mode of an event alarm. <ul style="list-style-type: none"> ▪ Accumulated Trigger: When the trigger condition is met for a specified number of times in a monitoring period, alarm notifications are sent based on the preset interval. Assume that you set Event Name to VolumeResizeFailed, Monitoring Period to 20 minutes, Cumulative Times to ≥ 3, and Alarm Frequency to Every 5 minutes. If data volume scale-out fails for 3 or more times within 20 minutes, an alarm notification will be sent every 5 minutes unless the alarm is cleared. <p>NOTICE If you have selected Alarm noise reduction when setting the alarm notification policy, the alarm frequency set here does not take effect. Alarm notifications are sent at the frequency set during noise reduction configuration.</p> <ul style="list-style-type: none"> ▪ Immediate Trigger: An alarm is immediately generated when the trigger condition is met. - Alarm Severity: includes Critical, Major, Minor, and Warning. <p>In case of multiple events, click Batch Set to set alarm conditions for these events in batches.</p>

Step 6 Set an alarm notification policy. There are two alarm notification modes. Select one as required.

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

Set whether to enable the alarm action rule as required. 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** in the drop-down list to create one. For details about how to set an alarm action rule, see [6.5.2 Creating an Alarm Action Rule](#).

- **Alarm noise reduction:** Alarms are sent only after being processed based on noise reduction rules, preventing alarm storms.
Select a grouping rule from the drop-down list. If existing grouping rules cannot meet your requirements, click **Create Rule** in the drop-down list to create one. For details, see [6.6.2 Creating a Grouping Rule](#).

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

When CCE resources meet the configured event alarm conditions, an event alarm will be generated on the alarm page. 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





6.1.4 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** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane, choose **Alarm Management > Alarm Rules**.
- Step 3** In the rule list, view all created alarm rules and perform the following operations as required. For details, see [Table 6-11](#).

Table 6-11 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 6.1.2 Creating a Metric Alarm Rule and 6.1.3 Creating an Event Alarm Rule .
Copying an alarm rule	Click  in the Operation column. For details, see 6.1.2 Creating a Metric Alarm Rule and 6.1.3 Creating an Event Alarm Rule .

Operation	Description
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 and click Delete in the displayed dialog box.
Enabling or disabling alarm rules	<ul style="list-style-type: none"> To enable or disable an alarm rule, turn on or off the button in the Status column. To enable or disable one or more alarm rules, select them and click Enable or Disable in the displayed dialog box.
Setting alarm notification policies in batches	Select one or more alarm rules of the same type. In the displayed dialog box, click Alarm Notification to set alarm notification policies in batches. Alarm notification policies vary depending on alarm rule types. For details, see Setting Alarm Notification Policies (1) or Setting Alarm Notification Policies (2) .
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.
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	<p>When the metric value of a resource meets threshold conditions during the configured consecutive periods, the system reports a threshold alarm.</p> <p>In the navigation pane, choose Alarm Management > Alarm List. On the Alarms tab page, view alarms. For details, see 6.3 Viewing Alarms.</p>
Viewing events	<p>When no metric data is reported during the configured consecutive periods, the system reports an insufficient data event.</p> <p>In the navigation pane, choose Alarm Management > Alarm List. On the Events tab page, view events. For details, see 6.4 Viewing Events.</p>

----End


6.2 Alarm Templates

An alarm template is a combination of alarm rules based on cloud services. You can use an alarm template to create threshold alarm rules, event alarm rules, or PromQL alarm rules for multiple metrics of one cloud service in batches.

Precautions

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

Background

AOM presets default alarm templates for key metrics (including CPU usage, physical memory usage, host status, and service status) of all hosts and services. They are displayed on the **Alarm Templates > Default** page. You can locate the desired default alarm template and click  in the **Operation** column to quickly customize your own alarm template.

Creating an Alarm Template

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane, choose **Alarm Management > Alarm Templates**.
- Step 3** Click **Create Alarm Template**.
- Step 4** Set the basic information about an alarm template. [Table 6-12](#) describes the parameters.

Table 6-12 Basic information

Parameter	Description
Template Name	Name of an alarm template. 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.
Enterprise Project	Enterprise project. <ul style="list-style-type: none"> • If you have selected All for Enterprise Project on the global settings page, select one from the drop-down list here. • If you have already selected an enterprise project on the global settings page, this option will be grayed and cannot be changed. <p>NOTE To use the enterprise project function, contact engineers.</p>
Description	Description of the template. Enter up to 1,024 characters.

- Step 5** Add a cloud service to be monitored and an alarm rule to the template.
 1. Select a desired cloud service from the drop-down list.
 2. Switch to your desired cloud service tab. Then add an alarm rule for the cloud service. For details, see [Table 6-13](#).

Table 6-13 Parameters for adding an alarm rule for the cloud service

Cloud Service	Alarm Rule Type	Method
FunctionGraph, DRS, RDS, NAT, VPC, DCS, CSS, DC, CBR, DMS, ELB, EVS, OBS, DDS, and WAF	Metric alarm rule	<ol style="list-style-type: none"> 1. Click Add Threshold Alarm Rule. 2. In the displayed dialog box, set the rule name, metric data, and alarm condition. For details, see Creating Metric Alarm Rules by Selecting Metrics from All Metrics. 3. Click OK.
CCEFromProm	Event alarm rule	See Step 6 .
	PromQL alarm rule	See Step 7 .

Step 6 (Optional) Add an event alarm rule for the CCEFromProm service.


1. Choose **Add Alarm Rule > Add Event Alarm Rule**.
2. In the displayed dialog box, set the rule name and event rule details. For details, see [Table 6-14](#).
 - You can click **Add Event** to add more events and set information such as the trigger mode and alarm severity for the events.
 - In case of multiple events, click **Batch Set** to set alarm conditions for these events in batches.
 - Click  next to the event details to copy them and then modify them as required.

Table 6-14 Event rule parameters

Parameter	Description
Rule Name	Enter a maximum of 256 characters and do not start or end with an underscore (_) or hyphen (-). Only letters, digits, underscores, and hyphens are allowed.
Event Name	Select a value from the drop-down list. By default, all events are selected.

Parameter	Description
Trigger Mode	<p>Trigger mode of an event alarm.</p> <ul style="list-style-type: none"> - Accumulated Trigger: When the trigger condition is met for a specified number of times in a monitoring period, alarm notifications are sent based on the preset interval. Assume that you set Event Name to VolumeResizeFailed, Monitoring Period to 20 minutes, Cumulative Times to 3, and Alarm Frequency to Every 5 minutes. If data volume scale-out fails three times within 20 minutes, an alarm notification will be sent every five minutes unless the alarm is cleared. - Immediate Trigger: An alarm is immediately generated when the trigger condition is met.
Alarm Severity	Severity of an event alarm. Options: Critical , Major , Minor , and Warning .



3. Click **OK**.

Step 7 (Optional) Add a PromQL alarm rule for the CCEFromProm service.

1. Choose **Add Alarm Rule > Add PromQL Alarm Rule**.
2. In the displayed dialog box, set the rule name, default rule, and alarm severity. For details, see [Table 6-15](#).

Table 6-15 PromQL alarm rule parameters

Parameter	Description
Rule Name	Enter a maximum of 256 characters and do not start or end with an underscore (_) or hyphen (-). Only letters, digits, underscores, and hyphens are allowed.
Default Rule	<p>Detection rule generated based on Prometheus statements. The system provides two input modes: Custom and CCEFromProm.</p> <ul style="list-style-type: none"> - Custom: If you have known the metric name and IP address and are familiar with the Prometheus statement format, select Custom from the drop-down list and manually enter a Prometheus command. - CCEFromProm: used when you do not know the metric information or are unfamiliar with the Prometheus format. Select CCEFromProm from the drop-down list and then select a desired template from the CCE templates. The system then automatically fills in the Prometheus command based on the selected template. <p>For details, see 14.2 Prometheus Statements.</p>
Alarm Severity	Severity of a metric alarm. Options: Critical , Major , Minor , and Warning .

Parameter		Description
Dimensions		Metric monitoring dimension, which is automatically generated based on the Prometheus statement you set.
Duration		A metric alarm will be triggered when the alarm condition is met for the specified duration. For example, if Duration is set to 2 minutes , a metric alarm will be triggered when the alarm condition is met for two minutes.
Advanced Settings	Check Interval	Interval at which metric query and analysis results are checked. <ul style="list-style-type: none"> - XX hours: Check the query and analysis results every <i>XX</i> hours. - XX minutes: Check the query and analysis results every <i>XX</i> minutes.
	Alarm Tag	Alarm identification attribute in the format of "key:value". It is used in alarm noise reduction scenarios. It is automatically generated based on the Prometheus statement you set. You can modify it as required. To add more alarm tags, click  . For details, see 14.1 Alarm Tags and Annotations .
	Alarm Annotation	Click  to add an alarm annotation. Alarm non-identification attribute in the format of "key:value". It is used in alarm notification and message template scenarios. For details, see 14.1 Alarm Tags and Annotations .
Notification Content		Alarm notification content. It is automatically generated based on the Prometheus statement you set.

3. Click **OK**.

Step 8 Click **OK** to create the alarm template.

Step 9 (Optional) In the displayed **Bind Alarm Template with Prometheus Instance/Cluster** dialog box, set the cluster or Prometheus instance to be bound with the alarm template. For details about the parameters, see [Table 6-16](#). After the setting is complete, click **OK**.

Table 6-16 Parameters for binding an alarm template

Parameter	Description
Instance	This parameter is optional. If the cloud services selected in Step 5.1 contain services other than CCEFromProm, this parameter will be displayed. The drop-down list displays all Prometheus instances for cloud services under your account. Select your desired instance.

Parameter	Description
Cluster	<p>This parameter is optional. If the cloud services selected in Step 5.1 contain CCEFromProm, this parameter will be displayed.</p> <p>The drop-down list displays all CCE clusters of your account. Select your desired cluster.</p>
Notify When	<p>Set the scenario for sending alarm notifications.</p> <ul style="list-style-type: none"> ● Alarm triggered: If the alarm trigger condition is met, the system sends an alarm notification to the specified personnel by email or SMS. ● Alarm cleared: If the alarm clearance condition is met, the system sends an alarm notification to the specified personnel by email or SMS.
Alarm Mode	<ul style="list-style-type: none"> ● Direct alarm reporting: An alarm is directly sent when the alarm condition is met. If you select this mode, set an interval for notification and specify whether to enable an action rule. Frequency: interval for sending alarm notifications. Select a desired value from the drop-down list. 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 in the drop-down list to create one. For details, see Creating an Alarm Action Rule. ● Alarm noise reduction: Alarms are sent only after being processed based on noise reduction rules, preventing alarm storms. If you select this mode, the silence rule is enabled by default. You can determine whether to enable Grouping Rule as required. After this function is enabled, select a grouping rule from the drop-down list. If existing grouping rules cannot meet your requirements, click Create Rule in the drop-down list to create one. For details, see 6.6.2 Creating a Grouping Rule.

Step 10 View the created alarm template on the **Custom** tab page.





If a resource or metric meets the alarm condition set in the alarm template, an alarm will be triggered. In the navigation pane, choose **Alarm Management > Alarm List** to view the alarm. The system also sends alarm notifications to specified personnel by email or SMS.

----End

More Operations

After the alarm template is created, you can also perform the operations listed in [Table 6-17](#).

Table 6-17 Related operations

Operation	Description
Viewing an alarm template	In the template list, you can view the rule set name, number of rules, bound cluster, and enterprise project.
Binding an alarm template with a Prometheus instance or cluster	Click  in the Operation column. For details, see Step 9 .
Modifying an alarm template	Choose ... > Edit in the Operation column. For details, see Creating an Alarm Template .
Copying an alarm template	Click  in the Operation column.
Deleting an alarm template	<ul style="list-style-type: none"> To delete an alarm template, choose ... > Delete in the Operation column. To delete one or more alarm templates, select them and click Delete in the displayed dialog box.
Searching for an alarm template	Enter a template name in the search box in the upper right corner and click  .
Viewing alarm rules created using a template	In the navigation pane on the left, choose Alarm Management > Alarm Rules . Enter a template name keyword in the search box above the alarm rule list and click  . If an alarm template has been bound with a Prometheus instance or cluster, you can also search for the alarm rule by the bound Prometheus instance or cluster name.
Viewing alarms	<p>When the metric value of a resource meets an alarm condition, an alarm will be generated.</p> <p>In the navigation pane, choose Alarm Management > Alarm List. On the Alarms tab page, view alarms. For details, see 6.3 Viewing Alarms.</p>
Viewing events	<p>When no metric data is reported during the configured consecutive periods, the system reports an insufficient data event.</p> <p>In the navigation pane, choose Alarm Management > Alarm List. On the Events tab page, view events. For details, see 6.4 Viewing Events.</p>

6.3 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 Log in to the AOM 2.0 console.


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 (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 4 Perform the operations listed in [Table 6-18](#) as required:

Table 6-18 Operations

Operation	Description
Viewing alarm statistics	Click  , and view alarm statistics that meet filter criteria within a specific time range on a bar graph.

Operation	Description
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	<p>Click an alarm name to view alarm details, including alarm information and handling suggestions. You can also view a bound alarm action rule or alarm noise reduction rule if there is any.</p> <p>On the Alarm Info tab page, click the alarm rule in blue to drill down to view details.</p>
Viewing cleared alarms	<p>Click Active Alarms in the upper right corner and select Historical Alarms from the drop-down list to view alarms that have been cleared.</p>

----End

6.4 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** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane, choose **Alarm Management > Alarm List**.
- Step 3** Click the **Events** tab to view the event information.
- 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.
 - Set the event refresh interval. Click  and select a value from the drop-down list, such as **Refresh manually** or **1 minute auto refresh**.
 - Set filter criteria and click  to view the events generated in the period.
- Step 4** Perform the operations listed in [Table 6-19](#) as required:

Table 6-19 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.

----End

6.5 Alarm Action Rules

6.5.1 Overview

AOM 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. After an alarm action rule is created, you can choose **Alarm Management > Alarm Noise Reduction > Grouping Rules**, create a grouping rule, and associate it with the alarm action rule.

6.5.2 Creating an Alarm Action Rule

You can create an alarm action rule and associate it with an SMN topic and a message template. If 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** Log in to the AOM 2.0 console.
- 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 6-20](#).

Table 6-20 Parameters of an alarm action rule

Parameter	Description
Rule Name	Name of an action rule. Enter up to 100 characters and do not start or end with an underscore (_) or hyphen (-). Only digits, letters, hyphens, and underscores are allowed.
Enterprise Project	Enterprise project. <ul style="list-style-type: none"> If you have selected All for Enterprise Project on the global settings page, select one from the drop-down list here. If you have already selected an enterprise project on the global settings page, this option will be grayed and cannot be changed. <p>NOTE To use the enterprise project function, contact engineers.</p>
Description	Description of the action rule. Enter up to 1,024 characters.
Action Type	Type of the action. Select one from the drop-down list. Only Metric/Event is supported.
Action	Type of action that is associated with the SMN topic and message template. Select one 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 6.5.3 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 6-21](#).

Table 6-21 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 or grouping 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  .

6.5.3 Creating a Message Template

In AOM, you can create message templates to customize notifications. When a preset notification rule is triggered, notifications can be sent to specified personnel by email, SMS, HTTP, or HTTPS. If no message template is created, the default message template will be used.

Functions

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

Precautions

- You can create a maximum of 100 message templates. If the number of message templates reaches 100, delete unnecessary ones.
- By default, two message templates are 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 Log in to the AOM 2.0 console.

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, message template type, and description, and specify an enterprise project.

Table 6-22 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.
Message Template	Type of the message template. Option: Metric/Event .
Enterprise Project	Enterprise project. <ul style="list-style-type: none"> - If you have selected All for Enterprise Project on the global settings page, select one from the drop-down list here. - If you have already selected an enterprise project on the global settings page, this option will be grayed and cannot be changed. <p>NOTE To use the enterprise project function, contact engineers.</p>

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 6-23](#).

 **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 6-23 Variables in the default message template

Variable	Description	Definition
Alarm Name	Name of the alarm rule that is triggered.	<code>\${event_name}</code>
Alarm ID	ID of the alarm rule that is triggered.	<code>\${id}</code>

Variable	Description	Definition
Action Rule	Name of the alarm action rule that triggers notification.	<code>\${action_rule}</code>
Occurred	Time when the alarm or event is triggered.	<code>\${starts_at}</code>
Event Severity	Alarm or event severity. Options: Critical , Major , Minor , and Warning .	<code>\${event_severity}</code>
Alarm Info	Detailed alarm information.	<code>\${alarm_info}</code>
Resource Identifier	Resource for which the alarm or event is triggered.	<code>\${resources_new}</code>
Custom tag	Extended tag.	<code>\$event.metadata.key1</code>
Suggestion	Suggestion about handling the alarm. For non-custom reporting, "NA" is displayed.	<code>\${alarm_fix_suggestion_zh}</code>
Custom annotation	Extended annotation.	<code>\$event.annotations.key2</code>

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


----End

More Operations

After creating a message template, you can perform the operations listed in [Table 6-24](#).

Table 6-24 Related operations

Operation	Description
Editing a message template	Click Edit in the Operation column.
Copying a message template	Click Copy in the Operation column.

Operation	Description
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  .

6.6 Alarm Noise Reduction

6.6.1 Overview

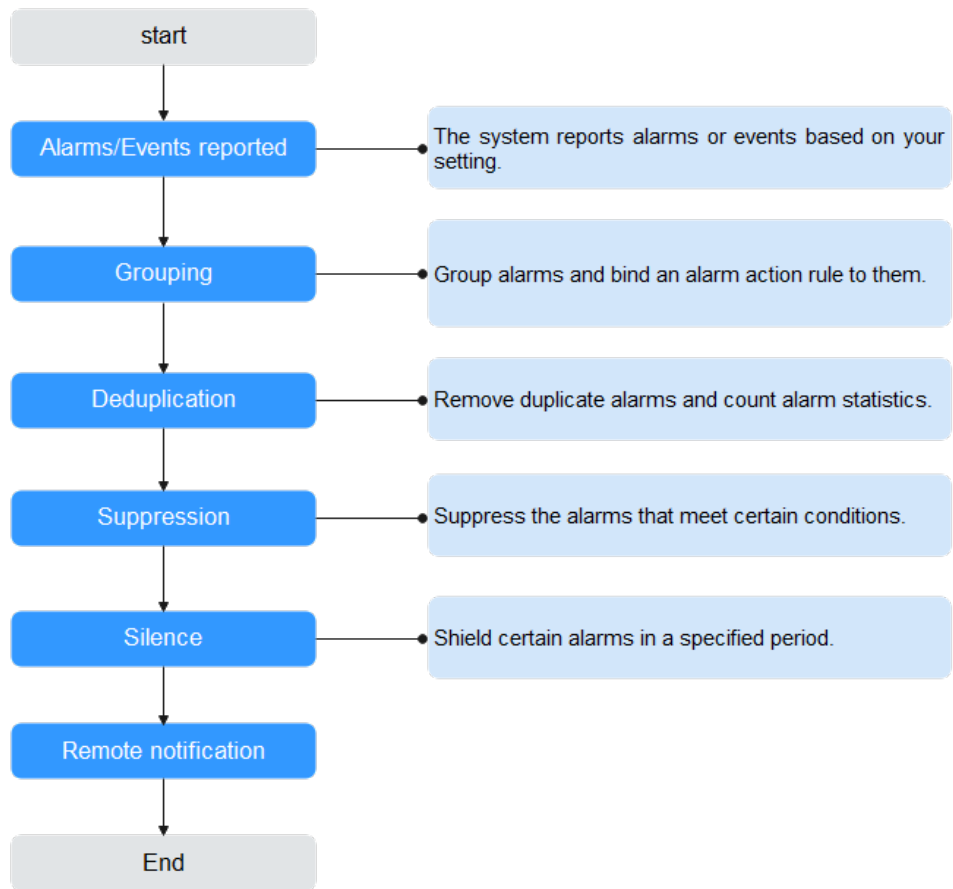
AOM supports alarm noise reduction. Alarms can be processed based on the alarm noise reduction rules to prevent notification storms.

Alarm noise reduction consists of four parts: grouping, deduplication, suppression, and silence.

AOM uses built-in deduplication rules. The service backend automatically deduplicates alarms. You do not need to manually create rules.

You need to manually create grouping, suppression, and silence rules. For details, see [6.6.2 Creating a Grouping Rule](#), [6.6.3 Creating a Suppression Rule](#), and [6.6.4 Creating a Silence Rule](#).

Figure 6-1 Alarm noise reduction process



NOTE

1. This module is used only for message notification. All triggered alarms and events can be viewed on the [alarm list](#) page.
2. All conditions of alarm noise reduction rules are obtained from **metadata** in alarm structs. You can use the default fields or customize your own fields.

