

Application Operations Management 2.0

User Guide

Date **2025-08-30**

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..... 2
 - 1.5 Relationships Between AOM and Other Services..... 4
 - 1.6 Restrictions..... 7
 - 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 Basic Metrics: ModelArts Metrics..... 59
 - 1.7.5 Metric Dimensions..... 71
 - 1.8 Basic Concepts..... 74
 - 1.8.1 Resource Monitoring..... 74
 - 1.8.2 Collection Management..... 75
 - 1.9 Permissions Management..... 76
 - 1.10 Privacy Statement..... 90
- 2 Getting Started..... 91**
 - 2.1 Monitoring CCE Metrics..... 91
 - 2.2 Using Prometheus to Monitor ECS Metrics..... 97
- 3 Using IAM to Grant Access to AOM..... 107**
 - 3.1 Creating a User and Granting Permissions..... 107
 - 3.2 Creating a Custom Policy..... 108
- 4 AOM Overview..... 110**
- 5 Connecting to AOM..... 113**
 - 5.1 AOM Access Overview..... 113
 - 5.2 Managing Collector Base UniAgent..... 115
 - 5.2.1 Installing UniAgents..... 115
 - 5.2.2 (New) Installing UniAgents..... 122
 - 5.2.3 Managing UniAgents..... 131
 - 5.2.4 Managing ICAgent Plug-ins for Hosts..... 133

5.2.5 Managing UniAgents and ICAgents in CCE Clusters.....	134
5.2.6 Managing Host Groups.....	136
5.2.7 (New) Managing Host Groups.....	137
5.2.8 Configuring a Proxy Area and Proxy.....	144
5.2.9 Viewing Operation Logs.....	146
5.3 Connecting Cloud Services to AOM.....	147
5.4 Connecting Open-Source Monitoring Systems to AOM.....	150
5.5 Connecting Custom Plug-ins to AOM.....	151
5.6 Managing Log Ingestion.....	156
6 (New) Connecting to AOM.....	158
6.1 AOM Access Overview.....	158
6.2 Managing Collector Base UniAgent.....	159
6.2.1 Installing UniAgents.....	159
6.2.2 (New) Installing UniAgents.....	167
6.2.3 Managing UniAgents.....	176
6.2.4 Managing ICAgent Plug-ins for Hosts.....	178
6.2.5 Managing UniAgents and ICAgents in CCE Clusters.....	179
6.2.6 Managing Host Groups.....	181
6.2.7 (New) Managing Host Groups.....	182
6.2.8 Configuring a Proxy Area and Proxy.....	189
6.2.9 Viewing Operation Logs.....	191
6.3 Connecting Self-Built Middleware to AOM.....	192
6.3.1 Overview About Middleware Connection to AOM.....	192
6.3.2 Ingesting MySQL Metrics to AOM.....	194
6.3.3 Ingesting Redis Metrics to AOM.....	197
6.3.4 Ingesting Kafka Metrics to AOM.....	199
6.3.5 Ingesting Nginx Metrics to AOM.....	202
6.3.6 Ingesting MongoDB Metrics to AOM.....	206
6.3.7 Ingesting Consul Metrics to AOM.....	209
6.3.8 Ingesting HAProxy Metrics to AOM.....	212
6.3.9 Ingesting PostgreSQL Metrics to AOM.....	215
6.3.10 Ingesting Elasticsearch Metrics to AOM.....	218
6.3.11 Ingesting RabbitMQ Metrics to AOM.....	221
6.4 Connecting Running Environments to AOM.....	224
6.5 Ingesting Data to AOM Using Open-Source APIs and Protocols.....	228
6.6 Managing Metric and Log Ingestion.....	231
7 Observability Metric Browsing.....	234
8 Dashboard Monitoring.....	236
8.1 AOM Dashboard Overview.....	236
8.2 Creating a Dashboard.....	237
8.3 (New) Creating a Dashboard.....	245

8.4 Setting Full-Screen Online Duration for an AOM Dashboard.....	256
8.5 Adding AOM Dashboard Filters.....	257
8.6 (New) Setting Filters for AOM Dashboards.....	259
8.7 Graph Description.....	263
8.8 (New) Graphs.....	268
9 Alarm Monitoring.....	275
9.1 AOM Alarm Monitoring Overview.....	275
9.2 Configuring AOM Alarm Notification.....	275
9.2.1 Creating AOM Alarm Message Templates.....	275
9.2.2 Creating an AOM Alarm Notification Rule.....	281
9.3 Configuring AOM Alarm Rules.....	283
9.3.1 AOM Alarm Rule Overview.....	283
9.3.2 Creating an AOM Metric Alarm Rule.....	284
9.3.3 Creating an AOM Event Alarm Rule.....	294
9.3.4 Creating an AOM Log Alarm Rule.....	298
9.3.5 Creating AOM Alarm Rules in Batches.....	302
9.3.6 Managing AOM Alarm Rules.....	310
9.3.7 Alarm Tags and Annotations.....	314
9.3.8 Prometheus Statements.....	315
9.4 Checking AOM Alarms or Events.....	319
9.5 Configuring AOM Alarm Noise Reduction.....	322
9.5.1 AOM Alarm Noise Reduction Overview.....	322
9.5.2 Creating an AOM Alarm Grouping Rule.....	323
9.5.3 Creating an AOM Alarm Suppression Rule.....	327
9.5.4 Creating an AOM Alarm Silence Rule.....	330
10 (New) Log Management.....	334
11 (Old) Log Management.....	338
11.1 Configuring VM Log Collection Paths.....	338
11.2 Searching for Logs.....	339
11.3 Checking Log Files.....	341
11.4 Dumping Logs to OBS.....	342
12 Prometheus Monitoring.....	347
12.1 Prometheus Monitoring Overview.....	347
12.2 Managing Prometheus Instances.....	354
12.3 Managing Prometheus Instance Metrics.....	358
12.4 Using Prometheus Monitoring to Monitor CCE Cluster Metrics.....	360
12.5 Configuring Multi-Account Aggregation for Unified Monitoring.....	361
12.6 Configuring Metric Collection Rules for CCE Clusters.....	363
12.7 Configuring Recording Rules to Improve Metric Query Efficiency.....	366
12.8 Ingesting Middleware Metrics to AOM in VM Scenarios.....	367
12.8.1 Ingesting MySQL Metrics to AOM.....	367

12.8.2 Ingesting Redis Metrics to AOM.....	371
12.8.3 Ingesting Kafka Metrics to AOM.....	374
12.8.4 Ingesting Nginx Metrics to AOM.....	377
12.8.5 Ingesting MongoDB Metrics to AOM.....	381
12.8.6 Ingesting Consul Metrics to AOM.....	384
12.8.7 Ingesting HAProxy Metrics to AOM.....	388
12.8.8 Ingesting PostgreSQL Metrics to AOM.....	391
12.8.9 Ingesting Elasticsearch Metrics to AOM.....	394
12.8.10 Ingesting RabbitMQ Metrics to AOM.....	398
12.8.11 Ingesting Other Middleware Metrics to AOM.....	401
12.9 Configuring the Remote Read Address to Enable Self-built Prometheus to Read Data from AOM..	404
12.10 Configuring the Remote Write Address to Report Self-Built Prometheus Data to AOM.....	406
12.11 Checking Prometheus Instance Data Through Grafana.....	408
12.12 Checking the Number of Metric Samples Reported by Prometheus Instances.....	411
13 Infrastructure Monitoring.....	413
13.1 Using AOM to Monitor Workloads.....	413
13.2 Using AOM to Monitor Clusters.....	414
13.3 Using AOM to Monitor Hosts.....	417
13.4 Monitoring Processes Using AOM.....	419
13.4.1 Configuring AOM Application Discovery Rules.....	419
13.4.2 Using AOM to Monitor Application Processes.....	424
13.4.3 Using AOM to Monitor Component Processes.....	425
14 Global Settings.....	428
14.1 Authorizing AOM to Access Other Cloud Services.....	428
14.2 Managing Access Codes.....	428
14.3 Global Configuration of AOM.....	429
15 Querying AOM Traces.....	431
16 Migrating Data from AOM 1.0 to AOM 2.0.....	434
17 Accessing AOM 2.0.....	436
18 FAQs.....	437
18.1 Dashboard.....	437
18.1.1 Can I Import Grafana Views to AOM Dashboards?.....	437
18.2 Alarm Management.....	437
18.2.1 How Do I Distinguish Alarms from Events?.....	438
18.2.2 Why No Alarm Data Is Generated When the Statistical Period Is Set to 1 Minute?.....	438
18.3 Log Analysis.....	439
18.3.1 Does AOM Display Logs in Real Time?.....	439
18.3.2 How Do I Check Which Application Generates Logs in AOM?.....	439
18.4 Prometheus Monitoring.....	439
18.4.1 How Do I Connect Prometheus Data to AOM?.....	439

18.4.2 How Do I Distinguish Basic Metrics from Custom Metrics Collected by Prometheus Monitoring? 440

18.4.3 How Do I Obtain the Service Address of a Prometheus Instance?..... 440

18.4.4 Why Can't Metrics Prefixed with aom_prom_fixed Be Discarded?.....441

18.5 Infrastructure Monitoring.....442

18.5.1 Why Can't AOM Detect Workloads After the Pod YAML File Is Deployed Using Helm?..... 442

18.6 Collection Management..... 444

18.6.1 Are ICAgent and UniAgent the Same?..... 444

18.6.2 What Can I Do If an ICAgent Is Offline?..... 445

18.6.3 Why Is an Installed ICAgent Displayed as "Abnormal" on the UniAgents Page?.....446

18.6.4 Why Can't I View the ICAgent Status After It Is Installed?..... 446

18.6.5 Why Can't AOM Monitor CPU and Memory Usage After ICAgent Is Installed?..... 448

18.6.6 FAQs About UniAgent and ICAgent Installation.....449

18.6.7 Why Cannot the Installation Script Be Downloaded When I Try to Install UniAgent on a Cloud
Server?..... 449

18.7 Other FAQs..... 451

18.7.1 Comparison Between AOM 1.0 and AOM 2.0.....451

18.7.2 What Are the Differences Between AOM and APM?.....452

18.7.3 What Are the Differences Between the Log Functions of AOM and LTS?.....452

18.7.4 How Do I Create the apm_admin_trust Agency?..... 452

19 Change History..... 454

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 O&M 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 dumping through Kafka, and data viewing through Grafana.

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.
- **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.
- **Precise alarm reporting**
AOM has a unified alarm system, covering metric, event, and log alarms. It provides alarm noise reduction policies, such as grouping, suppression, and silence. It also supports alarm notification, 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 log data, 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 ingested 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.
	Prometheus monitoring	AOM is fully interconnected with the open-source Prometheus ecosystem, monitors various components, and flexibly expands cloud native component metric plug-ins.	Not supported.	Supported.

Function		Description	AOM 1.0	AOM 2.0
	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.

As AOM 1.0 functions are gradually replaced by 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 [Migrating Data from AOM 1.0 to AOM 2.0](#).

1.5 Relationships Between AOM and Other Services

AOM can work with Distributed Message Service (DMS), and Cloud Trace Service (CTS). 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.

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.

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 incorporates APM functions for unified O&M. APM also has its own independent console and can be used separately.

VPC

VPC is a logically isolated virtual network. It is created for ECSs, 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 failure, 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. 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 with 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	Item	Description
Dashboards	Dashboards	A maximum of 1,000 dashboards can be created in a region.
	Graphs in a dashboard	A maximum of 50 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.
Metrics	Metric storage duration	<ul style="list-style-type: none">Metric data can be stored for up to 30 days.ICAgent collects data at an interval of one minute. This interval cannot be changed.
	Storage duration of associated metric items	After resources (such as clusters, components, and hosts) are deleted, their metric items can still be stored for up to 30 days.
	Metric dimensions	A maximum of 20 dimensions can be configured for a metric.
	Metrics queried using the 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.

Category	Item	Description
	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.
	Application metric	<ul style="list-style-type: none"> When the number of containers on a host exceeds 1,000, 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 1,000, the ICAgent resumes the collection of application metrics and the ICAgent Stopped Collecting Application Metrics alarm is cleared.
	Job metric	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.
	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 1,000 containers run on a single node.
	Metric dimension format	<p>Metric dimension tags must comply with the AOM or Prometheus standard format so that the metrics can be reported to AOM.</p> <ul style="list-style-type: none"> AOM standard format: Only letters, digits, and underscores (_) are allowed. Start with a letter or underscore. Prometheus standard format: Only ASCII letters, digits, and underscores (_) are allowed. The following regular expression must be met: <code>[a-zA-Z_][a-zA-Z0-9_]*</code>.
Alarm rules	Alarm rules	A maximum of 3,000 alarm rules (including metric alarm rules and event alarm rules) can be created.

Category	Item	Description
	Alarm templates	A maximum of 150 alarm templates can be created.
Alarm list	Time range for alarm query	You can query alarms generated within 31 days in the last year.
	Time range for event query	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
 - For Linux x86_64 hosts, all the OSs and versions listed in [Table 1-3](#) are supported.
 - For Linux Arm hosts, CentOS 7.4/7.5/7.6, EulerOS 2.0, and Ubuntu 18.04 are supported.

Table 1-3 Linux OSs and versions supported by UniAgent

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	

Table 1-4 Windows OSs and versions supported by UniAgent

OS	Version
Windows Server	Windows Server 2012 R2 Standard 64-bit
	Windows Server 2012 R2 Standard English 64-bit
	Windows Server 2012 R2 Datacenter 64-bit

OS	Version
	Windows Server 2012 R2 Datacenter English 64-bit
	Windows Server 2016 Standard 64-bit
	Windows Server 2016 Standard English 64-bit
	Windows Server 2016 Datacenter 64-bit
	Windows Server 2016 Datacenter English 64-bit
	Windows Server 2019 Standard 64-bit
	Windows Server 2019 Standard English 64-bit
	Windows Server 2019 Datacenter 64-bit
	Windows Server 2019 Datacenter English 64-bit

- Resource Restrictions

Table 1-5 Resource restrictions

Item	Description
UniAgent client	When the average CPU usage is greater than 50% or the memory is greater than 100 MB for two minutes, the UniAgent client automatically restarts.
Installing, upgrading, or uninstalling UniAgents	You can install, upgrade, or uninstall UniAgents for a maximum of 100 hosts at a time.
Deleting hosts	You can delete a maximum of 50 hosts where UniAgents are not installed, offline, or fail to be installed 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.

NOTE

This section describes only the metrics defined by the collection plug-in. Metrics reported by other cloud services or APIs are not included.

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 1-6](#).

Table 1-6 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 [1.7.5 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 categories, names, and meanings of VM metrics reported by ICAgents to AOM.

- 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**, thin pool metrics can be viewed. Otherwise, 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.

Table 1-7 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
	aom_node_network_receive_error_packets	Downlink Error Rate	Number of error packets received by a NIC per second	≥ 0	Packets/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	Packets/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

Cate gory	Metric	Metric Name	Description	Value Range	Unit
Disk parti tion metr ics	aom_host_diskpartition_thinpool_metadata_percent	Thin Pool 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 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 Disk Partition Space	Total thin pool disk partition space on a CCE node	≥ 0	MB
File syste m metr ics	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 metr ics	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	%

Cate gory	Metric	Metric Name	Description	Value Range	Unit
	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	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	%
	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	NPU Memory	NPU memory of a measured object Only NPU metrics of CCE hosts can be collected.	> 0	MB
	aom_node_npu_memory_usage	NPU Memory Usage	Percentage of the used NPU memory to the total NPU memory Only NPU metrics of CCE hosts can be collected.	0–100	%
	aom_node_npu_memory_used_megabytes	Used NPU Memory	NPU memory used by a measured object Only NPU metrics of CCE hosts can be collected.	≥ 0	MB

Cate gory	Metric	Metric Name	Description	Value Range	Unit
	aom_node_npu_usage	NPU Usage	NPU usage of a measured object Only NPU metrics of CCE hosts can be collected.	0–100	%
	aom_node_npu_temperature_c entigrade	NPU Temperat ure	NPU temperature of a measured object Only NPU metrics of CCE hosts can be collected.	-	°C
	aom_node_me mory_usage	Physical Memory Usage	Percentage of the used physical memory to the total physical memory applied for a measured object	0–100	%
	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: Conn ecte d 1: Not conn ecte d 	N/A

Cate gory	Metric	Metric Name	Description	Value Range	Unit
	aom_node_ntp_status	NTP Synchroni zation 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: Synchron ous 1: Asyn chro nous 	N/A
	aom_node_proc ess_number	Processes	Number of processes on a measured object	≥ 0	Count
	aom_node_gpu _temperature_c entigrade	GPU Temperat ure	GPU temperature of a measured object	-	°C
	aom_node_me memory_total_me gabytes	Total Physical Memory	Total physical memory that has been applied for a measured object	≥ 0	MB
	aom_node_virtu al_memory_tot al_megabytes	Total Virtual Memory	Total virtual memory that has been applied for a measured object	≥ 0	MB
	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	Count
	aom_node_sys_ max_threads_n um	Max. Threads	Maximum number of threads that can be created on a host	≥ 0	Count
	aom_node_phy _disk_total_cap acity_megabyte s	Total Physical Disk Space	Total disk space of a host	≥ 0	MB

Cate gory	Metric	Metric Name	Description	Value Range	Unit
	aom_node_physical_disk_total_used_megabytes	Used Physical Disk Space	Used disk space of a host	≥ 0	MB
	aom_billing_hostUsed	Hosts	Number of hosts connected per day	≥ 0	Count
Cluster metrics	aom_cluster_cpu_limit_core	Total CPU Cores	Total number of CPU cores that have been applied for a measured object	≥ 1	Cores
	aom_cluster_cpu_used_core	Used CPU Cores	Number of CPU cores used by a measured object	≥ 0	Cores
	aom_cluster_cpu_usage	CPU Usage	CPU usage of a measured object	0–100	%
	aom_cluster_disk_available_capacity_megabytes	Available Disk Space	Disk space that has not been used	≥ 0	MB
	aom_cluster_disk_capacity_megabytes	Total Disk Space	Total disk space	≥ 0	MB
	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	%

Cate gory	Metric	Metric Name	Description	Value Range	Unit
	aom_cluster_gp u_memory_use d_megabytes	Used GPU Memory	GPU memory used by a measured object	≥ 0	MB
	aom_cluster_gp u_usage	GPU Usage	GPU usage of a measured object	0-100	%
	aom_cluster_m emory_usage	Physical Memory Usage	Percentage of the used physical memory to the total physical memory applied for a measured object	0-100	%
	aom_cluster_ne twork_receive_b ytes	Downlink Rate (BPS)	Inbound traffic rate of a measured object	≥ 0	Bytes/s
	aom_cluster_ne twork_transmit _bytes	Uplink Rate (BPS)	Outbound traffic rate of a measured object	≥ 0	Bytes/s
	aom_cluster_m emory_total_m egabytes	Total Physical Memory	Total physical memory that has been applied for a measured object	≥ 0	MB
	aom_cluster_vir tual_memory_t otal_megabytes	Total Virtual Memory	Total virtual memory of a measured object	≥ 0	MB
	aom_cluster_vir tual_memory_u sage	Virtual Memory Usage	Percentage of the used virtual memory to the total virtual memory	0-100	%
Cont ainer metr ics	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

Category	Metric	Metric Name	Description	Value Range	Unit
	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
	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

Cate gory	Metric	Metric Name	Description	Value Range	Unit
	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	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	NPU Memory	NPU memory of a measured object	> 0	MB
	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	%

Cate gory	Metric	Metric Name	Description	Value Range	Unit
	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	Physical memory (resident set size) used by 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	Packets/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
	aom_container_network_transmit_error_packets	Uplink Error Rate	Number of error packets sent by a NIC per second	≥ 0	Packets/s
	aom_container_network_transmit_packets	Uplink Rate (PPS)	Number of data packets sent by a NIC per second	≥ 0	Packets/s

Cate gory	Metric	Metric Name	Description	Value Range	Unit
	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
Proc ess metr ics	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	Count
	aom_process_max_handle_count	Max. Handles	Maximum number of handles used by a measured object	≥ 0	Count
	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	%

Cate gory	Metric	Metric Name	Description	Value Range	Unit
	aom_process_m emory_used_m egabytes	Used Physical Memory	Physical memory (resident set size) used by a measured object	≥ 0	MB
	aom_process_th read_count	Threads	Number of threads used by a measured object	≥ 0	Count
	aom_process_vi rtual_memory_t otal_megabytes	Total Virtual Memory	Total virtual memory that has been applied for a measured object	≥ 0	MB

1.7.3 Basic Metrics: Container Metrics

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

Table 1-8 Metrics of containers running in CCE or on-premises Kubernetes clusters

Target Name	Job Name	Metric	Description
<ul style="list-style-type: none">• serviceMon itor/ monitoring /coredns/0• serviceMon itor/ 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 CoreDNS cache
		coredns_cache_size	CoreDNS cache size
		coredns_cache_hits_to tal	Number of CoreDNS cache hits
		coredns_cache_misses _total	Number of CoreDNS cache misses
		coredns_cache_reques ts_total	Total number of CoreDNS resolution requests in different dimensions
		coredns_dns_request_ duration_seconds_buc ket	CoreDNS request latency

Target Name	Job Name	Metric	Description
		coredns_dns_request_duration_seconds_count	CoreDNS request processing time (seconds)
		coredns_dns_request_duration_seconds_sum	Total CoreDNS request processing time (seconds)
		coredns_dns_request_size_bytes_bucket	Size of the CoreDNS request in bytes
		coredns_dns_request_size_bytes_count	CoreDNS request byte count
		coredns_dns_request_size_bytes_sum	Total CoreDNS request bytes
		coredns_dns_requests_total	Total number of CoreDNS requests
		coredns_dns_response_size_bytes_bucket	Size of the returned CoreDNS response in bytes
		coredns_dns_response_size_bytes_count	CoreDNS response byte count
		coredns_dns_response_size_bytes_sum	Total CoreDNS response bytes
		coredns_dns_responses_total	Total number of CoreDNS response codes
		coredns_forward_conn_cache_hits_total	Total number of cache hits for each protocol and data flow
		coredns_forward_conn_cache_misses_total	Total number of cache misses for each protocol and data flow
		coredns_forward_healthcheck_broken_total	Total forwarding health check failures
		coredns_forward_healthcheck_failures_total	Total forwarding health check faults
		coredns_forward_max_concurrent_rejects_total	Total number of requests rejected due to excessive concurrent requests

Target Name	Job Name	Metric	Description
		coredns_forward_request_duration_seconds_bucket	CoreDNS forwarding request latency
		coredns_forward_request_duration_seconds_count	CoreDNS forwarding request duration in seconds
		coredns_forward_request_duration_seconds_sum	Total CoreDNS forwarding request duration in seconds
		coredns_forward_requests_total	Total number of requests for each data flow
		coredns_forward_responses_total	Total number of responses to each data flow
		coredns_health_request_duration_seconds_bucket	CoreDNS health check request latency
		coredns_health_request_duration_seconds_count	CoreDNS health check request duration in seconds
		coredns_health_request_duration_seconds_sum	Total CoreDNS health check request duration in seconds
		coredns_health_request_failures_total	Total number of failed CoreDNS health check requests
		coredns_hosts_reload_timestamp_seconds	Timestamp of CoreDNS's last reload of the host file
		coredns_kubernetes_dns_programming_duration_seconds_bucket	DNS programming latency
		coredns_kubernetes_dns_programming_duration_seconds_count	DNS programming duration in seconds
		coredns_kubernetes_dns_programming_duration_seconds_sum	Total DNS programming duration in seconds

Target Name	Job Name	Metric	Description
		coredns_local_localhost_requests_total	Total number of localhost requests processed by CoreDNS
		coredns_nodecache_setup_errors_total	Total number of node cache plug-in setting errors
		coredns_dns_response_rcode_count_total	Cumulative count of response codes
		coredns_dns_request_count_total	Cumulative count of DNS requests made per zone, protocol, and family
		coredns_dns_request_do_count_total	Cumulative count of requests with the DO bit set
		coredns_dns_do_requests_total	Number of requests with the DO bit set
		coredns_dns_request_type_count_total	Cumulative count of DNS requests per type
		coredns_panic_total	Total number of CoreDNS abnormal exits
		coredns_plugin_enabled	Whether a plugin is enabled in CoreDNS
		coredns_reload_failed_total	Total number of configuration files that fail to be reloaded
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

Target Name	Job Name	Metric	Description
		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
		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	Counter of API server requests broken out for code and other items
		go_goroutines	Number of goroutines that exist
		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
		rest_client_requests_total	Total number of HTTP requests, partitioned by status code and method
		workqueue_adds_total	Total number of additions handled by a work queue
		workqueue_depth	Current depth of a work queue
		workqueue_queue_duration_seconds_bucket	Duration that a task stays in the current queue

Target Name	Job Name	Metric	Description
		aggregator_unavailable_apiservice_total	Number of unavailable APIServices
		rest_client_request_duration_seconds_bucket	Number of HTTP requests, partitioned by status code and method
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 for destruction and update operations
		kubelet_cgroup_manager_duration_seconds_count	Number of destruction and update operations
		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 for relisting pods in PLEG
		kubelet_pleg_relist_duration_seconds_count	Duration in seconds for relisting pods in PLEG
		kubelet_pleg_relist_interval_seconds_bucket	Interval between relisting operations in PLEG
		kubelet_pod_start_duration_seconds_count	Number of pods that have been started

Target Name	Job Name	Metric	Description
		kubelet_pod_start_duration_seconds_bucket	Duration from the kubelet seeing a pod for the first time to the pod starting to run
		kubelet_pod_worker_duration_seconds_bucket	Duration for synchronizing a single pod.
		kubelet_running_containers	Number of running containers
		kubelet_running_pods	Number of running pods
		kubelet_runtime_operations_duration_seconds_bucket	Time of every operation
		kubelet_runtime_operations_errors_total	Number of errors in operations at runtime level
		kubelet_runtime_operations_total	Number of runtime operations of each type
		kubelet_volume_stats_available_bytes	Number of available bytes in a volume
		kubelet_volume_stats_capacity_bytes	Capacity in bytes of a volume
		kubelet_volume_stats_inodes	Maximum 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 for each storage operation
		storage_operation_duration_seconds_count	Number of storage operations
		storage_operation_errors_total	Number of storage operation errors
		volume_manager_total_volumes	Number of volumes in Volume Manager

Target Name	Job Name	Metric	Description
		rest_client_requests_total	Total number of HTTP requests, partitioned by status code and method
		rest_client_request_duration_seconds_bucket	Number of HTTP requests, partitioned by status code and method
		process_resident_memory_bytes	Size of the resident memory set
		process_cpu_seconds_total	Total process CPU time
		go_goroutines	Number of goroutines that exist
serviceMonitor/monitoring/kubelet/1	kubelet	container_cpu_cfs_periods_total	Total number of elapsed enforcement periods
		container_cpu_cfs_throttled_periods_total	Number of throttled periods
		container_cpu_cfs_throttled_seconds_total	Total duration a 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	Total CPU time consumed
		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	Total number of inodes in a file system
		container_fs_io_time_seconds_total	Cumulative time spent on doing I/Os by the disk or file system

Target Name	Job Name	Metric	Description
		container_fs_limit_bytes	Total disk or file system capacity that can be consumed by a container
		container_fs_read_seconds_total	Total time a 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
		container_fs_write_seconds_total	Total time a 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 memory usage

Target Name	Job Name	Metric	Description
		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 a 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 a 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 a container
		container_spec_memory_limit_bytes	Memory limit for a container
		machine_cpu_cores	Number of CPU cores of the physical machine or VM
		machine_memory_bytes	Total memory size of the physical machine or VM
serviceMonitor/monitoring/kube-state-metrics/0	kube-state-metrics-prom	kube_cronjob_status_active	Whether the cronjob is actively running jobs

Target Name	Job Name	Metric	Description
		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
		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

Target Name	Job Name	Metric	Description
		kube_deployment_metadata_generation	Sequence number representing a specific generation of the desired state for a Deployment
		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
		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	Job information
		kube_namespace_labels	Namespace labels
		kube_node_labels	Node labels
		kube_node_info	Node information
		kube_node_spec_taint	Taint of a node
		kube_node_spec_unschedulable	Whether new pods can be scheduled to a node

Target Name	Job Name	Metric	Description
		kube_node_status_allocatable	Allocatable resources on a node
		kube_node_status_capacity	Capacity for different resources on a node
		kube_node_status_condition	Node status condition
		kube_node_volcano_oversubscription_status	Node oversubscription status
		kube_persistentvolume_status_phase	PV status
		kube_persistentvolumeclaim_status_phase	PVC status
		kube_persistentvolume_info	PV information
		kube_persistentvolumeclaim_info	PVC information
		kube_pod_container_info	Information about a container running in the pod
		kube_pod_container_resource_limits	Container resource limits
		kube_pod_container_resource_requests	Number of resources requested by a container
		kube_pod_container_status_last_terminated_reason	The last reason a container was in terminated state
		kube_pod_container_status_ready	Whether a container is in ready state
		kube_pod_container_status_restarts_total	Number of container restarts
		kube_pod_container_status_running	Whether a container is in running state
		kube_pod_container_status_terminated	Whether a container is in terminated state
		kube_pod_container_status_terminated_reason	The reason a container is in terminated state

Target Name	Job Name	Metric	Description
		kube_pod_container_status_waiting	Whether a container is in waiting state
		kube_pod_container_status_waiting_reason	The reason a container is in waiting state
		kube_pod_info	Pod information
		kube_pod_labels	Pod labels
		kube_pod_owner	Object to which the pod belongs
		kube_pod_status_phase	Phase of the pod
		kube_pod_status_ready	Whether the pod is in ready state
		kube_secret_info	Secret information
		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	Generation observed by the StatefulSet controller
		kube_statefulset_status_replicas	Number of stateful replicas in a StatefulSet
		kube_statefulset_status_replicas_ready	Number of ready replicas in a StatefulSet
		kube_statefulset_status_replicas_updated	Number of updated replicas in a StatefulSet

Target Name	Job Name	Metric	Description
		kube_job_spec_comple tions	Desired number of successfully finished pods that should run with the job
		kube_job_status_failed	Failed jobs
		kube_job_status_succe eded	Successful jobs
		kube_node_status_allo catable_cpu_cores	Number of allocatable CPU cores of a node
		kube_node_status_allo catable_memory_byte s	Total allocatable memory of a node
		kube_replicaset_owner	ReplicaSet owner.
		kube_resourcequota	Resource quota
		kube_pod_spec_volum es_persistentvolume- claims_info	Information about the PVC associated with the pod
serviceMonitor/monitoring/ prometheus- lightweight/0	prometheus- lightweight	vm_persistentqueue_b locks_dropped_total	Total number of dropped blocks in a send queue
		vm_persistentqueue_b locks_read_total	Total number of blocks read by a send queue
		vm_persistentqueue_b locks_written_total	Total number of blocks written to a send queue
		vm_persistentqueue_b ytes_pending	Number of pending bytes in a send queue
		vm_persistentqueue_b ytes_read_total	Total number of bytes read by a send queue
		vm_persistentqueue_b ytes_written_total	Total number of bytes written to a send queue
		vm_promscrape_active _scrapers	Number of collected shards
		vm_promscrape_conn_ read_errors_total	Total number of read errors during scrapes
		vm_promscrape_conn_ write_errors_total	Total number of write errors during scrapes

Target Name	Job Name	Metric	Description
		vm_promscrape_max_scrape_size_exceeded_errors_total	Total number of scrapes failed because responses exceed the size limit
		vm_promscrape_scrape_duration_seconds_sum	Time required for the scrape
		vm_promscrape_scrape_duration_seconds_count	Total time required for the scrape
		vm_promscrape_scrapes_total	Number of scrapes
		vmagent_remotewrite_bytes_sent_total	Total number of bytes sent through remote write
		vmagent_remotewrite_duration_seconds_sum	Time consumed by remote writes
		vmagent_remotewrite_duration_seconds_count	Total time consumed by remote writes
		vmagent_remotewrite_packets_dropped_total	Total number of dropped packets during remote write
		vmagent_remotewrite_pending_data_bytes	Number of pending bytes during remote write
		vmagent_remotewrite_requests_total	Total number of remote write requests
		vmagent_remotewrite_retries_count_total	Total number of remote write retries
		go_goroutines	Number of goroutines that exist
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 the CPUs spent in each mode

Target Name	Job Name	Metric	Description
		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 time 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
		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	Error in the mounted file system device
		node_filesystem_free_bytes	Remaining space of a file system
		node_filesystem_readonly	Read-only file system

Target Name	Job Name	Metric	Description
		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
		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	Total number of packets dropped during reception
		node_network_receive_errs_total	Total number of errors encountered during reception
		node_network_receive_packets_total	Total number of packets received
		node_network_transmit_bytes_total	Total number of sent bytes
		node_network_transmit_drop_total	Total number of dropped packets
		node_network_transmit_errs_total	Total number of errors encountered during transmission

Target Name	Job Name	Metric	Description
		node_network_transmit_packets_total	Total number of packets sent
		node_procs_blocked	Blocked processes
		node_procs_running	Running processes
		node_sockstat_sockets_used	Number of sockets in use
		node_sockstat_TCP_all	Number of allocated TCP sockets
		node_sockstat_TCP_in	Number of TCP sockets in use
		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_in	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	System kernel information
		node_vmstat_oom_kill	Number of processes terminated due to insufficient memory
		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

Target Name	Job Name	Metric	Description
		process_resident_memory_bytes	Size of the resident memory set
		process_start_time_seconds	Process start time
		process_virtual_memory_bytes	Virtual memory size
		process_virtual_memory_max_bytes	Maximum available virtual memory capacity
		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 page faults in vmstat
		node_vmstat_pgpgout	Number of page out in vmstat
		node_vmstat_pgfault	Number of page faults in vmstat
		node_vmstat_pgpgin	Number of page in in vmstat
		node_processes_max_processes	Maximum number of processes
		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

Target Name	Job Name	Metric	Description
		promhttp_metric_handler_requests_in_flight	Number of metrics being processed
		go_goroutines	Number of goroutines that exist
		node_filesystem_files	Number of files in the file system on the node
		node_filesystem_files_free	Number of available files in the file system on the node
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

Target Name	Job Name	Metric	Description
		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
		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 isolated GPU memory pages with single-bit errors
		cce_gpu_retired_pages_dbe	Number of isolated GPU memory pages with dual-bit errors
		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

Target Name	Job Name	Metric	Description
		gpu_schedule_policy	There are three GPU modes. 0 : GPU memory isolation, compute sharing mode. 1 : GPU memory and compute isolation mode. 2 : default mode, indicating that the GPU is not virtualized.
		xgpu_device_health	Health status of xGPU. 0 : xGPU is healthy. 1 : xGPU is unhealthy.
serviceMonitor/monitoring/prometheus-server/0	prometheus-server	prometheus_build_info	Prometheus build information
		prometheus_engine_query_duration_seconds	Time for query, in seconds
		prometheus_engine_query_duration_seconds_count	Number of queries
		prometheus_sd_discovered_targets	Number of metrics collected by different targets
		prometheus_remote_storage_bytes_total	Total number of bytes of data (non-metadata) sent by the queue after compression
		prometheus_remote_storage_enqueue_retries_total	Number of retries upon enqueueing failed due to full shard queue
		prometheus_remote_storage_highest_timestamp_in_seconds	Latest timestamp in the remote storage
		prometheus_remote_storage_queue_highest_sent_timestamp_seconds	Highest timestamp successfully sent by remote storage

Target Name	Job Name	Metric	Description
		prometheus_remote_storage_samples_dropped_total	Number of samples dropped before being 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 sent to remote storage
		prometheus_remote_storage_samples_pending	Number of samples pending in shards to be sent to remote storage
		prometheus_remote_storage_samples_retried_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 queue's 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

Target Name	Job Name	Metric	Description
		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 time series stored in the head
		prometheus_tsdb_head_samples_appended_total	Number of appended samples
		prometheus_wal_watcher_current_segment	Current segment the WAL watcher is reading records from
		prometheus_target_interval_length_seconds	Metric collection interval
		prometheus_target_interval_length_seconds_count	Number of metric collection intervals
		prometheus_target_interval_length_seconds_sum	Sum of metric collection intervals
		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 of 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	Target synchronization interval

Target Name	Job Name	Metric	Description
		prometheus_target_sync_length_seconds_count	Number of target synchronization intervals
		prometheus_target_sync_length_seconds_sum	Sum of target synchronization intervals
		promhttp_metric_handler_requests_in_flight	Current number of scrapes being served
		promhttp_metric_handler_requests_total	Total scrapes
		go_goroutines	Number of goroutines that exist
podMonitor/ monitoring/ virtual-kubelet-pods/0	monitoring/ virtual-kubelet-pods	container_cpu_load_average_10s	Value of container CPU load average over the last 10 seconds
		container_cpu_system_seconds_total	Cumulative CPU time of a container system
		container_cpu_usage_seconds_total	Cumulative CPU time consumed by a container in core-seconds
		container_cpu_user_seconds_total	Cumulative CPU time of a user
		container_cpu_cfs_periods_total	Number of elapsed enforcement period intervals
		container_cpu_cfs_throttled_periods_total	Number of throttled period intervals
		container_cpu_cfs_throttled_seconds_total	Total duration a container has been throttled
		container_fs_inodes_free	Number of available inodes in a file system
		container_fs_usage_bytes	File system usage
		container_fs_inodes_total	Number of inodes in a file system

Target Name	Job Name	Metric	Description
		container_fs_io_current	Number of I/Os currently in progress in a disk or file system
		container_fs_io_time_seconds_total	Cumulative time spent on doing I/Os by the disk or file system
		container_fs_io_time_weighted_seconds_total	Cumulative weighted I/O time of a disk or file system
		container_fs_limit_bytes	Total disk or file system capacity that can be consumed by a container
		container_fs_reads_bytes_total	Cumulative amount of disk or file system data read by a container
		container_fs_read_seconds_total	Time a 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 a 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

Target Name	Job Name	Metric	Description
		container_fs_write_seconds_total	Time a 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
		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 a 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 a container network

Target Name	Job Name	Metric	Description
		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 a 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_processes	Number of processes running inside a container
		container_sockets	Number of open sockets for a container
		container_file_descriptors	Number of open file descriptors for a container
		container_threads	Number of threads running inside a container
		container_threads_max	Maximum number of threads allowed inside a container
		container_ulimits_soft	Soft ulimit value of process 1 in a container Unlimited if the value is -1, except priority and nice.

Target Name	Job Name	Metric	Description
		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 a container
		container_spec_cpu_shares	CPU share of a container
		container_spec_cpu_quota	CPU quota of a container
		container_spec_memory_limit_bytes	Memory limit for a container
		container_spec_memory_reservation_limit_bytes	Memory reservation limit for a container
		container_spec_memory_swap_limit_bytes	Memory swap limit for a container
		container_start_time_seconds	Running time of a 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 a 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	Invoking of different functions
		everest_function_duration_seconds_bucket	Number of times that different functions are executed at different time

Target Name	Job Name	Metric	Description
		everest_function_duration_seconds_count	Number of invoking times of different functions
		everest_function_duration_seconds_sum	Total invoking time of different functions
		everest_function_duration_quantile_seconds	Time quantile required for invoking different functions
		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
		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 duration of I/O operations
		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

Target Name	Job Name	Metric	Description
		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	Total read queue waiting time
		node_volume_read_rtt_time_milliseconds_total	Total read RTT
		node_volume_write_transmissions_total	Total number of write transmissions
		node_volume_write_timeouts_total	Total number of write timeouts
		node_volume_write_queue_time_milliseconds_total	Total write queue waiting time
		node_volume_write_rtt_time_milliseconds_total	Total write RTT
		node_volume_localvolume_stats_capacity_bytes	Total local volume capacity
		node_volume_localvolume_stats_available_bytes	Available local volume capacity
		node_volume_localvolume_stats_used_bytes	Used local volume capacity
		node_volume_localvolume_stats_inodes	Number of inodes for a local volume
		node_volume_localvolume_stats_inodes_used	Used inodes for a local volume

Target Name	Job Name	Metric	Description
podMonitor/ monitoring/ nginx-ingress- controller/0	monitoring/ nginx-ingress- controller	nginx_ingress_controll er_connect_duration_s econds_bucket	Duration for connecting to the upstream server
		nginx_ingress_controll er_connect_duration_s econds_sum	Duration for connecting to the upstream server
		nginx_ingress_controll er_connect_duration_s econds_count	Duration for connecting to the upstream server
		nginx_ingress_controll er_request_duration_s econds_bucket	Time required for processing a request, in milliseconds
		nginx_ingress_controll er_request_duration_s econds_sum	Time required for processing a request, in milliseconds
		nginx_ingress_controll er_request_duration_s econds_count	Time required for processing a request, in milliseconds
		nginx_ingress_controll er_request_size_bucke t	Length of a request (including the request line, header, and body)
		nginx_ingress_controll er_request_size_sum	Length of a request (including the request line, header, and body)
		nginx_ingress_controll er_request_size_count	Length of a request (including the request line, header, and body)
		nginx_ingress_controll er_response_duration_ seconds_bucket	Time required for receiving the response from the upstream server
		nginx_ingress_controll er_response_duration_ seconds_sum	Time required for receiving the response from the upstream server
		nginx_ingress_controll er_response_duration_ seconds_count	Time required for receiving the response from the upstream server

Target Name	Job Name	Metric	Description
		nginx_ingress_controller_response_size_bucket	Length of a response (including the request line, header, and request body)
		nginx_ingress_controller_response_size_sum	Length of a response (including the request line, header, and request body)
		nginx_ingress_controller_response_size_count	Length of a response (including the request line, header, and request body)
		nginx_ingress_controller_header_duration_seconds_bucket	Time required for receiving the first header from the upstream server
		nginx_ingress_controller_header_duration_seconds_sum	Time required for receiving the first header from the upstream server
		nginx_ingress_controller_header_duration_seconds_count	Time required for receiving the first header from the upstream server
		nginx_ingress_controller_bytes_sent	Number of bytes sent to the client
		nginx_ingress_controller_ingress_upstream_latency_seconds	Upstream service latency
		nginx_ingress_controller_requests	Total number of client requests
		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)

Target Name	Job Name	Metric	Description
		nginx_ingress_controller_process_num_procs	Number of processes
		nginx_ingress_controller_process_oldest_start_time_seconds	Start time in seconds since January 1, 1970
		nginx_ingress_controller_process_read_bytes_total	Total number of bytes read
		nginx_ingress_controller_process_requests_total	Total number of requests processed by Nginx since startup
		nginx_ingress_controller_process_resident_memory_bytes	Resident memory set usage of a process, that is, the actual physical memory usage
		nginx_ingress_controller_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_process_writes_bytes_total	Total amount of data written by the process to disks or other devices for long-term storage
		nginx_ingress_controller_build_info	A metric with a constant '1' labeled with information about the build
		nginx_ingress_controller_check_success	Cumulative count of syntax check operations of the Nginx ingress controller
		nginx_ingress_controller_config_hash	Configured hash value

Target Name	Job Name	Metric	Description
		nginx_ingress_controller_config_last_reload_successful	Whether the last configuration reload attempt was successful
		nginx_ingress_controller_config_last_reload_successful_timestamp_seconds	Timestamp of the last successful configuration reload seconds
		nginx_ingress_controller_ssl_certificate_info	All information associated with a certificate
		nginx_ingress_controller_success	Cumulative number of reload operations of the Nginx ingress controller
		nginx_ingress_controller_orphan_ingress	Status of an orphaned ingress (1 indicates an orphaned ingress). 0: Not isolated. namespace: namespace of the ingress ingress: name of the ingress type: status of the ingress. The value can be no-service or 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

Target Name	Job Name	Metric	Description
		nginx_ingress_controller_admission_tested_ingresses	Length of ingresses processed by the admission controller
podMonitor/ monitoring/ cceaddon-npd/0	monitoring/ cceaddon-npd	problem_counter	Number of times that the check item is found abnormal
		problem_gauge	Whether the check item has triggered an exception <ul style="list-style-type: none">• 0: not triggered• 1: triggered

1.7.4 Basic Metrics: ModelArts Metrics

This section describes the ModelArts metrics reported to AOM through the Agent.

Table 1-9 Metrics reported by ModelArts to AOM through the Agent

Category	Metric	Metric Name	Description	Value Range	Unit
CPU	ma_container_cpu_util	CPU Usage	CPU usage of a measured object	0-100	%
	ma_container_cpu_used_core	Used CPU Cores	Number of CPU cores used by a measured object	≥ 0	Cores
	ma_container_cpu_limit_core	Total CPU Cores	Total number of CPU cores that have been applied for a measured object	≥ 1	Cores
Memory	ma_container_memory_capacity_megabytes	Memory	Total physical memory that has been applied for a measured object	≥ 0	MB
	ma_container_memory_util	Physical Memory Usage	Percentage of the used physical memory to the total physical memory applied for a measured object	0-100	%

Category	Metric	Metric Name	Description	Value Range	Unit
	ma_container_memory_used_megabytes	Used Physical Memory	Physical memory that has been used by a measured object (container_memory_working_set_bytes in the current working set). (Memory usage in a working set = Active anonymous and cache, and file-backed page ≤ container_memory_usage_bytes)	≥ 0	MB
Storage I/O	ma_container_disk_read_kilo bytes	Disk Read Rate	Volume of data read from a disk per second	≥ 0	KB/s
	ma_container_disk_write_kilo bytes	Disk Write Rate	Volume of data written into a disk per second	≥ 0	KB/s
GPU memory	ma_container_gpu_mem_total_megabytes	GPU Memory Capacity	Total GPU memory of a training job	> 0	MB
	ma_container_gpu_mem_util	GPU Memory Usage	Percentage of the used GPU memory to the total GPU memory	0-100	%
	ma_container_gpu_mem_used_megabytes	Used GPU Memory	GPU memory used by a measured object	≥ 0	MB
GPU	ma_container_gpu_util	GPU Usage	GPU usage of a measured object	0-100	%

Category	Metric	Metric Name	Description	Value Range	Unit
	ma_container_gpu_mem_copy_util	GPU Memory Bandwidth Usage	GPU memory bandwidth usage of a measured object. For example, the maximum memory bandwidth of NVIDIA GPU V100 is 900 GB/s. If the current memory bandwidth is 450 GB/s, the memory bandwidth usage is 50%.	0-100	%
	ma_container_gpu_enc_util	GPU Encoder Usage	GPU encoder usage of a measured object	0-100	%
	ma_container_gpu_dec_util	GPU Decoder Usage	GPU decoder usage of a measured object	0-100	%
	DCGM_FI_DEV_GPU_TEMP	GPU Temperature	GPU temperature	> 0	°C
	DCGM_FI_DEV_POWER_USAGE	GPU Power	GPU power	> 0	W
	DCGM_FI_DEV_MEMORY_TEMP	Memory Temperature	Memory temperature	> 0	°C

Category	Metric	Metric Name	Description	Value Range	Unit
	DCGM_FI_PROF_GR_ENGINE_ACTIVE	Graphics Engine Activity	Percentage of the time when the graphic or compute engine is in the active state within a period. This is an average value of all graphic or compute engines. An active graphic or compute engine indicates that the graphic or compute context is associated with a thread and the graphic or compute context is busy.	0–1.0	Percentage (fraction)
	DCGM_FI_PROF_SM_OCCUPANCY	SM Occupancy	<p>Ratio of the number of thread bundles that reside on the SM to the maximum number of thread bundles that can reside on the SM within a period.</p> <p>This is an average value of all SMs within a period.</p> <p>A high value does not mean a high GPU usage. Only when the GPU memory bandwidth is limited, a high value of workloads (DCGM_FI_PROF_DRAM_ACTIVE) indicates more efficient GPU usage.</p>	0–1.0	Percentage (fraction)

Category	Metric	Metric Name	Description	Value Range	Unit
	DCGM_FI_PROF_PIPE_TENSOR_ACTIVE	Tensor Activity	<p>Fraction of the period during which the tensor (HMMA/IMMA) pipe is active.</p> <p>This is an average value within a period, not an instantaneous value.</p> <p>A higher value indicates a higher utilization of tensor cores.</p> <p>Value 1 (100%) indicates that a tensor instruction is sent every instruction cycle in the entire period (one instruction is completed in two cycles).</p> <p>If the value is 0.2 (20%), the possible causes are as follows:</p> <p>During the entire period, 20% of the SM tensor cores run at 100% utilization.</p> <p>During the entire period, all SM tensor cores run at 20% utilization.</p> <p>During 1/5 of the entire period, all SM tensor cores run at 100% utilization.</p> <p>Other combinations</p>	0–1.0	Percentage (fraction)

Category	Metric	Metric Name	Description	Value Range	Unit
	DCGM_FI_PROF_DRAM_ACTIVE	Memory BW Utilization	<p>Percentage of the time for sending data to or receiving data from the device memory within a period.</p> <p>This is an average value within a period, not an instantaneous value.</p> <p>A higher value indicates a higher utilization of device memory.</p> <p>Value 1 (100%) indicates that a DRAM instruction is executed once per cycle throughout a period (the maximum value can be reached at a peak of about 0.8).</p> <p>If the value is 0.2 (20%), indicating that data is read from or written into the device memory during 20% of the cycle within a period.</p>	0–1.0	Percentage (fraction)

Category	Metric	Metric Name	Description	Value Range	Unit
	DCGM_FI_PROF_PIPE_FP16_ACTIVE	FP16 Engine Activity	<p>Fraction of the period during which the FP16 (half-precision) pipe is active.</p> <p>This is an average value within a period, not an instantaneous value.</p> <p>A larger value indicates a higher usage of FP16 cores.</p> <p>Value 1 (100%) indicates that the FP16 instruction is executed every two cycles (for example, Volta cards) in a period.</p> <p>If the value is 0.2 (20%), the possible causes are as follows:</p> <p>During the entire period, 20% of the SM FP16 cores run at 100% utilization.</p> <p>During the entire period, all SM FP16 cores run at 20% utilization.</p> <p>During 1/5 of the entire period, all SM FP16 cores run at 100% utilization.</p> <p>Other combinations</p>	0–1.0	Percentage (fraction)

Category	Metric	Metric Name	Description	Value Range	Unit
	DCGM_FI_PROF_PIPE_FP32_ACTIVE	FP32 Engine Activity	<p>Fraction of the period during which the fused multiply-add (FMA) pipe is active. Multiply-add applies to FP32 (single precision) and integers.</p> <p>This is an average value within a period, not an instantaneous value.</p> <p>A larger value indicates a higher usage of FP32 cores.</p> <p>Value 1 (100%) indicates that the FP32 instruction is executed every two cycles (for example, Volta cards) in a period.</p> <p>If the value is 0.2 (20%), the possible causes are as follows:</p> <p>During the entire period, 20% of the SM FP32 cores run at 100% utilization.</p> <p>During the entire period, all SM FP32 cores run at 20% utilization.</p> <p>During 1/5 of the entire period, all SM FP32 cores run at 100% utilization.</p> <p>Other combinations</p>	0–1.0	Percentage (fraction)

Category	Metric	Metric Name	Description	Value Range	Unit
	DCGM_FI_PROF_PIPE_FP64_ACTIVE	FP64 Engine Activity	<p>Fraction of the period during which the FP64 (double precision) pipe is active.</p> <p>This is an average value within a period, not an instantaneous value.</p> <p>A larger value indicates a higher usage of FP64 cores.</p> <p>Value 1 (100%) indicates that the FP64 instruction is executed every four cycles (for example, Volta cards) in a period.</p> <p>If the value is 0.2 (20%), the possible causes are as follows:</p> <p>During the entire period, 20% of the SM FP64 cores run at 100% utilization.</p> <p>During the entire period, all SM FP64 cores run at 20% utilization.</p> <p>During 1/5 of the entire period, all SM FP64 cores run at 100% utilization.</p> <p>Other combinations</p>	0–1.0	Percentage (fraction)

Category	Metric	Metric Name	Description	Value Range	Unit
	DCGM_FI_PROF_SM_ACTIVE	SM Activity	<p>Fraction of the time during which at least one thread bundle is active on an SM within a period.</p> <p>This is an average value of all SMs and is insensitive to the number of threads in each block.</p> <p>A thread bundle is active after being scheduled and allocated with resources. The thread bundle may be in the computing state or a non-computing state (for example, waiting for a memory request).</p> <p>If the value is less than 0.5, GPUs are not efficiently used. The value should be greater than 0.8.</p> <p>For example, a GPU has N SMs:</p> <p>A kernel function uses N thread blocks to run on all SMs in a period. In this case, the value is 1 (100%).</p> <p>A kernel function runs N/5 thread blocks in a period. In this case, the value is 0.2.</p> <p>A kernel function uses N thread blocks and runs only 1/5 of cycles in a period. In this case, the value is 0.2.</p>	0–1.0	Percentage (fraction)

Category	Metric	Metric Name	Description	Value Range	Unit
	DCGM_FI_PROF_PCIE_TX_BYTES DCGM_FI_PROF_PCIE_RX_BYTES	PCIe Bandwidth	<p>Rate of data transmitted or received over the PCIe bus, including the protocol header and data payload.</p> <p>This is an average value within a period, not an instantaneous value.</p> <p>The rate is averaged over the period. For example, if 1 GB of data is transmitted within 1 second, the transmission rate is 1 GB/s regardless of whether the data is transmitted at a constant rate or burst. Theoretically, the maximum PCIe Gen3 bandwidth is 985 MB/s per channel.</p>	≥ 0	Bytes/s

Category	Metric	Metric Name	Description	Value Range	Unit
	DCGM_FI_PROF_NVLINK_RX_BYTES DCGM_FI_PROF_NVLINK_TX_BYTES	NVLink Bandwidth	<p>Rate at which data is transmitted or received through NVLink, excluding the protocol header.</p> <p>This is an average value within a period, not an instantaneous value.</p> <p>The rate is averaged over the period. For example, if 1 GB of data is transmitted within 1 second, the transmission rate is 1 GB/s regardless of whether the data is transmitted at a constant rate or burst. Theoretically, the maximum NVLink Gen2 bandwidth is 25 GB/s per link in each direction.</p>	≥ 0	Bytes/s
Network I/O	ma_container_network_receive_bytes	Downlink Rate (BPS)	Inbound traffic rate of a measured object	≥ 0	Bytes/s
	ma_container_network_receive_packets	Downlink Rate (PPS)	Number of data packets received by a NIC per second	≥ 0	Packets/s
	ma_container_network_receive_error_packets	Downlink Error Rate	Number of error packets received by a NIC per second	≥ 0	Count/s
	ma_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
	ma_container_network_transmit_error_packets	Uplink Error Rate	Number of error packets sent by a NIC per second	≥ 0	Count/s
	ma_container_network_transmit_packets	Uplink Rate (PPS)	Number of data packets sent by a NIC per second	≥ 0	Packets/s
NPU	ma_container_npu_util	NPU Usage	NPU usage of a measured object	0-100	%
	ma_container_npu_memory_util	NPU Memory Usage	Percentage of the used NPU memory to the total NPU memory	0-100	%
	ma_container_npu_memory_used_megabytes	Used NPU Memory	NPU memory used by a measured object	≥ 0	MB
	ma_container_npu_memory_total_megabytes	Total NPU Memory	Total NPU memory of a measured object	≥ 0	MB

1.7.5 Metric Dimensions

Dimensions of VM Metrics Reported by ICAgents

Table 1-10 Dimensions of VM metrics reported by ICAgents

Category	Metric Dimension	Description
Network metrics	clusterId	Cluster ID
	hostId	Host ID
	nameSpace	Cluster namespace
	netDevice	NIC name

Category	Metric Dimension	Description
	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
	npulD	NPU ID
	hostID	Host ID
	nameSpace	Cluster namespace
	nodeIP	Host IP address
	hostName	Host name
Cluster metrics	clusterId	Cluster ID

Category	Metric Dimension	Description
	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
	serviceID	Inventory ID

1.8 Basic Concepts

1.8.1 Resource Monitoring

Table 1-11 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, 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, or CCE encounters some changes. Events do not necessarily cause service exceptions. Events do not need to be handled.</p>
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.

Terminology	Description
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 notification rule	<p>An alarm notification 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 1-12 Basic concepts of collection management

Terminology	Description
UniAgent	<p>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.</p>

Terminology	Description
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 on the ECS or BMS console, manually install ICAgents. For the hosts that are 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, 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 using roles to grant permissions, you may also need to assign other roles on which the permissions depend to take effect. 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 1-13](#) lists all the system permissions supported by AOM.

Table 1-13 System permissions supported by AOM

Subservice Name	Policy Name	Description	Type	Dependency Permissions
Monitoring center / collection management	AOM Admin	Administrator permissions for AOM 2.0. Users granted these permissions can operate and use AOM.	System-defined policy	CCE FullAccess, DMS ReadOnly Access, CCE Namespace-level Permissions, LTS FullAccess For CCE namespaces, users or user groups must be granted the administrator (cluster-admin) or custom permissions. If custom permissions are granted, the get, list, and update permissions must be included and the resources of configmaps, prometh

Subse rvice Name	Policy Name	Description	Type	Depende ncy Permissi ons
				euses, servicem onitors, podmoni tors, and namespa ces must also be specified .

Subservice Name	Policy Name	Description	Type	Dependency Permissions
	AOM Viewer	Read-only permissions for AOM 2.0. Users granted these permissions can only view AOM data.	System-defined policy	CCE ReadOnly Access, DMS ReadOnly Access, CCE Namespace-level Permissions, LTS ReadOnly Access For CCE namespaces, users or user groups must be granted the administrator (cluster-admin) or custom permissions. If custom permissions are granted, the get and list permissions must be included and the resources of configmaps, prometheuses,

Subservice Name	Policy Name	Description	Type	Dependencies Permissions
				servicemonitors, podmonitors, and namespaces must also be specified.

Common Operations and System Permissions for Resource Monitoring

Table 1-14 lists the common operations supported by each system-defined policy of resource monitoring. Select policies as required.

Table 1-14 Common operations supported by each system-defined policy

Operation	AOM Admin	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 notification rule	✓	x
Modifying an alarm notification rule	✓	x
Deleting an alarm notification rule	✓	x
Creating a message template	✓	x
Modifying a message template	✓	x

Operation	AOM Admin	AOM Viewer
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
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 1-15 lists the common operations supported by each system-defined policy of collection management. Select policies as required.

Table 1-15 Common operations supported by each system-defined policy of collection management

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

Operation	AOM Admin	AOM Viewer
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	√	√
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	√	√

Operation	AOM Admin	AOM Viewer
Deleting an installation host	√	x
Upgrading Agents in batches	√	x
Querying historical task logs	√	√
Querying historical task details	√	√
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	√	√

Operation	AOM Admin	AOM Viewer
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	√	√
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

Operation	AOM Admin	AOM Viewer
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 1-16](#).

