



云日志 V2.0.0 使用手册

2017 年 9 月

Copyright © 2017 杭州玳数科技有限公司

前言

一、版权声明：

本文中出现的任何文字叙述，文档格式、插图、图片、方法、过程等内容，除另有特别注明，版权均归杭州玳数科技有限公司所有，并保留一切权利。未经书面许可，任何公司和个人不得将此文档中的内容翻录、转载或以其他方式散发给第三方。否则，必将追究其法律责任。

二、关于我们：

杭州玳数科技有限公司旗下品牌袋鼠云，由多名前阿里云资深技术专家创立，核心员工来自阿里巴巴、神州数码等，作为阿里云重要的合作伙伴，专注于为企业客户提供云计算和大数据智能服务及产品。袋鼠云是阿里云数加平台首个金牌合作伙伴、Aliware 金牌合作伙伴、云盾金牌合作伙伴，也是阿里云认证的区域服务商和云市场供应商。

袋鼠云总部位于杭州，在北京、上海、贵州设有分公司（办事处）。

三、联系我们：

1、公司官网

<https://www.dtstack.com/>

2、公司地址

杭州总部：杭州市西湖区紫霞街 176 号互联网创新创业园 2 号楼 8F

北京分部：北京市朝阳区时间国际 5 号楼 903

3、支持与帮助

如需获取更详尽的玳数科技专业服务信息、商务信息，可通过如下方式与我们联系：

服务热线：18106578848

邮箱支持：support@dtstack.com

一、	产品简介	5
二、	产品特点	5
三、	基本概念	5
四、	用户指南	6
1	日志上传	6
1.1	AGENT 接入	6
1.2	数据接入	7
2	搜索	11
2.1	多标签页视图	12
2.2	查询范围选择、过滤	12
2.3	日志文件选择	13
2.4	搜索框	13
2.5	时间范围选择	13
2.6	事件直方图	13
2.7	事件视图	13
3	搜索语法	14
3.1	全文检索	14
3.2	短语查询	14
3.3	字段值	14
3.4	逻辑运算符	15
3.5	数值范围	16
3.6	通配符	16
3.7	特殊字符的检索处理	17
3.8	区分大小写	18
3.9	时间方案	18
3.10	搜索技巧	18
4	解析规则	19
4.1	自定义解析规则	19
4.2	解析规则配置说明	21
5	应用	24

5.1	应用/仪表盘创建	24
5.2	应用 / 仪表盘管理	26
6	告警	26
6.1	设置告警接收人/分组	26
6.2	告警规则配置	27
6.3	告警历史查询	31
7	数据脱敏	31
7.1	脱敏规则创建	32
7.2	脱敏概况	33
8	数据源管理	33
9	容量管理	33
10	权限管理	34
10.1	功能权限	34
10.2	组织架构	34
10.3	数据权限	35
10.4	用户管理	35
11	用户中心	36
11.1	账户体系	36
11.2	用户权限分配	37
11.3	进入账户中心	37
11.4	产品中心	38
11.5	租户内成员管理	38
11.6	查看成员	38
11.7	添加成员	38
11.8	赋予成员租户角色	39
11.9	赋予成员产品角色	39
11.10	移除成员	39
11.11	重置成员密码	39
11.12	修改租户信息	40
11.13	个人信息管理	40

一、 产品简介

云日志是基于 Elasticsearch 构建的一款高性能可扩展的日志集中、搜索和分析产品，致力于降低企业客户直接使用 ELK 开源产品的部署和使用成本，并且根据客户日志内容及需求抽象出更多的使用场景，帮助企业进行业务实时监控、异常原因定位、安全合规审计、日志及业务数据统计分析，以降低企业运维成本、帮助企业优化运营决策。

二、 产品特色

日志集中，多设备日志实时采集，统一保存，集中管理；

应用场景，对实时采集的日志进行提取、计算，实现业务流程端对端可视化；

实时追踪，实时调试多设备应用日志，高效运维；

稳定安全，提供高可靠的日志收集机制和安全的数据传输；

数据迁移，结构化日志数据实时同步到大数据平台，进一步进行 BI 分析及数据挖掘。

权限控制，用户、数据源进行分离，精细粒度访问权限控制；

三、 基本概念

- **日志解析：**云日志系统可将采集到的非结构化数据（日志数据）结构化，便于用户对日志进行统计、分析；
- **数据脱敏：**云日志系统支持屏蔽用户日志内包含的身份证号、手机号、银行卡号等隐私数据，以响应“网络安全法”保障用户隐私安全；
- **仪表盘：**云日志系统支持利用 SQL & Groovy 对数据进行聚合、计算，将结果转化为报表，组成仪表盘，以辅助运维、运营决策；
- **应用：**用户可将由不同数据建立的仪表盘指定为不同的应用，以便于资源管理、权限控制；

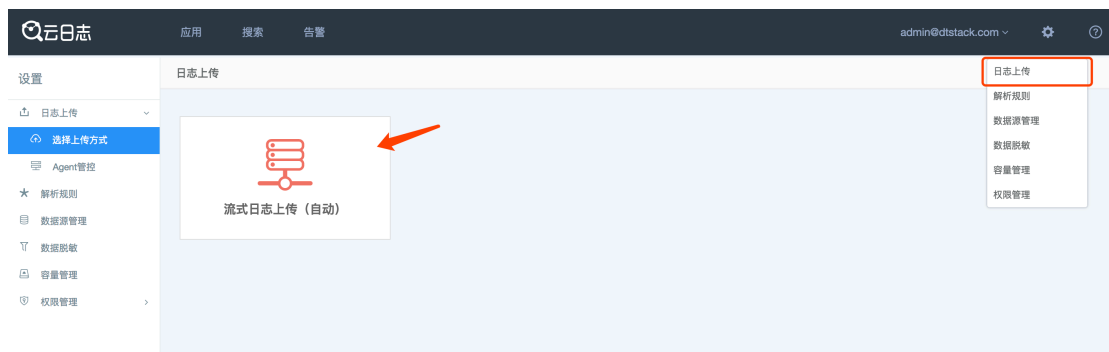
四、 用户指南

1 日志上传

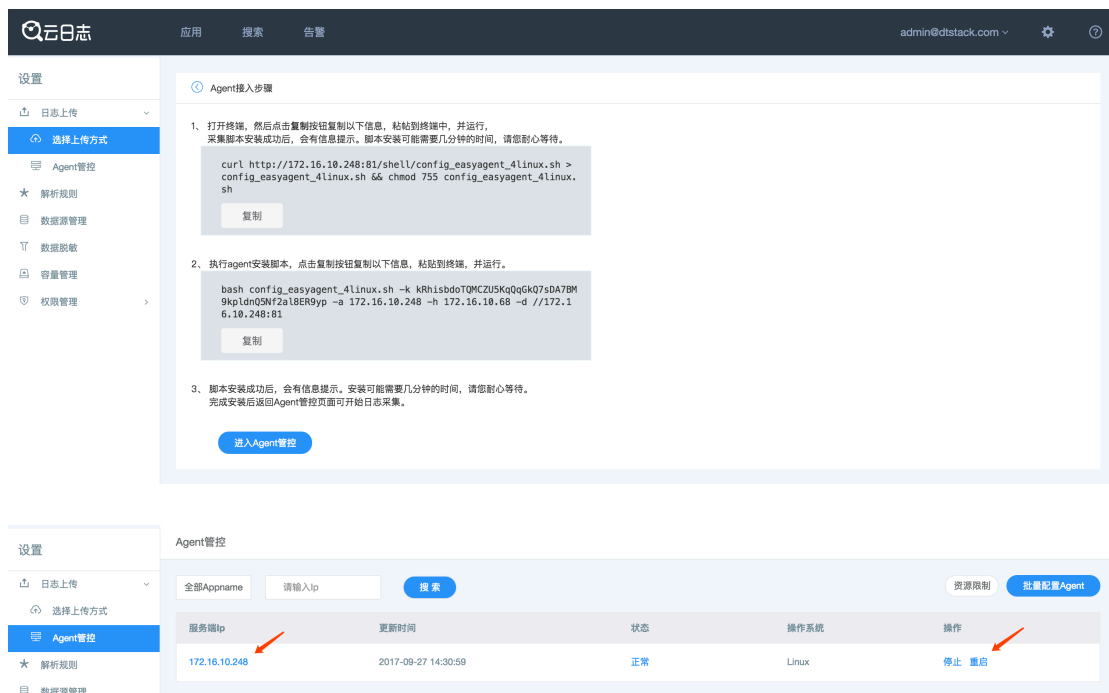
登录云日志平台后首先需要进行数据接入，云日志推荐的上传方式为“流式上传”，通过配置 Agent 实时采集数据；