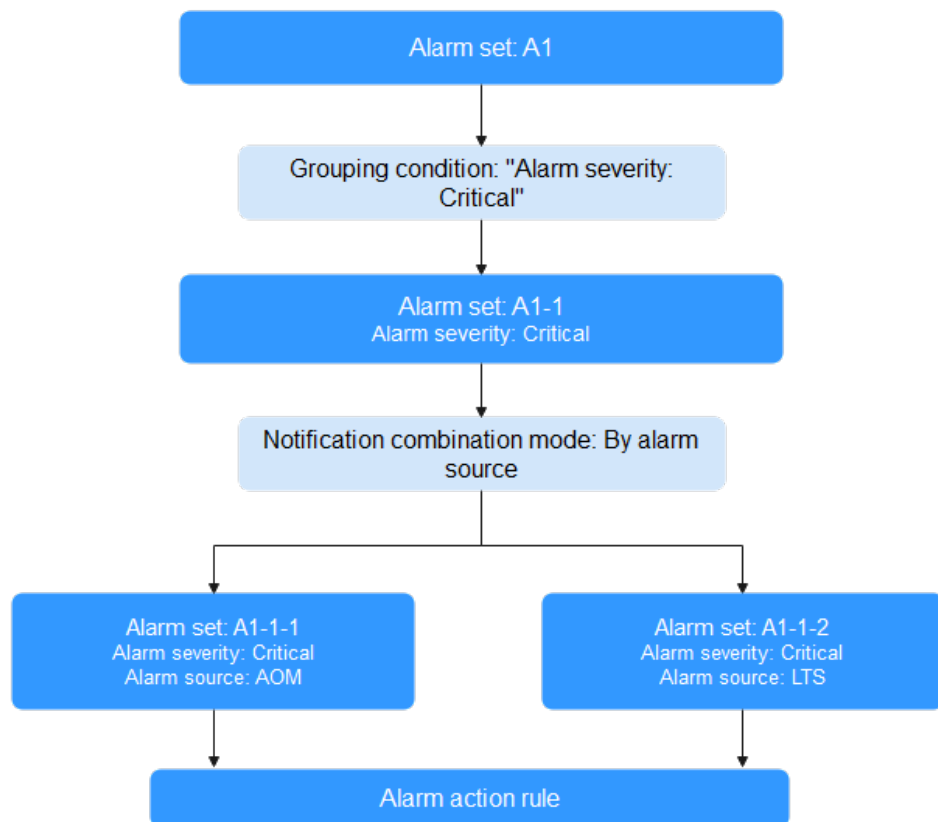
```
{
  "starts_at" : 1579420868000,
  "ends_at" : 1579420868000,
  "timeout" : 60000,
  "resource_group_id" : "5680587ab6*****755c543c1f",
  "metadata" : {
    "event_name" : "test",
    "event_severity" : "Major",
    "event_type" : "alarm",
    "resource_provider" : "ecs",
    "resource_type" : "vm",
    "resource_id" : "ecs123",
    "key1" : "value1" // Alarm tag configured when the alarm rule is created
  },
  "annotations" : {
    "alarm_probableCause_en_us": " Possible causes",
    "alarm_fix_suggestion_en_us": "Handling suggestion"
  }
}
```


6.6.2 Creating a Grouping Rule

You can filter alarm subsets and then group them based on the grouping conditions. Alarms in the same group are aggregated to trigger one notification.

As shown in [Figure 6-2](#), when **Alarm Severity** under **Grouping Condition** is set to **Critical**, the system filters out the critical alarms, and then combines these alarms based on the specified mode. The combined alarms can then be associated with an action rule for sending notifications.

Figure 6-2 Grouping process



Procedure

You can create up to 100 grouping rules.

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane, choose **Alarm Management > Alarm Noise Reduction**.
- Step 3** On the **Grouping Rules** tab page, click **Create** and set parameters such as the rule name and grouping condition. For details, see [Table 6-25](#).

Table 6-25 Grouping rule parameters

Category	Parameter	Description
-	Rule Name	Name of a grouping rule. Enter up to 100 characters and do not start or end with an underscore (_). Only letters, digits, and underscores are allowed.
	Enterprise Project	Enterprise project. <ul style="list-style-type: none"> • If you have selected All for Enterprise Project on the global settings page, select one from the drop-down list here. • If you have already selected an enterprise project on the global settings page, this option will be grayed and cannot be changed. <p>NOTE To use the enterprise project function, contact engineers.</p>
	Description	Description of a grouping rule. Enter up to 1024 characters.

Category	Parameter	Description
Grouping Rule	Grouping Condition	<p>Conditions set to filter alarms. After alarms are filtered out, you can set alarm action rules for them.</p> <p>Value range and description:</p> <ul style="list-style-type: none"> • Alarm Severity: severity of a metric or event alarm. Options: Critical, Major, Minor, and Warning. Example: Alarm Severity Equals to Critical • Resource Type: resource type selected when you create an alarm rule or customize alarm reporting. Options: host, container, process, and so on. Example: Resource Type Equals to container • Alarm Source: name of the service that triggers the alarm or event. Options: AOM, LTS, CCE, and so on. Example: Alarm Source Equals to AOM • Tag: alarm identification attribute, which consists of the tag name and tag value and can be customized. Example: Tag aom_monitor_level Equals to infrastructure • XX Exists: indicates the alarm whose metadata contains parameter <i>XX</i>. Example: For Alarm Source Exists, the alarms whose metadata contains the provider will be filtered. • XX Regular Expression: indicates the alarm whose parameter <i>XX</i> matches the regular expression. Example: For Resource Type Regular Expression host*, the alarms whose resource type contains host will be filtered. <p>Rule description:</p> <ul style="list-style-type: none"> • You can create a maximum of 10 parallel conditions, each of which can contain up to 10 serial conditions. One or more alarm action rules can be set for each parallel condition. • Serial conditions are in the AND relationship whereas parallel conditions are in the OR relationship. An alarm must meet all serial conditions under one of the parallel conditions. <p>For example, if two serial conditions (that is, Alarm Severity = Critical and Provider = AOM) are set under a parallel condition, critical AOM alarms are filtered out, and notification actions are performed based on the alarm action rule you set.</p>

Category	Parameter	Description
Combination Rule	Combine Notifications	<p>Combines grouped alarms based on specified fields. Alarms in the same group are aggregated for sending one notification.</p> <p>Notifications can be combined:</p> <ul style="list-style-type: none"> • By alarm source: Alarms triggered by the same alarm source are combined into one group for sending notifications. • By alarm source + severity: Alarms triggered by the same alarm source and of the same severity are combined into one group for sending notifications. • By alarm source + all tags: Alarms triggered by the same alarm source and with the same tag are combined into one group for sending notifications.
	Initial Wait Time	<p>Interval for sending an alarm notification after alarms are combined for the first time. It is recommended that the time be set to seconds to prevent alarm storms.</p> <p>Value range: 0s to 10 minutes. Recommended: 15s.</p>
	Batch Processing Interval	<p>Waiting time for sending an alarm notification after the combined alarm data changes. It is recommended that the time be set to minutes. If you want to receive alarm notifications as soon as possible, set the time to seconds.</p> <p>The change here refers to a new alarm or an alarm status change.</p> <p>Value range: 5s to 30 minutes. Recommended: 60s.</p>
	Repeat Interval	<p>Waiting time for sending an alarm notification after the combined alarm data becomes duplicate. It is recommended that the time be set to hours.</p> <p>Duplication means that no new alarm is generated and no alarm status is changed while other attributes (such as titles and content) are changed.</p> <p>Value range: 0 minutes to 15 days. Recommended: 1 hour.</p>


Step 4 Click **Confirm**.

----End

More Operations

After creating a grouping rule, perform the operations listed in [Table 6-26](#) if needed.

Table 6-26 Related operations

Operation	Description
Modifying a grouping rule	Click Modify in the Operation column.
Deleting a grouping 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. To delete one or more rules, select them and click Delete above the rule list.
Searching for a grouping rule	Enter a rule name in the search box in the upper right corner and click  .

6.6.3 Creating a Suppression Rule

By using suppression rules, you can suppress or block notifications related to specific alarms. For example, when a major alarm is generated, less severe alarms can be suppressed. Another example, when a node is faulty, all other alarms of the processes or containers on this node can be suppressed.

Precautions

If the source alarm corresponding to the suppression condition is cleared before the alarm notification is sent, the suppression rule becomes invalid. For the suppressed object (alarm suppressed by the source alarm), the alarm notification can still be sent as usual.

You can create up to 100 suppression rules.

Procedure

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane, choose **Alarm Management > Alarm Noise Reduction**.
- Step 3** On the **Suppression Rules** tab page, click **Create** and set parameters such as the rule name and source alarm.

Table 6-27 Setting a suppression rule

Category	Parameter	Description
-	Rule Name	Name of a suppression rule. Enter up to 100 characters and do not start or end with an underscore (_). Only letters, digits, and underscores are allowed.

Category	Parameter	Description
	Enterprise Project	Enterprise project. <ul style="list-style-type: none"> • If you have selected All for Enterprise Project on the global settings page, select one from the drop-down list here. • If you have already selected an enterprise project on the global settings page, this option will be grayed and cannot be changed. <p>NOTE To use the enterprise project function, contact engineers.</p>
	Description	Description of a suppression rule. Enter up to 1024 characters.

Category	Parameter	Description
Suppression Rule	Source Alarm	<p>Alarm that triggers suppression.</p> <p>Value range and description:</p> <ul style="list-style-type: none"> • Alarm Severity: severity of a metric or event alarm. Options: Critical, Major, Minor, and Warning. Example: Alarm Severity Equals to Critical • Resource Type: resource type selected when you create an alarm rule or customize alarm reporting. Options: host, container, process, and so on. Example: Resource Type Equals to container • Alarm Source: name of the service that triggers the alarm or event. Options: AOM, LTS, CCE, and so on. Example: Alarm Source Equals to AOM • Tag: alarm identification attribute, which consists of the tag name and tag value and can be customized. Example: Tag aom_monitor_level Equals to infrastructure • XX Exists: indicates the alarm whose metadata contains parameter XX. Example: For Alarm Source Exists, the alarms whose metadata contains the provider will be filtered. • XX Regular Expression: indicates the alarm whose parameter XX matches the regular expression. Example: For Resource Type Regular Expression host*, the alarms whose resource type contains host will be filtered. <p>Rule description:</p> <p>A maximum of 10 parallel conditions can be set for root alarms, and a maximum of 10 serial conditions can be set for each parallel condition. Serial conditions are in the AND relationship whereas parallel conditions are in the OR relationship. An alarm must meet all serial conditions under one of the parallel conditions.</p> <p>Example: For a serial condition, if Alarm Severity is set to Critical, critical alarms are filtered out as the root alarms.</p>
	Suppressed Alarm	<p>Alarm that is suppressed by the root alarm.</p> <p>Set parameters for the suppressed alarm in the same way that you set parameters for the source alarm.</p> <p>If Alarm Severity is set to Critical in the source alarm's serial condition and set to Warning in the suppressed alarm's serial condition, warnings will be suppressed when critical alarms are generated.</p>

Step 4 Click **Confirm**.


After a suppression rule is created, it will take effect for all alarms that are grouped.

----End

More Operations

After creating a suppression rule, perform the operations listed in [Table 6-28](#) if needed.

Table 6-28 Related operations

Operation	Description
Modifying a suppression rule	Click Modify in the Operation column.
Deleting a suppression 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. To delete one or more rules, select them and click Delete above the rule list.
Searching for a suppression rule	Enter a rule name in the search box in the upper right corner and click  .

6.6.4 Creating a Silence Rule

You can shield alarm notifications in a specified period. A silence rule takes effect immediately after it is created.

Procedure

You can create up to 100 silence rules.

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane, choose **Alarm Management > Alarm Noise Reduction**.
- Step 3** On the **Silence Rules** tab page, click **Create** and set parameters such as the rule name and silence condition.

Table 6-29 Setting a silence rule

Category	Parameter	Description
-	Rule Name	Name of a silence rule. Enter up to 100 characters and do not start or end with an underscore (_). Only letters, digits, and underscores are allowed.

Category	Parameter	Description
	Enterprise Project	Enterprise project. <ul style="list-style-type: none"> • If you have selected All for Enterprise Project on the global settings page, select one from the drop-down list here. • If you have already selected an enterprise project on the global settings page, this option will be grayed and cannot be changed. <p>NOTE To use the enterprise project function, contact engineers.</p>
	Description	Description of a silence rule. Enter up to 1024 characters.

Category	Parameter	Description
Silence Rule	Silence Condition	<p>Any alarm notifications that meet the silence condition will be shielded.</p> <p>Value range and description:</p> <ul style="list-style-type: none"> • Alarm Severity: severity of a metric or event alarm. Options: Critical, Major, Minor, and Warning. Example: Alarm Severity Equals to Critical • Resource Type: resource type selected when you create an alarm rule or customize alarm reporting. Options: host, container, process, and so on. Example: Resource Type Equals to container • Alarm Source: name of the service that triggers the alarm or event. Options: AOM, LTS, CCE, and so on. Example: Alarm Source Equals to AOM • Tag: alarm identification attribute, which consists of the tag name and tag value and can be customized. Example: Tag aom_monitor_level Equals to infrastructure • XX Exists: indicates the alarm whose metadata contains parameter <i>XX</i>. Example: For Alarm Source Exists, the alarms whose metadata contains the provider will be filtered. • XX Regular Expression: indicates the alarm whose parameter <i>XX</i> matches the regular expression. Example: For Resource Type Regular Expression host*, the alarms whose resource type contains host will be filtered. <p>Rule description:</p> <p>You can create up to 10 parallel conditions under Silence Condition, and up to 10 serial conditions under each parallel condition. Serial conditions are in the AND relationship whereas parallel conditions are in the OR relationship. An alarm must meet all serial conditions under one of the parallel conditions.</p> <p>Example: If Alarm Severity is set to Warning in a serial condition, warnings will be shielded.</p>
	Silence Time	<p>Time when alarm notifications are shielded. There are two options:</p> <ul style="list-style-type: none"> • Fixed time: Alarm notifications are shielded only in a specified period. • Cycle time: Alarm notifications are shielded periodically.

Category	Parameter	Description
	Time Zone/ Language	Time zone and language for which alarm notifications are shielded. The time zone and language configured in Preferences are selected by default. You can change them as required.


Step 4 Click **Confirm**.

----End

More Operations

After creating a silence rule, you can also perform the operations listed in [Table 6-30](#).

Table 6-30 Related operations

Operation	Description
Modifying a silence rule	Click Modify in the Operation column.
Deleting a silence 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. • To delete one or more rules, select them and click Delete above the rule list.
Searching for a silence rule	Enter a rule name in the search box in the upper right corner and click  .

7 Metric Analysis

7.1 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 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Metric Analysis > Metric Browsing**.

Step 3 Select a target Prometheus instance from the drop-down list.

Step 4 Select one or more metrics from all metrics or by running Prometheus statements.




- Select metrics from all metrics.


For details about how to set monitoring conditions, see [Table 6-2](#).

After selecting a target metric, you can set condition attributes to filter information. For example, different RDS DB instances have the CPU usage metric. You need to view the CPU usage metric of a specified RDS DB instance type. The procedure is as follows:

In the **Metric** text box, select the CPU usage metric of the corresponding RDS DB instance. In the **Conditions** area, set the dimension name to **RDS for MySQL** or **RDS for PostgreSQL** and select the corresponding dimension value. The CPU usage metric of the specified RDS DB instance type will be displayed.

You can click **Add Metric** to add metrics and set information such as statistical period for the metrics. After moving the cursor to the metric data and monitoring condition, you can perform the following operations as required:

- Click  next to a monitoring condition to hide the corresponding metric data record in the graph.
- Click  next to a monitoring condition to convert the metric data and monitoring condition into a Prometheus command.
- Click  next to a monitoring condition to quickly copy the metric data and monitoring condition and modify them as required.

- Click  next to a monitoring condition to remove a metric data record from monitoring.
- Select metrics by running Prometheus statements. For details about Prometheus statements, see [14.2 Prometheus Statements](#).

Step 5 Set metric parameters by referring to [Table 7-1](#), view the metric graph in the upper part of the page, and analyze metric data from multiple perspectives.

Table 7-1 Metric parameters

Parameter	Description
Statistic	Method used to measure metrics. Options: Avg, Min, Max, Sum, and Samples. NOTE Samples: the number of data points.
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.

Step 6 (Optional) Set the display layout of metric data.

On the right of the page, click the arrow next to the graph type, select your target graph type from the drop-down list, and set graph parameters, such as the X-axis name, Y-axis name, and displayed value. For details about the parameters, see [Metric Data Graphs \(Line/Digit/Top N/Table/Bar/Digital Line Graphs\)](#).

 **NOTE**


A maximum of 200 metric data records can be displayed in a line graph.



----End

More Operations

You can also perform the operations listed in [Table 7-2](#).

Table 7-2 Related operations

Operation	Description
Adding an alarm rule for a metric	After selecting a metric, click  in the upper right corner of the metric list to add an alarm rule for the metric. NOTE When you are redirected to the Create Alarm Rule page, your settings made on the Metric Browsing page will be automatically applied to Alarm Rule Settings and Alarm Rule Details areas.

Operation	Description
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.

7.2 Prometheus Monitoring

7.2.1 Creating Prometheus Instances

7.2.1.1 Prometheus Instance for Cloud Services

This type of instance is recommended when you need to monitor multiple metrics of cloud services.

Precautions

- Only one Prometheus instance for cloud services can be created in an enterprise project.

Creating a Prometheus Instance for Cloud Services

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane on the left, choose **Metric Analysis > Prometheus Monitoring**. On the displayed page, click **Add Prometheus Instance**.
- Step 3** Set the instance name, enterprise project, and instance type.

Table 7-3 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.

Parameter	Description
Enterprise Project	<p>Enterprise project.</p> <ul style="list-style-type: none"> If you have selected All for Enterprise Project on the global settings page, select one from the drop-down list here. If you have already selected an enterprise project on the global settings page, this option will be grayed and cannot be changed. <p>NOTE To use the enterprise project function, contact engineers.</p>
Instance Type	Type of the Prometheus instance. Select Prometheus for Cloud Services .

Step 4 Click **OK**.

----End

Connecting Cloud Services

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane on the left, choose **Metric Analysis > Prometheus Monitoring**.

Step 3 On the Prometheus instance list page, click a Prometheus instance for cloud services.

Step 4 Click **Connect Cloud Service** to connect desired cloud services.

Step 5 Click **Confirm**.

----End

7.2.1.2 Prometheus Instance for CCE

This type of instance is recommended when you need to monitor CCE clusters and applications running on them. By default, CCE clusters are monitored. If needed, add component monitoring through the access center.

Precautions

- You can connect clusters only when the kube-prometheus-stack add-on exists on the **Add-ons** page of CCE.
- Before installing the kube-prometheus-stack add-on, ensure that there are at least 4 vCPUs and 8 GiB memory. Otherwise, this add-on cannot work.

Creating a Prometheus Instance for CCE

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane on the left, choose **Metric Analysis > Prometheus Monitoring**. On the displayed page, click **Add Prometheus Instance**.

Step 3 Set the instance name, enterprise project, and instance type.

Table 7-4 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.
Enterprise Project	Enterprise project. <ul style="list-style-type: none"> If you have selected All for Enterprise Project on the global settings page, select one from the drop-down list here. If you have already selected an enterprise project on the global settings page, this option will be grayed and cannot be changed. <p>NOTE To use the enterprise project function, contact engineers.</p>
Instance Type	Type of the Prometheus instance. Select Prometheus for CCE .

Step 4 Click **OK**.

----End

Connecting a CCE Cluster

Step 1 In the navigation pane on the left, choose **Metric Analysis > Prometheus Monitoring**.

Step 2 In the instance list, click a Prometheus instance for CCE.

Step 3 On the **Integration Center** page, click **Connect Cluster**. In the cluster list, you can view the cluster information, installation status, and collection status.

Step 4 Locate a target cluster and click **Install** in the **Operation** column to install the Prometheus add-on.

Step 5 After the installation is complete, click **Close** to connect the CCE cluster and bind it with the current Prometheus instance.

To disconnect the CCE cluster, click **Uninstall**.

----End

7.2.1.3 Prometheus Instance for Remote Write

This type of instance is recommended when Prometheus servers have been built. The availability and scalability of Prometheus storage need to be ensured through remote write.

Creating a Prometheus Instance for Remote Write

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane on the left, choose **Metric Analysis > Prometheus Monitoring**. On the displayed page, click **Add Prometheus Instance**.
- Step 3** Set the instance name, enterprise project, and instance type.

Table 7-5 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.
Enterprise Project	Enterprise project. <ul style="list-style-type: none"> • If you have selected All for Enterprise Project on the global settings page, select one from the drop-down list here. • If you have already selected an enterprise project on the global settings page, this option will be grayed and cannot be changed. <p>NOTE To use the enterprise project function, contact engineers.</p>
Instance Type	Type of the Prometheus instance. Select Prometheus for Remote Write .

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

----End

7.2.1.4 Prometheus Instance for Multi-Account Aggregation

This type of instance is recommended when you need to monitor the cloud service metrics of multiple accounts in an organization.

Prerequisites

- You have enabled trusted access to AOM on the Organizations console.
- Cloud service metrics have been connected for multiple accounts in an organization.

