

# 产品简介

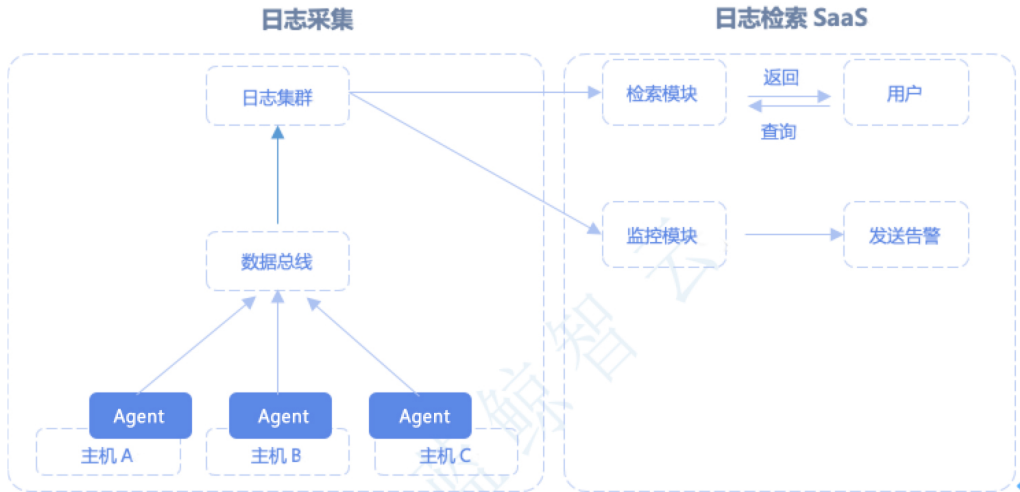
蓝鲸日志检索是为了解决运维场景中“日志查询与处理”的问题而推出的一款 SaaS，基于蓝鲸体系中三大平台的核心性能（蓝鲸管控平台的采集和上报日志信息，蓝鲸配置平台的“模块”化拓扑管理采集器，蓝鲸数据平台的大数据存储服务），从而实现从业务主机到日志数据的高效查询与处理。它通过关键字匹配的简单查询功能和语法组合的复杂查询能力，让用户无需登录主机即可完成对日志数据的检索和分析工作，同时还提供了日志实时滚动和上下文检索的能力；为了进一步增强产品特性，推出了“关键字监控”的功能是提升研发和运维效率的利器。



# 术语解释

- 采集项： 针对配置平台某个模块进行日志采集配置的对象，可针对一个模块采集多个路径的日志。

# 产品架构图



## 采集项管理

“

以“模块”为单位管理采集项，且支持在同一个模块上同时采集多个文件。

”

采集项管理

新建采集项

☐ 全部展开

请输入模块/IP/路径 按回车键搜索

模块/IP	采集路径	下发时间	采集状态	操作
暂无数据				

## 用户操作审计

“

用户的每一次操作，都会以历史记录在系统中，方便审计。

”

历史记录				
发布时间	发布人员	发布内容	状态	操作
2017-03-22 20:03:30	admin	新增配置	发布失败	执行详情 配置详情
2017-03-22 12:22:14	admin	新增配置	发布失败	执行详情 配置详情
2017-03-22 12:21:56	admin	新增配置	发布失败	执行详情 配置详情
2017-03-22 12:21:49	admin	删除采集项	发布失败	执行详情 配置详情
2017-03-22 12:21:44	admin	删除采集项	发布失败	执行详情 配置详情
2017-03-22 11:13:31	admin	删除采集项	发布失败	执行详情 配置详情
2017-03-22 11:05:28	admin	新增配置	发布失败	执行详情 配置详情
2017-03-20 15:41:58	admin	新增配置	发布失败	执行详情 配置详情
2017-03-20 10:49:12	admin	新增配置	发布失败	执行详情 配置详情
2017-03-16 17:16:11	admin	新增配置	发布失败	执行详情 配置详情

# 关联蓝鲸配置平台

“

本应用还会关联蓝鲸的配置平台，通过模块会在后台直接转换成 ip 下发。

”

## 新建采集项

业务：验收测试

### 基础信息

模块 \*

请选择

### 采集项配置信息

过期时间 \*

天

日志路径 \*

日志路径可以用简单的通配符，如/data/\*.log，类似linux中的ls \*.log匹配，多个地址以换行隔开

排除类型

请输入排除文件类型，如txt、tar,多个文件类型请用换行分隔

下发配置

# 多关键字关联查询

“

通过多个关键字组合查询，更精确的获取查询结果

”

serverip:192.168.1.16 && log:from

搜索一下

语法规则

找到 223 条结果 (用时 0.01 秒)