Table 1-16 Fine-grained permissions of AOM

Permission	Description	Permission Dependency	Application Scenario
aom:alarm:put	Reporting an alarm	N/A	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
aom:event2AlarmRule:list	Querying all event alarm rules		Querying all event alarm rules
aom:actionRule:create	Adding an alarm notification rule		Adding an alarm notification rule
aom:actionRule:delete	Deleting an alarm notification rule		Deleting an alarm notification rule
aom:actionRule:list	Querying the alarm notification rule list		Querying the alarm notification rule list

Permission	Description	Permission Dependency	Application Scenario
aom:actionRule:update	Modifying an alarm notification rule		Modifying an alarm notification rule
aom:actionRule:get	Querying an alarm notification rule by name		Querying an alarm notification 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
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

Permission	Description	Permission Dependency	Application Scenario
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 Dependency Services

If an IAM user needs to view data or use functions on the AOM console, grant the **AOM Admin** or **AOM Viewer** policy to the user group to which the user belongs and then add the roles or policies required by dependency services by referring to [Table 1-17](#). **When you subscribe to AOM for the first time, AOM will automatically create a service agency. In addition to the AOM Admin permission, the Security Administrator permission must be granted.**

Table 1-17 Roles/Policies required by AOM dependency services

Console Function	Dependency Service	Policy/Role Required
<ul style="list-style-type: none">• Workload monitoring• Cluster monitoring• Prometheus for CCE	CCE	To use workload and cluster monitoring and Prometheus for CCE, you need to set the CCE FullAccess and CCE Namespace permissions.
<ul style="list-style-type: none">• Log management• Log transfer• Log ingestion rules• Host group management• Log alarm rules	LTS	To use log management, log transfer, log ingestion rules, host group management, and log alarm rules, you need to set the LTS FullAccess permission.

Console Function	Dependency Service	Policy/Role Required
Enterprise project	Enterprise Project Management Service (EPS)	To use enterprise projects, you need to set the EPS ReadOnlyAccess 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

During the installation of UniAgent and ICAgent on Linux hosts, the history recording function is disabled. Therefore, your AK/SK and access code cannot be viewed by running commands. Additionally, credentials are encrypted for storage to prevent leaks.

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 Monitoring CCE Metrics

Cloud Container Engine (CCE) is an enterprise-level cluster hosting service. It allows you to quickly build reliable container clusters based on cloud servers, and easily create and manage different containerized workloads. AOM is a one-stop, multi-dimensional O&M platform for cloud applications. It enables you to monitor real-time running of applications, resources, and services and detect faults in a timely manner, improving O&M efficiency. After CCE is interconnected with AOM, CCE cluster information can be reported to AOM. AOM can monitor the status and performance of CCE clusters and provide alarm notifications in real time.

You can set alarm rules in AOM to check whether resources in CCE clusters are normal and learn about real-time cluster running. This section uses **aom_container_cpu_usage** as an example to describe how to set an alarm rule.



Procedure

1. **Subscribing to AOM 2.0 for the First Time and Granting Permissions**
2. **Monitoring Containers:** Purchase a cluster and node on CCE. The ICAgent is then automatically installed to report cluster metrics to AOM.
3. **Setting an Alarm Notification Rule:** Create an alarm notification rule and associate it with an SMN topic and a message template. If the CCE metric data meets the alarm condition, the system sends an alarm notification accordingly. If you do not want to receive alarm notifications by email or SMS, there is no need to set alarm notification rules.
4. **Setting an Alarm Rule:** Create an alarm rule for the CCE metric. If the metric data meets the alarm condition, an alarm will be generated.

Preparation

This section uses a CCE metric as an example. You need to purchase a cluster and node in CCE in advance. If you already have a cluster and node, skip this step.

Subscribing to AOM 2.0 for the First Time and Granting Permissions

1. Register an account and perform real-name authentication.
Before using AOM 2.0, register an account and perform real-name authentication.
2. Subscribe to AOM 2.0.
Before using AOM 2.0, subscribe to it. If you have subscribed to AOM 2.0, skip the following operations.
 - a. Log in to the management console.
 - b. Click  in the upper left corner and select your desired region from the drop-down list.
 - c. Click  on the left and choose **Management & Deployment > Application Operations Management**. In the navigation pane on the left, choose **AOM 2.0**. The AOM 2.0 page is displayed.
 - d. On the displayed dialog box, read the billing changes for switching AOM 1.0 to AOM 2.0.
 - e. Click **Authorize**. On the displayed **Service Authorization** page, read the *Authorization Statement* and select "I have read and agreed to the *Authorization Statement*".
 - f. Click **Subscribe and Authorize for Free** for AOM 2.0.
3. Grant the AOM and CCE permissions to the user.
Ensure that **AOM FullAccess** and **CCE FullAccess** permissions are granted.

Monitoring Containers

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane, choose **Infrastructure Monitoring > Container Insights > Workload Monitoring**.
- Step 3** Click a workload on any workload tab page. The workload details such as the name, status, cluster, and namespace are displayed. For example, monitor workload **coredns**, which belongs to cluster **aom-doc-test**.

You can also create more workloads to monitor.

----End

Setting an Alarm Notification Rule

- Step 1** In the navigation pane, choose **Alarm Center > Alarm Notification**.
- Step 2** On the **Notification Rules** tab page, click **Create**. On the displayed page, set parameters by referring to [Table 2-1](#).

Table 2-1 Alarm notification rule parameters

Parameter	Description	Example
Notification Rule Name	Name of an alarm notification 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.	Mon_alarm
Enterprise Project	Select the required enterprise project. The default value is default . <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.• To use the enterprise project function, contact engineers.	default
Description	Description of the notification rule. Enter up to 1,024 characters. In this example, leave this parameter blank.	-
Rule Type	Type of an alarm notification rule. Select Prometheus monitoring in this example. Prometheus monitoring: If a metric or an event meets the alarm condition, the system sends an alarm notification based on the associated SMN topic and message template.	Prometheus monitoring
Topic	SMN topic. Select a 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.	-

Step 3 Click **OK**.

----End

Setting an Alarm Rule

Metric alarm rules can be created using the following modes: **Select from all metrics** and **PromQL**.

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

Step 1 In the navigation pane, choose **Alarm Center > Alarm Rules**. Then, click **Create Alarm Rule**.

Step 2 Set basic information about the alarm rule by referring to [Table 2-2](#).

Table 2-2 Basic information

Parameter	Description	Example
Original Rule Name	Original name of a rule. Enter a maximum of 256 characters and do not start or end with underscores (_) or hyphens (-). Only letters, digits, underscores, and hyphens are allowed.	monitor_cc e
Rule Name	Name of a rule. Enter a maximum of 256 characters and do not start or end with underscores (_) or hyphens (-). Only letters, digits, underscores, and hyphens are allowed.	-
Enterprise Project	Select the required enterprise project. The default value is default . <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.• To use the enterprise project function, contact engineers.	default
Description	Description of the rule. Enter up to characters. In this example, leave this parameter blank.	-


Step 3 Set the detailed information about the alarm rule.

1. **Rule Type: Metric alarm rule.**
2. **Configuration Mode: Select from all metrics.** Then you can set alarm conditions for different types of resources.
3. Select a target Prometheus instance from the drop-down list. In this example, select **Prometheus_AOM_Default**.
4. Set alarm rule details by referring to [Table 2-3](#).

After the setting is complete, the monitored metric data is displayed in a line graph above the alarm conditions. You can click **Add Metric** to add more metrics and set the statistical period and detection rules for them.

Table 2-3 Alarm rule details



Parameter	Description	Example
Multiple Metrics	Calculation is performed based on the preset alarm conditions one by one. An alarm is triggered when one of the conditions is met.	Multiple Metrics

Parameter	Description	Example
Metric	Metric to be monitored. Click the Metric text box. In the resource tree on the right, you can select a target metric by resource type.	aom_container_cpu_usage
Statistical Period	Interval at which metric data is collected.	1 minute
Conditions	Metric monitoring scope. If this parameter is left blank, all resources are covered. Set the condition based on the workload mentioned in 3 .	Cluster name=aom-doc-test AND Workload name=coredns
Grouping Condition	Aggregate metric data by the specified field and calculate the aggregation result.	Not grouped
Rule	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.	Avg > 10
Trigger Condition	When the metric value meets the alarm condition for a specified number of consecutive periods, a metric alarm will be generated.	3
Alarm Severity	Severity of a metric alarm.	

Step 4 Click **Advanced Settings** and set information such as **Check Interval** and **Alarm Clearance**. For details about the parameters, see [Table 2-4](#).

Table 2-4 Advanced settings

Parameter	Description	Example
Check Interval	Interval at which metric query and analysis results are checked.	Custom interval: 1 minute
Alarm Clearance	The alarm will be cleared when the alarm condition is not met for a specified number of consecutive periods.	1

Parameter	Description	Example
Action Taken for Insufficient Data	Action to be taken if there is no or insufficient metric data within the monitoring period. Enable this option if needed.	Enabled: If the data is insufficient for 1 period, the status will change to Insufficient data and an alarm will be sent.
Tags	Click  to add an alarm rule tag. It is an alarm identification attribute in the format of "key:value". It is used in alarm noise reduction scenarios. In this example, leave this parameter blank. For details, see Alarm Tags and Annotations .	-
Annotations	Click  to add an alarm rule annotation. It is an alarm non-identification attribute in the format of "key:value". It is used in alarm notification and message template scenarios. In this example, leave this parameter blank. For details, see Alarm Tags and Annotations .	-

Step 5 Set an alarm notification policy. For details, see [Table 2-5](#).

Table 2-5 Alarm notification policy parameters

Parameter	Description	Example
Notify When	Set the scenario for sending alarm notifications. By default, Alarm triggered and Alarm cleared are selected. <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.	Retain the default value.

Parameter	Description	Example
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 a notification rule.• Frequency: frequency for sending alarm notifications. Select a desired value from the drop-down list.• Notification Rule: After the rule is enabled, the system sends notifications based on the associated SMN topic and message template. If there is no alarm notification rule you want to select, click Add Rule in the drop-down list to create one. For details about how to set alarm notification rules, see Setting an Alarm Notification Rule.	Alarm Mode: Select Direct alarm reporting . Frequency: Select Once . Notification Rule: Mon_alarm

Step 6 Click **Confirm**. Then click **View Rule** to view the created 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 the alarm, choose **Alarm Center > 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

Related Information

After an alarm rule is configured, you can perform the following operations if needed:

- On the workload details page, click the **Alarms** tab to check alarms. Alternatively, choose **Alarm Center > Alarm List** to check alarms. For details, see [Checking AOM Alarms or Events](#).
- Create metric alarm rules in different ways. For details, see [Creating an AOM Metric Alarm Rule](#).

2.2 Using Prometheus to Monitor ECS Metrics

An Elastic Cloud Server (ECS) is a computing server consisting of the CPU, memory, OS, and Elastic Volume Service (EVS) disk. It supports on-demand allocation and auto scaling. ECSs integrate Virtual Private Cloud (VPC), security group, and Cloud Firewall (CFW) capabilities to create an efficient, reliable, and secure computing environment. This ensures stable and uninterrupted running of services. AOM is a one-stop, multi-dimensional O&M platform for cloud applications. It enables you to monitor real-time running of applications, resources, and services and detect faults in a timely manner, improving O&M efficiency. After an ECS is connected to AOM, AOM can monitor the ECS in real time and send alarm notifications.

This section uses the **node_network_up** metric of an ECS as an example to describe how to use AOM.

Constraints

The ECS must be in the same region as the AOM console.

Procedure

1. **Installing UniAgent on the ECS:** Install UniAgent on the host in the region where the AOM console is located to centrally manage metric collection plugins.
2. **Creating a Host Group:** Create a host group for better host management and more efficient data collection.
3. **Connecting an ECS to AOM:** Connect an ECS to AOM. Then you can install Node Exporter and configure collection tasks for the host group. The collected metrics will be stored in the Prometheus instance for ECS for easy management.
4. **Setting a Metric Alarm Rule:** Create an alarm rule for the ECS metric. If the metric data meets the alarm condition, an alarm will be generated.

Prerequisites

- You have purchased an ECS.. If you already have an ECS, skip this step.
- You have **subscribed to AOM 2.0 and granted permissions**.

Installing UniAgent on the ECS

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Settings > Global Settings**.

Step 3 On the displayed page, choose **Collection Settings > UniAgents** and click **Try New Version** in the upper right corner of the page.

Step 4 On the displayed page, check the UniAgent status of the ECS.

- If the UniAgent status is **Running**, UniAgent has been installed. In this case, go to **Creating a Host Group**.
- If the UniAgent status is **Offline**, UniAgent is abnormal.
- If the UniAgent status is **Installing**, UniAgent is being installed. Wait for UniAgent installation.
- If the UniAgent status is **Installation failed** or **Not installed**, UniAgent fails to be installed or is not installed on the host. In this case, install it.

Step 5 On the **ECS** tab page, click **Install UniAgent** and then select the **Install via Script (Recommended)** scenario.

Step 6 On the **Install UniAgent** page, set parameters.

Table 2-6 Installation parameters

Parameter	Description	Example
Server Region	Region where the target server is located. Current region: The network between AOM and the server in the current region is connected.	Current region
Server Type	Options: ECSs and Other Servers . Select ECSs . ECSs: hosts managed by the ECS service.	ECSs
Installation Mode	Option: CLI . You need to remotely log in to the server to run the installation command provided on the console.	CLI
OS	Options: Linux and Windows . Select Linux in this example.	Linux
UniAgent Version	Select a UniAgent version. The latest version is selected by default.	Latest version
Copy and Run Installation Command	Click Copy to copy the installation command.	Copy the Linux installation command.

Step 7 Log in to the ECS and run the Linux installation command copied in [6](#) as the **root** user.

Step 8 Check the UniAgent status in the UniAgent list. If the UniAgent status is **Running**, the installation is successful.

----End

Creating a Host Group

You can create host groups of the IP address and custom identifier types. In this example, select the IP address type.

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Settings > Global Settings**.

Step 3 On the **Global Settings** page, choose **Collection Settings > Host Groups** and click **Create Host Group**.

Step 4 On the displayed page, set related parameters.

Table 2-7 Parameters

Parameter	Description	Example
Host Group	Name of a host group. Enter 1 to 64 characters. Do not start with a period (.) or underscore (_) or end with a period. Only letters, digits, hyphens (-), underscores, and periods are allowed.	aom-ecs
Host Group Type	Type of the host group. Options: IP and Custom identifier . In this example, select IP .	IP
Host Type	Host type. Default: Linux .	Linux
Remark	Host group remarks. Enter up to 1,024 characters. In this example, leave this parameter blank.	-

Step 5 In the host list, select one or more hosts to add to the group and click **OK**.

----End

Connecting an ECS to AOM

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Access Center > Access Center**. Click **Try New Version** in the upper right corner of the page.

Step 3 Locate the **Elastic Cloud Server (ECS)** card under **Running environments** and click **Ingest Metric (AOM)** on the card.

Step 4 Set parameters for connecting to the ECS.

1. Select a Prometheus instance.
 - a. **Instance Type:** Select a Prometheus instance type. Options: **Prometheus for ECS** and **Common Prometheus instance**.
 - b. **Instance Name:** Select a Prometheus instance from the drop-down list. If no Prometheus instance is available, click **Create Instance**. For details, see [Table 2-8](#).

Table 2-8 Creating a Prometheus instance

Parameter	Description	Example
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.	mon_ECS

Parameter	Description	Example
Enterprise project.	Select the required enterprise project. The default value is default . <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.▪ To use the enterprise project function, contact engineers.	default
Instance Type	Type of the Prometheus instance. Options: Prometheus for ECS and Common Prometheus instance .	Prometheus for ECS

2. Select a host group.

In the host group list, select the host group created in [Creating a Host Group](#).

3. Configure the collection.

Under **Configure Collection**, set parameters by referring to the following table.

Table 2-9 Collection configuration

Category	Parameter	Description	Example
Basic Settings	Configuration Name	Name of a metric ingestion rule. Enter up to 50 characters starting with a letter. Only letters, digits, underscores (_), and hyphens (-) are allowed.	ecs-rule
Metric Collection Rule	Metric Collection Interval (s)	Interval for collecting metrics, in seconds. Options: 10 , 30 , and 60 (default).	60
	Metric Collection Timeout (s)	Timeout period for executing a metric collection task, in seconds. Options: 10 , 30 , and 60 (default). The timeout period cannot exceed the collection interval.	60
	Executor	User who executes the metric ingestion rule, that is, the user of the selected host group. Default: root .	root

Category	Parameter	Description	Example
Other	Custom Dimensions	Dimensions (key-value pairs) added to specify additional metric attributes. You can click Add Dimension to add multiple custom dimensions (key-value pairs). In this example, leave this parameter blank.	-
	Import ECS Tags as Dimensions	This function is disabled by default. If it is enabled, ECS tags (key-value pairs) will be written to metric dimensions and tag changes will be synchronized to AOM.	Disable

Step 5 After the configuration is complete, click **Next**. The ECS metrics can then be ingested.

----End

Setting a Metric Alarm Rule

Metric alarm rules can be created in the following modes: **Select from all metrics** and **PromQL**.

The following describes how to create an alarm rule when **Configuration Mode** is set to **Select from all metrics**.

Step 1 In the navigation pane, choose **Alarm Center > Alarm Rules**. Then, click **Create Alarm Rule**.

Step 2 Set basic information about the alarm rule by referring to [Table 2-10](#).

Table 2-10 Basic information

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

Parameter	Description	Example
Enterprise Project	Select the required enterprise project. The default value is default . <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.• To use the enterprise project function, contact engineers.	default
Description	Description of the rule. Enter up to 1,024 characters. In this example, leave this parameter blank.	-






Step 3 Set the detailed information about the alarm rule.

1. **Rule Type: Metric alarm rule.**
2. **Configuration Mode: Select from all metrics.** Then you can set alarm conditions for different types of resources.
3. Select the target Prometheus instance from the drop-down list. In this example, select the instance created in [Step 4.1.b](#).
4. Set alarm rule details. [Table 2-11](#) describes the parameters.

After the setting is complete, the monitored metric data is displayed in a line graph above the alarm conditions. You can click **Add Metric** to add more metrics and set the statistical period and detection rules for them.

Table 2-11 Alarm rule details



Parameter	Description	Example
Multiple Metrics	Calculation is performed based on the preset alarm conditions one by one. An alarm is triggered when one of the conditions is met.	Multiple Metrics
Metric	Metric to be monitored. Click the Metric text box. In the resource tree on the right, select a target metric by resource type.	node_net work_up
Statistical Period	Interval at which metric data is collected.	1 minute
Conditions	Metric monitoring scope. If this parameter is left blank, all resources are covered. In this example, leave this parameter blank.	-
Grouping Condition	Aggregate metric data by the specified field and calculate the aggregation result.	Not grouped

Parameter	Description	Example
Rule	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.	Avg > 1
Trigger Condition	When the metric value meets the alarm condition for a specified number of consecutive periods, a metric alarm will be generated.	3
Alarm Severity	Severity of a metric alarm. <ul style="list-style-type: none">– : a critical alarm.– : a major alarm.– : a minor alarm.– : a warning.	

Step 4 Click **Advanced Settings** and set information such as **Check Interval** and **Alarm Clearance**. For details about the parameters, see [Table 2-12](#).

Table 2-12 Advanced settings

Parameter	Description	Example
Check Interval	Interval at which metric query and analysis results are checked.	Custom interval: 1 minute
Alarm Clearance	The alarm will be cleared when the alarm condition is not met for a specified number of consecutive periods.	1
Action Taken for Insufficient Data	Action to be taken if there is no or insufficient metric data within the monitoring period. Enable this option if needed.	Enabled: If the data is insufficient for 1 period, the status will change to Insufficient data and an alarm will be sent.

Parameter	Description	Example
Tags	Click  to add an alarm rule tag. It is an alarm identification attribute in the format of "key:value". It is used in alarm noise reduction scenarios. In this example, leave this parameter blank. For details, see Alarm Tags and Annotations .	-
Annotations	Click  to add an alarm rule annotation. It is an alarm non-identification attribute in the format of "key:value". It is used in alarm notification and message template scenarios. In this example, leave this parameter blank. For details, see Alarm Tags and Annotations .	-

Step 5 Set an alarm notification policy. For details, see [Table 2-13](#).

Table 2-13 Alarm notification policy parameters

Parameter	Description	Example
Notify When	Set the scenario for sending alarm notifications. By default, Alarm triggered and Alarm cleared are selected. <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.	Retain the default value.
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 a notification rule.• Frequency: frequency for sending alarm notifications. Select a desired value from the drop-down list.• Notification Rule: After the rule is enabled, the system sends notifications based on the associated SMN topic and message template. If there is no alarm notification rule you want to select, click Add Rule in the drop-down list to create one. For details about how to set alarm notification rules, see Setting an Alarm Notification Rule.	<ul style="list-style-type: none">• Alarm Mode: Select Direct alarm reporting.• Frequency: Select Once.• Notification Rule: Mon_aom

Step 6 Click **Confirm**. Then click **View Rule** to view the created 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 the alarm, choose **Alarm Center > 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

Related Information

After an alarm rule is configured, you can perform the following operations if needed:

- Choose **Alarm Center > Alarm List** to check alarms. For details, see [Checking AOM Alarms or Events](#).
- Create metric alarm rules in different ways. For details, see [Creating an AOM Metric Alarm Rule](#).

3 Using IAM to Grant Access to AOM

3.1 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.

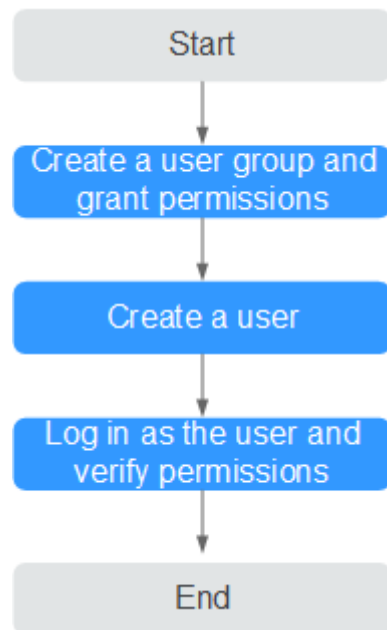
This section describes the procedure for granting permissions (see [Figure 3-1](#)).

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 "Permission Description" in Help Center.

Process Flow

Figure 3-1 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.

3.2 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: Create a JSON policy or edit an existing one.

For details about how to create custom policies, see [Creating a Custom Policy](#). The following lists examples of common AOM custom policies.

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"
      ]
    }
  ]
}
```

4 AOM Overview

The **Overview** page provides panoramic monitoring of resources and logs. It displays [Updates](#), [Alarm Overview](#), [Usage Overview](#), [Prometheus Monitoring](#), [Log Monitoring](#), [Common Functions](#), and [FAQs](#).

Constraints

- To view LTS data on the **Panorama** page, you need to obtain the **lts:trafficStatistic:get** and **lts:groups:list** permissions in advance.
- AOM automatically checks ICAgent versions. If AOM detects that an ICAgent version is no longer maintained, a message indicating that the ICAgent version is too early will be displayed when you log in to the AOM console. You can authorize an automatic ICAgent upgrade during off-peak hours or [manually upgrade the ICAgent](#) on the UniAgent management page. If you do not need to upgrade ICAgent, select **Do not show again**.



Viewing Overview

Step 1 Log in to the AOM 2.0 console.

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

Step 3 Click the time selection box in the upper right corner of the page and select a period from the drop-down list. Options: **Last 30 minutes**, **Last hour**, **Last 6 hours**, **Last day**, and **Last week**.

You can also perform the following operations if needed:

- Manual refresh: Click  in the upper right corner of the page to manually refresh the page.
- Automatic refresh: Click the drop-down arrow next to  in the upper right corner of the page and select an automatic refresh interval.

----End

Updates

This card displays the latest functions of AOM 2.0.

Alarm Overview

This card displays the total number of alarms, number of alarms of each severity, and alarm sources. You can click **alarm rules** to [configure alarm rules](#).

Usage Overview

This card displays the number of resources under Prometheus and cloud log monitoring.

- **Prometheus Monitoring:** displays the number of Prometheus instances. You can click **Ingest Metric** to go to the [instance list](#) page.
- **Cloud Log Monitoring:** displays the number of monitored log groups and log streams. You can click **Ingest Log** to go to the [Log Management](#) page.

Prometheus Monitoring

This card displays the Prometheus instances you have created. You can view the instance name, instance type, basic metrics, custom metrics, and billing mode of each instance. By default, the five Prometheus instances with the most basic metrics are displayed. You can also sort the instances by instance name, custom metrics, or billing mode.

- **Usage Statistics:** Click **Usage Statistics** to go to the [Usage Statistics](#) page.
- **Create an instance:** Click **Create an Instance** to go to the [Instances](#) page.
- **Access Center:** Click **Access Center** to go to the [Access Center](#) page.

Log Monitoring

This card displays the read/write traffic, index traffic-standard log stream graph, and top 5 log groups with the most log streams. By default, only the top 5 log groups with the most log streams are displayed. You can sort log groups by log group name, remark, log streams, or tags.

- **Usage Statistics:** Click **Usage Statistics** to go to the [Log Management](#) page.
- **Add Log Group:** Click **Add Log Group** to go to the [Log Management](#) page.
- **Access Center:** Click **Access Center** to go to the [Access Center](#) page.

Common Functions

This card displays common functions of AOM.

- **Customize Alarm Template:** Click **Customize Alarm Template** to go to the [Alarm Templates](#) page.
- **Create Alarm Rule:** Click **Create Alarm Rule** to create [a metric alarm rule](#) or [an event alarm rule](#).
- **Create Notification Rule:** Click **Create Notification Rule** to go to the [Alarm Notifications](#) page.
- **Create Message Template:** Click **Create Message Template** to go to the [Message Templates](#) page.
- **Customize Dashboard:** Click **Customize Dashboard** to go to the [Dashboard](#) page.

FAQs

This card displays the FAQs about AOM 2.0. For more details, see [FAQs](#).

5 Connecting to AOM

5.1 AOM Access Overview

AOM monitors metric and log data from multiple dimensions at different layers in multiple scenarios. Through the old access center, you can quickly ingest metrics and logs to monitor. After the ingestion is complete, you can view the metrics, logs, and statuses of related resources or applications on the [Metric Browsing](#) page.

Constraints

If you want to switch from the new access center to the old one, you need to click **Back to Old Version** in the upper right corner.

Ingesting Metrics or Logs to AOM

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane, choose **Access Center** > **Access Center**.
- Step 3** Ingest metrics or logs based on monitored object types.

Table 5-1 Access overview

Type	Monitored Object	Data Source	Access Mode
Prometheus running environment access	Cloud Container Engine (CCE) (ICAgent)	Metrics	Uses ICAgent to collect CCE cluster metrics. By default, ICAgent is installed when you purchase a CCE cluster and node. ICAgent automatically reports CCE cluster metrics to AOM. For details about the CCE cluster metrics that are automatically reported to AOM, see Basic Metrics: VM Metrics .
Prometheus cloud service access	Supported cloud services	Metrics	5.3 Connecting Cloud Services to AOM
Open-source monitoring system access	Common Prometheus instance	Metrics	5.4 Connecting Open-Source Monitoring Systems to AOM
Prometheus API/SDK access	AOM APIs	Metrics	See section "Adding Monitoring Data" in the <i>Application Operations Management (AOM) API Reference</i> .
Custom Prometheus plug-in access	Custom Prometheus plug-ins	Metrics	5.5 Connecting Custom Plug-ins to AOM
Log ingestion	Cloud services, self-built software, APIs/SDKs, and cross-account ingestion-log streams	Logs	Section "Log Ingestion" in the <i>Log Tank Service (LTS) User Guide</i>

----End

5.2 Managing Collector Base UniAgent

5.2.1 Installing UniAgents

UniAgents centrally manage the life cycle of collection plug-ins and deliver instructions (such as script delivery and execution). UniAgents do not collect metric data themselves. O&M data is collected by collection plug-ins. You can install collection plug-ins through the access center and create collection tasks to collect metric data.

AOM allows you to install UniAgents on cloud servers in a VPC.

Prerequisite

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

Constraints

- For details about the Linux and Windows OSs supported by the UniAgent, see [Collection Management Restrictions](#).
- To switch from the new UniAgent page to the old one, choose **Settings** > **Global Settings** > **Collection Settings** > **UniAgents** in the navigation tree on the left and click **Back to Old Version** in the upper right corner. To go to the [new UniAgent](#) page, click **Try New Version** in the upper right corner of the **UniAgents** page.

Installation Methods

Install a UniAgent on a host manually or remotely. Select an installation mode based on site requirements.

Table 5-2 Installation methods

Method	Scenario
Manual UniAgent Installation	Suitable for initial installation and single-node installation scenarios. Log in to the host where the UniAgent is to be installed and manually run the installation command. When installing a UniAgent for the first time, you must install it manually.
Remote UniAgent Installation	Suitable for the scenario where UniAgents are installed in batches. Set a host where a UniAgent has been installed to be an installation host , and use it to install UniAgents on other hosts. (Enter the information about the hosts where UniAgents are to be installed on the installation page.)


Manual UniAgent 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 on the left, choose **Settings > Global Settings**.
- Step 3** In the navigation pane, choose **Collection Settings > UniAgents**. Click **Install UniAgent** in the upper right corner and select **Manual**. (When you install the UniAgent for the first time, the **Manual** page is displayed by default.)
- Step 4** On the **Install UniAgent** page, set parameters to install a UniAgent.

Table 5-3 Parameters for manual installation

Parameter	Description	Example
UniAgent Version	Version of a UniAgent. This parameter is mandatory.	1.1.8
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 install the UniAgent on a host through the proxy.	Direct access
Proxy Area	Manages proxies by category. When Access Mode is set to Proxy access , you need to select or add a proxy area. A proxy area must contain an available proxy. This proxy must be a cloud host where a UniAgent has been installed.	Select a proxy area.

Parameter	Description	Example
Installation Command	<p>Command for installing the UniAgent. Commands for Linux and Windows are different.</p> <p>Linux</p> <ol style="list-style-type: none"> Click  to copy the installation command. <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 -p xxxxxx -d https://aom-uniagent-xxxxxx -m https://aom.mgr-lb. xxxxxx,https://xx.xx.xx.xx:xxxx -v 1.x.x -q false set -o history;</pre> <p>Windows</p> <ol style="list-style-type: none"> Copy the download address (https://aom-uniagent-{region_name}.obs.{region_name}.{site domain name suffix}/+uniagentd-{version}-win32.zip) to the browser to download the installation package. <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. Enter the following configuration (obtained from the installation page) to the C:\uniagentd\conf\uniagentd.conf file: <pre>master=https://aom-mgr-lb.xxxxxxxxxxxx,https:// xx.xx.xx.xx:xxxxx project_id=xxxxxxxxxxxxxxxxx public_net=xxxx</pre> Run start.bat in the C:\uniagentd\bin directory as the administrator. 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.
- Linux host: Use a remote login tool to log in to the target host and run the installation command copied in the [previous step](#) as the **root** user to install the UniAgent.
 - Windows host: Log in to the target host, and download the installation package based on the installation command in the [previous step](#) to install the UniAgent.

Step 6 Check whether the UniAgent is displayed in the UniAgent list.

----End

Remote UniAgent Installation

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane on the left, choose **Settings > Global Settings**.
- Step 3** In the navigation pane on the left, choose **Collection Settings > UniAgents**. Click **Install UniAgent** in the upper right corner.
- Step 4** On the **Install UniAgent** page, choose **Remote** and set parameters to install a UniAgent. (When you install the UniAgent for the first time, the **Manual** page is displayed by default. **Remote** is not available. Remote installation can be performed only when you have an installation host.)

Table 5-4 Parameters for remotely installing a UniAgent

Parameter	Description	Example
UniAgent Version	Version of a UniAgent. This parameter is mandatory.	1.1.8
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	Manages proxies by category. When Access Mode is set to Proxy access , you need to select or add a proxy area. A proxy area must contain an available proxy. This proxy must be a cloud host where a UniAgent has been installed.	Select a proxy area.

Parameter	Description	Example
Installation Host	<p>An installation host is used to execute commands for remote installation. This parameter is mandatory. To install the UniAgent remotely, ensure that the installation host does not run Windows.</p> <p>If no installation host has been configured, perform the following steps:</p> <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.	Select an installation host.

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>Add a maximum of 100 hosts:</p> <ul style="list-style-type: none"> • Host IP Address: IP address of a host. • OS: operating system of the host, which can be Linux or Windows. To install the UniAgent remotely, ensure that the host does not run Windows. • 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. • Login Port: port for accessing the host. • Authentication Mode: Currently, only password-based authentication is supported. • Password: password for logging in to the host. • Connectivity Test Result: shows whether the network between the installation host and the host where the UniAgent is to be installed is normal. <p>After entering the host information, you can delete, copy, or test the connectivity of hosts in the Operation column.</p> <p>The connectivity test checks the network between the installation host and the host where the UniAgent is to be installed. The test result is displayed in the Connectivity Test Result column. (Windows hosts do not support connectivity tests.)</p>	Enter the information about the hosts where UniAgents are to be installed.
Install ICAgent	<p>The ICAgent is a plug-in for collecting metrics and logs. The Install ICAgent option is enabled by default. It is optional. To install the ICAgent remotely, ensure that the host does not run Windows.</p>	-

Step 5 Click **Install**. After the installation is complete, you can [view the UniAgent status](#) in the UniAgent list.

----End

Checking the UniAgent Status

On the **VM Access** page, check the UniAgent status of the target host. For details, see [Table 5-5](#).




Table 5-5 UniAgent statuses


Status	Description
Running	The UniAgent is working.
Offline	The UniAgent is abnormal.
Installing	The UniAgent is being installed. The installation takes about 1 minute to complete.
Installation failed	The UniAgent fails to be installed. Uninstall the UniAgent and then reinstall it.
Not installed	The UniAgent has not been installed.

Other Operations

If needed, perform the following operations on the host where the UniAgent has been installed.

Table 5-6 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.

Operation	Description
Sorting hosts	In the table heading of the host list, click  next to UniAgent Heartbeat Time to sort hosts.
Deleting a host	<p>If a UniAgent is Abnormal, Not installed, or Installation failed, you can delete the corresponding host.</p> <p>Locate the target host and choose Delete in the Operation column.</p> <p>Precautions:</p> <ul style="list-style-type: none">• Hosts with UniAgent being installed, upgraded, or uninstalled cannot be deleted. Refresh the page and wait.• Running hosts with UniAgent installed cannot be deleted. Uninstall UniAgent first.• Hosts set as installation hosts or proxies cannot be deleted. Ensure that they are not installation hosts or proxies.
Configuring an installation host	<p>To set the name of an installation host, do as follows:</p> <p>Choose Configure Installation Host in the Operation column, and enter a desired name.</p>
Canceling an installation host	<p>To cancel an installation host, do as follows:</p> <p>Choose Cancel Installation Host in the Operation column to cancel an installation host.</p>
Changing the name of an installation host	<p>To change the name of a configured installation host, do as follows:</p> <p>Click the name of the installation host. In the dialog box that is displayed, rename it.</p>

5.2.2 (New) Installing UniAgents

UniAgents centrally manage the life cycle of collection plug-ins and deliver instructions (such as script delivery and execution). UniAgents do not collect metric data themselves. O&M data is collected by collection plug-ins. You can install collection plug-ins through the access center and create collection tasks to collect metric data.

AOM allows you to install UniAgents on ECSs or other servers in the current region.

- **Current region:** Install UniAgents on the hosts in the region where the AOM console is located.

Prerequisites

- You have determined the servers where UniAgent is to be installed and have obtained the accounts with the **root** permission and passwords for logging in to them.

- To install UniAgent through a jump server, ensure that the jump server (where UniAgent has been installed) can communicate with the servers where UniAgent is to be installed.
- Ensure that at least one access code is available. For details, see [14.2 Managing Access Codes](#).

Constraints

- For details about the Linux and Windows OSs supported by the UniAgent, see [Collection Management Restrictions](#).
- To switch from the old UniAgent page to the new one, choose **Settings > Collection Settings > UniAgents** in the navigation tree on the left and click **Try New Version** in the upper right corner. To go to the [old UniAgent](#) page, click **Back to Old Version** in the upper right corner of the **UniAgents** page.
- If the servers where UniAgent is to be installed contain CCE cluster-hosted servers, you are advised to install UniAgent on the [K8s Clusters](#) page.

Installation Methods

AOM allows you to install UniAgent on hosts. The following table lists the methods to install UniAgent.

Table 5-7 Installation methods

Method	Scenario
Install via Script (Recommended)	Suitable for initial installation and single-node installation scenarios. Use a remote login tool to log in to the host where UniAgent is to be installed and manually run the installation command. For details, see: <ul style="list-style-type: none">• Quickly Installing UniAgents Using Scripts (Current Region)
Install via Console	Applicable to the scenario where UniAgents are installed in batches on the AOM console. In the same VPC, use a jump server (an ECS where UniAgent has been installed) to install UniAgents on other ECSs in batches. For details, see Manually Installing UniAgents via Console (Current Region) . Ensure that a server with UniAgent installed is available. If UniAgent is installed for the first time, you need to install it using the script.

Quickly Installing UniAgents Using Scripts (Current Region)

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane on the left, choose **Settings > Global Settings**.
- Step 3** On the displayed page, choose **Collection Settings > UniAgents** and click **Try New Version** in the upper right corner of the page.

- Step 4** On the displayed page, click the **ECS** tab and click **Install UniAgent**.
- Step 5** On the displayed page, select **Install via Script (Recommended)**. (For servers on the **Other** tab page, UniAgents can be installed only by script. After you click **Install UniAgent** on this page, there is no need to select an installation scenario. The [Install UniAgent](#) page is directly displayed.)
- Step 6** On the **Install UniAgent** page, set parameters to install a UniAgent.

Table 5-8 Installation parameters

Parameter	Description	Example
Server Region	Select the region where the target cloud server is located. <ul style="list-style-type: none"> Current region: The network between AOM and the server in the current region is connected by default. 	Current region
Server Type	Options: <ul style="list-style-type: none"> ECSs: hosts managed by the ECS service. Other servers: other hosts. 	ECSs
Installation Mode	Option: CLI . You need to remotely log in to the server to run the installation command provided on the console.	CLI
OS	Options: Linux and Windows .	Linux
UniAgent Version	Select a UniAgent version. The latest version is selected by default.	Latest Version

Parameter	Description	Example
Copy and Run Installation Command	<p>Command for installing the UniAgent. Commands for Linux and Windows are different.</p> <ul style="list-style-type: none"> If the ECS OS is Linux: <ol style="list-style-type: none"> Click Copy to copy the installation command. <pre>set +o history; curl -k -X GET -m 20 --retry 1 --retry-delay 10 -o /tmp/install_uniagent https://aom-uniagent-*****.com/install_uniagent.sh;bash /tmp/install_uniagent -p ***** -d https://aom-uniagent-xxxxxx -m https://aom-mgr-lb. xxxxxx,https://xx.xx.xx.xx:xxxx -v 1.x.x -q false && /usr/local/uniagentd/xxxx -p icagent -s install -c "{\"PROJECT_ID\":\"xxxx\"}" -d https://icagent-xx-xx/ICAgent_linux -v x.x.x -m "{\"accessip\":\"x.x.x.x\", \"aomaksk\":\"*****\", \"tsaksk\":\"*****\", \"obsdomain\":\"x.x.x.x\", \"region\":\"xxx\"}" set -o history;</pre> Use a remote login tool to log in to the Linux server where the UniAgent is to be installed and run the copied installation command using an account with the root permission. <p>If neither the UniAgent nor the ICAgent is installed, run the preceding command to install both of them. If either the UniAgent or the ICAgent is installed, run the preceding command to install the uninstalled one.</p> If the ECS OS is Windows (only the UniAgent can be installed in this mode): <ol style="list-style-type: none"> Log in to the Windows server where the UniAgent is to be installed. Download the installation package <i>uniagentd-x.x.x.x-winxx.zip</i>. 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. Decompress the package, click uniagentd.msi, and specify path C:\uniagentd for installation. (Optional) Modify the C:\uniagentd\conf\uniagentd.conf file and enter the following configuration: 	Copy and run the installation command.

Parameter	Description	Example
	<p>master=https:// xxxxxx.xxxxxxxxxxxx,https:// xx.xx.xx.xx:xxxxx</p> <p>project_id=xxxxxxxxxxxxxx</p> <p>public_net=xxxx</p> <p>Click Copy to copy the preceding configuration.</p> <p>5. Run start.bat in the C:\uniagentd\bin directory as the administrator.</p>	

Step 7 Check the **UniAgent status** in the UniAgent list.

----End

Manually Installing UniAgents via Console (Current Region)

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane on the left, choose **Settings > Global Settings**.

Step 3 On the displayed page, choose **Collection Settings > UniAgents** and click **Try New Version** in the upper right corner of the page.

Step 4 On the displayed page, click the **ECS** tab and click **Install UniAgent**.

Step 5 Select **Install via Console**. (Only hosts on the **ECS** tab page support manual installation of UniAgents through the console.)

Step 6 On the **Install UniAgent** page, set parameters.



1. Configure basic information, select a server, and click **Next**.

Table 5-9 Installation parameters

Parameter	Description	Example
Server Region	The region where the target server is located can only be Current region . The network between AOM and the server in the current region is connected by default.	Current region
Server Type	Only ECSs are supported.	ECSs
Installation Mode	Options: CLI and GUI .	GUI
OS	Options: Linux and Windows . (This parameter is required only when Installation Mode is CLI .)	Linux

Parameter	Description	Example
UniAgent Version	Select a UniAgent version. The latest version is selected by default.	Latest Version



Parameter	Description	Example
Copy and run the installation command.	<p>Command for installing the UniAgent. Commands for Linux and Windows are different. (This parameter is required only when Installation Mode is CLI.) :</p> <ul style="list-style-type: none"> - If the ECS OS is Linux: <ol style="list-style-type: none"> 1. Click Copy to copy the installation command. <pre>set +o history; curl -k -X GET -m 20 --retry 1 --retry-delay 10 -o /tmp/install_uniagent https://aom-uniagent-*****.com/install_uniagent.sh;bash /tmp/install_uniagent -p ***** -d https://aom-uniagent-xxxxxx -m https://aom-mgr-lb. xxxxx,https://xx.xx.xx.xx:xxxx -v 1.x.x -q false && /usr/local/uniagentd/xxxx -p icagent -s install -c "{\"PROJECT_ID\":\"xxxx\"}" -d https://icagent-xx-xx/ICAgent_linux -v x.x.x -m "{\"accessip\":\"x.x.x.x\",\"aomask\":\"*****\",\"ltsask\":\"*****\",\"obsdomain\":\"x.x.x.x\",\"region\":\"xxx\"}" set -o history;</pre> 2. Use a remote login tool to log in to the Linux server where the UniAgent is to be installed and run the copied installation command using an account with the root permission. <p>If neither the UniAgent nor the ICAgent is installed, run the preceding command to install both of them. If either the UniAgent or the ICAgent is installed, run the preceding command to install the uninstalled one.</p> - If the ECS OS is Windows (only the UniAgent can be installed in this mode): <ol style="list-style-type: none"> 1. Log in to the Windows server where the UniAgent is to be installed. 2. Download the installation package <i>uniagentd-x.x.x.x-winxx.zip</i>. 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. 3. Decompress the package, click uniagentd.msi, and specify path C:\uniagentd for installation. 	Copy and run the installation command.

Parameter	Description	Example
	<p>4. (Optional) Modify the C:\uniagentd\conf\uniagentd.conf file and enter the following configuration:</p> <pre>master=https:// xxxxxx.xxxxxxxxxxxx,https:// xx.xx.xx.xx:xxxxx project_id=xxxxxxxxxxxxxx public_net=xxxxx</pre> <p>Click Copy to copy the preceding configuration.</p> <p>5. Run start.bat in the C:\uniagentd\bin directory as the administrator.</p>	
Select Server	<p>Click Add Server. In the dialog box that is displayed, select the cloud server where the UniAgent is to be installed. (This step is required only when Installation Mode is GUI.)</p> <ul style="list-style-type: none"> On the Add Server page, select one or more servers. Only servers running Linux can be selected. After selecting servers, perform the following operations if needed: <ul style="list-style-type: none"> To remove a selected server, click Remove. Filter servers by server ID or name. Click  and select or deselect columns to display. Click  to manually refresh the server list. 	Select servers.

- Check whether a transition host exists in the VPC to which the servers selected belong. (That is, check whether there is any server in the same VPC has been installed with the UniAgent. If yes, the server is automatically filtered out and used as a transition host.) Click **Next**. (This step is required only when **Installation Mode** is **GUI**.)

On the **Check Transition Host** page, perform the following operations if needed:

- If there are multiple servers with the UniAgent installed in the VPC, click **Change Transition Host** in the **Operation** column of the VPC and select a desired host as the transition host.
- If the UniAgent is not installed on any server in the VPC, click **Set Transition Host** in the **Operation** column of the VPC, copy the

- installation command, and manually run the installation command on a server to install the UniAgent and set the server to be a transition host.
- Filter the list by **VPC** or **Transition Host Set or Not**.
 - Click  and select or deselect columns to display.
 - Click  to manually refresh the transition host list.
3. Perform a connectivity test. (This step is required only when **Installation Mode** is **GUI**.)
 - a. Set **Account (with Root Permissions)**, **Password**, and **Port** for your server.
 - b. Click **Test** in the **Operation** column.

If multiple servers have the same account (with root permissions), password, and port number, select these servers, click **Set Login Account and Password** to set the account, password, and port number, and then click **Test**.
 4. After the connectivity test is successful, click **Finish**.

Step 7 Check the UniAgent status in the UniAgent list.

----End

Checking the UniAgent Status

On the **UniAgents** page, check the UniAgent status of the target host. For details, see [Table 5-10](#).




Table 5-10 UniAgent statuses

Status	Description
Running	The UniAgent is working.
Offline	The UniAgent is abnormal.
Installing	The UniAgent is being installed. The installation takes about 1 minute to complete.
Installation failed	The UniAgent fails to be installed. Uninstall the UniAgent and then reinstall it.
Not installed	The UniAgent has not been installed.

Other Operations

If needed, perform the following operations on the host where the UniAgent has been installed.

Table 5-11 Related operations

Operation	Description
Searching for a host	In the search box above the host list, search for a host by host ID, name, status, or 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.
Sorting hosts	In the table header of the host list, click  in each column to sort hosts.

5.2.3 Managing UniAgents

After UniAgents are installed, you can reinstall, upgrade, uninstall, or delete them when necessary.

Constraints

- If the host where a UniAgent is installed runs Windows, you need to manually reinstall or uninstall the UniAgent.
- UniAgents will not be automatically upgraded. Manually upgrade them if needed.
- During UniAgent management, if CCE cluster-hosted servers are selected or the UniAgent has already been installed on the **K8s Clusters** page, go to the [K8s Clusters](#) page to manage the UniAgent.

Reinstalling UniAgents

Reinstall UniAgents when they are offline or not installed or fail to be installed.

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane on the left, choose **Settings > Global Settings**.
- Step 3** In the navigation pane on the left, choose **Collection Settings > UniAgents**. The old VM access page is displayed. You can click **Try New Version** in the upper right corner to go to the new UniAgent management page.
- Step 4** Select one or more servers where UniAgents are to be reinstalled and perform the following operations:
- (Old) On the **VM Access** page, choose **UniAgent Batch Operation > Reinstall**. On the displayed page, [reinstall UniAgents](#) as prompted.
 - (New) On the **UniAgents** page, switch to the **ECS** or **Other** tab page and click **Reinstall**. On the displayed page, [reinstall UniAgents](#) as prompted. (If CCE cluster-hosted servers are selected or the UniAgent has already been installed

on the **K8s Clusters** page, go to the **K8s Clusters** page to reinstall the UniAgent.)

----End

Upgrading UniAgents

Upgrade your UniAgent to a more reliable, stable new version.

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane on the left, choose **Settings > Global Settings**.
- Step 3** In the navigation pane on the left, choose **Collection Settings > UniAgents**. The old VM access page is displayed. You can click **Try New Version** in the upper right corner to go to the new UniAgent management page.
- Step 4** Select one or more servers where UniAgents are to be upgraded and perform the following operations:
- (Old) On the **VM Access** page, choose **UniAgent Batch Operation > Upgrade**. On the displayed page, select the target version and click **OK**.
 - (New) On the **UniAgents** page, switch to the **ECS** or **Other** tab page and click **Upgrade**. On the displayed page, select the target version and click **OK**. (If CCE cluster-hosted servers are selected or the UniAgent has already been installed on the **K8s Clusters** page, go to the **K8s Clusters** page to upgrade the UniAgent.)

Wait for about 1 minute until the UniAgent upgrade is complete.

----End

Uninstalling UniAgents

Uninstall UniAgents when necessary.

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane on the left, choose **Settings > Global Settings**.
- Step 3** In the navigation pane on the left, choose **Collection Settings > UniAgents**. The old VM access page is displayed. You can click **Try New Version** in the upper right corner to go to the new UniAgent management page.
- Step 4** Select one or more servers where UniAgents are to be uninstalled and perform the following operations:
- (Old) On the **VM Access** page, choose **UniAgent Batch Operation > Uninstall**. On the displayed page, click **OK**.
 - (New) On the **UniAgents** page, switch to the **ECS** or **Other** tab page and click **Uninstall**. On the displayed page, click **OK**. (If CCE cluster-hosted servers are selected or the UniAgent has already been installed on the **K8s Clusters** page, go to the **K8s Clusters** page to uninstall the UniAgent.)

You can also log in to the target server as the **root** user and run the following command to uninstall the UniAgent:

```
bash /usr/local/uniagentd/bin/uninstall_uniagent.sh;
```

----End

Deleting UniAgents

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

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane on the left, choose **Settings > Global Settings**.
- Step 3** In the navigation pane on the left, choose **Collection Settings > UniAgents**. The old VM access page is displayed. You can click **Try New Version** in the upper right corner to go to the new UniAgent management page.
- Step 4** Select one or more servers where UniAgents are to be deleted and perform the following operations:
- (Old) On the **VM Access** page, choose **UniAgent Batch Operation > Delete**. On the displayed page, click **OK**.
 - (New) On the **UniAgents** page, switch to the **ECS** or **Other** tab page and click **Delete**. On the displayed page, click **OK**.

----End

5.2.4 Managing ICAgent Plug-ins for Hosts

AOM will support interconnection with other types of plug-ins. You can install, upgrade, uninstall, start, stop, and restart plug-ins in batches for hosts.

Currently, only ICAgents are supported. An ICAgent is a plug-in for collecting metrics and logs. ICAgent collects data at an interval of 1 minute. This interval cannot be changed.

Managing ICAgent Plug-ins in Batches

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane on the left, choose **Settings > Global Settings**.
- Step 3** In the navigation pane on the left, choose **Collection Settings > UniAgents**. The old VM access page is displayed. You can click **Try New Version** in the upper right corner to go to the new UniAgent management page.
- Step 4** Select one or more target servers and click **Plug-in Batch Operation**.
- Step 5** In the displayed dialog box, select an operation type, set the plug-in information, and click **OK**. (When selecting a CCE host, you are advised to go to the [K8s Clusters](#) page to operate the ICAgent.)

Table 5-12 Plug-in operation parameters

Parameter	Description
Operation	The following batch operations are supported: install, upgrade, uninstall, start, stop, and restart.
Plug-in	Select the plug-in to be operated. The ICAgent of the latest version can be installed.
AK/SK	<p>Access Key ID/Secret Access Key (AK/SK) to be entered based on your plug-in type and version.</p> <p>You need to enter an AK/SK only when installing the ICAgent of an earlier version. (If there is no text box for you to enter the AK/SK, the ICAgent of the new version has already been installed.)</p> <p>Procedure to obtain an AK/SK:</p> <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.

----End

5.2.5 Managing UniAgents and ICAgents in CCE Clusters

Kubernetes cluster management allows you to manage the lifecycle of UniAgents and ICAgents on hosts in CCE clusters under your account, for example, batch installation, upgrade, and uninstall.

Prerequisites

- You have CCE clusters and nodes under your account.

Viewing the CCE Clusters Connected to AOM

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane on the left, choose **Settings > Global Settings**.

Step 3 In the navigation pane, choose **Collection Settings > K8s Clusters**.

Step 4 On the **K8s Clusters** page, check the CCE clusters connected to AOM.

- Enter a CCE cluster name or ID in the search box to search for a cluster. Fuzzy match is supported.
- To collect container logs and output them to AOM 1.0, enable **Output to AOM 1.0**. (This function is supported only by ICAgent 5.12.133 or later.) You are advised to collect container logs and output them to LTS instead of AOM

1.0. For details, see "Ingesting CCE Application Logs to LTS" in the *Log Tank Service (LTS) User Guide*.

----End

Managing the UniAgents of CCE Clusters

You can install, upgrade, and uninstall UniAgent on hosts in CCE clusters connected to AOM.

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane on the left, choose **Settings > Global Settings**.
- Step 3** On the **Global Settings** page, choose **Collection Settings > K8s Clusters** in the navigation pane.
- Step 4** On the displayed page, select the target cluster from the cluster list and perform the operations listed in the following table if needed.

Table 5-13 Operations on UniAgents

Operation	Description
Install UniAgent	<ol style="list-style-type: none"> 1. Click Install UniAgent and select a UniAgent version to install. 2. Click OK. The UniAgent of the specified version and the ICAgent of the latest version will be installed on all hosts of the cluster.
Upgrade UniAgent	<ol style="list-style-type: none"> 1. Click Upgrade UniAgent and select a UniAgent version to upgrade. 2. Click OK. The UniAgents on all hosts of the cluster will be upgraded to the version you specified.
Uninstall UniAgent	<ol style="list-style-type: none"> 1. Click Uninstall UniAgent. On the displayed page, click OK. The UniAgents will be uninstalled from all hosts of the cluster. ICAgents will also be uninstalled if there are any. Only the UniAgents installed on the K8s Clusters page can be uninstalled here.

----End

Managing ICAgents in CCE Clusters

You can install, upgrade, and uninstall ICAgents on hosts in CCE clusters connected to AOM.

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane on the left, choose **Settings > Global Settings**.
- Step 3** On the **Global Settings** page, choose **Collection Settings > K8s Clusters** in the navigation pane.

- Step 4** On the **K8s Clusters** page, select the cluster where you want to perform ICAgent operations and click **Plug-in Operations**.

Plug-in operations are supported only when your UniAgent has been installed through the K8s Clusters page. If your UniAgent is not installed through the K8s Clusters page, click Install UniAgent to install the UniAgent on the hosts in your CCE cluster before performing plug-in operations.

- Step 5** In the displayed dialog box, select the operations listed in the following table if needed.

Table 5-14 Plug-in operations

Operation	Description
Install	<ol style="list-style-type: none">1. Select the Install operation and ICAgent plug-in. (Only the ICAgent can be installed.)2. Click OK. The ICAgent of the latest version will then be installed on all hosts that meet criteria.
Upgrade	<ol style="list-style-type: none">1. Select the Upgrade operation and ICAgent plug-in. (Only the ICAgent can be upgraded.)2. Click OK. The ICAgent on all hosts that meet criteria will then be upgraded to the latest version.
Uninstall	<ol style="list-style-type: none">1. Select the Uninstall operation and ICAgent plug-in. (Only the ICAgent can be uninstalled.)2. Click OK. The ICAgent will then be uninstalled from all hosts that meet criteria.

----End

5.2.6 Managing Host Groups

AOM is a unified platform for observability analysis. It does not provide log functions by itself. Instead, it integrates the host group management function of Log Tank Service (LTS). You can perform operations on the AOM 2.0 or LTS console.

To use the host group management function on the AOM 2.0 console, enable LTS first.

Table 5-15 Description

Function	Description	AOM 2.0 Console	LTS Console	References
Host group management	Host groups allow you to configure host log ingestion efficiently. You can add multiple hosts to a host group and associate the host group with log ingestion configurations. The ingestion configurations will then be applied to all the hosts in the host group.	<ol style="list-style-type: none">1. Log in to the AOM 2.0 console.2. In the navigation pane, choose Settings > Global Settings.3. On the displayed page, choose Collection Settings > Host Groups in the navigation pane.	<ol style="list-style-type: none">1. Log in to the LTS console.2. In the navigation pane, choose Host Management.	Section "Managing Host Groups" in the <i>Log Tank Service (LTS) User Guide</i>

- To use LTS functions on the AOM console, you need to obtain LTS permissions in advance.
- AOM 2.0 also provides a new version of host group management. After you switch to the new access center, the **new host group management** page will be displayed.

5.2.7 (New) Managing Host Groups

Host groups allow you to configure host data ingestion efficiently. You can add multiple hosts to a host group and associate the host group with ingestion configurations. The ingestion configurations will then be applied to all the hosts in the host group. When there is a new host, simply add it to a host group and the host will automatically inherit the log ingestion configurations associated with the host group.

You can create host groups of the IP address and custom identifier types.

- **Host Group Type** set to **IP**: Select hosts of the IP address type and add them to the host group.
- **Host Group Type** set to **Custom Identifier**: You need to create identifiers for each host group and host. Hosts with an identifier will automatically be included in the corresponding host group sharing that identifier.

Constraints


To use the new host group management function, switch to the new access center. To go to the [old host group management](#) page, choose **Access Center > Access Center** in the navigation pane on the left and then click **Back to Old Version** in the upper right corner.


Creating a Host Group (IP Address)

1. Log in to the AOM 2.0 console.
2. In the navigation pane, choose **Settings > Global Settings**.
3. On the **Global Settings** page, choose **Collection Settings > Host Groups** and click **Create Host Group** in the upper left corner.
4. On the displayed page, set the host group parameters.

Table 5-16 Parameters

Parameter	Description	Example
Host Group	Name of a host group. Enter 1 to 64 characters. Do not start with a period (.) or underscore (_) or end with a period. Only letters, digits, hyphens (-), underscores, and periods are allowed.	IPHostGroup1
Host Group Type	Type of the host group. Options: IP and Custom Identifier . In this example, select IP .	IP
Host Type	Host type. Default: Linux .	Linux
Remark	Host group remarks. Enter up to 1,024 characters.	-

5. In the host list, select one or more hosts to add to the group and click **OK**.
 - You can filter hosts by host name/ID or private IP address. You can also click  and enter multiple host IP addresses in the displayed search box to search.
 - If your desired hosts are not in the list, click **Install UniAgent**. On the displayed page, install UniAgents on the hosts as prompted. For details, see [5.2.2 \(New\) Installing UniAgents](#).
 - When the selected hosts do not have UniAgent installed but have an earlier version of ICAgent installed, an upgrade prompt appears. To enable automatic UniAgent installation later, click **Upgrade** to first upgrade ICAgent to the latest version.
 - If the selected hosts do not have both UniAgent and ICAgent installed (either UniAgent or ICAgent is in the **Not installed** state), click **OK**. A dialog box will pop up, indicating the missing UniAgent or ICAgent and the number of hosts without UniAgent or ICAgent installed.

- When selecting an ECS, click **OK** in the dialog box. The system will then issue a task for automatically installing either UniAgent or ICAgent. Otherwise, the host cannot be added to the host group. (Only ECSs running Linux support automatic UniAgent or ICAgent installation.)
 - When selecting a host of the **Other** type, manually install UniAgent and ICAgent first. Otherwise, the host cannot be added to the host group. For details, see [5.2.2 \(New\) Installing UniAgents](#).
- Click  in the upper right corner of the host list to manually refresh the list.

Creating a Host Group (Custom Identifier)

1. Log in to the AOM 2.0 console.
2. In the navigation pane on the left, choose **Settings > Global Settings**. On the displayed page, choose **Collection Settings > Host Groups** and click **Create Host Group** in the upper left corner.
3. On the displayed page, set the host group parameters.

Table 5-17 Parameters

Parameter	Description	Example
Host Group	Name of a host group. Enter 1 to 64 characters. Do not start with a period (.) or underscore (_) or end with a period. Only letters, digits, hyphens (-), underscores, and periods are allowed.	HostGroup
Host Group Type	Type of the host group. Options: IP and Custom Identifier . In this example, select Custom Identifier .	Custom Identifier
Host Type	Host type. Default: Linux .	Linux
Remark	Host group remarks. Enter up to 1,024 characters.	-
Custom Identifier	Click Add to add a custom identifier. Max.: 128 characters. Only letters, digits, underscores (_), and hyphens (-) are allowed. Up to 10 custom identifiers can be added.	aom

4. Click **OK**. After the host group is created, add hosts to it by referring to [5](#).
5. Log in to the host and perform the following operations as the **root** user to create the **custom_tag** file for storing host tags.
 - a. Run the **cd /opt/cloud** command.

- If the **/opt/cloud** directory already exists, navigate to it and run the **mkdir lts** command to create the **lts** directory in it.
- If the **/opt/cloud** directory does not exist, run the **mkdir /opt/cloud/** command to create it and enter it, and then run the **mkdir lts** command to create the **lts** directory.
- b. Run the **chmod 750 lts** command to modify the permission on the **lts** directory.
- c. Run the **touch custom_tag** command in the **lts** directory to create the **custom_tag** file.
- d. Run the **chmod 640 custom_tag;vi custom_tag** command to modify the **custom_tag** file permission and open the file.
- e. Press **i** to enter the insert mode, enter a custom identifier, press **Esc**, enter **:wq!**, save the modification and exit.
- f. Use either of the following methods to add a host to the custom identifier host group:



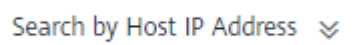


Table 5-18 Methods





Type	Method 1 (Recommended)	Method 2
Linux host	<ol style="list-style-type: none">1. View the host identifier in the custom_tag file under the /opt/cloud/lts directory of the host.2. On the host group configuration page, add the host identifier as the custom identifier for the host group to include the host in that group. For example, in the custom_tag file of the /opt/cloud/lts directory on the host, the identifier of the host is test1, and the custom identifier of the host group is set to test1. In this way, the host is added to the host group.	<ol style="list-style-type: none">1. Configure a custom identifier before creating a host group.2. Add the custom identifier to the custom_tag file in the /opt/cloud/lts directory of the host. The host can then be added to the specified host group. For example, if the custom identifier of the host group is set to test during host group creation, enter test in the custom_tag file to add the host to the host group. <p>If multiple custom identifiers are added, enter any custom identifier in the custom_tag file of the /opt/cloud/lts directory on the host to add the host to the host group.</p>




Other Operations

You can change a created host group, add hosts to or remove hosts from a host group, or associate a host group with log ingestion configurations.

Table 5-19 Operations on host groups

Operation	Procedure
Changing a host group	<ol style="list-style-type: none"> 1. Locate the target host group and click  in the Operation column. 2. On the displayed dialog box, modify the information such as the host group name, custom identifier, and remark. 3. Click OK.
Adding hosts to a host group	<ol style="list-style-type: none"> 1. Click  next to the target IP address host group. 2. Click Add Host. 3. In the displayed slide-out panel, all hosts that are not in the host group and run the selected OS type are displayed. Select the hosts to be added to the host group. For details, see 5. <ul style="list-style-type: none"> • You can filter hosts by host name/ID or private IP address. <p>You can also click  and enter multiple host IP addresses in the displayed search box to search.</p> <ul style="list-style-type: none"> • If your desired hosts are not in the list, click Install UniAgent. On the displayed page, install UniAgents on the hosts as prompted. For details, see 5.2.2 (New) Installing UniAgents. 4. Click OK. <p>This operation is not supported for hosts in a custom identifier host group. To add hosts to a custom identifier host group, refer to 5.</p>
Removing a host from a host group	<ol style="list-style-type: none"> 1. Click  next to the target IP address host group. 2. Locate the target host and click Remove in the Operation column. 3. In the displayed dialog box, click OK. <p>This operation is not supported for hosts in a custom identifier host group.</p>
Removing hosts in batches	<ol style="list-style-type: none"> 1. Locate the target host group and click  next to it. 2. Select the target hosts and click Remove above the list. 3. Click OK. <p>This operation is not supported for hosts in a custom identifier host group.</p>

Operation	Procedure
Viewing log ingestion rules	<ol style="list-style-type: none"> 1. Locate the target host group and click  next to it. 2. Click the Associated Ingestion Configurations tab to view the log ingestion rules configured for the host group. <p>For how to configure log ingestion rules for the host group, see 6.6 Managing Metric and Log Ingestion.</p>
Viewing metric access rules	<ol style="list-style-type: none"> 1. Locate the target host group and click  next to it. 2. Click the Metric Access Rules tab to view the metric access rules configured for the host group. <p>For how to configure metric ingestion rules for the host group, see 6.6 Managing Metric and Log Ingestion.</p>
Associating a host group with an ingestion configuration	<ol style="list-style-type: none"> 1. Locate the target host group and click  next to it. 2. Click the Associated Ingestion Configurations tab and then click Associate. 3. In the displayed slide-out panel, select the target ingestion configuration. 4. Click OK. The associated ingestion configuration is displayed in the list.
Disassociating a host group from an ingestion configuration	<ol style="list-style-type: none"> 1. Click the Associated Ingestion Configurations tab, locate the target ingestion configuration, and then click Disassociate in the Operation column. 2. Click OK.
Disassociating a host group from multiple ingestion configurations	<ol style="list-style-type: none"> 1. Click the Associated Ingestion Configurations tab, select target ingestion configurations, and then click Disassociate above the list. 2. Click OK.
Copying host group information	<p>Hover your cursor over a host group name to copy a host group ID.</p>
Deleting a host group	<ol style="list-style-type: none"> 1. Locate the target host group and click  in the Operation column. 2. In the displayed dialog box, click OK.

Operation	Procedure
Deleting host groups in batches	<ol style="list-style-type: none">1. Select multiple host groups to be deleted and click Delete above the list.2. In the displayed dialog box, click OK.
Managing tags	<p>Tag log groups as required.</p> <ol style="list-style-type: none">1. Locate the target host group and click  in the Operation column.2. On the displayed page, enter a tag key and value. <p>Precautions:</p> <ul style="list-style-type: none">• To add more tags, repeat the preceding step.• To delete a tag, locate the target host group and click  in the Operation column. On the displayed page, locate the target tag and click  in the Operation column.• A tag key can contain up to 128 characters, and a tag value can contain up to 255 characters.• A tag key must be unique.

5.2.8 Configuring a Proxy Area and Proxy

To enable network communication between multiple clouds, you need to configure an ECS as a proxy. The target host forwards O&M data to AOM through the proxy. A proxy area is used to manage proxies by category. It consists of multiple proxies.

Procedure

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane on the left, choose **Settings > Global Settings**.
- Step 3** In the navigation pane, choose **Collection Settings > Proxy Areas**.
- Step 4** Click **Add Proxy Area** and set proxy area parameters.

Table 5-20 Proxy area parameters

Parameter	Description	Example
Proxy Area Name	Name of a proxy area. Max.:	test

- Step 5** Click **OK** to add a proxy area.
- Step 6** Locate the new proxy area, click **Add Proxy**, and set proxy parameters.




Table 5-21 Proxy parameters

Parameter	Description	Example
Proxy Area	Select a proxy area that you have created.	test
Host	Select a host where the UniAgent has been installed. Hosts running Windows cannot be added as proxies.	-
Proxy IP Address	Set the IP address of the proxy.	192.168.0.0
Port	Set a port number and proxy protocol. <ul style="list-style-type: none">• The default port number is 32555. Range: 1,025 to 65,535.• The proxy protocol can only be SOCKS5.	32555

Step 7 Click **OK**.

After configuring the proxy area and proxy, perform the following operations if needed:

Table 5-22 Managing the proxy area and proxy

Operation	Description
Searching for a proxy area	Click  next to Add Proxy Area . Then, in the search box, enter a keyword to search for your target proxy area.
Modifying a proxy area	Hover the pointer over a proxy area and choose  > Edit . In the dialog box that is displayed, enter a new name, and click OK .
Deleting a proxy area	Hover the pointer over a proxy area and choose  > Delete . In the dialog box that is displayed, click Yes to delete the proxy area.
Checking a proxy	Click a proxy area to check the proxy in it.
Modifying a proxy IP address	Click Modify Proxy IP in the Operation column of the proxy. On the page that is displayed, modify the proxy IP address.
Deleting a proxy	Click Delete in the Operation column of the proxy. In the displayed dialog box, click Yes to delete the proxy.

----End

5.2.9 Viewing Operation Logs

AOM records operation logs of tasks such as installation/upgrade/uninstall/start/stop/restart related to UniAgent and other plug-ins. You can check the operation logs of related tasks.

Viewing UniAgent Operation Logs

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane on the left, choose **Settings > Global Settings**.
- Step 3** In the navigation tree on the left, choose **Collection Settings > Operation Logs**. The **UniAgent Logs** tab page is displayed by default.
- Step 4** Set criteria to search for historical tasks.
- Filter data by executor name.
 - Filter historical tasks by date. Options: **Last hour**, **Last 6 hours**, **Last day**, **Last 3 days**, and **Custom**. You can query historical tasks of half a year at most.
- Step 5** Click a task ID. On the task details page that is displayed, click **View Log** to view UniAgent operation logs.

----End

Viewing Plug-In Operation Logs




- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane on the left, choose **Settings > Global Settings**.
- Step 3** In the navigation tree on the left of the **Global Settings** page, choose **Collection Settings > Operation Logs**. On the displayed page, click the **Plug-in Logs** tab.
- Step 4** Set criteria to search for historical tasks.
- Filter data by executor name.
 - Filter historical tasks by date. Options: **Last hour**, **Last 6 hours**, **Last day**, **Last 3 days**, and **Custom**. You can query historical tasks of half a year at most.
- Step 5** Click a task ID. On the task details page that is displayed, click **View Log** in the **Operation** column to view plug-in operation logs.

----End

Other Operations

On the **Operation Logs** page, perform the operations listed in the following table if needed.

Table 5-23 Related operations

Operation	Description
Refreshing the task list	Click  in the upper right corner of the task list to refresh the list.
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 operation 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 task orders.

5.3 Connecting Cloud Services to AOM

AOM provides a unified entry for observability analysis of cloud services. Through the access center, you can connect cloud services to AOM. Cloud service metrics (such as CPU usage and memory usage) can then be reported to AOM.

To quickly connect cloud services to AOM, perform the following steps:

1. Create a Prometheus instance for cloud services. This instance is used to store collected data. For details, see [Creating a Prometheus Instance for Cloud Services](#).
2. Connect cloud services to AOM. For details, see [Connecting Cloud Services to AOM](#).
3. After cloud services are connected to AOM, their metrics can be reported to AOM. You can go to the [Metric Browsing](#) page to monitor metrics.

Constraints

- 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 **Prometheus Monitoring > Instances**. On the displayed page, click **Add Prometheus Instance**.

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

Table 5-24 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 dimmed and cannot be changed. • To use the enterprise project function, contact engineers.
Instance Type	Type of the Prometheus instance. Select Prometheus for Cloud Services .

Step 4 Click **OK**.

----End

Connecting Cloud Services to AOM

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane on the left, ingest cloud service metrics through either of the following entries:

- Entry 1:
 - a. Choose **Access Center > Access Center**. The **Access Center** page is displayed. (To switch from the new access center to the old one, click **Back to Old Version** in the upper right corner.)
 - b. Click the cloud service to be connected on the **Cloud Services** panel.
- Entry 2:
 - a. Choose **Prometheus Monitoring > Instances** and then click a target Prometheus instance.
 - b. In the **Unconnected Cloud Services** area, click the cloud service to be connected.

Step 3 In the displayed dialog box, set information about the cloud service.

Table 5-25 Connecting a cloud service

Parameter	Description
Select Prometheus Instance for Cloud Services	<p>Select the Prometheus instance for metric ingestion.</p> <ul style="list-style-type: none">Enterprise Project<ul style="list-style-type: none">Connecting cloud services on the Cloud Service Connection page of the Prometheus instance details page: By default, the enterprise project is the same as that selected during the creation of the Prometheus instance for cloud services. This option is grayed and cannot be changed.Connecting cloud services through the access center: Select a required enterprise project from the drop-down list. If the existing enterprise projects cannot meet your requirements, create one.Prometheus Instance for Cloud Services<ul style="list-style-type: none">Connecting cloud services on the Cloud Service Connection page of the Prometheus instance details page: By default, the value of this parameter is set to the target Prometheus instance selected in 1. This option is grayed and cannot be changed.Connecting cloud services through the access center: By default, the value of this parameter is the Prometheus instance for cloud services under your selected enterprise project. If there is no such a Prometheus instance, create one.
Connect Cloud Service Tags	<p>You can determine whether to add cloud service tags to metric dimensions. After this function is enabled, tags of cloud service resources will be added to metric dimensions. Tag changes will be synchronized every hour. If the existing tags cannot meet your requirements, click Go to Tag Management Service (TMS) to add tags.</p>

Step 4 Click **Connect Now**.

----End

Other Operations

You can also perform the operations listed in **Table 5-26** on the **Cloud Service Connection** page of the Prometheus instance for cloud services.

Table 5-26 Related operations

Operation	Description
Searching for cloud services	On the Cloud Service Connection page, enter a keyword in the search box to search for a cloud service.

Operation	Description
Disconnecting cloud services	On the Cloud Service Connection page, click a target cloud service. In the displayed dialog box, click Disconnect Cloud Service .
Checking or modifying tag configurations of connected cloud services	On the Cloud Service Connection page, click a cloud service under Connected Cloud Services to change cloud service tag settings. For details, see Table 5-25 .

5.4 Connecting Open-Source Monitoring Systems to AOM

AOM provides a unified entry for observability analysis of cloud services. Through the access center, you can create a common Prometheus instance to connect open-source monitoring systems to AOM.

Scenario

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 Common Prometheus Instance

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane on the left, create a common Prometheus instance through either of the following entries:

- Entry 1:
 - a. Choose **Access Center > Access Center**. The **Access Center** page is displayed. (To switch from the new access center to the old one, click **Back to Old Version** in the upper right corner.)
 - b. In the **Open-Source Monitoring** panel, click the **Common Prometheus instance** card.
- Entry 2:
Choose **Prometheus Monitoring > Instances** and click **Add Prometheus Instance**.

Step 3 In the displayed dialog box, set an instance name, enterprise project, and instance type.

Table 5-27 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 dimmed and cannot be changed.• To use the enterprise project function, contact engineers.
Instance Type	Type of the Prometheus instance. Select Common Prometheus Instance .

Step 4 Click **OK**.

----End

5.5 Connecting Custom Plug-ins to AOM

Create a plug-in, specify the metrics to be reported to AOM using a script, and create a collection task. Then the specified metrics can be reported to AOM for monitoring.

Prerequisites

- [The UniAgent has been installed](#) and is running.
- [A Prometheus instance for ECS has been created](#).

Creating a Custom Plug-in

You can create a plug-in using a custom script and create a collection task [during the connection of the custom plug-in](#) to report metrics to AOM.

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Access Center > Access Center** to go to the old access center. (The new access center does not support the connection of custom plug-ins. To switch from the new access center to the old one, click **Back to Old Version** in the upper right corner.)

Step 3 In the **Custom Prometheus Plug-in Access** panel, click **Custom Plug-in**.

Step 4 On the displayed page, set related parameters.

- Plug-in information

Table 5-28 Plug-in parameters

Parameter	Description
Plug-in Name	Name of a custom plug-in. Enter a maximum of 32 characters starting with a letter. Only letters, digits, and underscores (_) are allowed.
Plug-in Type	Type of a plug-in. The default value is Custom .
Description	Description of the plug-in to be created. Enter a maximum of 20,000 characters.

- Set Plug-in

Table 5-29 Plug-in configuration parameters


Parameter	Description
Plug-in Version	Version of the custom plug-in.
Plug-in Script	<p>Custom plug-in script. You need to specify the metrics to be reported to AOM in this script. The script type can be Linux or Windows.</p> <p>Linux: Shell or Python script.</p> <p>Example:</p> <pre>#!/bin/bash #Examples echo "metric_name{label_name=\"label_value\"} 100"</pre> <p>Windows: BAT script</p> <p>Example:</p> <pre>::Examples @echo off echo metric_name{label_name="label_value"} 100</pre>
Default Script Parameter	<p>Default parameters of the custom plug-in script. Set default parameters for script modeling. You can also leave them empty. Rules:</p> <p>$\\${Parameter}$: Enter a maximum of 64 characters starting with a letter. Only letters, digits, and underscores (_) are allowed. For example, $\\${a_b}$.</p> <p>You can combine parameters as required and separate them with spaces. Max.: 250 characters. For example, $\\${a} \\${b}$.</p>




Parameter	Description
Script Parameter	<p>Configure the attributes of the default parameters in the custom plug-in script. You can configure the following information as required:</p> <ul style="list-style-type: none">– Mandatory: If this option is enabled, the parameter value in the plug-in debugging area is mandatory. If this option is disabled, the parameter value in the plug-in debugging area is optional.– Parameter: name of a script parameter. The system automatically identifies the script parameter name based on Default Script Parameter you have already configured. The parameter here is grayed and cannot be configured.– Default Value: default value of the script parameter.– Description: description of the parameter. <p>When you configure a collection task for the custom plug-in, script parameters are displayed based on the script parameter attributes configured here. You can configure collection based on the script parameter attributes.</p>

Step 5 Click **Save**.

After a plug-in is created, you can modify it, create a version for it, or delete it.

Table 5-30 Related operations

Operation	Description
Checking the plug-in status	<p>Locate the target plug-in, hover the mouse pointer over the plug-in, and choose  > Version. On the page that is displayed, check the plug-in status.</p> <ul style="list-style-type: none">• Unreleased: When you create a plug-in or create a plug-in version, the plug-in status is Unreleased. You can click the version number to edit the plug-in.• Released: After you click Release in the Operation column, the plug-in status changes to Released. You can click the version number to view the plug-in details.

Operation	Description
Creating a version	Locate the target plug-in, hover the mouse pointer over the plug-in, and choose  > Version . Click Create Version . On the displayed page, set the plug-in information. Precautions: <ul style="list-style-type: none">• A maximum of five versions can be created for a plug-in.• If there is only one plug-in version, only Copy is available in the Operation column. If there is more than one plug-in, both Copy and Delete are available in the Operation column. You can click Delete to delete a plug-in version.
Modifying a plug-in	Locate the target plug-in, hover the mouse pointer over the plug-in, and choose  > Modify . On the displayed page, modify the plug-in information.
Deleting a plug-in	Locate the target plug-in, hover the mouse pointer over the plug-in, and choose  > Delete . On the displayed page, click Yes to delete the plug-in. If a collection task has been configured for a plug-in, deleting the plug-in will also delete the collection task.

----End

Connecting Custom Plug-ins to AOM

Step 1 Log in to the AOM 2.0 console.


Step 2 In the navigation pane, choose **Access Center** > **Access Center** to go to the old access center. (The new access center does not support the connection of custom plug-ins. To switch from the new access center to the old one, click **Back to Old Version** in the upper right corner.)

Step 3 In the **Custom Prometheus Plug-in Access** panel, click the created custom plug-in.

Step 4 On the displayed page, set parameters by referring to the following table.

Table 5-31 Parameters for configuring a collection task

Operation	Parameter	Description
Select Instance	Prometheus Instance	Select a Prometheus instance for ECS to store collected data. A collection task is associated with the Prometheus instance to mark and classify collected data. If no Prometheus instance is available, create one .




Operation	Parameter	Description
Set Plug-in	OS	Operating system of the host. Options: Linux and Windows . For a custom plug-in, the OS is automatically selected.
	Collection Plug-in	(Default) Created custom plug-in.
	Plug-in Version	Select a plug-in version. Plug-in versions that have not been released are dimmed and cannot be selected.
Set Collection Task	Collection Task Name	Name of a collection task. Enter 1 to 50 characters starting with a letter. Only letters, digits, underscores (_), and hyphens (-) are allowed.
	Host	<p>Click Add Host. On the Add Host page, select the host for configuring the collection task and installing Exporter.</p> <ul style="list-style-type: none"> Search for and select a host by the host name, IP address, or Agent status. You can click  in the upper right corner to deselect the selected host. Ensure that the UniAgent of the selected host is running. Otherwise, no data can be collected.
	Plug-in Collection Parameters	Set parameters for the custom plug-in script. They come from the default script parameters you define when creating a custom plug-in script .
	Advanced Settings	<p>Configure the following parameters:</p> <ul style="list-style-type: none"> Collection Period (s): O&M data collection period, in seconds. Options: 10s, 30s, and 60s (default). Timeout Period (s): the maximum time allowed for executing a collection task, in seconds. Options: 10s, 30s, and 60s (default). The timeout period cannot exceed the collection period. Executor: user who executes the collection task, that is, the user of the selected host. Default: root. Enter a username. Recommended: root.

Step 5 Click **Create**.

Step 6 The connected plug-in will be displayed on the **Collection Tasks** tab page of the plug-in card. Click the plug-in card. On the **Collection Tasks** tab page, click the target collection task to view its details.

You can also perform the operations listed in the following table on the collection task.

Table 5-32 Related operations

Operation	Description
Checking a collection task	Click a collection task to go to its details page.
Starting or stopping a collection task	Click the button in the Start/Stop column of a collection task to start or stop it.
Searching for a collection task	Set filter criteria or enter keywords to search for a collection task.
Changing target hosts	Click  in the Operation column of the target collection task. On the displayed page, change target hosts. You can only change the target hosts for the collection tasks created using custom plug-ins.
Sorting collection tasks	Click  in the Timeout Period or Collection Period column to sort collection tasks.
Copying a collection task	Click  in the Operation column of a collection task. On the displayed page, modify parameters as required.
Modifying a collection task	Choose ... > Modify in the Operation column of the target collection task. On the displayed page, modify parameters as required.
Deleting a collection task	Locate a collection task and choose ... > Delete in the Operation column. On the displayed page, confirm the deletion.

----End

5.6 Managing Log Ingestion

AOM is a unified platform for observability analysis of cloud services. It does not provide log functions by itself. Instead, it integrates the access management function of Log Tank Service (LTS). You can perform operations on the AOM 2.0 or LTS console.

Constraints

- To use the access management function on the AOM 2.0 console, enable LTS first.

- To use LTS functions on the AOM console, obtain the LTS permissions in advance. For details, see section "Permissions" in the *Log Tank Service (LTS) User Guide*.

Table 5-33 Function description

Function	Description	AOM 2.0 Console	LTS Console	References
Access management	Logs can be ingested through ICAgents, cloud services, APIs, and SDKs. After logs are ingested, they are displayed in a simple and orderly manner on the console and can be queried easily.	<ol style="list-style-type: none">1. Log in to the AOM 2.0 console.2. In the navigation pane on the left, choose Access Center > Access Management.	<ol style="list-style-type: none">1. Log in to the LTS console.2. In the navigation pane on the left, choose Log Ingestion > Ingestion Management.	Section "Log Ingestion" in the <i>Log Tank Service (LTS) User Guide</i>

6 (New) Connecting to AOM

6.1 AOM Access Overview

AOM is a unified platform for observability analysis of cloud services. You can quickly ingest AOM metrics and LTS logs through the new access center. After the ingestion is complete, you can view the resource or application running status, metric usage, and LTS logs on the [Metric Browsing](#) and [Log Management](#) pages.

Constraints

If the old access center is displayed, click **Try New Version** in the upper right corner.

Ingesting Metrics/Logs to AOM

Step 1 Log in to the AOM 2.0 console.

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

Step 3 Click **Try New Version** in the upper right corner of the page. The new access center is displayed.

The **Recommended** area displays six popular cards. They will be automatically updated to the six cards you have recently used.

Step 4 Set criteria to quickly query the metrics or logs to be ingested.

- **Filter:** Filter content by data source or type.
- **Attribute filtering:** Click the search box and search for content by keyword, data source, or type. You can also enter a keyword to search.

Table 6-1 Access overview

Type	Monitored Object (Card)	Data Source	Access Mode
Self-built middleware	<ul style="list-style-type: none">• MySQL• Redis• Kafka• Nginx• MongoDB• Consul• HAProxy• PostgreSQL• Elasticsearch• RabbitMQ	Metrics	6.3 Connecting Self-Built Middleware to AOM
Running environments	<ul style="list-style-type: none">• Elastic Cloud Server (ECS)• Cloud Container Engine (CCE)	Logs/ Metrics	6.4 Connecting Running Environments to AOM
APIs/ protocols...	<ul style="list-style-type: none">• AOM APIs• LTS APIs• Custom Prometheus Metrics	Logs/ Metrics	6.5 Ingesting Data to AOM Using Open-Source APIs and Protocols

Step 5 Hover the pointer over the card and click the blue text to check LTS documents or ingest metrics.

- Click **Ingest Metric (AOM)** to quickly ingest metrics.
- Click **Ingest Log (LTS)** on **Ingest Log (LTS) Details** to quickly ingest logs or click **Details** to check documents related to log ingestion.

----End

6.2 Managing Collector Base UniAgent

6.2.1 Installing UniAgents

UniAgents centrally manage the life cycle of collection plug-ins and deliver instructions (such as script delivery and execution). UniAgents do not collect metric data themselves. O&M data is collected by collection plug-ins. You can install collection plug-ins through the access center and create collection tasks to collect metric data.

AOM allows you to install UniAgents on cloud servers in a VPC.

Prerequisite

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

Constraints

- For details about the Linux and Windows OSs supported by the UniAgent, see [Collection Management Restrictions](#).
- To switch from the new UniAgent page to the old one, choose **Settings > Global Settings > Collection Settings > UniAgents** in the navigation tree on the left and click **Back to Old Version** in the upper right corner. To go to the [new UniAgent](#) page, click **Try New Version** in the upper right corner of the **UniAgents** page.

Installation Methods

Install a UniAgent on a host manually or remotely. Select an installation mode based on site requirements.

Table 6-2 Installation methods

Method	Scenario
Manual UniAgent Installation	Suitable for initial installation and single-node installation scenarios. Log in to the host where the UniAgent is to be installed and manually run the installation command. When installing a UniAgent for the first time, you must install it manually.
Remote UniAgent Installation	Suitable for the scenario where UniAgents are installed in batches. Set a host where a UniAgent has been installed to be an installation host , and use it to install UniAgents on other hosts. (Enter the information about the hosts where UniAgents are to be installed on the installation page.)


Manual UniAgent 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 on the left, choose **Settings > Global Settings**.
- Step 3** In the navigation pane, choose **Collection Settings > UniAgents**. Click **Install UniAgent** in the upper right corner and select **Manual**. (When you install the UniAgent for the first time, the **Manual** page is displayed by default.)
- Step 4** On the **Install UniAgent** page, set parameters to install a UniAgent.

Table 6-3 Parameters for manual installation

Parameter	Description	Example
UniAgent Version	Version of a UniAgent. This parameter is mandatory.	1.1.8
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 install the UniAgent on a host through the proxy.	Direct access
Proxy Area	<p>Manages proxies by category. When Access Mode is set to Proxy access, you need to select or add a proxy area.</p> <p>A proxy area must contain an available proxy. This proxy must be a cloud host where a UniAgent has been installed.</p>	Select a proxy area.

Parameter	Description	Example
Installation Command	<p>Command for installing the UniAgent. Commands for Linux and Windows are different.</p> <p>Linux</p> <ol style="list-style-type: none"> Click  to copy the installation command. <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 -p xxxxxx -d https://aom-uniagent-xxxxxx -m https://aom.mgr-lb. xxxxxx,https://xx.xx.xx.xx:xxxx -v 1.x.x -q false set -o history;</pre> <p>Windows</p> <ol style="list-style-type: none"> Copy the download address (https://aom-uniagent-{region_name}.obs.{region_name}.{site domain name suffix}/+uniagentd-{version}-win32.zip) to the browser to download the installation package. <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. Enter the following configuration (obtained from the installation page) to the C:\uniagentd\conf\uniagentd.conf file: <pre>master=https://aom-mgr-lb.xxxxxxxxxxxx,https:// xx.xx.xx.xx:xxxxx project_id=xxxxxxxxxxxxxxxxx public_net=xxxx</pre> Run start.bat in the C:\uniagentd\bin directory as the administrator. 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.
- Linux host: Use a remote login tool to log in to the target host and run the installation command copied in the [previous step](#) as the **root** user to install the UniAgent.
 - Windows host: Log in to the target host, and download the installation package based on the installation command in the [previous step](#) to install the UniAgent.

Step 6 Check whether the UniAgent is displayed in the UniAgent list.

----End

Remote UniAgent Installation

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane on the left, choose **Settings > Global Settings**.
- Step 3** In the navigation pane on the left, choose **Collection Settings > UniAgents**. Click **Install UniAgent** in the upper right corner.
- Step 4** On the **Install UniAgent** page, choose **Remote** and set parameters to install a UniAgent. (When you install the UniAgent for the first time, the **Manual** page is displayed by default. **Remote** is not available. Remote installation can be performed only when you have an installation host.)

Table 6-4 Parameters for remotely installing a UniAgent

Parameter	Description	Example
UniAgent Version	Version of a UniAgent. This parameter is mandatory.	1.1.8
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	Manages proxies by category. When Access Mode is set to Proxy access , you need to select or add a proxy area. A proxy area must contain an available proxy. This proxy must be a cloud host where a UniAgent has been installed.	Select a proxy area.

Parameter	Description	Example
Installation Host	<p>An installation host is used to execute commands for remote installation. This parameter is mandatory. To install the UniAgent remotely, ensure that the installation host does not run Windows.</p> <p>If no installation host has been configured, perform the following steps:</p> <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.	Select an installation host.

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>Add a maximum of 100 hosts:</p> <ul style="list-style-type: none"> • Host IP Address: IP address of a host. • OS: operating system of the host, which can be Linux or Windows. To install the UniAgent remotely, ensure that the host does not run Windows. • 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. • Login Port: port for accessing the host. • Authentication Mode: Currently, only password-based authentication is supported. • Password: password for logging in to the host. • Connectivity Test Result: shows whether the network between the installation host and the host where the UniAgent is to be installed is normal. <p>After entering the host information, you can delete, copy, or test the connectivity of hosts in the Operation column.</p> <p>The connectivity test checks the network between the installation host and the host where the UniAgent is to be installed. The test result is displayed in the Connectivity Test Result column. (Windows hosts do not support connectivity tests.)</p>	Enter the information about the hosts where UniAgents are to be installed.
Install ICAgent	<p>The ICAgent is a plug-in for collecting metrics and logs. The Install ICAgent option is enabled by default. It is optional. To install the ICAgent remotely, ensure that the host does not run Windows.</p>	-

Step 5 Click **Install**. After the installation is complete, you can [view the UniAgent status](#) in the UniAgent list.

----End

Checking the UniAgent Status

On the **VM Access** page, check the UniAgent status of the target host. For details, see [Table 6-5](#).




Table 6-5 UniAgent statuses


Status	Description
Running	The UniAgent is working.
Offline	The UniAgent is abnormal.
Installing	The UniAgent is being installed. The installation takes about 1 minute to complete.
Installation failed	The UniAgent fails to be installed. Uninstall the UniAgent and then reinstall it.
Not installed	The UniAgent has not been installed.

Other Operations

If needed, perform the following operations on the host where the UniAgent has been installed.

Table 6-6 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.

Operation	Description
Sorting hosts	In the table heading of the host list, click  next to UniAgent Heartbeat Time to sort hosts.
Deleting a host	<p>If a UniAgent is Abnormal, Not installed, or Installation failed, you can delete the corresponding host.</p> <p>Locate the target host and choose Delete in the Operation column.</p> <p>Precautions:</p> <ul style="list-style-type: none">• Hosts with UniAgent being installed, upgraded, or uninstalled cannot be deleted. Refresh the page and wait.• Running hosts with UniAgent installed cannot be deleted. Uninstall UniAgent first.• Hosts set as installation hosts or proxies cannot be deleted. Ensure that they are not installation hosts or proxies.
Configuring an installation host	<p>To set the name of an installation host, do as follows:</p> <p>Choose Configure Installation Host in the Operation column, and enter a desired name.</p>
Canceling an installation host	<p>To cancel an installation host, do as follows:</p> <p>Choose Cancel Installation Host in the Operation column to cancel an installation host.</p>
Changing the name of an installation host	<p>To change the name of a configured installation host, do as follows:</p> <p>Click the name of the installation host. In the dialog box that is displayed, rename it.</p>

6.2.2 (New) Installing UniAgents

UniAgents centrally manage the life cycle of collection plug-ins and deliver instructions (such as script delivery and execution). UniAgents do not collect metric data themselves. O&M data is collected by collection plug-ins. You can install collection plug-ins through the access center and create collection tasks to collect metric data.

AOM allows you to install UniAgents on ECSs or other servers in the current region.

- **Current region:** Install UniAgents on the hosts in the region where the AOM console is located.

Prerequisites

- You have determined the servers where UniAgent is to be installed and have obtained the accounts with the **root** permission and passwords for logging in to them.

- To install UniAgent through a jump server, ensure that the jump server (where UniAgent has been installed) can communicate with the servers where UniAgent is to be installed.
- Ensure that at least one access code is available. For details, see [14.2 Managing Access Codes](#).

Constraints

- For details about the Linux and Windows OSs supported by the UniAgent, see [Collection Management Restrictions](#).
- To switch from the old UniAgent page to the new one, choose **Settings > Collection Settings > UniAgents** in the navigation tree on the left and click **Try New Version** in the upper right corner. To go to the [old UniAgent](#) page, click **Back to Old Version** in the upper right corner of the **UniAgents** page.
- If the servers where UniAgent is to be installed contain CCE cluster-hosted servers, you are advised to install UniAgent on the [K8s Clusters](#) page.

Installation Methods

AOM allows you to install UniAgent on hosts. The following table lists the methods to install UniAgent.

Table 6-7 Installation methods

Method	Scenario
Install via Script (Recommended)	Suitable for initial installation and single-node installation scenarios. Use a remote login tool to log in to the host where UniAgent is to be installed and manually run the installation command. For details, see: <ul style="list-style-type: none">• Quickly Installing UniAgents Using Scripts (Current Region)
Install via Console	Applicable to the scenario where UniAgents are installed in batches on the AOM console. In the same VPC, use a jump server (an ECS where UniAgent has been installed) to install UniAgents on other ECSs in batches. For details, see Manually Installing UniAgents via Console (Current Region) . Ensure that a server with UniAgent installed is available. If UniAgent is installed for the first time, you need to install it using the script.

Quickly Installing UniAgents Using Scripts (Current Region)

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane on the left, choose **Settings > Global Settings**.
- Step 3** On the displayed page, choose **Collection Settings > UniAgents** and click **Try New Version** in the upper right corner of the page.

- Step 4** On the displayed page, click the **ECS** tab and click **Install UniAgent**.
- Step 5** On the displayed page, select **Install via Script (Recommended)**. (For servers on the **Other** tab page, UniAgents can be installed only by script. After you click **Install UniAgent** on this page, there is no need to select an installation scenario. The **Install UniAgent** page is directly displayed.)
- Step 6** On the **Install UniAgent** page, set parameters to install a UniAgent.

Table 6-8 Installation parameters

Parameter	Description	Example
Server Region	Select the region where the target cloud server is located. <ul style="list-style-type: none"> Current region: The network between AOM and the server in the current region is connected by default. 	Current region
Server Type	Options: <ul style="list-style-type: none"> ECSs: hosts managed by the ECS service. Other servers: other hosts. 	ECSs
Installation Mode	Option: CLI . You need to remotely log in to the server to run the installation command provided on the console.	CLI
OS	Options: Linux and Windows .	Linux
UniAgent Version	Select a UniAgent version. The latest version is selected by default.	Latest Version

Parameter	Description	Example
Copy and Run Installation Command	<p>Command for installing the UniAgent. Commands for Linux and Windows are different.</p> <ul style="list-style-type: none"> If the ECS OS is Linux: <ol style="list-style-type: none"> Click Copy to copy the installation command. <pre>set +o history; curl -k -X GET -m 20 --retry 1 --retry-delay 10 -o /tmp/install_uniagent https://aom-uniagent-*****.com/install_uniagent.sh;bash /tmp/install_uniagent -p ***** -d https://aom-uniagent-xxxxxx -m https://aom-mgr-lb. xxxxxx,https://xx.xx.xx.xx:xxxx -v 1.x.x -q false && /usr/local/uniagentd/xxxx -p icagent -s install -c "{\"PROJECT_ID\":\"xxxx\"}" -d https://icagent-xx-xx/ICAgent_linux -v x.x.x -m "{\"accessip\":\"x.x.x.x\", \"aomaks\":\"*****\", \"tsaks\":\"*****\", \"obsdomain\":\"x.x.x.x\", \"region\":\"xxx\"}" set -o history;</pre> Use a remote login tool to log in to the Linux server where the UniAgent is to be installed and run the copied installation command using an account with the root permission. <p>If neither the UniAgent nor the ICAgent is installed, run the preceding command to install both of them. If either the UniAgent or the ICAgent is installed, run the preceding command to install the uninstalled one.</p> If the ECS OS is Windows (only the UniAgent can be installed in this mode): <ol style="list-style-type: none"> Log in to the Windows server where the UniAgent is to be installed. Download the installation package <i>uniagentd-x.x.x.x-winxx.zip</i>. 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. Decompress the package, click uniagentd.msi, and specify path C:\uniagentd for installation. (Optional) Modify the C:\uniagentd\conf\uniagentd.conf file and enter the following configuration: 	Copy and run the installation command.

Parameter	Description	Example
	<p>master=https:// xxxxxx.xxxxxxxxxxxx,https:// xx.xx.xx.xx:xxxxx</p> <p>project_id=xxxxxxxxxxxxxx</p> <p>public_net=xxxx</p> <p>Click Copy to copy the preceding configuration.</p> <p>5. Run start.bat in the C:\uniagentd\bin directory as the administrator.</p>	

Step 7 Check the **UniAgent status** in the UniAgent list.

----End

Manually Installing UniAgents via Console (Current Region)

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane on the left, choose **Settings > Global Settings**.

Step 3 On the displayed page, choose **Collection Settings > UniAgents** and click **Try New Version** in the upper right corner of the page.

Step 4 On the displayed page, click the **ECS** tab and click **Install UniAgent**.

Step 5 Select **Install via Console**. (Only hosts on the **ECS** tab page support manual installation of UniAgents through the console.)

Step 6 On the **Install UniAgent** page, set parameters.



1. Configure basic information, select a server, and click **Next**.

Table 6-9 Installation parameters

Parameter	Description	Example
Server Region	The region where the target server is located can only be Current region . The network between AOM and the server in the current region is connected by default.	Current region
Server Type	Only ECSs are supported.	ECSs
Installation Mode	Options: CLI and GUI .	GUI
OS	Options: Linux and Windows . (This parameter is required only when Installation Mode is CLI .)	Linux

Parameter	Description	Example
UniAgent Version	Select a UniAgent version. The latest version is selected by default.	Latest Version



Parameter	Description	Example
Copy and run the installation command.	<p>Command for installing the UniAgent. Commands for Linux and Windows are different. (This parameter is required only when Installation Mode is CLI.) :</p> <ul style="list-style-type: none"> - If the ECS OS is Linux: <ol style="list-style-type: none"> 1. Click Copy to copy the installation command. <pre>set +o history; curl -k -X GET -m 20 --retry 1 --retry-delay 10 -o /tmp/install_uniagent https://aom-uniagent-*****.com/install_uniagent.sh;bash /tmp/install_uniagent -p ***** -d https://aom-uniagent-xxxxxx -m https://aom-mgr-lb. xxxxx,https://xx.xx.xx.xx:xxxx -v 1.x.x -q false && /usr/local/uniagentd/xxxx -p icagent -s install -c "{\"PROJECT_ID\":\"xxxx\"}" -d https://icagent-xx-xx/ICAgent_linux -v x.x.x -m "{\"accessip\":\"x.x.x.x\",\"aomask\":\"*****\",\"ltsask\":\"*****\",\"obsdomain\":\"x.x.x.x\",\"region\":\"xxx\"}" set -o history;</pre> 2. Use a remote login tool to log in to the Linux server where the UniAgent is to be installed and run the copied installation command using an account with the root permission. <p>If neither the UniAgent nor the ICAgent is installed, run the preceding command to install both of them. If either the UniAgent or the ICAgent is installed, run the preceding command to install the uninstalled one.</p> - If the ECS OS is Windows (only the UniAgent can be installed in this mode): <ol style="list-style-type: none"> 1. Log in to the Windows server where the UniAgent is to be installed. 2. Download the installation package <i>uniagentd-x.x.x.x-winxx.zip</i>. 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. 3. Decompress the package, click uniagentd.msi, and specify path C:\uniagentd for installation. 	Copy and run the installation command.

Parameter	Description	Example
	<p>4. (Optional) Modify the C:\uniagentd\conf\uniagentd.conf file and enter the following configuration:</p> <pre>master=https:// xxxxxx.xxxxxxxxxxxx,https:// xx.xx.xx.xx:xxxxx project_id=xxxxxxxxxxxxxx public_net=xxxxx</pre> <p>Click Copy to copy the preceding configuration.</p> <p>5. Run start.bat in the C:\uniagentd\bin directory as the administrator.</p>	
Select Server	<p>Click Add Server. In the dialog box that is displayed, select the cloud server where the UniAgent is to be installed. (This step is required only when Installation Mode is GUI.)</p> <ul style="list-style-type: none"> On the Add Server page, select one or more servers. Only servers running Linux can be selected. After selecting servers, perform the following operations if needed: <ul style="list-style-type: none"> To remove a selected server, click Remove. Filter servers by server ID or name. Click  and select or deselect columns to display. Click  to manually refresh the server list. 	Select servers.

- Check whether a transition host exists in the VPC to which the servers selected belong. (That is, check whether there is any server in the same VPC has been installed with the UniAgent. If yes, the server is automatically filtered out and used as a transition host.) Click **Next**. (This step is required only when **Installation Mode** is **GUI**.)

On the **Check Transition Host** page, perform the following operations if needed:

- If there are multiple servers with the UniAgent installed in the VPC, click **Change Transition Host** in the **Operation** column of the VPC and select a desired host as the transition host.
- If the UniAgent is not installed on any server in the VPC, click **Set Transition Host** in the **Operation** column of the VPC, copy the

- installation command, and manually run the installation command on a server to install the UniAgent and set the server to be a transition host.
- Filter the list by **VPC** or **Transition Host Set or Not**.
 - Click  and select or deselect columns to display.
 - Click  to manually refresh the transition host list.
3. Perform a connectivity test. (This step is required only when **Installation Mode** is **GUI**.)
 - a. Set **Account (with Root Permissions)**, **Password**, and **Port** for your server.
 - b. Click **Test** in the **Operation** column.

If multiple servers have the same account (with root permissions), password, and port number, select these servers, click **Set Login Account and Password** to set the account, password, and port number, and then click **Test**.
 4. After the connectivity test is successful, click **Finish**.

Step 7 Check the UniAgent status in the UniAgent list.

----End

Checking the UniAgent Status

On the **UniAgents** page, check the UniAgent status of the target host. For details, see [Table 6-10](#).




Table 6-10 UniAgent statuses

Status	Description
Running	The UniAgent is working.
Offline	The UniAgent is abnormal.
Installing	The UniAgent is being installed. The installation takes about 1 minute to complete.
Installation failed	The UniAgent fails to be installed. Uninstall the UniAgent and then reinstall it.
Not installed	The UniAgent has not been installed.

Other Operations

If needed, perform the following operations on the host where the UniAgent has been installed.

Table 6-11 Related operations

Operation	Description
Searching for a host	In the search box above the host list, search for a host by host ID, name, status, or 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.
Sorting hosts	In the table header of the host list, click  in each column to sort hosts.

6.2.3 Managing UniAgents

After UniAgents are installed, you can reinstall, upgrade, uninstall, or delete them when necessary.

Constraints

- If the host where a UniAgent is installed runs Windows, you need to manually reinstall or uninstall the UniAgent.
- UniAgents will not be automatically upgraded. Manually upgrade them if needed.
- During UniAgent management, if CCE cluster-hosted servers are selected or the UniAgent has already been installed on the **K8s Clusters** page, go to the [K8s Clusters](#) page to manage the UniAgent.

Reinstalling UniAgents

Reinstall UniAgents when they are offline or not installed or fail to be installed.

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane on the left, choose **Settings > Global Settings**.
- Step 3** In the navigation pane on the left, choose **Collection Settings > UniAgents**. The old VM access page is displayed. You can click **Try New Version** in the upper right corner to go to the new UniAgent management page.
- Step 4** Select one or more servers where UniAgents are to be reinstalled and perform the following operations:
- (Old) On the **VM Access** page, choose **UniAgent Batch Operation > Reinstall**. On the displayed page, [reinstall UniAgents](#) as prompted.
 - (New) On the **UniAgents** page, switch to the **ECS** or **Other** tab page and click **Reinstall**. On the displayed page, [reinstall UniAgents](#) as prompted. (If CCE cluster-hosted servers are selected or the UniAgent has already been installed

on the **K8s Clusters** page, go to the **K8s Clusters** page to reinstall the UniAgent.)

----End

Upgrading UniAgents

Upgrade your UniAgent to a more reliable, stable new version.

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane on the left, choose **Settings > Global Settings**.
- Step 3** In the navigation pane on the left, choose **Collection Settings > UniAgents**. The old VM access page is displayed. You can click **Try New Version** in the upper right corner to go to the new UniAgent management page.
- Step 4** Select one or more servers where UniAgents are to be upgraded and perform the following operations:
- (Old) On the **VM Access** page, choose **UniAgent Batch Operation > Upgrade**. On the displayed page, select the target version and click **OK**.
 - (New) On the **UniAgents** page, switch to the **ECS** or **Other** tab page and click **Upgrade**. On the displayed page, select the target version and click **OK**. (If CCE cluster-hosted servers are selected or the UniAgent has already been installed on the **K8s Clusters** page, go to the **K8s Clusters** page to upgrade the UniAgent.)

Wait for about 1 minute until the UniAgent upgrade is complete.

----End

Uninstalling UniAgents

Uninstall UniAgents when necessary.

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane on the left, choose **Settings > Global Settings**.
- Step 3** In the navigation pane on the left, choose **Collection Settings > UniAgents**. The old VM access page is displayed. You can click **Try New Version** in the upper right corner to go to the new UniAgent management page.
- Step 4** Select one or more servers where UniAgents are to be uninstalled and perform the following operations:
- (Old) On the **VM Access** page, choose **UniAgent Batch Operation > Uninstall**. On the displayed page, click **OK**.
 - (New) On the **UniAgents** page, switch to the **ECS** or **Other** tab page and click **Uninstall**. On the displayed page, click **OK**. (If CCE cluster-hosted servers are selected or the UniAgent has already been installed on the **K8s Clusters** page, go to the **K8s Clusters** page to uninstall the UniAgent.)

You can also log in to the target server as the **root** user and run the following command to uninstall the UniAgent:

```
bash /usr/local/uniagentd/bin/uninstall_uniagent.sh;
```

----End

Deleting UniAgents

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

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane on the left, choose **Settings > Global Settings**.
- Step 3** In the navigation pane on the left, choose **Collection Settings > UniAgents**. The old VM access page is displayed. You can click **Try New Version** in the upper right corner to go to the new UniAgent management page.
- Step 4** Select one or more servers where UniAgents are to be deleted and perform the following operations:
- (Old) On the **VM Access** page, choose **UniAgent Batch Operation > Delete**. On the displayed page, click **OK**.
 - (New) On the **UniAgents** page, switch to the **ECS** or **Other** tab page and click **Delete**. On the displayed page, click **OK**.

----End

6.2.4 Managing ICAgent Plug-ins for Hosts

AOM will support interconnection with other types of plug-ins. You can install, upgrade, uninstall, start, stop, and restart plug-ins in batches for hosts.

Currently, only ICAgents are supported. An ICAgent is a plug-in for collecting metrics and logs. ICAgent collects data at an interval of 1 minute. This interval cannot be changed.

Managing ICAgent Plug-ins in Batches

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane on the left, choose **Settings > Global Settings**.
- Step 3** In the navigation pane on the left, choose **Collection Settings > UniAgents**. The old VM access page is displayed. You can click **Try New Version** in the upper right corner to go to the new UniAgent management page.
- Step 4** Select one or more target servers and click **Plug-in Batch Operation**.
- Step 5** In the displayed dialog box, select an operation type, set the plug-in information, and click **OK**. (When selecting a CCE host, you are advised to go to the [K8s Clusters](#) page to operate the ICAgent.)

Table 6-12 Plug-in operation parameters

Parameter	Description
Operation	The following batch operations are supported: install, upgrade, uninstall, start, stop, and restart.
Plug-in	Select the plug-in to be operated. The ICAgent of the latest version can be installed.
AK/SK	<p>Access Key ID/Secret Access Key (AK/SK) to be entered based on your plug-in type and version.</p> <p>You need to enter an AK/SK only when installing the ICAgent of an earlier version. (If there is no text box for you to enter the AK/SK, the ICAgent of the new version has already been installed.)</p> <p>Procedure to obtain an AK/SK:</p> <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.

----End

6.2.5 Managing UniAgents and ICAgents in CCE Clusters

Kubernetes cluster management allows you to manage the lifecycle of UniAgents and ICAgents on hosts in CCE clusters under your account, for example, batch installation, upgrade, and uninstall.

Prerequisites

- You have CCE clusters and nodes under your account.

Viewing the CCE Clusters Connected to AOM

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane on the left, choose **Settings > Global Settings**.

Step 3 In the navigation pane, choose **Collection Settings > K8s Clusters**.

Step 4 On the **K8s Clusters** page, check the CCE clusters connected to AOM.

- Enter a CCE cluster name or ID in the search box to search for a cluster. Fuzzy match is supported.
- To collect container logs and output them to AOM 1.0, enable **Output to AOM 1.0**. (This function is supported only by ICAgent 5.12.133 or later.) You are advised to collect container logs and output them to LTS instead of AOM

1.0. For details, see "Ingesting CCE Application Logs to LTS" in the *Log Tank Service (LTS) User Guide*.

----End

Managing the UniAgents of CCE Clusters

You can install, upgrade, and uninstall UniAgent on hosts in CCE clusters connected to AOM.

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane on the left, choose **Settings > Global Settings**.
- Step 3** On the **Global Settings** page, choose **Collection Settings > K8s Clusters** in the navigation pane.
- Step 4** On the displayed page, select the target cluster from the cluster list and perform the operations listed in the following table if needed.

Table 6-13 Operations on UniAgents

Operation	Description
Install UniAgent	<ol style="list-style-type: none"> 1. Click Install UniAgent and select a UniAgent version to install. 2. Click OK. The UniAgent of the specified version and the ICAgent of the latest version will be installed on all hosts of the cluster.
Upgrade UniAgent	<ol style="list-style-type: none"> 1. Click Upgrade UniAgent and select a UniAgent version to upgrade. 2. Click OK. The UniAgents on all hosts of the cluster will be upgraded to the version you specified.
Uninstall UniAgent	<ol style="list-style-type: none"> 1. Click Uninstall UniAgent. On the displayed page, click OK. The UniAgents will be uninstalled from all hosts of the cluster. ICAgents will also be uninstalled if there are any. Only the UniAgents installed on the K8s Clusters page can be uninstalled here.

----End

Managing ICAgents in CCE Clusters

You can install, upgrade, and uninstall ICAgents on hosts in CCE clusters connected to AOM.

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane on the left, choose **Settings > Global Settings**.
- Step 3** On the **Global Settings** page, choose **Collection Settings > K8s Clusters** in the navigation pane.

- Step 4** On the **K8s Clusters** page, select the cluster where you want to perform ICAgent operations and click **Plug-in Operations**.

Plug-in operations are supported only when your UniAgent has been installed through the K8s Clusters page. If your UniAgent is not installed through the K8s Clusters page, click Install UniAgent to install the UniAgent on the hosts in your CCE cluster before performing plug-in operations.

- Step 5** In the displayed dialog box, select the operations listed in the following table if needed.

Table 6-14 Plug-in operations

Operation	Description
Install	<ol style="list-style-type: none">1. Select the Install operation and ICAgent plug-in. (Only the ICAgent can be installed.)2. Click OK. The ICAgent of the latest version will then be installed on all hosts that meet criteria.
Upgrade	<ol style="list-style-type: none">1. Select the Upgrade operation and ICAgent plug-in. (Only the ICAgent can be upgraded.)2. Click OK. The ICAgent on all hosts that meet criteria will then be upgraded to the latest version.
Uninstall	<ol style="list-style-type: none">1. Select the Uninstall operation and ICAgent plug-in. (Only the ICAgent can be uninstalled.)2. Click OK. The ICAgent will then be uninstalled from all hosts that meet criteria.

----End

6.2.6 Managing Host Groups

AOM is a unified platform for observability analysis. It does not provide log functions by itself. Instead, it integrates the host group management function of Log Tank Service (LTS). You can perform operations on the AOM 2.0 or LTS console.

To use the host group management function on the AOM 2.0 console, enable LTS first.

Table 6-15 Description

Function	Description	AOM 2.0 Console	LTS Console	References
Host group management	Host groups allow you to configure host log ingestion efficiently. You can add multiple hosts to a host group and associate the host group with log ingestion configurations. The ingestion configurations will then be applied to all the hosts in the host group.	<ol style="list-style-type: none">1. Log in to the AOM 2.0 console.2. In the navigation pane, choose Settings > Global Settings.3. On the displayed page, choose Collection Settings > Host Groups in the navigation pane.	<ol style="list-style-type: none">1. Log in to the LTS console.2. In the navigation pane, choose Host Management.	Section "Managing Host Groups" in the <i>Log Tank Service (LTS) User Guide</i>

- To use LTS functions on the AOM console, you need to obtain LTS permissions in advance.
- AOM 2.0 also provides a new version of host group management. After you switch to the new access center, the **new host group management** page will be displayed.

6.2.7 (New) Managing Host Groups

Host groups allow you to configure host data ingestion efficiently. You can add multiple hosts to a host group and associate the host group with ingestion configurations. The ingestion configurations will then be applied to all the hosts in the host group. When there is a new host, simply add it to a host group and the host will automatically inherit the log ingestion configurations associated with the host group.

You can create host groups of the IP address and custom identifier types.

- **Host Group Type** set to **IP**: Select hosts of the IP address type and add them to the host group.
- **Host Group Type** set to **Custom Identifier**: You need to create identifiers for each host group and host. Hosts with an identifier will automatically be included in the corresponding host group sharing that identifier.

Constraints


To use the new host group management function, switch to the new access center. To go to the [old host group management](#) page, choose **Access Center > Access Center** in the navigation pane on the left and then click **Back to Old Version** in the upper right corner.


Creating a Host Group (IP Address)

1. Log in to the AOM 2.0 console.
2. In the navigation pane, choose **Settings > Global Settings**.
3. On the **Global Settings** page, choose **Collection Settings > Host Groups** and click **Create Host Group** in the upper left corner.
4. On the displayed page, set the host group parameters.

Table 6-16 Parameters

Parameter	Description	Example
Host Group	Name of a host group. Enter 1 to 64 characters. Do not start with a period (.) or underscore (_) or end with a period. Only letters, digits, hyphens (-), underscores, and periods are allowed.	IPHostGroup1
Host Group Type	Type of the host group. Options: IP and Custom Identifier . In this example, select IP .	IP
Host Type	Host type. Default: Linux .	Linux
Remark	Host group remarks. Enter up to 1,024 characters.	-

5. In the host list, select one or more hosts to add to the group and click **OK**.
 - You can filter hosts by host name/ID or private IP address. You can also click  and enter multiple host IP addresses in the displayed search box to search.
 - If your desired hosts are not in the list, click **Install UniAgent**. On the displayed page, install UniAgents on the hosts as prompted. For details, see [5.2.2 \(New\) Installing UniAgents](#).
 - When the selected hosts do not have UniAgent installed but have an earlier version of ICAgent installed, an upgrade prompt appears. To enable automatic UniAgent installation later, click **Upgrade** to first upgrade ICAgent to the latest version.
 - If the selected hosts do not have both UniAgent and ICAgent installed (either UniAgent or ICAgent is in the **Not installed** state), click **OK**. A dialog box will pop up, indicating the missing UniAgent or ICAgent and the number of hosts without UniAgent or ICAgent installed.

- When selecting an ECS, click **OK** in the dialog box. The system will then issue a task for automatically installing either UniAgent or ICAgent. Otherwise, the host cannot be added to the host group. (Only ECSs running Linux support automatic UniAgent or ICAgent installation.)
 - When selecting a host of the **Other** type, manually install UniAgent and ICAgent first. Otherwise, the host cannot be added to the host group. For details, see [5.2.2 \(New\) Installing UniAgents](#).
- Click  in the upper right corner of the host list to manually refresh the list.

Creating a Host Group (Custom Identifier)

1. Log in to the AOM 2.0 console.
2. In the navigation pane on the left, choose **Settings > Global Settings**. On the displayed page, choose **Collection Settings > Host Groups** and click **Create Host Group** in the upper left corner.
3. On the displayed page, set the host group parameters.

Table 6-17 Parameters

Parameter	Description	Example
Host Group	Name of a host group. Enter 1 to 64 characters. Do not start with a period (.) or underscore (_) or end with a period. Only letters, digits, hyphens (-), underscores, and periods are allowed.	HostGroup
Host Group Type	Type of the host group. Options: IP and Custom Identifier . In this example, select Custom Identifier .	Custom Identifier
Host Type	Host type. Default: Linux .	Linux
Remark	Host group remarks. Enter up to 1,024 characters.	-
Custom Identifier	Click Add to add a custom identifier. Max.: 128 characters. Only letters, digits, underscores (_), and hyphens (-) are allowed. Up to 10 custom identifiers can be added.	aom

4. Click **OK**. After the host group is created, add hosts to it by referring to [5](#).
5. Log in to the host and perform the following operations as the **root** user to create the **custom_tag** file for storing host tags.
 - a. Run the **cd /opt/cloud** command.

- If the **/opt/cloud** directory already exists, navigate to it and run the **mkdir lts** command to create the **lts** directory in it.
- If the **/opt/cloud** directory does not exist, run the **mkdir /opt/cloud/** command to create it and enter it, and then run the **mkdir lts** command to create the **lts** directory.
- b. Run the **chmod 750 lts** command to modify the permission on the **lts** directory.
- c. Run the **touch custom_tag** command in the **lts** directory to create the **custom_tag** file.
- d. Run the **chmod 640 custom_tag;vi custom_tag** command to modify the **custom_tag** file permission and open the file.
- e. Press **i** to enter the insert mode, enter a custom identifier, press **Esc**, enter **:wq!**, save the modification and exit.
- f. Use either of the following methods to add a host to the custom identifier host group:



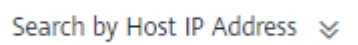


Table 6-18 Methods





Type	Method 1 (Recommended)	Method 2
Linux host	<ol style="list-style-type: none">1. View the host identifier in the custom_tag file under the /opt/cloud/lts directory of the host.2. On the host group configuration page, add the host identifier as the custom identifier for the host group to include the host in that group. For example, in the custom_tag file of the /opt/cloud/lts directory on the host, the identifier of the host is test1, and the custom identifier of the host group is set to test1. In this way, the host is added to the host group.	<ol style="list-style-type: none">1. Configure a custom identifier before creating a host group.2. Add the custom identifier to the custom_tag file in the /opt/cloud/lts directory of the host. The host can then be added to the specified host group. For example, if the custom identifier of the host group is set to test during host group creation, enter test in the custom_tag file to add the host to the host group. <p>If multiple custom identifiers are added, enter any custom identifier in the custom_tag file of the /opt/cloud/lts directory on the host to add the host to the host group.</p>




Other Operations

You can change a created host group, add hosts to or remove hosts from a host group, or associate a host group with log ingestion configurations.

Table 6-19 Operations on host groups

Operation	Procedure
Changing a host group	<ol style="list-style-type: none"> 1. Locate the target host group and click  in the Operation column. 2. On the displayed dialog box, modify the information such as the host group name, custom identifier, and remark. 3. Click OK.
Adding hosts to a host group	<ol style="list-style-type: none"> 1. Click  next to the target IP address host group. 2. Click Add Host. 3. In the displayed slide-out panel, all hosts that are not in the host group and run the selected OS type are displayed. Select the hosts to be added to the host group. For details, see 5. <ul style="list-style-type: none"> • You can filter hosts by host name/ID or private IP address. <p>You can also click  and enter multiple host IP addresses in the displayed search box to search.</p> <ul style="list-style-type: none"> • If your desired hosts are not in the list, click Install UniAgent. On the displayed page, install UniAgents on the hosts as prompted. For details, see 5.2.2 (New) Installing UniAgents. 4. Click OK. <p>This operation is not supported for hosts in a custom identifier host group. To add hosts to a custom identifier host group, refer to 5.</p>
Removing a host from a host group	<ol style="list-style-type: none"> 1. Click  next to the target IP address host group. 2. Locate the target host and click Remove in the Operation column. 3. In the displayed dialog box, click OK. <p>This operation is not supported for hosts in a custom identifier host group.</p>
Removing hosts in batches	<ol style="list-style-type: none"> 1. Locate the target host group and click  next to it. 2. Select the target hosts and click Remove above the list. 3. Click OK. <p>This operation is not supported for hosts in a custom identifier host group.</p>

Operation	Procedure
Viewing log ingestion rules	<ol style="list-style-type: none"> 1. Locate the target host group and click  next to it. 2. Click the Associated Ingestion Configurations tab to view the log ingestion rules configured for the host group. <p>For how to configure log ingestion rules for the host group, see 6.6 Managing Metric and Log Ingestion.</p>
Viewing metric access rules	<ol style="list-style-type: none"> 1. Locate the target host group and click  next to it. 2. Click the Metric Access Rules tab to view the metric access rules configured for the host group. <p>For how to configure metric ingestion rules for the host group, see 6.6 Managing Metric and Log Ingestion.</p>
Associating a host group with an ingestion configuration	<ol style="list-style-type: none"> 1. Locate the target host group and click  next to it. 2. Click the Associated Ingestion Configurations tab and then click Associate. 3. In the displayed slide-out panel, select the target ingestion configuration. 4. Click OK. The associated ingestion configuration is displayed in the list.
Disassociating a host group from an ingestion configuration	<ol style="list-style-type: none"> 1. Click the Associated Ingestion Configurations tab, locate the target ingestion configuration, and then click Disassociate in the Operation column. 2. Click OK.
Disassociating a host group from multiple ingestion configurations	<ol style="list-style-type: none"> 1. Click the Associated Ingestion Configurations tab, select target ingestion configurations, and then click Disassociate above the list. 2. Click OK.
Copying host group information	<p>Hover your cursor over a host group name to copy a host group ID.</p>
Deleting a host group	<ol style="list-style-type: none"> 1. Locate the target host group and click  in the Operation column. 2. In the displayed dialog box, click OK.

Operation	Procedure
Deleting host groups in batches	<ol style="list-style-type: none">1. Select multiple host groups to be deleted and click Delete above the list.2. In the displayed dialog box, click OK.
Managing tags	<p>Tag log groups as required.</p> <ol style="list-style-type: none">1. Locate the target host group and click  in the Operation column.2. On the displayed page, enter a tag key and value. <p>Precautions:</p> <ul style="list-style-type: none">• To add more tags, repeat the preceding step.• To delete a tag, locate the target host group and click  in the Operation column. On the displayed page, locate the target tag and click  in the Operation column.• A tag key can contain up to 128 characters, and a tag value can contain up to 255 characters.• A tag key must be unique.

6.2.8 Configuring a Proxy Area and Proxy

To enable network communication between multiple clouds, you need to configure an ECS as a proxy. The target host forwards O&M data to AOM through the proxy. A proxy area is used to manage proxies by category. It consists of multiple proxies.

Procedure

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane on the left, choose **Settings > Global Settings**.
- Step 3** In the navigation pane, choose **Collection Settings > Proxy Areas**.
- Step 4** Click **Add Proxy Area** and set proxy area parameters.

Table 6-20 Proxy area parameters

Parameter	Description	Example
Proxy Area Name	Name of a proxy area. Max.:	test

- Step 5** Click **OK** to add a proxy area.
- Step 6** Locate the new proxy area, click **Add Proxy**, and set proxy parameters.




Table 6-21 Proxy parameters

Parameter	Description	Example
Proxy Area	Select a proxy area that you have created.	test
Host	Select a host where the UniAgent has been installed. Hosts running Windows cannot be added as proxies.	-
Proxy IP Address	Set the IP address of the proxy.	192.168.0.0
Port	Set a port number and proxy protocol. <ul style="list-style-type: none"> The default port number is 32555. Range: 1,025 to 65,535. The proxy protocol can only be SOCKS5. 	32555

Step 7 Click **OK**.

After configuring the proxy area and proxy, perform the following operations if needed:

Table 6-22 Managing the proxy area and proxy

Operation	Description
Searching for a proxy area	Click  next to Add Proxy Area . Then, in the search box, enter a keyword to search for your target proxy area.
Modifying a proxy area	Hover the pointer over a proxy area and choose  > Edit . In the dialog box that is displayed, enter a new name, and click OK .
Deleting a proxy area	Hover the pointer over a proxy area and choose  > Delete . In the dialog box that is displayed, click Yes to delete the proxy area.
Checking a proxy	Click a proxy area to check the proxy in it.
Modifying a proxy IP address	Click Modify Proxy IP in the Operation column of the proxy. On the page that is displayed, modify the proxy IP address.
Deleting a proxy	Click Delete in the Operation column of the proxy. In the displayed dialog box, click Yes to delete the proxy.

----End

6.2.9 Viewing Operation Logs

AOM records operation logs of tasks such as installation/upgrade/uninstall/start/stop/restart related to UniAgent and other plug-ins. You can check the operation logs of related tasks.

Viewing UniAgent Operation Logs

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane on the left, choose **Settings > Global Settings**.
- Step 3** In the navigation tree on the left, choose **Collection Settings > Operation Logs**. The **UniAgent Logs** tab page is displayed by default.
- Step 4** Set criteria to search for historical tasks.
- Filter data by executor name.
 - Filter historical tasks by date. Options: **Last hour**, **Last 6 hours**, **Last day**, **Last 3 days**, and **Custom**. You can query historical tasks of half a year at most.
- Step 5** Click a task ID. On the task details page that is displayed, click **View Log** to view UniAgent operation logs.

----End

Viewing Plug-In Operation Logs




- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane on the left, choose **Settings > Global Settings**.
- Step 3** In the navigation tree on the left of the **Global Settings** page, choose **Collection Settings > Operation Logs**. On the displayed page, click the **Plug-in Logs** tab.
- Step 4** Set criteria to search for historical tasks.
- Filter data by executor name.
 - Filter historical tasks by date. Options: **Last hour**, **Last 6 hours**, **Last day**, **Last 3 days**, and **Custom**. You can query historical tasks of half a year at most.
- Step 5** Click a task ID. On the task details page that is displayed, click **View Log** in the **Operation** column to view plug-in operation logs.

----End

Other Operations

On the **Operation Logs** page, perform the operations listed in the following table if needed.

Table 6-23 Related operations

Operation	Description
Refreshing the task list	Click  in the upper right corner of the task list to refresh the list.
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 operation 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 task orders.

6.3 Connecting Self-Built Middleware to AOM

6.3.1 Overview About Middleware Connection to AOM

AOM provides a unified entry for observability analysis of cloud services. Through the access center, you can ingest the metrics of self-built middleware such as MySQL, Redis, and Kafka into AOM, and check documents related to log ingestion.

Procedure

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane on the left, choose **Access Center > Access Center** to go to the new access center.

If the old access center is displayed, click **Try New Version** in the upper right corner.

Step 3 Select **Self-built middleware** under **Types** to filter out your target middleware card.

Step 4 Click **Ingest Metric (AOM)** to quickly ingest middleware metrics to AOM.

- **Ingest Metric (AOM):** AOM enables quick installation and configuration for [self-built middleware](#). By creating collection tasks and executing plug-in scripts, Prometheus monitoring can monitor reported middleware metrics. It works with AOM and open-source Grafana to provide one-stop, comprehensive monitoring, helping you quickly detect and locate faults and reduce their impact on services. For details about the metrics that can be monitored by AOM, see [open-source Exporters](#).

To quickly ingest middleware metrics to AOM, perform the following steps:

- a. Install UniAgent on your VM for installing Exporters and creating collection tasks. For details, see [6.2.2 \(New\) Installing UniAgents](#).

- b. Create a Prometheus instance for ECS or a common Prometheus instance and associate it with a collection task to mark and categorize collected data. For details, see [12.2 Managing Prometheus Instances](#).
- c. Connect middleware to AOM. For details, see [6.3.2 Ingesting MySQL Metrics to AOM](#).
- d. After middleware is connected to AOM, their metrics can be reported to AOM. You can go to the [Metric Browsing](#) page to query metrics.

Table 6-24 Connecting self-built middleware to AOM

Card	Related Operation
MySQL	A stable, efficient relational database for heavy data volumes. Used for website and application development. For details, see: Ingesting MySQL Metrics to AOM .
Redis	In-memory storage system for multiple data structure types. Used as a database, cache, and message broker. For details, see: Ingesting Redis Metrics to AOM .
Kafka	Distributed stream processing platform with high throughput and low latency. Used for real-time data processing and log aggregation. For details, see: Ingesting Kafka Metrics to AOM .
Nginx	A high-performance HTTP/reverse proxy server for 50,000 concurrent requests. Reduces memory consumption. For details, see: Ingesting Nginx Metrics to AOM .
MongoDB	High-performance, open-source NoSQL database for document storage and flexible data models. For details, see Ingesting MongoDB Metrics to AOM .
Consul	Open-source distributed service discovery and configuration management, supporting multiple data centers and strong consistency. For details, see Ingesting Consul Metrics to AOM .
HAProxy	High-performance TCP/HTTP reverse proxy load balancer with high concurrency and flexible configuration for high service availability. For details, see Ingesting HAProxy Metrics to AOM .
PostgreSQL	A powerful, open source object-relational database system for complex queries and customization. For details, see Ingesting PostgreSQL Metrics to AOM .
Elasticsearch	Distributed full-text search engine with PB-level data storage and real-time retrieval. Used for full-text search, analysis, and monitoring. For details, see: Ingesting Elasticsearch Metrics to AOM .
RabbitMQ	Collect RabbitMQ monitoring data. For details, see Ingesting RabbitMQ Metrics to AOM .

----End

6.3.2 Ingesting MySQL Metrics to AOM

Install the MySQL Exporter provided by AOM, and then create a collection task by setting a metric ingestion rule to monitor MySQL metrics on a host.

Prerequisites

- [The UniAgent has been installed](#) and is running.
- [A Prometheus instance for ECS or a common Prometheus instance](#) has been created.
- To use the new MySQL Exporter ingestion function, switch to the new access center.

Connecting MySQL Exporter to AOM

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Access Center > Access Center**, filter the **MySQL** card under **Self-built middleware**, and click **Ingest Metric (AOM)**.

Step 3 On the displayed page, set parameters.

1. Set the Prometheus instance.
 - a. **Instance Type:** Select a Prometheus instance type. Options: **Prometheus for ECS** and **Common Prometheus instance**.
 - b. **Instance Name:** Select a Prometheus instance from the drop-down list and click **Next**.

You can click **View Instance** to go to the details page of the selected instance. If no Prometheus instance is available, click **Create Instance** to [create a Prometheus instance for ECS or a common Prometheus instance](#).
2. Install the plug-in and test the connectivity.
 - a. Set parameters to install the plug-in by referring to the following table.

Table 6-25 Parameters

Operation	Parameter	Description
Basic Settings	Ingestion Rule Name	Name of a custom metric ingestion rule. Enter 1 to 50 characters starting with a letter. Only letters, digits, underscores (_), and hyphens (-) are allowed.

Operation	Parameter	Description
Set Collection Plug-in	OS	Operating system of the host. Only Linux is supported.
	Collection Plug-in	The default value is MySQL Exporter . Select a plug-in version.
Select Server to Install Plug-in	Select Server	<p>Click Select Server to select a running server to configure a collection task and install Exporter.</p> <ul style="list-style-type: none"> On the Select Server page, search for servers by server ID, name, status, or IP address. Ensure that the UniAgent of the selected server is running. Otherwise, no data can be collected. If no server meets your requirements, UniAgent may be not installed. In that case, install UniAgent. In addition, ensure that the UniAgent version is 1.1.3 or later. Upgrade UniAgent when necessary.
Connect MySQL Instance	MySQL Username	Username of MySQL.
	MySQL Password	Password of MySQL.
	MySQL Address	IP address and port number of MySQL, for example, 10.0.0.1:3306 .

- b. Click **Install & Test Collection Plug-in** to deliver the Exporter installation task.
 - After the plug-in is installed, click **Next**.
 - Click **View Log** to view Exporter installation logs if the installation fails.
3. Set an ingestion rule.
Set a metric ingestion rule by referring to the following table.

Table 6-26 Parameters

Operation	Parameter	Description
Metric Collection Rule	Metric Collection Interval (s)	Interval for collecting metrics, in seconds. Options: 10 , 30 , and 60 (default).
	Metric Collection Timeout (s)	Timeout period for executing a metric collection task, in seconds. Options: 10 , 30 , and 60 (default). The timeout period cannot exceed the collection interval.
	Executor	User who executes the metric ingestion rule, that is, the user of the selected server. By default, the executor is root .
Other	Custom Dimensions	Dimensions (key-value pairs) added to specify additional metric attributes. You can click Add Dimension to add multiple custom dimensions (key-value pairs). <ul style="list-style-type: none">– Key: key of the additional attribute of a metric. Only letters, digits, and underscores (_) are allowed. Each name must start with a letter or underscore. Each key must be unique.– Value: corresponds to the key of the additional attribute of a metric. The following characters are not allowed: & ><\$;'!-() Up to 10 dimensions can be added. Example: Set the key to app and value to abc .

After the metric collection rule parameters are configured, you can click **YAML** to view the configuration data in YAML format.

Step 4 Click **Next** to connect MySQL Exporter.

After MySQL Exporter is connected, perform the following operations if needed:

- Back to the access center to connect other data sources. For details, see [6.1 AOM Access Overview](#).
- Go to the **Access Management** page to view and manage the ingestion configuration of the Exporter. For details, see [6.6 Managing Metric and Log Ingestion](#).
- Go to the **Metric Browsing** page to analyze metrics. For details, see [7 Observability Metric Browsing](#).

----End

6.3.3 Ingesting Redis Metrics to AOM

Install the Redis Exporter provided by AOM, and then create a collection task by setting a metric ingestion rule to monitor Redis metrics on a host.

Prerequisites

- [The UniAgent has been installed](#) and is running.
- [A Prometheus instance for ECS or a common Prometheus instance](#) has been created.
- To use the new Redis Exporter ingestion function, switch to the new access center.

Connecting Redis Exporter to AOM

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Access Center > Access Center**, filter the **Redis** card under **Self-built middleware**, and click **Ingest Metric (AOM)**.

Step 3 On the displayed page, set parameters.

1. Set the Prometheus instance.
 - a. **Instance Type:** Select a Prometheus instance type. Options: **Prometheus for ECS** and **Common Prometheus instance**.
 - b. **Instance Name:** Select a Prometheus instance from the drop-down list and click **Next**.

You can click **View Instance** to go to the details page of the selected instance. If no Prometheus instance is available, click **Create Instance** to [create a Prometheus instance for ECS or a common Prometheus instance](#).
2. Install the plug-in and test the connectivity.
 - a. Set parameters to install the plug-in by referring to the following table.

Table 6-27 Parameters

Operation	Parameter	Description
Basic settings	Ingestion Rule Name	Name of a custom metric ingestion rule. Enter 1 to 50 characters starting with a letter. Only letters, digits, underscores (_), and hyphens (-) are allowed.
Set Collection Plug-in	OS	Operating system of the host. Only Linux is supported.
	Collection Plug-in	The default value is Redis Exporter . Select a plug-in version.

Operation	Parameter	Description
Select Server to Install Plug-in	Select Server	<p>Click Select Server to select a running server to configure a collection task and install Exporter.</p> <ul style="list-style-type: none">On the Select Server page, search for servers by server ID, name, status, or IP address.Ensure that the UniAgent of the selected server is running. Otherwise, no data can be collected.If no server meets your requirements, UniAgent may be not installed. In that case, install UniAgent. In addition, ensure that the UniAgent version is 1.1.3 or later. Upgrade UniAgent when necessary.
Connect Redis Instance	Redis Address	IP address and port number of Redis, for example, 10.0.0.1:3306 .
	Redis Password	Password for logging in to Redis.

- b. Click **Install & Test Collection Plug-in** to deliver the Exporter installation task.
 - After the plug-in is installed, click **Next**.
 - Click **View Log** to view Exporter installation logs if the installation fails.
3. Set an ingestion rule.

Set a metric ingestion rule by referring to the following table.

Table 6-28 Parameters

Operation	Parameter	Description
Metric Collection Rule	Metric Collection Interval (s)	Interval for collecting metrics, in seconds. Options: 10 , 30 , and 60 (default).
	Metric Collection Timeout (s)	<p>Timeout period for executing a metric collection task, in seconds. Options: 10, 30, and 60 (default).</p> <p>The timeout period cannot exceed the collection interval.</p>

Operation	Parameter	Description
	Executor	User who executes the metric ingestion rule, that is, the user of the selected server. By default, the executor is root .
Other	Custom Dimensions	<p>Dimensions (key-value pairs) added to specify additional metric attributes. You can click Add Dimension to add multiple custom dimensions (key-value pairs).</p> <ul style="list-style-type: none">– Key: key of the additional attribute of a metric. Only letters, digits, and underscores (_) are allowed. Each name must start with a letter or underscore. Each key must be unique.– Value: corresponds to the key of the additional attribute of a metric. The following characters are not allowed: & ><\$;'!-() <p>Up to 10 dimensions can be added. Example: Set the key to app and value to abc.</p>

After the metric collection rule parameters are configured, you can click **YAML** to view the configuration data in YAML format.

Step 4 Click **Next** to connect Redis Exporter.

After Redis Exporter is connected, perform the following operations if needed:

- Back to the access center to connect other data sources. For details, see [6.1 AOM Access Overview](#).
- Go to the **Access Management** page to view and manage the ingestion configuration of the Exporter. For details, see [6.6 Managing Metric and Log Ingestion](#).
- Go to the **Metric Browsing** page to analyze metrics. For details, see [7 Observability Metric Browsing](#).

----End

6.3.4 Ingesting Kafka Metrics to AOM

Install the Kafka Exporter provided by AOM, and then create a collection task by setting a metric ingestion rule to monitor Kafka metrics on a host.

Prerequisites

- [The UniAgent has been installed](#) and is running.
- [A Prometheus instance for ECS or a common Prometheus instance](#) has been created.
- To use the new Kafka Exporter ingestion function, switch to the new access center.

Connecting Kafka Exporter to AOM

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Access Center > Access Center**, filter the **Kafka** card under **Self-built middleware**, and click **Ingest Metric (AOM)**.

Step 3 On the displayed page, set parameters.

1. Set the Prometheus instance.
 - a. **Instance Type:** Select a Prometheus instance type. Options: **Prometheus for ECS** and **Common Prometheus instance**.
 - b. **Instance Name:** Select a Prometheus instance from the drop-down list and click **Next**.

You can click **View Instance** to go to the details page of the selected instance. If no Prometheus instance is available, click **Create Instance** to [create a Prometheus instance for ECS or a common Prometheus instance](#).
2. Install the plug-in and test the connectivity.
 - a. Set parameters to install the plug-in by referring to the following table.

Table 6-29 Parameters

Operation	Parameter	Description
Basic Settings	Ingestion Rule Name	Name of a custom metric ingestion rule. Enter 1 to 50 characters starting with a letter. Only letters, digits, underscores (_), and hyphens (-) are allowed.
Set Collection Plug-in	OS	Operating system of the host. Only Linux is supported.
	Collection Plug-in	The default value is Kafka Exporter . Select a plug-in version.
Select Server to Install Plug-in	Select Server	<p>Click Select Server to select a running server to configure a collection task and install Exporter.</p> <ul style="list-style-type: none">On the Select Server page, search for servers by server ID, name, status, or IP address.Ensure that the UniAgent of the selected server is running. Otherwise, no data can be collected.If no server meets your requirements, UniAgent may be not installed. In that case, install UniAgent. In addition, ensure that the UniAgent version is 1.1.3 or later. Upgrade UniAgent when necessary.

Operation	Parameter	Description
Connect Kafka Instance	Kafka address	IP address and port number of Kafka, for example, 10.0.0.1:3306 .
	SASL enabled	Enter enabled or disabled . By default, SASL is disabled. <ul style="list-style-type: none">▪ enabled: Enable SASL.▪ disabled: Disable SASL.
	SASL username	SASL username.
	SASL password	SASL password.
	SASL mechanism	Enter an SASL mechanism. Options: plain , scram-sha512 , and scram-sha256 . By default, this parameter is left blank.
	TLS enabled	Enter enabled or disabled . By default, TLS is disabled. <ul style="list-style-type: none">▪ enabled: Enable TLS.▪ disabled: Disable TLS.

- b. Click **Install & Test Collection Plug-in** to deliver the Exporter installation task.

- After the plug-in is installed, click **Next**.
- Click **View Log** to view Exporter installation logs if the installation fails.

3. Set an ingestion rule.

Set a metric ingestion rule by referring to the following table.

Table 6-30 Parameters

Operation	Parameter	Description
Metric Collection Rule	Metric Collection Interval (s)	Interval for collecting metrics, in seconds. Options: 10 , 30 , and 60 (default).
	Metric Collection Timeout (s)	Timeout period for executing a metric collection task, in seconds. Options: 10 , 30 , and 60 (default). The timeout period cannot exceed the collection interval.

Operation	Parameter	Description
	Executor	User who executes the metric ingestion rule, that is, the user of the selected server. By default, the executor is root .
Other	Custom Dimensions	<p>Dimensions (key-value pairs) added to specify additional metric attributes. You can click Add Dimension to add multiple custom dimensions (key-value pairs).</p> <ul style="list-style-type: none">– Key: key of the additional attribute of a metric. Only letters, digits, and underscores (_) are allowed. Each name must start with a letter or underscore. Each key must be unique.– Value: corresponds to the key of the additional attribute of a metric. The following characters are not allowed: & ><\$;'!-() <p>Up to 10 dimensions can be added. Example: Set the key to app and value to abc.</p>

After the metric collection rule parameters are configured, you can click **YAML** to view the configuration data in YAML format.

Step 4 Click **Next** to connect Kafka Exporter.

After Kafka Exporter is connected, perform the following operations if needed:

- Back to the access center to connect other data sources. For details, see [6.1 AOM Access Overview](#).
- Go to the **Access Management** page to view and manage the ingestion configuration of the Exporter. For details, see [6.6 Managing Metric and Log Ingestion](#).
- Go to the **Metric Browsing** page to analyze metrics. For details, see [7 Observability Metric Browsing](#).

----End

6.3.5 Ingesting Nginx Metrics to AOM

Install the Nginx Exporter provided by AOM, and then create a collection task by setting a metric ingestion rule to monitor Nginx metrics on a host.

Prerequisites

- [The UniAgent has been installed](#) and is running.
- [A Prometheus instance for ECS or a common Prometheus instance](#) has been created.
- [The NGINX stub_status module has been enabled](#).

- To use the new Nginx Exporter ingestion function, switch to the new access center.

Enabling the Nginx stub_status Module

Nginx Prometheus Exporter monitors the Nginx service using the stub_status module. Ensure that this module is enabled.

- Step 1** Log in to the node where the Nginx service is deployed and run the following command (generally in the `/usr/local/nginx/sbin/nginx` directory) as the **root** user to check whether the stub_status module is enabled:

```
nginx -V 2>&1 | grep -o with-http_stub_status_module
```

- If **with-http_stub_status_module** is returned, the stub_status module is enabled.
- If no result is returned, enable the stub_status module by setting **--with-http_stub_status_module** in the configuration file. Example:

```
./configure \  
## Add the --with-http_stub_status_module parameter.  
--with-http_stub_status_module  
make  
sudo make install
```

- Step 2** After the stub_status module is enabled, add the following content to the **nginx.conf** file (which is generally in the `/usr/local/nginx/conf` directory):
Example:

1. Open the **nginx.conf** file using the vi editor:
`vi /usr/local/nginx/conf/nginx.conf`
2. Press **i** to enter the editing mode and add the following configuration information:

```
server {  
    listen 8080; # Listening port. Set this parameter based on service requirements.  
    listen [::]:8080; # IPv6 listening port. Set this parameter based on service requirements.  
    server_name localhost; # Set this parameter based on service requirements.  
    location = /stub_status { # Path. Set this parameter based on service requirements.  
        stub_status on;  
        access_log off;  
        allow 127.0.0.1;  
    }  
}
```

3. Press **Esc** and enter **:wq** to save the settings and exit.

- Step 3** Restart the Nginx service.

----End

Connecting Nginx Exporter to AOM

- Step 1** Log in to the AOM 2.0 console.

- Step 2** In the navigation pane, choose **Access Center > Access Center**, filter the **NGINX** card under **Self-built middleware**, and click **Ingest Metric (AOM)**.

- Step 3** On the displayed page, set parameters.

1. Set the Prometheus instance.
 - a. **Instance Type:** Select a Prometheus instance type. Options: **Prometheus for ECS** and **Common Prometheus instance**.

- b. **Instance Name:** Select a Prometheus instance from the drop-down list and click **Next**.

You can click **View Instance** to go to the details page of the selected instance. If no Prometheus instance is available, click **Create Instance** to [create a Prometheus instance for ECS or a common Prometheus instance](#).

2. Install the plug-in and test the connectivity.
- a. Set parameters to install the plug-in by referring to the following table.

Table 6-31 Parameters

Operation	Parameter	Description
Basic Settings	Ingestion Rule Name	Name of a custom metric ingestion rule. Enter 1 to 50 characters starting with a letter. Only letters, digits, underscores (_), and hyphens (-) are allowed.
Set Collection Plug-in	OS	Operating system of the host. Only Linux is supported.
	Collection Plug-in	The default value is Nginx Exporter . Select a plug-in version.
Select Server to Install Plug-in	Select Server	<p>Click Select Server to select a running server to configure a collection task and install Exporter.</p> <ul style="list-style-type: none">On the Select Server page, search for servers by server ID, name, status, or IP address.Ensure that the UniAgent of the selected server is running. Otherwise, no data can be collected.If no server meets your requirements, UniAgent may be not installed. In that case, install UniAgent. In addition, ensure that the UniAgent version is 1.1.3 or later. Upgrade UniAgent when necessary.

Operation	Parameter	Description
Connect Nginx Instance	Nginx URL	<p>Nginx URL, which is in the format of "Connection address of Nginx+Nginx service status path".</p> <ul style="list-style-type: none">▪ Connection address of Nginx: IP address and listening port number of the Nginx service. The listening port is specified in the nginx.conf file. Example: 10.0.0.1:8080▪ Nginx service status path: specified by the location parameter in the nginx.conf file, for example, /stub_status. <p>Example: https://10.0.0.1:8080/stub_status.</p>

- b. Click **Install & Test Collection Plug-in** to deliver the Exporter installation task.

- After the plug-in is installed, click **Next**.
- Click **View Log** to view Exporter installation logs if the installation fails.

3. Set an ingestion rule.

Set a metric ingestion rule by referring to the following table.

Table 6-32 Parameters

Operation	Parameter	Description
Metric Collection Rule	Metric Collection Interval (s)	Interval for collecting metrics, in seconds. Options: 10 , 30 , and 60 (default).
	Metric Collection Timeout (s)	Timeout period for executing a metric collection task, in seconds. Options: 10 , 30 , and 60 (default). The timeout period cannot exceed the collection interval.
	Executor	User who executes the metric ingestion rule, that is, the user of the selected server. By default, the executor is root .

Operation	Parameter	Description
Other	Custom Dimensions	<p>Dimensions (key-value pairs) added to specify additional metric attributes. You can click Add Dimension to add multiple custom dimensions (key-value pairs).</p> <ul style="list-style-type: none">– Key: key of the additional attribute of a metric. Only letters, digits, and underscores (_) are allowed. Each name must start with a letter or underscore. Each key must be unique.– Value: corresponds to the key of the additional attribute of a metric. The following characters are not allowed: & ><\$;'!-() <p>Up to 10 dimensions can be added. Example: Set the key to app and value to abc.</p>

After the metric collection rule parameters are configured, you can click **YAML** to view the configuration data in YAML format.

Step 4 Click **Next** to connect Nginx Exporter.

After Nginx Exporter is connected, perform the following operations if needed:

- Back to the access center to connect other data sources. For details, see [6.1 AOM Access Overview](#).
- Go to the **Access Management** page to view and manage the ingestion configuration of the Exporter. For details, see [6.6 Managing Metric and Log Ingestion](#).
- Go to the **Metric Browsing** page to analyze metrics. For details, see [7 Observability Metric Browsing](#).

----End

6.3.6 Ingesting MongoDB Metrics to AOM

Install the MongoDB Exporter provided by AOM, and then create a collection task by setting a metric ingestion rule to monitor MongoDB metrics on a host.

Prerequisites

- [The UniAgent has been installed](#) and is running.
- [A Prometheus instance for ECS or a common Prometheus instance](#) has been created.
- To use the new MongoDB Exporter ingestion function, switch to the new access center.

Connecting MongoDB Exporter to AOM

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Access Center > Access Center**, filter the **MongoDB** card under **Self-built middleware**, and click **Ingest Metric (AOM)**.

Step 3 On the displayed page, set parameters.

1. Set the Prometheus instance.
 - a. **Instance Type:** Select a Prometheus instance type. Options: **Prometheus for ECS** and **Common Prometheus instance**.
 - b. **Instance Name:** Select a Prometheus instance from the drop-down list and click **Next**.

You can click **View Instance** to go to the details page of the selected instance. If no Prometheus instance is available, click **Create Instance** to [create a Prometheus instance for ECS or a common Prometheus instance](#).
2. Install the plug-in and test the connectivity.
 - a. Set parameters to install the plug-in by referring to the following table.

Table 6-33 Parameters

Operation	Parameter	Description
Basic Settings	Ingestion Rule Name	Name of a custom metric ingestion rule. Enter 1 to 50 characters starting with a letter. Only letters, digits, underscores (_), and hyphens (-) are allowed.
Set Collection Plug-in	OS	Operating system of the host. Only Linux is supported.
	Collection Plug-in	The default value is MongoDB Exporter . Select a plug-in version.
Select Server to Install Plug-in	Select Server	<p>Click Select Server to select a running server to configure a collection task and install Exporter.</p> <ul style="list-style-type: none">▪ On the Select Server page, search for servers by server ID, name, status, or IP address.▪ Ensure that the UniAgent of the selected server is running. Otherwise, no data can be collected.▪ If no server meets your requirements, UniAgent may be not installed. In that case, install UniAgent. In addition, ensure that the UniAgent version is 1.1.3 or later. Upgrade UniAgent when necessary.

Operation	Parameter	Description
Connect MongoDB Instance	MongoDB Address	IP address of MongoDB, for example, 10.0.0.1 .
	MongoDB Port	Port number of MongoDB, for example, 3306 .
	MongoDB Username	Username for logging in to MongoDB.
	MongoDB Password	Password for logging in to MongoDB.

- b. Click **Install & Test Collection Plug-in** to deliver the Exporter installation task.
 - After the plug-in is installed, click **Next**.
 - Click **View Log** to view Exporter installation logs if the installation fails.
3. Set an ingestion rule.
Set a metric ingestion rule by referring to the following table.

Table 6-34 Parameters

Operation	Parameter	Description
Metric Collection Rule	Metric Collection Interval (s)	Interval for collecting metrics, in seconds. Options: 10 , 30 , and 60 (default).
	Metric Collection Timeout (s)	Timeout period for executing a metric collection task, in seconds. Options: 10 , 30 , and 60 (default). The timeout period cannot exceed the collection interval.
	Executor	User who executes the metric ingestion rule, that is, the user of the selected server. By default, the executor is root .

Operation	Parameter	Description
Other	Custom Dimensions	<p>Dimensions (key-value pairs) added to specify additional metric attributes. You can click Add Dimension to add multiple custom dimensions (key-value pairs).</p> <ul style="list-style-type: none">– Key: key of the additional attribute of a metric. Only letters, digits, and underscores (_) are allowed. Each name must start with a letter or underscore. Each key must be unique.– Value: corresponds to the key of the additional attribute of a metric. The following characters are not allowed: & ><\$;'!-() <p>Up to 10 dimensions can be added. Example: Set the key to app and value to abc.</p>

After the metric collection rule parameters are configured, you can click **YAML** to view the configuration data in YAML format.

Step 4 Click **Next** to connect MongoDB Exporter.

After MongoDB Exporter is connected, perform the following operations if needed:

- Back to the access center to connect other data sources. For details, see [6.1 AOM Access Overview](#).
- Go to the **Access Management** page to view and manage the ingestion configuration of the Exporter. For details, see [6.6 Managing Metric and Log Ingestion](#).
- Go to the **Metric Browsing** page to analyze metrics. For details, see [7 Observability Metric Browsing](#).

----End

6.3.7 Ingesting Consul Metrics to AOM

Install the Consul Exporter provided by AOM, and then create a collection task by setting a metric ingestion rule to monitor Consul metrics on a host.

Prerequisites

- [The UniAgent has been installed](#) and is running.
- [A Prometheus instance for ECS or a common Prometheus instance](#) has been created.
- To use the new Consul Exporter ingestion function, switch to the new access center.

Connecting Consul Exporter to AOM

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Access Center > Access Center**, filter the **Consul** card under **Self-built middleware**, and click **Ingest Metric (AOM)**.

Step 3 On the displayed page, set parameters.

1. Set the Prometheus instance.
 - a. **Instance Type:** Select a Prometheus instance type. Options: **Prometheus for ECS** and **Common Prometheus instance**.
 - b. **Instance Name:** Select a Prometheus instance from the drop-down list and click **Next**.

You can click **View Instance** to go to the details page of the selected instance. If no Prometheus instance is available, click **Create Instance** to [create a Prometheus instance for ECS or a common Prometheus instance](#).
2. Install the plug-in and test the connectivity.
 - a. Set parameters to install the plug-in by referring to the following table.

Table 6-35 Parameters

Operation	Parameter	Description
Basic Settings	Ingestion Rule Name	Name of a custom metric ingestion rule. Enter 1 to 50 characters starting with a letter. Only letters, digits, underscores (_), and hyphens (-) are allowed.
Set Collection Plug-in	OS	Operating system of the host. Only Linux is supported.
	Collection Plug-in	The default value is Consul Exporter . Select a plug-in version.
Select Server to Install Plug-in	Select Server	<p>Click Select Server to select a running server to configure a collection task and install Exporter.</p> <ul style="list-style-type: none">▪ On the Select Server page, search for servers by server ID, name, status, or IP address.▪ Ensure that the UniAgent of the selected server is running. Otherwise, no data can be collected.▪ If no server meets your requirements, UniAgent may be not installed. In that case, install UniAgent. In addition, ensure that the UniAgent version is 1.1.3 or later. Upgrade UniAgent when necessary.

Operation	Parameter	Description
Connect Consul Instance	Consul Address	IP address and port number of Consul, for example, 10.0.0.1:3306 .

- b. Click **Install & Test Collection Plug-in** to deliver the Exporter installation task.
 - After the plug-in is installed, click **Next**.
 - Click **View Log** to view Exporter installation logs if the installation fails.
3. Set an ingestion rule.
Set a metric ingestion rule by referring to the following table.

Table 6-36 Parameters

Operation	Parameter	Description
Metric Collection Rule	Metric Collection Interval (s)	Interval for collecting metrics, in seconds. Options: 10 , 30 , and 60 (default).
	Metric Collection Timeout (s)	Timeout period for executing a metric collection task, in seconds. Options: 10 , 30 , and 60 (default). The timeout period cannot exceed the collection interval.
	Executor	User who executes the metric ingestion rule, that is, the user of the selected server. By default, the executor is root .

Operation	Parameter	Description
Other	Custom Dimensions	<p>Dimensions (key-value pairs) added to specify additional metric attributes. You can click Add Dimension to add multiple custom dimensions (key-value pairs).</p> <ul style="list-style-type: none">– Key: key of the additional attribute of a metric. Only letters, digits, and underscores (_) are allowed. Each name must start with a letter or underscore. Each key must be unique.– Value: corresponds to the key of the additional attribute of a metric. The following characters are not allowed: & ><\$;'!-() <p>Up to 10 dimensions can be added. Example: Set the key to app and value to abc.</p>

After the metric collection rule parameters are configured, you can click **YAML** to view the configuration data in YAML format.

Step 4 Click **Next** to connect Consul Exporter.

After Consul Exporter is connected, perform the following operations if needed:

- Back to the access center to connect other data sources. For details, see [6.1 AOM Access Overview](#).
- Go to the **Access Management** page to view and manage the ingestion configuration of the Exporter. For details, see [6.6 Managing Metric and Log Ingestion](#).
- Go to the **Metric Browsing** page to analyze metrics. For details, see [7 Observability Metric Browsing](#).

----End

6.3.8 Ingesting HAProxy Metrics to AOM

Install the HAProxy Exporter provided by AOM, and then create a collection task by setting a metric ingestion rule to monitor HAProxy metrics on a host.

Prerequisites

- [The UniAgent has been installed](#) and is running.
- [A Prometheus instance for ECS or a common Prometheus instance](#) has been created.
- To use the new HAProxy Exporter ingestion function, switch to the new access center.

Connecting HAProxy Exporter to AOM

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Access Center > Access Center**, filter the **HAProxy** card under **Self-built middleware**, and click **Ingest Metric (AOM)**.

Step 3 On the displayed page, set parameters.

1. Set the Prometheus instance.
 - a. **Instance Type:** Select a Prometheus instance type. Options: **Prometheus for ECS** and **Common Prometheus instance**.
 - b. **Instance Name:** Select a Prometheus instance from the drop-down list and click **Next**.

You can click **View Instance** to go to the details page of the selected instance. If no Prometheus instance is available, click **Create Instance** to [create a Prometheus instance for ECS or a common Prometheus instance](#).
2. Install the plug-in and test the connectivity.
 - a. Set parameters to install the plug-in by referring to the following table.

Table 6-37 Parameters

Operation	Parameter	Description
Basic Settings	Ingestion Rule Name	Name of a custom metric ingestion rule. Enter 1 to 50 characters starting with a letter. Only letters, digits, underscores (_), and hyphens (-) are allowed.
Set Collection Plug-in	OS	Operating system of the host. Only Linux is supported.
	Collection Plug-in	The default value is HAProxy Exporter . Select a plug-in version.
Select Server to Install Plug-in	Select Server	<p>Click Select Server to select a running server to configure a collection task and install Exporter.</p> <ul style="list-style-type: none">On the Select Server page, search for servers by server ID, name, status, or IP address.Ensure that the UniAgent of the selected server is running. Otherwise, no data can be collected.If no server meets your requirements, UniAgent may be not installed. In that case, install UniAgent. In addition, ensure that the UniAgent version is 1.1.3 or later. Upgrade UniAgent when necessary.

Operation	Parameter	Description
Connect HAProxy Instance	HAProxy URL	<p>HAProxy connection address. Format: <code>http://{username}:{password}@{IP}:{port}/haproxy_stats;csv</code>.</p> <ul style="list-style-type: none">▪ <code>{username}</code>: username for logging in to HAProxy.▪ <code>{password}</code>: password for logging in to HAProxy.▪ <code>{IP}:{port}</code>: HAProxy IP address and port number, for example, 10.0.0.1:3306. <p>Example: http://admin:*****@10.0.0.1:3306/haproxy_stats;csv.</p>

- b. Click **Install & Test Collection Plug-in** to deliver the Exporter installation task.
 - After the plug-in is installed, click **Next**.
 - Click **View Log** to view Exporter installation logs if the installation fails.
3. Set an ingestion rule.

Set a metric ingestion rule by referring to the following table.

Table 6-38 Parameters

Operation	Parameter	Description
Metric Collection Rule	Metric Collection Interval (s)	Interval for collecting metrics, in seconds. Options: 10 , 30 , and 60 (default).
	Metric Collection Timeout (s)	Timeout period for executing a metric collection task, in seconds. Options: 10 , 30 , and 60 (default). The timeout period cannot exceed the collection interval.
	Executor	User who executes the metric ingestion rule, that is, the user of the selected server. By default, the executor is root .

Operation	Parameter	Description
Other	Custom Dimensions	<p>Dimensions (key-value pairs) added to specify additional metric attributes. You can click Add Dimension to add multiple custom dimensions (key-value pairs).</p> <ul style="list-style-type: none">– Key: key of the additional attribute of a metric. Only letters, digits, and underscores (_) are allowed. Each name must start with a letter or underscore. Each key must be unique.– Value: corresponds to the key of the additional attribute of a metric. The following characters are not allowed: & ><\$;'!-() <p>Up to 10 dimensions can be added. Example: Set the key to app and value to abc.</p>

After the metric collection rule parameters are configured, you can click **YAML** to view the configuration data in YAML format.

Step 4 Click **Next** to connect HAProxy Exporter.

After HAProxy Exporter is connected, perform the following operations if needed:

- Back to the access center to connect other data sources. For details, see [6.1 AOM Access Overview](#).
- Go to the **Access Management** page to view and manage the ingestion configuration of the Exporter. For details, see [6.6 Managing Metric and Log Ingestion](#).
- Go to the **Metric Browsing** page to analyze metrics. For details, see [7 Observability Metric Browsing](#).

----End

6.3.9 Ingesting PostgreSQL Metrics to AOM

Install the PostgreSQL Exporter provided by AOM, and then create a collection task by setting a metric ingestion rule to monitor PostgreSQL metrics on a host.

Prerequisites

- [The UniAgent has been installed](#) and is running.
- [A Prometheus instance for ECS or a common Prometheus instance](#) has been created.
- To use the new PostgreSQL Exporter ingestion function, switch to the new access center.

Connecting PostgreSQL Exporter to AOM

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Access Center > Access Center**, filter the **PostgreSQL** card under **Self-built middleware**, and click **Ingest Metric (AOM)**.

Step 3 On the displayed page, set parameters.

1. Set the Prometheus instance.
 - a. **Instance Type:** Select a Prometheus instance type. Options: **Prometheus for ECS** and **Common Prometheus instance**.
 - b. **Instance Name:** Select a Prometheus instance from the drop-down list and click **Next**.

You can click **View Instance** to go to the details page of the selected instance. If no Prometheus instance is available, click **Create Instance** to [create a Prometheus instance for ECS or a common Prometheus instance](#).
2. Install the plug-in and test the connectivity.
 - a. Set parameters to install the plug-in by referring to the following table.

Table 6-39 Parameters

Operation	Parameter	Description
Basic Settings	Ingestion Rule Name	Name of a custom metric ingestion rule. Enter 1 to 50 characters starting with a letter. Only letters, digits, underscores (_), and hyphens (-) are allowed.
Set Collection Plug-in	OS	Operating system of the host. Only Linux is supported.
	Collection Plug-in	The default value is PostgreSQL Exporter . Select a plug-in version.
Select Server to Install Plug-in	Select Server	<p>Click Select Server to select a running server to configure a collection task and install Exporter.</p> <ul style="list-style-type: none">On the Select Server page, search for servers by server ID, name, status, or IP address.Ensure that the UniAgent of the selected server is running. Otherwise, no data can be collected.If no server meets your requirements, UniAgent may be not installed. In that case, install UniAgent. In addition, ensure that the UniAgent version is 1.1.3 or later. Upgrade UniAgent when necessary.

Operation	Parameter	Description
Connect PostgreSQL Instance	PostgreSQL Username	PostgreSQL username.
	PostgreSQL Password	PostgreSQL password.
	PostgreSQL Address	PostgreSQL connection address. For example, <code>http://{IP}:{port}/databasename</code> . <ul style="list-style-type: none">▪ <code>{IP}:{port}</code>: PostgreSQL IP address and port number, for example, 10.0.0.1:3306.▪ <code>{databasename}</code>: PostgreSQL database name. Example: http://10.0.0.1:3306/xxxx .

- b. Click **Install & Test Collection Plug-in** to deliver the Exporter installation task.
 - After the plug-in is installed, click **Next**.
 - Click **View Log** to view Exporter installation logs if the installation fails.

3. Set an ingestion rule.

Set a metric ingestion rule by referring to the following table.

Table 6-40 Parameters

Operation	Parameter	Description
Metric Collection Rule	Metric Collection Interval (s)	Interval for collecting metrics, in seconds. Options: 10 , 30 , and 60 (default).
	Metric Collection Timeout (s)	Timeout period for executing a metric collection task, in seconds. Options: 10 , 30 , and 60 (default). The timeout period cannot exceed the collection interval.
	Executor	User who executes the metric ingestion rule, that is, the user of the selected server. By default, the executor is root .

Operation	Parameter	Description
Other	Custom Dimensions	<p>Dimensions (key-value pairs) added to specify additional metric attributes. You can click Add Dimension to add multiple custom dimensions (key-value pairs).</p> <ul style="list-style-type: none">– Key: key of the additional attribute of a metric. Only letters, digits, and underscores (_) are allowed. Each name must start with a letter or underscore. Each key must be unique.– Value: corresponds to the key of the additional attribute of a metric. The following characters are not allowed: & ><\$;'!-() <p>Up to 10 dimensions can be added. Example: Set the key to app and value to abc.</p>

After the metric collection rule parameters are configured, you can click **YAML** to view the configuration data in YAML format.

Step 4 Click **Next** to connect PostgreSQL Exporter.

After PostgreSQL Exporter is connected, perform the following operations if needed:

- Back to the access center to connect other data sources. For details, see [6.1 AOM Access Overview](#).
- Go to the **Access Management** page to view and manage the ingestion configuration of the Exporter. For details, see [6.6 Managing Metric and Log Ingestion](#).
- Go to the **Metric Browsing** page to analyze metrics. For details, see [7 Observability Metric Browsing](#).

-----End

6.3.10 Ingesting Elasticsearch Metrics to AOM

Install the Elasticsearch Exporter provided by AOM, and then create a collection task by setting a metric ingestion rule to monitor Elasticsearch metrics on a host.

Prerequisites

- [The UniAgent has been installed](#) and is running.
- [A Prometheus instance for ECS or a common Prometheus instance](#) has been created.
- To use the new Elasticsearch Exporter ingestion function, switch to the new access center.

Connecting Elasticsearch Exporter to AOM

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Access Center > Access Center**, filter the **Elasticsearch** card under **Self-built middleware**, and click **Ingest Metric (AOM)**.

Step 3 On the displayed page, set parameters.

1. Set the Prometheus instance.
 - a. **Instance Type:** Select a Prometheus instance type. Options: **Prometheus for ECS** and **Common Prometheus instance**.
 - b. **Instance Name:** Select a Prometheus instance from the drop-down list and click **Next**.

You can click **View Instance** to go to the details page of the selected instance. If no Prometheus instance is available, click **Create Instance** to [create a Prometheus instance for ECS or a common Prometheus instance](#).
2. Install the plug-in and test the connectivity.
 - a. Set parameters to install the plug-in by referring to the following table.

Table 6-41 Parameters

Operation	Parameter	Description
Basic Settings	Ingestion Rule Name	Name of a custom metric ingestion rule. Enter 1 to 50 characters starting with a letter. Only letters, digits, underscores (_), and hyphens (-) are allowed.
Set Collection Plug-in	OS	Operating system of the host. Only Linux is supported.
	Collection Plug-in	The default value is Elasticsearch Exporter . Select a plug-in version.
Select Server to Install Plug-in	Select Server	<p>Click Select Server to select a running server to configure a collection task and install Exporter.</p> <ul style="list-style-type: none">▪ On the Select Server page, search for servers by server ID, name, status, or IP address.▪ Ensure that the UniAgent of the selected server is running. Otherwise, no data can be collected.▪ If no server meets your requirements, UniAgent may be not installed. In that case, install UniAgent. In addition, ensure that the UniAgent version is 1.1.3 or later. Upgrade UniAgent when necessary.

Operation	Parameter	Description
Connect Elasticsearch Instance	Elasticsearch URL	<p>Elasticsearch connection address. Format: http://{username}:{password}@{IP}:{port}.</p> <ul style="list-style-type: none">▪ <i>{username}</i>: username for logging in to Elasticsearch.▪ <i>{password}</i>: password for logging in to Elasticsearch.▪ <i>{IP}:{port}</i>: Elasticsearch IP address and port number, for example, 10.0.0.1:3306. <p>Example: http://admin:*****@10.0.0.1:3306.</p>

- b. Click **Install & Test Collection Plug-in** to deliver the Exporter installation task.
 - After the plug-in is installed, click **Next**.
 - Click **View Log** to view Exporter installation logs if the installation fails.
3. Set an ingestion rule.
Set a metric ingestion rule by referring to the following table.

Table 6-42 Parameters

Operation	Parameter	Description
Metric Collection Rule	Metric Collection Interval (s)	Interval for collecting metrics, in seconds. Options: 10 , 30 , and 60 (default).
	Metric Collection Timeout (s)	<p>Timeout period for executing a metric collection task, in seconds. Options: 10, 30, and 60 (default).</p> <p>The timeout period cannot exceed the collection interval.</p>
	Executor	User who executes the metric ingestion rule, that is, the user of the selected server. By default, the executor is root .

Operation	Parameter	Description
Other	Custom Dimensions	<p>Dimensions (key-value pairs) added to specify additional metric attributes. You can click Add Dimension to add multiple custom dimensions (key-value pairs).</p> <ul style="list-style-type: none">– Key: key of the additional attribute of a metric. Only letters, digits, and underscores (_) are allowed. Each name must start with a letter or underscore. Each key must be unique.– Value: corresponds to the key of the additional attribute of a metric. The following characters are not allowed: & ><\$;'!-() <p>Up to 10 dimensions can be added. Example: Set the key to app and value to abc.</p>

After the metric collection rule parameters are configured, you can click **YAML** to view the configuration data in YAML format.

Step 4 Click **Next** to connect Elasticsearch Exporter.

After Elasticsearch Exporter is connected, perform the following operations if needed:

- Back to the access center to connect other data sources. For details, see [6.1 AOM Access Overview](#).
- Go to the **Access Management** page to view and manage the ingestion configuration of the Exporter. For details, see [6.6 Managing Metric and Log Ingestion](#).
- Go to the **Metric Browsing** page to analyze metrics. For details, see [7 Observability Metric Browsing](#).

-----End

6.3.11 Ingesting RabbitMQ Metrics to AOM

Install the RabbitMQ Exporter provided by AOM, and then create a collection task by setting a metric ingestion rule to monitor RabbitMQ metrics on a host.

Prerequisites

- [The UniAgent has been installed](#) and is running.
- [A Prometheus instance for ECS or a common Prometheus instance](#) has been created.
- To use the new RabbitMQ Exporter ingestion function, switch to the new access center.

Connecting RabbitMQ Exporter to AOM

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Access Center > Access Center**, filter the **RabbitMQ** card under **Self-built middleware**, and click **Ingest Metric (AOM)**.

Step 3 On the displayed page, set parameters.

1. Set the Prometheus instance.
 - a. **Instance Type:** Select a Prometheus instance type. Options: **Prometheus for ECS** and **Common Prometheus instance**.
 - b. **Instance Name:** Select a Prometheus instance from the drop-down list and click **Next**.

You can click **View Instance** to go to the details page of the selected instance. If no Prometheus instance is available, click **Create Instance** to [create a Prometheus instance for ECS or a common Prometheus instance](#).
2. Install the plug-in and test the connectivity.
 - a. Set parameters to install the plug-in by referring to the following table.

Table 6-43 Parameters

Operation	Parameter	Description
Basic Settings	Ingestion Rule Name	Name of a custom metric ingestion rule. Enter 1 to 50 characters starting with a letter. Only letters, digits, underscores (_), and hyphens (-) are allowed.
Set Collection Plug-in	OS	Operating system of the host. Only Linux is supported.
	Collection Plug-in	The default value is RabbitMQ Exporter . Select a plug-in version.
Select Server to Install Plug-in	Select Server	<p>Click Select Server to select a running server to configure a collection task and install Exporter.</p> <ul style="list-style-type: none">On the Select Server page, search for servers by server ID, name, status, or IP address.Ensure that the UniAgent of the selected server is running. Otherwise, no data can be collected.If no server meets your requirements, UniAgent may be not installed. In that case, install UniAgent. In addition, ensure that the UniAgent version is 1.1.3 or later. Upgrade UniAgent when necessary.

Operation	Parameter	Description
Connect RabbitMQ Instance	RabbitMQ Username	RabbitMQ username.
	RabbitMQ Password	RabbitMQ password.
	RabbitMQ Address	IP address and port number of RabbitMQ, for example, 10.0.0.1:3306 .

- b. Click **Install & Test Collection Plug-in** to deliver the Exporter installation task.
 - After the plug-in is installed, click **Next**.
 - Click **View Log** to view Exporter installation logs if the installation fails.
3. Set an ingestion rule.
Set a metric ingestion rule by referring to the following table.

Table 6-44 Parameters

Operation	Parameter	Description
Metric Collection Rule	Metric Collection Interval (s)	Interval for collecting metrics, in seconds. Options: 10 , 30 , and 60 (default).
	Metric Collection Timeout (s)	Timeout period for executing a metric collection task, in seconds. Options: 10 , 30 , and 60 (default). The timeout period cannot exceed the collection interval.
	Executor	User who executes the metric ingestion rule, that is, the user of the selected server. By default, the executor is root .

Operation	Parameter	Description
Other	Custom Dimensions	<p>Dimensions (key-value pairs) added to specify additional metric attributes. You can click Add Dimension to add multiple custom dimensions (key-value pairs).</p> <ul style="list-style-type: none">– Key: key of the additional attribute of a metric. Only letters, digits, and underscores (_) are allowed. Each name must start with a letter or underscore. Each key must be unique.– Value: corresponds to the key of the additional attribute of a metric. The following characters are not allowed: & ><\$;'!-() <p>Up to 10 dimensions can be added. Example: Set the key to app and value to abc.</p>

After the metric collection rule parameters are configured, you can click **YAML** to view the configuration data in YAML format.

Step 4 Click **Next** to connect RabbitMQ Exporter.

After RabbitMQ Exporter is connected, perform the following operations if needed:

- Back to the access center to connect other data sources. For details, see [6.1 AOM Access Overview](#).
- Go to the **Access Management** page to view and manage the ingestion configuration of the Exporter. For details, see [6.6 Managing Metric and Log Ingestion](#).
- Go to the **Metric Browsing** page to analyze metrics. For details, see [7 Observability Metric Browsing](#).

----End

6.4 Connecting Running Environments to AOM

AOM provides a unified entry for observability analysis of cloud services. Through the access center, you can ingest the metrics of running environments (such as ECS and CCE) to AOM and check documents related to log ingestion.

Procedure

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane on the left, choose **Access Center** > **Access Center** to go to the new access center.

If the old access center is displayed, click **Try New Version** in the upper right corner.

Step 3 Select the check box next to **Running environments** under **Types** to filter out the running environment cards.

Step 4 Click **Ingest Metric (AOM)** to quickly ingest metrics or click **Ingest Log (LTS) Details** to check documents related to log ingestion.

- **Ingest Metric (AOM):** AOM supports metric ingestion for running environments. By clicking **Ingest Metric (AOM)**, you can quickly ingest metrics of running environments.
- **Ingest Log (LTS) Details:** AOM provides an entry for ingesting logs of running environments to LTS.
 - By clicking **Details** on **Ingest Log (LTS) Details**, you can check the documents related to log ingestion. You can ingest logs according to the documents.
 - By clicking **Ingest Log (LTS)** on **Ingest Log (LTS) Details**, you can quickly ingest logs of running environments.

Table 6-45 Connecting running environments to AOM

Card	Related Operation
Elastic Cloud Server (ECS)	<p>ECS is a cloud server that allows on-demand allocation and elastic computing capability scaling. It helps you build a reliable, secure, flexible, and efficient application environment to ensure that your services can run stably and continuously, improving O&M efficiency. For details, see:</p> <ul style="list-style-type: none">• section "Ingesting ECS Text Logs to LTS" in the <i>Log Tank Service (LTS) User Guide</i>.• Ingesting ECS Metrics (AOM)
Cloud Container Engine (CCE)	<p>CCE is a high-performance, high-reliability service through which enterprises can manage containerized applications. CCE supports native Kubernetes applications and tools, allowing you to easily establish a container runtime environment on the cloud. For details, see:</p> <ul style="list-style-type: none">• CCE metric ingestion to AOM: By default, ICAgents are installed on CCE clusters upon your purchase. CCE cluster metrics will be automatically reported to AOM.• See section "Ingesting CCE Application Logs to LTS" in the <i>Log Tank Service (LTS) User Guide</i>.

----End

Connecting an ECS to AOM

Node Exporter is an open-source metric collection plug-in from Prometheus. It collects different types of data from target jobs and converts them into the time series data supported by Prometheus. Connect an ECS to AOM. Then you can install Node Exporter and configure collection tasks for the host group. The collected metrics will be stored in the Prometheus instance for ECS for easy management.

Constraints

A host supports only one Node Exporter.

Prerequisites

- You have connected a Prometheus instance for ECS or a common Prometheus instance. For details, see [12.2 Managing Prometheus Instances](#) or [5.4 Connecting Open-Source Monitoring Systems to AOM](#).
- A host group has been created. For details, see [5.2.7 \(New\) Managing Host Groups](#).

Procedure

1. Log in to the AOM 2.0 console.
2. In the navigation pane, choose **Access Center** > **Access Center**. Click **Try New Version** in the upper right corner of the page.
3. Locate the **Elastic Cloud Server (ECS)** card under **Running environments** and click **Ingest Metric (AOM)** on the card.
4. Set parameters for connecting to the ECS.
 - a. Select a Prometheus instance.
 - i. **Instance Type:** Select a Prometheus instance type. Options: **Prometheus for ECS** and **Common Prometheus instance**.
 - ii. **Instance Name:** Select a Prometheus instance from the drop-down list.

If no Prometheus instance is available, click [Create Instance](#) to create one.
 - b. Select a host group.
In the host group list, select a target host group.
 - If no host group is available, click [Create Host Group](#) to create one.
 - You can also perform editing, deletion, and other operations on the host group as needed. For details, see [6.2.7 \(New\) Managing Host Groups](#).

Collection configurations are delivered by host group. Therefore, it is easy for you to configure data collection for multiple hosts. When there is a new host, simply add it to a host group and the host will automatically inherit the log ingestion configurations associated with the host group.
 - c. Configure the collection.
Under **Configure Collection**, set parameters by referring to the following table.

Table 6-46 Collection configuration

Category	Parameter	Description
Basic Settings	Configuration Name	Name of a custom metric ingestion rule. Enter 1 to 50 characters starting with a letter. Only letters, digits, underscores (_), and hyphens (-) are allowed.
Metric Collection Rule	Metric Collection Interval (s)	Interval for collecting metrics, in seconds. Options: 10 , 30 , and 60 (default).
	Metric Collection Timeout (s)	Timeout period for executing a metric collection task, in seconds. Options: 10 , 30 , and 60 (default). The timeout period cannot exceed the collection interval.
	Executor	User who executes the metric ingestion rule, that is, the user of the selected host group. Default: root .
Other	Custom Dimensions	<p>Dimensions (key-value pairs) added to specify additional metric attributes. You can click Add Dimension to add multiple custom dimensions (key-value pairs).</p> <ul style="list-style-type: none"> • Key: key of the additional attribute of a metric. Enter 1 to 64 characters starting with a letter or underscore (_). Only letters, digits, and underscores are allowed. • Value: corresponds to the key of the additional attribute of a metric. <p>Up to 10 dimensions can be added. Example: Set the key to app and value to abc.</p>

Category	Parameter	Description
	Import ECS Tags as Dimensions	<p>Whether to import ECS tags as dimensions.</p> <ul style="list-style-type: none">• Disable: AOM does not write ECS tags (key-value pairs) into metric dimensions. ECS tag changes (such as addition, deletion, and modification) will not be synchronized to metric dimensions. This function is disabled by default.• Enable: AOM writes ECS tags (key-value pairs) into metric dimensions. ECS tag changes (such as addition, deletion, and modification) will be synchronized to metric dimensions.

5. After the configuration is complete, click **Next**. The ECS is then connected. After connecting to the ECS, perform the following operations if needed:
 - Go to the **Metric Browsing** page to analyze metrics. For details, see [7 Observability Metric Browsing](#).
 - Go to the **Access Management** page to view, edit, or delete the configured ingestion rule. For details, see [6.6 Managing Metric and Log Ingestion](#).
 - Go to the **Infrastructure Monitoring** > **Host Monitoring** page to view host monitoring information. For details, see [Host Monitoring](#).

6.5 Ingesting Data to AOM Using Open-Source APIs and Protocols

AOM provides a unified entry for observability analysis of cloud services. Through the access center, you can ingest metrics into AOM using open-source APIs and protocols, ingest traces to APM, and check documents related to log ingestion to LTS.

Procedure

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane on the left, choose **Access Center** > **Access Center** to go to the new access center.

If the old access center is displayed, click **Try New Version** in the upper right corner.
- Step 3** Select the check box next to **APIs/protocols...** under **Types** to filter out target cards.
- Step 4** Click **Ingest Metric (AOM)** to quickly ingest metrics, or click **Ingest Log (LTS) Details** to ingest logs or check documents related to log ingestion.

- **Ingest Metric (AOM):** AOM supports metric ingestion using open-source APIs and protocols. By clicking **Ingest Metric (AOM)**, you can quickly ingest metrics using open-source APIs and protocols.
- **Ingest Trace (APM):** AOM provides an entry for ingesting traces to APM using open-source APIs and protocols. By clicking **Ingest Trace (AOM)**, you can quickly ingest traces using open-source APIs and protocols.
- **Ingest Log (LTS) Details:** AOM provides an entry for ingesting logs to LTS using open-source APIs and protocols.
 - By clicking **Details** on **Ingest Log (LTS) Details**, you can check documents related to log ingestion. You can ingest logs according to the documents.
 - For some components, you can quickly ingest their logs by clicking **Ingest Log (LTS)**. For example, the **Cross-Account Ingestion - Log Stream Mapping** card.

Table 6-47 Ingesting data to AOM using open-source APIs and protocols

Card	Related Operation
AOM APIs	Use the open APIs of AOM to report metric data. For details, see section "Adding Monitoring Data" in the <i>Application Operations Management (AOM) API Reference</i> .
LTS APIs	Use the open APIs of LTS to report log data. For details, see section "Using APIs to Ingest Logs to LTS" in the <i>Log Tank Service (LTS) User Guide</i> .
Custom Prometheus Metrics	Ingest custom Prometheus metrics. For details, see Ingesting Custom Prometheus Metrics to AOM .

----End

Ingesting Custom Prometheus Metrics to AOM

You can ingest custom Prometheus metrics. They can be automatically reported to AOM.

- **Prerequisites**
 - You have connected a Prometheus instance for ECS or a common Prometheus instance. For details, see [12.2 Managing Prometheus Instances](#) or [5.4 Connecting Open-Source Monitoring Systems to AOM](#).
 - A host group has been created. For details, see [5.2.7 \(New\) Managing Host Groups](#).
- **Procedure**
 1. Log in to the AOM 2.0 console.
 2. In the navigation pane, choose **Access Center** > **Access Center**. Click **Try New Version** in the upper right corner of the page.

3. Click **Custom Prometheus Metrics** under **APIs/Protocols...**, and then click **Ingest Metric (AOM)** on the card to enter the configuration page.
4. Configure parameters for ingesting custom Prometheus metrics.
 - a. Select a Prometheus instance.
 - i. **Instance Type:** Select a Prometheus instance type. Options: **Prometheus for ECS** and **Common Prometheus instance**.
 - ii. **Instance Name:** Select a Prometheus instance from the drop-down list.
If no Prometheus instance is available, click [Create Instance](#) to create one.

- b. Select a host group.

In the host group list, select a target host group.

- If no host group is available, click [Create Host Group](#) to create one.
- You can also perform editing, deletion, and other operations on the host group as needed. For details, see [6.2.7 \(New\) Managing Host Groups](#).

Collection configurations are delivered by host group. Therefore, it is easy for you to configure data collection for multiple hosts. When there is a new host, simply add it to a host group and the host will automatically inherit the log ingestion configurations associated with the host group.

- c. Configure the collection.

Under **Configure Collection**, set parameters by referring to the following table.

Table 6-48 Parameters for configuring a collection task

Operation	Parameter	Description
Basic Settings	Configuration Name	Name of a custom metric ingestion rule. Enter 1 to 50 characters starting with a letter. Only letters, digits, underscores (_), and hyphens (-) are allowed.
Metric Collection Rule	Collection Target	Enter the target IP address and port number for collecting Prometheus metrics, for example, 10.0.0.1:3306 .
	Metric Collection Interval (s)	Interval for collecting metrics, in seconds. Options: 10 , 30 , and 60 (default).
	Metric Collection Timeout (s)	Timeout period for executing a metric collection task, in seconds. Options: 10 , 30 , and 60 (default). The timeout period cannot exceed the collection interval.

Operation	Parameter	Description
	Executor	User who executes the metric ingestion rule, that is, the user of the selected host group. By default, the executor is root .
Other	Custom Dimensions	<p>Dimensions (key-value pairs) added to specify additional metric attributes. You can click Add Dimension to add multiple custom dimensions (key-value pairs).</p> <ul style="list-style-type: none">• Key: key of the additional attribute of a metric. Enter 1 to 64 characters starting with a letter or underscore (_). Only letters, digits, and underscores are allowed.• Value: corresponds to the key of the additional attribute of a metric. <p>A maximum of 10 custom dimensions can be added. Example: Set the key to app and value to abc.</p>

After the parameters are configured, you can click **YAML** to view the configuration data in YAML format.

5. After the configuration is complete, click **Next**. The custom Prometheus metrics can then be ingested.

After ingesting custom Prometheus metrics, you can perform the following operations:

- Go to the **Metric Browsing** page to analyze metrics. For details, see [7 Observability Metric Browsing](#).
- Go to the **Access Management** page to view, edit, or delete the configured ingestion rule. For details, see [6.6 Managing Metric and Log Ingestion](#).

6.6 Managing Metric and Log Ingestion

After ingesting metrics to AOM and logs to LTS in the access center, you can manage ingestion rules on the **Access Management** page.

Constraints

- AOM provides both old and new access management functions. To switch from the **old function** to the new function, click **Try New Version** in the upper right corner of the **Access Center** page and then go to the **Access Management** page.
- To use LTS functions on the AOM console, obtain the LTS permissions in advance. For details, see section "Permissions" in the *Log Tank Service (LTS) User Guide*.



- To use the log ingestion rule function on the AOM 2.0 console, enable LTS first.

Managing Metric Ingestion Rules

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane on the left, choose **Access Center > Access Management**. The **Metric Ingestion Rules** tab page is displayed.
- Step 3** Click **Ingest Metric**. In the dialog box, select a target card. For details, see [6.1 AOM Access Overview](#).
- Step 4** After the ingestion is complete, check the rule on the **Metric Ingestion Rules** tab page under **Access Management**.

Perform the operations listed in [Table 6-49](#) if needed.

Table 6-49 Related operations

Operation	Description
Searching for a metric ingestion rule	Search for metric ingestion rules by Ingestion Configuration , Ingestion Type , or Status in the search box. Alternatively, enter a keyword to search for a metric ingestion rule.
Refreshing the metric ingestion rules list	Click  in the upper right corner of the list to refresh current metric ingestion rules.
Setting the metric ingestion rule list	Click  in the upper right corner of the list. In the displayed dialog box, customize column display. <ul style="list-style-type: none">• Basic settings<ul style="list-style-type: none">– Table Text Wrapping: If you enable this function, excess text will move down to the next line; otherwise, the text will be truncated.– Operation Column: If you enable this function, the Operation column is always fixed at the rightmost position of the table.• Custom Columns: Select or deselect the columns to display.
Editing a metric ingestion rule	Click Edit in the Operation column to modify a metric ingestion rule. For details, see 6.1 AOM Access Overview .
Deleting a metric ingestion rule	<ul style="list-style-type: none">• To delete a metric ingestion rule, click Delete in the Operation column.• To delete one or more metric ingestion rules, select them and click Delete above the list.

Operation	Description
Enabling or disabling a metric ingestion rule	<ul style="list-style-type: none">• Enable or disable the rule in the Status column.• To enable or disable one or more rules, select them and click Enable or Disable above the list.
Viewing the associated Prometheus instance	Click an instance in the Instance Name column to go to the instance details page.

----End

Managing Log Ingestion Rules

AOM is a unified platform for observability analysis of cloud services. It does not provide log functions by itself. Instead, it integrates the log ingestion rule function of Log Tank Service (LTS). You can perform operations on the AOM 2.0 or LTS console.

Table 6-50 Description

Function	Description	AOM 2.0 Console	LTS Console	References
Log ingestion rules	Logs can be ingested through ICAgents, cloud services, APIs, and SDKs. After logs are ingested, they are displayed in a simple and orderly manner on the console and can be queried easily.	<ol style="list-style-type: none">1. Log in to the AOM 2.0 console.2. In the navigation pane on the left, choose Access Center > Access Management.3. Click the Log Ingestion Rules tab.	<ol style="list-style-type: none">1. Log in to the LTS console.2. In the navigation pane on the left, choose Log Ingestion > Ingestion Management.	Section "Log Ingestion" in the <i>Log Tank Service (LTS) User Guide</i>

7 Observability 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 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. For details about how to set monitoring conditions, see [Table 8-3](#).

- Select metrics from all metrics.

After selecting a target metric, you can set condition attributes to filter information.

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

- 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 [9.3.8 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. 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 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](#). **Up to 200 metric data records can be displayed in a line graph.**

----End

Related 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. 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.
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.

8 Dashboard Monitoring

8.1 AOM Dashboard Overview

Dashboards enable you to monitor metrics in real time. You can create dashboards for metrics, so that monitoring data can be displayed in graphs on the monitoring panel. This helps you monitor and analyze metrics.

Function Introduction

Table 8-1 Function introduction

Function	Description
8.2 Creating a Dashboard	With a dashboard, different graphs are displayed on the same screen, so you can view metrics comprehensively.
8.3 (New) Creating a Dashboard	With a dashboard, different graphs are displayed on the same screen, so you can view metrics comprehensively.
8.4 Setting Full-Screen Online Duration for an AOM Dashboard	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.
8.5 Adding AOM Dashboard Filters	You can customize filters by adding variables to filter monitoring data when viewing or adding graphs on the Dashboard page.
8.6 (New) Setting Filters for AOM Dashboards	Add filters to new AOM dashboards to filter statistical graphs based on specified conditions. Filters are used to modify query criteria for statistical graphs in new dashboards in batches. Each statistical graph is actually the results of a query and analysis statement.

Constraints

- 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.
- Up to 50 graphs can be added to a dashboard.
- Up to 200 metric data records can be displayed in a line graph.
- Only one resource can be displayed on a digit graph.

8.2 Creating a Dashboard

With a dashboard, different graphs are displayed on the same screen, so you can view metrics comprehensively.

Creating a Dashboard


- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane, choose **Dashboard > Dashboard**. (To switch from the new dashboard to the old one, click **Back to Old Version** in the upper right corner.)
- 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 8-2 Parameters for creating a dashboard

Parameter	Description
Dashboard Name	Name of a dashboard. Enter a maximum of 255 characters. The following special characters are not allowed: "\$# %&'+'<=>?\\"
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 dimmed and cannot be changed.• To use the enterprise project function, contact engineers.

Parameter	Description
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. Enter a maximum of 255 characters. The following special characters are not allowed: "\$# %&'<=>?\\"

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 [8.7 Graph Description](#). The data can be metric data. Select a graph type as required.

- Add a metric graph. Set parameters by referring to [Table 8-3](#). Then click **Save**.

Table 8-3 Adding a metric graph

Parameter	Description
Graph Name	Name of a graph to distinguish it from other graphs. For graph names, variables can be added to dynamically filter graph information. Duplicate names are supported. Enter a maximum of 255 characters. The following special characters are not allowed: "\$# %&'<=>?\\"
Data Source	The default value is Metric Sources .
Graph Type	Options: line, digit, top N, table, bar, and digital line.
How to Add	Add metrics as required. You can select metrics from All metrics or using Prometheus statements.

Parameter	Description
All metrics	<p>Select target metrics from the metric drop-down list.</p> <ul style="list-style-type: none"> – Calculation method: <ul style="list-style-type: none"> ▪ Multiple Metrics: Performs calculation for metrics and their conditions separately, and displays the results on the graph. ▪ Combined Operations: Performs calculation on multiple metrics and their conditions based on expressions, and displays the results on the graph. – Metric: Select a target metric from the drop-down list. You can also directly enter a metric name in the search box and click Generate. If no metric is reported, configure one. – Statistical Period: Interval at which metric data is collected. The statistical periods that are available for you to select vary according to the time range. For details, see Relationship Between the Time Range and Statistical Period. If you use new dashboards, see Relationship between the time range and statistical period. – Condition: Metric monitoring scope. Each metric condition is in "key:value" format and can be selected from the drop-down list. You can also enter a dimension name and value, and click Generate to add a metric condition. You can also click  and select AND or OR to add more conditions for the metric. – 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. – Formatted Legend Name: Use a fixed name or variable as the legend name. <ul style="list-style-type: none"> ▪ Format: <i>{{dimension name}}</i>. ▪ If the displayed legend name is {{dimension name}}, there is no dimension. For example, enter {{hostname}} and a host name will be displayed as the legend name. ▪ Tables and digit/line graphs do not support Formatted Legend Name. <p>You can click Add Metric to add more metrics. A maximum of 100 can be added.</p>

Parameter	Description
Prometheus statement	<p>Add metric data by entering a Prometheus statement related to the metric.</p> <ul style="list-style-type: none"> – Prometheus Statement: See 9.3.8 Prometheus Statements. – Formatted Legend Name: Use a fixed name or variable as the legend name. If the displayed legend name is {{dimension name}}, there is no dimension. Format: <i>{{dimension name}}</i>. For example, enter {{hostname}} and a host name will be displayed as the legend name. <p>You can click Add Prometheus Statement to add up to 100 metrics.</p>
Graph Settings	<p>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.</p> <p>If you create a dashboard of the new version, see Metric Data Graphs.</p>
Statistic	<p>Method used to measure metrics. Options: Avg, Min, Max, Sum, and Samples.</p>
Time Range	<p>Time range in which metric data is collected. Options: Last 30 minutes, Last hour, Last 6 hours, Last day, Last week, and Custom.</p> <p>If you use new dashboards, you can select From now, From last, and Specified.</p> <ul style="list-style-type: none"> – From now: queries data generated in a time range that ends with the current time, such as the previous 1, 5, or 15 minutes. For example, if the current time is 19:20:31 and 1 hour is selected as the relative time from now, the graphs on the dashboard display the data that is generated from 18:20:31 to 19:20:31. – From last: queries data generated in a time range (on the hour) that ends with the current time, such as the previous 1 or 15 minutes. For example, if the current time is 19:20:31 and 1 hour is selected as the relative time from last, the graphs on the dashboard display the data that is generated from 18:00:00 to 19:00:00. – Specified: queries data that is generated in a specified time range.
Refresh Frequency	<p>Interval at which the metric data is refreshed. Options: Refresh manually, 30 seconds auto refresh, 1 minute auto refresh, and 5 minutes auto refresh.</p>








Step 4 Click **Save**. 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 8-4](#).

Table 8-4 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"> In the dashboard list, click a dashboard name. Go to the dashboard page and click a dashboard name in the upper left corner. Move the cursor to the target dashboard group and choose  > Modify to change the group name.
Deleting a dashboard group	<p>You can delete a dashboard through either of the following entries:</p> <p>Entry 1:</p> <ol style="list-style-type: none"> In the dashboard list, click a dashboard name. Go to the dashboard page and click a dashboard name in the upper left corner. Move the cursor to the target dashboard group and choose  > Delete. In the displayed dialog box, click OK. <p>Entry 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>

Operation	Description
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 .
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 .
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.

Operation	Description
Adding alarm rules	<ul style="list-style-type: none"> Adding an alarm rule when adding a graph <ol style="list-style-type: none"> Click Add Graph on the page or click  in the upper right corner of the page. 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 9.3.2 Creating an AOM Metric Alarm Rule. Adding an alarm rule when modifying a graph <ol style="list-style-type: none"> Locate a target dashboard, move the cursor to the upper right corner of a graph, and choose  > Modify. 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 9.3.2 Creating an AOM 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 .
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 8.4 Setting Full-Screen Online Duration for an AOM Dashboard .
Setting a dashboard	Click a target dashboard and click  in the upper right corner of the dashboard details page. For details, see 8.5 Adding AOM Dashboard Filters .
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	<p>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:</p> <p>Method 1: In the dashboard list, locate a dashboard, and choose  > Export Dashboard in the Operation column.</p> <p>Method 2: Click a dashboard to go to its details page and choose  > Export Dashboard in the upper right corner.</p>

Operation	Description
Importing a dashboard	<p>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:</p> <p>Method 1: On the Dashboard page, click Import Dashboard.</p> <p>Method 2: In the dashboard group list, locate the group to which the dashboard is to be imported, and choose ... > Import Dashboard.</p> <p>Procedure:</p> <ol style="list-style-type: none">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 8-2.3. Click OK.
Exporting a monitoring report	<p>Select the target dashboard, click  in the upper right corner of the Dashboard page, and click Export Line Graph Report to export the line graph as a CSV file for local storage and further analysis.</p>

Relationship Between the Time Range and Statistical Period

In AOM, a maximum of 1,440 data points can be returned for a single metric query. The relationship between the time range and statistical period is as follows:

Maximum time range = Statistical period x 1,440

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 8-5 Relationship between the time range and statistical period

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

Time Range	Statistical Period
Custom	1 minute, 5 minutes, 15 minutes, or 1 hour

8.3 (New) Creating a Dashboard

With a dashboard, different graphs are displayed on the same screen, so you can view metrics comprehensively.

Constraints

The graph configurations of new dashboards are different from those of old dashboards.

- Old dashboards are incompatible with the graph configurations of new dashboards.
- However, new dashboards are compatible with the graph configurations of old dashboards.

Procedure

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane on the left, choose **Dashboard > Dashboard**. Click **Try New Version** in the upper right corner of the page.

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 8-6 Parameters for creating a dashboard

Parameter	Description
Dashboard Name	Name of a dashboard. Enter a maximum of 255 characters. The following special characters are not allowed: "\$# %&'<=>?\\"

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 dimmed and cannot be changed. • To use the enterprise project function, contact engineers.
Group Type	<p>Options: Existing and New.</p> <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. Enter a maximum of 255 characters. The following special characters are not allowed: "\$# %&'+'<=>?\\"

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 [8.8 \(New\) Graphs](#). The data can be metric or log data. Select a graph type as required.

- Adding a metric graph: Set parameters by referring to [Table 8-7](#) and click **Save**.

Table 8-7 Adding a metric graph

Parameter	Description
Graph Name	Name of a graph to distinguish it from other graphs. For graph names, variables can be added to dynamically filter graph information. Duplicate names are supported. Enter a maximum of 255 characters. The following special characters are not allowed: "\$# %&'<=>?\\"
Data Source	The default value is Metric Sources .
Graph Type	Options: line, digit, top N, table, bar, and digital line.
How to Add	Add metrics as required. You can select metrics from All metrics or using Prometheus statements.

Parameter	Description
All metrics	<p>Select target metrics from the metric drop-down list.</p> <ul style="list-style-type: none"> – Calculation method: <ul style="list-style-type: none"> ▪ Multiple Metrics: Performs calculation for metrics and their conditions separately, and displays the results on the graph. ▪ Combined Operations: Performs calculation on multiple metrics and their conditions based on expressions, and displays the results on the graph. – Metric: Select a target metric from the drop-down list. You can also directly enter a metric name in the search box and click Generate. If no metric is reported, configure one. – Statistical Period: Interval at which metric data is collected. The statistical periods that are available for you to select vary according to the time range. For details, see Relationship Between the Time Range and Statistical Period. If you use new dashboards, see Relationship between the time range and statistical period. – Condition: Metric monitoring scope. Each metric condition is in "key:value" format and can be selected from the drop-down list. You can also enter a dimension name and value, and click Generate to add a metric condition. You can also click  and select AND or OR to add more conditions for the metric. – 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. – Formatted Legend Name: Use a fixed name or variable as the legend name. <ul style="list-style-type: none"> ▪ Format: <i>{{dimension name}}</i>. ▪ If the displayed legend name is {{dimension name}}, there is no dimension. For example, enter {{hostname}} and a host name will be displayed as the legend name. ▪ Tables and digit/line graphs do not support Formatted Legend Name. <p>You can click Add Metric to add more metrics. A maximum of 100 can be added.</p>

Parameter	Description
Prometheus statement	<p>Add metric data by entering a Prometheus statement related to the metric.</p> <ul style="list-style-type: none"> – Prometheus Statement: See 9.3.8 Prometheus Statements. – Formatted Legend Name: Use a fixed name or variable as the legend name. If the displayed legend name is {{dimension name}}, there is no dimension. Format: <i>{{dimension name}}</i>. For example, enter {{hostname}} and a host name will be displayed as the legend name. <p>You can click Add Prometheus Statement to add up to 100 metrics.</p>
Graph Settings	<p>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.</p> <p>If you create a dashboard of the new version, see Metric Data Graphs.</p>
Statistic	<p>Method used to measure metrics. Options: Avg, Min, Max, Sum, and Samples.</p>
Time Range	<p>Time range in which metric data is collected. Options: Last 30 minutes, Last hour, Last 6 hours, Last day, Last week, and Custom.</p> <p>If you use new dashboards, you can select From now, From last, and Specified.</p> <ul style="list-style-type: none"> – From now: queries data generated in a time range that ends with the current time, such as the previous 1, 5, or 15 minutes. For example, if the current time is 19:20:31 and 1 hour is selected as the relative time from now, the graphs on the dashboard display the data that is generated from 18:20:31 to 19:20:31. – From last: queries data generated in a time range (on the hour) that ends with the current time, such as the previous 1 or 15 minutes. For example, if the current time is 19:20:31 and 1 hour is selected as the relative time from last, the graphs on the dashboard display the data that is generated from 18:00:00 to 19:00:00. – Specified: queries data that is generated in a specified time range.
Refresh Frequency	<p>Interval at which the metric data is refreshed. Options: Refresh manually, 30 seconds auto refresh, 1 minute auto refresh, and 5 minutes auto refresh.</p>





Step 4 Click **Save**. 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 8-8](#).




Table 8-8 Related operations

Operation	Description
Setting column display	<p>Click  in the upper right corner of the dashboard list. In the displayed dialog box, customize column display.</p> <ul style="list-style-type: none">• Basic Settings<ul style="list-style-type: none">– Table Text Wrapping: If you enable this function, excess text will move down to the next line; otherwise, the text will be truncated.– Operation Column: If you enable this function, the Operation column is always fixed at the rightmost position of the table.• Custom Columns: Select or deselect the columns to display.
Adding dashboards to favorites	<p>In the dashboard list, locate a dashboard and click Add to Favorites in the Operation column.</p>
Moving dashboards to another group	<ul style="list-style-type: none">• Move a dashboard group.<ul style="list-style-type: none">– In the dashboard list, locate a dashboard and click Move in the Operation column.– Click a dashboard in the dashboard list to access the dashboard page. In the upper left corner, locate the target dashboard, and choose  > Move.• To move multiple dashboards, select them and click Move above the list.
Deleting a dashboard	<ul style="list-style-type: none">• In the dashboard list, locate a dashboard and click Delete in the Operation column.• Click a dashboard in the dashboard list to access the dashboard page. In the upper left corner, locate the target dashboard, and choose  > Delete.• Click a dashboard in the dashboard list to access the dashboard page. In the upper right corner, click . In the displayed dialog box, click OK.

Operation	Description
Changing a dashboard group name	<ol style="list-style-type: none"> 1. Click a dashboard in the dashboard list to access the dashboard page. 2. In the upper left corner, locate the target dashboard. 3. Choose  > Modify to change the group name.
Deleting a dashboard group	<p>You can delete a dashboard through either of the following entries:</p> <p>Entry 1:</p> <ol style="list-style-type: none"> 1. Click a dashboard in the dashboard list to access the dashboard page. 2. In the upper left corner, locate the target dashboard. 3. Choose  > Delete. 4. In the displayed dialog box, click OK. <p>Entry 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 a dashboard in the dashboard list to access the dashboard page. In the upper right corner, click . 2. Move the pointer to the upper right corner of a graph and choose  > Delete. 3. Click .
Relocating a graph on a dashboard	<ol style="list-style-type: none"> 1. Click a dashboard in the dashboard list to access the dashboard page. In the upper right corner, click . 2. Move the cursor into the target graph and move it to any position in the dashboard. 3. Click .
Full-screen display	Click a dashboard in the dashboard list to access the dashboard page. In the upper right corner, click  .
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 a dashboard in the dashboard list to access the dashboard page. In the upper right corner, click  .
Auto refresh	Click a dashboard in the dashboard list to access the dashboard page. In the upper right corner, click the arrow next to  and select a refresh mode or frequency. Options: Refresh now , Refresh every 5 seconds , Refresh every 10 seconds , Refresh every 30 seconds , and Refresh every 1 minute .

Operation	Description
Manually refreshing a graph	Click the target dashboard, move the cursor to the upper right corner of a graph, and choose  > Refresh .
Modifying a graph	<ol style="list-style-type: none"> Click the target dashboard, move the cursor to the upper right corner of a graph, and choose  > Edit to modify the graph. For details, see Adding a Graph to a Dashboard. Click Save. 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"> Click Add Graph on the page or click  in the upper right corner of the page. 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 9.3.2 Creating an AOM Metric Alarm Rule. Adding an alarm rule when modifying a graph <ol style="list-style-type: none"> Locate a target dashboard, move the cursor to the upper right corner of a graph, and choose  > Modify. 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 9.3.2 Creating an AOM Metric Alarm Rule.
Rotating dashboards	Click a dashboard in the dashboard list to access the dashboard page. In the upper right corner, click  . Set full-screen display by referring to 8.4 Setting Full-Screen Online Duration for an AOM Dashboard .
Setting a dashboard	Click a dashboard in the dashboard list to access the dashboard page. In the upper right corner, click  . For details, see 8.6 (New) Setting Filters for AOM Dashboards .

Operation	Description
Setting the query time	<p>Click a dashboard in the dashboard list to access the dashboard page. In the upper right corner, click the time selection box to set a time range to query. Options: From now, From last, and Specified.</p> <ul style="list-style-type: none"> • From now: queries data generated in a time range that ends with the current time, such as the previous 1, 5, or 15 minutes. For example, if the current time is 19:20:31 and 1 hour is selected as the relative time from now, the graphs on the dashboard display the data that is generated from 18:20:31 to 19:20:31. • From last: queries data generated in a time range (on the hour) that ends with the current time, such as the previous 1 or 15 minutes. For example, if the current time is 19:20:31 and 1 hour is selected as the relative time from last, the graphs on the dashboard display the data that is generated from 18:00:00 to 19:00:00. • Specified: queries data that is generated in a specified time range.
Exporting a dashboard	<p>Click a dashboard in the dashboard list to access the dashboard page. In the upper right corner, click  and click Export Dashboard to export the metric graph data in JSON format and save the data to the local PC for further analysis.</p>
Importing a dashboard	<p>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:</p> <p>Method 1: On the Dashboard page, click Import Dashboard.</p> <p>Method 2: In the dashboard group list, locate a target dashboard group and choose ... > Import Dashboard.</p> <p>Procedure:</p> <ol style="list-style-type: none"> 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 Step 5. 3. Click OK.
Exporting a monitoring report	<p>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.</p>

Operation	Description
Copying a dashboard	<ol style="list-style-type: none">1. Click a target system built-in dashboard or custom dashboard and then click  in the upper right corner of the dashboard details page.2. In the dialog box that is displayed, set information such as the dashboard name by referring to Step 5.3. After the settings are complete, click OK.
Setting a dashboard group	<ol style="list-style-type: none">1. Click a target dashboard and click Add Chart Pane in the upper right corner of the dashboard details page to create a group.2. Click  next to the created group to set a group name.3. Select a graph and then drag it into the corresponding group. When dragging a graph, left-click the graph and then drag it as required. If only one group is created, all graphs are in that group by default. If there are multiple groups, drag graphs into the desired group as needed.4. Click  in the upper right corner of the dashboard page to save.

Relationship Between the Time Range and Statistical Period (for New Dashboards)

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:

Maximum time range = Statistical period × 1,440

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 8-9 (New) Relationship between the time range and statistical period

Type	Time Range	Statistical Period
From now	1 minute	1 minute or 5 minutes
	5 minutes	
	15 minutes	
	30 minutes	
	1 hour	

Type	Time Range	Statistical Period
	4 hours	1 minute, 5 minutes, 15 minutes, or 1 hour
	1 day	
	Today	
	1 week	1 hour
	This week	
	30 days	
	This month	
	Specified	1 minute, 5 minutes, 15 minutes, or 1 hour
From last	1 minute	1 minute or 5 minutes
	15 minutes	
	30 minutes	
	1 hour	
	4 hours	1 minute, 5 minutes, 15 minutes, or 1 hour
	1 day	
	1 week	1 hour
	30 days	
	Today	1 minute, 5 minutes, 15 minutes, or 1 hour
	Yesterday	
	Two days ago	
	This week	1 hour
	Last week	
	This month	
	Last month	
	Specified	1 minute, 5 minutes, 15 minutes, or 1 hour
Custom	Custom	1 minute, 5 minutes, 15 minutes, or 1 hour

8.4 Setting Full-Screen Online Duration for an AOM Dashboard

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.

Constraints

- 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 > Dashboard**. If you want to use new dashboards, choose **Dashboard** in the navigation pane and then click **Try New Version** in the upper right corner of the page.
- 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 8-10](#).

Table 8-10 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

8.5 Adding AOM Dashboard Filters


You can customize filters by adding variables to filter monitoring data when viewing or adding graphs on the **Dashboard** page.

Adding Variables

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Dashboard > Dashboard**. (To switch from the new dashboard to the old one, click **Back to Old Version** in the upper right corner.)

To use the new dashboard function, choose **Dashboard** in the navigation pane and then click **Try New Version** in the upper right corner of the page. For details about the filters of the new dashboard, see [8.6 \(New\) Setting Filters for AOM Dashboards](#).

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 8-11](#).

Table 8-11 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. Enter up to 1,024 characters.
Data Source	Source of the data. Select a data source on the Dashboard page. It is dimmed here and cannot be selected. The default Prometheus instance is selected by default.
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 8-12](#) if needed.

Table 8-12 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 8-11 .
Deleting a variable	Click  in the Operation column of the target variable. In the displayed dialog box, click Yes .
Filling a dashboard graph name with variables	Dashboards support the function of filling graph names using variables. After variables are added, dashboard graph names can be filled using <code>\${variable name}</code> during graph name configuration . The graph name is dynamically displayed based on the variable value you select from the drop-down list. For example, if the original graph name is Dashboard and the new variable is <i>ClusterName</i> , you can set the dashboard graph name to <code>\${ClusterName} Dashboard</code> . Then, select values from the drop-down list of ClusterName . These values will be dynamically combined with the original dashboard graph name for display.

8.6 (New) Setting Filters for AOM Dashboards

Add filters to new AOM dashboards to filter statistical graphs based on specified conditions. Filters are used to modify query criteria for statistical graphs in new dashboards in batches. Each statistical graph is actually the results of a query and analysis statement.

AOM supports the following types of filters:


- Custom variable: You can set static or dynamic variable values and use them in query statements for batch statement modification. In this way, you can filter statistical graphs based on custom variables.

Configuring a Filter of the Custom Variable Type

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane on the left, choose **Dashboard > Dashboard**. Click **Try New Version** in the upper right corner of the page.

Step 3 Click a dashboard to go to its details page.

Step 4 Click  in the upper right corner of the dashboard details page. The **Dashboard Settings** page is displayed.

Step 5 Click **Create**. On the page that is displayed, set parameters for the filter of the custom variable type.

1. Configure a filter of the custom variable type by referring to the following table.

Table 8-13 Basic information

Parameter	Description
Name	Name of a filter. Each name must be unique. Enter up to 255 characters and do not start or end with an underscore (_). Only digits, letters, and underscores are allowed.
Alias	(Optional) Alias of the filter. Enter up to 255 characters and do not start or end with an underscore (_) or hyphens (-). Only digits, letters, hyphens, and underscores are allowed. After the filter alias is set, it is displayed preferentially.
Description	(Optional) Description of the filter. Enter up to 1,000 characters.
Type	Type of the filter. Select Custom variable . You can set static or dynamic variable values and use them in query statements for batch statement modification.

2. (Optional) Configure a static variable value for the filter of the custom variable type.
 - a. Click **Add Static Variable Value** in the **Static Variable Value** area.
 - b. Configure a static variable by referring to the following table.


Table 8-14 Static variable configuration

Parameter	Description
Value	Field value of the static variable. Enter up to 255 characters and do not start or end with an underscore (_). Only digits, letters, and underscores are allowed.
Alias	(Optional) Alias of the field value of the static variable. Enter up to 64 characters. Only letters, digits, hyphens (-), underscores (_), and periods (.) are allowed. Do not start with a period or underscore or end with a period. After an alias is set, it will be displayed preferentially.
Default Value	Whether to use the value of the static variable as the default value. (If an alias has been set, the alias will be displayed preferentially): <ul style="list-style-type: none">▪ Enable: The value of the static variable is automatically selected as the default value of the filter.▪ Disable: The value of the static variable is not automatically selected as the default value of the filter.

To delete a static variable value, click **Delete** in the **Operation** column.

3. (Optional) Configure a dynamic variable value for the filter of the custom variable type.
 - a. Toggle on **Dynamic Variable Value**.
 - b. Configure the source of the dynamic variable value:
 - **Prometheus instance:** Query dynamic variable values from a Prometheus instance.
 - c. Configure dynamic variable parameters.
 - When **Dynamic Variable Value Source** is set to **Prometheus instance**, set parameters by referring to the following table.

Table 8-15 Dynamic variable configuration (source: Prometheus instance)

Parameter	Description
Prometheus instance	Prometheus instance from which dynamic variable values are queried. By default, the Prometheus instance selected in the upper left corner after you access the dashboard details page is used. This parameter is grayed here and cannot be selected. To change the Prometheus instance, select another Prometheus instance on the dashboard details page.
Query Method	Option: Metric field match .
Metric Name	Select a metric under the selected Prometheus instance.
Variable Display Field	Select a field of the metric to display. The values corresponding to this field will be displayed in the dashboard filter drop-down list. Example: If this parameter is set to Cluster Name , specific cluster names will be displayed in the dashboard filter drop-down list.
Variable Value Field	Select an actual field for filtering. For example, if Variable Display Field is set to Cluster Name and Variable Value Field is set to Cluster ID , when you select a cluster name from the dashboard filter drop-down list, the actual cluster ID will be used as the criterion for filtering.
Filter Criteria	Configure a dimension name and value. The = and != operators are supported. You can click  to use AND to set multiple filter criteria for the same metric.
Sort By	Configure how the options will be displayed in the dashboard filter drop-down list. Option: None .

4. Configure other information about the filter of the custom variable type.
 - **Default Value:** Configure the default value of the filter. You can select the static or dynamic variable values configured in [2](#) or [3](#).
 - **Multi-Option Allowed:** Whether multiple options can be selected for the filter. This function is enabled by default. After this function is enabled, multiple options are selectable for the filter.
 - **Include "Select All":** Whether the **Select All** option is available in the drop-down list. This function is enabled by default. After this function is enabled, the **Select All** option is selectable.
5. Click **Preview** to preview your filter settings.

Step 6 Click **OK** to create a filter of the custom variable type.


The new filter is displayed on the dashboard details page and the page for adding a graph. You can click the filter and enter a criterion in the search box or select a criterion from the drop-down list to filter statistical graphs in a dashboard.

----End

More Operations

After a filter is created, perform the operations listed in [Table 8-16](#) on the **Dashboard Settings** page if needed.

Table 8-16 More operations

Parameter	Description
Searching for a filter	Search for filters by name, alias, type, or description. Enter or select a keyword in the search box above the filter list and click  to search.
Editing a filter	Click Modify in the Operation column that contains the target filter.
Deleting a filter	Click Delete in the Operation column that contains the target filter. In the dialog box that is displayed, click Yes .
Using a filter to fill in a dashboard graph title	After a filter is added, use <i>`\${Filter name}`</i> to dynamically fill in a dashboard graph title . (If an alias has been configured for the filter, it will be used preferentially.) The graph title can then be dynamically displayed based on the filter drop-down list values. For example, if the original graph name is Dashboard and the new filter is <i>ClusterName</i> , you can set the dashboard graph name to <i>`\${ClusterName}` Dashboard</i> . Then, select values from the drop-down list of ClusterName . These values will be dynamically combined with the original dashboard graph name for display.

8.7 Graph Description

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

Metric Data Graphs

Metric data graphs support the following types: **line**, **number**, **top N**, **table**, **bar**, and **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. The following figure shows the CPU usage of different hosts.

Figure 8-1 Line graph

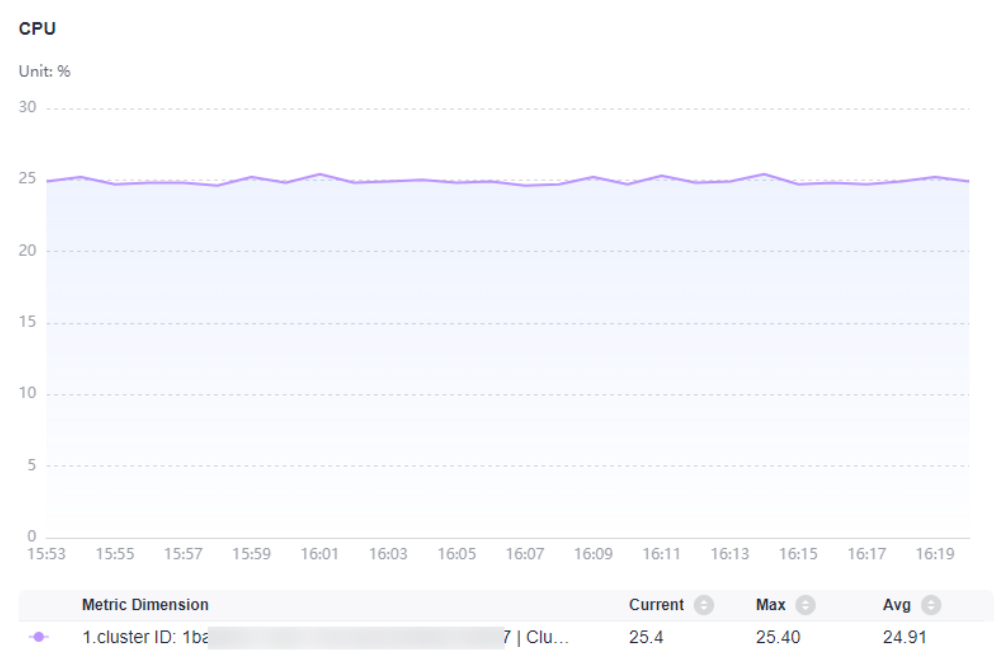


Table 8-17 Line graph parameters

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.

Category	Parameter	Description
	Hide Y Axis Label	Whether to hide the Y axis label.
	Display Background	If this option is enabled, the background will be displayed in the line graph.
	Y Axis Range	Value range of the Y axis.
Advanced Settings	Left Margin	Distance between the axis and the left boundary of the graph.
	Right Margin	Distance between the axis and the right boundary of the graph.
	Top Margin	Distance between the axis and the upper boundary of the graph.
	Bottom Margin	Distance between the axis and the lower boundary of the graph.

- **Digit graph:** highlights a single value. It can display the latest value and the growth or decrease rate of a resource in a specified period. Use this type of graph to monitor the latest value of a metric in real time.

As shown in the following figure, you can view the CPU usage of the host in real time. **2.85%** indicates the latest CPU usage, and **-0.08%** indicates the decrease rate in the current monitoring period.

Figure 8-2 Digit graph

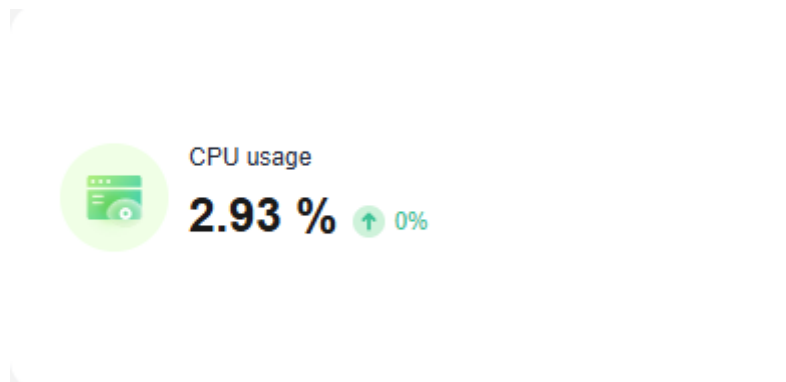


Table 8-18 Digit graph parameters

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.

In the following graph, the top 5 hosts with the highest CPU usage are displayed.

Figure 8-3 Top N graph

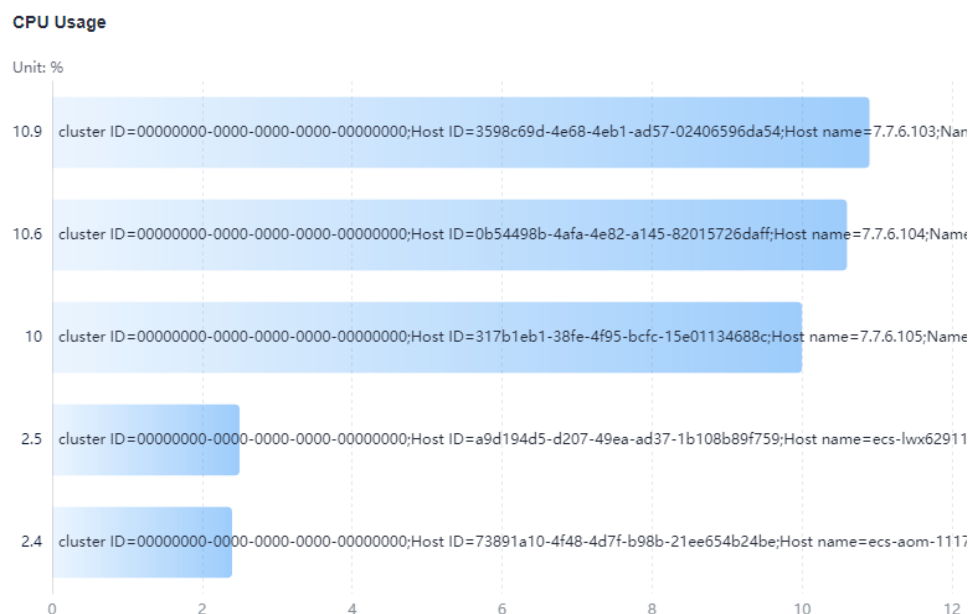


Table 8-19 Top N graph parameters

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.
	Show Value	After this function is enabled, the value on the Y axis is displayed.

Category	Parameter	Description
	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.
In the following figure, you can view the CPU usage of different hosts in a table.

Figure 8-4 Table
CPU Usage

Metric Na...	cluster ID	Host ID	Host name	Namespace	Host IP	Node Name	Value
CPU us...	000000...	0b5449...		default			10.3
CPU us...	000000...	195e90...		default			1.6
CPU us...	000000...	317b1e...		default			9.7
CPU us...	000000...	3598c6...		default			10.5

Table 8-20 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 in a graph.

Figure 8-5 Bar graph

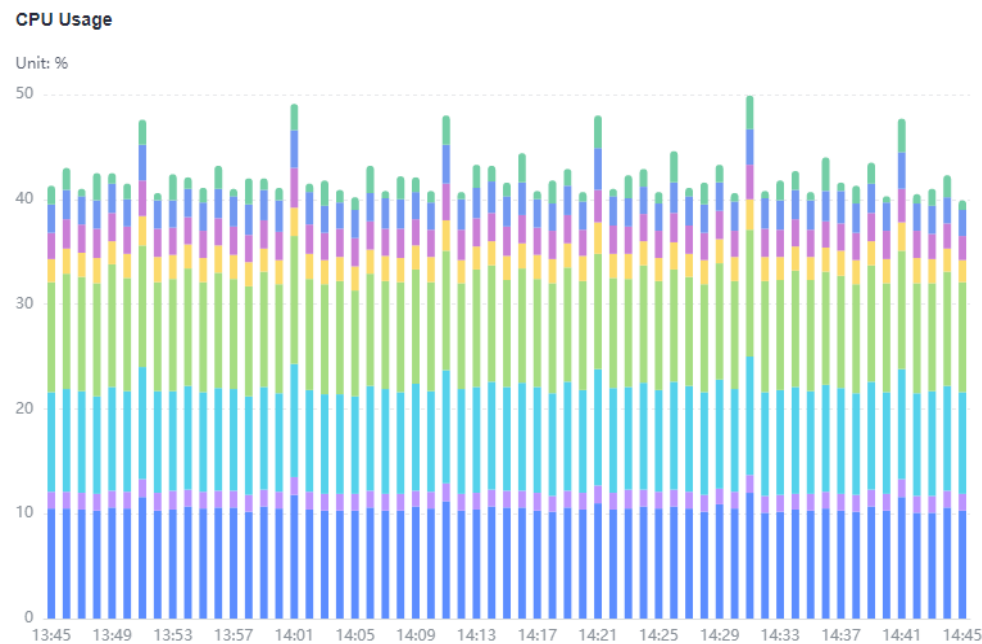


Table 8-21 Bar graph parameters

Category	Parameter	Description
-	X Axis Title	Title of the X axis.
	Y Axis Title	Title of the Y axis.
	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.
	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.

- **Digital line graph:** a trend analysis graph. It shows the change of a group of ordered data (usually in a continuous time interval) and intuitively displays related data analysis. It can display the latest data and the growth or decrease rate of the resource in a specified monitoring period. Use this type of

graph when you need to monitor the metric data trend of one or more resources within a period.

As shown in the following figure, the CPU usages in different periods are displayed in the same graph. **2.93%** indicates the latest CPU usage, and **0.00%** indicates the growth rate of the CPU usage in the current monitoring period.

Table 8-22 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.

8.8 (New) Graphs

Dashboard graphs show the query and analysis results of metrics.

Metric Data Graphs

The following types of graphs are supported: [line graphs](#), [digit graphs](#), [top N graphs](#), [tables](#), [bars](#), and [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. The following figure shows the CPU usage of different hosts.

Figure 8-6 Line graph



Table 8-23 Line graph parameters

Category	Parameter	Description
Graphics	Line Shape	Line type. Options: Straight and Curved .
	Display Background	If this option is enabled, the background will be displayed in the line 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.
	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.
X Axis	Show	Whether to display the X axis.
	X Axis Title	Title of the X axis.
Y Axis	Show	Whether to display the Y axis.
	Y Axis Title	Title of the Y axis.
	Y Axis Range	Value range of the Y axis.

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

In the following figure, you can view the CPU usage of a host in real time.

Figure 8-7 Digit graph

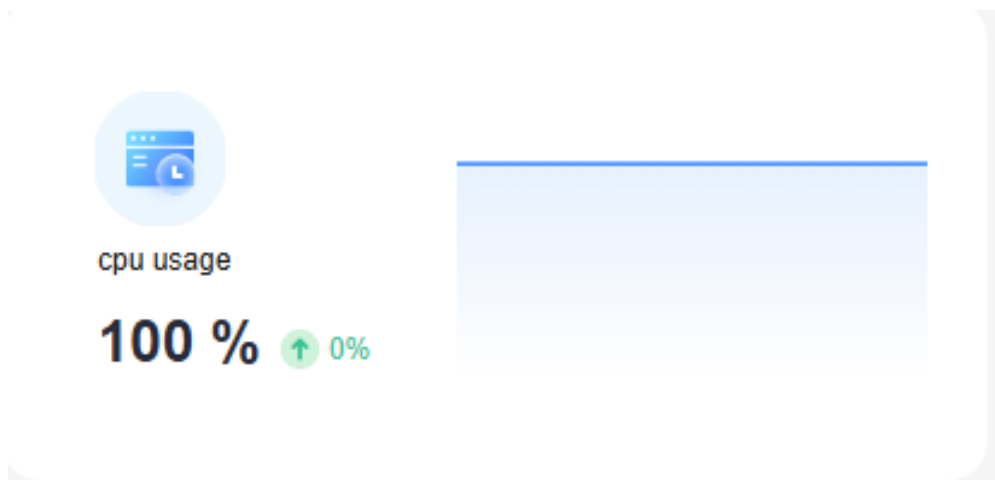


Table 8-24 Digit graph parameters

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.

In the following graph, the top 5 hosts with the highest CPU usage are displayed.

Figure 8-8 Top N graph

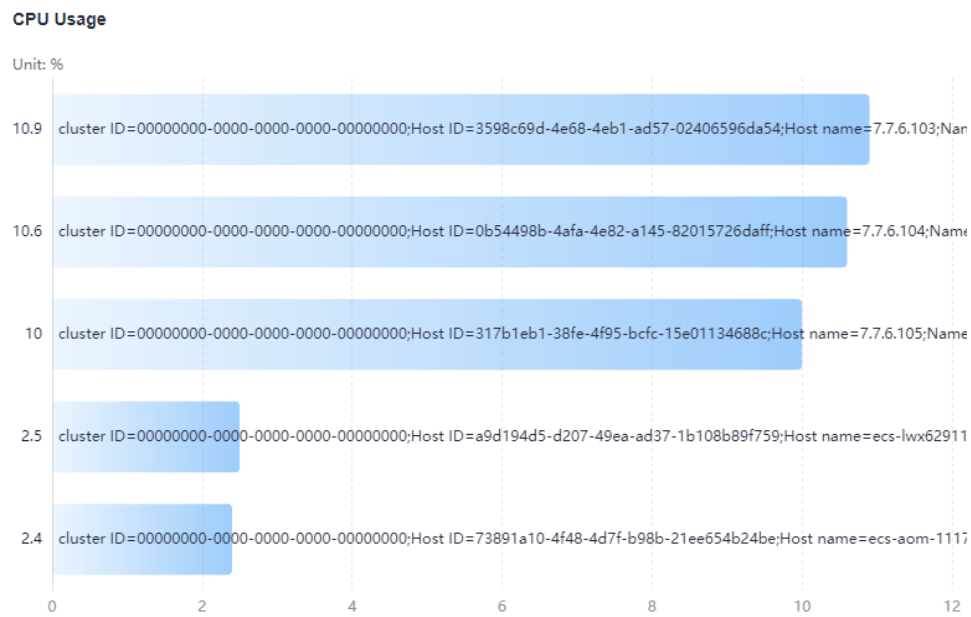


Table 8-25 Top N graph parameters

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.
	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.

Category	Parameter	Description
	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.
In the following figure, you can view the CPU usage of different hosts in a table.

Figure 8-9 Table

CPU Usage

Metric Na...	cluster ID	Host ID	Host name	Namespace	Host IP	Node Name	Value
CPU us...	000000...	0b5449...		default			10.3
CPU us...	000000...	195e90...		default			1.6
CPU us...	000000...	317b1e...		default			9.7
CPU us...	000000...	3598c6...		default			10.5

Table 8-26 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 in a graph.

Figure 8-10 Bar graph

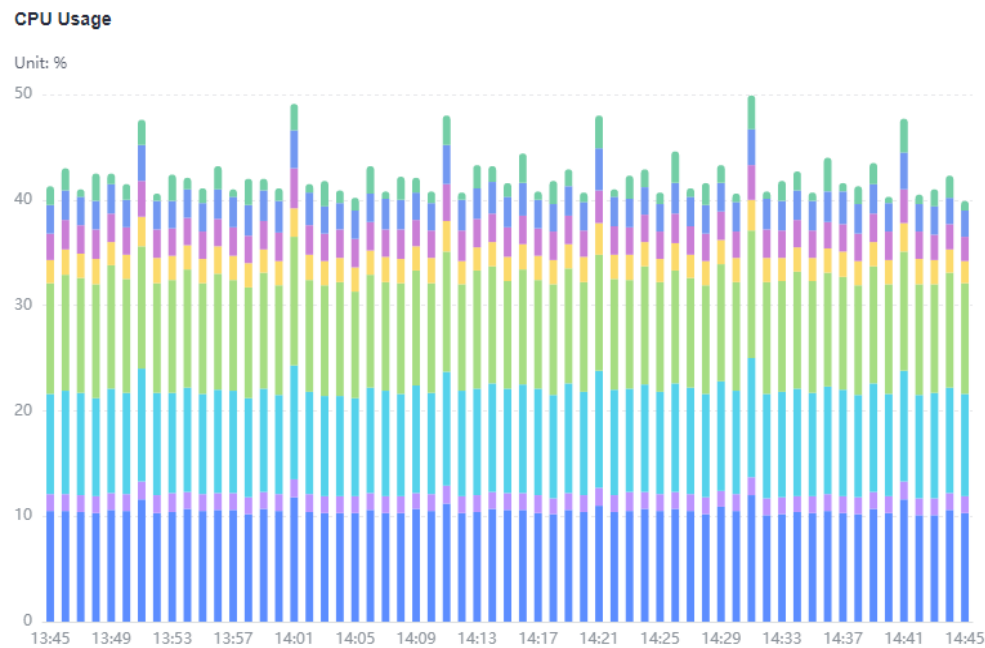


Table 8-27 Bar graph parameters

Category	Parameter	Description
Graphics	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.
	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.
X Axis	Show	Whether to display the X axis.
	X Axis Title	Title of the X axis.
Y Axis	Show	Whether to display the Y axis.
	Y Axis Title	Title of the Y axis.
	Y Axis Range	Value range of the Y axis.

- **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.
In the following figure, you can view the CPU usage in different periods in a graph.

Figure 8-11 Digital line graph

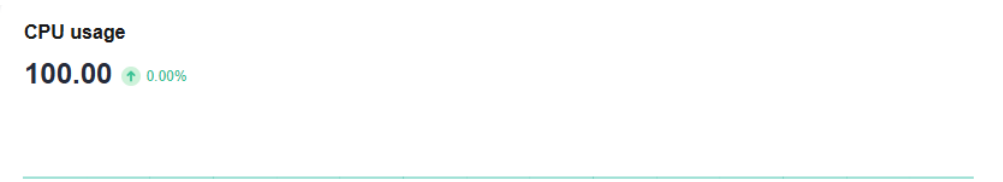


Table 8-28 Digital line graph parameters

Category	Parameter	Description
Chart Mode	Line Shape	Line type. Options: Straight and Curved .
	Hide Legend	Whether to hide legends.
	Show	Whether to display the X axis.
	Show	Whether to display the Y axis.
	Show Data Markers	Whether to display the connection points.

9 Alarm Monitoring

9.1 AOM Alarm Monitoring Overview

AOM provides alarm monitoring capabilities. 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. Events generally carry some important information. They are reported when AOM or an external service has some changes. Such changes do not necessarily cause service exceptions.

Description

- Alarm notification: Create a notification rule and associate it with an SMN topic and a message template. If the resource/metric data meets the alarm condition, the system sends an alarm notification based on the associated SMN topic and message template.
- Alarm noise reduction: The system processes alarms based on noise reduction rules to prevent an alarm storm.
- Alarm rules: Create alarm or event rules to monitor resource usage in real time.
- Viewing alarms or events: Query alarms and events for quick fault detection, locating, and recovery.

9.2 Configuring AOM Alarm Notification

9.2.1 Creating AOM Alarm Message Templates

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, HTTP, or HTTPS.

Function Introduction

- Message templates for emails, HTTP, and HTTPS are supported.

- You can customize message templates. For details, see [Step 3.3](#).

Constraints

- You can create a maximum of 100 metric/event (Prometheus monitoring) or log (log monitoring) message templates. If the number of message templates of a certain type reaches 100, delete unnecessary ones.
- AOM provides preset message templates. They cannot be deleted or edited. If there is no custom message template, notifications are sent based on a preset message template by default.
- If no message template is created, the default message template will be used.

Creating a Message Template

Step 1 Log in to the AOM 2.0 console.

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

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 9-1 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: Prometheus monitoring or Log monitoring .
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 dimmed and cannot be changed.– To use the enterprise project function, contact engineers.

2. Select a language (for example, English).
3. Customize the template content (default fields are automatically filled in when a Prometheus monitoring template is created). There are templates for emails. For details about Prometheus monitoring message templates, see [Table 9-2](#). For details about log monitoring message templates, see [Table 9-3](#).

- 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.
- 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 copy required variables.
- The **TMS tag**: **`$event.annotations.tms_tags`** variable configured in the alarm message template takes effect only after **TMS Tag Display** is enabled.
- If you select **Emails**, you can click **Preview** to view the final effect. On the **Preview** page, change the message topic if necessary.

Table 9-2 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>
Notification Rule	Name of the alarm notification rule.	<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>
Suggestion	Suggestion about handling the alarm. For non-custom reporting, "NA" is displayed.	<code>\${alarm_fix_suggestion_zh}</code>

Table 9-3 Log message template parameters

Parameter	Description	Check Rule	Example
Topic	Message topic.	Customize the topic name or use variables. (Max. 512 characters) Only email templates need a topic name.	test

Parameter	Description	Check Rule	Example
Body	Message content.	Add variables: <ul style="list-style-type: none"> Original rule name: <code>\${event_name}</code> Alarm severity: <code>\${event_severity}</code> Occurrence time: <code>\${starts_at}</code> Occurrence region: <code>\${region_name}</code> Account: <code>\${domain_name}</code> Alarm source: <code>\${event.metadata.resource_provider}</code> Resource type: <code>\${event.metadata.resource_type}</code> Resource ID: <code>\${resources}</code> Alarm status: <code>\${event.annotations.alarm_status}</code> Expression: <code>\${event.annotations.condition_expression}</code> Current value: <code>\${event.annotations.current_value}</code> Statistical period: <code>\${event.annotations.frequency}</code> Rule name: <code>\${event.annotations.alarm_rule_alias}</code> Keyword variables <ol style="list-style-type: none"> Query time: <code>\${event.annotations.results[0].time}</code> Query logs: <code>\${event.annotations.results[0].raw_results}</code> Query URL: <code>\${event.annotations.results[0].url}</code> 	<code>\${event_name}</code> <code>\$</code> <code>{event_severity}</code> <code>\${starts_at}</code> <code>\${region_name}</code>

Parameter	Description	Check Rule	Example
		<p>4. Log group/stream name: <code>\$event.annotations.results[0].resource_id</code> Only the original name of the log group or stream created for the first time can be added.</p> <p>– SQL variables</p> <p>1. Log group/stream names of chart 0: <code>\$event.annotations.results[0].resource_id</code> Only the original name of the log group or stream created for the first time can be added.</p> <p>2. Query statement of chart 0: <code>\$event.annotations.results[0].sql</code></p> <p>3. Query time of chart 0: <code>\$event.annotations.results[0].time</code></p> <p>4. Query URL of chart 0: <code>\$event.annotations.results[0].url</code></p> <p>5. Query logs of chart 0: <code>\$event.annotations.results[0].raw_results</code></p>	

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

----End

More Operations

After creating a message template, you can perform the operations listed in [Table 9-4](#).

Table 9-4 Related operations

Operation	Description
Editing a message template	Click Edit in the Operation column.
Copying a message template	Click Copy in the Operation column.
Deleting a message template	<ul style="list-style-type: none">To delete a single message template, click Delete in the Operation column in the row that contains the template, and then click Yes on the displayed page.To delete one or more message templates, select them, click Delete above the template list, and then click Yes on the displayed page. Before deleting a message template, delete the alarm notification rules bound to it.
Searching for a message template	You can search for message templates by template name, description, type, and update time, or enter a keyword to search for message templates.

9.2.2 Creating an AOM Alarm Notification Rule

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

Prerequisites

- You have created a topic.
- You have configured a topic policy.
- You have added a subscriber (that is, an email or SMS message recipient) for the topic.
- To obtain SMN topics when creating a notification rule, you must obtain the **smn:topic:list** permission in advance.

Constraints

- You can create a maximum of 1,000 alarm notification rules. If the number of rules reaches 1,000, delete unnecessary ones.

Creating an Alarm Notification Rule

Step 1 Log in to the AOM 2.0 console.

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

Step 3 On the displayed page, click **Create**.

Step 4 Set the notification rule name, type, and other parameters by referring to [Table 9-5](#).

Table 9-5 Parameters for configuring an alarm notification rule

Parameter	Description
Notification Rule Name	Name of the 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 dimmed and cannot be changed.• To use the enterprise project function, contact engineers.
Description	Description of the rule. Enter up to 1,024 characters.
Rule Type	Notification rule type. <ul style="list-style-type: none">• Prometheus monitoring If a metric or event meets the alarm condition, the system sends an alarm notification based on the associated SMN topic and message template.• Log monitoring If the log data meets the alarm condition, the system sends an alarm notification based on the associated SMN topic and message template.
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. AOM provides preset message templates. If the preset templates do not meet requirements, click Create Template to create a template. For details, see 9.2.1 Creating AOM Alarm Message Templates .

Step 5 After the settings are complete, click **OK**. The rule is created. You can then perform the following operations:

- Go to the **Alarm Noise Reduction** page, [create a grouping rule](#), and associate it with the notification rule.
- Go to the **Alarm Rules** page, [create an alarm rule](#), and associate it with the notification rule.

----End

More Operations

After an alarm notification rule is created, you can perform operations described in [Table 9-6](#).

Table 9-6 Related operations

Operation	Description
Editing an alarm notification rule	Click Modify in the Operation column.
Deleting an alarm notification 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>Precautions:</p> <ul style="list-style-type: none">Delete the bound alarm rules or grouping rules before deleting alarm notification rules.If an alarm notification rule is deleted, alarm notifications cannot be received in a timely manner.To delete alarm notification rules in batches, ensure that they are under the same enterprise project.
Searching for an alarm notification rule	You can filter alarm notification rules by rule name, description, type, enterprise project, message template, and update time, or enter a keyword to search.

9.3 Configuring AOM Alarm Rules

9.3.1 AOM Alarm Rule Overview

AOM allows you to set alarm and event rules. You can create metric/log alarm rules to monitor the real-time usage of resources such as hosts and components in the environment, helping you quickly detect, locate, and rectify faults. By creating event alarm rules, you can simplify alarm notifications and quickly troubleshoot resource usage problems.

Description

- [9.3.2 Creating an AOM Metric Alarm Rule](#)

For metric alarm rules, you can set threshold conditions for resource metrics. If a metric value meets a threshold condition, AOM generates a threshold alarm. If no metric data is reported, AOM generates an insufficient data event.

- **9.3.3 Creating an AOM 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.
- **9.3.4 Creating an AOM Log Alarm Rule**
You can create alarm rules based on keyword statistics so that AOM can monitor log data in real time and report alarms if there are any.
- **9.3.5 Creating AOM Alarm Rules in Batches**
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.

Constraints

A maximum of 3,000 metric/event alarm rules can be created. If the number of alarm rules has reached the upper limit, delete unnecessary rules and create new ones.

9.3.2 Creating an AOM Metric Alarm Rule

For metric alarm rules, you can set threshold conditions for resource metrics. If a metric value meets a threshold condition, AOM generates a threshold alarm. If no metric data is reported, AOM generates an insufficient data event.

Creation Mode

You can create metric alarm rules in the following ways: [Select from all metrics](#) and [PromQL](#).

Constraints

- If you need AOM to send email notifications when the metric alarm rule status (**Exceeded**, **Normal**, **Effective**, or **Disabled**) changes, set an alarm notification rule by referring to [9.2.2 Creating an AOM Alarm Notification Rule](#).
- Second-level monitoring is supported when you create metric alarm rules by selecting metrics from all metrics or using PromQL. The timeliness of metric alarms depends on the metric reporting period, rule check interval, and notification send time.
- A maximum of 3,000 metric/event alarm rules can be created.

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 Center** > **Alarm Rules**.

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

Step 4 Set basic information about the alarm rule by referring to [Table 9-7](#).

Table 9-7 Basic information

Parameter	Description
Original Rule Name	Original name of the alarm 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.
Rule Name	Name of a rule. Max.: 256 characters. Only letters, digits, hyphens (-), and underscores (_) are allowed. Do not start or end with a hyphen or underscore. NOTE <ul style="list-style-type: none">• If you set Rule Name, it will be displayed preferentially.• After an alarm rule is created, you can change Rule Name but cannot change Original Rule Name. When you change Rule Name and then move the cursor over it, both Original Rule Name and Rule Name can be viewed.
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 dimmed and cannot be changed.• To use the enterprise project function, contact engineers.
Description	Description of the rule. Enter up to 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 9-8](#) describes the parameters.

After the setting is complete, the monitored metric data is displayed in a line graph above the alarm condition. A maximum of 50 metric data records can be displayed. 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.

You can perform the following operations after moving the cursor to the metric data and alarm condition:










- 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 9-8 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.</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 15 seconds, 30 seconds, 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	<p>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.</p> <p>NOTE The period refers to Check Interval set in Advanced Settings. For example, if Statistical Period is set to 5 minutes, Consecutive Periods is set to 2, and Check Interval is set to 1 minute, the metric data within 5 minutes is calculated, and a metric alarm is triggered if the detection rule is met for two consecutive periods (a total of 2 minutes).</p>
Alarm Severity	<p>Metric alarm severity. Options:</p> <ul style="list-style-type: none">– : critical alarm.– : major alarm.– : minor alarm.– : warning.

Step 6 Click **Advanced Settings** and set information such as **Check Interval** and **Alarm Clearance**. For details about the parameters, see [Table 9-9](#).

Table 9-9 Advanced settings

Parameter	Description
Check Interval	<p>Interval at which metric query and analysis results are checked.</p> <ul style="list-style-type: none">• Hourly: Query and analysis results are checked every hour.• Daily: Query and analysis results are checked at a fixed time every day.• Weekly: Query and analysis results are checked at a fixed time point on a specified day of a week.• Custom interval: The query and analysis results are checked at a fixed interval. You can set Check Interval to 15 seconds or 30 seconds to implement second-level monitoring.• 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.

Parameter	Description
Alarm Clearance	<p>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.</p> <p>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.</p>
Action Taken for Insufficient Data	<p>Action to be taken when no metric data is generated or metric data is insufficient for a specified number of consecutive periods. You can set this option based on your requirements. 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>
Tags	<p>Click  to add tags for alarm rules. They will be synchronized to TMS. They can be used to filter alarm rules and group alarms to reduce noise. They can also be referenced as "\${event.metadata.tag key}" in message templates.</p> <p>Tags are alarm identification attributes in the format of "key:value". For details, see Alarm Tags and Annotations.</p>
Annotations	<p>Click  to add attributes (key-value pairs) for alarm rules. Annotations will not be synchronized to TMS, but can be used to group alarms to reduce noise and referenced as "\${event.metadata.annotation key}" in message templates.</p> <p>Annotations are alarm non-identification attributes in the format of "key:value". For details, see Alarm Tags and Annotations.</p>

Step 7 Set an alarm notification policy. For details, see [Table 9-10](#).

Table 9-10 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 a notification rule. Frequency: interval for sending alarm notifications. Select a desired value from the drop-down list. After a notification rule is enabled, the system sends notifications based on the associated SMN topic and message template. If there is no notification rule you want to select, click Add Rule in the drop-down list to create one. For details about how to set a notification rule, see 9.2.2 Creating an AOM Alarm Notification 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 9.5.2 Creating an AOM Alarm Grouping Rule. The alarm severity and tag configured in the selected grouping rule must match those configured in the alarm rule. Otherwise, the grouping rule does not take effect.

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 Center > 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 Using PromQL

Step 1 Log in to the AOM 2.0 console.

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

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

Step 4 Set basic information about the alarm rule by referring to [Table 9-11](#).

Table 9-11 Basic information






Parameter	Description
Original Rule Name	Original name of the alarm 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.
Rule Name	Name of a rule. Max.: 256 characters. Only letters, digits, hyphens (-), and underscores (_) are allowed. Do not start or end with a hyphen or underscore. NOTE <ul style="list-style-type: none">• If you set Rule Name, it will be displayed preferentially.• After an alarm rule is created, you can change Rule Name but cannot change Original Rule Name. When you change Rule Name and then move the cursor over it, both Original Rule Name and Rule Name can be viewed.
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 dimmed and cannot be changed.• To use the enterprise project function, contact engineers.
Description	Description of the rule. Enter up to characters.

Step 5 Set the detailed information about the alarm rule.

1. Set **Rule Type** to **Metric alarm rule**.
2. Set **Configuration Mode** to **PromQL**.
3. Select a target Prometheus instance from the drop-down list.
4. Set alarm rule details. [Table 9-12](#) describes the parameters.

After the setting is complete, the monitored metric data is displayed in a line graph above the alarm condition. A maximum of 50 metric data records can be displayed. Click the line icon before each metric data record to hide the metric data in the graph.



Table 9-12 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 9.3.8 Prometheus Statements.</p>
Alarm Severity	<p>Metric alarm severity. Options:</p> <ul style="list-style-type: none">– : critical alarm.– : major alarm.– : minor alarm.– : warning.
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 is triggered when the default rule condition is met for 2 minutes.

Step 6 Click **Advanced Settings** and set information such as **Check Interval** and **Alarm Clearance**. For details about the parameters, see [Table 9-13](#).

Table 9-13 Advanced settings

Parameter	Description
Check Interval	<p>Interval at which metric query and analysis results are checked.</p> <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.

Parameter	Description
Tags	<p>Tags are automatically generated based on the Prometheus statement you set. You can modify them as required. Tags are alarm identification attributes in the format of "key:value".</p> <p>Click  to add tags for alarm rules. They will be synchronized to TMS. They can be used to filter alarm rules and group alarms to reduce noise. They can also be referenced as "\${event.metadata.tag key}" in message templates. For details, see 9.3.7 Alarm Tags and Annotations.</p>
Annotations	<p>Click  to add attributes (key-value pairs) for alarm rules. Annotations will not be synchronized to TMS, but can be used to group alarms to reduce noise and referenced as "\${event.metadata.annotation key}" in message templates.</p> <p>Annotations are alarm non-identification attributes in the format of "key:value". For details, see 9.3.7 Alarm Tags and Annotations.</p>

Step 7 Set an alarm notification policy. For details, see [Table 9-14](#).

Table 9-14 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 a notification rule. Frequency: interval for sending alarm notifications. Select a desired value from the drop-down list. After a notification rule is enabled, the system sends notifications based on the associated SMN topic and message template. If the existing alarm notification rules cannot meet your requirements, click Add Rule in the drop-down list to create one. For details about how to set a notification rule, see 9.2.2 Creating an AOM Alarm Notification 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 9.5.2 Creating an AOM Alarm Grouping Rule. The alarm severity and tag configured in the selected grouping rule must match those configured in the alarm rule. Otherwise, the grouping rule does not take effect.
Notification Template	Alarm notification content to be sent. This content is automatically generated when Default Rule is set to CCEFromProm .

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 Center** > **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

9.3.3 Creating an AOM 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.

Constraints

- If you want to receive email/SMS notifications when the resource data meets the event condition, set an alarm notification rule by referring to [9.2.2 Creating an AOM Alarm Notification Rule](#).

- A maximum of 3,000 metric/event alarm rules can be created.
- When setting an alarm notification policy, enabling alarm noise reduction and associating the policy with a grouping rule are not recommended. This is because accumulated triggering is similar to alarm noise reduction.

Procedure

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane, choose **Alarm Center > Alarm Rules**.
- Step 3** On the displayed page, click **Create Alarm Rule**.
- Step 4** Set basic information about the alarm rule by referring to [Table 9-15](#).

Table 9-15 Basic information





Parameter	Description
Original Rule Name	Original name of the alarm 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.
Rule Name	Name of a rule. Max.: 256 characters. Only letters, digits, hyphens (-), and underscores (_) are allowed. Do not start or end with a hyphen or underscore. NOTE <ul style="list-style-type: none">• If you set Rule Name, it will be displayed preferentially.• After an alarm rule is created, you can change Rule Name but cannot change Original Rule Name. When you change Rule Name and then move the cursor over it, both Original Rule Name and Rule Name can be viewed.
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 dimmed and cannot be changed.• To use the enterprise project function, contact engineers.
Description	Description of the rule. Enter up to 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.
 - **System**: events ingested to AOM by default. Options: CCE/IoTDA/ModelArts.
 - **Custom**: third-party service events ingested to AOM. Select an event source from the existing service list.

3. Set alarm rule details.

Table 9-16 Alarm rule parameters

Parameter	Description
Monitored Object	Select criteria to filter service events. You can select Notification Type, Event Name, Alarm Severity, Custom Attributes, Namespace, or Cluster Name as the filter criterion. One or more criteria can be selected. Set Event Name as the filter criterion. If no event name is selected, all events are selected by default.

Parameter	Description
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: A notification is triggered at a preset frequency after an event or alarm trigger condition is met for a specified number of times. If Alarm Frequency is set to N/A, there is no limit on the number of notifications. That is, one notification is sent when an event or alarm trigger condition is met for a specified number of times. 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 three or more times within 20 minutes, an alarm notification will be sent every five minutes unless the alarm is cleared. 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.▪ Immediate Trigger: A notification is triggered immediately after an event or alarm trigger condition is met.– Alarm Severity: severity of an event alarm. Options:<ul style="list-style-type: none">▪ : critical alarm.▪ : major alarm.▪ : minor alarm.▪ : 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 notification rule. After the rule is enabled, the system sends notifications based on the associated SMN topic and message template. If existing alarm notification rules cannot meet your requirements,

create one. For details about how to set alarm notification rules, see [9.2.2 Creating an AOM Alarm Notification 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 [9.5.2 Creating an AOM Alarm Grouping Rule](#).
The alarm severity and tag configured in the selected grouping rule must match those configured in the alarm rule. Otherwise, the grouping rule does not take effect.

Step 7 Click **Confirm**. Then click **View Rule** 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 it, choose **Alarm Center > Alarm List** in the navigation pane. The system also sends alarm notifications to specified personnel by email or SMS.

----End

9.3.4 Creating an AOM Log Alarm Rule

You can create alarm rules based on keyword statistics so that AOM can monitor log data in real time and report alarms if there are any.

Prerequisites

- You have created a log group and log stream.
- You have structured logs using the new edition of log structuring.

Creation Mode


Log alarm rules can be created by referring to [Creating Log Alarm Rules by Keyword](#).

Creating Log Alarm Rules by Keyword

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane, choose **Alarm Center > Alarm Rules**.
- Step 3** On the **Log Monitoring** tab page, click **Create Alarm Rule**.
- Step 4** On the displayed page, set alarm rule parameters by referring to [Table 9-17](#).

Table 9-17 Alarm condition parameters

Category	Parameter	Description
Basic Info	Rule Name	Name of a rule. Enter 1 to 64 characters and do not start or end with a hyphen (-) or underscore (_). Only letters, digits, hyphens, and underscores are allowed. After an alarm rule is created, the rule name can be modified. After the modification, move the cursor over the rule name to view both new and original rule names.
	Description	Description of the rule. Enter up to 64 characters.
Statistical Analysis	Statistics	By keyword: applicable to scenarios where log alarm rules are created based on the counted keywords.
	Query Condition	Log Group Name: Select a log group.
		Log Stream Name: Select a log stream. If a log group contains more than one log stream, you can select multiple log streams when creating an alarm rule based on search analysis.
		Query Time Range: Specify the statement query period. It is one period earlier than the current time. For example, if Query Time Range is set to one hour and the current time is 9:00, the query statement period is 8:00–9:00. <ul style="list-style-type: none"> • The value ranges from 1 to 60 in the unit of minutes. • The value ranges from 1 to 24 in the unit of hours.
		Keywords: Enter keywords that you want AOM to monitor in logs. Exact and fuzzy matches are supported. A keyword is case-sensitive and contains up to 1024 characters.

Category	Parameter	Description
	Check Rule	<p>Configure a condition that will trigger the alarm.</p> <ul style="list-style-type: none"> • Matching Log Events: When the number of log events that contain the configured keywords reaches the specified value, an alarm is triggered. Four comparison operators are supported: greater than (>), greater than or equal to (>=), less than (<), and less than or equal to (<=). • The alarm severity can be Critical (default), Major, Minor, or Info. • Specify the number of queries and the number of times the condition (keyword contained in log events) must be met to trigger an alarm. The number of queries must be greater than or equal to the number of times the condition must be met. Number of queries: 1–10 • Click + to add a conditional expression with an OR relationship. A maximum of 20 conditional expressions can be added. • Click  to delete a conditional expression.

Category	Parameter	Description
Advanced Settings	Query Frequency	<p>Options:</p> <ul style="list-style-type: none"> • Hourly: The query is performed at the top of each hour. • Daily: The query is performed at a specific time every day. • Weekly: The query is performed at a specific time on a specific day every week. • Custom interval: You can specify the interval from 1 minute to 60 minutes or from 1 hour to 24 hours. When the query time range is larger than 1 hour, the interval must be at least 5 minutes. For example, if the current time is 9:00 and the Custom interval is set to 5 minutes, the first query is at 9:00, the second query is at 9:05, the third query is at 9:10, and so on. • CRON: Cron expressions use the 24-hour format and are precise down to the minute. Examples: <ul style="list-style-type: none"> – 0/10 * * * *: The query starts from 00:00 and is performed every 10 minutes at 00:00, 00:10, 00:20, 00:30, 00:40, 00:50, 01:00, and so on. For example, if the current time is 16:37, the next query is at 16:50. – 0 0/5 * * *: The query starts from 00:00 and is performed every 5 hours at 00:00, 05:00, 10:00, 15:00, 20:00, and so on. For example, if the current time is 16:37, the next query is at 20:00. – 0 14 * * *: The query is performed at 14:00 every day. – 0 0 10 * *: The query is performed at 00:00 on the 10th day of every month.
	Restores	<p>Configure a policy for sending an alarm clearance notification.</p> <p>If alarm clearance notification is enabled and the trigger condition has not been met for the specified number of statistical periods, an alarm clearance notification will be sent.</p> <p>Number of last queries: 1–10</p>

Category	Parameter	Description
	Notify When	<ul style="list-style-type: none">• Alarm triggered: Specify whether to send a notification when an alarm is triggered. If this option is enabled, a notification will be sent when the trigger condition is met.• Alarm cleared: Specify whether to send a notification when an alarm is cleared. If this option is enabled, a notification will be sent when the recovery policy is met.
	Frequency	You can select Once , Every 5 minutes , Every 10 minutes , Every 15 minutes , Every 30 minutes , Every hour , Every 3 hours , or Every 6 hours to send alarms. Once indicates that a notification is sent once an alarm is generated. Every 10 minutes indicates that the minimum interval between two notifications is 10 minutes, preventing alarm storms.
	Notification Rule	Select a desired rule from the drop-down list. If no rule is available, click Create Rule on the right. For details, see 9.2.2 Creating an AOM Alarm Notification Rule .
	Languages	Specify the language (English) in which alarms are sent.

Step 5 Click **Confirm**. The alarm rule is created.

----End


9.3.5 Creating AOM Alarm Rules in Batches

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.

Constraints

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 Center > Alarm Templates**.
- Step 3** On the **Prometheus Monitoring** tab page, click **Create Custom Template**.
- Step 4** In the **Select Alarm Source** dialog box, select **Prometheus monitoring** and click **Create Custom Template**.
- Step 5** Set the basic information about an alarm template. [Table 9-18](#) describes the parameters.

Table 9-18 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 dimmed and cannot be changed.• To use the enterprise project function, contact engineers.
Description	Description of the template. Enter up to 1024 characters.

- Step 6** 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. Then add an alarm rule for the cloud service. For details, see [Table 9-19](#).

Table 9-19 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 Step 5.4 and Step 6 in Creating Metric Alarm Rules by Selecting Metrics from All Metrics.3. Click OK.
CCEFromProm	Event alarm rule	See Step 7 .

Cloud Service	Alarm Rule Type	Method
	PromQL alarm rule	See Step 8 .
CCI2	PromQL alarm rule	<ol style="list-style-type: none">1. Click Add PromQL Alarm Rule.2. In the displayed Create Rule dialog box, set the original rule name, default rule, and alarm severity. For details about the parameters, see Table 9-21.3. Click OK.

Step 7 (Optional) Add an event alarm rule for the CCEFromProm service.






1. Choose **Add Alarm Rule > Add Event Alarm Rule**.
2. In the displayed **Create Rule** dialog box, set the original rule name and event details. For details, see [Table 9-20](#).
 - 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 9-20 Event rule parameters

Parameter	Description
Original 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.
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 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.




Parameter	Description
Alarm Severity	Event alarm severity. Options: <ul style="list-style-type: none">– : critical alarm.– : major alarm.– : minor alarm.– : warning.






3. Click **OK**.


Step 8 (Optional) Add a PromQL alarm rule for the CCEFromProm or CCI2 service.

1. Choose **Add Alarm Rule > Add PromQL Alarm Rule**.
2. In the displayed **Create Rule** dialog box, set the original rule name, default rule, and alarm severity. For details, see [Table 9-21](#).

Table 9-21 PromQL alarm rule parameters

Parameter	Description
Original 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 supports the following two input modes:</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>Click  next to the alarm rule details to lock the content. Then you can perform the following operations:</p> <ul style="list-style-type: none">– Click  next to the alarm rule details to unlock the content.– Click  next to the alarm rule details to copy the Prometheus statement. <p>For details, see 9.3.8 Prometheus Statements.</p>

Parameter		Description
Alarm Severity		<p>Metric alarm severity. Options:</p> <ul style="list-style-type: none"> – : critical alarm. – : major alarm. – : minor alarm. – : warning.
Dimensions		Metric monitoring dimension, which is automatically generated based on the Prometheus statement you set.
Duration		<p>A metric alarm will be triggered when the alarm condition is met for the specified duration. Options: Include Immediately, 15 seconds, 30 seconds, 1 minute, 2 minutes, 5 minutes, and 10 minutes. For example, if Duration is set to 2 minutes, a metric alarm is triggered when the default rule condition is met for 2 minutes.</p>
Advanced Settings	Check Interval	<p>Interval at which metric query and analysis results are checked.</p> <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. – XX seconds: Check the query and analysis results every <i>XX</i> seconds. <p>You can set Check Interval to 15 seconds or 30 seconds to implement second-level monitoring. The timeliness of metric alarms depends on the metric reporting period, rule check interval, and notification send time.</p> <p>For example, if the metric reporting period is 15 seconds, rule check interval is 15 seconds, and notification send time is 3 seconds, an alarm can be detected and an alarm notification can be sent within 33 seconds.</p>
	Tags	<p>Tags are alarm identification attributes in the format of "key:value".</p> <p>Tags are automatically generated based on the Prometheus statement you set. You can modify them as required. Click  to add tags for alarm rules. They will be synchronized to TMS. They can be used to filter alarm rules and group alarms to reduce noise. They can also be referenced as "\${event.metadata.tag key}" in message templates. For details, see 9.3.7 Alarm Tags and Annotations.</p>

Parameter		Description
	Annotations	Click  to add attributes (key-value pairs) for alarm rules. Annotations will not be synchronized to TMS, but can be used to group alarms to reduce noise and referenced as "\$ {event.metadata. <i>annotation key</i> }" in message templates. Annotations are alarm non-identification attributes in the format of "key:value". For details, see 9.3.7 Alarm Tags and Annotations .
	Notification Content	Alarm notification content to be sent. This content is automatically generated when Default Rule is set to CCEFromProm .

3. Click **OK**.

Step 9 (Optional) Manage variables. When adding a PromQL alarm rule to the CCEFromProm or CCI2 service, manage variables and apply them to the alarm template PromQL.

1. Click **Manage Variable**.
2. In the displayed dialog box, set variable names and values. A maximum of 50 variables can be added.
3. Click **OK**.

Step 10 Click **OK** to create the alarm template.

Step 11 (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 9-22](#). After the settings are complete, click **OK**.

Table 9-22 Parameters for binding an alarm template

Parameter	Description
Instance	<p>This parameter is optional. If the cloud services selected in Step 6.1 contain services other than CCEFromProm, this parameter will be displayed.</p> <p>The drop-down list displays all Prometheus instances for cloud services and the default/common Prometheus instances under your account. Select your desired instance.</p> <p>If the cloud service selected in Step 6.1 is CCI2 only, you can only associate common Prometheus instances.</p>
Cluster	<p>This parameter is optional. If the cloud services selected in Step 6.1 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>

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 a notification rule. Frequency: interval for sending alarm notifications. Select a desired value from the drop-down list. After a notification rule is enabled, the system sends notifications based on the associated SMN topic and message template. If the existing alarm notification rules cannot meet your requirements, click Add Rule in the drop-down list to create one. For details about how to set a notification rule, see 9.2.2 Creating an AOM Alarm Notification 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 9.5.2 Creating an AOM Alarm Grouping Rule. The alarm severity and tag configured in the selected grouping rule must match those configured in the alarm rule. Otherwise, the grouping rule does not take effect.

Step 12 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 Center > Alarm List** to view the alarm. The system also sends alarm notifications to specified personnel by email or SMS.

----End

Importing an Alarm Template

If you need to reuse the alarm templates of other regions or tenants, export the template files and then import them to quickly create alarm templates.

Step 1 Log in to the AOM 2.0 console.

- Step 2** In the navigation pane on the left, choose **Alarm Center > Alarm Templates**. On the **Prometheus Monitoring** tab page, click **Custom**. On the displayed page, choose ***** > Export** in the **Operation** column of the target alarm template.
- Step 3** Log in to the AOM 2.0 console in the target region. In the navigation pane, choose **Alarm Center > Alarm Templates**.
- Step 4** On the **Prometheus Monitoring** tab page, click **Import Alarm Template**.
- Step 5** In the **Import Alarm Template** dialog box, set parameters and upload the alarm template file (JSON) exported in [2](#). For details about the parameters, see [Table 9-23](#). Click **OK**.

Table 9-23 Parameters for importing an alarm template

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. Select a value from the drop-down list.
Template File	Directly upload or drag a JSON file to the box to upload. You can export the JSON file by exporting an alarm template. On the Custom tab page under Prometheus Monitoring , choose *** > Export in the Operation column of the target alarm template.

- Step 6** View the created alarm template on the **Custom** tab page.





----End

More Operations

After the alarm template is created, you can also perform the operations listed in [Table 9-24](#).

Table 9-24 Related operations

Operation	Description
Checking a Prometheus alarm template	In the template list, check the information such as Template Name , Alarm Rules/Conditions , Associated Cluster , and Enterprise Project .

Operation	Description
Binding alarm templates with Prometheus instances/clusters	Click  in the Operation column. For details, see Bind alarm templates with Prometheus instances/clusters .
Modifying an alarm template	Choose ... > Edit in the Operation column. For details, see Creating an Alarm Template .
Exporting a custom alarm template	Choose ... > Export in the Operation column.
Copying an alarm template	Click  in the Operation column.
Deleting an alarm template	<ul style="list-style-type: none"> To delete an alarm template, 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 Center > Alarm Rules . Enter a template name keyword in the search box above the alarm rule list and click  .
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 Center > Alarm List. On the Alarms tab page, view alarms. For details, see 9.4 Checking AOM Alarms or Events.</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 Center > Alarm List. On the Events tab page, check events. For details, see 9.4 Checking AOM Alarms or Events.</p>









9.3.6 Managing AOM 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 for Managing Prometheus Alarm Rules

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane, choose **Alarm Center > Alarm Rules**. The **Prometheus Monitoring** tab page is displayed by default.
- Step 3** In the rule list, view all created alarm rules and perform the following operations as required. For details, see [Table 9-25](#).

Table 9-25 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 9.3.2 Creating an AOM Metric Alarm Rule and 9.3.3 Creating an AOM Event Alarm Rule . If the alarm rule configuration is modified, the rule may fail to monitor the target resource or to take effect. Exercise caution.
Copying an alarm rule	Click  in the Operation column. For details, see 9.3.2 Creating an AOM Metric Alarm Rule and 9.3.3 Creating an AOM Event Alarm Rule .
Deleting alarm rules	<ul style="list-style-type: none"> To delete an alarm rule, choose  >  in the Operation column. To delete one or more alarm rules, select them and click Delete in the displayed dialog box.
Managing alarm rule tags	Choose  >  in the Operation column of an alarm rule to manage its tags. <ul style="list-style-type: none"> Adding a tag: Click Add Tags. In the Edit dialog box, enter a key and value, and click OK. Deleting a tag: In the Edit dialog box, click Delete.
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.

Operation	Description
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 Center > Alarm List. On the Alarms tab page, view alarms. For details, see 9.4 Checking AOM Alarms or Events.</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 Center > Alarm List. On the Events tab page, check events. For details, see 9.4 Checking AOM Alarms or Events.</p>









----End


Managing Log Alarm Rules

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane, choose **Alarm Center > Alarm Rules**.
- Step 3** Click the **Log Monitoring** tab.
- Step 4** In the rule list, view all created alarm rules and perform the operations listed in [Table 9-26](#) if needed.

Table 9-26 Operations related to log alarm rules

Operation	Description
Searching for alarm rules	Enter an alarm rule name to search.

Operation	Description
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 9.3.4 Creating an AOM Log Alarm Rule . A rule name can be changed. After they are changed, you can move the cursor to the rule name. Both the new and original names can be viewed.
Disabling alarm rules	<ul style="list-style-type: none"> To disable an alarm rule, click  in the Operation column. To disable one or more alarm rules, select them and click Disable in the displayed dialog box.
Enabling alarm rules	<ul style="list-style-type: none"> To enable an alarm rule, click  in the Operation column. To enable one or more alarm rules, select them and click Enable in the displayed dialog box.
Disabling an alarm rule temporarily	<ul style="list-style-type: none"> For an alarm rule, click  in the Operation column. In the displayed dialog box, set the expiration date. For one or more alarm rules, select them. In the displayed dialog box, click Disable Temporarily.
Re-enabling an alarm rule	Select one or more alarm rules. In the displayed dialog box, click Re-enable .
Copying an alarm rule	To copy an alarm rule, choose  > Copy in the Operation column. For details, see 9.3.4 Creating an AOM Log Alarm Rule .
Deleting alarm rules	<ul style="list-style-type: none"> To delete an alarm rule, choose  > Delete in the Operation column. In the displayed dialog box, click Yes. To delete one or more alarm rules, select them and click Delete in the displayed dialog box.
Enabling/Disabling alarm clearance	<ul style="list-style-type: none"> For an alarm rule, enable or disable the option in the Clearance column. For one or more alarm rules, select them. In the displayed dialog box, click Enable Alarm Clearance or Disable Alarm Clearance.

Operation	Description
Viewing detailed alarm information	<ul style="list-style-type: none">Click  next to a rule name to view details.Click a rule name. In the dialog box that is displayed, view all parameters of the alarm rule.
Viewing alarms	<p>During the configured consecutive periods, if a log data record meets the preset condition, an alarm will be generated.</p> <p>In the navigation pane, choose Alarm Center > Alarm List. On the Alarms tab page, view alarms. For details, see 9.4 Checking AOM Alarms or Events.</p>

-----End

9.3.7 Alarm Tags and Annotations

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

Alarm Rule Tag Description






- Alarm rule 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 a maximum of 20 custom tags. Each key and value can contain only 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 9-2](#).

Alarm Rule Annotation Description

- Annotations are attributes that cannot be used to identify alarms. They are used in scenarios such as alarm notification and message templates.
- Each annotation is in "key:value" format and can be customized. You can create a maximum of 20 custom annotations. Each key and value can contain only letters, digits, and underscores (_).
- In a message template, the `$event.annotations.key2` variable specifies an annotation. For details, see [Table 9-2](#).

Managing Alarm Rule 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 Center > 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 Rule Tag** or **Alarm Rule Annotation**, click  and enter a key and value.
- Step 6** Click **OK** to add an alarm rule tag or annotation.
- Adding multiple alarm rule tags or annotations: Click  multiple times to add alarm rule tags or annotations (max.: 20).
 - Modifying an alarm rule tag or annotation: Move the cursor to a desired alarm rule tag or annotation and click  to modify them.
 - Deleting an alarm rule tag or annotation: Move the cursor to a desired alarm rule tag or annotation and click  to delete them.
- End

9.3.8 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="2261xxxxxxfc1213",nodeIP="192.xx.xx.x  
x"}) by (nodeIP) / sum(aom_node_memory_total_megabytes{nodeIP="192.xx.xx.xx"}) 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="192.xx.xx.xx ",podID="3361xxxxxxab1613"}) by  
(nodeIP) / sum(aom_node_cpu_limit_core{nodeIP="192.xx.xx.xx"}) 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="2363xxxxxxxab1315",nodeIP="192.xx.xx.xx"}) by (nodeIP) / sum(aom_node_memory_total_megabytes{nodeIP="192.xx.xx.xx"}) 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="5663xxxxxxxcd3265",nodeIP="192.xx.xx.xx"}) by (nodeIP) / sum(aom_node_cpu_limit_core{nodeIP="192.xx.xx.xx"}) by (nodeIP)
```