Creating a Prometheus Instance for Multi-Account Aggregation

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane on the left, choose **Metric Analysis > Prometheus Monitoring**. On the displayed page, click **Add Prometheus Instance**.

Step 3 Set the instance name, enterprise project, and instance type.

Table 7-6 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.
Enterprise Project	Enterprise project. <ul style="list-style-type: none"> If you have selected All for Enterprise Project on the global settings page, select one from the drop-down list here. If you have already selected an enterprise project on the global settings page, this option will be grayed and cannot be changed. <p>NOTE To use the enterprise project function, contact engineers.</p>
Instance Type	Type of the Prometheus instance. Select Prometheus for Multi-Account Aggregation .

Step 4 Click **OK**.

----End

Connecting Accounts

You can connect accounts only after logging in as an organization administrator or a delegated administrator.

NOTICE

- If a delegated administrator cannot connect accounts, grant the following permissions :
 - organizations:trustedServices:list
 - organizations:organizations:get
 - organizations:delegatedAdministrators:list
 - organizations:accounts:list
 - organizations:delegatedServices:list
- AOM only supports connection to member accounts under an organizational unit (OU). When the relationship between the OU and member accounts changes, AOM will not automatically synchronize that information.

To connect accounts, do as follows:

Step 1 Log in to the AOM 2.0 console. Then choose **Metric Analysis > Prometheus Monitoring**.

- Step 2** On the Prometheus instance list page, click a Prometheus instance for multi-account aggregation.
- Step 3** On the **Account Access** page, manage member accounts, connect cloud services, configure data storage, and add supported metrics.
- Managing member accounts: AOM supports account management. It allows you to incorporate cloud accounts into your organization for centralized management. There are three types of members in an organization: administrator, delegated administrator, and common user. Common users do not have the permission to monitor multi-account metrics on AOM.
 - To monitor the metrics of a member account, click the **Member Account** text box and enter an account keyword in the displayed search box. Related member accounts are automatically displayed. Then select your desired ones.
 - To stop monitoring the metrics of a member account, delete the account from the **Member Account** text box on the **Account Access** page.
 - Connecting cloud services: Select one or more cloud services from the drop-down list.
 - Data storage: Member accounts retain metric data after they are connected to a Prometheus instance for aggregation. By default, this function is disabled.
 - Adding metrics supported by cloud services: Click **Add Metric** to add metrics for connected cloud services.

----End


7.2.2 Managing Prometheus Instances











You can view the names, types, and enterprise projects of Prometheus instances in the instance list and modify and delete them as required.



Procedure

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane on the left, choose **Metric Analysis > Prometheus Monitoring**. In the instance list, check the created Prometheus instances and perform the operations listed in [Table 7-7](#) if needed.

Table 7-7 Related operations

Operation	Description
Searching for a Prometheus instance	Enter an instance name in the search box and click  .

Operation	Description
Filtering and displaying Prometheus instances	Click  next to the Instance Type column to filter Prometheus instances.
Refreshing Prometheus instances	Click  in the upper right corner of the Prometheus instance list to obtain their latest information in real time.
Sorting Prometheus instances	Click  in the Created column to sort Prometheus instances.  indicates the default order.  indicates the ascending order by time (the latest instance is displayed at the bottom).  indicates the descending order by time (the latest instance is displayed at the top).
Viewing a Prometheus instance	<p>The Prometheus instance list displays information such as the instance name, instance type, enterprise project, and creation time in real time.</p> <ul style="list-style-type: none"> • When you have an access code: <ul style="list-style-type: none"> Click an instance name. On the displayed instance details page, choose Settings and view the basic information and credential of the instance. <ul style="list-style-type: none"> - By default, the AppSecret is hidden. To show it, click  or  reflects the status of the AppSecret. - In the Grafana Data Source Info area, obtain the Grafana data source configuration code in the private or public network of the desire Prometheus instance. Then click  on the right to copy the code to the corresponding file. - In the Service Addresses area, obtain the configuration code in the private or public network of the desire Prometheus instance. Then click  on the right to copy the code to the corresponding file. For details, see 7.2.5 Obtaining the Service Address of a Prometheus Instance. • When you do not have an access code: <ol style="list-style-type: none"> 1. Click an instance name. On the displayed instance details page, choose Settings and view the basic information about the instance. The system displays a message indicating that there is no access code. 2. Click Add Access Code. In the displayed dialog box, click OK. Then, choose Management > Global Configuration in the navigation pane of the AOM 2.0 console. On the displayed page, choose Authentication in the navigation pane and manage access codes. For details, see More Operations.

Operation	Description
Modifying a Prometheus instance	<ul style="list-style-type: none"> Modify a Prometheus instance name: Click  in the Operation column that contains the target Prometheus instance. The name of each Prometheus instance in an enterprise project must be unique. Modify Prometheus instance configurations: In the Prometheus instance list, click the name of a Prometheus instance for cloud services, CCE and modify the connected cloud services/CCE clusters if needed.
Deleting a Prometheus instance	Click  in the Operation column that contains the target Prometheus instance.

----End

7.2.3 Configuring a Recording Rule

Recording rules can be used for secondary development of metric data. Some queries may require a large amount of computing on the query end, resulting in high pressure on this end. By setting recording rules, you can move the computing process to the write end, reducing resource usage on the query end. Especially in large-scale clusters and complex service scenarios, recording rules can reduce PromQL complexity, thereby improving the query performance and preventing slow user configuration and queries.

Prerequisite

Both your service and CCE cluster have been connected to a Prometheus instance for CCE. For details, see [7.2.1.2 Prometheus Instance for CCE](#).

Configuring a Recording Rule

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane on the left, choose **Metric Analysis > Prometheus Monitoring**.
- Step 3** In the instance list, click a Prometheus instance for CCE.
- Step 4** In the navigation pane on the left, choose **Settings**. In the **Recording Rules** area, click **Edit RecordingRule.yaml**.
- Step 5** In the dialog box that is displayed, delete the default content and enter a custom recording rule.

NOTE

Only one **RecordingRule.yaml** file needs to be configured for a cluster. Each rule group name must be unique.

Table 7-8 Recording rule parameters

Parameter	Description
groups	Rule group. You can set multiple rule groups in one RecordingRule.yaml file.
name	Rule group name. Each rule group name must be unique.
interval	(Optional) Execution interval of a rule group. The default value is 60s .
rules	Rule. A rule group can contain multiple rules.
record	Name of a rule. The name must comply with Prometheus metric name specifications .
expr	Calculation expression. It is used to calculate metric values. It must comply with PromQL requirements .
labels	(Optional) Label of a metric.

Example of a recording rule:

```
groups:
- name: apiserver_request_total
  interval: 60s
  rules:
- record: apiserver_request_rate
  expr: avg by (job, instance, mode) (rate(apiserver_request_total[5m]))
  labels:
    team: operations
- record: job:apiserver_request_total:sum_rate10m
  expr: sum by (job)(rate(apiserver_request_total[10m]))
  labels:
    team: operations
```

Step 6 Click **OK**.

----End

Viewing Recording Rule Metrics

After a recording rule is configured, you can view its metrics on the **Metric Browsing** page of AOM or using Grafana.

Method 1: Viewing Metrics on the **Metric Browsing** Page of AOM

Step 1 On the **Metric Analysis > Metric Browsing** page, select a Prometheus instance for which a recording rule has been configured from the drop-down list.

Step 2 Click **All metrics** and enter the name of a recording rule metric in the search box to view its details.

----End

Method 2: Viewing Metrics Using Grafana

For details, see **7.2.7 Viewing Metric Data in AOM Using Grafana**.

7.2.4 Configuring Service Discovery

7.2.4.1 Configuring Metrics

You can view the metrics of a default Prometheus instance, or a Prometheus instance for CCE or cloud services, and add or discard metrics.

Prerequisites

- Both your service and CCE cluster have been connected to a Prometheus instance for CCE. For details, see [7.2.1.2 Prometheus Instance for CCE](#).
- Both your service and cloud services have been connected to a Prometheus instance for cloud services. For details, see [7.2.1.1 Prometheus Instance for Cloud Services](#).

Precautions

- Only the default Prometheus instance, and Prometheus instance for CCE or cloud services support the functions of viewing, adding, and discarding metrics.
- Default Prometheus instance: Metrics whose names start with **aom_** or **apm_** and resource type is **ICAgent** cannot be discarded.
- Prometheus instances for CCE:
Only the metrics reported by kube-prometheus-stack 3.9.0 or later installed on CCE **Add-ons** or AOM **Integration Center** can be discarded. Ensure that this add-on is running when discarding metrics.

NOTE

To view the kube-prometheus-stack status, log in to the CCE console and access the cluster page, choose **Add-ons** in the navigation pane, and locate that add-on on the right.

Viewing the Metrics of a Prometheus Instance of CCE

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane on the left, choose **Metric Analysis > Prometheus Monitoring**.
- Step 3** In the instance list, click a Prometheus instance for CCE.
- Step 4** In the navigation pane on the left, choose **Service Discovery**. On the **Metrics** tab page, view the metric names and types of the current Prometheus instance.

You can also filter metrics by cluster name, job name, or metric type, or enter a metric name keyword to search.

Table 7-9 Metric parameters

Parameter	Description
Metric Name	Name of a metric.

Parameter	Description
Metric Type	Type of a metric. Options: Basic metric and Custom metric .
Metrics in Last 10 Min	Number of metrics that are stored in the last 10 minutes.
Proportion	Number of a certain type of metrics/Total number of metrics

----End

Viewing the Metrics of a Prometheus Instance of Cloud Services

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane on the left, choose **Metric Analysis > Prometheus Monitoring**.
- Step 3** In the instance list, click a Prometheus instance for cloud services.
- Step 4** In the navigation pane on the left, choose **Service Discovery**. Then view the metric names and types of the current Prometheus instance.

You can also filter metrics by metric or resource type, or enter a metric name keyword to search.

Table 7-10 Metric parameters

Parameter	Description
Metric Name	Name of a metric.
Metric Type	Type of a metric. Options: Basic metric and Custom metric .
Resource Type	Type of a resource. That is, the type of the connected cloud service.

----End

Viewing the Metrics of a Default Prometheus Instance

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane on the left, choose **Metric Analysis > Prometheus Monitoring**.
- Step 3** In the instance list, click a default Prometheus instance.
- Step 4** In the navigation pane on the left, choose **Service Discovery**. Then view the metric names and types of the current Prometheus instance.

You can also filter metrics by metric or resource type, or enter a metric name keyword to search.

Table 7-11 Metric parameters






Parameter	Description
Metric Name	Name of a metric.
Metric Type	Type of a metric. Options: Basic metric and Custom metric .
Resource Type	Type of a resource.
Metrics in Last 10 Min	Number of metrics that are stored in the last 10 minutes.
Proportion	Number of a certain type of metrics/Total number of metrics

----End

More Operations

You can also perform the operations listed in [Table 7-12](#) if needed.

Table 7-12 Related operations

Operation	Description
Sorting metrics	Click  next to the Metrics in Last 10 Min or Proportion column to change the orders of metrics in the list.  indicates the default order.  indicates the ascending order (that is, the largest value is displayed at the bottom).  indicates the descending order (that is, the smallest value is displayed at the bottom).
Adding metrics	Click Add Metric , select desired metrics from the metric list, and click OK . NOTE A maximum of 100 metrics can be added each time.
Discarding metrics	<ul style="list-style-type: none"> To discard a metric, locate it and click  in the Operation column. To discard one or more metrics, select them and click Discard in the displayed dialog box. NOTE A maximum of 100 metrics can be discarded each time.

7.2.4.2 Configuring Service Discovery for CCE Clusters

By adding ServiceMonitor or PodMonitor, you can configure Prometheus collection rules to monitor the applications deployed in CCE clusters.

Prerequisite

Both your service and CCE cluster have been connected to a Prometheus instance for CCE. For details, see [7.2.1.2 Prometheus Instance for CCE](#).

Precautions

Only when kube-prometheus-stack installed on the **Add-ons** page of CCE or the **Integration Center** page of AOM is 3.9.0 or later and is still running, can you enable or disable collection rules.

NOTE

To view the kube-prometheus-stack status, log in to the CCE console and access the cluster page, choose **Add-ons** in the navigation pane, and locate that add-on on the right.

Adding ServiceMonitor

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane on the left, choose **Metric Analysis > Prometheus Monitoring**.

Step 3 In the instance list, click a Prometheus instance for CCE.

Step 4 In the navigation pane on the left, choose **Service Discovery**. On the **Settings** tab page, click **ServiceMonitor**.

Step 5 Click **Add ServiceMonitor**. In the displayed dialog box, set related parameters and click **OK**.

After the configuration is complete, the new collection rule is displayed in the service discovery list.

----End

Adding PodMonitor

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane on the left, choose **Metric Analysis > Prometheus Monitoring**.

Step 3 In the instance list, click a Prometheus instance for CCE.

Step 4 In the navigation pane on the left, choose **Service Discovery**. On the **Settings** tab page, click **PodMonitor**.

Step 5 Click **Add PodMonitor**. In the displayed dialog box, set related parameters and click **OK**.






After the configuration is complete, the new collection rule is displayed in the service discovery list.

----End

More Operations

Perform the operations listed in [Table 7-13](#) if needed.

Table 7-13 Related operations

Operation	Description
Viewing service discovery	<ul style="list-style-type: none"> In the service discovery list, view information such as the name, tag, namespace, and configuration mode. You can filter information by cluster name, namespace, or configuration mode. Click  in the Operation column. In the displayed dialog box, view details about the ServiceMonitor or PodMonitor collection rule.
Enabling or disabling collection rules	<p>On the Settings tab page of the Service Discovery page, click  in the Status column to enable or disable collection rules.  indicates that collection rules are disabled.  indicates that collection rules are enabled.</p>
Deleting service discovery	Click  in the Operation column.

7.2.5 Obtaining the Service Address of a Prometheus Instance

In the **Service Addresses** area on the **Settings** tab page of the default Prometheus instance or of the Prometheus instance for CCE, and remote write, you can obtain the configuration code for Prometheus remote read and write. In the **Service Addresses** area on the **Settings** tab page of the Prometheus instance for cloud services, you can obtain the configuration code for Prometheus remote read.

Prerequisites

Your service has been connected for Prometheus monitoring. For more details, see:

- [7.2.1.1 Prometheus Instance for Cloud Services](#)
- [7.2.1.2 Prometheus Instance for CCE](#)
- [7.2.1.3 Prometheus Instance for Remote Write](#)

Procedure

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane on the left, choose **Metric Analysis > Prometheus Monitoring**. In the instance list, click the created Prometheus instance.
- Step 3** On the instance details page, choose **Settings** in the navigation pane to obtain the service address of the current instance.

The following describes how to obtain the service address of a Prometheus instance for CCE.


- Click the **Intranet** tab to obtain the configuration code for Prometheus remote read and write in the intranet. Click  on the right of the code to copy the code to the corresponding file.
- Obtain the configuration code for Prometheus remote read.

Figure 7-1 Configuration code for Prometheus remote read

```
Configuration Code for Prometheus Remote Read

remote_read:
  - url: https://aom
    its_config
      insecure_skip_verify: true
      bearer_token: 'Cv**H5'
      read_recent: true
```

Remote read address:

url: 'https://aom.{region_name}-.{Site domain name suffix}/v1/{project_id}/api/v1/read'

Remote read address parameters:

- **region_name**: domain name or IP address of the server where the REST service is deployed. The value varies depending on services and regions.
 - **Site domain name suffix**: site domain name suffix.
 - **project_id**: project ID.
- Obtain the configuration code for Prometheus remote write.

Figure 7-2 Configuration code for Prometheus remote write

```
Configuration Code for Prometheus Remote Write

remote_write:
  - url: https://aom
    its_config
      insecure_skip_verify: true
      bearer_token: 'Cv**H5'
```

Remote write address in the intranet:

url: 'https://aom-internal-access.{region_name}-.{Site domain name suffix}:8443/v1/{project_id}/push'

Remote write address in the public network:

url: 'https://aom-access.{region_name}-.{Site domain name suffix}:8443/v1/{project_id}/push'

Remote write address parameters:

- **region_name**: domain name or IP address of the server where the REST service is deployed. The value varies depending on services and regions.
- **Site domain name suffix**: site domain name suffix.
- **project_id**: project ID.

----End

7.2.6 Reporting Prometheus Data to AOM

On the **Settings** tab page of the default Prometheus instance or of the Prometheus instance for CCE, or remote write, you can obtain the remote write address of the current Prometheus instance. Native Prometheus metrics can then be reported to AOM through remote write. In this way, time series data can be stored for long.

If the open-source Prometheus has been deployed and is being used, directly go to [Step 4](#).

Prerequisites

- Your service has been connected for Prometheus monitoring. For more details, see:
 - [7.2.1.2 Prometheus Instance for CCE](#)
 - [7.2.1.3 Prometheus Instance for Remote Write](#)

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 2.0 console.
2. In the navigation pane, choose **Management > Global Configuration**.
3. In the navigation pane on the left, choose **Authentication**. Click **Add Access Code**.
4. In the dialog box that is displayed, click **OK**. The system then 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.

Step 3 Obtain the configuration code for Prometheus remote write.

1. Log in to the AOM 2.0 console.
2. In the navigation pane on the left, choose **Metric Analysis > Prometheus Monitoring**. In the instance list, click the target Prometheus instance.
3. On the displayed page, choose **Settings** in the navigation pane and obtain the configuration code for Prometheus remote write from the **Service Addresses** area.

Step 4 Log in to the target ECS and configure the **prometheus.yml** file.

Run the following command to find and start the **prometheus.yml** file:

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

Add the configuration code for Prometheus remote write obtained in [Step 3](#) to the end of the **prometheus.yml** file.

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']
# Replace the italic content with the configuration code for Prometheus remote write obtained in Step 3.
remote_write:
  - url: 'https://aom-*.***.{Site domain name suffix}:8443/v1/6d6df***2ab7/58d6***c3d/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. Therefore, ensure that the host where Prometheus is located can resolve the private domain name.

Step 6 Restart Prometheus.

Step 7 [View metric data in AOM using Grafana](#) to check whether data is successfully reported after the preceding configurations are modified.

----End

7.2.7 Viewing Metric Data in AOM Using Grafana

After connecting a cloud service or CCE cluster to a Prometheus instance, you can use Grafana to view the metrics of the cloud service or cluster.

Prerequisites

- You have created an ECS.
- You have created an EIP and bound it to the created ECS.
- Your service has been connected for Prometheus monitoring. For more details, see:
 - [7.2.1.2 Prometheus Instance for CCE](#)
 - [7.2.1.3 Prometheus Instance for Remote Write](#)

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 2.0 console.
2. In the navigation pane, choose **Management** > **Global Configuration**.
3. In the navigation pane on the left, choose **Authentication**. Click **Add Access Code**.
4. In the dialog box that is displayed, click **OK**. The system then 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.

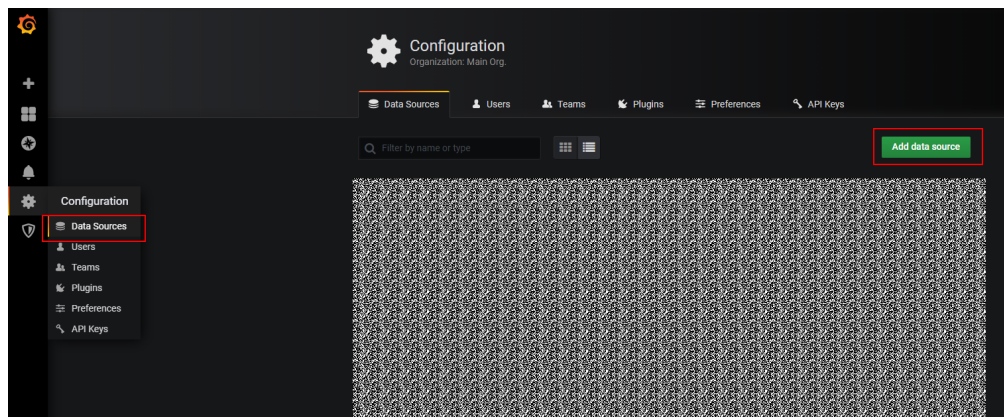
Step 3 Obtain the Grafana data source configuration code.

1. Log in to the AOM 2.0 console.
2. In the navigation pane on the left, choose **Metric Analysis > Prometheus Monitoring**. In the instance list, click the target Prometheus instance.
3. On the displayed page, choose **Settings** in the navigation pane and obtain the Grafana data source information from the **Grafana Data Source Info** area.

Step 4 Configure Grafana.

