

Security Level:

# AOM简介

## 日志篇

[www.huawei.com](http://www.huawei.com)

Author/ Email: Author's name/Author's email

Version: V1.0 (20YYMMDD)

**HUAWEI TECHNOLOGIES CO., LTD.**



# AOM日志简介

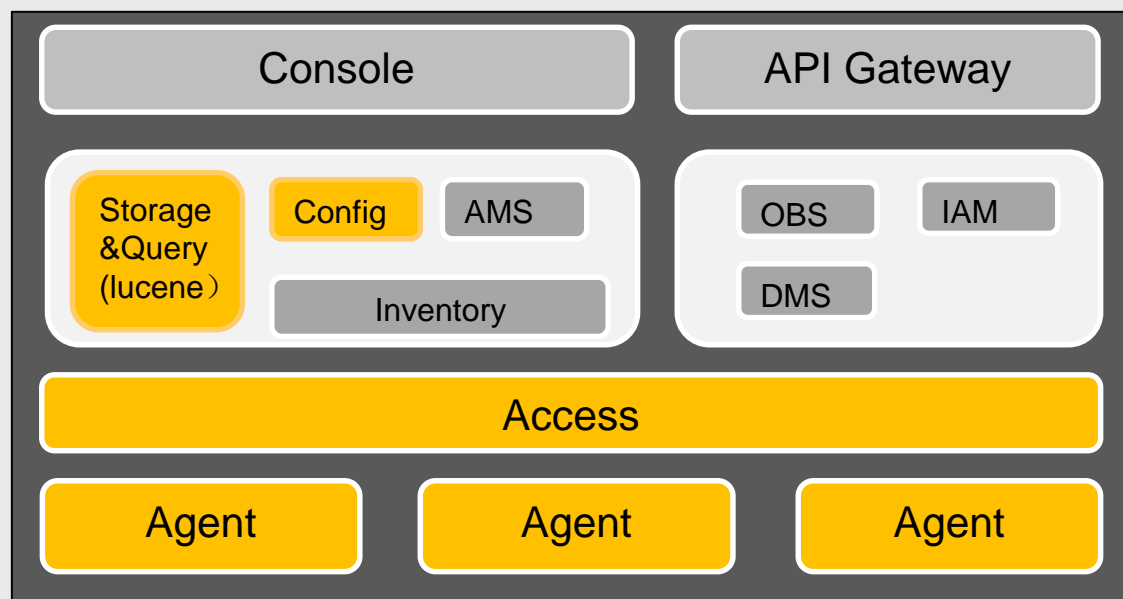
云化&容器化场景下，对于一个日志服务来说，需要解决如下问题：

1. 如何实时从各个主机上收集各种类型日志。 --采集探针
2. 收集日志如何存储。 --存储集群， 成本？
3. 日志查询&分析。 --分析计算集群， 成本？
4. 报表 --报表服务， 成本？

日志（Application Log Service，简称ALS）是针对运行在华为公有云上的应用，提供的实时日志存储&分析服务。提供的服务内容包括：日志数据收集，海量日志检索，日志存储和转储，日志订阅，关键词统计报表等。低成本，高效运维客户日志。

# AOM日志简介

ALS架构图: 存储和查询的实现基于开源lucene, <http://lucene.apache.org/>。



## 微服务简介

**Access:** 数据收集代理, 接受ICAgent上报数据

**Config:** 日志配置管理, 包括日志文件模型, 以及用户相关配置等, 并对接外部所有查询请求。

**Storage&Query:** 日志存储, 并提供内部查询接口。

## 流程简介

上报过程: ICAgent采集日志->Access(Proxy)->DMS

存储过程: Storage从DMS消费数据存储->写入配置到Config

查询过程: Console(API-G)->Config->Storage

# 功能简介

## 日志数据收集

AOM服务中ICAgent默认提供日志采集能力，包括使用CCE（云容器引擎）部署容器日志以及主机上的系统日志等。另外，日志服务提供自定义日志路径采集的能力，日志路径包括主机上指定目录和指定服务日志路径

## 日志实时查看

简单的tail功能

## 海量日志检索

支持通过过滤条件+关键字的方式对租户下日志的全文检索，过滤条件包括集群，服务，主机，时间范围等。

## 日志存储和转储

用户日志收集上来后，默认集中存储到日志服务中，7天+2G永久免费，更多计费详情参考[https://www.huaweicloud.com/price\\_detail.html#/aom\\_detail](https://www.huaweicloud.com/price_detail.html#/aom_detail)。同时，日志服务支持将重要日志转储到OBS（对象存储服务）中，用户可以定义日志桶和转储策略，日志服务以桶为单位，将日志转储至OBS。

