SinoSecOp 机器大数据分析平台

用户手册

北京神州新桥科技有限公司

2017 年 9 月 1 日

目 录

1 前言

1.1 产品介绍

SinoSecOp 机器大数据分析平台，主要提供海量日志数据收集，存储，和搜索服务。以及通过日志实现监控告警和日志分析服务。

SinoSecOp 主要技术特点包括：

- 采用分布式架构，具备横向扩展能力，可以支持每秒数万条日志的处理量，保证不因处理性能而遗漏日志。
- 采集客户端支持断点续传，当遇到传输故障时，支持从传输断点从新传输日志信息，保证日志信息的完备性。
- 支持日志流实时匹配日志的内容或一段时间内的日志条数进行告警。
- 全文检索的搜索引擎技术，满足日志的事后审计检索或合规检查。

1.2 术语与符号说明

表格1.　术语与符号说明

术语/符号	说明
SinoSecOp	神州新桥大数据日志分析平台
Elasticsearch	ElasticSearch 是一个基于 Lucene 的搜索服务器。它提供了一个分布式多用户能力的全文搜索引擎，基于 RESTful web 接口。
Gork 模式	基于正则表达式的日志提取器语法

1.3 获取更多服务

了解机器大数据分析平台产品请访问：

http://www.sino-bridge.com/sinosecop/

了解更多软件产品和服务请访问：

http://www.sino-bridge.com/

2 安装部署

2.1 Server 部署

2.1.1 单机部署

2.1.1.1 硬件配置要求与操作系统支持列表

表格2. 单机部署配置要求与操作系统支持列表

设备	物理机(推荐)/虚拟机
CPU	32C
内存	64GB
硬盘	4TB
操作系统支持列表	RedHat 、CentOS、SUSE

2.1.1.2 SinoSecOp 服务端环境要求

SinoSecOp 包含多个组件，如 SinoSecOp server、ElasticSearch、MongoDB 等。这些组件都应部署在同一台机器上。配置好系统的 hostname 和 DNS 域名解析，配置好 yum 源，软件安装前准备工作包括：

关于 SELinux，SELinux 对开放哪些端口，有非常严格的限制， 我们在将日志输入到 SinoSecOp 系统时，会新建一个 Input，会涉及到要开启一个端口，根据以往经验，绝大多数的端口不通，都是因为 SELinux 问题，因此，我们会选择关闭 SELinux.

 # setenforce 0 （临时关闭 SELinux）

 # vi /etc/selinux/config （永久关闭 SELinux）

修改 SELINUX=enforced 为 SELINUX=disabled，重启操作系统使 SELinux 的设置生效。

关于防火墙，由上述可知，在新建一个 Input 时会开一个端口，为安全起见，应该要添加一个相应的 iptables 规则，这样显示比较麻烦，又因为我们的系统是在客户的内网里，可以认为是比较安全的环境，所以我们也选择关闭掉防火墙。

 # systemctl disable firewalld

 # systemctl stop firewalld

关于修改操作系统内存，Elasticsearch 是我们系统的组件之一，Elasticsearch 使用 mmapfs/niofs 存放索引，操作系统缺省的 mmap 配置无法满足要求，需要运行命令 **sysctl -w vm.max_map_count=262144**，来修改操作系统内存参数。如果想让修改在操作系统重启后仍然生效，在文件**/etc/sysctl.conf** 中，添加下面一行：

vm.max_map_count=262144

2.1.1.3 SinoSecOp 软件安装

下载我司提供的 SinoSecOp-2.0.0-0.el6.x86_64.rpm 安装包， 用 rpm 命令直接安装：

 # rpm –ivh SinoSecOp-2.0.0-0.el6.x86_64.rpm

上述 rpm 命令直接安装之后，会把文件拷贝到/opt/elap/目录下，安装完成后会有一个命令提示，要求您按照下面的命令进行 SinoSecOp 初始化，直接执行即可。

 # sudo elap-ctl reconfigure

上面的初始化命令会把系统的管理员用户与密码都设置为admin，将SinoSecOp开启的9000端口代理到 Nginx 本地的 80 端口。还有比如创建 elap 用户，初始化配置文件，启动进程等都是 reconfigure 做的。此时，可用以下命令查看 SinoSecOp 服务状态：

 # elap-ctl status

如果是正常启动，应该可以看到有 5 个组件都是 run 状态，如下：

```
[root@localhost ~]# elap-ctl status
run: elap-server: (pid 3552) 33247s; run: log: (pid 3413) 33255s
run: elasticsearch: (pid 5658) 10149s; run: log: (pid 3321) 33259s
run: etcd: (pid 3304) 33261s; run: log: (pid 3303) 33261s
run: mongodb: (pid 3381) 33257s; run: log: (pid 3380) 33257s
run: nginx: (pid 3584) 33246s; run: log: (pid 3469) 33249s
[root@localhost ~]#
```

附图1. 查看 Server 运行状态

至此，您可以打开浏览器，输入服务地址 http://<SinoSecOp 服务器的 IP>/，输入默认的用户名与密码 admin/admin，即可进入 SinoSecOp 机器大数据分析平台。详见【4.1.1】

2.1.1.4 管理命令

SinoSecOp 服务端使用 runit 监控各个服务程序，一旦服务程序出错退出，runit 负责自动将其重启。当您需要启动、关闭、重启所有 SinoSecOp 组件时，可如下操作：

 # elap-ctl start

 # elap-ctl stop

 # elap-ctl restart

当您需要只重启 SinoSecOp server 或 ElasticSearch 时，只需：

 # elap-ctl restart elap-server

 # elap-ctl restart elasticsearcch

2.1.1.5 修改管理员密码

接下来，我们来看看如何修改管理员的密码，vi 打开/opt/elap/conf/elap.conf 文件，搜索关键字 password，找到如下两行：

```
# You MUST set a secret to secure/pepper the stored user passwords here. Use at least 64 characters.
# Generate one by using for example: pwgen -N 1 -s 96
password_secret = da3a11795bbebff307cc3e27b98bd841c4969a2b42ac4e5264671f46e65667f64b3dd412bbe88e540f6fb453baa3979fd99be055
67222dd6048bd02ba3b292b1

# The default root user is named 'admin'
root_username = admin

# You MUST specify a hash password for the root user (which you only need to initially set up the
# system and in case you lose connectivity to your authentication backend)
# This password cannot be changed using the API or via the web interface. If you need to change it,
# modify it in this file.
# Create one by using for example: echo -n yourpassword | shasum -a 256
# and put the resulting hash value into the following line
root_password_sha2 = 8c6976e5b5410415bde908bd4dee15dfb167a9c873fc4bb8a81f6f2ab448a918
```

附图2. 根据配置文件修改管理员密码

修改密码时，就运行上图中的两个命令即可：

 # pwgen -N 1 -s 96 #运行此命令并记录该值

 # echo -n PASSWORD | shasum -a 256 #运行此命令并记录该值

用上面两个命令返回的字符串，分别替换/opt/elap/conf/elap.conf 文件中的 password_secret 和 root_password_sha2 的值，然后重启 SinoSecOp server.

另外，在此配置文件中要把搜索高亮显示开头打开，搜索关键字 high，确认如下配置：

allow_highlighting = true

2.1.2 集群部署

尊敬的客户您好，您目前选择的版本不支持集群部署，如需更多服务请参考【1.3 获取更多服务】章节。

2.2 Agent 部署

2.2.1 Linux 环境部署

2.2.1.1 Nxlog 采集日志

从 http://nxlog.co/products/nxlog-community-edition/download 下载 nxlog for Linux 安装包。运行命令安装：

rpm –ivh nxlog-ce-2.9.1716-1_rhel7.x86_64.rpm

安装成功后在 nxlog 配置文件/etc/nxlog.conf 中增加配置信息：

```
<Input in>
    Module    im_file
    File      "/opt/*.log"                    # 要收集的日志所在的位置
    SavePos TRUE
</Input>
<Output out>
    Module    om_tcp
    Host      192.168.113.83     # SinoSecOp 服务器的 IP 地址
    Port      12346              # SinoSecOp 服务器接收日志的端口
</Output>
<Route 1>
    Path            in => out
</Route>
```

上面黑体部分配置的意思是：收集 /opt 目录下的所有后缀名是.log 的文件，通过 TCP 命令传输到 IP 地址是 192.168.113.83 的 SinoSecOp 服务器的 12346 端口。

重启 nxlog 服务：

 # service nxlog restart

2.2.2 Windows 环境部署

从 http://nxlog.co/products/nxlog-community-edition/download，下载 nxlog for Windows 安装包，安装成功后在 nxlog 配置文件 nxlog.conf 中增加配置，注意在写配置时，首行要敲一个 Tab 键，即两个空格。

```
<Input in>
    Module im_file
    File "C:\\test\\\*.log"
    SavePos TRUE
</Input>
<Output out>
    Module      om_tcp
    Host 192.168.113.83
    Port 12345
</Output>
<Route 1>
    Path in => out
</Route>
```