Common Prometheus Commands

Table 9-27 lists the common Prometheus commands for querying metrics. You can modify parameters such as the IP address and ID based on site requirements.

Table 9-27 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	{aomApplicationID="",aomApplicationName=""}	http_requests_success_rate{aomApplicationID="06dc9f3b0d8cb867453ecd273416ce2a",aomApplicationName="root"}
Host component CPU usage	{appName="",serviceID="",clusterId=""}	aom_process_cpu_usage{appName="icagent",serviceID="2d29673a69cd82fab345be5f0f7dc5f",clusterId="00000000-0000-0000-0000-00000000"}
Host process threads	{processCmd="",processName=""}	aom_process_thread_count{processCmd="cdabc06c2c05b58d598e9430fa133aff7_b14ee84c-2b78-4f71-9ecc-2d06e053172c_ca4d29a846e9ad46a187ade88048825e",processName="icwatchdog"}
Cluster disk usage	{clusterId="",clusterName=""}	aom_cluster_disk_usage{clusterId="4ba8008c-b93c-11ec-894a-0255ac101afc",clusterName="aom-test"}
Cluster virtual memory usage	{clusterId="",clusterName=""}	aom_cluster_virtual_memory_usage{clusterId="4ba8008c-b93c-11ec-894a-0255ac101afc",clusterName="aom-test"}
Available cluster virtual memory	{clusterId="",clusterName=""}	aom_cluster_virtual_memory_free_megabytes{clusterId="4ba8008c-b93c-11ec-894a-0255ac101afc",clusterName="aom-test"}

Metric	Tag Definition	PromQL
Workload file system usage	{appName="",serviceID="",clusterId="",nameSpace=""}	aom_container_filesystem_usag e{appName="icagent",serviceID ="cfebc2222b1ce1e29ad827628 325400e",clusterId="af3cc895- bc5b-11ec- a642-0255ac101a0b",nameSpa ce="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="",container Name=""}	aom_container_network_trans mit_bytes{containerID="16bf66 e9b62c08493ef58ff2b7056aae5 d41496d5a2e4bac908c268518e b2cbc",containerName="coredn s"}

9.4 Checking AOM Alarms or Events

The **Alarm List** page allows you to query and handle alarms and events, so that you can quickly detect, locate, and rectify faults.

Function Introduction

- The alarm list provides the following key functions:
 - Alarm list: Check alarm information by alarm severity in a graph.
 - Advanced filtering: Filter alarms by alarm severity, source, or keyword in the search box. By default, alarms are filtered by alarm severity.
 - Alarm clearance: Clear alarms one by one or in batches.
 - Alarm details: Check the alarm object and handling suggestions in the alarm details. Handling suggestions are provided for all alarms.
- The event list provides the following key functions:
 - Event list: Check event information by event severity in a graph.
 - Advanced filtering: Filter events by event severity, source, or keyword in the search box. By default, events are filtered by event severity.

Procedure

Step 1 Log in to the AOM 2.0 console.

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

Step 3 Click the **Alarms** or **Events** tab to check alarms or events.



1. Set a time range to check alarms or events. You can use a predefined time label, such as **Last hour** and **Last 6 hours**, or customize a time range. Max.: 31 days.
2. Set the interval for refreshing alarms or events. 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 check the alarms or events generated in the period. You can filter alarms or events through the search box.



Table 9-28 Search criteria


Search Criteria	Description	Example
Alarm/ Event Severity	Search by alarm/ event severity. Options: – Critical – Major – Minor – Warning	Major: Filter the alarms whose severity is Major within the specified time range.
Resource Type	Search by resource type.	Host: Filter the alarms whose resource type is Host within the specified time range.
Alarm/ Event Source	You can select an alarm source to search for alarms or select an event source to search for events.	AOM: Filter the alarms whose source is AOM within the specified time range.

Search Criteria	Description	Example
Alarm/ Event Keyword	<ul style="list-style-type: none"> – Alarm Keyword: Fuzzy search by alarm name, alarm source, or resource type. Select Alarm Keyword in the search box and then enter a keyword. – Event Keyword: Fuzzy search by event name, event source, resource type, or other keywords. Select Event Keyword in the search box and then enter a keyword. 	AOMRule: Filter the alarm named AOMRule within the specified time range.
Custom Attribute	Exact query by custom attribute. Select Custom Attribute in the search box and then enter "custom attribute name=custom attribute value".	<ul style="list-style-type: none"> – nodeIP=192.168.0.106: Filter the alarms whose host IP address is 192.168.0.106 within the specified time range.

Step 4 Perform the operations listed in [Table 9-29](#) as required:

Table 9-29 Operations

Operation	Description
Checking alarm/ event statistics	Click  , and check alarm/event statistics that meet filter criteria within a specific time range on a bar graph.
Downloading alarms	Click  to download alarms. A maximum of 10,000 alarms can be downloaded each time.

Operation	Description
Clearing alarms	<p>You can clear alarms after the problems that cause them are resolved.</p> <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.
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 notification rule or noise reduction rule if there is any.</p> <ul style="list-style-type: none">• On the Alarm Info tab page, click the alarm rule in blue to drill down to check details.• On the Alarm Info tab page, click a custom attribute and choose Copy or Add to Search.<ul style="list-style-type: none">– Copy: Copy the custom attribute.– Add to Search: Filter alarms by custom attribute in the search box on the Alarm List page.
Checking event details	<p>Click an event name to check event details and handling suggestions.</p>
Checking cleared alarms	<p>Click Active Alarms in the upper right corner and select Historical Alarms from the drop-down list to check alarms that have been cleared.</p>

----End

9.5 Configuring AOM Alarm Noise Reduction

9.5.1 AOM Alarm Noise Reduction Overview

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

Description

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 [9.5.2 Creating an AOM Alarm Grouping Rule](#), [9.5.3 Creating an AOM Alarm Suppression Rule](#), and [9.5.4 Creating an AOM Alarm Silence Rule](#).