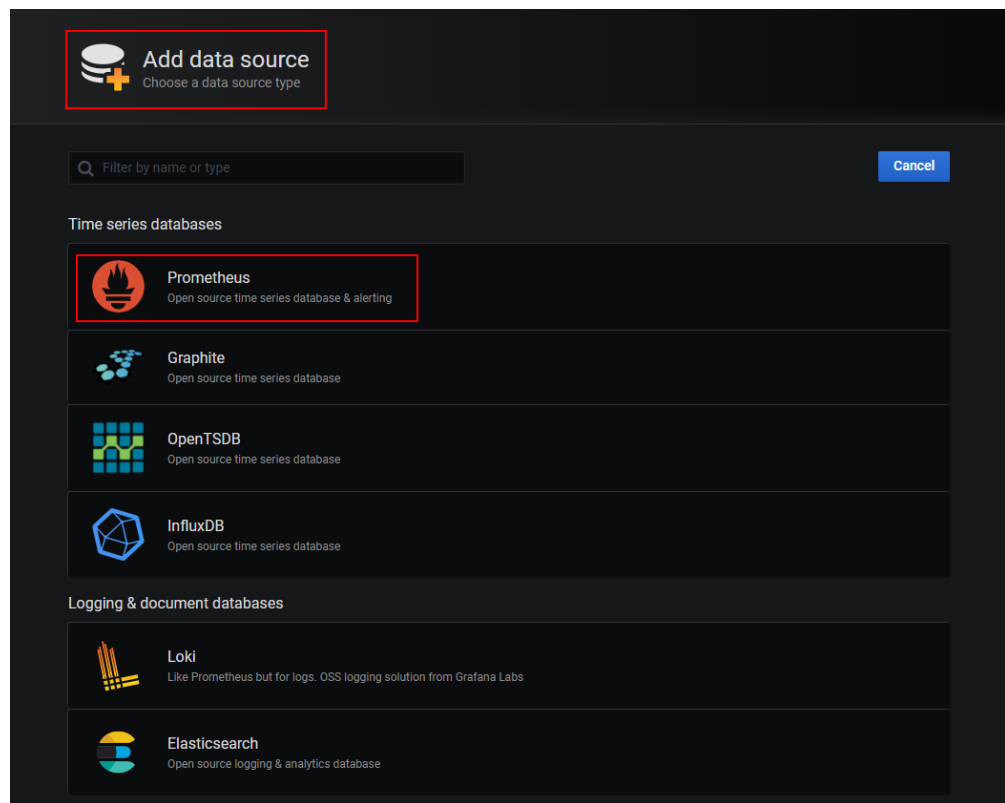
1. Log in to Grafana.
2. In the navigation pane, choose **Configuration > Data Sources**. Then click **Add data source**.

Figure 7-3 Configuring Grafana



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

Figure 7-4 Prometheus configuration page

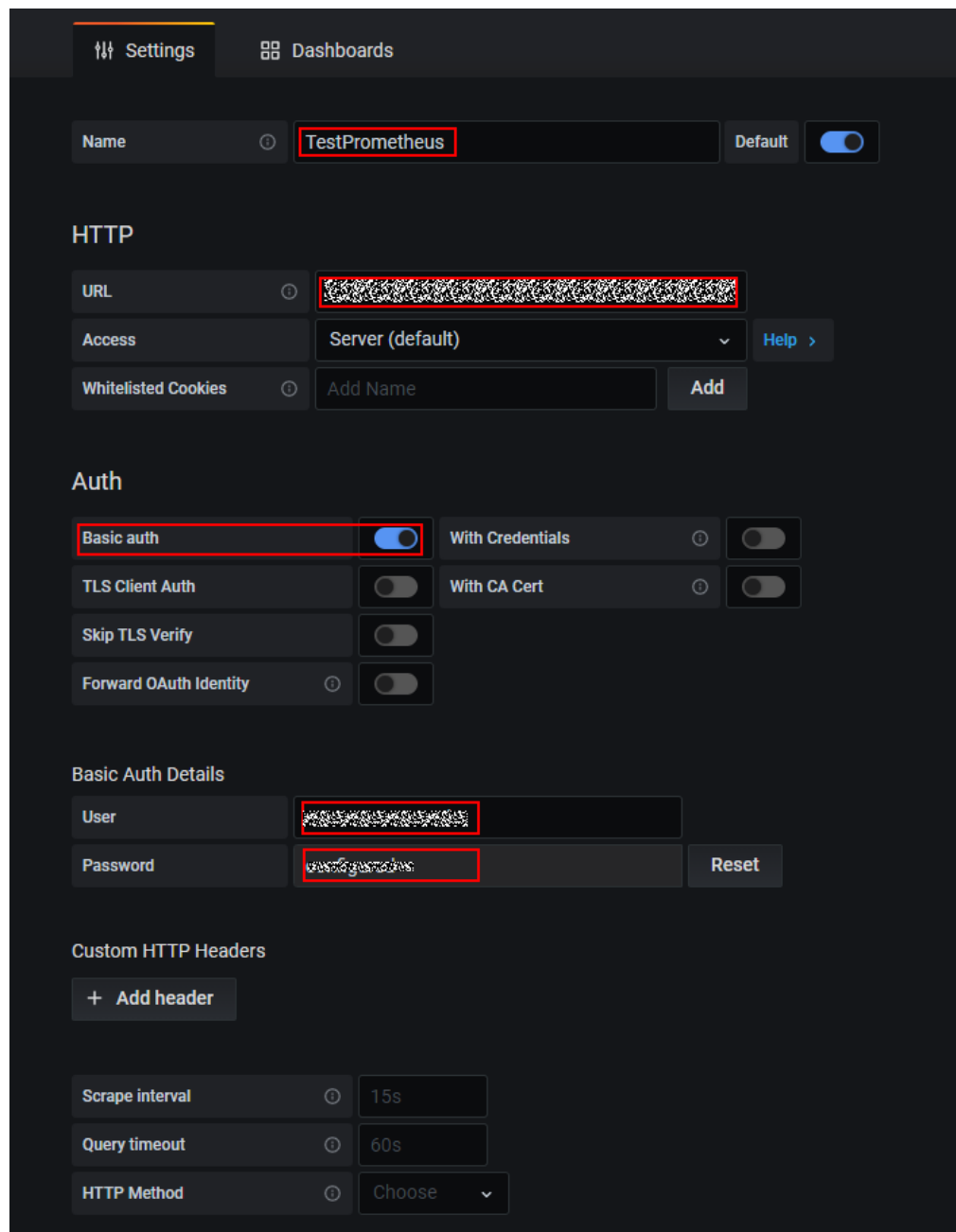


4. Set Grafana data source parameters.
 - **URL:** HTTP URL obtained in [Step 3](#).
 - **User:** username obtained in [Step 3](#).
 - **Password:** password obtained in [Step 3](#).

 **NOTE**

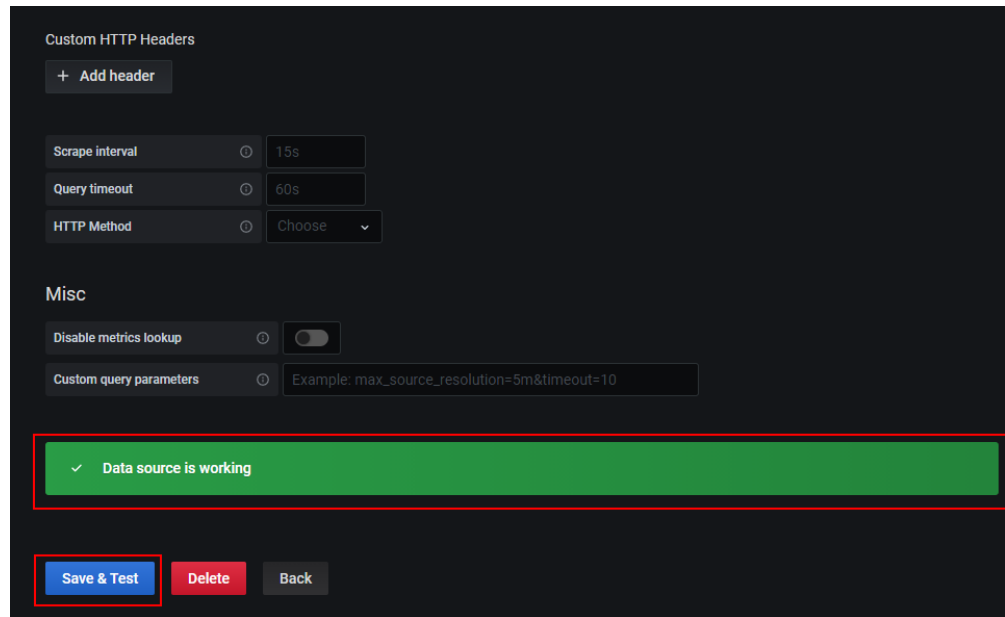
The **Basic auth** and **Skip TLS Verify** options under **Auth** must be enabled.

Figure 7-5 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 7-6 Checking whether the configuration is successful



----End

7.3 Resource Usage Statistics

After metric data is reported to AOM through Prometheus monitoring, you can view the number of reported basic and custom metric samples on the **Resource Usage** page.

Prerequisites

- Your service has been connected for Prometheus monitoring. For more details, see:
 - [7.2.1.2 Prometheus Instance for CCE](#)
 - [7.2.1.3 Prometheus Instance for Remote Write](#)

Precautions

- The **Resource Usage** page does not display the number of basic and custom metric samples reported by Prometheus instances for cloud services.
- Metric samples are reported every hour. If you specify a time range shorter than one hour, the query result of total metric samples may be 0.
- The number of metric samples displayed on the **Resource Usage** page may be different from the actual number.

Procedure

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane, choose **Metric Analysis > Resource Usage**.
- Step 3** In the upper left corner of the page, select a desired Prometheus instance.

Step 4 In the upper right corner of the page, set filter criteria.

1. Set a time range in either of the following ways:

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 30 days at most.

2. Set the interval for refreshing information. Click  and select a value from the drop-down list, such as **Refresh manually** or **1 minute auto refresh**.

Step 5 View the number of basic metrics and that of custom metrics reported by the Prometheus instance.

- **Custom Metric Samples:** include the number of custom metric samples reported within 24 hours and that reported within a specified time range.
- **Basic Metric Samples:** include the number of basic metric samples reported within 24 hours and that reported within a specified time range.
- **Custom Metrics:** indicates the number of custom metric types reported within a specified time range.
- **Basic Metrics:** indicates the number of basic metric types reported within a specified time range.
- **Top 10 Custom Metric Samples:** displays the top 10 custom metric samples within a specified time range.

Step 6 In the **Instance Info** area, view **Total Custom Metric Samples (Million)**, **Total Basic Metric Samples (Million)**, **Custom Metric Samples in 24 Hours (Million)**, **Basic Metric Samples in 24 Hours (Million)**, **Custom Metrics**, and **Basic Metrics**.

----End

8 Log Analysis (Beta)

8.1 Searching for and Viewing Logs

8.1.1 Searching for Logs

AOM enables you to quickly query logs, and locate faults based on log sources and contexts.

Setting a Filter

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Log Analysis (Beta) > Log Search**.

Step 3 In the filter area on the left of the **Log Search** page, filter logs by setting different perspectives (such as cloud log) and parameters. Set log search criteria as prompted.

Step 4 Click **Search**.

If a message indicating that no logs found is displayed, ingest logs by referring to section "Log Ingestion" in *Log Tank Service (LTS) User Guide*.

----End

Searching for Raw Logs

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Log Analysis (Beta) > Log Search**.

Step 3 Set filters by referring to [Setting a Filter](#).

Step 4 In the upper right corner of the **Raw Logs** tab page, select a time range.

Step 5 Search for raw logs in the following ways:

- In the search area, enter a keyword or select a keyword from the drop-down list, and click **Search**.

 NOTE

- After you set log structuring, the drop-down list displays both the built-in fields and fields configured for structuring.
- Built-in fields include **appName**, **category**, **clusterId**, **clusterName**, **collectTime**, **containerName**, **hostIP**, **hostIPv6**, **hostId**, **hostName**, **nameSpace**, **pathFile**, **podName** and **serviceID**. By default, the fields are displayed in simplified mode, and **hostIP**, **hostName**, and **pathFile** are displayed at the beginning.
- The structured fields are displayed in **key:value** format.
- Click a field in blue in the log content and the field will be used as a filter. All logs that meet the filtering criteria are displayed.
- On the **Raw Logs** page, click a field in blue in the log content and the field will be used as a filter. All logs that meet the filtering criteria are displayed.
- Click a field for which quick analysis has been created to add it to the search box.

 NOTE

If the field you click already exists in the search box, it will be replaced by this newly added one. If the field is added the first time, fields in the search box are searched using the AND operator.

- In the search area, press the up and down arrows on the keyboard to select a keyword or search syntax from the drop-down list, press **Tab** or **Enter** to select a keyword or syntax, and click **Search**.

----End

Analyzing Real-Time Logs

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Log Analysis (Beta) > Log Search**.

Step 3 Set filters by referring to [Setting a Filter](#).

Step 4 Click the **Real-Time Logs** tab to view the corresponding real-time logs.

Logs are refreshed every 5s. You may wait for up to 1 minute before the logs are displayed.

You can also customize log display by clicking **Clear** or **Pause** in the upper right corner.

- **Clear:** Displayed logs will be cleared from the real-time view.
- **Pause:** Loading of new logs to the real-time view will be paused.
After you click **Pause**, the button changes to **Continue**. You can click **Continue** to resume the log loading to the real-time view.

 NOTE









Stay on the **Real-Time Logs** tab to keep updating them in real time. If you leave the **Real-Time Logs** tab, logs will not be loaded in real time. The next time you access the tab, the logs that were shown before you left the tab will not be displayed.



----End

Common Log Search Operations

These operations include adding alarms, selecting a time range to display logs, and refreshing logs. For details, see [Table 8-1](#).

Table 8-1 Common operations

Operation	Description
Configuring quick search	Click  and configure quick search .
Refreshing logs	Click  to refresh logs. There are two refresh modes: manual and automatic. <ul style="list-style-type: none"> Manual refresh: Click Refresh Now to refresh logs. Automatic refresh: Select an interval from the drop-down list to automatically refresh logs. The interval can be 15 seconds, 30 seconds, 1 minute, or 5 minutes.
Copying logs	Click  to copy log content.
Viewing the context	Click  to view the log context.
Simplifying field details	Click  to view the simplified field details.
Unfolding	Click  to unfold log content. They will be displayed in different lines.
Downloading logs	Click  . On the page that is displayed, download logs to the local host. <p>Direct Download: Download log files to the local PC. Up to 5000 logs can be downloaded at a time.</p> <p>Select .csv or .txt from the drop-down list and click Download to export logs to the local PC.</p> <p>NOTE</p> <ul style="list-style-type: none"> If you select .csv, logs are exported as a table. If you select .txt, logs are exported as a .txt file.
JSON	Move the cursor over  , click JSON , and set JSON formatting. <p>NOTE</p> <p>Formatting is enabled by default. The default number of expanded levels is 2.</p> <ul style="list-style-type: none"> Formatting enabled: Set the default number of expanded levels. Maximum value: 10. Formatting disabled: JSON logs will not be formatted for display.

Operation	Description
Collapse configuration	<p>Move the cursor over , click Log Collapse, and set the maximum characters to display in a log.</p> <p>If the number of characters in a log exceeds the maximum, the extra characters will be hidden. Click Expand to view all.</p> <p>NOTE Logs are collapsed by default, with a default character limit of 400.</p>
Log time display	<p>Move the cursor over  and click Log time display. On the page that is displayed, set whether to display milliseconds and whether to display the time zone.</p> <p>NOTE By default, the function of displaying milliseconds is enabled.</p>

Syntax and Examples of Searching by Keyword

Search syntax:

Table 8-2 Search syntax

Condition	Description
Exact search by keyword	<p>Enter a keyword (case-sensitive) for exact search. A keyword is the word between two adjacent delimiters.</p> <p>You can add an asterisk (*) after a keyword, for example, error*, if you are not familiar with delimiters.</p>
Exact search by phrase	Enter a phrase (case-sensitive) for exact search.
&&	Intersection of search results.
	Union of search results.
AND	Intersection of search results.
OR	Union of search results.
NOT	Logs that do not contain the keyword after NOT .
?	Fuzzy search. A question mark (?) can be put in the middle or at the end of a keyword to represent a character.
*	Fuzzy search. The asterisk (*) can only be after a keyword. It represents 0–N characters.

 **NOTE**

Operators (such as **&&**, **||**, **AND**, **OR**, **NOT**, *****, **?**, **:**, **>**, **<**, **=**, **>=**, and **<=**) contained in raw logs cannot be used to search for logs.

Search rules:

- Fuzzy search is supported.
For example, if you enter **error***, all logs containing **error** will be displayed and those start with **error** will be highlighted.
- You can use a combination of multiple search criteria in the key and value format: *key1:value1* **AND** *key2:value2* or *key1:value1* **OR** *key2:value2*. After entering or selecting *key1:value1*, you need to add **AND** or **OR** before entering or selecting *key2:value2* in the search box.
- Click a keyword and select one of the three operations from the displayed drop-down list: **Copy**, **Add To Search**, and **Exclude from Search**.
 - **Copy**: Copy the field.
 - **Add To Search**: Add **AND** *field: value* to the search statement.
 - **Exclude from Search**: Add **NOT** *field: value* to the query statement.

Search examples:

- Search for logs containing **start**: Enter **start**.
- Search for logs containing **start to refresh**: Enter **start to refresh**.
- Search for the logs containing both keyword **start** and **unexpected**: Enter **start && unexpected**.
- Search for logs containing both **start** and **unexpected**: Enter **start AND unexpected** or **start and unexpected**.
- Search for the logs containing keyword **start** or **unexpected**: Enter **start || unexpected**.
- Search for logs containing **start** or **unexpected**: Enter **start OR unexpected** or **start or unexpected**.
- Logs that do not contain *query1*: **NOT content: query1** or **not content: query1**.
- **error***: logs that contain **error**.
- **er?or**: logs that start with **er**, is followed by any single character, and end with **or**.
- If your keyword contains a colon (:), use the **content: Keyword** format.
Example: **content: "120.46.138.115:80"** or **content: 120.46.138.115:80**.
- **query1 AND query2 AND NOT content: query3**: logs that contain both *query1* and *query2* but not *query3*.

 **NOTE**

- When you enter a keyword to query logs, the keyword is case-sensitive. Both the log contents you queried and the highlighted log contents are case-sensitive.
- The asterisk (*) and question mark (?) do not match special characters such as hyphens (-) and spaces.
- For fuzzy match, a keyword cannot start with a question mark (?) or an asterisk (*). For example, you can enter **ER?OR** or **ER*R**.

8.1.2 Quickly Analyzing Logs

Monitoring keywords in logs helps you trace system performance and services. For example, the number of **ERROR** keywords indicates the system health, and the

number of **BUY** keywords indicates the sales volume. With AOM quick analysis, your specified keywords can be counted and metric data can be generated for real-time monitoring.

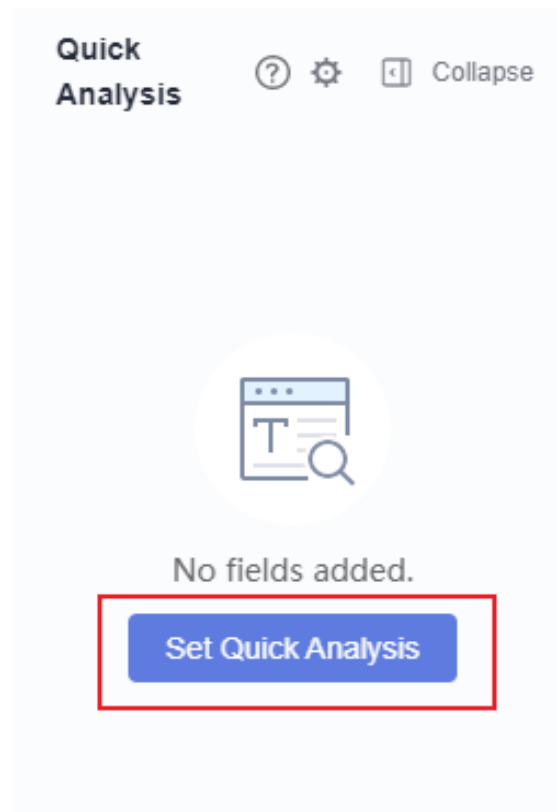
Precautions

Quick analysis is conducted on fields extracted from structured logs. before you create a quick analysis task.