## 日志订阅&投递

用户可以把日志服务作为一个收集日志的通道，从DMS（分布式消息服务）中直接获取日志，从而处理自己的业务日志

## 关键词统计&报表

关键词统计是针对日志对象，统计一段时间内特定关键词出现的频率，我们称之为“统计规则”，每一个统计规则的作用单用是前文提到的日志桶。每一条规则统计的结果将会作为一个指标被投递到AMS（应用监控服务）中，用户可以在AMS对这个指标进行监控和管理，如生成报表或者设置告警规则。

操作视频：

[https://support.huaweicloud.com/aom\\_video/index.html](https://support.huaweicloud.com/aom_video/index.html)

# 日志数据收集

前提：安装好采集探针ICAgent

采集配置：

1. CCE集群下容器日志收集，我们采用的采集方案是通过挂载volume的方式将容器内的日志落地到宿主机，宿主机上通过日志采集ICAgent采集，标准输入stdout和stderr未重定向的日志默认采集，不需要配置。配置方式参考如下：

生命周期

健康检查

环境变量

数据存储

安全设置

容器日志

容器日志用于配置工作负载日志策略，便于日志收集分析，以及按周期防爆处理

类型	主机路径	挂载路径
HostPath	/var/paas/sys/log/shoppingmalldb	/var/log/apm

添加日志策略

主机实际路径

容器内日志目录

2. 主机日志数据收集，通过用户配置采集路径规则，采集目标主机上的日志文件。配置方式参考：

日志管理

日志文件

日志搜索

路径配置

<input type="checkbox"/>	虚拟机名称	私有IP	虚拟机状态	日志采集路径	操作
<input type="checkbox"/>	ecs-92a3	192.168.0.10	正常	/var/log/ntp.log	配置

主机上日志目录或者文件

# 日志实时查看

日志实时查看，类比Linux上的tail功能， 通过此功能，可以实时查看最新的日志内容。

使用方式：  
选择指定日志文件，点击“开启实时查看”，开始实时查看相关日志。  
点击“关闭实时查看”，或者离开当前页面后，停止实时查看功能。

使用限制：暂时不支持tail + grep功能，开启实时查看后，不支持关键词过滤。

日志文件 > 查看

oss.icAgent.trace

最新写入时间：2018/11/03 17:31:18 GMT+08:00 所在进程: asfaaaaaadf

请输入要搜索的日志内容，支持精确搜索及模糊搜索等

2018/11/03

											17:30 - 17:35	
16:35	16:40	16:45	16:50	16:55	17:00	17:05	17:10	17:15	17:20	17:25	17:30	17:35

2018/11/03 17:32:36

全屏

关闭实时查看

2018-11-03 17:32:59.550 (10471)[W] node\_collect.go:189 addNTPCountAlarm k:NTPAbnormalAlarm, v:26679, threshold:10

2018-11-03 17:32:59.573 (10471)[W] sender.go:359 httpsend send success,dataType:MONITOR,plugin:node,len:1227

2018-11-03 17:32:59.573 (10471)[W] sender.go:359 httpsend send success,dataType:MONITOR,plugin:fs,len:4188

2018-11-03 17:32:59.651 (10471)[W] selfstatus.go:59 icagent resource:CpuUsage[16.667],HandleCount[34],MemUsed[46],ThreadsCount[31],VirMemCapacity[621],memLimit[0]

2018-11-03 17:32:59.651 (10471)[W] podlist.go:15 not paas mode nor master mode, donot get podlist

2018-11-03 17:32:59.651 (10471)[W] podlist.go:15 not paas mode nor master mode, donot get podlist

2018-11-03 17:32:59.655 (10471)[W] agent\_status.go:69 Set Agent metrics:&agent\_status.AgentMetric{Pid:10471, CpuUsage:16.667, HandleCount:34, MemUsed:46, ThreadsCount:31, AppLogTaskCount:0, PodCount:0, ExporterCount:0, SvriessLogTaskCount:0, TraceNamedTaskCount:0, KpiNamedTaskCount:0, StdLogTaskCount:0, NodeCpuCore:1, NodeMemCapacity:991}