1.1 Agent 接入

- a) 单击顶部导航设置按钮进入“日志上传——选择上传方式”模块，云日志推荐流式上传方式，单击进入获取 Agent 管控安装、执行脚本，准备 Agent 接入；



- b) 按照下图步骤将脚本在指定服务器上运行，进行 Agent 接入，执行完毕后进入“Agent 管控”界面，可查看到对应的机器已被接入并进行管控；

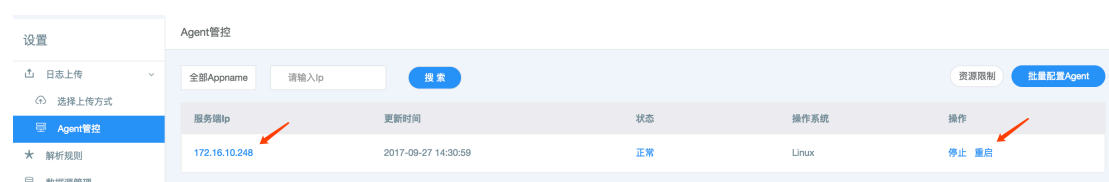


c) 脚本安装成功后，服务上会打印如下提示信息：

```
[root@iZbp19pivcm1fllkmg1jcwZ easyagentar_th_one]# ./easyagent_4linux.sh -k user_token_dtstack
The network is reachable to recv.log.dtstack.com
The Operating system is CentOS !
...The filebeat install... [Success]
...The easyagent install... [Success]
Add to rc local service success!
Finished install easyagent service.
Starting easyagent [ OK ]
start easyagent success!
[root@iZbp19pivcm1fllkmg1jcwZ easyagentar_th_one]# [ ]
start easyagent success!
[root@iZbp19pivcm1fllkmg1jcwZ easyagentar_th_one]# [ ]
```

1.2 数据接入

a) Agent 接入操作执行完毕后，单击侧边栏 Agent 管控进入，可查看当前接入的机器信息（IP、最后心跳上报时间、运行状态、操作系统），如下图点击对应的 IP 开始 Agent 配置；



可根据 IP 进行检索，快速查询对应的机器，可对指定机器下的 Agent 进行启动、停止、重启、删除（Agent 停止后才可进行删除操作）

资源限制：批量对采集工具进行传输资源的限制（下文会单独进行详细说明）；

批量配置 Agent：同一业务类型、日志目录结构相同的机器，可根据一个配置文件进行批量配置（下文会单独进行详细说明）；

b) 点击“添加日志”按钮，进行日志文件接入，若已有生成好的配置文件可通过上传配置文件的方式进行日志采集；



c) 填写对应的配置信息

日志文件配置

1. 输入需要采集的日志文件绝对路径，例如： /var/log/access.log

日志文件绝对路径

2. 选择解析规则，有助于更精准地解析日志

官方规则

不解析

dttracker

packetbeat_log

packetbeat_log1

metricbeat_log

metricbeat_log1

keepalived_log

lvs_log

PHP-FPM_log

redis_log

mysql_audit_log

zookeeper_log

kafka_server_log

elasticsearch_log

browser

browser1

nginx_error_log

ssh_log

mysql_log

apache_access_log

自定义规则:设置页面可以自定义您需要的解析规则

filterrule

caoge_1

ilog_log_type

esb_parser_in

xw_channel_log_type

adfasdf

liangchen

3. 输入appname将有助于后续查询日志，例如itemcenter usercenter等

请输入appname少于20字符

4. 输入自定义标签(tag)有助于日志精细化搜索，例如： server,app,api等。多个标签(tag)使用英文逗号分隔。

自定义标签tag

5. 选择保存类型

sofa日志(1天)

取消

确定

- 日志文件绝对路径：填写所需采集的日志文件所在路径 Path，可填写绝对路径，也支持通配符（如*.log），可针对某一路径下的搜索日志文件进行采集；
- 选择解析规则，解析规则分为两部分，一是系统默认给出的官方规则（常见的日志格式对应的解析规则），二是自定义解析规则（对于不支持的日志格式，用户可以在产品页面的“设置”标签下的“解析规则”标签里配置日志格式解析规则）建议用户在接入日之前配置好解析规则，方便后续根据日志字段进行管理（下文会针对解析规则进行详细说明）；
- 输入 Appname，用来定义所上传的日志类型，方便后续分类、管理；
- 输入 Tag，给所上传的日志打标签，同样方便后续做检索、管理；
- 选择日志保存周期，用户根据自身需求选择对应的保存时间；

点击确定即开始采集此机器对应目录下的日志文件。

d) 验证数据接入正确性

云日志

应用 搜索 告警

admin@dtstack.com 设置 帮助

设置

日志上传 选择上传方式 Agent管控 解析规则 数据源管理 数据脱敏 容量管理 权限管理

日志文件 Host: 172.16.10.248 添加日志 配置文件 上传配置文件

appname	tag	path	状态	操作
test	messages	/var/log/messages	已启动	停止 删除 查看
new	retry	/var/log/test.log	已启动	停止 删除 查看
cg	cgtag	/root/log/CG.log	已启动	停止 删除 查看
cg	cg1	/root/log/CG-1.log	已启动	停止 删除 查看
sms	sms	/root/log/SMS.log	已启动	停止 删除 查看
ilog	ilog	/root/log/ilog.log	已启动	停止 删除 查看
channel	channel	/root/log/channel.log	已启动	停止 删除 查看
csp	csp	/root/log/CSP.log	已启动	停止 删除 查看
esb	esb	/root/log/esb.log	已启动	停止 删除 查看
liangchen	liangchen	/root/log/liangchen_send.log	已启动	停止 删除 查看
hpA	HPA	/root/log/app.log	已启动	停止 删除 查看

资源限制(传输过程中, 资源消耗可被控制在所设范围内)

CPU限制	CPU自制	流量限制	流量自制	内存自制	状态	操作
不限制	不限制	不限制	不限制	不限制	已关闭	配置

日志列表页面显示对应的配置项，可查看当前采集状态，且可进行启停、删除操作；

点击查看可进入搜索页面查看当前日志是否开始上传（验证数据接入正确性）；

完成数据接入后，可以开始“云日志”平台整体功能的使用；

e) 配置文件

Agent配置文件

```
1 output:
2   logstash:
3     hosts: ['172.16.10.147:8635']
4     compression_level: 3
5     console: {pretty: false, enabled: false}
6 logging:
7   to_files: true
8   level: warning
9   files: {path: /home/admin/filebeat/logs/mybeat, keepfiles: 7, name: mybeat.log}
10  to_syslog: false
11 filebeat:
12   prospectors:
13     - tail_files: true
14       fields_under_root: true
15       paths: [/var/log/messages]
16       input_type: log
17       fields: {logtype: no_log, keeptype: business, appname: test, tag: messages, user_token: kRhisbdoTQMCZU5KqQgKQ7sDA7BM9kpldnQ5Nf2a18ER9yp,
18         uuid: 4caa8221-60db-4e01-a806-55a8e2b6aa12_filebeat}
```