Creating a Quick Analysis Task

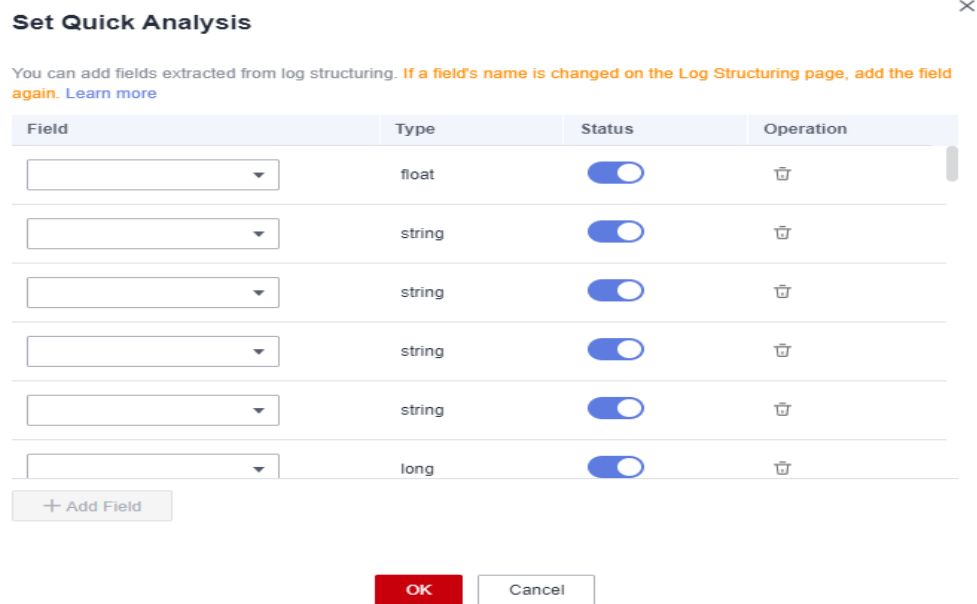
- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane, choose **Log Analysis (Beta) > Log Search**.
- Step 3** On the **Raw Logs** page, click **Set Quick Analysis**, as shown in [Figure 8-1](#).

Figure 8-1 Creating a quick analysis task



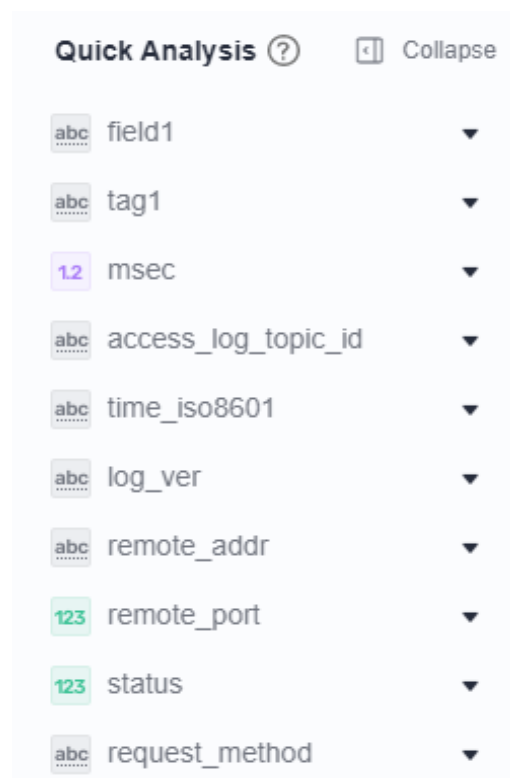
- Step 4** On the displayed **Set Quick Analysis** page, select fields for quick analysis.

Figure 8-2 Adding fields







Step 5 Click **OK**. The quick analysis task is created.

Figure 8-3 Viewing quick analysis results



 **NOTE**

-  indicates a field of the **string** type.
-  indicates a field of the **float** type.
-  indicates a field of the **long** type.
- The maximum length of a field for quick analysis is 2000 bytes.
- The quick analysis field area displays the first 100 records.
- Click  in the upper right corner of the **Quick Analysis** area to modify or delete an existing field. If you delete a field or modify the name of a field on the **Log Structuring** page, the field will be updated in the quick analysis.
- If a structured field does not occur in logs during the specified time range, its occurrence percentage will be displayed as **null**.
 - When you click **null** to **add a float or long field to the search box**, *Field: 0 OR NOT Field: ** will be displayed.
 - When you click **null** to **add a string field to the search box**, *Field: null OR NOT Field: ** will be displayed.

----End

8.1.3 Quickly Querying Logs

To search for logs using a keyword repeatedly, perform the following operations to configure quick search.

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Log Analysis (Beta) > Log Search**.


Step 3 On the **Raw Logs** tab page, click  and configure quick search. For details, see [Table 8-3](#).

Table 8-3 Quick search parameters

Parameter	Description
Name	Quick search name, which is used to distinguish quick search statements. Enter 1 to 64 characters. Only letters, digits, hyphens (-), and underscores (_) are allowed. Do not start with a period (.) or underscore (_) or end with a period.
Keyword	Keyword that needs to be repeatedly used during log search, for example, error* .

Step 4 Click **OK**.

After the creation is complete, click the quick query name to quickly view log details.


----End

8.1.4 Viewing the Context

You can check the logs generated before and after a log for quick fault locating.

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Log Analysis (Beta) > Log Search**.

Step 3 On the **Raw Logs** tab page, click  to view the context.

The context of the log is displayed.

----End

9 Container Insights

9.1 Workload Monitoring

Workload monitoring is for CCE workloads. It enables you to monitor the resource usage, status, and alarms of workloads in a timely manner so that you can quickly handle alarms or events to ensure smooth workload running. Workloads are classified into Deployments, StatefulSets, DaemonSets, Jobs, and Pods.

Functions

- The workload monitoring solution is ready-to-use. After AOM is enabled, the workload status, CPU usage, and physical memory usage of CCE are displayed on the workload monitoring page by default.
- For customer-built Kubernetes containers, only Prometheus remote write is supported. After container metrics are written into AOM's metric library, you can query metric data by following instructions listed in [7.1 Metric Browsing](#).
- Workload monitoring adopts the layer-by-layer drill-down design. The hierarchy is as follows: workload > Pod instance > container > process. You can view their relationships on the UI. Metrics and alarms are monitored at each layer.

Procedure

Step 1 Log in to the AOM 2.0 console.


Step 2 In the navigation pane, choose **Container Insights > Workload Monitoring**.



Step 3 In the upper right corner of the page, set filter criteria.

1. Set a time range to view the workloads reported. 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 30 days at most.

2. Set the interval for refreshing information. Click  and select a value from the drop-down list, such as **Refresh manually** or **1 minute auto refresh**.

- Step 4** Click any workload tab to view information, such as workload name, status, cluster, and namespace.
- In the upper part of the workload list, filter workloads by cluster or namespace name.
 - Click  in the upper right corner to obtain the latest workload information within the time range specified in [Step 3.1](#).
 - Click  in the upper right corner and select or deselect columns to display.
 - Click the name of a workload to view its details.
 - On the **Pods** tab page, view the all pod conditions of the workload. Click a pod name to view the resource usage and health status of the pod's containers.
 - On the **Monitoring Views** tab page, view the resource usage of the workload.
 - On the **Alarms** tab page, view the alarm details of the workload. For details, see [6.3 Viewing Alarms](#).
 - On the **Events** tab page, view the event details of the workload. For details, see [6.4 Viewing Events](#).

----End

9.2 Cluster Monitoring

Clusters deployed using CCE are monitored. On the **Cluster Monitoring** page, you can view multiple basic metrics (such as cluster status, CPU usage, memory usage, and node status), and related alarms and events in real time. Based on them, you can monitor cluster statuses and handle risks in a timely manner, ensuring stable cluster running.

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.


Procedure

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane, choose **Container Insights > Cluster Monitoring**.
- Step 3** In the upper right corner of the page, set cluster filter criteria.
1. Set a time range to view the CCE clusters that report information. 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 30 days at most.

2. Set the interval for refreshing information. Click  and select a value from the drop-down list, such as **Refresh manually** or **1 minute auto refresh**.

Step 4 Set search criteria (such as the creation time, CPU usage, and cluster name) to find the target cluster.


Step 5 Click a cluster to go to its details page. In the navigation pane on the left, monitor cluster running conditions by cluster, dashboard, or alarm.


- View information about nodes, workloads, pods (container groups), and containers by cluster.
 - In the navigation pane on the left, choose **Insights > Node** to view information about all nodes in the cluster in real time, including the status, IP address, pod status, CPU usage, and memory usage.
 - In the upper part of the node list, filter nodes by node name.
 - Click  in the upper right corner and select or deselect options as required.
 - Click a node to view its related resources, alarms, and events, and common system devices such as GPUs and NICs.
 - On the **Overview** tab page, **Cloud-Native Monitoring (New)** is selected by default. You can view metrics such as CPU, memory, and network. Click **Using ICAgent (Old)** and select a target Prometheus instance from the drop-down list. You can view metrics such as CPU, physical memory, and host status.


 **NOTE**


To use cloud-native monitoring, connect your cluster to a Prometheus instance for CCE first.

If there is no Prometheus instance for CCE, click **Prometheus Monitoring** to create a Prometheus instance by referring to [7.2.1.2 Prometheus Instance for CCE](#). After the instance is created, click its name. On the instance details page, choose **Integration Center** and then connect the CCE cluster.




 Last 30 minutes ▾

Click  in the upper right corner and select a predefined time label or customize a time range from the drop-down list to view resource information.

Click  in the upper right corner to obtain the latest resource information in real time.

Click  in the upper right corner of the page to view resource information in full screen.

- On the **Related Resources** tab page, the pod (container group) to which the node belongs is displayed.
- In the navigation pane on the left, choose **Insights > Workload** to view the status and resource usage of all workloads in the cluster.

- In the upper part of the workload list, filter workloads by workload name.
- Click  in the upper right corner and select or deselect options as required.
- Click a workload to view its related resources, alarms, events, and dashboards.
 - On the **Overview** tab page, **Cloud-Native Monitoring (New)** is selected by default. You can view metrics such as CPU, memory, and network. Click **Using ICAgent (Old)** and select a target Prometheus instance from the drop-down list. You can view metrics such as CPU, physical memory, and file system.
 - On the **Related Resources** tab page, the pod (container group) to which the workload belongs is displayed.
- In the navigation pane on the left, choose **Insights > Pod** to view the status and resource usage of all pods in the cluster.
 - In the upper part of the container group list, filter container groups by name.
 - Click  in the upper right corner and select or deselect options as required.
 - Click a container group to view its related resources, alarms, events, and dashboards.
 - On the **Overview** tab page, **Cloud-Native Monitoring (New)** is selected by default. You can view metrics such as CPU, memory, and network. Click **Using ICAgent (Old)** and select a target Prometheus instance from the drop-down list. You can view metrics such as CPU, physical memory, and file system.
 - On the **Related Resources** tab page, view nodes, workloads, and containers by name.
- In the navigation pane on the left, choose **Insights > Container** to view the status and resource usage of all containers in the cluster.
 - In the upper part of the container list, filter containers by name.
 - Click  in the upper right corner and select or deselect options as required.
 - Click a container to view its related resources, alarms, events, and dashboards. On the **Related Resources** tab page, the container group to which the container belongs is displayed by default. View nodes, workloads, and container groups by name.
- View the cluster running status from the alarm management perspective.
 - In the navigation pane on the left, choose **Alarm Management > Alarm List** to view alarm details of the cluster. For details, see [6.3 Viewing Alarms](#).

- In the navigation pane on the left, choose **Alarm Management > Event List** to view event details of the cluster. For details, see [6.4 Viewing Events](#).
- In the navigation pane on the left, choose **Alarm Management > Alarm Rules** to view the alarm rules related to the cluster. Modify the alarm rules as required. For details, see [6.1.4 Managing Alarm Rules](#).
- In the navigation pane on the left, choose **Dashboard** to view the running status of the current cluster.
 - A CCE Prometheus instance has been connected:
Select **Cluster View**, **Pod View**, **Host View**, or **Node View** from the drop-down list to view key metrics such as the CPU usage and physical memory usage.
 - No CCE Prometheus instance is connected:
Choose **Prometheus Monitoring** and then add a Prometheus instance. For details, see [7.2.1.2 Prometheus Instance for CCE](#) After the instance is created, click its name. On the instance details page, choose **Integration Center** and then connect the CCE cluster.

----End

10 Infrastructure Monitoring

10.1 Host Monitoring

Hosts include the Elastic Cloud Server (ECS) and Bare Metal Server (BMS). AOM can monitor the hosts created during CCE and ServiceStage cluster creation and those created in non-CCE and -ServiceStage environments. In addition, hosts support IPv4 addresses.

Host monitoring displays resource usage, trends, and alarms, so that you can quickly respond to malfunctioning hosts and handle errors to ensure smooth host running.



Precautions

- A maximum of five tags can be added to a host, and each tag must be unique.
- The same tag can be added to different hosts.

Procedure

Step 1 Log in to the AOM 2.0 console.

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

- Set filter criteria (such as the running status, host type, host name, and IP address) above the host list.
- You can enable or disable **Hide master host**. By default, this option is enabled.
- Click  next to **Hide master host** to synchronize host information.
- In the upper right corner of the page, set filter criteria.
 - 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. 30 days).
 - 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.

- 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.

- **Adding a tag**

Tags are identifiers of hosts. You can manage hosts using tags. After a tag is added, you can quickly identify and select a host.

In the host list, click  in the **Operation** column of the target host. In the displayed dialog box, enter a tag key and value, and click  and **OK**.

- **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. On the displayed host details page, you can view the running status and ID of the host.

Step 6 Click any tab. In the list, you can monitor the instance resource usage and health status, and information about common resources such as GPUs and NICs.

- On the **Process List** tab page of the ECS host, you can view the process status and IP address of the host.
 - In the search box in the upper right corner of the process list, you can set search criteria such as the process name to filter processes.
 - Click  in the upper right corner to obtain the latest process information within the specified time range.
- On the **Pods** tab page of the CCE host, you can view the pod status and node IP address.
 - Click a pod name to view details about the container and process of the pod.
 - In the search box in the upper right corner of the pod list, you can set search criteria such as pod names to filter pods.
 - Click  in the upper right corner to obtain the latest pod information within the specified time range.

- On the **Monitoring Views** tab page, view key metric graphs of the host.
- On the **Events** tab page, view the event details of the host. For details, see [6.4 Viewing Events](#).
- On the **Alarms** tab page, view the alarm details of the host. For details, see [6.3 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 Views** page.
- On the **Disks** tab page, view the basic information about the disks of the host. Click a disk to monitor its metrics on the **Monitoring Views** page.
- On the **Disk Partitions** tab page, view the disk partition information about the host. Click a disk partition to monitor its metrics on the **Monitoring Views** page.
- Click the **NICs** tab to view the basic information about the NICs of the host. Click a NIC to monitor its metrics on the **Monitoring Views** page.
- Click the **GPUs** tab to view the basic information about the GPUs of the host. Click a GPU to monitor its metrics on the **Monitoring Views** page.
- On the **File Systems, Disks, Disk Partitions, NICs, or GPUs** tab page, click  in the upper right corner of the resource list and select or deselect items to display.

 **NOTE**

Disk partitions are supported by CentOS 7.x and EulerOS 2.5.

----End

11 Process Monitoring

11.1 Application Monitoring


An application groups identical or similar components based on service 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.



After application discovery rules are set, AOM automatically discovers applications that meet the rules and monitors related metrics. For details, see [11.3 Application Discovery](#).

Procedure

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Process Monitoring > Application Monitoring**. On the displayed page, view the application list.

- Set filter criteria in the search box to filter applications.
- Click  in the upper right corner of the page and select or deselect the items to display.


Step 3 Click  **Last 30 minutes**  in the upper right corner of the page and select a desired value from the drop-down list.

1. Set a time range to view applications. There are two methods to set a time range:

Method 1: Use a predefined time label, such as **Last 30 minutes** or **Last hour** in the upper right corner of the page. 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 30 days at most.

2. Set the interval for refreshing information. Click   and select a value from the drop-down list, such as **Refresh manually** or **1 minute auto refresh**.

- Step 4** Click an application name. On the page that is displayed, you can view the component list, host list, monitoring views, and alarms of the current application.
- On the **Component List** tab page, you can view the running status and resource usage of components.
 - On the **Host List** tab page, you can view the running status and resource usage of hosts.
 - On the **Monitoring Views** tab page, select a desired Prometheus instance to view the resource usage of the application. Click  in the upper right corner of the page to view resource information in full screen.
 - On the **Alarms** tab page, view the alarm details of the application. For details, see [6.3 Viewing Alarms](#).


----End

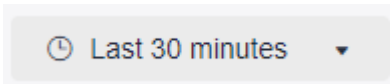
11.2 Component Monitoring

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

The component list displays the name, running status, and application of each component. AOM supports drill-down from a component to an instance, and then to a process. By viewing the status of each layer, you can implement dimensional monitoring for components.

Procedure


- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane, choose **Process Monitoring > Component Monitoring**. On the displayed page, view the component list.
- 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** as required. By default, system components are hidden.
 - Click  in the upper right corner of the page and select or deselect the columns to display.

- Step 3** Click  in the upper right corner of the page and select a desired value from the drop-down list.

1. Set a time range to view components. There are two methods to set a time range:

Method 1: Use a predefined time label, such as **Last 30 minutes** or **Last hour** in the upper right corner of the page. 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 30 days at most.

2. Set the interval for refreshing information. Click  and select a value from the drop-down list, such as **Refresh manually** or **1 minute auto refresh**.

Step 4 Perform the following operations as required:


- **Adding an alias**

If a component name is complex 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.

- **Adding a tag**

Tags are identifiers of components. You can distinguish system components from non-system components based on tags. By default, AOM adds the **System Service** tag to system components (including icagent, css-defender, nvidia-driver-installer, nvidia-gpu-device-plugin, kube-dns, org.tanukisoftware.wrapper.WrapperSimpleApp, evs-driver, obs-driver, sfs-driver, icwatchdog, and sh).

In the component list, click  in the **Operation** column of the target component. In the displayed dialog box, enter a tag key and value, click



, select the **Mark as system component** check box, and click **OK**.

 **NOTE**

- A maximum of five tags can be created for each component.
- Tag key: max. 36 characters; tag value: max. 43 characters
- A tag value can contain only letters, digits, hyphens (-), and underscores (_).

Step 5 Set filter criteria to search for the desired component.

 **NOTE**


Components cannot be searched by alias.

Step 6 Click the component name. The component details page is displayed.

- On the **Instance List** tab page, view the instance details.

 **NOTE**

Click an instance name to view the monitoring view and alarm information.

- On the **Host List** tab page, view the host details.
- On the **Monitoring Views** tab page, select a desired Prometheus instance to view the resource usage of the component. Click  in the upper right corner of the page to view resource information in full screen.
- On the **Alarms** tab page, view the alarm details of the component. For details, see [6.3 Viewing Alarms](#).

- On the **Events** tab page, view the event details of the component. For details, see [6.4 Viewing Events](#).

----End

11.3 Application Discovery

AOM can discover applications and collect their metrics based on configured rules. There are two modes to configure application discovery: auto mode and manual mode. This section mainly describes the manual mode.

- **Auto mode**

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

- **Manual mode**

If you customize an application discovery rule and apply it to the host where the ICAgent is installed, the ICAgent discovers applications on the host based on the custom rule and displays them on the **Application Monitoring** page.

Filtering Rules

The ICAgent periodically detects 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 11-1](#). 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.

Information similar to the following is displayed:

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 11-1 Filtering rules

Filtering Rule	Example
If the COMMAND value of a process is docker-containe , vi , vim , pause , ssh , ps , sleep , grep , tailf , tail , or systemd-udevd , and the process is not running in a 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 .

Filtering Rule	Example
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) .
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 Discovery Rules

AOM provides two built-in discovery rules: **Sys_Rule** and **Default_Rule**. These rules are executed on all hosts, including hosts added later. The priority of **Sys_Rule** is higher than that of **Default_Rule**. That is, **Sys_Rule** is executed on the host first. If **Sys_Rule** is met, **Default_Rule** is not executed. Otherwise, **Default_Rule** is executed. Rule details are as follows:

Sys_Rule (cannot be disabled)

When **Sys_Rule** is used, the component name and application name must be used together. 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.

Creating a Custom Discovery Rule

Step 1 Log in to the AOM 2.0 console.

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

Step 3 On the displayed page, 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 must add at least one check item and can add up to five check items. 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 20s, modify the discovery rule and detect processes again. Only when at least one process is detected can you proceed to the next step.

Step 6 Set an application name and component name.

1. Set an application name.

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

 **NOTE**

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


2. Set a component name.

In the **Component Name Settings** area, specify an application type and click **Add Naming Rule** to set a component name for the discovered process. For example, add the text **app-test** as a component name.

 **NOTE**

- Application types are specified to identify application categories. They are used only for better rule classification and console display. You can enter any field. For example, enter **Java** or **Python** by technology stack, or enter **collector** or **database** by function.
- If you do not set a component name, the default name **unknownapplicationname** is used.
- When you add multiple naming rules, all the naming rules are combined as the component name of the process. Metrics of the same component are aggregated.

3. Preview the component name.

If the name does not meet your requirements, click  in the **Preview Component Name** table to rename the component.

Step 7 Set a priority and detection range.

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

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

Step 9 After about two minutes, choose **Process Monitoring > Component Monitoring** in the navigation pane to view the monitored components.

----End

More Operations

After creating an application discovery rule, perform the operations listed in [Table 11-2](#) if needed.

Table 11-2 Related operations

Operation	Description
Viewing rule details	In the Name column, click the name of an application discovery rule.