2018-11-03 17:32:59.666 (10471)[W] selfcheck.go:61 icagent resource:CpuUsage[8.333],HandleCount[34],MemUsed[46],ThreadsCount[31],VirMemCapacity[621],memLimit[495]

2018-11-03 17:32:59.729 (10471)[W] sender.go:359 httpsend send success,dataType:MONITOR,plugin:inscollect,len:5781

2018-11-03 17:33:07.186 (10471)[E] util.go:19 stat file[/opt/output/paas-apm/88540/vmall/vmall-user-service/log/pinpoint.log] err[stat /opt/output/paas-apm/88540/vmall/vmall-user-service/log/pinpoint.log: no such file or directory]

2018-11-03 17:33:07.186 (10471)[E] util.go:19 stat file[/opt/output/paas-apm/88538/vmall/vmall-dao-service/log/pinpoint.log /opt/output/paas-apm/88539/vmall/vmall-apigw-service/log/pinpoint.log /opt/output/paas-apm/88540/vmall/vmall-user-service/log/pinpoint.log /opt/output/paas-apm/88541/vmall/vmall-product-service/log/pinpoint.log /opt/output/paas-apm/88542/vmall/vmall-ui-service/log/pinpoint.log] err[stat /opt/output/paas-apm/88538/vmall/vmall-dao-service/log/pinpoint.log /opt/output/paas-apm/88539/vmall/vmall-apigw-service/log/pinpoint.log /opt/output/paas-apm/88540/vmall/vmall-user-service/log/pinpoint.log /opt/output/paas-apm/88541/vmall/vmall-product-service/log/pinpoint.log /opt/output/paas-apm/88542/vmall/vmall-ui-service/log/pinpoint.log: no such file or directory]

# 海量日志检索--日志文件查看

很多时候，我们需要从日志中找出一些异常或者ERROR的关键信息， 可以借助日志检索功能实现这样的诉求。

日志检索分为两大块内容：

日志文件：

日志文件实际上是一个“文件树”的视图， 通过“文件树”，能够快速的查找各个服务对应的日志文件的基本信息，包括文件名称、路径、写入时间等。

使用方式：

支持“集群”、“命名空间”、“服务名称”等过滤信息快速查找相关日志文件

日志管理

• 日志文件

• 日志搜索

• 路径配置

、

服务自定义

集群：

bcs-demo

命名空间：

default

隐藏系统服务

华为云系统服务，如：ICAgent等

请输入服务名称

peer-499f9c89388bad96e4...  
orderer-f772d25e2af402b...

当前日志

文件名称	实例名称	最新写入时间	操作
check.log	peer-499f9c89388bad96a322b552b929...	2018/11/03 15:49:43 GMT+08:00	<a href="#">查看</a>

# 海量日志检索--日志搜索

如果我们需要从日志中找出一些异常或者ERROR的关键信息， 可以借助日志检索功能实现这样的诉求。

日志搜索：

简单而且好用的一个功能，快速对选定范围内的日志内容进行关键词检索，并且提供模糊和简单的管理搜索能力，如“？”，“\*”等模糊，“|”(或)， “&&”(与)等这样的关联查询

使用方式：

关键字+过滤条件+时间范围

关键字支持的搜索条件参考下面截图“提示”

过滤条件（包括高级搜索）能够有效地提高搜索结果命中率和搜索效率。

同时支持搜索结果的导出功能，将搜索结果导出为csv结构

The screenshot shows a log search interface. At the top right, there are time range filters: "最近5分钟", "最近30分钟" (selected), "最近1小时", and "自定义时间段". Below these are tabs for "服务", "系统", and "自定义". The "自定义" tab is active, and a callout box points to it with the text "自定义路径获取的日志". On the left, there is a "refresh" button and a "导出" (Export) button. A search bar contains "bcs-demo" and a "命名空间" (Namespace) dropdown. A "高级搜索" (Advanced Search) button is on the right. A "提示" (Tips) popup is displayed in the center, listing four search rules. The main log table has columns for "时间" (Time) and "描述" (Description). The first row shows a log entry: "2018/11/03 15:55:42.965 GMT+08:00" and "refresh is not true.". A "查看上下文" (View Context) link is at the bottom right.