上面添加的黑体部分配置的意思是：收集 C:\test 目录下的所有后缀名是.log 的文件，通过 TCP 命令传输到 IP 地址是 192.168.113.83 的 SinoSecOp 服务器的 12345 端口。

在计算机管理>服务与应用程序>服务>选择 nxlog 服务>重新启动。

2.3 Agent 支持列表

表格3. Nxlog 支持平台

Windows	支持
Android	支持
Debian Squeeze i386	支持
Debian Squeeze amd64	支持
Debian Wheezy amd64	支持
Debian Jessie amd64	支持
Ubuntu 12.04 amd64	支持
Ubuntu 14.04 amd64	支持
Ubuntu 16.04 amd64	支持
Centos/RedHat 7 x86_64	支持
Centos/RedHat 6 x86_64	支持
SUSE 11	支持
SUSE 12	支持

以上信息仅供参考，请以 nxlog 官网最新信息为准。

3 快速入门

本章节是建立在已完成系统安装部署为前提，并以接收 syslog 日志为例，完成从日志的输入、解析、搜索、分析。

下面假设通过 SysLog UDP 协议来发送日志，分析日志格式后创建提取器进行日志分析，之后对日志进行分流操作，分流后进行日志告警及告警通知设置，最后划分用户的访问权限。

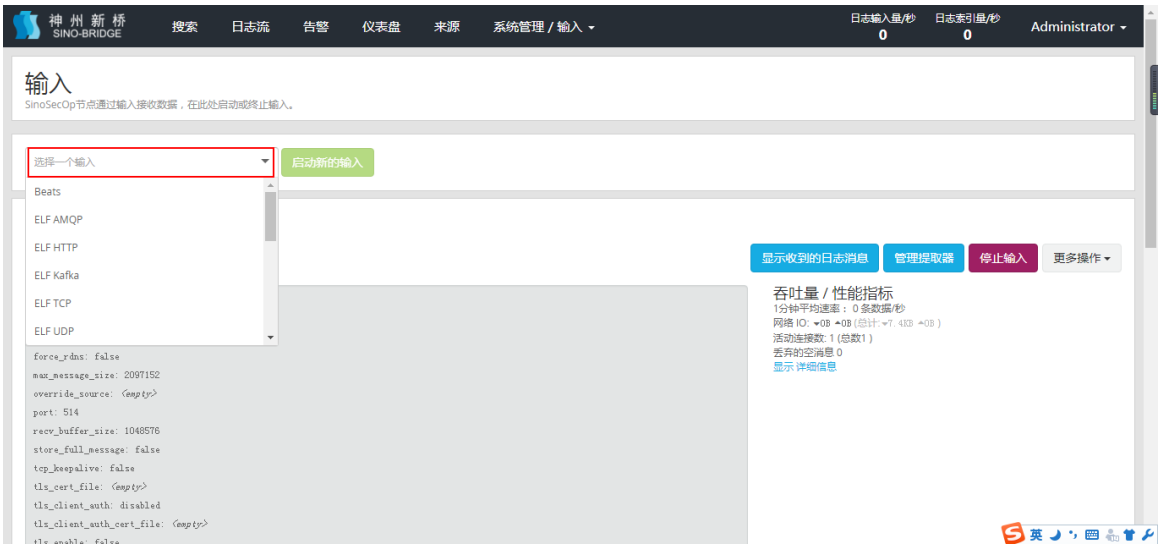
3.1 创建输入

创建 syslog UDP 输入，并监听在 514 端口上。

在导航栏中选择【系统管理】，单击【输入】按钮：

附图3. 创建输入-进入输入页面

选择一个输入模式：



附图4.　创建输入-选择模式

选择输入模式后单击【启动新的输入】：

附图5.　创建输入-启动新的输入

勾选全局启用，填写标题、端口号：

附图6.　创建输入-启动新的输入页面

鼠标滚轮下滑至底端，单击“保存”，完成输入的创建：

附图7.　创建新输入-保存输入

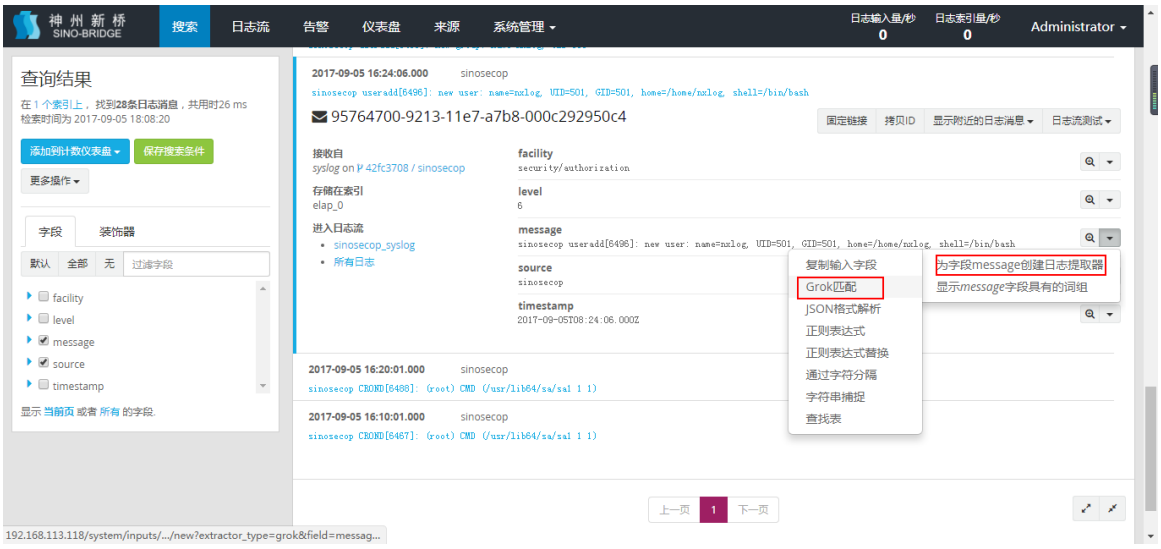
创建完成后可显示相关日志：

附图8.　创建输入-显示日志

3.2 创建日志提取器

选择需要做提取器的日志，单击日志展开，在 message 字段后单击  按钮，选择“为字段 message 创建日志提取器”，我们可以选择很多方式创建提取器，下面我们以“Grok

匹配”的方式为例，创建一个提取器。



附图9.　创建日志提取器

填写相应的 Grok：如 name={%WORD:name}，将日志解析：

附图10. 创建日志提取器-填写 Grok

添加提取条件，填写提取器标题：“用户名提取器”，单击【创建提取器】，完成提取器创建：

附图11. 创建日志提取器-完成

3.3 日志搜索

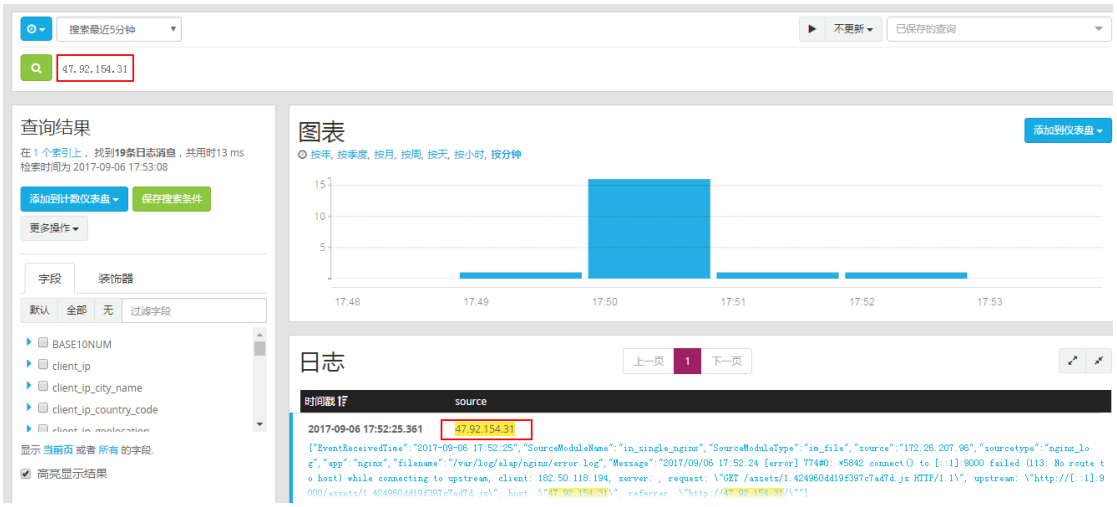
在导航栏单击“搜索”，选择时间点：

附图12. 按时间搜索日志-选择日志产生时间

添加搜索条件，然后敲回车键或者单击  按钮完成日志搜索：

附图13. 按条件搜索日志-输入查询条件

如搜索关键字‘47.92.154.31’