下载配置文件

取消

修改/重启

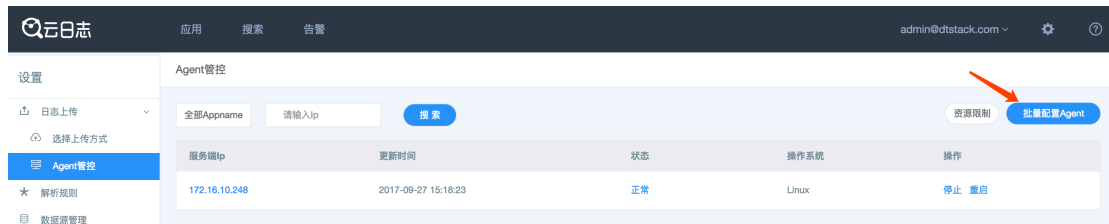
点击配置文件按钮，可查看、编辑、下载当前 Filebeat 配置信息；

若其他设备的日志结构与此设备相同，可将配置文件下载在其他设备上上传，提升配置效率；（手动修改配置文件需谨慎）

f) 批量配置 Agent（同一个应用在不同机器上，可使用批量操作）

打开配置文件对话框——单击下载配置文件到本地；

回到 Agent 管理页面，如下图单击“批量配置 Agent”按钮，进入批量配置流程；



- 上传下载好的配置文件；
- 选择需要统一配置的机器：左侧为所有可配置的机器 IP、操作系统类型可根据 IP 查找指定机器，右侧为当前已选择的机器，点击下一步，开始针对这些机器执行配置文件；
- 查看批量配置结果，点击下方按钮可返回 Agent 管理界面；

g) 传输资源限制

日志文件列表下方，可对采集工具进行传输资源限制，点击配置可进行相关参数设置；

可选择是否开启传输资源限制；开启后可针对 CPU、流量、内存进行限制；



限制阈值表示 Filebeat 保证在该值以下运行，不会超过设定的值，避免抢占业务系统资源的风险；

自刎阈值表示若传输过程中，发生异常资源消耗突破了限制值，达到某一值的时候采集工具即自动停止，避免影响业务；

资源限制

状态：

开启

关闭

限制内容	限制阈值	自刎阈值
CPU	10%	30%
流量 ?	7 Mb/s	20 Mb/s
内存	-	100M

取消

确定

h) 批量资源限制

点击 Agent 管理页面“资源限制”按钮，开始批量资源限制操作；

Q云日志

应用 搜索 告警

admin@dtstack.com

设置

Agent管控

全部Appname 请输入ip 搜索

资源限制 批量配置Agent

服务端ip	更新时间	状态	操作系统	操作
172.16.10.248	2017-09-27 15:33:34	正常	Linux	停止 重启

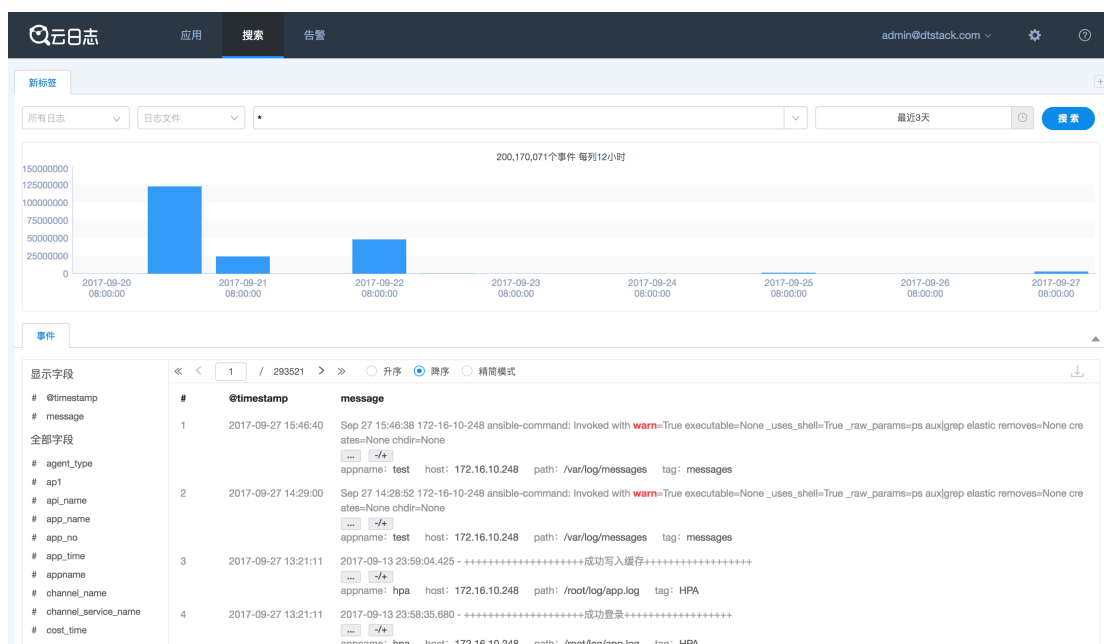
- 选择需要限制资源的机器：左侧为所有可配置的机器 IP、操作系统类型可根据 IP 查找指定机器，右侧为当前已选择的机器；
- 开始针对这些机器进行资源限制参数的配置；
- 同单台机器的资源限制一样，选择是否开启限制，配置对应的资源限制值、自刎阈值，点击下一步完成，对应机器资源限制参数已完成配置；

2 搜索

搜索是指根据一定测略、条件进行过滤查询需要的记录，快速过滤并找到相关的结果。

单击顶部导航蓝“搜索”按钮进入，主要功能如下：

- 多标签页视图
- 查询范围选择、过滤（含数据结构、日志分组）
- 对应范围下的日志文件选择
- 搜索框，查询语句检索
- 时间范围选择
- 保存当前搜索条件、使用已保存的搜索条件
- 直方图，统计所选时间的日志事件数量
- 事件视图



2.1 多标签页视图

支持同时处理多个任务，每个 tab 显示对应的查询内容，双击 tab 名称可重命名；

2.2 查询范围选择、过滤

默认范围为所有上传的日志，点击展开，包含数据结构、日志分组两种查询范围选择；

如下图，数据结构为当前用户所拥有权限的整体数据源结构树，点击某一节点即把此节点视作日志搜索范围；日志分组指的是日志数据的逻辑分组。搜索日志中的源数据必须通过上传日志中定义的主机名（hostname）、应用程序

(appname)、标签 (tag) 进行组合定义，选择日志分组后即视作将此分组作为搜索范围；（下列设置模块会对日志分组管理、创建 进行详细描述）

2.3 日志文件选择

日志文件对应左侧查询范围，显示的是该范围内的日志文件路径，支持多选，选择文件后，系统会将文件路径作为查询条件，点击搜索按钮即开始查询；

2.4 搜索框

搜索语句支持 Lucene 语法对日志进行实时搜索，目前支持以下搜索语法：

- 全文检索
- 短语查询
- 字段值查询
- 逻辑运算符
- 数值范围
- 通配符
- 特殊字符的检索处理
- 区分大小写

2.5 时间范围选择

时间范围选择可以自定义不同的时间区间，也可以快捷选择时间，查询跨度最大为 30 天；

2.6 事件直方图

默认会按照时间区间给出柱状图分布，可以根据此来判断日志事件随时间变化的整体趋势，并且可以点击柱状图上任意的时间段查看选定时间范围内的事件。

2.7 事件视图

字段列表显示在页面左侧，默认显示字段@timestamp 和 message，可将指定字段过滤出来，单独显示。

点击列表 “...” 按钮显示所有字段；

点击列表“-/+”按钮，查询当前文件、应用中相同文件、所有相同文件，前后1分钟、5分钟、10分钟事件；
精简模式显示日志原文。

3 搜索语法

日志检索过程中使用部分基础语法，可以极大提高故障排查效率。

3.1 全文检索

检索一个或多个查询词时，系统不区分大小写。如果查询多个关键字，则不区分这些词的先后顺序，且查询结果将同时包含这些词。例如

```
hello world
```