系统日志

自定义路径获取的日志

最近5分钟 最近30分钟 最近1小时 自定义时间段

refresh

服务 系统 自定义

导出 bcs-demo 命名空间

提示

1. 支持关键词精确搜索。关键词指相邻两分词符之间的单词。
2. 支持关键词模糊匹配搜索，例如输入“ER?OR”或“ROR”或“ER”R”。
3. 支持短语精确搜索。例如输入“Start to refresh”或“Start-to-refresh”(-为分词符)。
4. 支持与、“或”组合搜索。格式为“query logs&&erro\*”或“query logs||error”。

正序 高级搜索

时间	描述	操作
2018/11/03 15:55:42.965 GMT+08:00	refresh is not true.	<a href="#">查看上下文</a>



# 海量日志检索一分词

日志服务默认提供安装“空格”进行分词。在此基础上，用户如果需要通过其他字符进行分词的能力，可以在日志界面上添加。

请输入要搜索的日志内容，支持精确搜索及模糊搜索等

搜索

- 统计规则 new
- 日志订阅
- 分词配置 new

分词配置入口有两个：

1. 日志搜索界面，如右图，这里设置的规则，只在当前会话生效，参考“提示”

2. 也可以在分词配置界面配置分词规则，这里配置的分词规则将一直生效，如左图

默认字符集：, "; = @ & < > /

## 设置查询分词符

温馨提示：设置的查询分词符生效周期为本次会话（刷新界面、退出登录会重置到默认分词符）

自定义分词符：, "; = @ & < > /

特殊分词符：

ASCII值	控制字符	解释	操作
12	FF	换页键	删除

添加特殊分词符

确认

取消

其他特殊分词：熟悉ASCII码的同学可以直接设置

自定义分词符：, "; = @ & < > /

特殊分词符：

ASCII值	控制字符	解释	操作
12	FF	换页键	删除

添加特殊分词符

字段预览：

预览

清空

test@huawei.com

test huawei.com

确认

重置

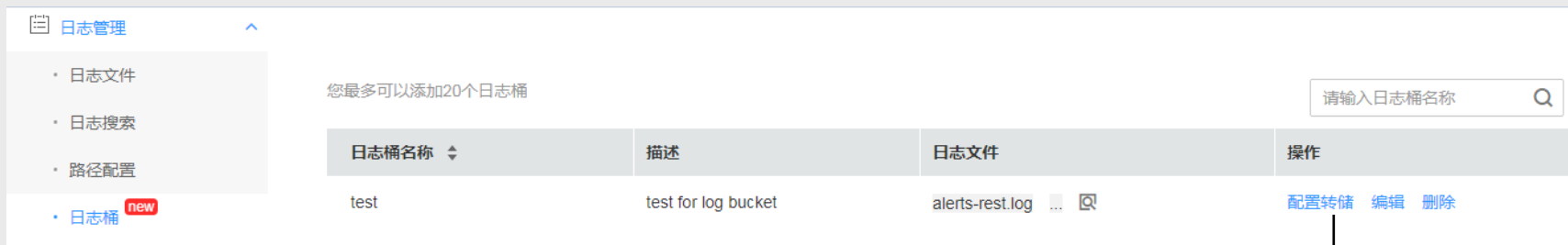
对设置的分词结果预览

# 日志存储和转储

1. 日志存储，日志服务将收集上来的日志集中存储在日志服务集群中。日志存储时长不超过7天且占用空间不超过2GB，永久免费，更高规格的参考计费说明：[https://support.huaweicloud.com/price-aom/aom\\_01\\_0002.html](https://support.huaweicloud.com/price-aom/aom_01_0002.html)