Constraints

- This module is used only for message notification. All triggered alarms and events can be viewed on the [alarm list](#) page.
- 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"
  }
}
```

9.5.2 Creating an AOM Alarm Grouping Rule

After you create alarm grouping rules, AOM filters alarm subsets and then groups them based on grouping conditions.

Constraints

- You can create a maximum of 100 grouping 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 Center > 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 9-30](#).

Table 9-30 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.

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 dimmed and cannot be changed.• To use the enterprise project function, contact engineers.
	Description	Description of a grouping rule. Enter up to 1,024 characters.

Category	Parameter	Description
Grouping Rule	Grouping Condition	<p>Conditions set to filter alarms. After alarms are filtered out, you can set notification 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: include host, container, and process. Example: Resource Type Equals to container• Alarm Source: name of the service that triggers the alarm or event. Options: include AOM, LTS, and CCE. 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• Notify When: scenario when notifications are triggered. Options: Alarm triggered and Alarm cleared. For example, select Notify When and then select Alarm triggered.• 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 AOM alarm notification 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 notification 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 9-31](#) if needed.

Table 9-31 Related operations

Operation	Description
Checking a grouping rule	Click the name of a grouping rule in the rule list to view its details.
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  .

9.5.3 Creating an AOM Alarm Suppression Rule

By using suppression rules, you can suppress or block notifications related to specific alarms. For example, if a major alarm is generated, the alarms of lower severities can be suppressed. If a node is faulty, all the alarms of the process or container on the node can be suppressed.

Constraints

- 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 a maximum of 100 suppression 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 Center** > **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 9-32 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.
	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 dimmed and cannot be changed. • To use the enterprise project function, contact engineers.
	Description	Description of a suppression rule. Enter up to 1,024 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: include host, container, and process. Example: Resource Type Equals to container • Alarm Source: name of the service that triggers the alarm or event. Options: include AOM, LTS, and CCE. 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 9-33](#) if needed.

Table 9-33 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  .

9.5.4 Creating an AOM Alarm Silence Rule

Alarm silence rules can mask alarm notifications in specified periods.

Constraints

- You can create a maximum of 100 silence rules. If this number has been reached, delete unnecessary rules.
- Once a silence rule is created, it takes effect immediately.

Procedure

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Alarm Center > 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 9-34 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.
	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. • To use the enterprise project function, contact engineers.
	Description	Description of a silence rule. Enter up to 1,024 characters.

Cate gory	Parameter	Description
Silen ce 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: include host, container, and process. Example: Resource Type Equals to container• Alarm Source: name of the service that triggers the alarm or event. Options: include AOM, LTS, and CCE. 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>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.


Step 4 Click **Confirm**.

----End

More Operations

After creating a silence rule, you can also perform the operations listed in [Table 9-35](#).

Table 9-35 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  .

10 (New) Log Management

AOM provides a unified entry for observability analysis of cloud services. It does not provide log functions by itself. Instead, it uses the log management, ingestion, and transfer functions of Log Tank Service (LTS). You can perform operations on the AOM 2.0 or LTS console.

Constraints

- Before using the log management, ingestion, and transfer functions on the AOM 2.0 console, you need to enable LTS first.
- To use LTS functions on the AOM console, obtain the LTS permissions in advance. For details, see section "Permissions" in the *Log Tank Service (LTS) User Guide*.
- **Log management (old)** provides log search, log files, log paths, log dumps, and log settings. To switch from the new log management function to the old one, click **Old Edition** in the upper right corner of the page.

Table 10-1 Function description

Function	Description	AOM Console	LTS Console	References
Log management	<p>The overview page provides the following:</p> <ul style="list-style-type: none"> Log management Provides Statistics, Log Applications, My Favorites/My Favorites (Local Cache), Recently Visited, and FAQs. Log search and analysis Enables you to quickly query logs, and locate faults based on log sources and contexts. 	<ol style="list-style-type: none"> Log in to the AOM 2.0 console. In the navigation pane, choose Log Management > Log Management. 	<ol style="list-style-type: none"> Log in to the LTS console. In the navigation pane, choose Log Management. 	<ul style="list-style-type: none"> Section "Log Management" in the <i>Log Tank Service (LTS) User Guide</i> Log search and analysis <ul style="list-style-type: none"> Section "Log Search and Analysis" in the <i>Log Tank Service (LTS) User Guide</i>
Log transfer	<p>After the log data of hosts and cloud services is reported to AOM or LTS, you can set the storage period as required. Log data that exceeds the storage period will be automatically deleted. You can transfer logs to other cloud services for long-term storage.</p>	<ol style="list-style-type: none"> Log in to the AOM 2.0 console. In the navigation pane, choose Log Management > Log Transfer. 	<ol style="list-style-type: none"> Log in to the LTS console. In the navigation pane, choose Log Transfer. 	<p>Section "Log Transfer" in the <i>Log Tank Service (LTS) User Guide</i></p>

Function	Description	AOM Console	LTS Console	References
Log settings	<p>Quota configuration</p> <p>When the monthly free quota (500 MB) is used up, you will be billed for any excess usage on a pay-per-use basis. To avoid extra expenses, you can stop log collection when the quota runs out.</p>	<ol style="list-style-type: none"> 1. Log in to the AOM 2.0 console. 2. In the navigation pane, choose Log Management > Log Settings. 3. Click the Quota Configuration tab. 	<ol style="list-style-type: none"> 1. Log in to the LTS console. 2. In the navigation pane, choose Configuration Center. 	<p>Section "Configuration Center" in the <i>Log Tank Service (LTS) User Guide</i></p>
	<p>Delimiters</p> <p>You can configure delimiters to split log content into words, so you can search for logs by these words.</p>	<ol style="list-style-type: none"> 1. Log in to the AOM 2.0 console. 2. In the navigation pane, choose Log Management > Log Settings. 3. Click the Delimiters tab. 	<ol style="list-style-type: none"> 1. Log in to the LTS console. 2. In the navigation pane, choose Configuration Center. 3. Click the Delimiters tab. 	

Function	Description	AOM Console	LTS Console	References
	ICAgent collection Configure ICAgent collection as required to reduce memory, database, and disk space usage.	<ol style="list-style-type: none">1. Log in to the AOM 2.0 console.2. In the navigation pane, choose Log Management > Log Settings.3. Click the ICAgent Collection tab.	<ol style="list-style-type: none">1. Log in to the LTS console.2. In the navigation pane, choose Configuration Center.3. Click the ICAgent Collection tab.	

11 (Old) Log Management

11.1 Configuring VM Log Collection Paths

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

Prerequisites

You need to install an ICAgent on your VM. About five minutes after the ICAgent is installed, you can view your VM in the VM list on the **Log Analysis > Log Paths** page.

Constraints

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

Configuring Log Collection Paths

Step 1 Log in to the AOM 2.0 console.


Step 2 In the navigation pane, choose **Log Management > Log Management**. On the displayed page, click **Old Edition** in the upper right corner.

Step 3 On the **Log Paths** tab page, click  in the **Operation** column of the target host to configure one or more log collection paths.

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

- **Using the Paths Automatically Identified by the ICAgent**

The ICAgent automatically scans the log files of your VM, and displays all the **.log**, **.trace**, or **.out** log files with handles and their paths on the page.

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

- **Manual configuration**

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

Step 4 Click **Confirm**.

----End

Viewing VM Logs

After the log collection paths are configured, the ICAgent collects log files from them. This operation takes about 1 minute to complete. After collecting logs, you can perform the following operations:

- **Viewing VM Log Files**

In the navigation pane, choose **Log Management > Log Files**. Click the **Host** tab to view the collected log files. For details, see [11.3 Checking Log Files](#).

- **Viewing and Analyzing VM logs**

In the navigation pane, choose **Log Management > Log Search**. Click the **Host** tab to view and analyze the collected logs by time range, keyword, and context. For details, see [11.2 Searching for Logs](#).

11.2 Searching for Logs

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

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Log Management > Log Management**. On the displayed page, click **Old Edition** in the upper right corner.





Step 3 On the **Log Search** page, click the **Component**, **System**, or **Host** tab and set filter criteria as prompted.

- You can search for logs by component, system, or host.
 - For component logs, you can set filter criteria such as **Cluster**, **Namespace**, and **Component**. You can also click **Advanced Search** and

set filter criteria such as **Instance**, **Host**, and **File**, and choose whether to enable **Hide System Component**.

- For system logs, you can set filter criteria such as **Cluster** and **Host**.
- For host logs, you can set filter criteria such as **Cluster** and **Host**.
- Enter a keyword in the search box. Rules are as follows:
 - Enter keywords for exact search. A keyword is the word between two adjacent delimiters.
 - Use an asterisk (*) or question mark (?) for fuzzy search, for example, **ER?OR**, **ROR***, or **ER*R**.
 - Enter a phrase for exact search. For example, enter **Start to refresh** or **Start-to-refresh**. Note that hyphens (-) are delimiters.
 - Enter a keyword containing AND (&&) or OR (||) for search. For example, enter **query logs&&error*** or **query logs||error**.
 - If no log is returned, narrow down the search range, or add an asterisk (*) to the end of a keyword for fuzzy match.

Step 4 View the search result of logs.

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


1. AOM allows you to view context. Click **Context** in the **Operation** column to view the previous or next logs of a log for fault locating.

To ensure normal host and component running, some components (for example, kube-dns) provided by the system will run on the hosts. The logs of these components will also be queried during tenant log query.

- In the **Display Rows** drop-down list, set the number of rows that display raw context data of the log.

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

- If there are 100 logs or more printed before a log and 99 or more logs printed following the log, the preceding 100 logs and following 99 logs are displayed as the context.
 - If there are fewer than 100 logs (for example, 90) printed before a log and fewer than 99 logs (for example, 80) printed following the log, the preceding 90 logs and following 80 logs are displayed as the context.
 - Click **Export Current Page** to export displayed raw context data of the log to a local PC.
2. Click **View Details** on the left of the log list to view details such as host IP address and source.

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

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

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

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

----End

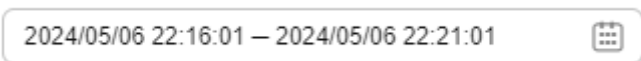
11.3 Checking Log Files

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

Procedure

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane, choose **Log Management > Log Management**. On the displayed page, click **Old Edition** in the upper right corner.
- Step 3** On the page that is displayed, click the **Component** or **Host** tab and click a name. Information such as the log file name and latest written time is displayed on the right of the page.
- Step 4** Click **View** in the **Operation** column of the desired instance. [Table 11-1](#) shows how to view log file details.

Table 11-1 Operations

Operation	Settings	Description
Setting a time range	Date	Click  to select a date.
Viewing log files	Clear	Click Clear to clear the logs displayed on the screen. Logs displayed on the screen will be cleared, but will not be deleted.

Operation	Settings	Description
	Viewing logs in real time	<p>Real-time viewing is disabled by default. You can click Enable Real-Time Viewing as required. After this function is enabled, the latest written logs can be viewed. Logs can be searched only when real-time viewing is disabled.</p> <p>For real-time log viewing, AOM automatically highlights exception keywords in logs, facilitating fault locating. Such keywords are case-sensitive. For example, when you enter format to search, format in logs will be highlighted, but Format and FORMAT will not.</p>

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

----End

11.4 Dumping Logs to OBS

AOM enables you to dump logs to Object Storage Service (OBS) buckets for long-term storage. To store logs for a longer time, add log dumps.

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

- **Periodic dump:** Current logs are dumped in real time into an OBS bucket and 1-day logs are divided based on the dump cycle.
To periodically store logs for a long period, add periodic dumps. For details, see [Adding Periodical Dumps](#).
- **One-off dump:** Dump historical logs to a log file of an OBS bucket at one time.
One-off dump is similar to the export function on the **Log Search** page. You can export up to 5000 logs on that page. When you need to export more logs but the export function cannot meet your needs, dump the logs at a time according to [Adding One-Off Dumps](#).

Constraints

- To add a log dump task, you must have OBS administrator permissions in addition to AOM and LTS permissions.
- If you need to dump logs to OBS buckets in real time for long-term storage, use the log dump function of LTS.
- Periodical dump is a near-real-time dump but has latency in minutes. The latency varies depending on the number of logs and log size. Details are as follows:
 - If the number of logs generated within 5 minutes exceeds 1000 or the log size exceeds 2 MB, the logs are dumped in real time.

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

Adding Periodical Dumps

Assume that you need to dump the logs of the **als0320a** component into files in the **/home/Periodical Dump** directory of the **obs-store-test** OBS bucket in real time, and the dump cycle is 3 hours, perform the following steps:

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane, choose **Log Management > Log Management**. On the displayed page, click **Old Edition** in the upper right corner.
- Step 3** On the **Log Transfer** tab page, click **Add Log Dump** in the upper right corner of the page. Then, set parameters according to [Table 11-2](#) and click **OK**.

Table 11-2 Periodical dump parameters

Parameter	Description	Example
Dump Mode	Select Periodic dump .	Periodic dump
Filter Criteria	Logs can be filtered by multiple criteria such as log type, cluster, or namespace, so that you can dump the logs that meet specific criteria.	Select the Component log type and select the als0320a component.
Log Group	Logs can be categorized into logical groups, so that you can dump them based on groups.	log-group1
Dump Cycle	You can divide 1-day logs based on the dump cycle. There are "N" time segments in a day (Number of time segments = 24 hours/Dump cycle). The logs of the same time segment are dumped into the same log file. For example, if the dump cycle is set to 3 hours, there are 8 time segments in a day. The logs generated at 00:00–03:00 in a day are dumped to the log file in the Log collection date (format: YYYY-MM-DD) > 00 path, and the logs generated at 03:00–06:00 in a day are dumped to the log file in the Log collection date (format: YYYY-MM-DD) > 03 path. Other time segments can be deduced by analogy.	3 hours
Target OBS Bucket	OBS bucket for storing logs. To create an OBS bucket, click View OBS to go to the OBS console.	obs-store-test
OBS Bucket Directory	OBS bucket directory for storing logs.	/home/ Periodical Dump

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

In the preceding example, the logs of **als0320a** will be dumped into log files in the **/home/Periodical Dump** directory of the **obs-store-test** OBS bucket in real time, and the dump cycle is 3 hours.

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

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

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

Table 11-3 Paths of the log files dumped to the OBS bucket

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

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

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

----End

Adding One-Off Dumps

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

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane, choose **Log Management > Log Management**. On the displayed page, click **Old Edition** in the upper right corner.
- Step 3** On the **Log Transfer** tab page, click **Add Log Dump** in the upper right corner of the page. Then, set parameters according to [Table 11-4](#) and click **OK**.

Table 11-4 One-off dump parameters

Parameter	Description	Example
Dump Mode	Select One-off dump .	One-off dump
Filter Criteria	Logs can be filtered by multiple criteria such as log collection time, cluster, or namespace, so that you can dump the logs that meet specific criteria.	Set the log collection time to Last 30 minutes , select the als0320a component, and set the keyword to warn .
Log Group	Logs can be categorized into logical groups, so that you can dump them based on groups. After a dump task is deleted, log groups will also be deleted.	log-group2
Target OBS Bucket	OBS bucket for storing logs. <ul style="list-style-type: none">If no OBS bucket is available, click View OBS to create a bucket on the OBS console.If you select an unauthorized OBS bucket, AOM will take 15 minutes to authorize the ACL for the bucket. If your configuration fails, try again 15 minutes later.Data cannot be dumped to an OBS bucket whose storage class is Archive or for which cross-region replication has been configured.	obs-store-test
OBS Bucket Directory	OBS bucket directory for storing logs. If this parameter is left blank, logs are stored in the root directory of the OBS bucket by default.	/home/One-off Dump

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

For example, the historical logs that contain the **warn** keyword in the last 30 minutes of **als0320a** will be dumped to the **log-group2_shard_0(custom).log** file in the **/home/One-off Dump** directory of the **obs-store-test** OBS bucket at one time.

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

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

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

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

Table 11-5 Names of the log files dumped to the OBS bucket

Log File Name
<ul style="list-style-type: none">- Log group name_shard_0(custom), for example, log-group2_shard_0(custom).log- Log group name_shard_1(custom)

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

----End

12 Prometheus Monitoring

12.1 Prometheus Monitoring Overview

Prometheus monitoring fully interconnects with the open-source Prometheus ecosystem. It monitors various components, and provides multiple out-of-the-box dashboards and fully hosted Prometheus services.

Prometheus is an open-source monitoring and alarm system. It features multi-dimensional data models, flexible PromQL statement query, and visualized data display. For more information, see [official Prometheus documents](#).

Prometheus instances are logical units used to manage Prometheus data collection, storage, and analysis. [Table 12-1](#) lists different types of instances classified based on monitored objects and application scenarios.

Table 12-1 Prometheus instance description

Prometheus Instance Type	Monitored Object	Monitoring Capability	Scenario
Default Prometheus instance	<ul style="list-style-type: none">Metrics reported using the API for adding monitoring dataMetrics reported using ICAgents	Monitors the metrics reported to AOM using APIs or ICAgents.	Applicable to both the scenario where self-built Prometheus remote storage (remote write) is used and the scenario where container, cloud service, or host metrics are ingested.

Prometheus Instance Type	Monitored Object	Monitoring Capability	Scenario
Prometheus for CCE	CCE	<ul style="list-style-type: none"> Provides native container service integration and container metric monitoring capabilities. By default, the following service discovery capabilities are enabled: Kubernetes SD, ServiceMonitor, and PodMonitor. 	Applicable when you need to monitor CCE clusters and applications running on them.
Prometheus for ECS	ECS	Provides integrated monitoring for ECS applications and components (such as databases and middleware) in a Virtual Private Cloud (VPC) using the UniAgent (Exporter) installed in this VPC.	Applicable when you need to monitor application components running in a VPC (usually an ECS cluster). You can add Prometheus middleware and custom plug-ins to monitor through the access center.
Prometheus instance for cloud services	Multiple cloud services	Monitors multiple cloud services. Only one Prometheus instance for cloud services can be created in an enterprise project.	Applicable when you need to centrally collect, store, and display monitoring data of cloud services.
Common Prometheus instance	Self-built Prometheus	<ul style="list-style-type: none"> Provides remote storage for Prometheus time series databases. Provides a self-developed monitoring dashboard to display data. You maintain self-built Prometheus servers. You need to configure metric management and metric data collection by yourselves. 	Applicable when you have your own Prometheus servers but need to ensure data storage availability and scalability through remote write.

Prometheus Instance Type	Monitored Object	Monitoring Capability	Scenario
Prometheus for multi-account aggregation	CCE, ECS, and other cloud service resources of multiple accounts in the same organization	Aggregates the data of CCE, ECS, and other cloud service resources of multiple accounts in the same organization for monitoring and maintenance.	Applicable when you need to centrally monitor the CCE, ECS, and other cloud service resources of multiple accounts in the same organization.

Functions

AOM Prometheus monitoring supports monitoring metric data collection, storage, computing, display, and alarm reporting. It monitors metrics of containers, cloud services, middleware, databases, applications, and services. The following lists the functions supported by AOM Prometheus monitoring.

Table 12-2 Monitored object access

Function	Description
Managing Prometheus Instances	AOM supports multiple types of Prometheus instances. You can create Prometheus instances as required.
Connecting a CCE Cluster	AOM supports the Prometheus cloud-native monitoring plug-in. You can install the plug-in for CCE clusters through Integration Center to report metrics to the Prometheus instance for CCE. Only Prometheus instances for CCE support this function.
12.8 Ingesting Middleware Metrics to AOM in VM Scenarios	AOM supports the Prometheus middleware plug-in. You can install the middleware Exporter for VMs through Access Center to report metrics to the Prometheus instance for ECS. Only Prometheus instances for ECS support this function.
Connecting Cloud Services to AOM	You can connect cloud services to AOM through Cloud Service Connection to report metrics to the Prometheus instance for cloud services. Only Prometheus instances for cloud services support this function.

Table 12-3 Monitoring metric collection

Function	Description
12.3 Managing Prometheus Instance Metrics	<p>You can check, add, and discard metrics.</p> <p>Only the default/common Prometheus instance and the Prometheus instances for CCE/cloud services/ECS are supported.</p>

Table 12-4 Data processing

Function	Description
12.9 Configuring the Remote Read Address to Enable Self-built Prometheus to Read Data from AOM	<p>With the remote read and write addresses, you can store the monitoring data of self-built Prometheus to AOM Prometheus instances for remote storage.</p>
12.7 Configuring Recording Rules to Improve Metric Query Efficiency	<p>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.</p> <p>Only Prometheus instances for CCE and common Prometheus instances support this function.</p>

Advantages

Table 12-5 Advantages

<p>Out-of-the-box usability</p> <ul style="list-style-type: none">• Installs and deploys Kubernetes and cloud products in a few clicks.• Connects to various application components and alarm tools in a few clicks.	<p>Low cost</p> <ul style="list-style-type: none">• Multiple metrics, including those of standard Kubernetes components, are free of charge.• Provides fully hosted services and eliminates the need to purchase additional resources, reducing monitoring costs and generating almost zero maintenance costs.• Integrates with CCE for monitoring services, reducing the time for creating a container monitoring system from 2 days to 10 minutes. A Prometheus instance for CCE can report the data of multiple CCE clusters.
<p>Open-source compatibility</p> <ul style="list-style-type: none">• Supports custom multi-dimensional data models, HTTP API modules, and PromQL query.• Monitored objects can be discovered through static file configuration and dynamic discovery, facilitating migration and access.	<p>Unlimited data</p> <ul style="list-style-type: none">• Supports cloud storage. There is no limit on the data to store. Distributed storage on the cloud ensures data reliability.• Supports the Prometheus instance for multi-account aggregation. Therefore, metric data of multiple accounts can be aggregated for unified monitoring.

High performance <ul style="list-style-type: none">• Is more lightweight and consumes fewer resources than open-source products. Uses single-process integrated Agents to monitor Kubernetes clusters, improving collection performance by 20 times.• Deploys Agents on the user side to retain the native collection capability and minimize resource usage.• Uses the collection-storage-separated architecture to improve the overall performance.• Optimizes the collection component to improve the single-replica collection capability and reduce resource consumption.• Balances collection tasks through multi-replica horizontal expansion to implement dynamic scaling and solve open-source horizontal expansion problems.	High availability <ul style="list-style-type: none">• Dual-replica: Metric data collection, processing, and storage components support multi-replica horizontal expansion, ensuring the high availability of core data links.• Horizontal expansion: Elastic scaling can be performed based on the cluster sca
---	--

Basic Concepts

The following lists the basic concepts about Prometheus monitoring.

Table 12-6 Basic concepts

Item	Description
Exporter	Collects monitoring data and regulates the data provided for external systems using the Prometheus monitoring function. Hundreds of official or third-party exporters are available. For details, see Exporters .
Target	Target to be captured by a Prometheus probe. A target either exposes its own operation and service metrics or serves as a proxy to expose the operation and service metrics of a monitored object.
Job	Configuration set for a group of targets. Jobs specify the capture interval, access limit, and other behavior for a group of targets.
Prometheus monitoring	Prometheus monitoring fully interconnects with the open-source Prometheus ecosystem. It monitors various components, and provides multiple out-of-the-box dashboards and fully hosted Prometheus services.

Item	Description
12.2 Managing Prometheus Instances	Logical units used to collect, store, and analyze Prometheus data.
Prometheus probes	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.
PromQL	Prometheus query language. Supports both query based on specified time spans and instantaneous query, and provides multiple built-in functions and operators. Raw data can be aggregated, sliced, predicted, and combined.
Sample	Value corresponding to a time point in a timeline. For Prometheus monitoring, each sample consists of a value of the float64 data type and a timestamp with millisecond precision.
Alarm rules	Alarm configuration for Prometheus monitoring. An alarm rule can be specified using PromQL.
Tags	A key-value pair that describes a metric.
Metric management	Automatically discovers collection targets without static configuration. Supports multiple metric management modes (such as Kubernetes SD, Consul, and Eureka) and exposes collection targets through ServiceMonitor or PodMonitor.
Recording rules	Prometheus monitoring's recording rule capability. You can use PromQL to process raw data into new metrics to improve query efficiency.
Time series	Consist of metric names and tags. Time series are streams of timestamped values belonging to the same metric and the same set of tagged dimensions.
Remote storage	Self-developed time series data storage component. It supports the remote write protocol related to Prometheus monitoring and is fully hosted by cloud products.
Cloud product monitoring	Seamlessly integrates monitoring data of multiple cloud products. To monitor cloud products, connect them first.
Metrics	Labeled data exposed by targets, which can fully reflect the operation or service status of monitored objects. Prometheus monitoring uses the standard data format of OpenMetrics to describe metrics.

12.2 Managing Prometheus Instances

AOM allows you to create multiple types of 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.

Creating a Prometheus Instance

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

Table 12-7 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 dimmed and cannot be changed.• To use the enterprise project function, contact engineers.
Instance Type	Type of the Prometheus instance. Options: <ul style="list-style-type: none">• Prometheus for CCE• Prometheus for ECS• Prometheus for Cloud Services• Common Prometheus Instance• Prometheus for Multi-Account Aggregation Select a Prometheus instance type by referring to Table 12-1 . The following instances cannot be directly created: <ul style="list-style-type: none">• default: Prometheus_AOM_Default is preset.

- Step 4** Click **OK**. The Prometheus instance is created.

Then you can perform the operations listed in the following table as required.

Table 12-8 Related operations

Sub-Menu	Description
Connecting a CCE Cluster	AOM supports the Prometheus cloud-native monitoring plug-in. You can install the plug-in for CCE clusters through Integration Center to report metrics to the Prometheus instance for CCE. Only Prometheus instances for CCE support this function.
12.8 Ingesting Middleware Metrics to AOM in VM Scenarios	AOM supports the Prometheus middleware plug-in. You can install the middleware Exporter for VMs through Access Center to report metrics to the Prometheus instance for ECS. Only Prometheus instances for ECS support this function.
Connecting Cloud Services to AOM	You can connect cloud services to AOM through Cloud Service Connection to report metrics to the Prometheus instance for cloud services. Only Prometheus instances for cloud services support this function.
Connecting Accounts	You can connect multiple member accounts within the same organization through Account Access to monitor metrics. Through data multi-write, cross-VPC access can be achieved without exposing the network information about servers. Only Prometheus instances for multi-account aggregation support this function.
12.3 Managing Prometheus Instance Metrics	AOM allows you to view Prometheus instance metrics, including new and discarded ones on the Metric Management page. Only the default/common Prometheus instances, and the Prometheus instances for cloud services/ECS/CCE support this function.
12.9 Configuring the Remote Read Address to Enable Self-built Prometheus to Read Data from AOM	AOM allows you to check the basic information, call credentials, and service address of a Prometheus instance on the Settings page. Only the default/common Prometheus instances, and the Prometheus instances for cloud services/ECS/CCE support this function.




----End







Managing Prometheus Instances

Step 1 Log in to the AOM 2.0 console.

- Step 2** In the navigation pane on the left, choose **Prometheus Monitoring > Instances**. In the instance list, view the created Prometheus instances and perform the operations listed in [Table 12-9](#) as required.

Table 12-9 Related operations

Operation	Description
Searching for a Prometheus instance	Enter an instance name in the search box and click  .
Viewing a Prometheus instance ID	Hover the mouse pointer over a Prometheus instance name. The Prometheus instance ID and name will then be displayed.
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.

Operation	Description
Checking a Prometheus instance	<p>The Prometheus instance list displays information such as the instance name, instance type, and enterprise project 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 network of the desired Prometheus instance. Then click  on the right to copy the code to the corresponding file. In the Service Addresses area, obtain the remote read and write configuration code in the private network of the desired Prometheus instance. Then click  on the right to copy the code to the corresponding file. For details, see Obtaining the Service Address of a Prometheus Instance. When you do not have an access code: <ol style="list-style-type: none"> 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. Click Add Access Code. In the displayed dialog box, click OK. Then, choose Settings > Global Settings 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 Other Operations.
Modifying a Prometheus instance	<ul style="list-style-type: none"> Modify a Prometheus instance name: <p>Click  in the Operation column that contains the target Prometheus instance. Each Prometheus instance name must be unique. (The default instance names cannot be changed.)</p> Modify Prometheus instance configurations: <p>In the Prometheus instance list, click the name of a Prometheus instance (such as a Prometheus instance for cloud services/ECS/CCE) and modify the information (such as the cloud services/access center/CCE clusters) if needed.</p>
Deleting a Prometheus instance	<p>Click  in the Operation column that contains the target Prometheus instance.</p> <ul style="list-style-type: none"> The default instances cannot be deleted. If you delete a Prometheus instance connected to a CCE cluster, cluster metrics cannot be hosted to this instance after it is deleted.

----End

12.3 Managing Prometheus Instance Metrics

You can check the metrics of a default/common Prometheus instance, or a Prometheus instance for CCE/ECS/cloud services, and add/discard metrics.

Prerequisites

Your service has been connected for Prometheus monitoring. For details, see [12.2 Managing Prometheus Instances](#).

Constraints

- Only the default/common Prometheus instance, and Prometheus instance for CCE/ECS/cloud services support the functions of checking/discarding metrics.
- On the **Metric Management** page, you can query only the metrics reported in the last three hours.
- Default Prometheus instance: Metrics whose names start with **aom_** or **apm_** cannot be discarded.
- Prometheus instances for ECS: Only the metrics collected through collection tasks delivered by UniAgent can be displayed.
- Prometheus instances for CCE:
Only the metrics reported by kube-prometheus-stack (later than 3.9.0) installed on CCE **Add-ons** or AOM Prometheus instance for CCE **Integration Center** can be discarded. Ensure that this add-on is running when discarding metrics.
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 Prometheus Instance Metrics

Only the default/common Prometheus instance, and Prometheus instance for CCE/ECS/cloud services support the functions of checking metrics.

- 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 **Metric Management**. On the **Metrics** tab page, view the metric names and types of the current Prometheus instance.
 - Prometheus instance for CCE: You can filter metrics by cluster name, job name, or metric type, or enter a metric name keyword for fuzzy search.
 - Prometheus instance for cloud services: You can filter metrics by metric type, or enter a metric name keyword for fuzzy search.

- Prometheus instance for ECS: You can filter metrics by metric type, plug-in type, or collection task, or enter a metric name keyword for fuzzy search.
- Default Prometheus instance: You can filter metrics by metric type, or enter a metric name keyword for fuzzy search.
- Common Prometheus instance: You can filter metrics by metric type, or enter a metric name keyword for fuzzy search.

Table 12-10 Metric parameters

Parameter	Description
Metric Name	Name of a metric.
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. This parameter is not supported for Prometheus instances for cloud services.
Proportion	Number of a certain type of metrics/Total number of metrics This parameter is not supported for Prometheus instances for cloud services.

----End

Discarding Prometheus Instance Metrics

If Prometheus instance metrics do not need to be reported, discard them.


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, choose **Metric Management**.

Step 5 Perform the following operations to discard metrics:

- To discard a metric, locate it and click  in the **Operation** column.
- To discard one or more metrics, select them and click **Delete** in the displayed dialog box.

----End

Adding Prometheus Instance Metrics

After metrics in a Prometheus instance are discarded, you can add them again.

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, choose **Metric Management**.
- Step 5** Click **Add Metric**. In the displayed dialog box, select one or more metrics to restore and click **OK**.
- End

12.4 Using Prometheus Monitoring to Monitor CCE Cluster Metrics

Based on the Prometheus monitoring ecosystem, AOM provides hosted Prometheus instances for CCE, which are suitable for monitoring CCE clusters and applications running on them. By default, Prometheus instances for CCE support integration with the Cloud Native Cluster Monitoring add-on. After installing the add-on, metrics will be automatically reported to a specified Prometheus instance for CCE.

Constraints

- Only when the Cloud Native Cluster Monitoring add-on (kube-prometheus-stack) exists on the **Add-ons** page of CCE, can you install the add-on for clusters.
- 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 **Prometheus Monitoring > Instances**. On the displayed page, click **Add Prometheus Instance**.
- Step 3** Set an instance name, enterprise project, and instance type.

Table 12-11 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	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 dimmed and cannot be changed.• To use the enterprise project function, contact engineers.
Instance Type	Type of the Prometheus instance. Select Prometheus for CCE .

Step 4 Click **OK**.

----End

Connecting a CCE Cluster

Step 1 Log in to the AOM 2.0 console.

Step 2 Choose **Prometheus Monitoring > Instances**.

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

Step 4 On the **Integration Center** page, click **Connect Cluster**. In the cluster list, you can view the cluster information, installation status, and collection status.

Step 5 Locate a target cluster and click **Install** in the **Operation** column to install the Cloud Native Cluster Monitoring add-on.

Step 6 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

12.5 Configuring Multi-Account Aggregation for Unified Monitoring

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.

Constraints

- Only the organization administrator or delegated administrator can create Prometheus instances for multi-account aggregation and connect accounts.
- If a delegated administrator cannot connect accounts, assign the following permissions to the delegated administrator :
 - organizations:trustedServices:list
 - organizations:organizations:get
 - organizations:delegatedAdministrators:list
 - organizations:roots: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.

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 **Prometheus Monitoring > Instances**. On the displayed page, click **Add Prometheus Instance**.

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

Table 12-12 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 dimmed and cannot be changed.• To use the enterprise project function, contact engineers.
Instance Type	Type of the Prometheus instance. Select Prometheus for Multi-Account Aggregation .

Step 4 Click **OK**.

----End

Connecting Accounts

- Step 1** Log in to the AOM 2.0 console.
- 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

12.6 Configuring Metric Collection Rules for CCE Clusters

By adding ServiceMonitor or PodMonitor, you can configure metric 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 [12.4 Using Prometheus Monitoring to Monitor CCE Cluster Metrics](#).

Constraints

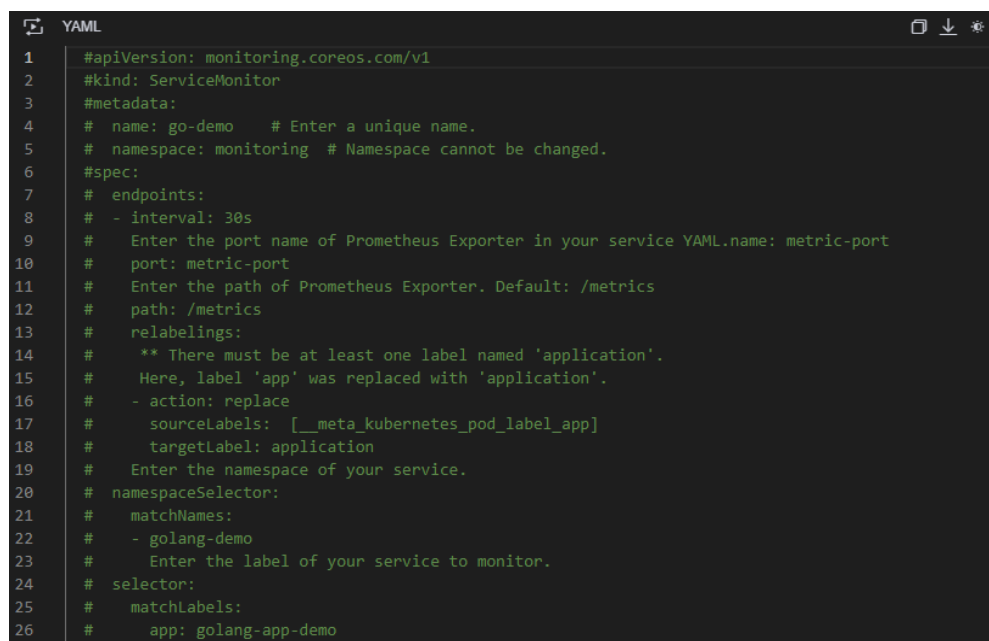
Only when kube-prometheus-stack installed on the **Add-ons** page of CCE or the **Integration Center** page of the Prometheus instance for CCE on AOM is 3.9.0 or later and is still running, can you enable or disable collection rules.

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 **Prometheus Monitoring > Instances**.
- Step 3** In the instance list, click a Prometheus instance for CCE.
- Step 4** In the navigation pane on the left, choose **Metric Management**. On the **Settings** tab page, click **ServiceMonitor**.
- Step 5** Click **Add ServiceMonitor**. In the displayed dialog box, set related parameters and click **OK**.

Figure 12-1 Adding ServiceMonitor



```
1 #apiVersion: monitoring.coreos.com/v1
2 #kind: ServiceMonitor
3 #metadata:
4 #  name: go-demo      # Enter a unique name.
5 #  namespace: monitoring # Namespace cannot be changed.
6 #spec:
7 #  endpoints:
8 #    - interval: 30s
9 #      # Enter the port name of Prometheus Exporter in your service YAML.name: metric-port
10 #      port: metric-port
11 #      # Enter the path of Prometheus Exporter. Default: /metrics
12 #      path: /metrics
13 #      relabelings:
14 #        ** There must be at least one label named 'application'.
15 #        Here, label 'app' was replaced with 'application'.
16 #        - action: replace
17 #          sourceLabels: [__meta_kubernetes_pod_label_app]
18 #          targetLabel: application
19 #      # Enter the namespace of your service.
20 #      namespaceSelector:
21 #        matchNames:
22 #          - golang-demo
23 #      # Enter the label of your service to monitor.
24 #      selector:
25 #        matchLabels:
26 #          app: golang-app-demo
```

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

----End

Adding PodMonitor

- 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 Prometheus instance for CCE.
- Step 4** In the navigation pane on the left, choose **Metric Management**. On the **Settings** tab page, click **PodMonitor**.
- Step 5** Click **Add PodMonitor**. In the displayed dialog box, set related parameters and click **OK**.

Figure 12-2 Adding PodMonitor

```
YAML
1 #apiVersion: monitoring.coreos.com/v1
2 #kind: PodMonitor
3 #metadata:
4 #   name: go-demo      # Enter a unique name.
5 #   namespace: monitoring # Namespace cannot be changed.
6 #spec:
7 #   podMetricsEndpoints:
8 #     - interval: 30s
9 #       Enter the port name of Prometheus Exporter in your pod YAML.name: metric-port
10 #       port: metric-port
11 #       Enter the path of Prometheus Exporter. Default: /metrics
12 #       path: /metrics
13 #       relabelings:
14 #         ** There must be at least one label named 'application'.
15 #         Here, label 'app' was replaced with 'application'.
16 #         - action: replace
17 #           sourceLabels: [__meta_kubernetes_pod_label_app]
18 #           targetLabel: application
19 #       Enter the namespace of your pod.
20 #       namespaceSelector:
21 #         matchNames:
22 #           - golang-demo
23 #       Enter the label of your pod to monitor.
24 #       selector:
25 #         matchLabels:
26 #           app: golang-app-demo
```




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

----End

Other Operations

Perform the operations listed in [Table 12-13](#) if needed.

Table 12-13 Related operations

Operation	Description
Viewing a metric	<ul style="list-style-type: none">In the 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 a collection rule	On the Metric Management > Settings page, click  in the Status column to enable or disable a collection rule.
Deleting a metric	Click  in the Operation column to delete a metric.

12.7 Configuring Recording Rules to Improve Metric Query Efficiency

Recording rules can be used for secondary development of metric data. By setting recording rules, you can move the computing process to the write end, reducing resource usage on the query end.

Scenario

Some metrics may require much calculation on the query end, affecting query performance. You can configure recording rules to calculate common or complex metrics in advance. Especially in large-scale clusters and complex service scenarios, recording rules can reduce PromQL complexity, improve metric query performance, and prevent slow configuration and query.

Prerequisite

- Both your service and CCE cluster have been connected to a Prometheus instance for CCE. For details, see [12.4 Using Prometheus Monitoring to Monitor CCE Cluster Metrics](#).
- Your service has been connected to a common Prometheus instance. For details, see [12.2 Managing Prometheus Instances](#).

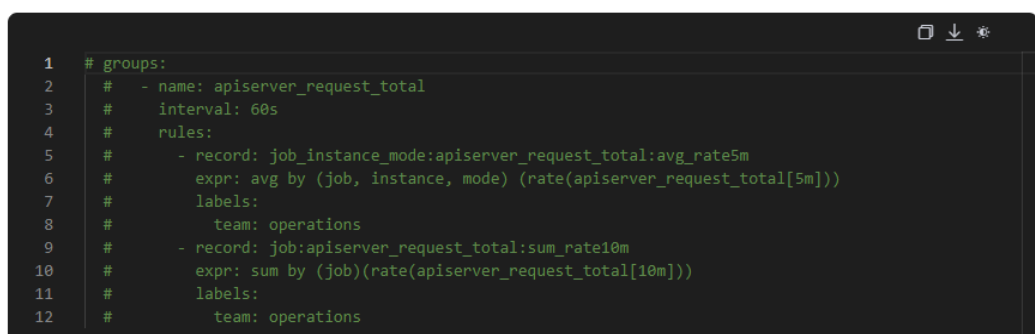
Configuring a Recording Rule

- 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 Prometheus instance for CCE or a common Prometheus instance.
- 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.

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

Figure 12-3 Configuring a recording rule

Edit RecordingRule.yaml



```
1 # groups:
2 #   - name: apiserver_request_total
3 #     interval: 60s
4 #     rules:
5 #       - record: job_instance_mode:apiserver_request_total:avg_rate5m
6 #         expr: avg by (job, instance, mode) (rate(apiserver_request_total[5m]))
7 #         labels:
8 #           team: operations
9 #       - record: job:apiserver_request_total:sum_rate10m
10 #        expr: sum by (job)(rate(apiserver_request_total[10m]))
11 #        labels:
12 #          team: operations
```

Table 12-14 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	Execution interval of a rule group. The default value is 60s . (Optional)
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	Metric label. Labels must comply with Prometheus metric label specifications . (Optional)

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**.

After the recording rule is configured, you can view metrics through:

- [Metric Browsing](#) page
- [Grafana](#)

----End

12.8 Ingesting Middleware Metrics to AOM in VM Scenarios

12.8.1 Ingesting MySQL Metrics to AOM

Create a collection task and install MySQL Exporter to monitor MySQL metrics on a host.

Prerequisites

- **The UniAgent has been installed** and is running.
- **A Prometheus instance for ECS has been created.**

Procedure


Step 1 Log in to the AOM 2.0 console.


Step 2 In the navigation pane on the left, ingest middleware metrics:

- Choose **Prometheus Monitoring > Instances**. Click a Prometheus instance for ECS. On the instance details page, choose **Access Center** and then click the **MySQL** card.

Step 3 On the displayed page, set parameters by referring to the following table.

Table 12-15 Parameters for configuring a collection task

Operation	Parameter	Description
Select Instance	Prometheus Instance	Select a Prometheus instance for ECS to store collected data. A collection task is associated with the Prometheus instance to mark and classify collected data. If no Prometheus instance is available, create one .
Set Plug-in	OS	Operating system of the host. Only Linux is supported.
	Collection Plug-in	The default value is MYSQL .
	Plug-in Version	Select a plug-in version. Plug-in versions that have not been released are dimmed and cannot be selected.
Set Collection Task	Collection Task Name	Name of a collection task. Enter 1 to 50 characters starting with a letter. Only letters, digits, underscores (_), and hyphens (-) are allowed.
	Host	Click Add Host . On the Add Host page, select the host for configuring the collection task and installing Exporter. <ul style="list-style-type: none">• Search for and select a host by the host name, IP address, or Agent status.• You can click  in the upper right corner to deselect the selected host.• Ensure that the UniAgent of the selected host is running. Otherwise, no data can be collected.

Operation	Parameter	Description
	Metric Dimension	<p>Click . In the displayed dialog box, select Built-in or Custom to add a metric dimension.</p> <ul style="list-style-type: none">• Metric dimension name:<ul style="list-style-type: none">– Built-in metric dimensions: _app, _comp, and _env are available, which are used to identify applications, components, and environments, respectively.– Custom metric dimension: Enter a metric dimension name. Each name can contain 1 to 64 characters. Only letters, digits, and underscores (<code>_</code>) are allowed. Each name must start with a letter or underscore. <p>For a host, each metric dimension name must be unique.</p> <ul style="list-style-type: none">• Metric dimension value: Enter the value of a metric dimension. This value can be duplicate but cannot be empty. Each value can contain 1 to 128 characters. The following characters are not allowed: <code>& ><\$;'!-()</code> <p>Up to 10 dimensions can be added. For example, if the dimension name is label1 and the dimension value is label2, label1:"label2" will be displayed.</p>
	Advanced Settings	<p>Configure the following parameters:</p> <ul style="list-style-type: none">• Collection Period (s): O&M data collection period, in seconds. Options: 10s, 30s, and 60s (default).• Timeout Period (s): the maximum time allowed for executing a collection task, in seconds. Options: 10s, 30s, and 60s (default). The timeout period cannot exceed the collection period.• Executor: user who executes the collection task, that is, the user of the selected host. The default value is root. Currently, only the root user is supported.

Step 4 Set Exporter installation parameters and click **Install**. Click **View Log** to view Exporter installation logs.

Exporter collects monitoring data and regulates the data provided for external systems through Prometheus monitoring.




Parameter	Description
MySQL Username	Username of MySQL.

Parameter	Description
MySQL Password	Password of MySQL.
MySQL Address	IP address and port number of MySQL, for example, 10.0.0.1:3306 .

Step 5 Click **Install** to connect the MySQL plug-in. The connected plug-in will be displayed on the **Collection Tasks** tab page of the plug-in card. Click the plug-in card. On the **Collection Tasks** tab page, click the target collection task to view its details.

You can also perform the operations listed in the following table on the collection task.

Table 12-16 Related operations

Operation	Description
Checking a collection task	Click a collection task to go to its details page.
Starting or stopping a collection task	Click the button in the Start/Stop column of a collection task to start or stop it.
Searching for a collection task	Set filter criteria or enter keywords to search for a collection task.
Changing target hosts	Click  in the Operation column of the target collection task. On the displayed page, change target hosts. You can only change the target hosts for the collection tasks created using custom plug-ins.
Sorting collection tasks	Click  in the Timeout Period or Collection Period column to sort collection tasks.
Copying a collection task	Click  in the Operation column of a collection task. On the displayed page, modify parameters as required.
Modifying a collection task	Choose *** > Modify in the Operation column of the target collection task. On the displayed page, modify parameters as required.
Deleting a collection task	Locate a collection task and choose *** > Delete in the Operation column. On the displayed page, confirm the deletion.

----End

12.8.2 Ingesting Redis Metrics to AOM

Create a collection task and install Redis Exporter to monitor Redis metrics on a host.

Prerequisites

- **The UniAgent has been installed** and is running.
- **A Prometheus instance for ECS has been created.**

Procedure

Step 1 Log in to the AOM 2.0 console.



Step 2 In the navigation pane on the left, ingest middleware metrics:

- Choose **Prometheus Monitoring > Instances**. Click a Prometheus instance for ECS. On the instance details page, choose **Access Center** and then click the **Redis** card.

Step 3 On the displayed page, set parameters by referring to the following table to configure a collection task and click **Next**.

Table 12-17 Parameters for configuring a collection task

Operation	Parameter	Description
Select Instance	Prometheus Instance	Select a Prometheus instance for ECS to store collected data. A collection task is associated with the Prometheus instance to mark and classify collected data. If no Prometheus instance is available, create one .
Set Plug-in	OS	Operating system of the host. Only Linux is supported.
	Collection Plug-in	The default value is REDIS .
	Plug-in Version	Select a plug-in version. Plug-in versions that have not been released are dimmed and cannot be selected.
Set Collection Task	Collection Task Name	Name of a collection task. Enter 1 to 50 characters starting with a letter. Only letters, digits, underscores (_), and hyphens (-) are allowed.

Operation	Parameter	Description
	Host	<p>Click Add Host. On the Add Host page, select the host for configuring the collection task and installing Exporter.</p> <ul style="list-style-type: none"> Search for and select a host by the host name, IP address, or Agent status. You can click  in the upper right corner to deselect the selected host. Ensure that the UniAgent of the selected host is running. Otherwise, no data can be collected.
	Metric Dimension	<p>Click . In the displayed dialog box, select Built-in or Custom to add a metric dimension.</p> <ul style="list-style-type: none"> Metric dimension name: <ul style="list-style-type: none"> Built-in metric dimensions: _app, _comp, and _env are available, which are used to identify applications, components, and environments, respectively. Custom metric dimension: Enter a metric dimension name. Each name can contain 1 to 64 characters. Only letters, digits, and underscores (_) are allowed. Each name must start with a letter or underscore. <p>For a host, each metric dimension name must be unique.</p> Metric dimension value: Enter the value of a metric dimension. This value can be duplicate but cannot be empty. Each value can contain 1 to 128 characters. The following characters are not allowed: & ><\$;'!-() <p>Up to 10 dimensions can be added. For example, if the dimension name is label1 and the dimension value is label2, label1:"label2" will be displayed.</p>
	Advanced Settings	<p>Configure the following parameters:</p> <ul style="list-style-type: none"> Collection Period (s): O&M data collection period, in seconds. Options: 10s, 30s, and 60s (default). Timeout Period (s): the maximum time allowed for executing a collection task, in seconds. Options: 10s, 30s, and 60s (default). The timeout period cannot exceed the collection period. Executor: user who executes the collection task, that is, the user of the selected host. The default value is root. Currently, only the root user is supported.

- Step 4** Set Exporter installation parameters and click **Install**. Click **View Log** to view Exporter installation logs.





Exporter collects monitoring data and regulates the data provided for external systems through Prometheus monitoring.

Parameter	Description
Redis Address	IP address and port number of Redis, for example, 127.0.0.1:3306 .
Redis Password	Password for logging in to Redis.

- Step 5** Click **Create** to connect the Redis plug-in. The connected plug-in will be displayed on the **Collection Tasks** tab page of the plug-in card. Click the plug-in card. On the **Collection Tasks** tab page, click the target collection task to view its details.

You can also perform the operations listed in the following table on the collection task.

Table 12-18 Related operations

Operation	Description
Checking a collection task	Click a collection task to go to its details page.
Starting or stopping a collection task	Click the button in the Start/Stop column of a collection task to start or stop it.
Searching for a collection task	Set filter criteria or enter keywords to search for a collection task.
Changing target hosts	Click  in the Operation column of the target collection task. On the displayed page, change target hosts. You can only change the target hosts for the collection tasks created using custom plug-ins.
Sorting collection tasks	Click  in the Timeout Period or Collection Period column to sort collection tasks.
Copying a collection task	Click  in the Operation column of a collection task. On the displayed page, modify parameters as required.
Modifying a collection task	Choose  > Modify in the Operation column of the target collection task. On the displayed page, modify parameters as required.

Operation	Description
Deleting a collection task	Locate a collection task and choose ... > Delete in the Operation column. On the displayed page, confirm the deletion.

----End

12.8.3 Ingesting Kafka Metrics to AOM

Create a collection task and install Kafka Exporter to monitor Kafka metrics on a host.

Prerequisites

- [The UniAgent has been installed](#) and is running.
- [A Prometheus instance for ECS has been created](#).

Procedure

Step 1 Log in to the AOM 2.0 console.



Step 2 In the navigation pane on the left, ingest middleware metrics:

- Choose **Prometheus Monitoring** > **Instances**. Click a Prometheus instance for ECS. On the instance details page, choose **Access Center** and then click the **Kafka** card.

Step 3 On the displayed page, set parameters by referring to the following table to configure a collection task and click **Next**.

Table 12-19 Parameters for configuring a collection task

Operation	Parameter	Description
Select Instance	Prometheus Instance	Select a Prometheus instance for ECS to store collected data. A collection task is associated with the Prometheus instance to mark and classify collected data. If no Prometheus instance is available, create one .
Set Plug-in	OS	Operating system of the host. Only Linux is supported.
	Collection Plug-in	The default value is KAFKA .
	Plug-in Version	Select a plug-in version. Plug-in versions that have not been released are dimmed and cannot be selected.

Operation	Parameter	Description
Set Collection Task	Collection Task Name	Name of a collection task. Enter 1 to 50 characters starting with a letter. Only letters, digits, underscores (_), and hyphens (-) are allowed.
	Host	<p>Click Add Host. On the Add Host page, select the host for configuring the collection task and installing Exporter.</p> <ul style="list-style-type: none"> Search for and select a host by the host name, IP address, or Agent status. You can click  in the upper right corner to deselect the selected host. Ensure that the UniAgent of the selected host is running. Otherwise, no data can be collected.
	Metric Dimension	<p>Click . In the displayed dialog box, select Built-in or Custom to add a metric dimension.</p> <ul style="list-style-type: none"> Metric dimension name: <ul style="list-style-type: none"> Built-in metric dimensions: _app, _comp, and _env are available, which are used to identify applications, components, and environments, respectively. Custom metric dimension: Enter a metric dimension name. Each name can contain 1 to 64 characters. Only letters, digits, and underscores (_) are allowed. Each name must start with a letter or underscore. <p>For a host, each metric dimension name must be unique.</p> Metric dimension value: Enter the value of a metric dimension. This value can be duplicate but cannot be empty. Each value can contain 1 to 128 characters. The following characters are not allowed: & ><\$;'!-() Up to 10 dimensions can be added. For example, if the dimension name is label1 and the dimension value is label2, label1:"label2" will be displayed.

Operation	Parameter	Description
	Advanced Settings	<p>Configure the following parameters:</p> <ul style="list-style-type: none">• Collection Period (s): O&M data collection period, in seconds. Options: 10s, 30s, and 60s (default).• Timeout Period (s): the maximum time allowed for executing a collection task, in seconds. Options: 10s, 30s, and 60s (default). The timeout period cannot exceed the collection period.• Executor: user who executes the collection task, that is, the user of the selected host. The default value is root. Currently, only the root user is supported.

Step 4 Set Exporter installation parameters and click **Install**. Click **View Log** to view Exporter installation logs.




Exporter collects monitoring data and regulates the data provided for external systems through Prometheus monitoring.

Parameter	Description
Kafka address	IP address and port number of Kafka, for example, 10.0.0.1:3306 .
SASL enabled	<p>Whether to enable Simple Authentication and Security Layer (SASL).</p> <ul style="list-style-type: none">• enabled: Enable SASL. If ciphertext access has been enabled for Kafka instances, enable SASL.• disabled: Disable SASL. If plaintext access has been enabled for Kafka instances, disable SASL. The default value is disabled.
SASL username	SASL username.
SASL password	SASL password.
SASL mechanism	Enter an SASL mechanism. Options: plain , scram-sha512 , and scram-sha256 . By default, this parameter is left blank.
TLS enabled	<p>Whether to enable Transport Layer Security (TLS) verification.</p> <ul style="list-style-type: none">• enabled: Enable TLS. If ciphertext access has been enabled for Kafka instances, enable TLS.• disabled: Disable TLS. If plaintext access has been enabled for Kafka instances, disable TLS. The default value is TLS.

Step 5 Click **Create** to connect the Kafka plug-in. The connected plug-in will be displayed on the **Collection Tasks** tab page of the plug-in card. Click the plug-in card. On the **Collection Tasks** tab page, click the target collection task to view its details.

You can also perform the operations listed in the following table on the collection task.

Table 12-20 Related operations

Operation	Description
Checking a collection task	Click a collection task to go to its details page.
Starting or stopping a collection task	Click the button in the Start/Stop column of a collection task to start or stop it.
Searching for a collection task	Set filter criteria or enter keywords to search for a collection task.
Changing target hosts	Click  in the Operation column of the target collection task. On the displayed page, change target hosts. You can only change the target hosts for the collection tasks created using custom plug-ins.
Sorting collection tasks	Click  in the Timeout Period or Collection Period column to sort collection tasks.
Copying a collection task	Click  in the Operation column of a collection task. On the displayed page, modify parameters as required.
Modifying a collection task	Choose ... > Modify in the Operation column of the target collection task. On the displayed page, modify parameters as required.
Deleting a collection task	Locate a collection task and choose ... > Delete in the Operation column. On the displayed page, confirm the deletion.

----End

12.8.4 Ingesting Nginx Metrics to AOM

Create a collection task and install Nginx Exporter to monitor Nginx metrics on a host.

Prerequisites

- **The UniAgent has been installed** and is running.
- **A Prometheus instance for ECS has been created.**

Procedure


Step 1 Log in to the AOM 2.0 console.


Step 2 In the navigation pane on the left, ingest middleware metrics:

- Choose **Prometheus Monitoring > Instances**. Click a Prometheus instance for ECS. On the instance details page, choose **Access Center** and then click the **Nginx** card.

Step 3 On the displayed page, set parameters by referring to the following table to configure a collection task and click **Next**.

Table 12-21 Parameters for configuring a collection task

Operation	Parameter	Description
Select Instance	Prometheus Instance	Select a Prometheus instance for ECS to store collected data. A collection task is associated with the Prometheus instance to mark and classify collected data. If no Prometheus instance is available, create one .
Set Plug-in	OS	Operating system of the host. Only Linux is supported.
	Collection Plug-in	The default value is NGINX .
	Plug-in Version	Select a plug-in version. Plug-in versions that have not been released are dimmed and cannot be selected.
Set Collection Task	Collection Task Name	Name of a collection task. Enter 1 to 50 characters starting with a letter. Only letters, digits, underscores (_), and hyphens (-) are allowed.
	Host	Click Add Host . On the Add Host page, select the host for configuring the collection task and installing Exporter. <ul style="list-style-type: none">Search for and select a host by the host name, IP address, or Agent status.You can click  in the upper right corner to deselect the selected host.Ensure that the UniAgent of the selected host is running. Otherwise, no data can be collected.

Operation	Parameter	Description
	Metric Dimension	<p>Click . In the displayed dialog box, select Built-in or Custom to add a metric dimension.</p> <ul style="list-style-type: none">• Metric dimension name:<ul style="list-style-type: none">– Built-in metric dimensions: _app, _comp, and _env are available, which are used to identify applications, components, and environments, respectively.– Custom metric dimension: Enter a metric dimension name. Each name can contain 1 to 64 characters. Only letters, digits, and underscores (<code>_</code>) are allowed. Each name must start with a letter or underscore. <p>For a host, each metric dimension name must be unique.</p> <ul style="list-style-type: none">• Metric dimension value: Enter the value of a metric dimension. This value can be duplicate but cannot be empty. Each value can contain 1 to 128 characters. The following characters are not allowed: <code>& ><\$;'!-()</code> <p>Up to 10 dimensions can be added. For example, if the dimension name is label1 and the dimension value is label2, label1:"label2" will be displayed.</p>
	Advanced Settings	<p>Configure the following parameters:</p> <ul style="list-style-type: none">• Collection Period (s): O&M data collection period, in seconds. Options: 10s, 30s, and 60s (default).• Timeout Period (s): the maximum time allowed for executing a collection task, in seconds. Options: 10s, 30s, and 60s (default). The timeout period cannot exceed the collection period.• Executor: user who executes the collection task, that is, the user of the selected host. The default value is root. Currently, only the root user is supported.

Step 4 Set Exporter installation parameters and click **Install**. Click **View Log** to view Exporter installation logs.




Exporter collects monitoring data and regulates the data provided for external systems through Prometheus monitoring.

Parameter	Description
Nginx URL	<p>Nginx URL, which is in the format of "Connection address of Nginx+Nginx service status path".</p> <ul style="list-style-type: none">• Connection address of Nginx: IP address and listening port number of the Nginx service. The listening port is specified in the nginx.conf file. Example: 10.0.0.1:8080• Nginx service status path: specified by the location parameter in the nginx.conf file, for example, /stub_status. <p>Example: https://10.0.0.1:8080/stub_status</p>

Step 5 Click **Create** to connect the Nginx plug-in. The connected plug-in will be displayed on the **Collection Tasks** tab page of the plug-in card. Click the plug-in card. On the **Collection Tasks** tab page, click the target collection task to view its details.

You can also perform the operations listed in the following table on the collection task.

Table 12-22 Related operations

Operation	Description
Checking a collection task	Click a collection task to go to its details page.
Starting or stopping a collection task	Click the button in the Start/Stop column of a collection task to start or stop it.
Searching for a collection task	Set filter criteria or enter keywords to search for a collection task.
Changing target hosts	Click  in the Operation column of the target collection task. On the displayed page, change target hosts. You can only change the target hosts for the collection tasks created using custom plug-ins.
Sorting collection tasks	Click  in the Timeout Period or Collection Period column to sort collection tasks.
Copying a collection task	Click  in the Operation column of a collection task. On the displayed page, modify parameters as required.
Modifying a collection task	Choose ... > Modify in the Operation column of the target collection task. On the displayed page, modify parameters as required.

Operation	Description
Deleting a collection task	Locate a collection task and choose ... > Delete in the Operation column. On the displayed page, confirm the deletion.

----End

12.8.5 Ingesting MongoDB Metrics to AOM

Create a collection task and install MongoDB Exporter to monitor MongoDB metrics on a host.

Prerequisites

- [The UniAgent has been installed](#) and is running.
- [A Prometheus instance for ECS has been created](#).

Procedure

Step 1 Log in to the AOM 2.0 console.



Step 2 In the navigation pane on the left, ingest middleware metrics:

- Choose **Prometheus Monitoring** > **Instances**. Click a Prometheus instance for ECS. On the instance details page, choose **Access Center** and then click the **MongoDB** card.

Step 3 On the displayed page, set parameters by referring to the following table to configure a collection task and click **Next**.

Table 12-23 Parameters for configuring a collection task

Operation	Parameter	Description
Select Instance	Prometheus Instance	Select a Prometheus instance for ECS to store collected data. A collection task is associated with the Prometheus instance to mark and classify collected data. If no Prometheus instance is available, create one .
Set Plug-in	OS	Operating system of the host. Only Linux is supported.
	Collection Plug-in	The default value is MONGODB .
	Plug-in Version	Select a plug-in version. Plug-in versions that have not been released are dimmed and cannot be selected.

Operation	Parameter	Description
Set Collection Task	Collection Task Name	Name of a collection task. Enter 1 to 50 characters starting with a letter. Only letters, digits, underscores (_), and hyphens (-) are allowed.
	Host	<p>Click Add Host. On the Add Host page, select the host for configuring the collection task and installing Exporter.</p> <ul style="list-style-type: none"> Search for and select a host by the host name, IP address, or Agent status. You can click  in the upper right corner to deselect the selected host. Ensure that the UniAgent of the selected host is running. Otherwise, no data can be collected.
	Metric Dimension	<p>Click . In the displayed dialog box, select Built-in or Custom to add a metric dimension.</p> <ul style="list-style-type: none"> Metric dimension name: <ul style="list-style-type: none"> Built-in metric dimensions: _app, _comp, and _env are available, which are used to identify applications, components, and environments, respectively. Custom metric dimension: Enter a metric dimension name. Each name can contain 1 to 64 characters. Only letters, digits, and underscores (_) are allowed. Each name must start with a letter or underscore. <p>For a host, each metric dimension name must be unique.</p> Metric dimension value: Enter the value of a metric dimension. This value can be duplicate but cannot be empty. Each value can contain 1 to 128 characters. The following characters are not allowed: & ><\$;'!-() Up to 10 dimensions can be added. For example, if the dimension name is label1 and the dimension value is label2, label1:"label2" will be displayed.

Operation	Parameter	Description
	Advanced Settings	<p>Configure the following parameters:</p> <ul style="list-style-type: none">• Collection Period (s): O&M data collection period, in seconds. Options: 10s, 30s, and 60s (default).• Timeout Period (s): the maximum time allowed for executing a collection task, in seconds. Options: 10s, 30s, and 60s (default). The timeout period cannot exceed the collection period.• Executor: user who executes the collection task, that is, the user of the selected host. The default value is root. Currently, only the root user is supported.

Step 4 Set Exporter installation parameters and click **Install**. Click **View Log** to view Exporter installation logs.

Exporter collects monitoring data and regulates the data provided for external systems through Prometheus monitoring.




Parameter	Description
MongoDB Address	IP address of MongoDB, for example, 10.0.0.1 .
MongoDB Port	Port number of MongoDB, for example, 3306 .
MongoDB Username	Username for logging in to MongoDB.
MongoDB Password	Password for logging in to MongoDB.

Step 5 Click **Create** to connect the MongoDB plug-in. The connected plug-in will be displayed on the **Collection Tasks** tab page of the plug-in card. Click the plug-in card. On the **Collection Tasks** tab page, click the target collection task to view its details.

You can also perform the operations listed in the following table on the collection task.

Table 12-24 Related operations

Operation	Description
Checking a collection task	Click a collection task to go to its details page.
Starting or stopping a collection task	Click the button in the Start/Stop column of a collection task to start or stop it.

Operation	Description
Searching for a collection task	Set filter criteria or enter keywords to search for a collection task.
Changing target hosts	Click  in the Operation column of the target collection task. On the displayed page, change target hosts. You can only change the target hosts for the collection tasks created using custom plug-ins.
Sorting collection tasks	Click  in the Timeout Period or Collection Period column to sort collection tasks.
Copying a collection task	Click  in the Operation column of a collection task. On the displayed page, modify parameters as required.
Modifying a collection task	Choose *** > Modify in the Operation column of the target collection task. On the displayed page, modify parameters as required.
Deleting a collection task	Locate a collection task and choose *** > Delete in the Operation column. On the displayed page, confirm the deletion.

----End

12.8.6 Ingesting Consul Metrics to AOM

Create a collection task and install Consul Exporter to monitor Consul metrics on a host.


Prerequisites


- [The UniAgent has been installed](#) and is running.
- [A Prometheus instance for ECS has been created](#).

Procedure

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane on the left, ingest middleware metrics:
 - Choose **Prometheus Monitoring** > **Instances**. Click a Prometheus instance for ECS. On the instance details page, choose **Access Center** and then click the **Consul** card.
- Step 3** On the displayed page, set parameters by referring to the following table to configure a collection task and click **Next**.

Table 12-25 Parameters for configuring a collection task

Operation	Parameter	Description
Select Instance	Prometheus Instance	Select a Prometheus instance for ECS to store collected data. A collection task is associated with the Prometheus instance to mark and classify collected data. If no Prometheus instance is available, create one .
Set Plug-in	OS	Operating system of the host. Only Linux is supported.
	Collection Plug-in	The default value is CONSUL .
	Plug-in Version	Select a plug-in version. Plug-in versions that have not been released are dimmed and cannot be selected.
Set Collection Task	Collection Task Name	Name of a collection task. Enter 1 to 50 characters starting with a letter. Only letters, digits, underscores (_), and hyphens (-) are allowed.
	Host	Click Add Host . On the Add Host page, select the host for configuring the collection task and installing Exporter. <ul style="list-style-type: none">• Search for and select a host by the host name, IP address, or Agent status.• You can click  in the upper right corner to deselect the selected host.• Ensure that the UniAgent of the selected host is running. Otherwise, no data can be collected.

Operation	Parameter	Description
	Metric Dimension	<p>Click . In the displayed dialog box, select Built-in or Custom to add a metric dimension.</p> <ul style="list-style-type: none">• Metric dimension name:<ul style="list-style-type: none">– Built-in metric dimensions: _app, _comp, and _env are available, which are used to identify applications, components, and environments, respectively.– Custom metric dimension: Enter a metric dimension name. Each name can contain 1 to 64 characters. Only letters, digits, and underscores (_) are allowed. Each name must start with a letter or underscore. <p>For a host, each metric dimension name must be unique.</p> <ul style="list-style-type: none">• Metric dimension value: Enter the value of a metric dimension. This value can be duplicate but cannot be empty. Each value can contain 1 to 128 characters. The following characters are not allowed: & ><\$;'!-() <p>Up to 10 dimensions can be added. For example, if the dimension name is label1 and the dimension value is label2, label1:"label2" will be displayed.</p>
	Advanced Settings	<p>Configure the following parameters:</p> <ul style="list-style-type: none">• Collection Period (s): O&M data collection period, in seconds. Options: 10s, 30s, and 60s (default).• Timeout Period (s): the maximum time allowed for executing a collection task, in seconds. Options: 10s, 30s, and 60s (default). The timeout period cannot exceed the collection period.• Executor: user who executes the collection task, that is, the user of the selected host. The default value is root. Currently, only the root user is supported.

Step 4 Set Exporter installation parameters and click **Install**. Click **View Log** to view Exporter installation logs.




Exporter collects monitoring data and regulates the data provided for external systems through Prometheus monitoring.

Parameter	Description
Consul Address	IP address and port number of Consul, for example, 10.0.0.1:3306 .

Step 5 Click **Create** to connect the Consul plug-in. The connected plug-in will be displayed on the **Collection Tasks** tab page of the plug-in card. Click the plug-in card. On the **Collection Tasks** tab page, click the target collection task to view its details.

You can also perform the operations listed in the following table on the collection task.

Table 12-26 Related operations

Operation	Description
Checking a collection task	Click a collection task to go to its details page.
Starting or stopping a collection task	Click the button in the Start/Stop column of a collection task to start or stop it.
Searching for a collection task	Set filter criteria or enter keywords to search for a collection task.
Changing target hosts	Click  in the Operation column of the target collection task. On the displayed page, change target hosts. You can only change the target hosts for the collection tasks created using custom plug-ins.
Sorting collection tasks	Click  in the Timeout Period or Collection Period column to sort collection tasks.
Copying a collection task	Click  in the Operation column of a collection task. On the displayed page, modify parameters as required.
Modifying a collection task	Choose ... > Modify in the Operation column of the target collection task. On the displayed page, modify parameters as required.
Deleting a collection task	Locate a collection task and choose ... > Delete in the Operation column. On the displayed page, confirm the deletion.

----End

12.8.7 Ingesting HAProxy Metrics to AOM

Create a collection task and install HAProxy Exporter to monitor HAProxy metrics on a host.

Prerequisites



- **The UniAgent has been installed** and is running.
- **A Prometheus instance for ECS has been created.**

Procedure

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane on the left, ingest middleware metrics:
- Choose **Prometheus Monitoring > Instances**. Click a Prometheus instance for ECS. On the instance details page, choose **Access Center** and then click the **HAProxy** card.
- Step 3** On the displayed page, set parameters by referring to the following table to configure a collection task and click **Next**.

Table 12-27 Parameters for configuring a collection task

Operation	Parameter	Description
Select Instance	Prometheus Instance	Select a Prometheus instance for ECS to store collected data. A collection task is associated with the Prometheus instance to mark and classify collected data. If no Prometheus instance is available, create one .
Set Plug-in	OS	Operating system of the host. Only Linux is supported.
	Collection Plug-in	The default value is HAPROXY .
	Plug-in Version	Select a plug-in version. Plug-in versions that have not been released are dimmed and cannot be selected.
Set Collection Task	Collection Task Name	Name of a collection task. Enter 1 to 50 characters starting with a letter. Only letters, digits, underscores (_), and hyphens (-) are allowed.

Operation	Parameter	Description
	Host	<p>Click Add Host. On the Add Host page, select the host for configuring the collection task and installing Exporter.</p> <ul style="list-style-type: none"> • Search for and select a host by the host name, IP address, or Agent status. • You can click  in the upper right corner to deselect the selected host. • Ensure that the UniAgent of the selected host is running. Otherwise, no data can be collected.
	Metric Dimension	<p>Click . In the displayed dialog box, select Built-in or Custom to add a metric dimension.</p> <ul style="list-style-type: none"> • Metric dimension name: <ul style="list-style-type: none"> – Built-in metric dimensions: _app, _comp, and _env are available, which are used to identify applications, components, and environments, respectively. – Custom metric dimension: Enter a metric dimension name. Each name can contain 1 to 64 characters. Only letters, digits, and underscores (_) are allowed. Each name must start with a letter or underscore. <p>For a host, each metric dimension name must be unique.</p> • Metric dimension value: Enter the value of a metric dimension. This value can be duplicate but cannot be empty. Each value can contain 1 to 128 characters. The following characters are not allowed: & ><\$;'!-() <p>Up to 10 dimensions can be added. For example, if the dimension name is label1 and the dimension value is label2, label1:"label2" will be displayed.</p>
	Advanced Settings	<p>Configure the following parameters:</p> <ul style="list-style-type: none"> • Collection Period (s): O&M data collection period, in seconds. Options: 10s, 30s, and 60s (default). • Timeout Period (s): the maximum time allowed for executing a collection task, in seconds. Options: 10s, 30s, and 60s (default). The timeout period cannot exceed the collection period. • Executor: user who executes the collection task, that is, the user of the selected host. The default value is root. Currently, only the root user is supported.

- Step 4** Set Exporter installation parameters and click **Install**. Click **View Log** to view Exporter installation logs.




Exporter collects monitoring data and regulates the data provided for external systems through Prometheus monitoring.

Parameter	Description
HAProxy URL	<p>HAProxy connection address, which must be in the format of "http://{username}:{password}@{IP address}:{port}/haproxy_stats;csv".</p> <ul style="list-style-type: none">• {username}: username for logging in to HAProxy.• {password}: password for logging in to HAProxy.• {IP}:{port}: HAProxy IP address and port number, for example, 10.0.0.1:3306. <p>Example: http://admin:*****@10.0.0.1:3306/haproxy_stats;csv</p>

- Step 5** Click **Install** to connect the HAProxy plug-in. The connected plug-in will be displayed on the **Collection Tasks** tab page of the plug-in card. Click the plug-in card. On the **Collection Tasks** tab page, click the target collection task to view its details.

You can also perform the operations listed in the following table on the collection task.

Table 12-28 Related operations

Operation	Description
Checking a collection task	Click a collection task to go to its details page.
Starting or stopping a collection task	Click the button in the Start/Stop column of a collection task to start or stop it.
Searching for a collection task	Set filter criteria or enter keywords to search for a collection task.
Changing target hosts	<p>Click  in the Operation column of the target collection task. On the displayed page, change target hosts.</p> <p>You can only change the target hosts for the collection tasks created using custom plug-ins.</p>
Sorting collection tasks	Click  in the Timeout Period or Collection Period column to sort collection tasks.
Copying a collection task	Click  in the Operation column of a collection task. On the displayed page, modify parameters as required.

Operation	Description
Modifying a collection task	Choose *** > Modify in the Operation column of the target collection task. On the displayed page, modify parameters as required.
Deleting a collection task	Locate a collection task and choose *** > Delete in the Operation column. On the displayed page, confirm the deletion.

----End

12.8.8 Ingesting PostgreSQL Metrics to AOM

Create a collection task and install PostgreSQL Exporter to monitor PostgreSQL metrics on a host.

Prerequisites

- [The UniAgent has been installed](#) and is running.
- [A Prometheus instance for ECS has been created](#).

Procedure

Step 1 Log in to the AOM 2.0 console.



Step 2 In the navigation pane on the left, ingest middleware metrics:

- Choose **Prometheus Monitoring** > **Instances**. Click a Prometheus instance for ECS. On the instance details page, choose **Access Center** and then click the **PostgreSQL** card.

Step 3 On the displayed page, set parameters by referring to the following table to configure a collection task and click **Next**.

Table 12-29 Parameters for configuring a collection task

Operation	Parameter	Description
Select Instance	Prometheus Instance	Select a Prometheus instance for ECS to store collected data. A collection task is associated with the Prometheus instance to mark and classify collected data. If no Prometheus instance is available, create one .
Set Plug-in	OS	Operating system of the host. Only Linux is supported.
	Collection Plug-in	The default value is POSTGRESQL .

Operation	Parameter	Description
	Plug-in Version	Select a plug-in version. Plug-in versions that have not been released are dimmed and cannot be selected.
Set Collection Task	Collection Task Name	Name of a collection task. Enter 1 to 50 characters starting with a letter. Only letters, digits, underscores (_), and hyphens (-) are allowed.
	Host	<p>Click Add Host. On the Add Host page, select the host for configuring the collection task and installing Exporter.</p> <ul style="list-style-type: none"> Search for and select a host by the host name, IP address, or Agent status. You can click  in the upper right corner to deselect the selected host. Ensure that the UniAgent of the selected host is running. Otherwise, no data can be collected.
	Metric Dimension	<p>Click . In the displayed dialog box, select Built-in or Custom to add a metric dimension.</p> <ul style="list-style-type: none"> Metric dimension name: <ul style="list-style-type: none"> Built-in metric dimensions: _app, _comp, and _env are available, which are used to identify applications, components, and environments, respectively. Custom metric dimension: Enter a metric dimension name. Each name can contain 1 to 64 characters. Only letters, digits, and underscores (_) are allowed. Each name must start with a letter or underscore. <p>For a host, each metric dimension name must be unique.</p> Metric dimension value: Enter the value of a metric dimension. This value can be duplicate but cannot be empty. Each value can contain 1 to 128 characters. The following characters are not allowed: & ><\$;'!-() Up to 10 dimensions can be added. For example, if the dimension name is label1 and the dimension value is label2, label1:"label2" will be displayed.

Operation	Parameter	Description
	Advanced Settings	<p>Configure the following parameters:</p> <ul style="list-style-type: none">• Collection Period (s): O&M data collection period, in seconds. Options: 10s, 30s, and 60s (default).• Timeout Period (s): the maximum time allowed for executing a collection task, in seconds. Options: 10s, 30s, and 60s (default). The timeout period cannot exceed the collection period.• Executor: user who executes the collection task, that is, the user of the selected host. The default value is root. Currently, only the root user is supported.

Step 4 Set Exporter installation parameters and click **Install**. Click **View Log** to view Exporter installation logs.

Exporter collects monitoring data and regulates the data provided for external systems through Prometheus monitoring.




Parameter	Description
PostgreSQL Username	PostgreSQL username.
PostgreSQL Password	PostgreSQL password.
PostgreSQL Address	<p>PostgreSQL connection address. For example, <i>{IP}:{port}/databasename</i>.</p> <ul style="list-style-type: none">• <i>{IP}:{port}</i>: PostgreSQL IP address and port number, for example, 10.0.0.1:3306.• <i>{databasename}</i>: PostgreSQL database name. <p>Example: 10.0.0.1:3306/xxxx.</p>

Step 5 Click **Create** to connect the PostgreSQL plug-in. The connected plug-in will be displayed on the **Collection Tasks** tab page of the plug-in card. Click the plug-in card. On the **Collection Tasks** tab page, click the target collection task to view its details.

You can also perform the operations listed in the following table on the collection task.

Table 12-30 Related operations

Operation	Description
Checking a collection task	Click a collection task to go to its details page.

Operation	Description
Starting or stopping a collection task	Click the button in the Start/Stop column of a collection task to start or stop it.
Searching for a collection task	Set filter criteria or enter keywords to search for a collection task.
Changing target hosts	Click  in the Operation column of the target collection task. On the displayed page, change target hosts. You can only change the target hosts for the collection tasks created using custom plug-ins.
Sorting collection tasks	Click  in the Timeout Period or Collection Period column to sort collection tasks.
Copying a collection task	Click  in the Operation column of a collection task. On the displayed page, modify parameters as required.
Modifying a collection task	Choose ... > Modify in the Operation column of the target collection task. On the displayed page, modify parameters as required.
Deleting a collection task	Locate a collection task and choose ... > Delete in the Operation column. On the displayed page, confirm the deletion.

----End

12.8.9 Ingesting Elasticsearch Metrics to AOM

Create a collection task and install Elasticsearch Exporter to monitor Elasticsearch metrics on a host.

Prerequisites

- [The UniAgent has been installed](#) and is running.
- [A Prometheus instance for ECS has been created](#).

Procedure


Step 1 Log in to the AOM 2.0 console.


Step 2 In the navigation pane on the left, ingest middleware metrics:

- Choose **Prometheus Monitoring** > **Instances**. Click a Prometheus instance for ECS. On the instance details page, choose **Access Center** and then click the **Elasticsearch** card.

Step 3 On the displayed page, set parameters by referring to the following table to configure a collection task and click **Next**.

Table 12-31 Parameters for configuring a collection task

Operation	Parameter	Description
Select Instance	Prometheus Instance	Select a Prometheus instance for ECS to store collected data. A collection task is associated with the Prometheus instance to mark and classify collected data. If no Prometheus instance is available, create one .
Set Plug-in	OS	Operating system of the host. Only Linux is supported.
	Collection Plug-in	The default value is ELASTICSEARCH .
	Plug-in Version	Select a plug-in version. Plug-in versions that have not been released are dimmed and cannot be selected.
Set Collection Task	Collection Task Name	Name of a collection task. Enter 1 to 50 characters starting with a letter. Only letters, digits, underscores (_), and hyphens (-) are allowed.
	Host	Click Add Host . On the Add Host page, select the host for configuring the collection task and installing Exporter. <ul style="list-style-type: none"> Search for and select a host by the host name, IP address, or Agent status. You can click  in the upper right corner to deselect the selected host. Ensure that the UniAgent of the selected host is running. Otherwise, no data can be collected.

Operation	Parameter	Description
	Metric Dimension	<p>Click . In the displayed dialog box, select Built-in or Custom to add a metric dimension.</p> <ul style="list-style-type: none">• Metric dimension name:<ul style="list-style-type: none">– Built-in metric dimensions: _app, _comp, and _env are available, which are used to identify applications, components, and environments, respectively.– Custom metric dimension: Enter a metric dimension name. Each name can contain 1 to 64 characters. Only letters, digits, and underscores (_) are allowed. Each name must start with a letter or underscore. <p>For a host, each metric dimension name must be unique.</p> <ul style="list-style-type: none">• Metric dimension value: Enter the value of a metric dimension. This value can be duplicate but cannot be empty. Each value can contain 1 to 128 characters. The following characters are not allowed: & ><\$;'!-() <p>Up to 10 dimensions can be added. For example, if the dimension name is label1 and the dimension value is label2, label1:"label2" will be displayed.</p>
	Advanced Settings	<p>Configure the following parameters:</p> <ul style="list-style-type: none">• Collection Period (s): O&M data collection period, in seconds. Options: 10s, 30s, and 60s (default).• Timeout Period (s): the maximum time allowed for executing a collection task, in seconds. Options: 10s, 30s, and 60s (default). The timeout period cannot exceed the collection period.• Executor: user who executes the collection task, that is, the user of the selected host. The default value is root. Currently, only the root user is supported.

Step 4 Set Exporter installation parameters and click **Install**. Click **View Log** to view Exporter installation logs.




Exporter collects monitoring data and regulates the data provided for external systems through Prometheus monitoring.

Parameter	Description
Elasticsearch URL	<p>Elasticsearch connection address. Format: http://<i>{username}</i>:<i>{password}</i>@<i>{IP}</i>:<i>{port}</i>.</p> <ul style="list-style-type: none">• <i>{username}</i>: username for logging in to Elasticsearch.• <i>{password}</i>: password for logging in to Elasticsearch.• <i>{IP}</i>:<i>{port}</i>: Elasticsearch IP address and port number, for example, 10.0.0.1:3306. <p>Example: http://admin:****.*****@10.0.0.1:3306.</p>

Step 5 Click **Create** to connect the Elasticsearch plug-in. The connected plug-in will be displayed on the **Collection Tasks** tab page of the plug-in card. Click the plug-in card. On the **Collection Tasks** tab page, click the target collection task to view its details.

You can also perform the operations listed in the following table on the collection task.

Table 12-32 Related operations

Operation	Description
Checking a collection task	Click a collection task to go to its details page.
Starting or stopping a collection task	Click the button in the Start/Stop column of a collection task to start or stop it.
Searching for a collection task	Set filter criteria or enter keywords to search for a collection task.
Changing target hosts	<p>Click  in the Operation column of the target collection task. On the displayed page, change target hosts.</p> <p>You can only change the target hosts for the collection tasks created using custom plug-ins.</p>
Sorting collection tasks	Click  in the Timeout Period or Collection Period column to sort collection tasks.
Copying a collection task	Click  in the Operation column of a collection task. On the displayed page, modify parameters as required.
Modifying a collection task	Choose ... > Modify in the Operation column of the target collection task. On the displayed page, modify parameters as required.

Operation	Description
Deleting a collection task	Locate a collection task and choose ... > Delete in the Operation column. On the displayed page, confirm the deletion.

----End

12.8.10 Ingesting RabbitMQ Metrics to AOM

Create a collection task and install RabbitMQ Exporter to monitor RabbitMQ metrics on a host.

Prerequisites

- [The UniAgent has been installed](#) and is running.
- [A Prometheus instance for ECS has been created](#).

Procedure

Step 1 Log in to the AOM 2.0 console.



Step 2 In the navigation pane on the left, ingest middleware metrics:

- Choose **Prometheus Monitoring** > **Instances**. Click a Prometheus instance for ECS. On the instance details page, choose **Access Center** and then click the **RabbitMQ** card.

Step 3 On the displayed page, set parameters by referring to the following table to configure a collection task and click **Next**.

Table 12-33 Parameters for configuring a collection task

Operation	Parameter	Description
Select Instance	Prometheus Instance	Select a Prometheus instance for ECS to store collected data. A collection task is associated with the Prometheus instance to mark and classify collected data. If no Prometheus instance is available, create one .
Set Plug-in	OS	Operating system of the host. Only Linux is supported.
	Collection Plug-in	The default value is RABBITMQ .
	Plug-in Version	Select a plug-in version. Plug-in versions that have not been released are dimmed and cannot be selected.

Operation	Parameter	Description
Set Collection Task	Collection Task Name	Name of a collection task. Enter 1 to 50 characters starting with a letter. Only letters, digits, underscores (_), and hyphens (-) are allowed.
	Host	<p>Click Add Host. On the Add Host page, select the host for configuring the collection task and installing Exporter.</p> <ul style="list-style-type: none"> Search for and select a host by the host name, IP address, or Agent status. You can click  in the upper right corner to deselect the selected host. Ensure that the UniAgent of the selected host is running. Otherwise, no data can be collected.
	Metric Dimension	<p>Click . In the displayed dialog box, select Built-in or Custom to add a metric dimension.</p> <ul style="list-style-type: none"> Metric dimension name: <ul style="list-style-type: none"> Built-in metric dimensions: _app, _comp, and _env are available, which are used to identify applications, components, and environments, respectively. Custom metric dimension: Enter a metric dimension name. Each name can contain 1 to 64 characters. Only letters, digits, and underscores (_) are allowed. Each name must start with a letter or underscore. <p>For a host, each metric dimension name must be unique.</p> Metric dimension value: Enter the value of a metric dimension. This value can be duplicate but cannot be empty. Each value can contain 1 to 128 characters. The following characters are not allowed: & ><\$;'!-() Up to 10 dimensions can be added. For example, if the dimension name is label1 and the dimension value is label2, label1:"label2" will be displayed.

Operation	Parameter	Description
	Advanced Settings	Configure the following parameters: <ul style="list-style-type: none">• Collection Period (s): O&M data collection period, in seconds. Options: 10s, 30s, and 60s (default).• Timeout Period (s): the maximum time allowed for executing a collection task, in seconds. Options: 10s, 30s, and 60s (default). The timeout period cannot exceed the collection period.• Executor: user who executes the collection task, that is, the user of the selected host. The default value is root. Currently, only the root user is supported.

Step 4 Set Exporter installation parameters and click **Install**. Click **View Log** to view Exporter installation logs.

Exporter collects monitoring data and regulates the data provided for external systems through Prometheus monitoring.




Parameter	Description
RabbitMQ Username	RabbitMQ username.
RabbitMQ Password	RabbitMQ password.
RabbitMQ Address	IP address and port number of RabbitMQ, for example, 10.0.0.1:3306 .

Step 5 Click **Create** to connect the RabbitMQ plug-in. The connected plug-in will be displayed on the **Collection Tasks** tab page of the plug-in card. Click the plug-in card. On the **Collection Tasks** tab page, click the target collection task to view its details.

You can also perform the operations listed in the following table on the collection task.

Table 12-34 Related operations

Operation	Description
Checking a collection task	Click a collection task to go to its details page.
Starting or stopping a collection task	Click the button in the Start/Stop column of a collection task to start or stop it.

Operation	Description
Searching for a collection task	Set filter criteria or enter keywords to search for a collection task.
Changing target hosts	Click  in the Operation column of the target collection task. On the displayed page, change target hosts. You can only change the target hosts for the collection tasks created using custom plug-ins.
Sorting collection tasks	Click  in the Timeout Period or Collection Period column to sort collection tasks.
Copying a collection task	Click  in the Operation column of a collection task. On the displayed page, modify parameters as required.
Modifying a collection task	Choose ... > Modify in the Operation column of the target collection task. On the displayed page, modify parameters as required.
Deleting a collection task	Locate a collection task and choose ... > Delete in the Operation column. On the displayed page, confirm the deletion.

----End

12.8.11 Ingesting Other Middleware Metrics to AOM

If existing middleware Exporters do not meet your requirements, install your own Exporter and create a collection task to monitor middleware metrics.

Prerequisites

- [The UniAgent has been installed](#) and is running.
- [A Prometheus instance for ECS has been created](#).

Procedure


Step 1 Log in to the AOM 2.0 console.


Step 2 In the navigation pane on the left, ingest middleware metrics:

- Choose **Prometheus Monitoring** > **Instances**. Click a Prometheus instance for ECS. On the instance details page, choose **Access Center** and then click the **Other components** card.

Step 3 On the displayed page, set parameters by referring to the following table.

Table 12-35 Parameters for configuring a collection task

Operation	Parameter	Description
Select Instance	Prometheus Instance	Select a Prometheus instance for ECS to store collected data. A collection task is associated with the Prometheus instance to mark and classify collected data. If no Prometheus instance is available, create one .
Set Plug-in	OS	Operating system of the host. Only Linux is supported.
	Collection Plug-in	The default value is CUSTOM_EXPORTER .
	Plug-in Version	Select a plug-in version. Plug-in versions that have not been released are dimmed and cannot be selected.
Set Collection Task	Collection Task Name	Name of a collection task. Enter 1 to 50 characters starting with a letter. Only letters, digits, underscores (_), and hyphens (-) are allowed.
	Host	Click Add Host . On the Add Host page, select the host for configuring the collection task and installing Exporter. <ul style="list-style-type: none"> Search for and select a host by the host name, IP address, or Agent status. You can click  in the upper right corner to deselect the selected host. Ensure that the UniAgent of the selected host is running. Otherwise, no data can be collected.
	Plug-in Collection Parameters	Exporter Address: IP address and port number of the host where Exporter is installed. The format is "IP address:Port", for example, 10.0.0.1:9100




Operation	Parameter	Description
	Metric Dimension	<p>Click . In the displayed dialog box, select Built-in or Custom to add a metric dimension.</p> <ul style="list-style-type: none"> Metric dimension name: <ul style="list-style-type: none"> Built-in metric dimensions: _app, _comp, and _env are available, which are used to identify applications, components, and environments, respectively. Custom metric dimension: Enter a metric dimension name. Each name can contain 1 to 64 characters. Only letters, digits, and underscores (<code>_</code>) are allowed. Each name must start with a letter or underscore. <p>For a host, each metric dimension name must be unique.</p> Metric dimension value: Enter the value of a metric dimension. This value can be duplicate but cannot be empty. Each value can contain 1 to 128 characters. The following characters are not allowed: <code>& ><\$;'!-()</code> <p>Up to 10 dimensions can be added. For example, if the dimension name is label1 and the dimension value is label2, label1:"label2" will be displayed.</p>
	Advanced Settings	<p>Configure the following parameters:</p> <ul style="list-style-type: none"> Collection Period (s): O&M data collection period, in seconds. Options: 10s, 30s, and 60s (default). Timeout Period (s): the maximum time allowed for executing a collection task, in seconds. Options: 10s, 30s, and 60s (default). The timeout period cannot exceed the collection period. Executor: user who executes the collection task, that is, the user of the selected host. The default value is root. Currently, only the root user is supported.

Step 4 Click **Create**.

Step 5 The connected plug-in will be displayed on the **Collection Tasks** tab page of the plug-in card. Click the plug-in card. On the **Collection Tasks** tab page, click the target collection task to view its details.

You can also perform the operations listed in the following table on the collection task.

Table 12-36 Related operations

Operation	Description
Checking a collection task	Click a collection task to go to its details page.
Starting or stopping a collection task	Click the button in the Start/Stop column of a collection task to start or stop it.
Searching for a collection task	Set filter criteria or enter keywords to search for a collection task.
Changing target hosts	Click  in the Operation column of the target collection task. On the displayed page, change target hosts. You can only change the target hosts for the collection tasks created using custom plug-ins.
Sorting collection tasks	Click  in the Timeout Period or Collection Period column to sort collection tasks.
Copying a collection task	Click  in the Operation column of a collection task. On the displayed page, modify parameters as required.
Modifying a collection task	Choose ... > Modify in the Operation column of the target collection task. On the displayed page, modify parameters as required.
Deleting a collection task	Locate a collection task and choose ... > Delete in the Operation column. On the displayed page, confirm the deletion.

----End

12.9 Configuring the Remote Read Address to Enable Self-built Prometheus to Read Data from AOM

Prometheus monitoring provides the remote read API, which can categorize a series of Prometheus protocol data sources into oen single data source for query. This section describes how to read AOM Prometheus instance data through the remote read API when you use self-built Prometheus.

Constraints

When configuring Prometheus for remote read, ensure that **global:external_labels****: is correct since **external_labels** will be added to the search criteria. If a label is incorrect, required data may fail to be queried.


You can set **filter_external_labels: false** (Prometheus: v2.34 or later) to prevent **external_labels** from being added to the search criteria.

Prerequisite

Your service has been connected for Prometheus monitoring. For details, see [12.2 Managing Prometheus Instances](#).

Configuring the Remote Read Address

You are advised to configure the **prometheus.yml** file of self-built Prometheus.
Procedure:

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane on the left, choose **Prometheus Monitoring > Instances**. In the instance list, click the target Prometheus instance to go to the details page.
- Step 3** In the navigation pane on the left, choose **Settings**. On the **Intranet** tab page in the **Service Addresses** area, click  on the right to copy the configuration code for Prometheus remote read.