附图14. 按条件搜索日志-查询结果

搜索包含 message 字段的日志：

附图15. 包含 message 字段的日志

搜索 client_ip：182.50.118.194 的日志消息

附图16. 搜索 client_ip：182.50.118.194 的日志消息

附图17. 搜索结果

3.4 日志流

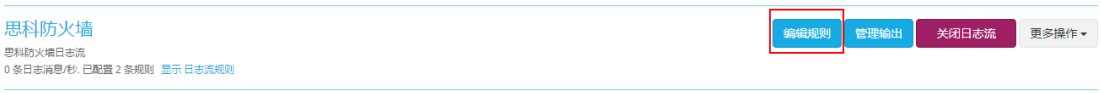
在导航栏单击【日志流】，然后单击【创建日志流】：

附图18. 创建日志流

填写标题为：思科防火墙日志流；描述为:思科防火墙日志里；单击【保存】：

附图19. 填写日志流标题及描述

单击【编辑规则】：



附图20. 编辑规则

单击【添加日志流规则】按钮：

附图21. 添加日志流规则

添加字段名，选择类型，可以选择添加或者省略描述，单击【保存】：

附图22. 保存添加的日志流规则

选择管理日志流规则，然后单击【完成】按钮，完成日志流规则创建：

附图23. 完成日志流的创建

最后单击【启动日志流】，完成日志流的创建：

附图24. 启动日志流

3.5 日志分析

第一步：生成图表；

1、选择 anti_virus_dst_ip 的快速值添加至仪表盘。

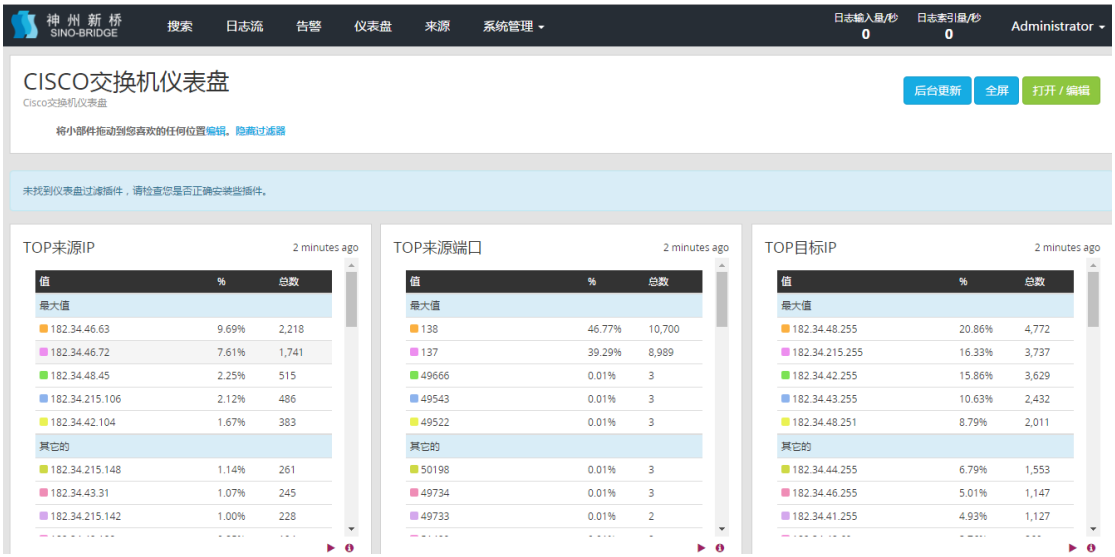
2、选择 anti_virus_src_port 的快速值添加至仪表盘。

3、选择 anti_virus_dst_ip 的快速值添加至仪表盘。

4、选择 anti_virus_dst_port 的快速值添加至仪表盘。

5、选择 loglevel 生成图表添加至仪表盘。

第二步：从仪表盘中可以看出日志分析结果：



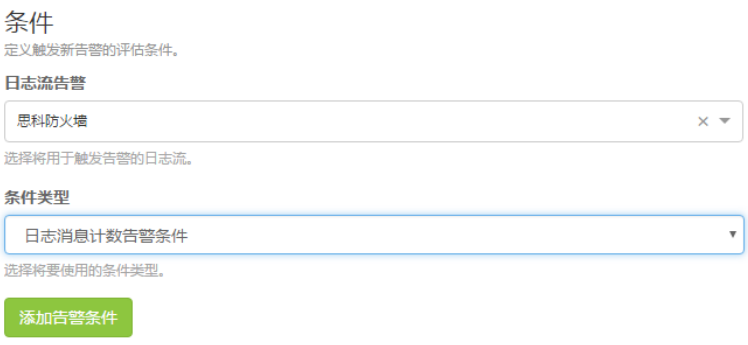
附图25. 查看日志分析结果

3.6 告警与通知

当满足定义的告警条件时会触发告警,问题解决(状态改变)后告警状态自动变成已解决。告警分为告警条件及告警通知，告警条件可以定义触发告警的条件，告警通知作用在日志流上，当该日志流相关的告警条件被触发，将以定义告警通知是所指定的通知方式，通知给相关人员。

3.6.1 定义告警

单击【添加新的条件】，进入创建告警条件页面：



附图26. 定义告警条件

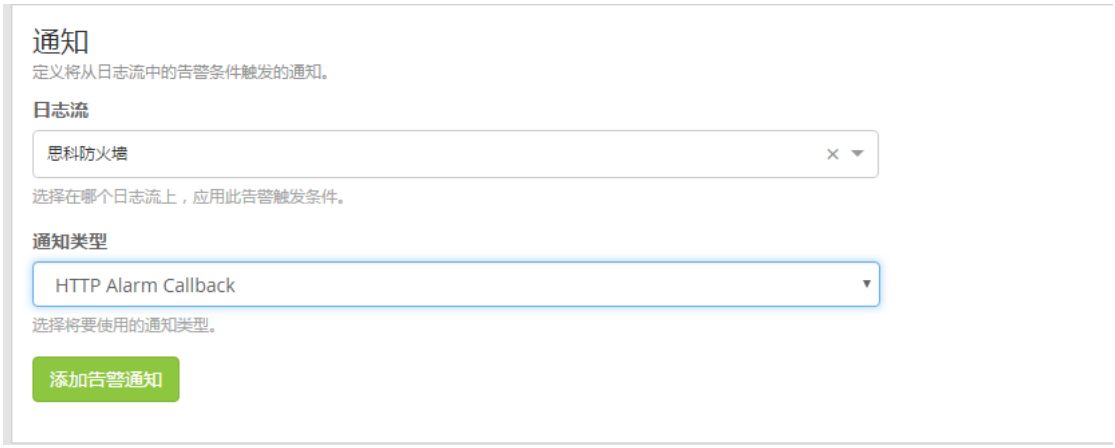
选择日志流及条件类型，单击添加告警条件：此时将为这个日志流添加告警条件。

附图27. 保存告警条件

按照提示，填写相关内容单击【保存】即可保存该告警条件。

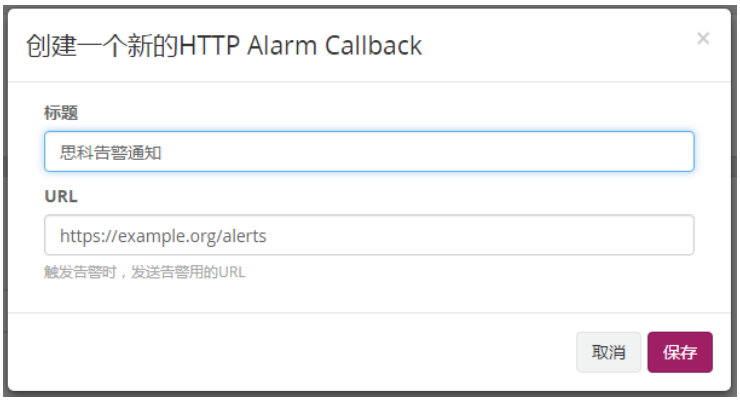
3.6.2 定义通知

单击【添加新的通知】，进入创建告警通知页面：



附图28. 创建告警通知

选择日志流、通知类型，单击【添加告警通知】：



附图29. 填写通知方式

输入标题单击【保存】，即可保存该通知。

3.7 权限

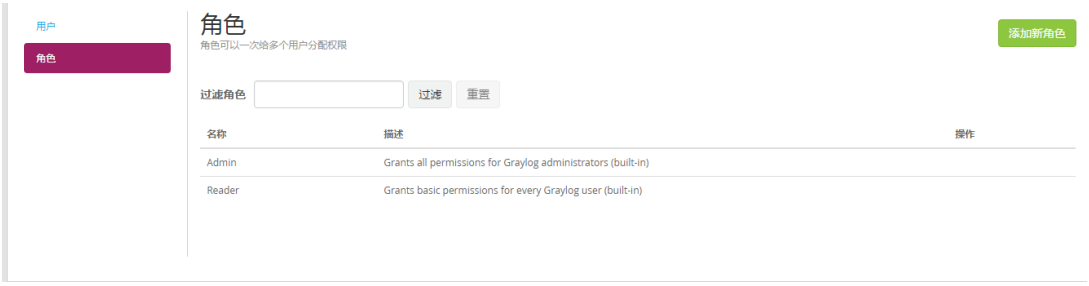
我们为两个用户（tom & jerry）赋予不同的角色，可以是不同的用户访问到的日志流和仪表盘不同。