## 2. 日志转储

1) 日志桶，日志桶是日志分析的基本单元。日志转储并不是日志服务默认行为，需要用户创建完日志桶后，选择关联日志，并对根据转储策略对指定日志以日志桶为单元进行转储

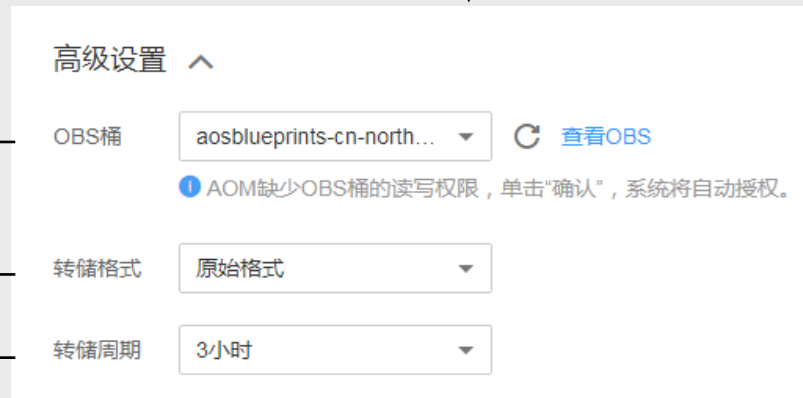


2) 日志转储，日志转储并不是日志服务默认行为，需要用户创建完日志桶后，选择关联日志，并对根据转储策略对指定日志以日志桶为单元进行转储

日志转储的前提是在OBS中创建了OBS桶，并完成用户授权。

日志转储的格式目前支持原始日志格式。

日志转储周期定义：3h,6h,12h,



# 日志下载

也行用户也会有一些下载诉求，也可以从日志界面中直接把日志生成原始日志文件，下载到本地进行处理。

日志下载：

请输入要搜索的日志内容，支持精确搜索及模糊搜索等

搜索

服务系统自定义

导出

vanke-demo

命名空间

服务

高级搜索

倒序

正序

	时间	描述	操作
▼	2018/11/21 14:28:20.180 GMT+08:00	W1121 14:28:14.626605 14120 eviction_manager.go:479] eviction manager: failed to retrieve config map multi-gpu-scheduling-config, error: configmaps "multi-gpu-scheduling-config" not found.	<a href="#">查看上下文</a>

kubelet.log

来源

/var/paas/sys/log/kub...

类型

服务

服务名称

sssssss

实例名称

sssssss

集群名称

vanke-demo

命名空间

default

主机IP

192.168.1.204

时间

2018/11/21 14:28:20.180 GMT+08:00

上下文显示行数

200

导出本页

# 日志订阅（投递）

也行用户也会有一些其他诉求，需要对日志进行二次处理。那么日志订阅这个能力，应该能满足诉求。

用户可以把日志服务作为一个收集日志的通道，从DMS（分布式消息服务）中直接获取日志，从而处理自己的业务日志

- 1) 需要提前创建好DMS队列
- 2) 需要队列对日志服务进行授权
- 3) 用户可以只订阅日志，不使用日志的存储和分析功能，参考如下提示

## 日志订阅

通过对接分布式消息队列可订阅您的服务日志。


启用订阅功能：☒

队列类型：Kafka

队列名称：

queue-228692872

[创建Kafka队列](#)

 该队列缺少“ProduceMessages”授权动作，单击“确认”后，系统会自动授权。

☒ 取消日志分析功能 勾选后日志数据将不会写入日志文件，在“日志搜索”界面将查询不到日志数据。

确认

取消

# 关键词统计&报表

关键词统计是针对日志对象，统计一段时间内特定关键词出现的频率，我们称之为“统计规则”，每一个统计规则的作用单用是前文提到的日志桶。每一条规则统计的结果将会作为一个指标被投递到AMS（应用监控服务）中，用户可以在AMS对这个指标进行监控和管理，如生成报表或者设置告警规则。

1.关键词统计规则，关键词默认精准匹配(分词符为空格)，支持使用\*或?进行模糊匹配（\*代表多个字符，?代表1个字符），也支持短语匹配（例如Hello World）

• 路径配置

• 日志桶 new

• 日志转储 new

• 统计规则 new

删除

全部规则类型

请输入规则名称/日志桶名称/关键词/描述

<input type="checkbox"/> 规则名称	日志桶	规则类型	关键词	文件列表	描述	操作
<input type="checkbox"/> test1234	test_bucket	关键词统计	*PKxyLbVL*			<a href="#">编辑</a> <a href="#">删除</a>
<input type="checkbox"/> test11	log-bucket1	关键词统计	break		ert	<a href="#">编辑</a> <a href="#">删除</a>

2.报表&告警设置，下图是“test11”规则产生的指标，可以针对该指标进行添加到视图生成报表，也可以对其设置阈值，监控其产生的频率

应用运维管理

总览 new

告警中心

视图管理

仪表盘

指标监控

主机监控

请输入服务或主机名称(别名)

选择指标

您最多可以选择12个指标

自定义集群

SLA

自定义指标

ALSAAlarm

logSizeCount

myrule

test11

clusterId=c693fa7c-54cd-11e...

近1小时

统计周期：1分钟

插值方式：null

16:01 16:03 16:05 16:07 16:09 16:11 16:13 16:15 16:17 16:19 17:01

aomdemo | test11

时区 ( GMT+08:00 )