相当于查询搜索包含 hello 和 world 的日志。

```
hello AND world
```

即日志结果中必须包含 hello 与 world。

3.2 短语查询

如果需要查询短语（即短语内的多个词都必须都出现，而且保持同样的顺序及相邻状况），需要用双引号把短语括起来，查询结果不区分大小写。例如查询“hello world”，匹配的日志也必须包含“hello world”。

3.3 字段值

格式 field:value

field 是字段名，应当为字符串，搜索时区分大小写字母，不得使用？*等字符；value 可以是字符串或数值，字符串区分大小写字母，可以使用？*等字符。此用法也可在界面左栏的字段值处点击建立字段过滤。例如

```
apptime:"test"
```

匹配 apptime 字段值为 "test" 的日志；

```
code:"200"
```

匹配 code 字段值为 200 的日志；

```
code:*
```

匹配带 code 字段的日志；

```
clientip:192.168.1.1*
```

匹配 clientip 为 192.168.1.1, 192.168.1.103, 192.168.1.114 等值的日志。

3.4 逻辑运算符

匹配 apache.clientip 为 192.168.1.1, 192.168.1.103, 192.168.1.114 等值的日志。

```
term1 AND term2
```

匹配的日志里 term1 和 term2 都必须都出现，AND 默认可缺省；

```
term1 OR term2
```

匹配的日志里 term1 或 term2 出现 1 个即可；

```
NOT term
```

匹配的日志里不含有 term；

由于 AND 的优先级比 OR 高，可用（）改变运算优先级，例如：

```
term1 AND (term2 OR term3)
```

表示匹配的日志里必须包含 term1, 以及 term2、term3 中的任一个。

3.5 数值范围

格式

```
field:[value1 TO value2]
field:{value1 TO value2}
field:{value1 TO value2}
field:[value1 TO value2]
field:>value
field:>=value
field:<value
field:<=value
```

value/value1/value2 为数值, TO 必须大写, "["、"]" 符号表示包含边界数值, "{"、"}" 不包含边界数值。

如:

```
code:[400 TO 500]
```

匹配 code 值在 400 到 500 之间的日志, 包含 400 和 500。

```
code:>400
```

匹配 code 值大于 400 的日志。

3.6 通配符

* 匹配 0 个或多个字符, 单独搜索 * 会显示所有日志; ? 匹配 1 个字符。例如:

```
syslog.appName:abc*
```

```
syslog.appName:ab?
```

都会匹配 syslog.appName 为 abc 的日志

```
tag:mytag*
```

匹配 tag 为 mytag 或 mytag1 的日志

```
tag:mytag?
```

匹配 tag 为 mytag1 的日志，但 无法匹配 tag 为 mytag 的日志。

3.7 特殊字符的检索处理

只有字母、数字和字符检索时会匹配在事件日志。特殊字符+ - | | ! () { } [] ^ " ~ * ? : \ 等不应包括在查询语句的一部分来匹配，如果你在搜索时有上述特殊字符请务必使用引号括起来。例如，这两个搜索将显示相同的结果：

例 1:

```
"http://yourwebsite.com:9000"
```

例 2:

```
"http yourwebsite com 9000"
```

下面这个搜索将导致一个无效的查询，由于 : 没有被""括起来引用：

```
http://yourwebsite.com:9000
```

3.8 区分大小写

云日志在搜索时除以下情况情况区分大小写之外，其他情况不区分大小写：

- 字段名称（字段值不区分大小写）
- 数值范围 TO
- 逻辑运算符 AND/OR/NOT

3.9 时间方案

使用下拉菜单快速挑选预设时间方案或设置一个自定义的时间范围。

预设时间方案：分钟（近 10 分钟、30 分钟）、小时（近 1 小时、3 小时、6 小时和 12 小时）、天（近 1 天、2 天、7 天）默认近 10 分钟；

自定义时间范围：选择起至的年/日/月/小时/分钟/秒/毫秒范围，日志如果超出保存时间将不会显示搜索结果。

3.10 搜索技巧

为了提高您的搜索效率，搜索时请注意以下事项；

a) 明确查询范围

可以通过搜索框左侧数据结构、日志分组、日志文件选择好需要检索的日志范围，可以跳高查询速度、效率；

b) 请避免直接使用特殊字符，如果需要请使用引号括起来

特殊字符：+ - & || ! () { } [] ^ " ~ * ? : \，请避免直接出现在查询中。

c) 扩大时间范围

请检查您选择的时间范围，您可能误把分钟当做小时。

d) 移除过滤字段和关键字

请检查搜索框中的关键字，减少选择的过滤字段。

e) 检查你的拼写

小心拼写错误，您的日志事件和查询语句都有可能出错。

4 解析规则

解析规则分为两部分：

- 系统默认给出的官方规则，云日志提供常见的日志格式对应的解析规则；
- 自定义解析规则，用户根据日志格式自定义配置；

单击顶部导航设置按钮进入“解析规则”模块；

4.1 自定义解析规则

解析规则列表页面，单击“新建解析规则”按钮，进入规则配置页面；

Q云日志 应用 搜索 告警 admin@dtstack.com

设置中心

- 日志上传
- 解析规则**
- 数据源管理
- 数据脱敏
- 容量管理
- 权限管理

创建解析规则

logtype: 请输入logtype, 30个字符以内

规则名称: 请输入规则名称, 30个字符以内

规则描述: 请输入规则描述, 80个字符以内

输入规则描述便于规则解释。例如: mysql_log的规则描述为“MySQL数据库日志文件的解析规则”;

日志样例 选择日志样例

2017-08-20 09:52:13 611 [AP1-local_in-20170714095213-056142] INFO pool-FrameExecutor-in244 NewAppIdentifyService:144 - 请求者的IP: 127.0.0.1

message:2017-08-20 09:52:13 611 [AP1-local_in-20170714095213-056142] INFO pool-FrameExecutor-in244 NewAppIdentifyS...

+ 添加解析单元

- **选择日志样例：**将需要解析的日志样例粘贴至“日志样例”文本框内，或者单击“选择日志样例”按钮选择一条日志作为解析样例（可根据appname、tag、path或关键字进行筛选）；

选择日志样例

请选择appname / tag / path

关键词搜索

选择	Event
<input type="radio"/>	2017-07-14 09:52:00 034 [DEBUG pool-Jetty-118 HTTPServiceListenerServlet:161 - Http ser...
<input type="radio"/>	2017-07-14 09:52:00 068 [AP1-local_in-20170714095200-055954] INFO pool-FrameExecutor-i...
<input type="radio"/>	2017-07-14 09:51:59 488 [AP1-local_in-20170714095159-055951] INFO pool-FrameExecutor-i...
<input type="radio"/>	2017-07-14 09:52:13 610 [AP1-local_in-20170714095144-055843] INFO pool-FrameExecutor-i...
<input type="radio"/>	2017-07-14 09:52:13 611 [AP1-local_in-20170714095213-056142] INFO pool-FrameExecutor-i...

系统默认抓取指定条件下前200条日志，可选择其中一条日志做为解析样例

取消

确定

- 样例日志选择 / 填写完毕后，下方会生成一条 message，点击末尾添加按钮开始规则配置；

日志样例 选择日志样例

2017-08-20 09:52:13 611 [AP1-local_in-20170714095213-056142] INFO pool-FrameExecutor-in244 NewApplIdentifyService:144 - 请求者的IP: 127.0.0.1

message:2017-08-20 09:52:13 611 [AP1-local_in-20170714095213-056142] INFO pool-FrameExecutor-in244 NewApplIdentifyS...