日志检索结果						<input type="checkbox"/> 全部展开	显示项	IP地址,时间,模块,日志内容	下载
IP地址	时间	模块	日志路径	操作	日志内容				
192.168.1.16	2017-11-20 19:52:00	接收->linux	/cai/cai.log		64 bytes from 127.0.0.1: icmp_seq=1000 ttl=64 time=0.039 ms				
192.168.1.16	2017-11-20 19:52:00	接收->linux	/cai/cai.log		64 bytes from 127.0.0.1: icmp_seq=999 ttl=64 time=0.042 ms				
192.168.1.16	2017-11-20 19:52:00	接收->linux	/cai/cai.log		64 bytes from 127.0.0.1: icmp_seq=998 ttl=64 time=0.040 ms				
192.168.1.16	2017-11-20 19:52:00	接收->linux	/cai/cai.log		64 bytes from 127.0.0.1: icmp_seq=997 ttl=64 time=0.040 ms				
192.168.1.16	2017-11-20 19:52:00	接收->linux	/cai/cai.log		64 bytes from 127.0.0.1: icmp_seq=996 ttl=64 time=0.031 ms				
192.168.1.16	2017-11-20 19:52:00	接收->linux	/cai/cai.log		64 bytes from 127.0.0.1: icmp_seq=995 ttl=64 time=0.029 ms				
192.168.1.16	2017-11-20 19:52:00	接收->linux	/cai/cai.log		64 bytes from 127.0.0.1: icmp_seq=994 ttl=64 time=0.041 ms				

## 关键字监控

“

通过配置对应模块需要监控的关键字，可以达到监控系统运行状态的目的。

”

关键字监控管理

新建监控项

关键字/模块/IP/路径

查询

状态	关键字	模块	IP	路径	操作
	20	作业平台->job			
	23	空闲机池->空闲机			
	1	空闲机池->空闲机			
	2	作业平台->job			
	ere	空闲机池->空闲机			
	20	空闲机池->空闲机			
	30	空闲机池->空闲机			
	12	空闲机池->空闲机			
	22222	配置平台->cmdb			

## 新建采集项

1)入口：采集器管理->新建采集器

2)采集器的 IP 地址可以以模块来添加，或者手动输入IP地址

3)日志路径可以用简单的通配符，如/data/.log，类似 linux 中的 ls .log 匹配

4)当通配符中有一些日志不需要采集的，可以通过排除文件来实现

## 新建采集项

业务：验收测试

### 基础信息

模块 \*

请选择

### 采集项配置信息

过期时间 \*

天

日志路径 \*

日志路径可以用简单的通配符，如/data/\*.log，类似linux中的ls \*.log匹配，多个地址以换行隔开

排除类型

请输入排除文件类型，如txt、tar,多个文件类型请用换行分隔

下发配置

## 日志检索搜索页

1)搜索历史显示一天内最近搜索的、次数最多的关键字

2)搜索的关键字可以用 \* 号通配符



## 结果展示

1)日志是按行匹配的，匹配到的关键字会高亮

2)可以自定义显示的列，日志内容是必显示项



## 场景案例

### 1. 可视化的采集项管理

采集项是用户采集日志的最小单元，用来管理从哪些主机哪些路径上采集日志，并且可以方便的在页面上进行变更，达到快速管理的目的。

### 1. 秒级查询

普通基于主机的检索，查询速度慢，返回时间长。蓝鲸智云日志检索基于强大的全文检索引擎并配合上统一查询模块，使查询结果可以达到秒级返回。

### 1. 灵活的查询语法

蓝鲸智云日志检索提供灵活的查询语法，可以指定模块、主机、路径等信息，还可以提供与、或、非等逻辑表达方法，满足复杂的查询场景。

### 1. 页面日志滚动

无需登录主机即可实现运维常见的tailf操作，主机上任何日志的变动，都可以快速在系统中得以体现。

## 常见问题

### 1. Q: 下发采集项失败

A: 请检查失败的IP地址是否能在作业平台正常执行脚本和下发文件。

### 1. Q: 下发采集项成功但是查不到数据

A: 请检查日志是否在持续上报，采集项下发成功以后，只会采集新产生的数据，不会采集老日志。

### 1. Q: 如何查看索引及数据量

A: 在中控机上 `source /data/install/utils.fc && curl`  
`${ES_IP}:${ES_REST_PORT}/_cat/indices | sort | less -N`