Operation	Description
Starting or stopping rules	<ul style="list-style-type: none"> • Click Start in the Operation column. • Click Stop in the Operation column. After a rule is disabled, AOM does not collect corresponding process metrics.
Deleting rules	<ul style="list-style-type: none"> • To delete a discovery rule, click Delete in the Operation column. • To delete one or more application discovery rules, select them and click Delete above the rule list. <p>NOTE Built-in discovery rules cannot be deleted.</p>
Modifying rules	<p>Click Modify in the Operation column.</p> <p>NOTE Built-in discovery rules cannot be modified.</p>

12 Collection Management

12.1 UniAgent Management

12.1.1 VM Access

12.1.1.1 Installing a UniAgent

Install a UniAgent on a host manually or remotely.

You can select an installation mode based on site requirements.

Table 12-1 Installation modes

Mode	Application Scenario
Manual Installation	When installing a UniAgent for the first time, you must install it manually.
Remote Installation	Ensure that an installation host is available. NOTE An installation host is used to execute commands for remote installation.

Installation Prerequisite

Ensure that the network between the installation host and the host where the UniAgent is to be installed is normal.

Manual Installation

When installing a UniAgent for the first time, you must install it manually.

Step 1 Log in to the AOM 2.0 console.


Step 2 In the navigation pane, choose **Collection Management**.

Step 3 In the navigation tree on the left, choose **UniAgent > VM Access**. On the displayed page, click **Install UniAgent** in the upper right corner. Then, choose **Manual**.

Step 4 On the **Install UniAgent** page, set parameters.

Table 12-2 Parameters for manual installation

Parameter	Description	Example
UniAgent Version	Version of a UniAgent. This parameter is mandatory.	1.0.8
Access Mode	<p>There are two access modes: direct access and proxy access.</p> <ul style="list-style-type: none"> • Direct access: A host is directly accessed. • Proxy access: Select a proxy area where a proxy has been configured and remotely install the UniAgent on a host through the proxy. 	Direct access

Parameter	Description	Example
Installation Command	<p>Command for installing the UniAgent. Commands for Linux and Windows are different.</p> <p>Click  to copy the installation command.</p> <p>Linux</p> <pre>set +o history; curl -k -X GET -m 20 --retry 1 --retry-delay 10 -o /tmp/install_uniagent https://aom-uniagent-xxxxxx/install_uniagent.sh;bash /tmp/install_uniagent -a xxxxxxxxxxx -s xxxxxxxxxxx -p xxxxxx -d https://aom-uniagent-xxxxxx -m https://uniagent.master.cnxxxxxx,https://xx.xx.xx.xx:xxxx -v 1.x.x set -o history;</pre> <p>Windows</p> <ol style="list-style-type: none"> Download the installation package from https://aom-uniagent-{region_name}.obs.{region_name}.{site domain name suffix}+uniagentd-{version}-win32.zip. <i>{region_name}</i> and <i>{version}</i> can be obtained from the installation page. <ul style="list-style-type: none"> <i>region_name</i>: domain name or IP address of the server where the REST service is deployed. The value varies depending on services and regions. Site domain name suffix: site domain name suffix. <i>version</i>: version of the installed UniAgent. Decompress the package, click uniagentd.msi, and specify path C:\uniagentd for installation. Modify the uniagentd.conf file in C:\uniagentd\conf and enter the following configuration: ak=XXXXXXXXXXXXXXXX sk=XXXXXXXXXXXXXXXX master=https://uniagent.master.XXXXXXXXXXX,https://XX.XX.XX.XX:XXXXX Run start.bat in the C:\uniagentd\bin directory as the administrator. <p>NOTE</p> <ul style="list-style-type: none"> If you need to verify the SHA256 value of the Windows installation package, check the file downloaded from https://aom-uniagent-{region_name}.obs.{region_name}.{site domain name suffix}+uniagentd-{version}-win32.zip.sha256. 	Copy the Linux installation command.

Step 5 Copy the installation command and run it on the host to install the UniAgent.

Step 6 View the information on the **VM Access** page.

----End

Remote Installation

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Collection Management**.

Step 3 In the navigation tree on the left, choose **UniAgent > VM Access**. On the displayed page, click **Install UniAgent** in the upper right corner.

Step 4 On the **Install UniAgent** page, choose **Remote** and set parameters.

Table 12-3 Parameters for remotely installing a UniAgent

Parameter	Description	Example
UniAgent Version	Version of a UniAgent. This parameter is mandatory.	1.0.8
Access Mode	There are two access modes: direct access and proxy access. <ul style="list-style-type: none"> • Direct access: A host is directly accessed. • Proxy access: Select a proxy area where a proxy has been configured and remotely install the UniAgent on a host through the proxy. 	Direct access
Proxy Area	When Access Mode is set to Proxy access , you need to select a proxy area or add a proxy area . A proxy area is used to group and manage proxies. A proxy must be a host installed with a UniAgent.	-
Installation Host	An installation host is used to execute commands for remote installation. This parameter is mandatory. If no installation host has been configured, perform the following steps: <ol style="list-style-type: none"> 1. Select Configure Installation Host from the drop-down list. 2. In the dialog box that is displayed, select the host to be set as an installation host and specify its name. 3. Click OK. 	-

Parameter	Description	Example
Hosts to Be Installed with UniAgents	<p>Detailed information about the host where the UniAgent is to be installed. This parameter is mandatory.</p> <p>Click Add Host and enter the following information:</p> <p>Host IP Address: IP address of a host.</p> <p>OS: operating system of the host, which can be Linux or Windows.</p> <p>Login Account: account for logging in to the host. If Linux is used, use the root account to ensure that you have sufficient read and write permissions.</p> <p>Login Port: port for accessing the host.</p> <p>Authentication Mode: Currently, only password-based authentication is supported.</p> <p>Password: password for logging in to the host.</p> <p>Connectivity Test Result: shows whether the network between the installation host and the host where the UniAgent is to be installed is normal.</p> <p>Operation: Delete, Copy, or Test Connectivity.</p> <p>NOTE</p> <ul style="list-style-type: none"> You can click Add Host to add up to 100 hosts. 	-
Install ICAgent	<p>An ICAgent is a plug-in for collecting metrics and logs. The Install ICAgent option is enabled by default. It is optional. Enter an AK and SK to install an ICAgent.</p>	-

Step 5 Click **Install**. After the installation is complete, you can view the UniAgent in the UniAgent list.

----End

UniAgent Statuses

The UniAgent status can be **Running**, **Abnormal**, **Installing**, **Installation failed**, or **Not installed**.

Table 12-4 UniAgent statuses

Status	Description
Running	The UniAgent is working.
Abnormal	The UniAgent is not working. Contact technical support.
Installing	The UniAgent is being installed. NOTE The installation takes about 1 minute to complete.
Installation failed	The UniAgent fails to be installed. Try again.
Not installed	The UniAgent has not been installed on the host. Install the UniAgent by referring to 12.1.1.1 Installing a UniAgent .

12.1.1.2 Operating UniAgents in Batches

You can reinstall, upgrade, uninstall, or delete UniAgents on hosts in batches.

Reinstalling UniAgents

Reinstall UniAgents when they are in the **Abnormal**, **Installation failed**, or **Not installed** state.

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane, choose **Collection Management**.
- Step 3** In the navigation pane, choose **UniAgent > VM Access**.
- Step 4** On the **VM Access** page, select the hosts where UniAgents are to be reinstalled and choose **UniAgent Batch Operation > Reinstall**.
- Step 5** On the page that is displayed, [install UniAgents](#).

 **NOTE**

The IP addresses of the hosts where UniAgents are to be reinstalled cannot be changed.

----End

Upgrading UniAgents

Upgrade your UniAgent to a more reliable, stable new version according to the following procedure:

 **NOTE**

UniAgents will not be automatically upgraded. Manually upgrade them if needed.

- Step 1** In the navigation tree on the left, choose **UniAgent > VM Access**.
 - Step 2** On the **VM Access** page, select the hosts where UniAgents are to be upgraded and choose **UniAgent Batch Operation > Upgrade**.
 - Step 3** On the displayed page, select the target version and click **OK**.
 - Step 4** Wait for about 1 minute until the upgrade is complete.
- End

Uninstalling UniAgents

- Step 1** In the navigation pane, choose **UniAgent > VM Access**.
 - Step 2** On the **VM Access** page, select the hosts where UniAgents are to be uninstalled and choose **UniAgent Batch Operation > Uninstall**.
 - Step 3** In the dialog box that is displayed, click **OK** to uninstall the UniAgents.
- End

Deleting UniAgents

Delete the UniAgents that are not used or cannot be used according to the following procedure:

- Step 1** In the navigation tree on the left, choose **UniAgent > VM Access**.
 - Step 2** On the **VM Access** page, select the hosts where UniAgents are to be deleted and choose **UniAgent Batch Operation > Delete**.
 - Step 3** In the dialog box that is displayed, click **OK** to delete the UniAgents.
- End

12.1.1.3 Operating ICAgents in Batches

Collection Management supports interconnection with ICAgents. You can upgrade or uninstall ICAgents for hosts in batches.

Installing ICAgents

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane, choose **Collection Management**.
- Step 3** In the navigation pane, choose **UniAgent > VM Access**.
- Step 4** On the **VM Access** page, select the hosts where ICAgents are to be installed and choose **ICAgent Batch Operation > Install**.
- Step 5** In the dialog box that is displayed, set required parameters.

Table 12-5 Plug-in operation parameters

Parameter	Description
Operation	Three types of operations are supported: Install , Uninstall , and Upgrade .
Plug-in	ICAgent. The ICAgent of the latest version can be installed.
AK/SK	Access key ID and secret access key. Procedure to obtain an AK/SK: <ol style="list-style-type: none"> 1. Hover over the username at the upper right corner and select My Credentials from the drop-down list. 2. Choose Access Keys in the navigation pane. On the displayed page, click Create Access Key above the list, enter the key description, and click OK. 3. Click Download. Obtain the AK and SK from the credential file.

Step 6 After the settings are complete, click **OK** to install the ICAgents.

----End

Upgrading ICAgents

Step 1 In the navigation pane, choose **UniAgent > VM Access**.

Step 2 On the **VM Access** page, select the hosts where ICAgents are to be upgraded and choose **ICAgent Batch Operation > Upgrade**.

Step 3 In the displayed dialog box, select an ICAgent version and enter an AK/SK.

Table 12-6 Plug-in operation parameters

Parameter	Description
Operation	Select Upgrade .
Plug-in	ICAgent. The ICAgent of the latest version can be installed.
AK/SK	Access key ID and secret access key. Procedure to obtain an AK/SK: <ol style="list-style-type: none"> 1. Hover over the username at the upper right corner and select My Credentials from the drop-down list. 2. Choose Access Keys in the navigation pane. On the displayed page, click Create Access Key above the list, enter the key description, and click OK. 3. Click Download. Obtain the AK and SK from the credential file.

Step 4 After the settings are complete, click **OK** to upgrade the ICAgents.

----End

Uninstalling ICAgents

Step 1 In the navigation pane, choose **UniAgent > VM Access**.

Step 2 On the **VM Access** page, select the hosts where ICAgents are to be uninstalled and choose **ICAgent Batch Operation > Uninstall**.








Step 3 In the dialog box that is displayed, click **OK** to uninstall the ICAgents.

----End

12.1.1.4 Other Operations

On the **UniAgent > VM Access** page, perform the following operations on the hosts where UniAgents are installed if needed:

Table 12-7 Related operations

Operation	Description
Searching for a host	In the search box above the host list, search for a host by host IP address, imported IP address, host name, installation host name, or proxy IP address.
Refreshing the host list	Click  in the upper right corner of the host list to refresh the list.
Customizing columns to display	Click  in the upper right corner of the host list to select the columns to display.
Filtering hosts	In the table heading of the host list, click  to filter hosts.
Sorting hosts	In the table heading of the host list, click  next to UniAgent Heartbeat Time to sort hosts.  indicates the default order.  indicates the ascending order (that is, the host with the latest UniAgent heartbeat time is displayed at the end).  indicates the descending order (that is, the host with the latest UniAgent heartbeat time is displayed at the top).
Viewing execution logs	Execution logs record the latest UniAgent installation, uninstallation and upgrade operations. Locate the desired host/IP address and click View Log in the Operation column. In the dialog box that is displayed, view UniAgent execution logs.

Operation	Description
Deleting a host	If a UniAgent is Abnormal, Not installed, or Installation failed , you can delete the corresponding host. Locate the target host and choose More > Delete in the Operation column.
Configuring an installation host	To set the name of an installation host, do as follows: Choose More > Configure Installation Host in the Operation column, and enter a desired name.
Canceling an installation host	To cancel an installation host, perform the following steps: Choose More > Cancel Installation Host in the Operation column to cancel an installation host.

12.1.2 CCE Access

CCE Access displays all the CCE clusters under your account. You can install, upgrade, and uninstall ICAGents on hosts in these clusters in batches.

Prerequisites

You already have a CCE cluster.

Viewing Clusters

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Collection Management**.

Step 3 In the navigation pane, choose **UniAgent > CCE Access** to view the connected CCE clusters. You can enter a keyword in the search box to search for your target cluster.

----End

Operating ICAGents

You can install, upgrade, and uninstall ICAGents on hosts in connected CCE clusters.

- Installing ICAGents: If no ICAGent has been installed on the hosts in a cluster, install ICAGents on them in batches.
 - a. In the **Cluster Name** area, locate the target cluster and click **Install ICAGent**.
 - b. On the page that is displayed, click **Yes** to install ICAGents on all hosts in the cluster.
- Upgrading ICAGents: If the ICAGents installed on hosts in a cluster are of an earlier version, upgrade ICAGents in batches.
 - a. In the **Cluster Name** area, locate the target cluster and click **Upgrade ICAGent**.

- b. On the page that is displayed, click **Yes** to upgrade ICAgents on all hosts in the cluster.
- Uninstalling ICAgents: Uninstall ICAgents from all hosts in a cluster if needed.
 - a. In the **Cluster Name** area, locate the target cluster and click **Uninstall ICAgent**.
 - b. On the page that is displayed, click **Yes** to uninstall ICAgents from all hosts in the cluster.

 **NOTE**

Uninstalling ICAgents will cause some application O&M functions to be unavailable. Exercise caution when performing this operation.

12.1.3 Proxy Area Management

To enable network communication between different clouds, set the ECS to a proxy. AOM then delivers deployment and control instructions to remote hosts and receives O&M data through the proxy. A proxy area contains multiple proxies for high availability.

12.1.3.1 Proxy Area

Proxy areas are used to manage proxy by category.

Adding a Proxy Area

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane, choose **Collection Management**.
- Step 3** In the navigation tree on the left, choose **UniAgent > Proxy Areas**. The **Proxy Areas** page is displayed.
- Step 4** Click **Add Proxy Area**. In the dialog box that is displayed, set parameters.

Table 12-8 Parameters for adding a proxy area

Parameter	Description	Example
Proxy Area Name	Enter a maximum of 64 characters.	test


- Step 5** Click **OK**. The proxy area is added.

----End

Modifying a Proxy Area

After the proxy area is created, you can modify it as required. The procedure is as follows:

- Step 1** In the navigation tree on the left, choose **UniAgent > Proxy Areas**. The **Proxy Areas** page is displayed.

Step 2 Hover over the target proxy area and choose  > **Edit**.

Step 3 In the displayed dialog box, enter a new name, and click **OK**.

----End

Deleting a Proxy Area

You can delete a proxy area that is no longer used. The procedure is as follows:

Step 1 In the navigation tree on the left, choose **UniAgent > Proxy Areas**. The **Proxy Areas** page is displayed.


Step 2 Hover over the target proxy area and choose  > **Delete**.

Step 3 In the dialog box that is displayed, click **Yes** to delete the proxy area.

----End

Searching for a Proxy Area

Step 1 In the navigation tree on the left, choose **UniAgent > Proxy Areas**. The **Proxy Areas** page is displayed.

Step 2 Click . Then, in the search box, enter a keyword to search for your target proxy area.

----End

12.1.3.2 Proxy

A proxy is an ECS under your account for network communication between different clouds.

Adding a Proxy

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Collection Management**.

Step 3 In the navigation tree on the left, choose **UniAgent > Proxy Areas**. The **Proxy Areas** page is displayed.

Step 4 Click **Add Proxy** and set related parameters.

Table 12-9 Parameters for adding a proxy

Parameter	Description	Example
Proxy Area	Select a proxy area that you have created.	qwertyddfsdfdf
Host	Select a host where the UniAgent has been installed.	-

Parameter	Description	Example
Proxy IP Address	Set the IP address of the proxy.	-
Port	Enter a port number, which cannot be greater than 65535.	-

Step 5 Click **Yes**. The proxy is added.

----End

Modifying a Proxy IP Address

After a proxy is created, you can change its IP address as required. The procedure is as follows:

Step 1 In the navigation tree on the left, choose **UniAgent > Proxy Areas**. The **Proxy Areas** page is displayed.

Step 2 Click **Modify Proxy IP** in the **Operation** column of the proxy. On the page that is displayed, modify the proxy IP address.

Step 3 Click **Yes**. The proxy IP address is modified.

----End

Viewing a Proxy

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Collection Management**.

Step 3 In the navigation tree on the left, choose **UniAgent > Proxy Areas**. The **Proxy Areas** page is displayed.

Step 4 Click a proxy area to view the proxy in it.

----End

Deleting a Proxy

You can delete a proxy that is no longer used. The procedure is as follows:

Step 1 In the navigation tree on the left, choose **UniAgent > Proxy Areas**. The **Proxy Areas** page is displayed.

Step 2 Click **Delete** in the **Operation** column of the target proxy.

Step 3 In the dialog box that is displayed, click **Yes** to delete the proxy.

----End

12.1.4 Historical Tasks

Historical tasks record the operations (such as installation, upgrade, and uninstallation) performed on UniAgents and ICAgents.

Viewing Historical UniAgent Tasks

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Collection Management**.

Step 3 In the navigation tree on the left, choose **UniAgent > Historical Tasks**. Then, click the **Historical UniAgent Tasks** tab.

 **NOTE**

You can search for historical tasks by date. The options are **Last hour**, **Last 6 hours**, **Last day**, **Last 3 days**, and **Custom**.

Step 4 Click a task ID to view the details of a historical UniAgent task.

----End

Viewing Historical ICAgent Tasks

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Collection Management**.

Step 3 In the navigation tree on the left, choose **UniAgent > Historical Tasks**. On the displayed page, click the **Historical ICAgent Tasks** tab.

 **NOTE**

You can search for historical tasks by date. The options are **Last hour**, **Last 6 hours**, **Last day**, **Last 3 days**, and **Custom**.


Step 4 Click the ID of a desired historical ICAgent task to view details.





----End

Other Operations

On the **Collection Management > Historical Tasks** page, perform the following operations if needed:

Table 12-10 Related operations

Operation	Description
Searching for historical tasks	In the search box above the task list, search for historical tasks by executor.
Filtering historical tasks by time range	In the upper part of the task list, search for historical tasks by time range. The options are Last hour , Last 6 hours , Last day , Last 3 days , and Custom .
Refreshing the task list	Click  in the upper right corner of the task list to refresh the list.

Operation	Description
Viewing task information	Click a task ID to view the task details, including the host name, IP address, plug-in type, task type, execution status, failure cause, execution event, duration, and task logs.
Filtering tasks	In the table heading of the task list, click  to filter tasks.
Sorting tasks	In the table heading of the task list, click  to sort orders.  indicates the ascending order while  indicates the descending order.

13 Configuration Management

13.1 Global Settings

13.1.1 Cloud Service Authorization

Grant permissions to access Resource Management Service (RMS), Log Tank Service (LTS), Cloud Container Engine (CCE), Cloud Container Instance (CCI), Cloud Eye, Distributed Message Service (DMS), and Elastic Cloud Server (ECS). The permission setting takes effect for the entire AOM 2.0 service.

Procedure

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane, choose **Management > Global Configuration**.
- Step 3** In the upper right corner of the cloud service authorization page, click **Authorize** to grant permissions to access the preceding cloud services with one click.

Upon authorization, the **aom_admin_trust** agency will be created in IAM.

If **Cancel Authorization** is displayed in the upper right corner of the page, you have the permissions to access the preceding cloud services.

----End

13.1.2 Access Management

An access code is an identity credential for calling APIs. Create an access code for setting API invocation permissions. The permission setting takes effect for the entire AOM 2.0 service.

Precautions

You can create up to two access codes.



Creating an Access Code

- Step 1** Log in to the AOM 2.0 console.
 - Step 2** In the navigation pane, choose **Management > Global Configuration**.
 - Step 3** In the navigation pane on the left, choose **Authentication**. Click **Add Access Code**.
 - Step 4** In the dialog box that is displayed, click **OK**. The system then automatically generates an access code.
- End

More Operations

After an access code is created, you can perform the operations listed in [Table 13-1](#).

Table 13-1 Related operations

Operation	Description
Viewing an access code	In the list, you can view the ID, access code, status, and creation time.
Searching for an access code	Enter the ID of the access code and click  to search.
Deleting an access code	Click Delete in the Operation column.
Refreshing an access code	Click  to obtain the latest information of the access code.

13.1.3 Global Settings

You can determine whether to enable **Metric Collection** to collect metrics (excluding SLA and custom metrics). You can also determine whether to enable **TMS Tag Display** to display cloud resource tags in alarm notifications to facilitate fault locating. The setting takes effect for entire AOM 2.0.