+

- 选择解析方式，由于日志格式多样，需要多种方法进行处理，目前云日志支持“正则解析”、“KeyAalue 分解”、“JSON 解析”、“字段值拆分”、“数值型字段转换”5 种解析方式（4.2 详述）；



以正则解析为例

日志原文：

```
tag:waf_log_system_run stat_time:2017-03-10 18:22:27 type:RULE_UPGRADE source:monitor info:Install rule upgrade package update_rule.v6.0.5.1.35489.wcl: installation succeeded.
```

我们希望能将日志按字段 info、source、tag、stat_time、type 拆分；编写如下正则表达式填入输入框：

```
:(?<tag>[^\ ]+)[^:]+:(?<stat_time>%{TIMESTAMP_ISO8601})[^\ ]+:(?<type>[^\ ]+)[^:]+:(?<source>[^\ ]+)[^:]+:(?<info>.*)
```

单击确定查看解析结果；

正则表达式无语法错误即可看到日志已按照解析规则结构化显示，单击保存解析即可生成自定义解析规则。

在日志上传入口可选择使用；列表页面将鼠标移至自定义解析规则图标上可对自定义解析规则进行编辑、删除和复制创建（重命名）操作；

- **解析单元：**一个解析单元针对一类型日志进行解析，云日志内支持一个解析规则多个解析单元，可解析同一文件下多种格式日志；
新增解析单元操作流程相同；

4.2 解析规则配置说明

目前云日志支持以下 5 种解析方式如下：

a) 正则解析

正则是处理文本解析的有力工具。需要您了解一些基本的正则表达式知识：

```
\, ?, +, *, [], (?:) (?<key>value)
```

例如有这样一条日志：

```
2014-05-14 23:24:47 15752 [Note] InnoDB: 128 rollback segment(s) are active
```

我们希望提取出以下字段：timestamp, pid, loglevel 和 message，可以配置如下的表达式：

```
(?<timestamp>\S+ \S+) (?<pid>\S+) \[(?<loglevel>\S+\] (?<message>.*)
```

其中\S 表示匹配非空格字符，\S+表示匹配连续的非空格字符，
(?<key>value) 表示提取名字为 key 的字段，其值为 value，会解析出如下字段：

```
1 timestamp: 2014-05-14 23:24:47
2 pid: 15752
3 loglevel: Note
4 message: InnoDB: 128 rollback segment(s) are active
```

除了正常的正则表达式，我们还提供了一些常用的正则表达式，可以通过%{XXX}的方式来引用。比如可以使用%{NOTSPACE}来代替\S+，这样的正则表达式为：

```
(?<timestamp>%{NOTSPACE} %{NOTSPACE}) %{NOTSPACE:pid} \[%{NOTSPACE:loglevel}\] %{GREEDYDATA:message}
```

默认的字段的值是 string 类型的，如果您想将其转换为 number 类型，可以在引用中加入 type 类型，目前仅支持 int 和 float 类型，例如：

```
%{XXX:int} 或者 %{XXX:float}
```

b) KeyValue 分解

KV 主要用来解析明显的 KV 字符串，例如现需解析日志为：

```
field=tag&filters=&order=desc&page=1&query=*&size=50&sourcegroup=all&sourcegroup
Cn=%E6%89%80%E6%9C%89%E6%97%A5%E5%BF%97&time_range=-2d,now&type
=fields
```

这是一个按照"&"和"="来分割的 KV 字段。添加解析规则：KeyValue 分解，source 字段选择 request_query，定义字段间分隔符为&，定义 k-v 分隔符为=，点击解析，可看到如下图所示解析结果：

c) 数值型字段转换

默认提取出来的字段都是字符串类型的。如果您希望将这个值转换成数值类型，以方便再后面做统计，则需要通过这个功能来做转换。转换时需要您配置数值的类型：int/float

例如： 您的日志经过解析得出如下字段：

```
k1: "123",k2: "123.0"
```

经过转换可以转变为：

```
k1: 123,k2: 123.0
```

d) JSON 解析

JSON 解析用来解析 JSON 格式的日志，例如原始日志为：

```
{"Name": "John Smith ", "Age": 23, "Employed": true, "Address": {"Street": "324 Chrome St", "City": "Portland, New York, Los Angeles ", "Country": "United States"}}
```

JSON 解析后如下图所示：

e) 字段值拆分

将字符串切分，例如：

```
key: "1.2.3.4, 2.4.5.6"
```

可以根据“，”来对其进行切分成两个 value：

```
key: ["1.2.3.4", "2.4.5.6"]
```

5 应用

云日志可视化模块，对采集到的数据进行加工计算，通过“应用”的形式呈现，用户查看应用内可视化报表快速定位问题，优化运维、运营决策；

登录云日志着陆页为应用页面或单击顶部导航“应用”按钮进入模块；

- 管理员具有所有应用及仪表盘创建、编辑权限，其余用户需被授予对应功能 / 资源权限；
- 创建者自身拥有的数据源，标志该仪表盘所能编辑的数据源，其他用户查看或编辑仪表盘，均在该数据源范围内；



5.1 应用/仪表盘创建

初次进入应用模块，系统默认分配一个应用，租户下权限归管理员所有，管理员可在该应用下创建仪表盘，可将仪表盘查看权限分配给其他用户，其他用户即可看见该应用及对应拥有权限的仪表盘；

a) 添加应用

单击左侧边栏顶部“+”按钮，选择创建应用，当前页面弹出对话框，填写应用名称（必填），点击确认即完成应用创建，左侧边栏新增应用，可在该应用下建立仪表盘；

b) 添加仪表盘

单击左侧边栏顶部“+”按钮，选择创建仪表盘，当前页面弹出对话框进行操作；

- 编辑仪表盘名称；
- 所属应用：选择仪表盘所属应用；

若不具备，则该模块只显示选择应用，下列显示选择应用名称下拉菜单，选择对应应用；

若具备，则选择应用外，提供创建应用选项，选择创建应用，下列切换为应用名称表单，编辑即快速新建应用；

资源权限分配，默认不选择为 仅自己及管理员可进行查看、编辑；

添加仪表盘

*

名称:

*

模式:

选择应用

新建应用

*

应用:

默认应用

权限:

用户

查看

222@dtstack.com

取消

确定

【提示】仪表盘详细编辑方式另附使用手册；

5.2 应用 / 仪表盘管理

- a) 左侧边栏，展示应用列表、各应用内部包含的仪表盘，默认展开第一个应用，其余折叠，显示第一个应用下的第一个仪表盘，点击展开应用，再次操作折叠；
- b) hover 应用名称，末尾显示操作按钮，可对应用进行重名、删除操作；
- c) hover 仪表盘名称，末尾显示操作按钮，点击操作按钮，可对该仪表盘进行“编辑基本信息”、“置顶”、“删除”操作；
- d) 左侧边栏提供搜索，通过应用、仪表盘名称搜索；

6 告警

云日志为您提供监控保障体系，您可对异常情况进行定义配置告警规则（如异常日志事件数），按预设计划周期性执行，当满足触发条件时我们将通过电子邮件及时通知您，及时帮助您发现、预防问题。