单击【系统管理】再单击【认证】

附图30. 认证页面

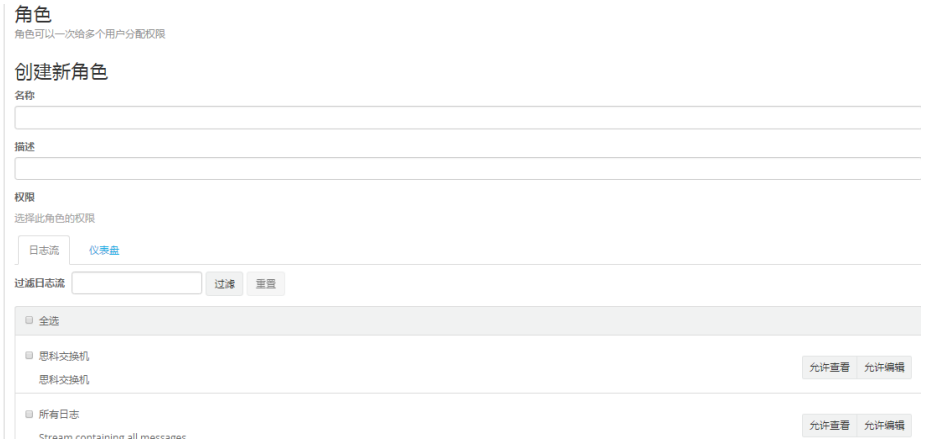
第一步：新增两个角色{思科防火墙管理员}和{交换机管理员}

单击【角色】进入角色页面：



附图31. 角色页面

单击【添加角色】



附图32. 添加角色

分别添加两个角色：

表格4. 添加两个角色

名称	描述	权限
思科防火墙管理员	思科防火墙管理员	选择防火墙日志流和 ASA 概览仪表盘 可编辑权限
交换机管理员	交换机管理员	选择交换机日志流 可读权限

第二步：添加用户

单击【用户】进入用户页面：

附图33. 用户页面

单击【添加新用户】

创建用户 tom

附图34. 添加 tom

创建用户 jerry

附图35. 添加 jerry

此时 tom 的权限是思科防火墙管理员：

附图36. 查看 tom 访问页面

Jerry 的权限是思科交换机管理员

附图37. 查看 jerry 访问页面

4 功能使用

4.1 登录与退出

4.1.1 登录

打开浏览器，地址栏输入：应用服务地址，然后按回车键，进入系统登录页面。

附图38. 系统登录界面

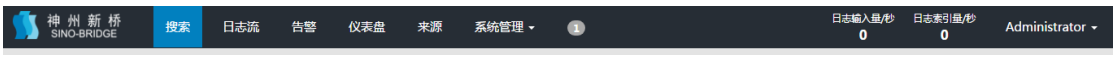
输入用户名、密码按回车键或单击登录按钮即可登录系统。系统缺省用户名密码是 admin / admin。Admin 用户的口令必须通过命令进行修改，具体修改方法请参考【安装部署】章节。

4.1.2 退出

将鼠标移至于右上角用户信息栏，单击【退出登录】即可退出。

附图39. 系统退出

4.2 导航菜单与日志量



附图40. 导航条

4.2.1 导航菜单

附图41. 导航菜单

（Admin 登录）导航菜单分为六部分搜索、日志流、告警、仪表盘、来源、系统管理；其中系统管理有分为概览、配置、节点、输入、输入、索引、认证、扩展包、Grok 模式、客户端、日志流处理器十一小项。