Procedure

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane, choose **Management > Global Configuration**.
- Step 3** On the displayed page, choose **Global Settings**. Enable or disable functions as required.

 **NOTE**

After metric collection is disabled, ICAgents will stop collecting metric data and related metric data will not be updated. However, custom metrics can still be reported.

----End

14 Remarks

14.1 Alarm Tags and Annotations

When creating alarm rules, you can set alarm tags and annotations. Tags are attributes that can be used to identify alarms. They are applied to alarm noise reduction scenarios. Annotations are attributes that cannot be used to identify alarms. They are applied to scenarios such as alarm notification and message templates.

Alarm Tag Description



- Alarm tags can apply to grouping rules, suppression rules, and silence rules. The alarm management system manages alarms and notifications based on the tags.
- Each tag is in "key:value" format and can be customized. You can create up to 10 custom tags. The key and value can only contain letters, digits, and underscores (_).
- If you set a tag when creating an alarm rule, the tag is automatically added as an alarm attribute when an alarm is triggered.
- In a message template, the `$event.metadata.key1` variable specifies a tag. For details, see [Table 6-23](#).

Alarm Annotation Description




- Annotations are attributes that cannot be used to identify alarms. They are applied to scenarios such as alarm notification and message templates.
- Each annotation is in "key:value" format and can be customized. You can create up to 10 custom annotations. The key and value can only contain letters, digits, and underscores (_).
- In a message template, the `$event.annotations.key2` variable specifies an annotation. For details, see [Table 6-23](#).

Managing Alarm Tags and Annotations

You can add, delete, modify, and query alarm tags or annotations on the alarm rule page.

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane, choose **Alarm Management > Alarm Rules**.
- Step 3** Click **Create Alarm Rule**, or locate a desired alarm rule and click  in the **Operation** column.
- Step 4** On the displayed page, click **Advanced Settings**.
- Step 5** Under **Alarm Tag** or **Alarm Annotation**, click  and enter a key and value.
- Step 6** Click **OK** to add an alarm tag or annotation.

 **NOTE**

- Adding multiple alarm tags or annotations: Click  multiple times to add alarm tags or annotations (max.: 10).
- Modifying an alarm tag or annotation: Move the cursor to a desired alarm tag or annotation and click  to modify them.
- Deleting an alarm tag or annotation: Move the cursor to a desired alarm tag or annotation and click  to delete them.

----End

14.2 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](#).

Examples of Using Prometheus Statements

- **Example 1: Memory usage of a specified pod in a node (excluding the control node)**
 - Define variables:
 - Used memory of the containers in a pod (a pod may contain multiple containers or instances): **aom_container_memory_used_megabytes**
 - Total memory of the node: **aom_node_memory_total_megabytes**
 - Query logic:
 - For **aom_container_memory_used_megabytes**, use the aggregation function **sum** to calculate the actual used memory of a specified pod under a specified node based on the node IP address and pod ID.

- For **aom_node_memory_total_megabytes**, use the aggregation function **sum** to calculate the total memory of a specified node based on the node IP address.
 - Both of them are filtered by node IP address. Therefore, the obtained metric values have the same metric dimension. (Only the values are different.)
 - The actual memory usage of the pod can be obtained by performing the "/" operation on the values of the preceding two metrics.
- To query the actual memory usage of the pod, use the following statement:


```
sum(aom_container_memory_used_megabytes{podID="****1461-41d8-****-bfeb-fc1213****",nodeIP="***.***.***.***"}) by (nodeIP) /
sum(aom_node_memory_total_megabytes{nodeIP="***.***.***.***"}) by (nodeIP)
```
- **Example 2: CPU usage of a specified pod in a node (excluding the control node)**
 - Define variables:
 - Used CPU cores of the containers in a pod:
aom_container_cpu_used_core
 - Actual total number of CPU cores of the node:
aom_node_cpu_limit_core
 - Query logic:
 - For **aom_container_cpu_used_core**, use the aggregation function **sum** to calculate the used CPU cores of a specified pod under a specified node based on the node IP address and pod ID.
 - For **aom_node_cpu_limit_core**, use the aggregation function **sum** to calculate the total CPU cores of a specified node based on the node IP address.
 - Both of them are filtered by node IP address. Therefore, the obtained metric values have the same metric dimension. (Only the values are different.)
 - The actual memory usage of the pod can be obtained by performing the "/" operation on the values of the preceding two metrics.
 - To obtain the actual CPU usage of the pod, use the following statement:


```
sum(aom_container_cpu_used_core{nodeIP="***.***.***.***",podID="****1461-41d8-****-bfeb-****13****"}) by (nodeIP) /
sum(aom_node_cpu_limit_core{nodeIP="***.***.***.***"}) by (nodeIP)
```
- **Example 3: Requested memory of a pod/Allocable memory of the node where the pod is located**
 - Define variables:
 - Memory allocated to the containers in a pod:
aom_container_memory_request_megabytes

- Total memory of the node: **aom_node_memory_total_megabytes**
- Query logic:
 - For **aom_container_memory_request_megabytes**, use the aggregation function **sum** to calculate the allocated memory of a specified pod under a specified node based on the node IP address and pod ID.
 - For **aom_node_memory_total_megabytes**, use the aggregation function **sum** to calculate the total memory of a specified node based on the node IP address.
 - Both of them are filtered by node IP address. Therefore, the obtained metric values have the same metric dimension. (Only the values are different.)
 - The actual memory usage of the pod can be obtained by performing the "/" operation on the values of the preceding two metrics.
- To obtain the actual memory allocation ratio of the pod, use the following statement:

```
sum(aom_container_memory_request_megabytes{podID="*****1461-41d8-4403-****-f***35*****",nodeIP="****.***.***.***"}) by (nodeIP) /  
sum(aom_node_memory_total_megabytes{nodeIP="****.***.***.***"}) by (nodeIP)
```
- **Example 4: Requested CPU cores of a pod/Allocable CPU cores of the node where the pod is located**
 - Define variables:
 - CPU cores allocated to the containers in the pod: **aom_container_cpu_limit_core**
 - CPU cores allocated to the node: **aom_node_cpu_limit_core**
 - Query logic:
 - For **aom_container_cpu_limit_core**, use the aggregation function **sum** to calculate the CPU cores allocated to a specified pod under a specified node based on the node IP address and pod ID.
 - For **aom_node_cpu_limit_core**, use the aggregation function **sum** to calculate the total CPU cores of a specified node based on the node IP address.
 - Both of them are filtered by node IP address. Therefore, the obtained metric values have the same metric dimension. (Only the values are different.)
 - The actual CPU usage of the pod can be obtained by performing the "/" operation on the values of the preceding two metrics.
 - To obtain the actual CPU allocation ratio of the pod, use the following statement:

```
sum(aom_container_cpu_limit_core{podID="*****461-41d8-****-bfef-****135*****",nodeIP="****.***.***.***"}) by (nodeIP) /  
sum(aom_node_cpu_limit_core{nodeIP="****.***.***.***"}) by (nodeIP)
```

Common Prometheus Commands

Table 14-1 lists the common Prometheus commands for querying metrics. You can modify parameters such as the IP address and ID based on site requirements.

Table 14-1 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"}
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="cdbbc06c2c05b58d598e9430fa133aff7_b14ee84c-2b78-4f71-9ecc-2d06e053172c_ca4d29a846e9ad46a187ade88048825e", processName="icwatchdog"}
Cluster disk usage	{clusterId="", clusterName=""}	aom_cluster_disk_usage{clusterId="4ba8008c-b93c-11ec-894a-0255ac101afc", clusterName="servicestage-test"}
Cluster virtual memory usage	{clusterId="", clusterName=""}	aom_node_virtual_memory_usage{nodeIP="192.168.10.4", clusterId="af3cc895-bc5b-11ec-a642-0255ac101a0b", nameSpace="default"}

Metric	Tag Definition	PromQL
Available cluster virtual memory	{clusterId="",clusterName=""}	aom_cluster_virtual_memory_free_megabytes{clusterId="4ba8008c-b93c-11ec-894a-0255ac101afc",clusterName="servicestage-test"}
Workload file system usage	{appName="",serviceID="",clusterId="",nameSpace=""}	aom_container_filesystem_usage{appName="icagent",serviceID="cfebc2222b1ce1e29ad827628325400e",clusterId="af3cc895-bc5b-11ec-a642-0255ac101a0b",nameSpace="kube-system"}
Pod kernel usage	{podID="",podName=""}	aom_container_cpu_used_core{podID="573663db-4f09-4f30-a432-7f11bdb8fb2e",podName="icagent-bkm6q"}
Container uplink rate (BPS)	{containerID="",containerName=""}	aom_container_network_transmit_bytes{containerID="16bf66e9b62c08493ef58ff2b7056aae5d41496d5a2e4bac908c268518eb2cbc",containerName="coredns"}

14.3 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 14-2 Relationship between the time range and statistical period

Time Range	Statistical Period
Last 30 minutes	1 minute or 5 minutes

Time Range	Statistical Period
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

15 Permissions Management

15.1 Creating a User and Granting Permissions

This section describes the fine-grained permissions management provided by IAM for your AOM. With IAM, you can:

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

If your account does not need individual IAM users, then you may skip over this section.

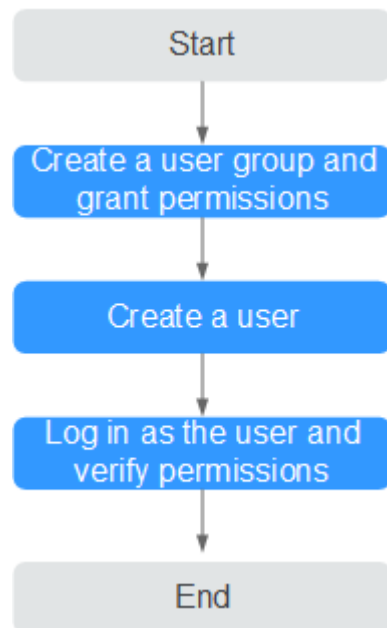
This section describes the procedure for granting permissions (see [Figure 15-1](#)).

Prerequisites

Before assigning permissions to user groups, you should learn about the AOM permissions listed in [Permissions Management](#). For the permissions of other services, see section "Permission Description" in the help center.

Process

Figure 15-1 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 a user and add the user to the user group.
Create a user on the IAM console and add the user to the group created in **1**.
3. Log in as an IAM user and verify permissions.
Log in to the AOM console as the created user, and verify that it only has read permissions for AOM.

15.2 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 alarm rules

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

```

    "Action": [
      "aom:alarmRule:create"
    ]
  }
]
}

```

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

A policy with only "Deny" permissions 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"
      ]
    }
  ]
}

```


16 Auditing

16.1 Operations Logged by CTS

AOM is a one-stop O&M platform that monitors applications and resources in real time. By analyzing dozens of metrics and correlation between alarms and logs, AOM helps O&M personnel quickly locate faults.

You can use AOM to comprehensively monitor and uniformly manage servers, storage, networks, web containers, and applications hosted in Docker and Kubernetes. This effectively prevents problems and helps O&M personnel locate faults in minutes, reducing O&M costs. Also, AOM provides unified APIs to interconnect in-house monitoring or report systems. Unlike traditional monitoring systems, AOM monitors services by application. It meets enterprises' requirements for high efficiency and fast iteration, provides effective IT support for their services, and protects and optimizes their IT assets, enabling enterprises to achieve strategic goals and maximize value. With CTS, you can record operations associated with AOM for future query, audit, and backtracking.

 **NOTE**

pe traces actually record AOM operations, but these operations are performed through CCE or ServiceStage.

Table 16-1 Operations logged by CTS

Function	Operation	Resource Type	Trace
Global Configuration	Adding an access code	icmgr	icmgrAddAccessCode
	Deleting an access code	icmgr	icmgrDelAccessCode
CMDDB	Creating an application	application	createApp
	Updating an application	application	updateApp

Function	Operation	Resource Type	Trace
	Deleting an application	application	deleteApp
	Creating an application (for other services to invoke)	application	createAomApp
	Modifying the EPS ID of an application (for EPS to invoke)	application	updateAppEpsId
	Adding a sub-application	sub_application	createSubApp
	Deleting a sub-application	sub_application	deleteSubApp
	Updating a sub-application	sub_application	updateSubApp
	Creating a sub-application (for other services to invoke)	sub_application	createAomSubApp
	Transferring a sub-application	sub_application	transferSubApp
	Adding a component	component	createComponent
	Transferring a component	component	transferComponent
	Updating a component	component	updateComponent
	Deleting a component	component	deleteComponent
	Creating a component (for other services to invoke)	component	createAomComponent
	Creating an environment	environment	createEnvironment
	Modifying an environment	environment	updateEnvironment

Function	Operation	Resource Type	Trace
	Deleting an environment	environment	deleteEnvironment
	Creating an environment (for other services to invoke)	environment	createAomEnv
	Creating an environment tag	tag	createTag
	Updating a tag	tag	updateTag
	Deleting an environment tag	tag	deleteTag
	Updating an environment tag	tag	updateEnvTag
	Adding a multi-cloud account	cloud_account	addCloudAccount
	Modifying a multi-cloud account	cloud_account	updateCloudAccount
	Deleting a multi-cloud account	cloud_account	deleteCloudAccount
	Creating a workload	workload	createWorkload
	Deleting a workload	workload	deleteWorkload
	Updating a workload	workload	updateWorkload
	Reporting ECS information	ecs	aomImportECS
Resource Monitoring	Creating a dashboard	dashboard	updateDashboard
	Deleting a dashboard	dashboard	deleteDashboard
	Updating a dashboard	dashboard	updateDashboard
	Creating a dashboard group	dashboard_folder	addDashboardFolder
	Updating a dashboard group	dashboard_folder	updateDashboardFolder

Function	Operation	Resource Type	Trace
	Deleting a dashboard group	dashboard_folder	deleteDashboardFolder
	Creating or updating an alarm rule	audit_v4_alarm_rule	addOrUpdateAlarm
	Deleting an alarm rule	audit_v4_alarm_rule	delAlarmRule
	Creating a process discovery rule	appDiscoveryRule	addAppDiscoveryRule
	Updating a process discovery rule	appDiscoveryRule	updateAppDiscoveryRule
	Deleting a process discovery rule	appDiscoveryRule	delAppDiscoveryRule
	Creating a data subscription rule	apminventory	createSubscribeRule
	Verifying DMS connectivity	apminventory	verifyConnect
	Deleting a data subscription rule	apminventory	deleteSubscribeRule
	Adding an alarm template	audit_v4_alarm_rule	addAlarmRuleTemplate
	Modifying an alarm template	audit_v4_alarm_rule	modAlarmRuleTemplate
	Deleting an alarm template	audit_v4_alarm_rule	delAlarmRuleTemplate
	Adding a grouping rule	groupRule	addGroupRule
	Modifying a grouping rule	groupRule	updateGroupRule
	Deleting a grouping rule	groupRule	delGroupRule
	Adding a suppression rule	inhibitRule	addInhibitRule
	Modifying a suppression rule	inhibitRule	updateInhibitRule
	Deleting a suppression rule	inhibitRule	delInhibitRule

Function	Operation	Resource Type	Trace
	Adding a silence rule	muteRule	addMuteRule
	Modifying a silence rule	muteRule	updateMuteRule
	Deleting a silence rule	muteRule	delMuteRule
	Adding an alarm action rule	actionRule	addActionRule
	Modifying an alarm action rule	actionRule	updateActionRule
	Deleting an alarm action rule	actionRule	delActionRule
	Adding a message template	notificationTemplate	addNotificationTemplate
	Modifying a message template	notificationTemplate	updateTemplate
	Deleting a message template	notificationTemplate	delTemplate

16.2 Querying Real-Time Traces


Scenarios




After you enable CTS and the management tracker is created, CTS starts recording operations on cloud resources. After a data tracker is created, the system starts recording operations on data in OBS buckets. CTS stores operation records generated in the last seven days.

This section describes how to query and export operation records of the last seven days on the CTS console.


- [Viewing Real-Time Traces in the Trace List of the New Edition](#)
- [Viewing Real-Time Traces in the Trace List of the Old Edition](#)



Viewing Real-Time Traces in the Trace List of the New Edition

1. Log in to the management console.
2. Click  in the upper left corner and choose Management & Deployment > **Cloud Trace Service**. The CTS console is displayed.
3. Choose **Trace List** in the navigation pane on the left.

4. On the **Trace List** page, use advanced search to query traces. You can combine one or more filters.
 - **Trace Name:** Enter a trace name.
 - **Trace ID:** Enter a trace ID.
 - **Resource Name:** Enter a resource name. If the cloud resource involved in the trace does not have a resource name or the corresponding API operation does not involve the resource name parameter, leave this field empty.
 - **Resource ID:** Enter a resource ID. Leave this field empty if the resource has no resource ID or if resource creation failed.
 - **Trace Source:** Select a cloud service name from the drop-down list.
 - **Resource Type:** Select a resource type from the drop-down list.
 - **Operator:** Select one or more operators from the drop-down list.
 - **Trace Status:** Select **normal**, **warning**, or **incident**.
 - **normal:** The operation succeeded.
 - **warning:** The operation failed.
 - **incident:** The operation caused a fault that is more serious than the operation failure, for example, causing other faults.
 - Time range: Select **Last 1 hour**, **Last 1 day**, or **Last 1 week**, or specify a custom time range.
5. On the **Trace List** page, you can also export and refresh the trace list, and customize the list display settings.
 - Enter any keyword in the search box and press Enter to filter desired traces.
 - Click **Export** to export all traces in the query result as an .xlsx file. The file can contain up to 5000 records.
 - Click  to view the latest information about traces.
 - Click  to customize the information to be displayed in the trace list. If **Auto wrapping** is enabled () , excess text will move down to the next line; otherwise, the text will be truncated. By default, this function is disabled.
6. For details about key fields in the trace structure, see section "Trace References" > "Trace Structure" and section "Trace References" > "Example Traces".
7. (Optional) On the **Trace List** page of the new edition, click **Go to Old Edition** in the upper right corner to switch to the **Trace List** page of the old edition.

Viewing Real-Time Traces in the Trace List of the Old Edition

1. Log in to the management console.
2. Click  in the upper left corner and choose **Management & Deployment** > **Cloud Trace Service**. The CTS console is displayed.
3. Choose **Trace List** in the navigation pane on the left.

4. Each time you log in to the CTS console, the new edition is displayed by default. Click **Go to Old Edition** in the upper right corner to switch to the trace list of the old edition.
5. Set filters to search for your desired traces. The following filters are available:
 - **Trace Type, Trace Source, Resource Type, and Search By:** Select a filter from the drop-down list.
 - If you select **Resource ID** for **Search By**, specify a resource ID.
 - If you select **Trace name** for **Search By**, specify a trace name.
 - If you select **Resource name** for **Search By**, specify a resource name.
 - **Operator:** Select a user.
 - **Trace Status:** Select **All trace statuses, Normal, Warning, or Incident.**
 - Time range: You can query traces generated during any time range in the last seven days.
 - Click **Export** to export all traces in the query result as a CSV file. The file can contain up to 5000 records.
6. Click **Query**.
7. On the **Trace List** page, you can also export and refresh the trace list.
 - Click **Export** to export all traces in the query result as a CSV file. The file can contain up to 5000 records.
 - Click  to view the latest information about traces.
8. Click  on the left of a trace to expand its details.

Trace Name	Resource Type	Trace Source	Resource ID	Resource Name	Trace Status	Operator	Operation Time	Operation
createDockerConfig	dockerlogincmd	SWR	-	dockerlogincmd	normal		Nov 16, 2023 10:54:04 GMT+08:00	View Trace

```

request
trace_id
code 200
trace_name createDockerConfig
resource_type dockerlogincmd
trace_rating normal
api_version
message createDockerConfig, Method: POST URI=/v2/management/ultrasecret, Reason:
source_ip
domain_id
trace_type ApiCall
        
```

9. Click **View Trace** in the **Operation** column. The trace details are displayed.

View Trace ×