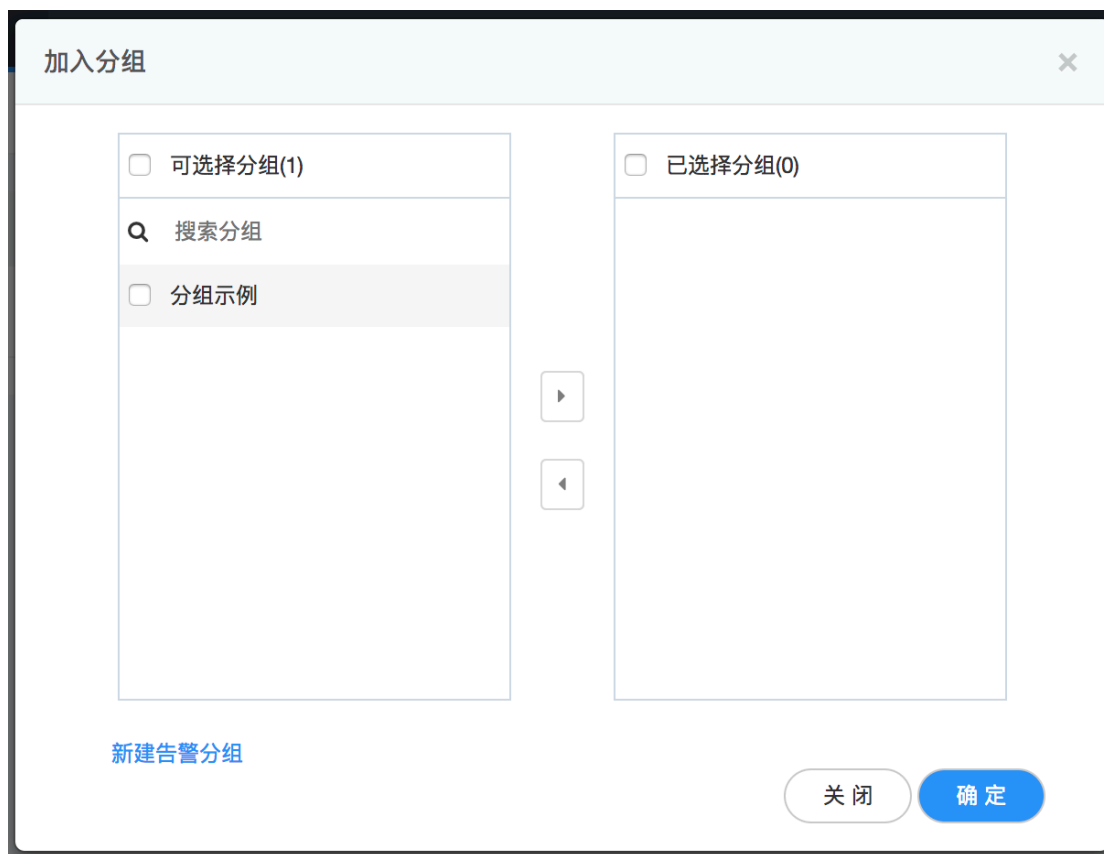
单击顶部导航“告警”按钮进入告警模块；

告警规则配置分两个步骤：1、告警接收人创建——>2、告警规则编辑；

6.1 设置告警接收人/分组

单击告警模块侧边栏“接收设置”进行接收人 / 分组创建；





单击“添加告警人”按钮，创建告警接收人，填写姓名、手机号、邮箱；
创建告警分组，将“告警人”添加至分组；
分组创建完毕后，即可开始创建告警规则；

6.2 告警规则配置

单击告警模块侧边栏“告警规则”进入告警规则列表，单击“创建规则”按钮，进入规则配置页面；



a) 选择所属应用

应用列表若已存在应用，告警规则可针对该应用创建规则，规则仅该应用下用户可见，若当前未创建应用或不针对应用内数据进行告警，也可选择“不属于任何应用”；

b) 选择监控类型

云日志提供如下 5 种告警类型：

- **事件数告警：**根据条件查询到的事件数进行告警，例如：5 分钟内“应用 A”的日志数超过 10 条时，系统进行告警；

事件数监控

字段统计监控

数值字段监控

字段分组统计监控

自定义监控

全部

中搜索

时, 如果

分钟 ▾

之内搜索结果的总条数

> ▾

阈值

紧急 ▾

+

- **字段统计告警：**根据条件查询到的事件中 指定字段的独立数、求和、平均值、最大值、最小值进行告警，例如：5 分钟内“应用 A”下含“error”字段的日志数>10 时，系统进行告警；

事件数监控

字段统计监控

数值字段监控

字段分组统计监控

自定义监控

全部

中搜索

时, 如果

分钟 ▾

之内的搜索结果中

字段

的

独立数(unique count) ▾

> ▾

阈值

紧急 ▾

+

- **数值型字段统计告警：**根据条件查询到的事件中 指定字段（必须为数值型字段）的值进行告警，例如：5 分钟内“应用 A”下“stats”字段下“404”的数量>10 时，系统进行告警；

事件数监控

字段统计监控

数值字段监控

字段分组统计监控

自定义监控

全部

中搜索

时, 如果

分钟 ▾

之内

字段

的值超过

阈值

的次数

> ▾

阈值

紧急 ▾

+

- **字段分组统计告警：**根据条件查询到的事件中，先对指定字段进行分组，计算结果中某一字段的独立数、求和、平均值、最大值、最小值进行告警，例如：5 分钟内“应用 A”下按“path”（文件名）进行分组，含 error

字段的日志数超过 10 条时，系统进行告警；

事件数监控

字段统计监控

数值字段监控

字段分组统计监控

自定义监控

全部

中搜索

时，如果

分钟

之中的搜索结果中根据

字段

分组，并计算

字段

独立计数

>

阈值

紧急

+

- **自定义监控：**系统支持根据 DSL 自定义查询，根据查询结果数进行告警；

事件数监控

字段统计监控

数值字段监控

字段分组统计监控

自定义监控

请输入DSL语句

校验

结果数

>

阈值

紧急

+

- c) **通知对象：**选择定义好的接收分组作为通知对象，可选择邮件、短信进行告警；
- d) **告警抑制：**可设定指定时段内，告警数量超过 N 次后不再进行告警，设定冷却时间进行恢复；

告警抑制：☒ 打开抑制

1

分钟

内，连续告警超过

1

次不再告警，

1

分钟

重置告警抑制。

- e) **执行计划：**分为基本执行计划、Cron 执行计划；

* 执行计划：☐ 基本计划 ☒ Cron计划

请输入Cron表达式

如: 每隔1分钟执行一次: 0 */1 *** ?

- **基本计划：**即告警执行频率，任务在指定时间范围内执行一次，系统默认建议为 1 分钟执行一次；
- **Cron 计划：**云日志支持通过 Crontab 格式设置告警执行频率；
Cron 格式：秒、分、时、日、月、周、年；（例如：0 */12 * * * * ）

* * * * *

- - - - -

```

|   |   |   |   |   |   |
|   |   |   |   |   |   + year [, - * /]
|   |   |   |   |   +----- day of week [, - * ? / L #]
|   |   |   |   +----- month [, - * /]
|   |   |   +----- day of month [, - * ? / L #]
|   |   +----- hour [, - * /]
|   +----- min [, - * /]
+----- second [, - * /]

```

通配符说明:

***** : 表示所有值. 例如: 在分的字段上设置 "*****", 表示每一分钟都会触发。

? : 表示不指定值。使用的场景为不需要关心当前设置这个字段的值。例如: 要在每月的 10 号触发一个操作, 但不关心是周几, 所以需要周位置的那个字段设置为"**?**" 具体设置为 0 0 0 10 ***** **?**

- : 表示区间。例如 在小时上设置 "10-12", 表示 10, 11, 12 点都会触发。

, : 表示指定多个值, 例如在周字段上设置 "MON,WED,FRI" 表示周一, 周三和周五触发

/ : 用于递增触发。如在秒上面设置"5/15" 表示从 5 秒开始, 每增 15 秒触发 (5, 20, 35, 50)。 在日字段上设置'1/3'所示每月 1 号开始, 每隔三天触发一次。

L : 表示最后的意思。在日字段设置上, 表示当月的最后一天(依据当前月份, 如果是二月还会依据是否是闰年[leap]), 在周字段上表示星期六, 相当于"7"或"SAT"。如果在"L"前加上数字, 则表示该数据的最后一个。 例如在周字段上设置"6L"这样的格式, 则表示 “本月最后一个星期五”