4.2.2 通知消息数量

附图42. 消息通知数量显示

【导航栏】右侧小气泡显示的为 SinoSecOp 会发出通知。

4.2.3 日志输入量与日志索引量

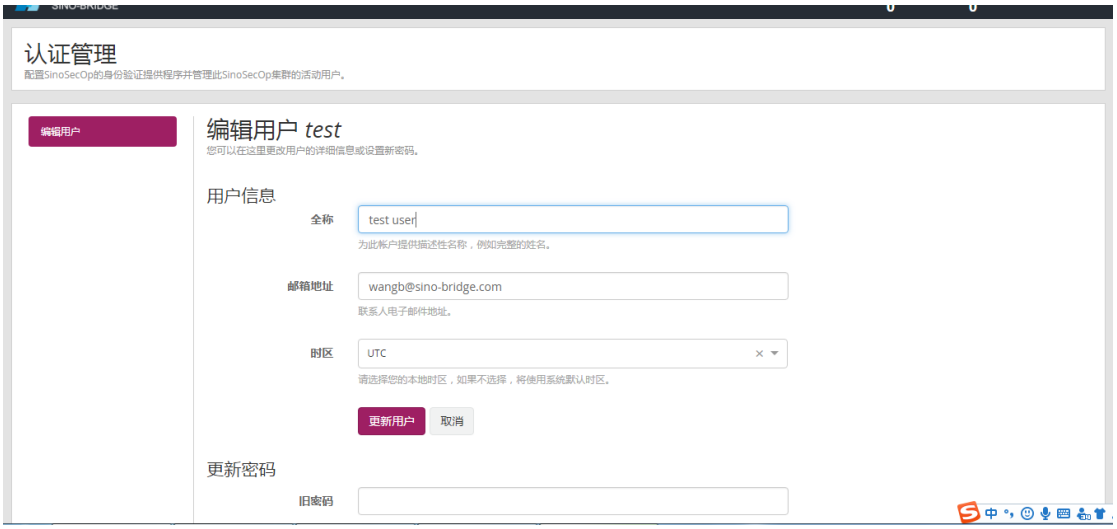
附图43. 日志输入和索引量

日志输入量和日志索引量可显示当前系统每秒钟接收日志及索引日志的数量。

4.3 编辑配置文件（当前登录用户）

将鼠标移至于右上角用户信息栏，单击【编辑配置文件】即可退出。

Admin 用户只能通过 SinoSecOp 配置文件来修改。修改方法参照【安装部署章节】。

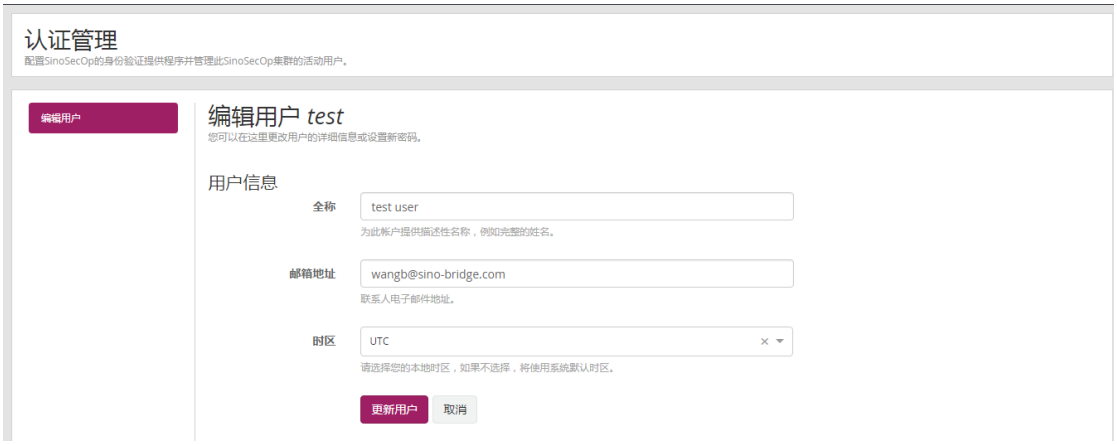


附图44. 修改登录用户信息

编辑用户分为两部分：用户信息、权限设置。

4.3.1 用户信息

用户信息：主要修改用户的全称、邮箱地址以及时区。



附图45. 编辑用户信息

修改全称/邮箱地址/时区后单击更新用户即可完成修改

4.3.2 更新密码

附图46. 修改密码

输入旧密码、新密码、重复新密码单击更新密码即可修改当前用户密码。

4.4 搜索

搜索页面可以搜索所需日志并且可设置显示样式，页面包含时间选择器、图表查询条件、设置日志刷新频率、对查询结果进行一些操作，图表及日志的展示。

附图47. 搜索页面

4.4.1 时间选择器

时间选择器定义在什么时间范围内搜索。它提供了三种不同的选择时间范围的方法，相对时间、绝对时间、关键词搜索。

附图48. 搜索-时间选择器

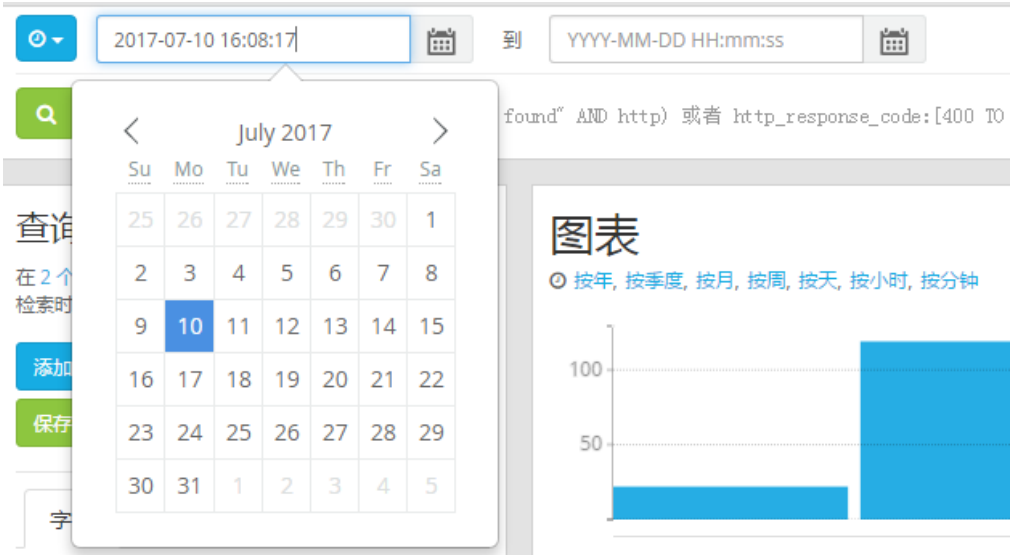
4.4.1.1 相对时间

相对时间选择可以选择搜索距当前时间的一个相对时间段：

附图49. 搜索-时间选择器-相对时间

4.4.1.2 绝对时间

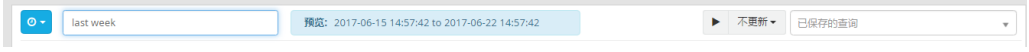
绝对时间选择可以筛选出某一个时间段内日志：



附图50. 搜索-时间选择器-绝对时间

4.4.1.3 关键词搜索

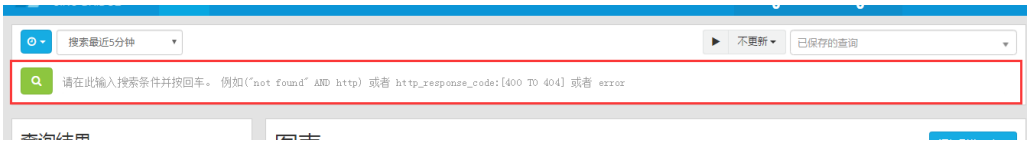
可以输入“last month” “4 hours ago” “1st of april to 2 days ago”等来搜索所需的日志：



附图51. 搜索-时间选择器-关键词搜索

4.4.2 通过搜索条件搜索

输入搜索条件按回车即可搜索：



附图52. 搜索-通过搜索条件搜索

系统的搜索语法非常接近 Lucene 语法。如果没有指定要搜索的消息字段，默认所有日志消息字段都包含在搜索中，但如果搜索大范围的日志，这样会十分耗时。

下面是一些例子，说明输入是如何对应搜索条件的：

表格5. 搜索语法示例

输入内容	对应的搜索条件
ssh	所有字段中包含词语 ssh 的日志
ssh login	所有字段中包含词语 ssh 或 login 的消息
"ssh login"	所有字段中正好包含词组 ssh login 的消息
type:ssh	字段 type 中包含 ssh 的消息
type:(ssh login)	字段 type 中包含 ssh 或 login 的消息
type:"ssh login"	字段 type 中匹配词组 ssh login 的消息
missing:type	没有字段 type 的消息
exists:type	有字段 type 的消息

默认情况下，所有词语或词组以 OR 连接，这样所有至少符合一个条件的消息都被返回。你可以使用布尔操作符和分组来控制，例如：

"ssh login" AND source:example.org ("ssh login" AND (source:example.org OR source:another.example.org)) OR _exists_:always_find_me

你也可以使用 NOT 操作符，例如：

"ssh login" AND NOT source:example.org NOT example.org

请注意，关键字 AND、OR 和 NOT 是区分大小写的，必须以大写。

通配符：使用?来代替一个字符，使用*来代替 0 个或多个字符，例如：

source:*.org source:exam?le.org source:exam?le.*

请注意，默认情况下，只有 message、full_message 和 source 字段可以用通配符搜索。

模糊搜索：你可以查找类似但不相等的词语，这样在即使有一些拼写错误，也不影响搜索结果，例如：

ssh logni~ 可以匹配到 “ssh login”

source:exmaple.org~ 可以匹配到 example.org

数字字段支持范围查询。方括号中的范围是闭区间，花括号的范围是开区间，也可以组合使用，例如：

http_response_code:[500 TO 504] http_response_code:{400 TO 404} bytes:{0 TO 64] http_response_code:[0 TO 64}

也可以用大于小于号搜索，例如：

http_response_code:>400 http_response_code:<400 http_response_code:>=400 http_response_code:<=400

转义，下面的字符必须用倒斜杠转义：

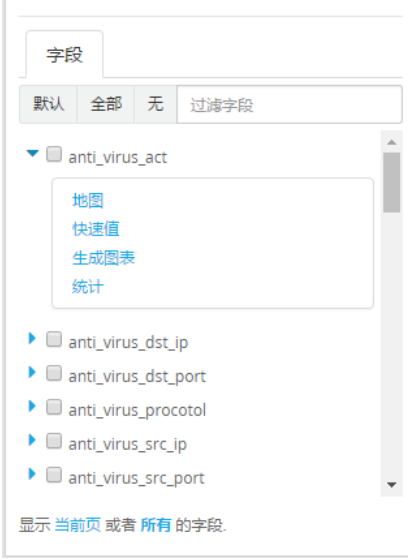
&& || : \ / + - ! ( ) { } [ ] ^ " ~ * ?

例如：

resource:\/posts\/45326

4.4.3 字段图表分析

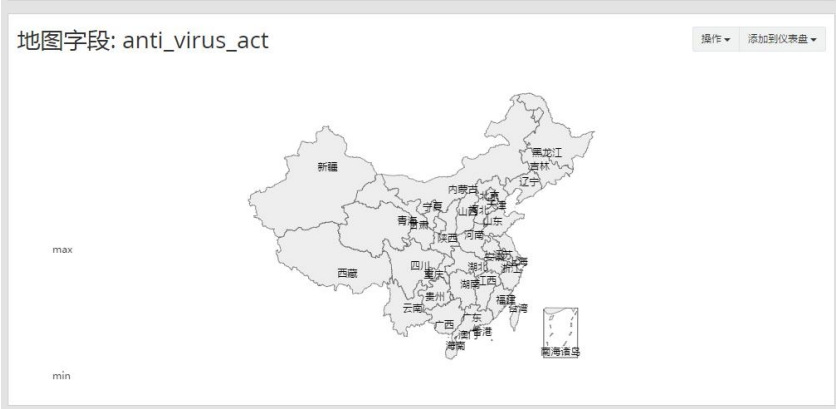
单击【字段名】可以选择根据字段生成一些字段图表：如地图、快速值、生成图表、统计。