```
{
  "request": "",
  "trace_id": " ",
  "code": "200",
  "trace_name": "createDockerConfig",
  "resource_type": "dockerlogincmd",
  "trace_rating": "normal",
  "api_version": "",
  "message": "createDockerConfig, Method: POST Url=/v2/manage/utis/secret. Reason:",
  "source_ip": " ",
  "domain_id": " ",
  "trace_type": "ApiCall",
  "service_type": "SWR",
  "event_type": "system",
  "project_id": " ",
  "response": "",
  "resource_id": "",
  "tracker_name": "system",
  "time": "Nov 16, 2023 10:54:04 GMT+08:00",
  "resource_name": "dockerlogincmd",
  "user": {
    "domain": {
      "name": " ",
      "id": " "
```

10. For details about key fields in the trace structure, see section "Trace References" > "Trace Structure" and section "Trace References" > "Example Traces" in the *CTS User Guide*.
11. (Optional) On the **Trace List** page of the old edition, click **New Edition** in the upper right corner to switch to the **Trace List** page of the new edition.

17 Upgrading to AOM 2.0

This section describes how to migrate data from AOM 1.0 to AOM 2.0. Currently, only collector and alarm rule upgrades are supported.

Functions

- **Collector Upgrade**
After the collector is upgraded, the process discovery capability is enhanced and the collector can automatically adapt to functions related to CMDB, and monitoring center.
- **Alarm Rule Upgrade**
After alarm rules are upgraded, alarm rule data is smoothly switched from AOM 1.0 to AOM 2.0, and is automatically adapted to alarm rule functions of AOM 2.0.

Collector Upgrade

- Step 1** Log in to the AOM 1.0 console.
- Step 2** In the navigation pane, choose **Configuration Management > Agent Management**.
- Step 3** Select **Other: custom hosts** from the drop-down list on the right of the page.
- Step 4** Select a host and click **Upgrade ICAgent**.
- Step 5** Select a target AOM 2.0 version from the drop-down list and click **OK**.
- Step 6** Wait for the upgrade. This process takes about a minute. When the ICAgent status changes from **Upgrading** to **Running**, the upgrade is successful.

NOTE

If the ICAgent is abnormal after the upgrade or if the upgrade fails, log in to the host and run the installation command again. Note that there is no need for you to uninstall the original ICAgent.

----End

Alarm Rule Upgrade

Step 1 Log in to the AOM 1.0 console.

Step 2 In the navigation pane on the left, choose **Alarm Center > Alarm Rules**.

Step 3 Select one or more alarm rules and click **Migrate to AOM 2.0** above the rule list.

NOTICE

- Migration cannot be undone. Exercise caution when performing this operation.
- If the alarm rules to be migrated depend on alarm templates, these alarm templates will also be migrated.

Step 4 In the displayed dialog box, click **Confirm**. The selected alarm rules will be migrated to AOM 2.0 in batches.

----End

18 FAQs

18.1 Overview

This chapter describes FAQs about Application Operations Management (AOM).

- [Dashboard](#)
- [Alarm Management](#)
- [Log Analysis](#)
- [Prometheus Monitoring](#)
- [Container Insights](#)
- [Application Monitoring](#)
- [Collection Management](#)
- [Other FAQs](#)

18.2 Dashboard

18.2.1 Can I Import Grafana Views to AOM Dashboards?

Symptom


Can I import Grafana views to AOM dashboards?

Solution

No. However, you can obtain the Prometheus statement of a Grafana view and then create a graph in AOM by using the Prometheus statement.

Procedure:

- Step 1** Log in to Grafana and obtain the Prometheus statement of a Grafana view.
- Step 2** Log in to the AOM 2.0 console.
- Step 3** In the navigation pane, choose **Metric Analysis > Metric Browsing**.

- Step 4** Select a target Prometheus instance from the drop-down list.
- Step 5** Click **Prometheus statement** and enter the Prometheus statement obtained in [Step 1](#).
- Step 6** Select a metric and click  in the upper right corner of the metric list.
- Step 7** In the **Add to Dashboard** dialog box, select a dashboard, set a graph name, and click **Confirm**.
- Then you can view the Grafana view in AOM.
- End

18.3 Alarm Management

18.3.1 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 ServiceStage or CCE) changes.

Differences Between Alarms and Events

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

18.4 Log Analysis

18.4.1 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.

18.4.2 How Do I Check Which Application Generates Logs in AOM?

Symptom

A large number of logs are generated everyday. How do I check which application generates specific logs?

Solution

AOM does not show the applications to which logs belong. To view that, ingest all logs to LTS and use its resource statistics function.

Procedure:

- Step 1** Create a log group and stream for your application. For details, see section "Creating Log Groups and Log Streams" in *LTS User Guide*.
- Step 2** Log in to the LTS console and check detailed resource statistics of top 100 log groups or streams using the resource statistics function.

----End

18.5 Prometheus Monitoring

18.5.1 How Do I Connect Prometheus Data to AOM?

To connect Prometheus data to AOM, do as follows:

- Step 1** Create a Prometheus instance.

For details, see:

- [Prometheus Instance for CCE](#)
- [Prometheus Instance for Remote Write](#)

- Step 2** Report native Prometheus metrics to AOM through the remote write address. For details, see:

[Reporting Prometheus Data to AOM](#)

----End

18.5.2 How Do I Distinguish Basic Metrics from Custom Metrics When Using Prometheus Monitoring?

Log in to the AOM console, go to the Prometheus instance details page, and view the types of metrics that are collected.

Only the default Prometheus instance, and Prometheus instance for CCE or cloud services support the function of viewing metrics.

Procedure:

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane on the left, choose **Prometheus Monitoring > Instances**.
- Step 3** In the instance list, click a desired Prometheus instance. The instance details page is displayed.
- Step 4** In the navigation pane on the left, choose **Service Discovery**. On the **Metrics** tab page, view the metric names and types of the current Prometheus instance.

----End

18.6 Container Insights

18.6.1 Why Can't AOM Detect Workloads After the Pod YAML File Is Deployed Using Helm?

Symptom

After the pod YAML file is deployed using Helm, AOM cannot detect workloads.

Possible Cause

Compare the YAML file deployed using Helm with that deployed on the CCE console. Environment parameters are found missing in the file deployed using Helm.

Figure 18-1 Comparing YAML files



Solution

- Step 1** Log in to the CCE console and click a target cluster.
- Step 2** Choose **Workloads** in the navigation pane, and select the type of workload whose metrics are to be reported to AOM.
- Step 3** Choose **More > Edit YAML** in the **Operation** column where the target workload is located.
- Step 4** In the displayed dialog box, locate **spec.template.spec.containers**.
- Step 5** Add environment parameters to the end of the **image** field, as shown in [Figure 18-2](#).

Figure 18-2 Adding environment parameters

```
128 spec:
129   replicas: 1
130   selector:
131     matchLabels:
132       app: test
133     version: v1
134   template:
135     metadata:
136       creationTimestamp: null
137     labels:
138       app: test
139     version: v1
140   spec:
141     containers:
142     - name: container-1
143       image: swr.cn-north-4.myhuaweicloud.com/cyd/iapp:latest
144       env:
145       - name: PAAS_APP_NAME
146         value:
147       - name: PAAS_NAMESPACE
148         value:
149       - name: PAAS_PROJECT_ID
150         value:
```

Step 6 Click **Confirm**.

----End

18.7 Application Monitoring

18.7.1 What Are the Differences Between Application Monitoring Under Application Insights and that Under Process Monitoring?

The monitored objects vary depending on the navigation path.

- **Application Insights > Application Monitoring:**
Resources and applications managed using CMDB. You can learn about the resource usage, status, and alarms of applications to quickly respond to requests and ensure smooth system running.
- **Process Monitoring > Application Monitoring:**
Applications discovered based on application discovery rules.

18.8 Collection Management

18.8.1 Are ICAgent and UniAgent the Same?

ICAgent is a plug-in, but UniAgent is not.

- UniAgent is an Agent for unified data collection and serves as the base of the cloud service O&M system. It delivers instructions, such as script delivery and execution, and integrates plug-ins (such as ICAgent, Cloud Eye, and

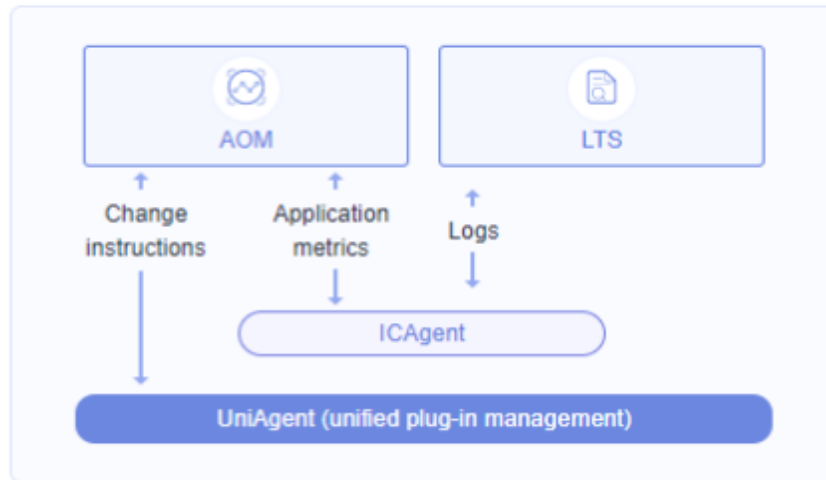
Telescope) and maintains their status. UniAgent provides middleware and custom metric collection capabilities, and provides operations channels for Cloud Operations Center (COC) and Cloud Auto Stress Test (CAST).

NOTE

UniAgent does not collect O&M data; instead, collection plug-ins do that.

- ICAgent collects metrics and logs for AOM and LTS.

Figure 18-3 ICAgent and UniAgent



18.8.2 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. 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 the ICAgent. If the installation still fails, contact technical support.

----End

18.8.3 Why Is an Installed ICAgent Displayed as "Abnormal" on the Agent Management Page?

The AK/SK is invalid, or no agency is set when **Installation Mode** is set to **Create Agency**. Obtain an AK and SK by referring to and install the ICAgent again.

Obtaining an AK/SK

- Step 1** Hover over the username in the upper right corner and select **My Credentials** from the drop-down list.
- Step 2** Choose **Access Keys** in the navigation pane. On the displayed page, click **Create Access Key** above the list, enter the key description, and click **OK**.
- Step 3** Click **Download**.
- Step 4** Obtain the AK and SK from the **credentials** file.

----End

18.8.4 Why Can't I View the ICAgent Status After It Is Installed?

Symptom

After the ICAgent is installed, its status cannot be viewed on the console.

Possible Cause

The virtual NIC is used on the user side. To obtain the ICAgent status, modify the script according to the following procedure.

Solution

- Step 1** Log in to a host where the ICAgent has been installed as the **root** user.
- Step 2** Check the host IP address in use, as shown in [Figure 18-4](#):

```
netstat -nap | grep establish -i
```

Figure 18-4 Checking the host IP address

```

[root@lts-auto-test-wushan-wudong-99404 home]# netstat -nap | grep establish -i
Active Internet connections (servers and established)
tcp        0      0 192.168.0.125:58216 10.247.0.1:443      ESTABLISHED 2122201/icagent
tcp        0      0 192.168.0.125:10255 192.168.0.125:41932 ESTABLISHED 2548046/kubelet
tcp        0      0 192.168.0.125:10250 192.168.0.79:60966 ESTABLISHED 2548046/kubelet
tcp        0      0 127.0.0.1:338      127.0.0.1:28001    ESTABLISHED 2122160/rsyslogd
tcp        0      0 192.168.0.125:40082 100.79.29.98:8149  ESTABLISHED 2122201/icagent
tcp        0      0 127.0.0.1:301      127.0.0.1:41038    ESTABLISHED 2122201/icagent
tcp        0      0 192.168.0.125:34294 100.79.29.98:30201 ESTABLISHED 2122201/icagent
tcp        0      0 192.168.0.125:19901 192.168.0.9:57414  ESTABLISHED 6345/node-problem
tcp        0      0 192.168.0.125:41932 192.168.0.125:10255 ESTABLISHED 2122201/icagent
tcp        0      0 192.168.0.125:41534 100.79.29.98:8149  ESTABLISHED 2122201/icagent
    
```

Step 3 Check the NIC corresponding to the IP address, as shown in [Figure 18-5](#):

```
ifconfig | grep IP address -B1
```

Figure 18-5 Checking the NIC corresponding to the IP address

```

[root@lts-auto-test-wushan-wudong-99404 home]# ifconfig | grep 192.168.0.125 -B1
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.125  netmask 255.255.255.0  broadcast 192.168.0.255
[root@lts-auto-test-wushan-wudong-99404 home]#
    
```

Step 4 Go to the `/sys/devices/virtual/net/` directory and check whether the NIC name exists.

- If it exists, it is a virtual NIC. Then go to [Step 5](#).
- If it does not exist, it is not a virtual NIC. Then contact technical support.

Step 5 Modify the ICAgent startup script:

1. Open the `icagent_mgr.sh` file (command varies depending on the ICAgent version):

```
vi /opt/oss/servicemgr/ICAgent/bin/manual/icagent_mgr.sh
```

Or

```
vi /var/opt/oss/servicemgr/ICAgent/bin/manual/icagent_mgr.sh
```

2. Modify the script file:

Add `export IC_NET_CARD=NIC name` to the file, as shown in [Figure 18-6](#).

Figure 18-6 Modifying the script

```

ICAGENT_CURRENT_PATH=$(cd $(dirname $BASH_SOURCE) && pwd)
APP_ROOT=$ICAGENT_CURRENT_PATH/../../
export APP_ROOT
export ConfFilePath="/opt/oss/servicemgr/ICAgent/enuv"
export GODEBUG=netdns=go
export IC_NET_CARD="eth1"
    
```

Step 6 Restart the ICAgent (commands vary depending on the ICAgent version):

```
sh /opt/oss/servicemgr/ICAgent/bin/manual/mstop.sh
sh /opt/oss/servicemgr/ICAgent/bin/manual/mstart.sh
```

Or

```
sh /opt/oss/servicemgr/ICAgent/bin/manual/mstop.sh
sh /var/opt/oss/servicemgr/ICAgent/bin/manual/mstop.sh
```

Step 7 Log in to the AOM console, choose **Collection Management**, and check whether the ICAgent status is displayed.

- If the ICAgent status is displayed, no further action is required.
- If the ICAgent status is still not displayed, contact technical support.

----End

18.8.5 Why Can't AOM Monitor CPU and Memory Usage After ICAgent Is Installed?

Symptom

AOM cannot monitor information (such as CPU and memory usage) after the ICAgent is installed.

Possible Cause

- Port 8149 is not connected.
- The node time on the user side is inconsistent with the time of the current time zone.

Solution

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

Step 2 Check whether the ICAgent can report metrics:

```
cat /var/ICAgent/oss.icAgent.trace | grep httpsend | grep MONITOR
```

- If the command output contains **failed**, the ICAgent cannot report metrics. In this case, go to [Step 3](#).
- If the command output does not contain **failed**, the ICAgent can report metrics. In this case, go to [Step 4](#).

Step 3 Check whether the port is connected.

1. Obtain the access IP address:

```
cat /opt/oss/servicemgr/ICAgent/envs/ICProbeAgent.properties | grep ACCESS_IP
```

2. Check the connectivity of port 8149:

```
curl -k https://ACCESS_IP:8149
```

- If **404** is returned, the port is connected. In this case, contact technical support.
- If **404** is not returned, the port is not connected. In this case, contact the network administrator to open the port and reinstall the ICAgent. If the installation still fails, contact technical support.

Step 4 Check the node time on the user side:

```
date
```

- If the queried time is the same as the time of the current time zone, contact technical support.
- If they are different, go to [Step 4](#).

Step 5 Reconfigure the node time on the user side:

```
date -s Time of the current time zone (for example, 12:34:56)
```

----End

18.8.6 How Do I Obtain an AK/SK?

Each user can create a maximum of two Access Key ID/Secret Access Key (AK/SK) pairs. Once they are generated, 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 **Create Access Key** above the list and enter the verification code or password.
4. Click **OK** to download the generated AK/SK.

You can obtain the AK from the access key list and SK from the downloaded CSV file.

NOTE

- Keep the CSV file properly. You can only download the file right after the access key is created. If you cannot find the file, you can create an access key again.
- Open the CSV file in the lower left corner, or choose **Downloads** in the upper right corner of the browser and open the CSV file.
- Keep your access keys secure and change them periodically for security purposes.

18.8.7 FAQs About ICAgent Installation

1. What can I do if the network between the ICAgent installation host and target host is disconnected ("[warn] ssh connect failed, 1.2.1.2:22")?
Check network connectivity before installing an Agent, and select an installation host that is accessible from the Internet.
2. What can I do if the heartbeat detection and registration fail and the network is disconnected after I install an ICAgent?
Run the **telnet proxy IP address** command on the target host to check whether the network between the proxy and target host is normal.
3. Ports 8149, 8102, 8923, 30200, 30201, and 80 need to be enabled during ICAgent installation. Can port 80 be disabled after ICAgent is installed?
Port 80 is used only for pulling Kubernetes software packages. You can disable it after installing the ICAgent.
4. Will the ICAgent installed in a Kubernetes cluster be affected after the cluster is upgraded?
After the cluster is upgraded, the system will restart the ICAgent and upgrade it to the latest version.

18.9 Other FAQs

18.9.1 Comparison Between AOM 1.0 and AOM 2.0

Do I Need to Be Authorized to Use AOM 2.0 While I Already Have AOM 1.0 Permissions?

AOM 2.0 billing is different from that of AOM 1.0. If you switch from AOM 1.0 to AOM 2.0 for the first time, apply for the permission to use AOM 2.0 by referring to [Subscribing to AOM 2.0](#).

What Are the Function Differences Between AOM 2.0 and AOM 1.0?

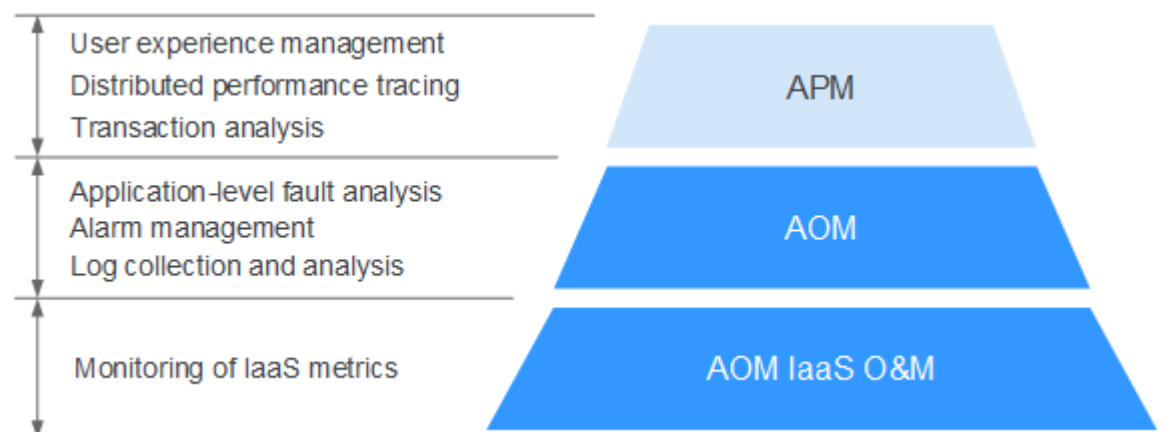
Based on AOM 1.0 functions and common application monitoring, AOM 2.0 collects and monitors more metrics and logs, and displays monitoring results in a visualized manner. For details, see [Comparison Between AOM 1.0 and AOM 2.0](#).

As functions of AOM 1.0 are gradually replaced by those of AOM 2.0, AOM 1.0 will be brought offline soon. You are advised to upgrade AOM 1.0 to AOM 2.0. For details, see [Upgrading to AOM 2.0](#).

18.9.2 What Are the Differences Between AOM and APM?

AOM and Application Performance Management (APM) belong to the multi-dimensional O&M solution and share the ICAgent collector. AOM provides application-level fault analysis, alarm management, and log collection and analysis capabilities, which effectively prevent problems and help O&M personnel quickly locate faults, reducing O&M costs. APM provides user experience management, distributed performance tracing, and transaction analysis capabilities, which help O&M personnel quickly locate and resolve faults and performance bottlenecks in a distributed architecture and optimize user experience. AOM provides basic O&M capabilities. APM is a supplement to AOM.

Figure 18-7 Multi-dimensional O&M solution



18.9.3 What Are the Differences Between the Log Functions of AOM and LTS?

AOM is a one-stop platform for service observability analysis. It integrates the log functions of . Charging data records (CDRs) are reported by LTS instead of AOM. You will not be billed twice.

18.9.4 How Do I Create the apm_admin_trust Agency?

Procedure

- Step 1** Log in to the IAM console.
- Step 2** In the navigation pane, choose **Agencies**.
- Step 3** On the page that is displayed, click **Create Agency** in the upper right corner. The **Create Agency** page is displayed.
- Step 4** Set parameters by referring to [Table 18-1](#).

Table 18-1 Parameters for creating an agency

Parameter	Description	Example
Agency Name	Set an agency name. NOTICE The agency name must be apm_admin_trust .	-
Agency Type	Select Cloud service .	Cloud service
Cloud Service	Select Application Operations Management (AOM) .	-
Validity Period	Select Unlimited .	Unlimited
Description	(Optional) Provide details about the agency.	-

- Step 5** Click **Next**. The **Authorize Agency** page is displayed.
- Step 6** On the **Select Policy/Role** tab page, select **DMS UserAccess** and click **Next**.
DMS UserAccess: Common user permissions for DMS, excluding permissions for creating, modifying, deleting, scaling up instances and dumping.
- Step 7** On the **Select Scope** tab page, set **Scope** to **Region-specific Projects** and select target projects under **Project [Region]**.
- Step 8** Click **OK**.
----End

19 Change History

Table 19-1 Change history

Released On	Description
2024-06-30	This issue is the first release of AOM 2.0.