W : 表示离指定日期的最近那个工作日(周一至周五)。例如在日字段上设置 "15W", 表示离每月 15 号最近的那个工作日触发。如果 15 号正好是周六, 则找最近的周五(14 号)触发, 如果 15 号是周末, 则找最近的下周一(16 号)触发。如果 15 号正好在工作日(周一至周五), 则就在该天触发。如果指定格式为 "1W", 它则表示每月 1 号往后最近的工作日触发。如果 1 号正是周六, 则将在 3 号下周一触发。(注, "W"前只能设置具体的数字, 不允许区间"-")。'L'和 'W'可以一组合使用。如果在日字段上设置"LW", 则表示在本月的最后一个工作

日触发

#：序号(表示每月的第几周星期几)，例如在周字段上设置"6#3"表示在每月的第三个周星期六. 注意如果指定"6#5"，正好第五周没有星期六，则不会触发该配置(用在母亲节和父亲节再合适不过了) 周字段的设置，若使用英文字母是不区分大小写的 MON 与 mon 相同。

6.3 告警历史查询

单击告警模块侧边栏“告警历史”查看；
顶部可根据创建的应用进行筛选，支持告警名称关键字进行查询；



7 数据脱敏

云日志支持针对数据中敏感信息制定脱敏规则，并管理敏感数据的读取权限，防范生产数据、用户隐私数据泄露等安全隐患；

单击顶部导航设置按钮进入“数据脱敏”模块；



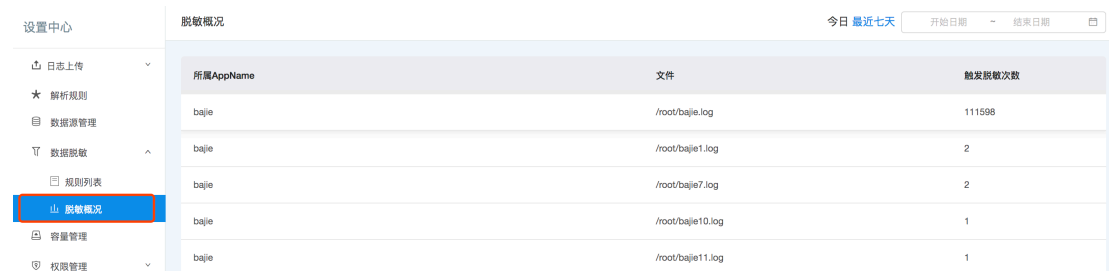
7.1 脱敏规则创建

单击规则列表页面“新建规则”按钮，开始配置；

- a) **作用域：**分为2类，“全局”、“指定 appname”；
 - 已知哪些文件有敏感数据的情况下，可针对性进行脱敏（更精准），可选择需要脱敏的应用；
 - 未知日志内容情况下，可针对全局进行脱敏，但凡匹配到脱敏规则的数据全部进行脱敏处理；
- b) **日志样本：**可填写含敏感信息的日志样例，下列规则需对样例进行效果预览；
- c) **脱敏正则：**编写正则表达式匹配敏感信息，系统内置常见脱敏正则表达式供用户选择，“身份证号”、“手机号”、“银行卡号”，可根据预设的正则进行调整，也可自行定义正则表达式过滤敏感信息，也可添加多条正则，提高敏感信息匹配率；
- d) **脱敏数据显示方式：**系统默认脱敏后‘***’显示，可指定将正则表达式匹配到的敏感信息替换为其他字符（支持部分替换），也可设置将整条日志脱敏不可见；
- e) **效果预览：**点击预览“查看脱敏效果”，预览当前脱敏后的效果，以此调整脱敏规则；
- f) **脱敏人群：**分为两种方式“黑名单”、“白名单”；
 - **黑名单：**脱敏规则对所选择的用户不生效，选定的用户可查看原数据；
 - **白名单：**脱敏规则对所选择的用户生效，选定的用户查看的数据都会事先经过过滤、屏蔽；
- g) **智能分析：**可选择是否开启，开启后系统将会对含规则内对应敏感信息的数据进行脱敏，“脱敏概况”模块可查看对应统计数据；

7.2 脱敏概况

单击数据脱敏模块侧边栏 “脱敏概况” 按钮进入；



所属AppName	文件	触发脱敏次数
bajie	/root/bajie.log	111598
bajie	/root/bajie1.log	2
bajie	/root/bajie7.log	2
bajie	/root/bajie10.log	1
bajie	/root/bajie11.log	1

若脱敏规则开启“智能分析”按钮，则该规则“作用域”内新上传的文件含敏感信息，系统会进行记录，统计对应日志文件敏感信息的条数；
支持查看不同时间段的敏感信息记录；

8 数据源管理

单击顶部导航设置按钮进入“数据源管理”模块；

管理当前平台内已接收到的数据源；

- 进入数据源管理模块，显示当前已接收的日志文件列表；
- 列表显示日志文件所属机器 IP、appname、tag、path（文件路径）、接入时间及日志最后上传时间，展开可查看该日志采集方式、所运用的解析规则、保存周期；
- 可跳转至搜索页面查询选定的日志文件详情；
- 支持通过自定义数据结构进行筛选，支持通过关键词查询；

9 容量管理

单击顶部导航设置按钮进入“容量管理”模块；

容量管理，空间使用量、总用量，各应用日志空间使用趋势；

- 进入容量管理模块，显示当前空间总使用量，最近 7 天空间使用趋势统计，不同应用下空间使用趋势；
- 保存周期管理，显示当前定义的保存周期列表，系统内容保存周期不可调整，可在日志上传时或配置文件处使用指定保存周期，日志会根据保存周期进行定期清理；

10 权限管理

云日志系统提供精细粒度功能、数据源权限控制，以“功能分组”、“数据源分组”的形式，将功能、数据源权限点进行组合，分角色授予对应用户，用户只能访问自己被授予的功能及数据源，提高对资源的监管能力；

单击顶部导航设置按钮进入“权限管理”模块；



权限管理分为 4 个模块：

- 用户管理；
- 功能权限；
- 数据权限；
- 组织架构；

10.1 功能权限

单击权限管理模块侧边栏“功能权限”按钮进入；

功能角色：角色类似于“分组”，是一组功能权限的集合，表示允许用户使用这些功能，选择对应功能权限创建一个分组，将分组赋予用户；

新建角色：输入角色名称、描述，选择对应功能点权限（功能点权限为树形，可展开），保存即创建为功能角色。

10.2 组织架构

单击权限管理模块侧边栏“组织架构”按钮进入；

本功能是业务结构树的管理入口，业务结构树实际上是数据源的结构，主要用

于数据源权限的分配（权限管理-权限分组-数据源权限，详细请参考上文 15.2 权限分组）。

编辑业务结构树时，在上方的文本输入框内，以文本形式输入数据源树形结构，输入规则为：以 appname 为叶子节点配置数据源权限结构，层级之间使用英文都好进行分隔；一行显示一个节点对应的层级关系（如：层级 1，层级 2，appname1）

点击“预览”，可在下方预览修改后的树形结构。

点击“保存”，即可形成此业务结构树。

在业务结构树中新增一个数据源时，所有的用户分组中，默认都不会具有此数据源的权限。必须将对应的数据源组建为数据分组，为这些用户分配这些新增的数据源权限。

该数据源结构将会被应用于“数据源管理”、“Agent 管控”、“搜索模块”

【注意】如果您新添加了一个数据源，必须在此业务结构树中进行配置，配置成功后，此数据源才能被其他用户查询、应用。

10.3 数据权限

单击权限管理模块侧边栏“数据权限”按钮进入；

数据角色：角色类似于“分组”，是一组数据源权限的集合，表示允许用户查看对应的数据源，选择对应数据源创建一个分组，将分组赋予用户；

新建角色：输入角色名称、描述，选择对应数据源（即方才创建好的组织架构，数据源树形结构），保存即创建为数据角色。

10.4 用户管理

用户列表中列出了本租户内云日志的所有用户，在“用户账号”一列，列表内管理员账号前具备相应标识，分租户管理员（超级管理员）、普通管理员；

- **租户管理员：**可管理所有用户功能、数据源权限，可将其他用户置为普通管理员；
- **普通管理员：**可管理普通用户功能、数据源权限；
- **赋权：**点击操作项“编辑功能/数据源权限”，当前页面弹出对话框，可将设置好的功能分组、数据源分组赋予指定用户，保存成功后，此用户立即