附图53. 搜索-字段图表

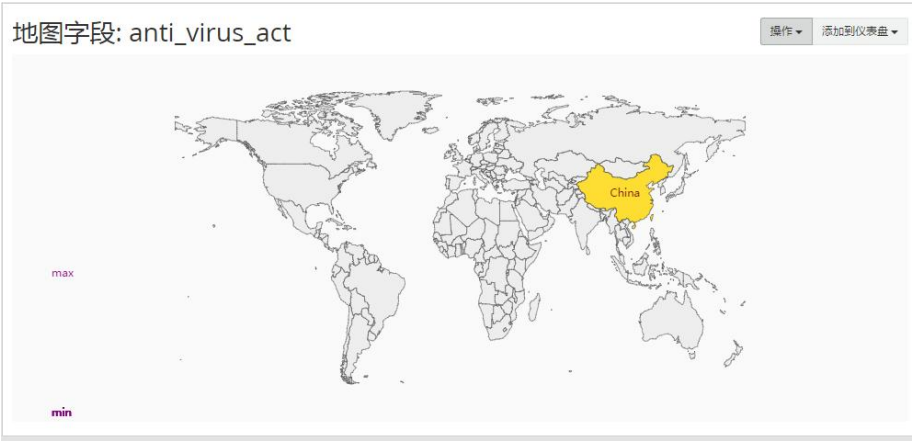
4.4.3.1 地图

单击【地图】，可显示地图：



附图54. 搜索-字段图表-生成地图

单击【操作】可以选择【关闭】该图，或者单击【世界地图】可将地图转化为世界地图。

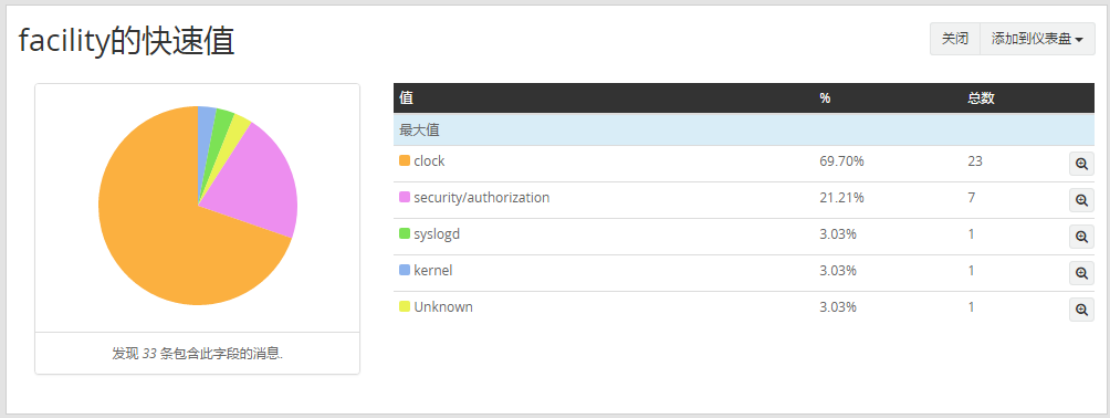


附图55. 搜索-字段图表-生成世界地图

单击【添加到仪表盘】，可以选择将地图添加某一个仪表盘中，添加方式可查阅【添加到仪表盘】章节：

4.4.3.2 快速值

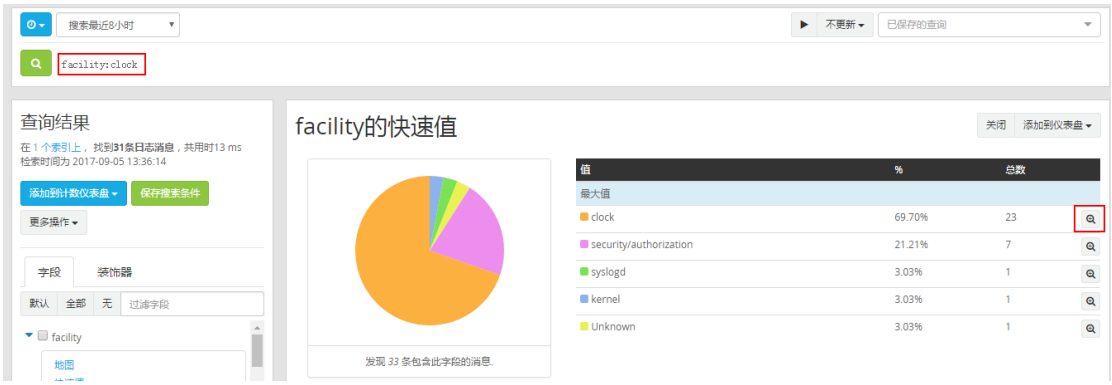
单击【快速值】可以查看该字段的快速值



附图56. 搜索-字段图表-快速值

单击【操作】可以选择【关闭】该图，单击【添加到仪表盘】，可以选择将快速值添加某一个仪表盘中，添加方式可查阅【添加到仪表盘】章节：

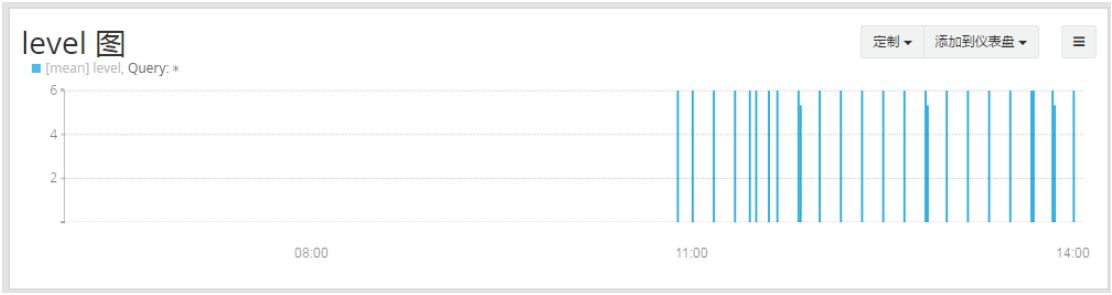
单击  可将该值添加到搜索条件：



附图57. 搜索-字段图表-添加至搜索条件

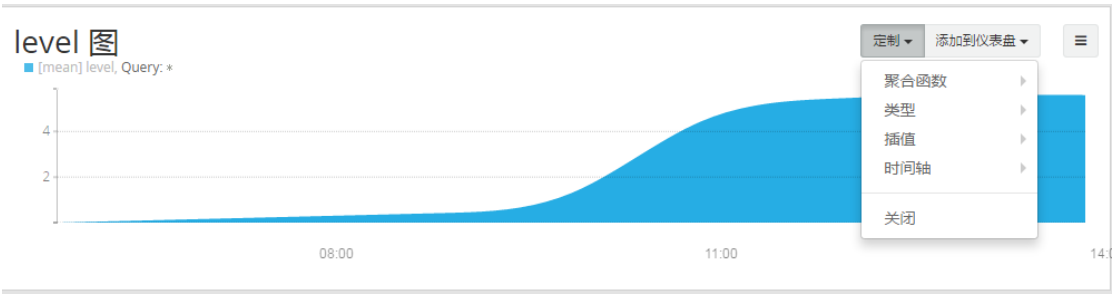
4.4.3.3 生成图表

数值类型的字段可以生成图表，单击【生成图表】，基于该字段生成图表：



附图58. 搜索-字段图-生成图表

单击【定制】可对生成的图表进行一些操作，如【聚合函数】、【类型】、【插值】、【时间轴】：



附图59. 搜索-字段图-生成图表-定制

选择【聚合函数】可选择图表的函数类型：

附图60. 搜索-字段图-生成图表-定制

聚合函数

Mean 平均数

Max 最大值

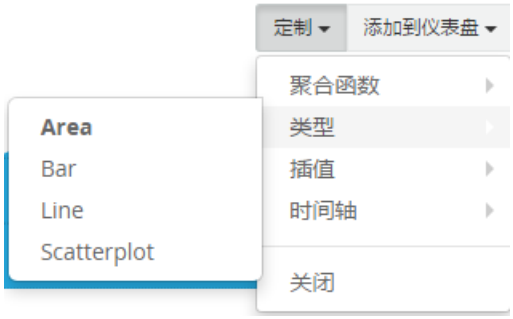
Min 最小值

Sum 求和

Total 总数、频次

Cardinality 去重后频次

选择【类型】可选择图表的显示类型：



附图61. 搜索-字段图-生成图表-定制

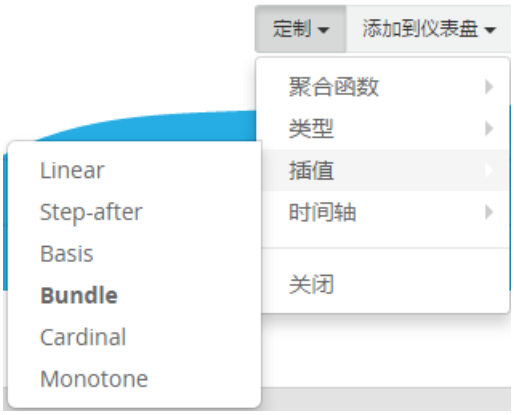
Area 面积图

Bar 柱状图

Line 折线图

Scatterplot 散点图

选择【插值】可选择图表显示形式：



附图62. 搜索-字段图-生成图表-定制

Linear 线性

Step-after 逐步

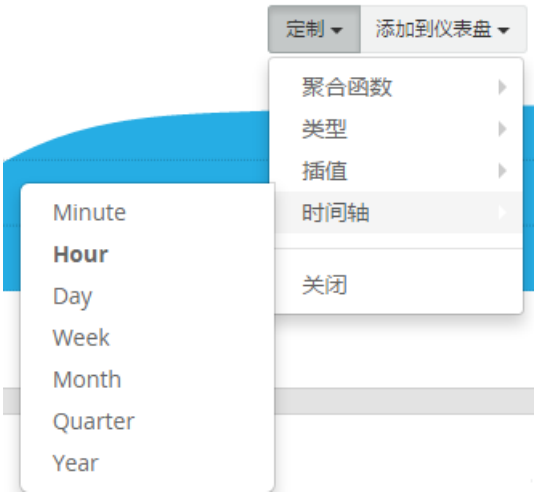
Basis 基础

Bundle 归并

Cardinal 基数

Monotone 单调

选择【时间轴】可选择图表展示的时间段：



附图63. 搜索-字段图-生成图表-定制

Minute 分钟

Hour 小时

Day 天

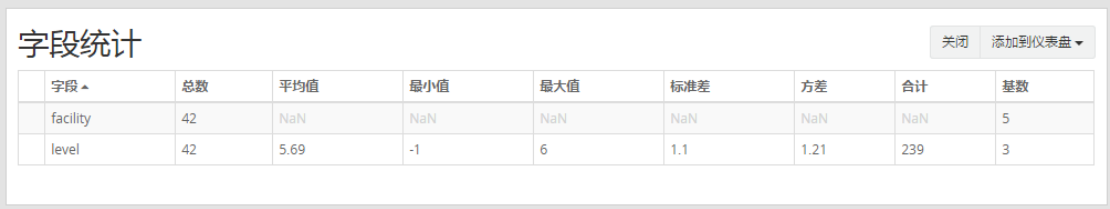
Week 星期

Quarter 季度

Year 年

4.4.3.4 统计

单击【统计】可字段值，字段统计主要同一字段的总数、平均值、最小值、最大值、标准差、方差、合计、基数；当多个字段进行字段统计显示在同一表格中：



字段	总数	平均值	最小值	最大值	标准差	方差	合计	基数
facility	42	NaN	NaN	NaN	NaN	NaN	NaN	5
level	42	5.69	-1	6	1.1	1.21	239	3