```
remote_read:
  - url: 'https://{region_name}-{Site domain name suffix}/v1/{project_id}/
    {prometheus_instance_id}/api/v1/read'
  tls_config:
    insecure_skip_verify: true
    bearer_token: '8H**LP'
  read_recent: true
```

- Step 4** Add the copied configuration code to the **prometheus.yml** file of self-built Prometheus.
- Step 5** Restart the self-built Prometheus service.

Then you can view AOM Prometheus data.

-----End

Complete Configuration Items of Remote Read

The configuration items in brackets ([]) are optional. The following lists the configurations of Prometheus v2.40. Some configuration items may be unavailable in earlier versions. For details, see [Prometheus official documents](#).

```
# API URL of the target Prometheus instance for remote read
url: <string>

# Unique name of a configuration for remote read
[ name: <string> ]

# Filtering conditions that must be contained in PromQL for remote read
required_matchers:
  [ <labelname>: <labelvalue> ... ]

# Timeout for remote read query
[ remote_timeout: <duration> | default = 1m ]

# Custom headers attached to remote read requests, which cannot overwrite the headers added by
Prometheus
headers:
  [ <string>: <string> ... ]

# Whether to directly read metrics from the local storage during Prometheus remote read
[ read_recent: <boolean> | default = false ]

# Add an authorization header for each remote read request. Select either password or password_file.
```

```
basic_auth:
  [ username: <string> ]
  [ password: <secret> ]
  [ password_file: <string> ]

# Custom authorization header configuration
authorization:
  # Authentication type
  [ type: <string> | default: Bearer ]
  #Authentication key. Select either credentials or credentials_file.
  [ credentials: <secret> ]
# Obtain the key from a file.
  [ credentials_file: <filename> ]

# OAuth 2.0 authentication, which cannot be used together with basic_auth authorization
oauth2:
  [ <oauth2> ]

# TLS configuration
tls_config:
  [ <tls_config> ]

# Proxy URL
[ proxy_url: <string> ]

# Whether 3XX redirection is allowed
[ follow_redirects: <boolean> | default = true ]

# Whether to enable HTTP2
[ enable_http2: <bool> | default: true ]

# Whether to attach external_labels during remote read
[ filter_external_labels: <boolean> | default = true ]
```

12.10 Configuring the Remote Write Address to Report Self-Built Prometheus Data to AOM

AOM can obtain the remote write address of a 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.

Prerequisites

- You have created an ECS.
- Your service has been connected for Prometheus monitoring. For details, see [12.2 Managing Prometheus Instances](#).

Reporting Self-Built Prometheus Instance Data to AOM

Step 1 Install and start open-source Prometheus. For details, see [Prometheus official documents](#). (Skip this step if open-source Prometheus has been deployed.)

Step 2 Add an access code.

1. Log in to the AOM 2.0 console.
2. In the navigation pane, choose **Settings > Global Settings**. The **Global Settings** page is displayed.
3. On the displayed page, choose **Authentication** in the navigation pane. Click **Add Access Code**.

4. In the dialog box that is displayed, click **OK**. The system then automatically generates an access code.

An access code is an identity credential for calling APIs. A maximum of two access codes can be created for each project. Keep them 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 **Prometheus Monitoring > Instances**. In the instance list, click the name of the target Prometheus instance.
3. On the displayed page, choose **Settings** in the navigation pane and click  on the right to copy the configuration code for Prometheus remote write from the **Service Addresses** area.

Figure 12-4 Configuration code for Prometheus remote write

Configuration Code for Prometheus Remote Write

```
remote_write:
- url: 'https://aom-
  ts_config:
    insecure_skip_verify: true
    bearer_token: 'Cv+H5'
```

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

1. Run the following command to find and start the **prometheus.yml** file:
./prometheus --config.file=prometheus.yml
2. 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

12.11 Checking Prometheus Instance Data Through 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 details, see [12.2 Managing Prometheus Instances](#).

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 **Settings > Global Settings**. The **Global Settings** page is displayed.
3. On the displayed page, choose **Authentication** in the navigation pane. Click **Add Access Code**.
4. In the dialog box that is displayed, click **OK**. The system then automatically generates an access code.

An access code is an identity credential for calling APIs. A maximum of two access codes can be created for each project. Keep them secure.

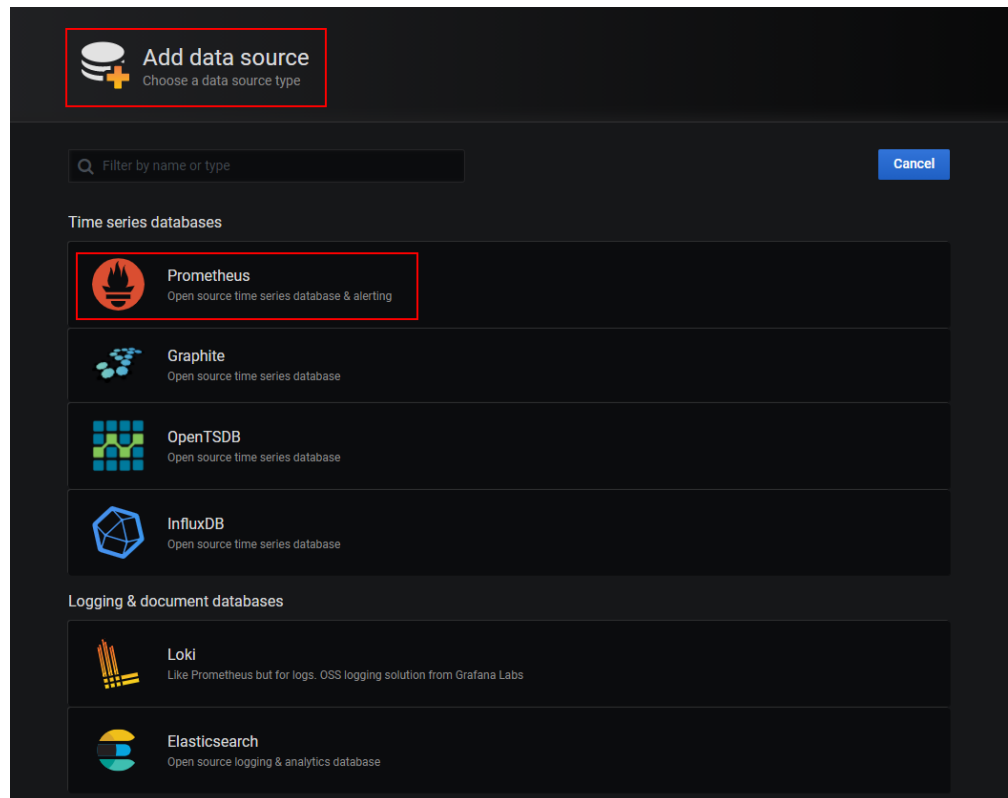
Step 3 Obtain the Grafana data source configuration code.

1. Log in to the AOM 2.0 console.
2. In the navigation pane on the left, choose **Prometheus Monitoring > Instances**. In the instance list, click the name of 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 **Connections > Data Sources**. Then click **Add data source**.
(Configuration parameters may vary depending on the Grafana version. Configure the parameters based on site requirements.)
3. Click **Prometheus** to access the configuration page.

Figure 12-5 Prometheus configuration page



4. Set Grafana data source parameters.
 - **Prometheus server URL**: HTTP URL obtained in [Step 3.3](#).
 - **User**: username obtained in [Step 3.3](#).
 - **Password**: password obtained in [Step 3.3](#).

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

Figure 12-6 Setting parameters

Name ⓘ Prometheus-5

Default ☐

HTTP

Prometheus server URL ⓘ http://localhost:9090

Allowed cookies ⓘ New tag (enter key to add)

Add

Timeout ⓘ Timeout in seconds

Auth

Basic auth ☒ With Credentials ⓘ ☐

TLS Client Auth ☐ With CA Cert ⓘ ☐

Skip TLS Verify ☒

Forward OAuth Identity ⓘ ☐

Basic Auth Details

User user

Password Password

Custom HTTP Headers

+ Add header

If the current version supports the configuration of performance parameters under **Advanced settings**, set **Prometheus type** to **Cortex** and **Cortex version** to **1.0.0**.

Performance

Prometheus type ⓘ Cortex

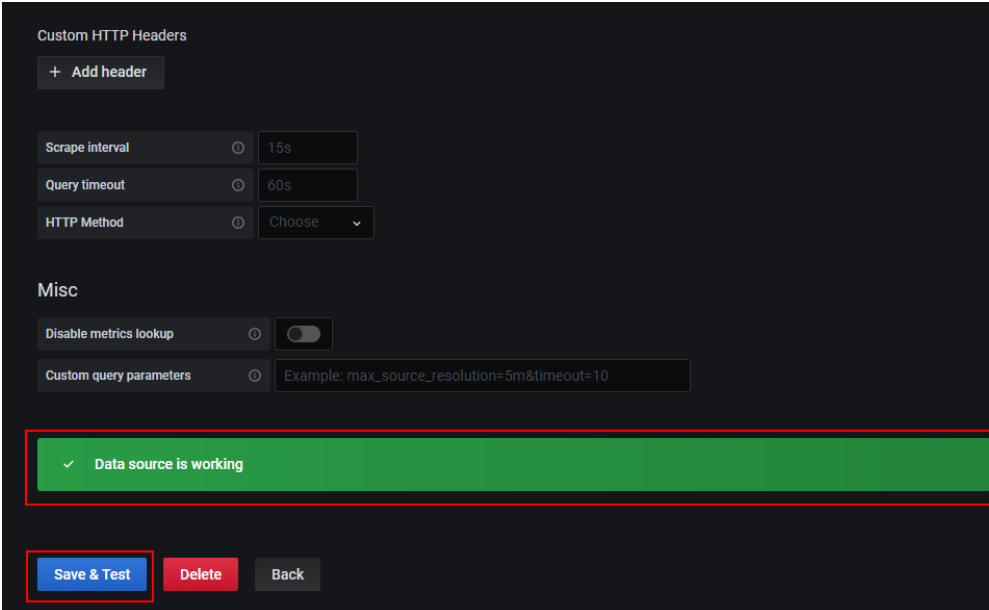
Cortex version ⓘ 1.0.0

Cache level ⓘ Low

Incremental querying (beta) ⓘ ☐

Disable recording rules (beta) ⓘ ☐

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 12-7 Checking whether the configuration is successful

----End

12.12 Checking the Number of Metric Samples Reported by Prometheus Instances

After metric data is reported to AOM through Prometheus monitoring, you can view the number of basic and custom metric samples reported by Prometheus instances.

Prerequisites

- Your service has been connected for Prometheus monitoring. For details, see [12.2 Managing Prometheus Instances](#).


Constraints

- 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 **Usage Statistics** 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 **Prometheus Monitoring > Usage Statistics**.
- 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. You can use a predefined time label, such as **Last hour** and **Last 6 hours**, or customize a time range. Max.: 30 days.

You are advised to select a time range longer than 1 hour.

2. Set the interval for refreshing information. Click the drop-down arrow next to  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

13 Infrastructure Monitoring

13.1 Using AOM to Monitor Workloads


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.

Function Introduction

- 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 Observability 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 **Infrastructure Monitoring > Container Insights > Workloads**.
- Step 3** In the upper right corner of the page, set filter criteria.
1. Set a time range to check the workloads reported. You can use a predefined time label, such as **Last hour** and **Last 6 hours**, or customize a time range. Max.: 30 days.

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.

To query namespaces, IAM users with the **AOM ReadOnlyAccess** permission need to log in to the CCE console, choose **Permissions** in the navigation pane, and click **Add Permission** in the upper right corner of the page to add required permissions. For CCE namespaces, users or user groups should be granted with read-only (view) or custom permissions. If custom permissions are granted, the list operation permission must be included and namespace resources must also be specified. .

- 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 **Logs** tab page, view the raw and real-time logs of the workload and analyze them as required.
 - On the **Alarms** tab page, view the alarm details of the workload. For details, see [9.4 Checking AOM Alarms or Events](#).
 - On the **Events** tab page, view the event details of the workload. For details, see [9.4 Checking AOM Alarms or Events](#).

----End

13.2 Using AOM to Monitor Clusters

Clusters deployed using CCE are monitored. Through cluster monitoring, 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.

Constraints

- 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.

- To use CCE functions on the AOM console, you need to obtain CCE permissions in advance.


Procedure

Step 1 Log in to the AOM 2.0 console.

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


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

1. Set a time range to check the CCE clusters reported. You can use a predefined time label, such as **Last hour** and **Last 6 hours**, or customize a time range. Max.: 30 days.

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 cluster name to filter the target cluster. You can also sort clusters by creation time, CPU usage, or memory usage.


Step 5 Click a cluster to go to its details page. In the navigation pane on the left, monitor cluster running conditions by cluster, on dashboards, or through **Alarm Management**.




- 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.

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 [12.4 Using Prometheus Monitoring to Monitor CCE Cluster Metrics](#). After the instance is created, click its name. On the instance details page, choose **Integration Center** and then connect the CCE cluster.

Click the time selection box 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. Check nodes, workloads, and container groups by name.
- Check the cluster running status through **Alarm Management**.
 - In the navigation pane on the left, choose **Alarm Management > Alarm List** to view alarm details of the cluster. For details, see [9.4 Checking AOM Alarms or Events](#).
 - In the navigation pane on the left, choose **Alarm Management > Event List** to view event details of the cluster. For details, see [9.4 Checking AOM Alarms or 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 [9.3.6 Managing AOM 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 [12.4 Using Prometheus Monitoring to Monitor CCE Cluster Metrics](#). After the instance is created, click its name. On the instance details page, choose **Integration Center** and then connect the CCE cluster.

----End

13.3 Using AOM to Monitor Hosts

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.




Constraints

- 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 check the hosts reported. You can use a predefined time label, such as **Last hour** and **Last 6 hours**, or customize a time range. 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 if needed:



- **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. **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 **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 **Events** tab page, view the event details of the host. For details, see [9.4 Checking AOM Alarms or Events](#).
- On the **Alarms** tab page, view the alarm details of the host. For details, see [9.4 Checking AOM Alarms or Events](#).
- 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. **Disk partitions are supported by CentOS 7.x and EulerOS 2.5.**

----End

13.4 Monitoring Processes Using AOM

13.4.1 Configuring AOM Application Discovery Rules

AOM can discover applications and components 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 or components on the host based on [Built-in Discovery Rules](#) and displays them on the application or component 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 Rule Description

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 13-1](#). 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 13-1 Filtering rules

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

Customizing a Discovery Rule

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Infrastructure Monitoring > Process Monitoring**. Next, click the **Application Discovery** tab.

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**. Enter 4 to 63 characters starting with a lowercase letter and ending with a lowercase letter or digit. Only lowercase letters, digits, and hyphens (-) are allowed.
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. Enter 1 to 255 characters.
For example, AOM can detect the processes whose command parameters contain **ovs-vswitchd unix:** and environment variables contain **SUDO_USER=paas**.
 - 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. Enter 1 to 255 characters.
 - 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. Enter 1 to 255 characters. For example, add the text **app-test** as a component name.

- Application types indicate 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 then collects metric data based on the discovery rule. After about two minutes, you can perform the following operations:

- On the **Application Monitoring** tab page, find the monitored application. For details, see [13.4.2 Using AOM to Monitor Application Processes](#).
- On the **Component Monitoring** tab page, find the monitored component. For details, see [13.4.3 Using AOM to Monitor Component Processes](#).

----End

More Operations

After creating an application discovery rule, perform the operations listed in [Table 13-2](#) if needed.

Table 13-2 Related operations

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

Operation	Description
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. Built-in discovery rules cannot be deleted.
Modifying rules	Click Modify in the Operation column. Built-in discovery rules cannot be modified.


13.4.2 Using AOM to Monitor Application Processes


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. The application list displays the name, running status, and deployment mode of each application. AOM supports drill-down from applications to components, instances, and processes. By viewing the status of each layer, you can implement dimensional monitoring for applications. After application discovery rules are set, AOM automatically discovers applications that meet the rules and monitors related metrics. For details, see [13.4.1 Configuring AOM Application Discovery Rules](#).

Procedure

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Infrastructure Monitoring** > **Process Monitoring**. On the **Application Monitoring** tab page, check the application list.

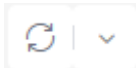
- Set filter criteria in the search box to filter applications.
- Click  in the upper right corner of the page and select or deselect the columns to display.


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

- 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.

- 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. Click a component name to view the instances of the component. Click an instance name to view the monitoring view and alarm information.
 - 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 [9.4 Checking AOM Alarms or Events](#).

----End


13.4.3 Using AOM to Monitor Component Processes


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.

Constraints

- 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 (_).
- Components cannot be filtered by alias.

Procedure


- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane, choose **Infrastructure Monitoring > Process Monitoring**. Next, click the **Component Monitoring** tab. Then you can 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  **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 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 if needed:


- **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**.

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

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

- On the **Instance List** tab page, view the instance details. 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 [9.4 Checking AOM Alarms or Events](#).

- On the **Events** tab page, view the event details of the component. For details, see [9.4 Checking AOM Alarms or Events](#).

----End

14 Global Settings

14.1 Authorizing AOM to Access Other Cloud Services

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.

Prerequisites

You have been granted the **AOM Admin** and **Security Administrator** permissions.

Authorizing AOM to Access Other Cloud Services

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane, choose **Settings > Global Settings**. The **Global Settings** page is displayed.

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 already have the permissions to access the preceding cloud services.
- To cancel authorization, click **Cancel Authorization**.

----End

14.2 Managing Access Codes

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

Constraints

- You can create up to two access codes.
- Deleted access codes cannot be recovered.

Creating an Access Code



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

----End

Other Operations

After an access code is created, you can perform the operations listed in [Table 14-1](#).

Table 14-1 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 to delete an access code. Deleting an access code may affect API calling. Exercise cautions.
Refreshing an access code	Click  to obtain the latest information of the access code.

14.3 Global Configuration of AOM

AOM supports the following global configuration:

- **Metric Collection:** whether to collect metrics (excluding SLA and custom metrics).
- **TMS Tag Display:** whether to display cloud resource tags in alarm notifications.

Constraints

- The global configuration takes effect for the entire AOM 2.0.
- The **TMS tag: `Sevent.annotations.tms_tags`** variable configured in the [alarm message template](#) takes effect only after **TMS Tag Display** is enabled.
- After metric collection is disabled, ICAgents will stop collecting metrics and related metric data will not be updated. However, custom metrics can still be reported.

Configuring Metric Collection

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane on the left, choose **Settings > Global Settings**.

Step 3 On the displayed page, choose **Global Configuration** in the navigation pane. Then enable or disable **Metric Collection** as required.

----End

Configuring TMS Tag Display

Step 1 Log in to the AOM 2.0 console.

Step 2 In the navigation pane on the left, choose **Settings > Global Settings**.

Step 3 In the navigation pane on the left, choose **Global Configuration**. Then enable or disable **TMS Tag Display** as required.

----End

15 Querying AOM Traces

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.

Enabling CTS

Before using CTS, enable it.

After CTS is enabled, if you want to view AOM traces, see "Querying Real-Time Traces" in the *Cloud Trace Service User Guide*.

AOM Operations That Can Be Recorded by CTS

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

Table 15-1 Operations logged by CTS

Function	Operation	Resource Type	Trace
Global Configuration	Adding an access code	icmgr	icmgrAddAccessCode
	Deleting an access code	icmgr	icmgrDelAccessCode

Function	Operation	Resource Type	Trace
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
	Deleting a dashboard group	dashboard_folder	deleteDashboardFolder
	Creating an alarm rule	audit_v4_alarm_rule	addAlarm
	Updating an alarm rule	audit_v4_alarm_rule	updateAlarm
	Deleting an alarm rule	audit_v4_alarm_rule	DeleteThresholdRule
	Creating a process discovery rule	appDiscoveryRule	addAppDiscoveryRule
	Updating a process discovery rule	appDiscoveryRule	updateAppDiscoveryRule
	Deleting a process discovery rule	appDiscoveryRule	delAppDiscoveryRule
	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

Function	Operation	Resource Type	Trace
	Adding a suppression rule	inhibitRule	addInhibitRule
	Modifying a suppression rule	inhibitRule	updateInhibitRule
	Deleting a suppression rule	inhibitRule	delInhibitRule
	Adding a silence rule	muteRule	addMuteRule
	Modifying a silence rule	muteRule	updateMuteRule
	Deleting a silence rule	muteRule	delMuteRule
	Adding an alarm notification rule	actionRule	addActionRule
	Modifying an alarm notification rule	actionRule	updateActionRule
	Deleting an alarm notification rule	actionRule	delActionRule
	Adding a message template	notificationTemplate	addNotificationTemplate
	Modifying a message template	notificationTemplate	updateTemplate
	Deleting a message template	notificationTemplate	delTemplate

16 Migrating Data from AOM 1.0 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.

Function Introduction

- **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.

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.

Precautions:

- Migration cannot be undone.
- 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



17 Accessing AOM 2.0

AOM resources are region-specific and cannot be used across regions. Select a region before accessing AOM.

Constraints

- To return to the AOM 1.0 console, choose **Back to 1.0** in the navigation pane of the AOM 2.0 console. To go to the AOM 2.0 console, choose **AOM 2.0** in the navigation pane of the AOM 1.0 console.

Procedure

- 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**. The AOM console is displayed.
- In the navigation pane, choose **AOM 2.0**. The AOM 2.0 console is displayed.
- Step 4** On the notice dialog box that is displayed, read the billing changes for switching AOM 1.0 to AOM 2.0.
- Step 5** 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 6** Click **Subscribe and Authorize for Free** for AOM 2.0.
- Step 7** In the navigation tree on the left, click a function, for example, **Dashboard**.

----End

18 FAQs

18.1 Dashboard

18.1.1 Can I Import Grafana Views to AOM Dashboards?


Symptom

Can I import Grafana views to AOM dashboards?

Solution

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 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

18.2 Alarm Management

18.2.1 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 some 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.

18.2.2 Why No Alarm Data Is Generated When the Statistical Period Is Set to 1 Minute?

Symptom

When the statistical period is set to 1 minute, no alarm data is generated.

Possible Cause

If the statistical period of a metric alarm rule is set to 1 minute and there is a delay in metric reporting, alarm data may not be generated.

Solution

Set the statistical period and detection rule based on the metric collection interval and delay, and business model.

- Statistical period: When creating a metric alarm rule, first check the metric collection delay (that is, the difference between the latest metric report time and the current time).
 - If they are the same, metric data is reported without delay. In this case, the statistical period can be set to 1 minute or longer.
 - If the time difference is longer than 1 minute but within 5 minutes, the statistical period can be set to 5 minutes or longer.
 - If the time difference is longer than 5 minutes but within 15 minutes, the statistical period can be set to 15 minutes or longer.
 - If the time difference exceeds 15 minutes, contact AOM support.

The latest metric report time can be obtained from the X axis of the metric graph after you select a metric during alarm rule creation. If the metric collection interval is 1 minute, set the statistical period based on the preceding principles. If the metric collection interval is not 1 minute, check the metric collection delay and then determine the statistical period (recommended: metric collection delay + metric collection interval).

- Detection rule: When creating a metric alarm rule, determine the statistics (**Avg**, **Min**, **Max**, **Sum**, and **Samples**), operators (\geq , \leq , $>$, and $<$), and thresholds for all metrics collected within the statistical period, and then set detection rules.

If you have requirements on metric breakpoints or collection delay, enable **Action Taken for Insufficient Data** under **Advanced Settings** of a metric alarm rule and specify the action to be taken when there is no data during a monitoring period.

18.3 Log Analysis

18.3.1 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.

18.3.2 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 view detailed resource statistics of top 100 log groups or streams using the resource statistics function.

-----End

18.4 Prometheus Monitoring

18.4.1 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 [Managing Prometheus Instances](#).

- Step 2** Report native Prometheus metrics to AOM through the remote write address. For details, see [Configuring the Remote Write Address to Report Self-Built Prometheus Data to AOM](#).

----End

18.4.2 How Do I Distinguish Basic Metrics from Custom Metrics Collected by Prometheus Monitoring?

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

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 **Metric Management**. On the **Metrics** tab page, view the metric names and types of the current Prometheus instance.

----End

18.4.3 How Do I Obtain the Service Address of a Prometheus Instance?

You can log in to the AOM console and go to the Prometheus instance details page to obtain the service address of the Prometheus instance.

Procedure:

- Step 1** Log in to the AOM 2.0 console.
- Step 2** In the navigation pane on the left, choose **Prometheus Monitoring > Instances**. In the instance list, click the target 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 18-1 Configuration code for Prometheus remote read

Configuration Code for Prometheus Remote Read

```
remote_read:
  - url: https://aom:
    ts_config:
      insecure_skip_verify: true
    bearer_token: CwYvlg
    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 18-2 Configuration code for Prometheus remote write

Configuration Code for Prometheus Remote Write

```
remote_write:
- url: https://aom-
  ts_config:
    insecure_skip_verify: true
    bearer_token: 'Cv""H9'
```

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 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

18.4.4 Why Can't Metrics Prefixed with `aom_prom_fixed` Be Discarded?

Symptom

Metrics prefixed with `aom_prom_fixed_` cannot be discarded on the **Metric Management** page. In addition, these metrics are billed when being reported to AOM.

Possible Cause

For custom metrics named after Prometheus functions (such as **count**, **max**, **min**, **avg**, **sum**, **count_values**, **stddev**, **stdvar**, **group**, **bottomk**, **topk**, or **quantile**) or operators (such as **and**, **or**, or **unless**), AOM will add the prefix `aom_prom_fixed_` to them when they are being reported to AOM to avoid PromQL query errors. For example, the original name of a custom metric is **count** and will be automatically converted to `aom_prom_fixed_count` when being reported. Due to name inconsistency, this metric fails to be discarded.

Solution

Do not use any Prometheus function (such as **count**, **max**, **min**, **avg**, **sum**, **count_values**, **stddev**, **stdvar**, **group**, **bottomk**, **topk**, or **quantile**) or operator (such as **and**, **or**, or **unless**) as metric names. Name custom metrics in the format of "xxx_xxx_xxx".

18.5 Infrastructure Monitoring

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

Symptom

After a pod is deployed using Helm, AOM cannot find the corresponding workload.

Possible Cause

On the workload page of the CCE console, find the record of the pod deployed using Helm, and compare its YAML file with the YAML file of the pod directly deployed on the CCE console. It is found that the YAML file of the pod deployed using Helm does not contain required environment parameters.

Figure 18-3 Comparing YAML files



Solution 1

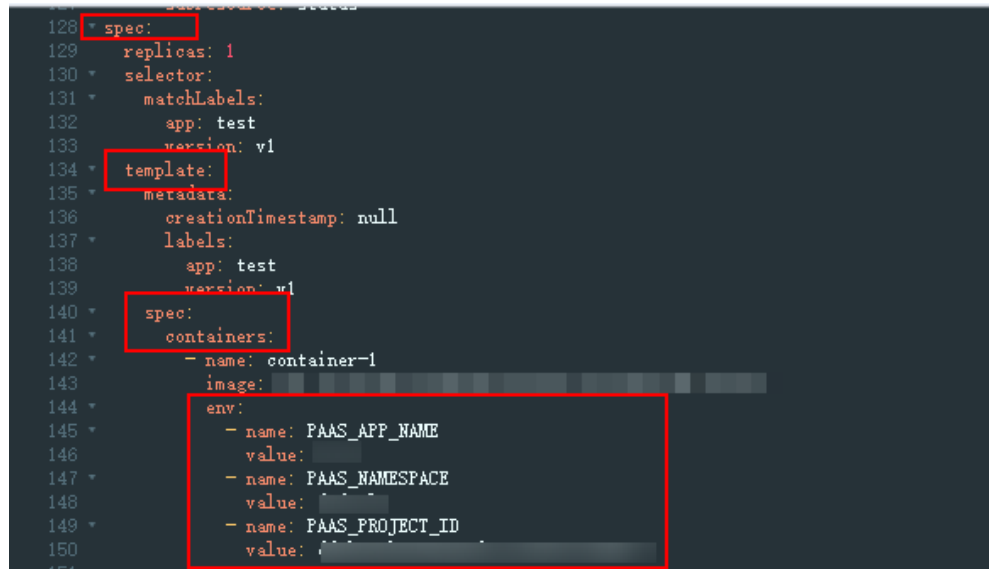
- Step 1** Log in to the CCE console and click a target cluster.
- Step 2** Choose **Workloads** in the navigation pane, and select the workload (pod deployed using Helm) whose metrics have not been reported to AOM.
- Step 3** Choose **More > Edit YAML** in the **Operation** column where the target workload 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 18-4](#).

```
env:
  - name: PAAS_APP_NAME
    value: XXXXXXXXXXXX
  - name: PAAS_NAMESPACE
    value: XXXXXXXXXXXX
  - name: PAAS_PROJECT_ID
    value: 2a*****cf
```

- **PAAS_APP_NAME**: application name, that is, the name of the workload to be deployed.

- **PAAS_NAMESPACE:** namespace of the CCE cluster where the workload to be deployed is located. To obtain the namespace, go to the namespace page on the CCE cluster details page.
- **PAAS_PROJECT_ID:** project ID of the tenant.
Replace the values of the preceding environment parameters based on site requirements.

Figure 18-4 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:
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

Solution 2

Add the following environment parameters to the YAML file for deploying the pod using Helm and then deploy the pod again.

```
env:
- name: PAAS_APP_NAME
  value: XXXXXXXXXXXX
- name: PAAS_NAMESPACE
  value: XXXXXXXXXXXX
- name: PAAS_PROJECT_ID
  value: 2a*****cf
```

- **PAAS_APP_NAME:** application name, that is, the name of the workload to be deployed.
- **PAAS_NAMESPACE:** namespace of the CCE cluster where the workload to be deployed is located. To obtain the namespace, go to the namespace page on the CCE cluster details page.
- **PAAS_PROJECT_ID:** project ID of the tenant.
Replace the values of the preceding environment parameters based on site requirements.

Figure 18-5 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: [redacted]
144       env:
145       - name: PAAS_APP_NAME
146         value: [redacted]
147       - name: PAAS_NAMESPACE
148         value: [redacted]
149       - name: PAAS_PROJECT_ID
150         value: [redacted]
```

18.6 Collection Management

18.6.1 Are ICAgent and UniAgent the Same?

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

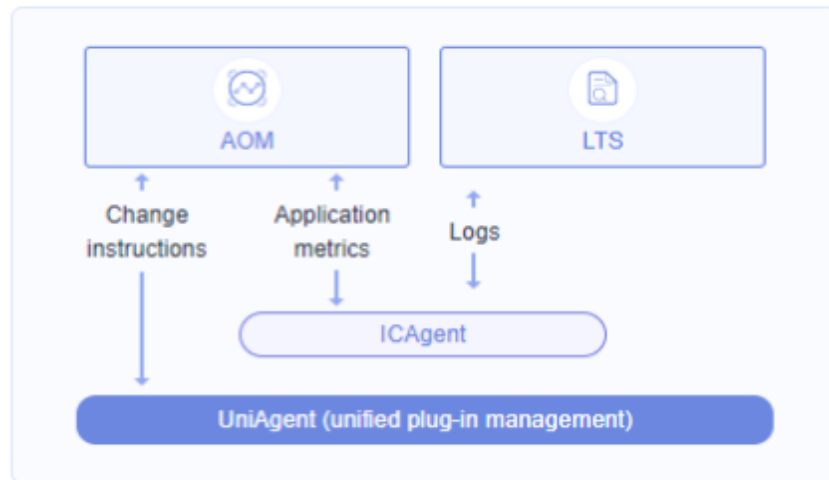
- UniAgent is an Agent for unified data collection and serves as the base of the cloud service O&M system. It delivers instructions, such as script delivery and execution, and integrates plug-ins (such as ICAgent, Cloud Eye, and Telescope) and maintains their status. UniAgent provides middleware and custom metric collection capabilities.

NOTE

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

- ICAgent collects metrics and logs for AOM and LTS.

Figure 18-6 ICAgent and UniAgent



18.6.2 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

18.6.3 Why Is an Installed ICAGENT Displayed as "Abnormal" on the UniAgents Page?

Symptom

An installed ICAGENT is displayed as "Abnormal" on the **UniAgents** page.

Possible Causes

The AK/SK are incorrect, or no agency is set.

Solution

Obtain an AK/SK and install the ICAGENT again. The procedure is as follows:

- 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

18.6.4 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 18-7](#):

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

Figure 18-7 Checking the host IP address

```
root@lts-auto-test-wushan-wudong-99404 home1# 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      0 127.0.0.1:938->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      0 127.0.0.1:901->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 18-8](#):

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

Figure 18-8 Checking the NIC corresponding to the IP address

```
root@lts-auto-test-wushan-wudong-99404 home1# 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 home1#
```

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 18-9](#).

Figure 18-9 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/enus"
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 and choose **Settings > Global Settings > Collection Settings > UniAgents** to 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

18.6.5 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 [3](#).
- If the command output does not contain **failed**, the ICAgent can report metrics. In this case, go to [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 [5](#).

Step 5 Reconfigure the node time on the user side:

```
date -s Time of the current time zone (for example, 12:34:56)
```

-----End

18.6.6 FAQs About UniAgent and ICAgent Installation

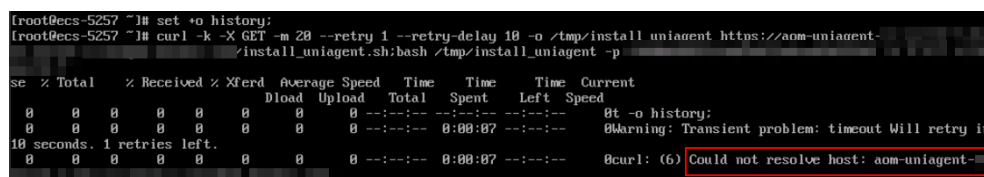
1. What Can I Do If the Network Between the UniAgent Installation Host and Target Host Is Disconnected ("[warn] ssh connect failed, 1.2.1.2:22")?
Check network connectivity before installing an Agent, and select an installation host that is accessible from the Internet.
2. What Can I Do If the Heartbeat Detection and Registration Fail and the Network Is Disconnected After I Install a UniAgent?
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 version is upgraded?
After the cluster version is upgraded, the system will restart the ICAgent and upgrade it to the latest version.

18.6.7 Why Cannot the Installation Script Be Downloaded When I Try to Install UniAgent on a Cloud Server?

Symptom

During UniAgent installation on a cloud server, the installation script cannot be downloaded. Message "Cloud not resolve host: aom-uniagent-xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx" is displayed.

Figure 18-10 Error information



```
root@ecs-5257 ~]# set +o history;
root@ecs-5257 ~]# curl -k -X GET -m 20 --retry 1 --retry-delay 10 -o /tmp/install_uniagent https://aom-uniagent-
/install_uniagent.sh;bash /tmp/install_uniagent -p
se % Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
0 0 0 0 0 0 0 0 --:--:-- --:--:-- --:--:-- 0t -o history:
0 0 0 0 0 0 0 0 --:--:-- 0:00:07 --:--:-- 0Warning: Transient problem: timeout Will retry in
10 seconds. 1 retries left.
0 0 0 0 0 0 0 0 --:--:-- 0:00:07 --:--:-- 0curl: (6) Could not resolve host: aom-uniagent-xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
```

Possible Cause


The host cannot resolve the Object Storage Service (OBS) domain name.


Solution

Add Domain Name Service (DNS) server addresses for the ECS running Linux and then add a security group.


You can add DNS server addresses for the ECS by running commands or through the management console.

- To add DNS server addresses by running commands, perform the following steps:

- a. Log in to the ECS as user **root**.
- b. Run the **vi /etc/resolv.conf** command to open the file.
- c. Add **nameserver xx.xx.xx** to the file.
xx.xx.xx indicates private DNS server addresses.
- d. Enter **:wq** and press **Enter** to save the settings and exit.
- To add DNS server addresses for the ECS through the management console, perform the following steps:
 - a. In the upper left corner of the management console, select a target region and project.
 - b. Click **Service List** in the upper left corner. Under **Compute**, select **Elastic Cloud Server**.
 - c. In the ECS list, click the ECS name to go to the ECS details page.
 - d. In the **Summary** tab page, click the VPC name.
The **Virtual Private Cloud** page is displayed.
 - e. In the VPC list, locate the target VPC and click its name.
 - f. In the **Networking Components** area, click the number following **Subnets**.
The **Subnets** page is displayed.
 - g. In the subnet list, locate the target subnet and click its name.
 - h. In the **Gateway and DNS Information** area, click  following **DNS Server Address**.

 **NOTE**

Set the DNS server address to the value of **nameserver** in [3](#).
 - i. Click **OK**.

 **NOTE**

The new DNS server address takes effect after the ECS is restarted.
- To add a security group through the management console, perform the following steps:
 - a. In the upper left corner of the management console, select a target region and project.
 - b. Click **Service List** in the upper left corner. Under **Compute**, select **Elastic Cloud Server**.
 - c. In the ECS list, click the ECS name to go to the ECS details page.
 - d. On the **Security Groups** tab page, click a security group name. The security group details page is displayed.
 - e. Go to the **Outbound Rules** tab page and then click **Add Rule**.
Add a rule by referring to [Table 18-1](#).

Table 18-1 Parameters for adding a security group rule

Priority	Action	Type	Protocol & Port		Destination	Description
1	Allow	IPv4	TCP	80	100.125.0.0/16	Used to download the UniAgent installation package from the OBS bucket to the ECS and obtain the metadata and authentication information of the ECS.
1	Allow	IPv4	TCP and UDP	53	100.125.0.0/16	Used by DNS to resolve domain names, for example, resolve the OBS domain name when you download the UniAgent installation package, and resolve the UniAgent address.
1	Allow	IPv4	TCP	443	100.125.0.0/16	Used to collect monitoring data and report them to AOM.

18.7 Other FAQs

18.7.1 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 AOM 1.0 billing. 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 log data, and displays monitoring results in a visualized manner. For details, see [Comparison Between AOM 1.0 and AOM 2.0](#).

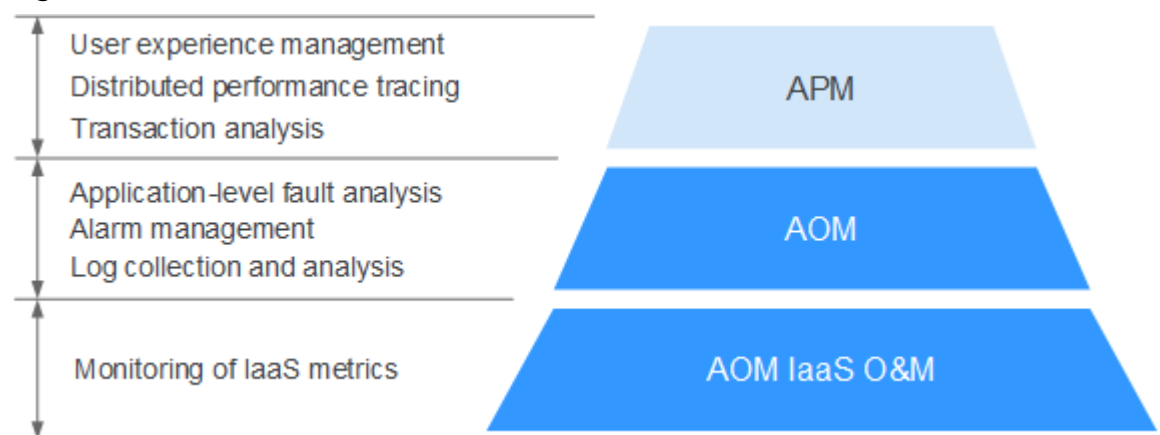
As AOM 1.0 functions are gradually replaced by AOM 2.0, AOM 1.0 will be brought offline soon. You are advised to upgrade AOM 1.0 to AOM 2.0. For details, see [Migrating Data from AOM 1.0 to AOM 2.0](#).

18.7.2 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, optimizing user experience.

AOM provides basic O&M capabilities. APM is a supplement to AOM.

Figure 18-11 Multi-dimensional O&M solution



18.7.3 What Are the Differences Between the Log Functions of AOM and 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 one-stop platform for service observability analysis. It integrates the log functions of Log Tank Service (LTS). Charging data records (CDRs) are reported by LTS instead of AOM. You will not be billed twice. AOM incorporates LTS functions for unified O&M. LTS also has its own independent console and can be used separately.

18.7.4 How Do I Create the apm_admin_trust Agency?

Creating the apm_admin_trust Agency

- 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 18-2](#).

Table 18-2 Parameters for creating an agency

Parameter	Description	Example
Agency Name	Set an agency name. 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 **OK**. In the displayed dialog box, click **Authorize Agency**.

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

Release Date	Description
2025-08-30	<ul style="list-style-type: none">Optimized section 9.2.1 Creating AOM Alarm Message Templates.Added section 9.3.4 Creating an AOM Log Alarm Rule.
2025-06-30	<ul style="list-style-type: none">Added the following sections:<ul style="list-style-type: none">4 AOM Overview6 (New) Connecting to AOM8.3 (New) Creating a Dashboard8.6 (New) Setting Filters for AOM Dashboards10 (New) Log Management11 (Old) Log Management12.8 Ingesting Middleware Metrics to AOM in VM Scenarios12.1 Prometheus Monitoring Overview5.2 Managing Collector Base UniAgentOptimized the following sections:<ul style="list-style-type: none">5 Connecting to AOM8 Dashboard Monitoring9 Alarm Monitoring12 Prometheus Monitoring7 Observability Metric Browsing13 Infrastructure Monitoring
2025-03-31	Added the following section: 18.2.2 Why No Alarm Data Is Generated When the Statistical Period Is Set to 1 Minute?
2024-06-30	This issue is the first release of AOM 2.0.