获得了相应的权限分组。

11 用户中心

用户中心包括产品中心、成员管理、个人信息管理三部分。账户中心是用户对自身信息管理的入口，同时也是主账号对租户内成员管理的入口。

11.1 账户体系

账户中心包括产品中心、成员管理、个人信息管理三部分。账户中心是用户对自身信息管理的入口，同时也是主账号对租户内成员管理的入口。

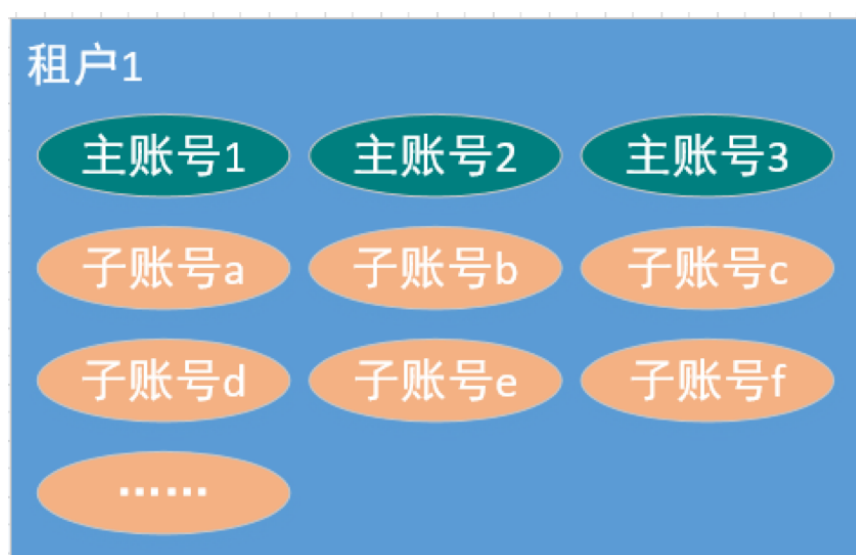
在描述账户体系前，需要解释一些基本概念：

租户是一组“资源”的集合，租户内通常会有多为用户相互协作，操作租户内的资源。不同的租户间的资源是相互隔离的（本产品目前具备单一租户功能，下一版本会增加多租户功能）。

租户角色：主账号、子账号

租户角色分为主账号和子账号，主账号具备租户内成员的管理功能（添加、移除、分配产品权限），子账号可以查看本租户内的成员（不具备管理功能）。

租户内的主账号、子账号关系如下图所示：



【注意】每个租户内至少有一个主账号，最多有 3 个主账号，每个主账号的权限相同。

产品角色：云日志管理员、云日志查看权限

云日志管理员可以为本租户内所有使用云日志产品的用户分配具体的功能权限、数据源权限。云日志查看不能为他人分配产品功能权限。

权限分组

权限分组表示一组云日志的功能点+数据源的权限组合，云日志管理员可以将某个用户置为这个权限分组内。

11.2 用户权限分配

由于账户中心采用租户模式，为用户分配权限需要分 2 步骤完成：

步骤一：由主账号在账户中心配置此用户是租户角色（是主账号还是子账号）、产品角色（是云日志管理员或是查看权限）。

步骤二：由云日志管理员在云日志产品内，将某个用户加入到一个权限分组中。请参考下文 9.1 权限分组。



11.3 进入账户中心

- 1、在云日志产品内，点击左上角的“展开”按钮（绿色 icon），展开左侧的功能菜单。
- 2、点击“用户名”，展开下拉菜单，下拉菜单中包括：当前租户名称、用户管理链接、退出登录。

3、点击“用户管理”，页面跳转至账户中心。



11.4 产品中心

产品中心包括 2 部分：

- 1、云日志产品入口：点击后进入云日志首页；
- 2、租户信息：显示当前所在的租户信息，包括租户名称、创建时间、租户备注、主账号的姓名、子账号数量等；若当前登录的账号为租户主账号，则租户卡片上会显示“我管理的”标签，若为租户子账号，则显示“我参与的”标签；

11.5 租户内成员管理

点击“成员管理”菜单，显示本租户内的所有成员，同时主账号可添加、移除成员，或执行分配权限等操作。下面以主账号 A、子账号 B 作为示例。

11.6 查看成员

主账号 A、子账号 B 均可以查看本租户内的所有成员，但 B 仅能查看成员信息，不具有任何操作权限。

11.7 添加成员

【注意】 仅主账号可以添加成员

- 1、进入成员管理页面，点击“添加成员”按钮，在弹窗中输入登录邮箱、用户姓名、产品角色后，点击“添加，并将密码复制到剪贴板”即可。
- 2、若用户邮箱已经存在，则不能再次添加。

3、添加成员完成后，主账号需要将用户名、密码发送给被添加的用户，被添加的用户即可登录。

11.8 赋予成员租户角色

【注意】 仅主账号可以分配租户角色

- 1、主账号添加成员时，被添加的成员默认为子账号。
- 2、已添加的成员，主账号可在“成员管理->成员列表->操作”中点击“置为主账号”或“置为子账号”修改其租户角色。
- 3、主账号可以修改其他主账号、子账号的租户角色，但不能修改自己的租户角色。
- 4、主账号 A 在修改住角色的同时，若被修改的账号 B 处于登录状态，则 B 会自动退出，重新登录后，会启用新的租户角色。

11.9 赋予成员产品角色

【注意】 仅主账号可以分配产品角色

- 1、主账号在添加成员时可以为该成员分配产品角色。
- 2、对于已添加的成员，主账号在成员列表中通过点击产品访问权限，选中则对应应用户可访问云日志产品。
- 3、主账号可以修改其他主账号、子账号以及自己的产品角色。

11.10 移除成员

【注意】 仅主账号可以移除成员

- 1、主账号在“成员管理->成员列表->操作”中，点击“移除成员”按钮，经弹窗确认后，即可将此用户移除租户。
- 2、主账号可以移除租户内的其他主账号、子账号，但不能将自己移除。
- 3、主账号 A 移除 B，仅表示 B 不再属于这个租户；若 B 还存在其他租户，B 仍可以登录成功，并进入其他租户进行操作；若 B 不存在其他租户，则 B 无法登录。

11.11 重置成员密码

【注意】 仅主账号可以为其他成员重置密码

- 1、当其他成员（例如 B）忘记密码时，需要线下联系主账号 A 为其重置密码。
- 2、A 在“成员管理->成员列表->操作”中，点击“重置密码”，进入重置密码页面，在页面中点击“重置密码”后，B 的密码即被重置。A 需要手动复制新密

码，并发送给 B，B 使用新密码登录。

3、若 B 在登录状态下被重置密码，则 B 会立即退出系统，必须使用新密码登录。

11.12 修改租户信息

【注意】仅主账号可以修改租户信息

1、租户信息包括租户名称、租户描述，主账号可以对其进行修改。

2、“成员管理->成员列表”中，在列表上方显示了租户信息，点击“修改”按钮后，弹出编辑弹窗，修改后保存即可。



11.13 个人信息管理

1、任何用户都可以修改自己的个人信息，包括姓名、公司名称、手机号码、密码；但登录邮箱不可修改。

2、用户在账户中心中，点击“个人中心->个人信息”页面，可以查看自己目前的信息，点击“修改”按钮，可在弹窗中修改各项信息。

3、修改密码：用户在账户中心中，点击“个人中心->修改密码”页面，输入当前密码，新密码，并确认新密码后，即可修改自己的密码。密码修改成功后，用户立即退出登录，页面跳转至登录页面，用户需要输入登录邮箱和新的密码重新登录。