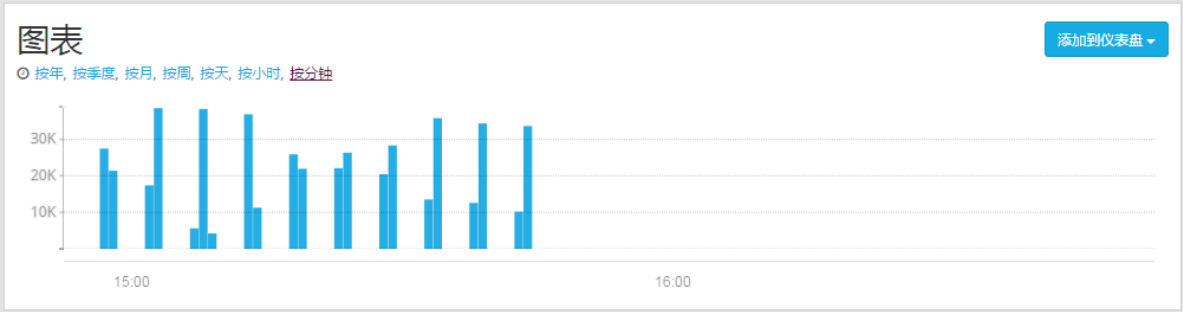
附图64. 搜索-字段图-字段统计

单击【添加到仪表盘】，可以选择将地图添加某一个仪表盘中，添加方式可查阅【添加到仪表盘】章节。

4.4.4 图表

4.4.4.1 默认图表按时间统计日志量

默认图表显示的柱状图 可以直观的看到收到日志的数量;可以选择不同的时间长度展示出想要的结果



附图65. 搜索-默认图表

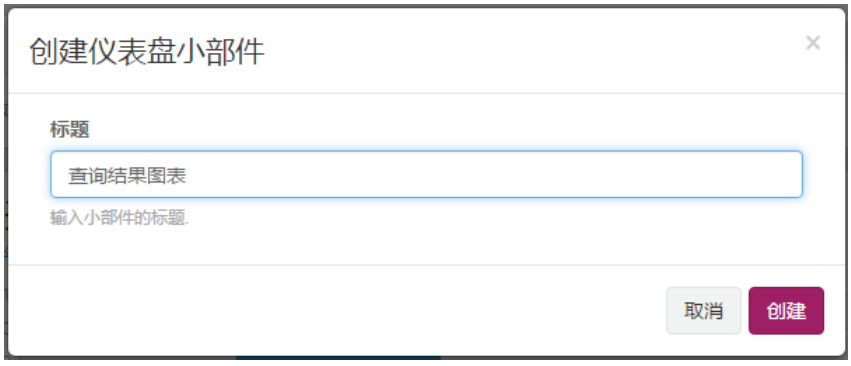
4.4.4.2 生成的图表

生成的图表可根据您的一些需要进行调整，生成图表的方式可查看【4.4.3】章节。

4.4.4.3 添加到仪表盘

4.4.4.3.1 添加到仪表盘

将已生成的图表添加到仪表盘：单击右上角的【添加到仪表盘】，选择要添加至哪个仪表盘，



附图66. 创建仪表盘小部件

输出小部件表填单击【创建】即可保存仪表盘小部件。保存完成的小部件可在仪表盘页面查看。

4.4.4.3.2 添加到计数仪表盘

查询结果下单击【添加到计数仪表盘】

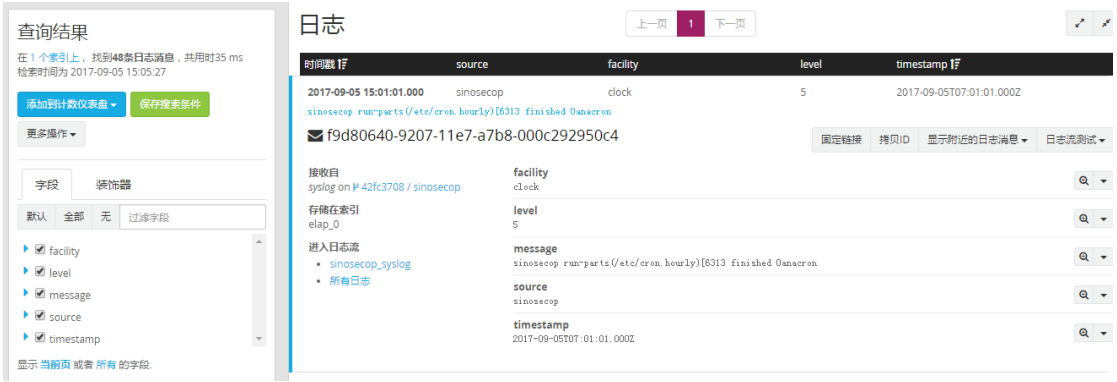
附图67. 添加到计数仪表盘

填写标题、勾选显示趋势，单击【创建】即可添加至计数仪表盘

附图68. 创建仪表盘小部件

4.4.5 查询结果

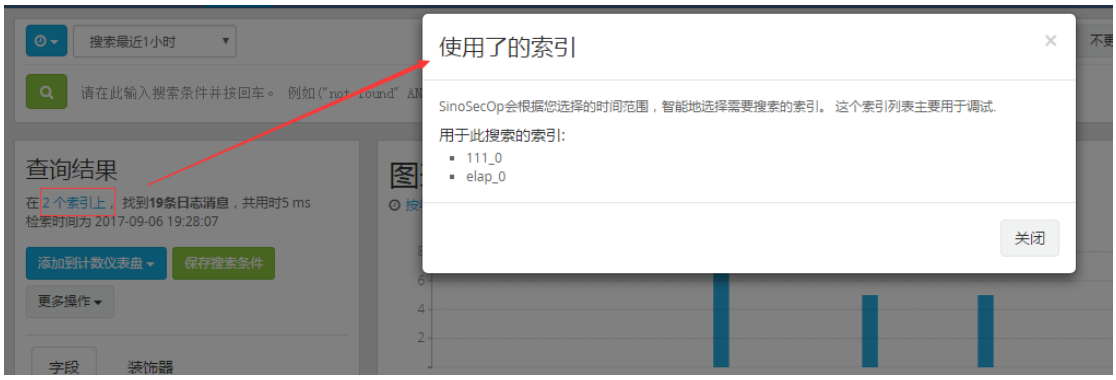
单击日志内容可查看日志全部信息：



附图69. 查看搜索结果

4.4.5.1 查询结果介绍

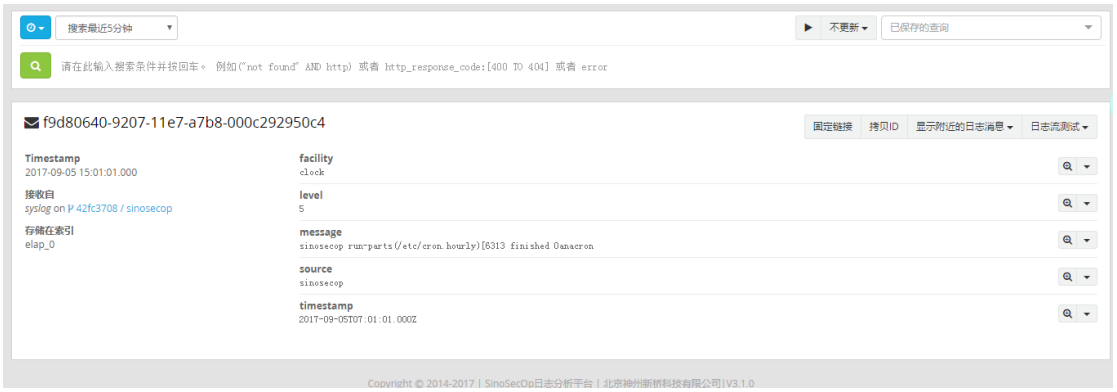
查看日志在哪些索引上被查找到：



附图70. 查看查询结果

4.4.5.2 固定链接显示日志

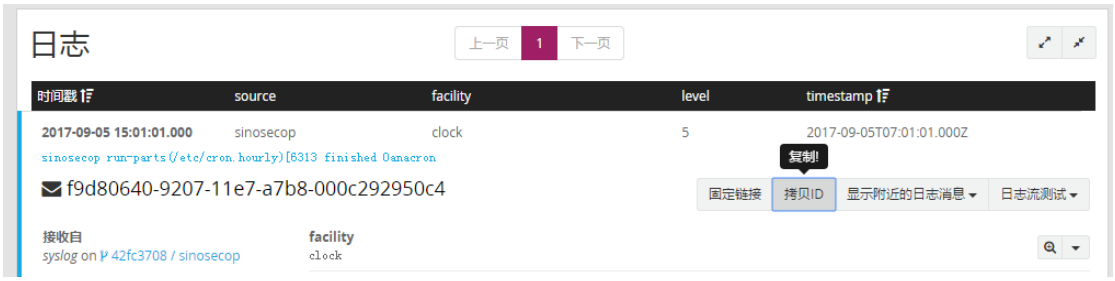
单击【固定链接】可单条显示日志



附图71. 固定链接显示日志

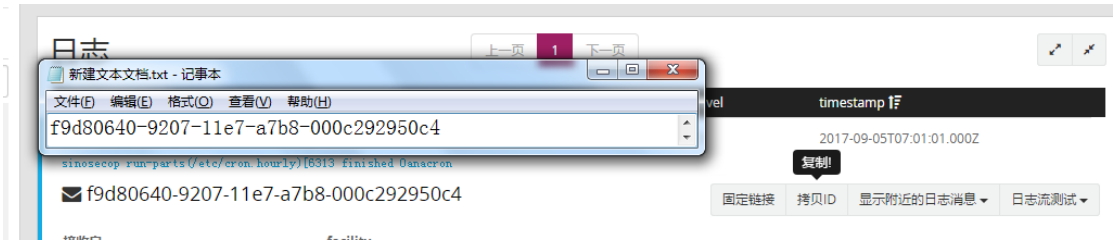
4.4.5.3 拷贝 ID

单击【拷贝 ID】，可复制 日志 ID:



附图72. 拷贝 id

复制完成后可粘贴到任意你需要的位置，您拷贝的 id 可以在再做日志解析的时候用到。

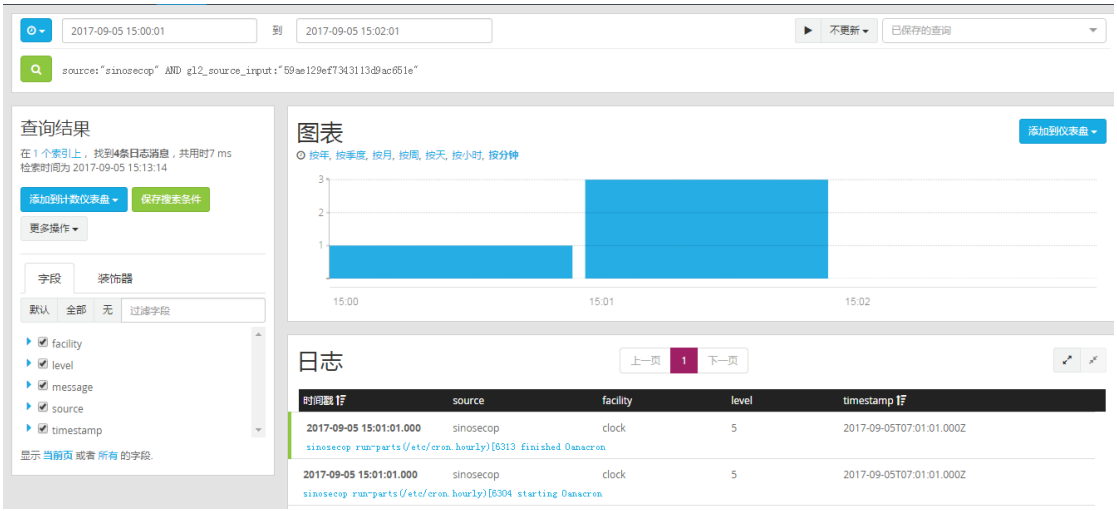


附图73. 粘贴出来的 id

4.4.5.4 显示附近的日志消息

单击【显示附近的日志消息】，可选择该条日志生成时间前后的日志：

如选择了 1 分钟，即显示该条日志前 1 分钟到后 1 分钟生成全部日志：

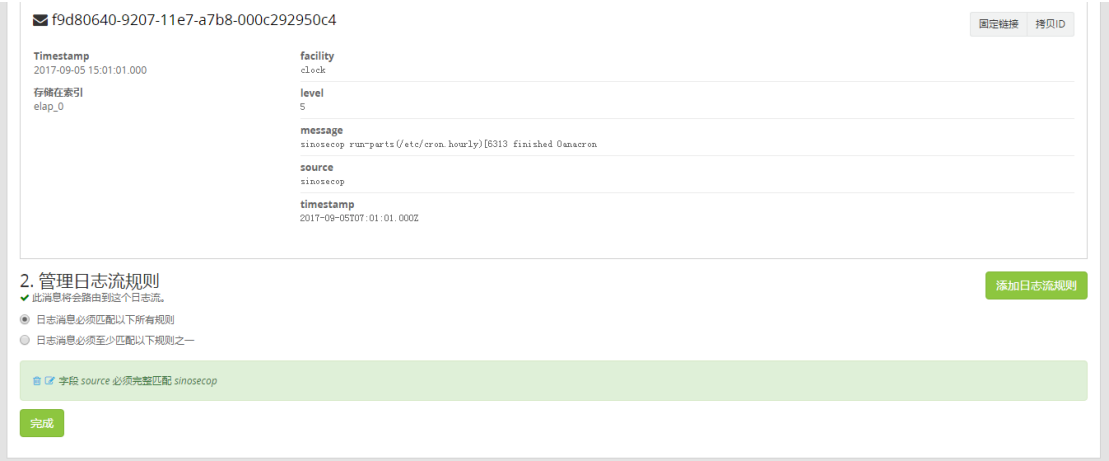


附图74. 显示附近的日志消息

4.4.5.5 日志流测试

日志流测试可测试该条日志是否可通过某条日志流规则路由到相应日志流中，从而也可以测试日志流规则是否合理：

单击【日志流测试】选择测试的日志流，可查看日志是否会路由到该日志流：



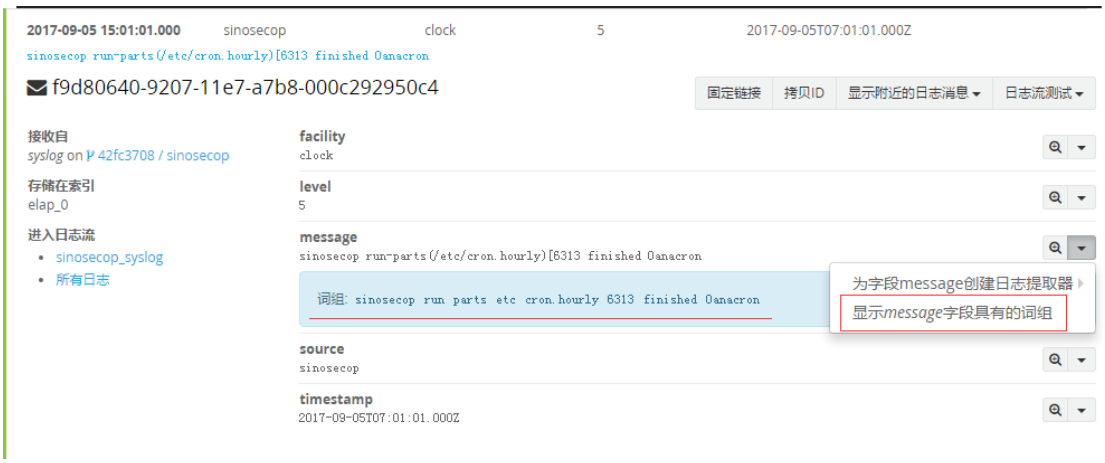
附图75. 日志流测试

4.4.5.6 为字段创建提取器

单击【为字段创建提取器】可为该字段创建提取器，创建方式可参考【管理提取器章节】。

4.4.5.7 显示字段具有的词组

单击【显示 message 字段具有的词组】，可去掉一些符号，显示该字段的所有词组：



附图76. 显示 message 字典具有的词组

4.4.6 周期刷新查询结果

如下所示可以设置日志查询结果的更新频率：

附图77. 更新结果查询

单击下拉箭头可选择更新频率或不更新。

4.4.7 保存搜索条件

单击【保存搜索条件】：

附图78. 保存搜索条件

为要保存的条件输入一个标题，以方便下次使用。

4.4.8 通过已保存的查询条件查询

消息更新频率选框右侧，可选择已保存的查询条件，进行查询：

附图79. 通过已保存的查询条件搜索

4.4.9 导出为 CSV

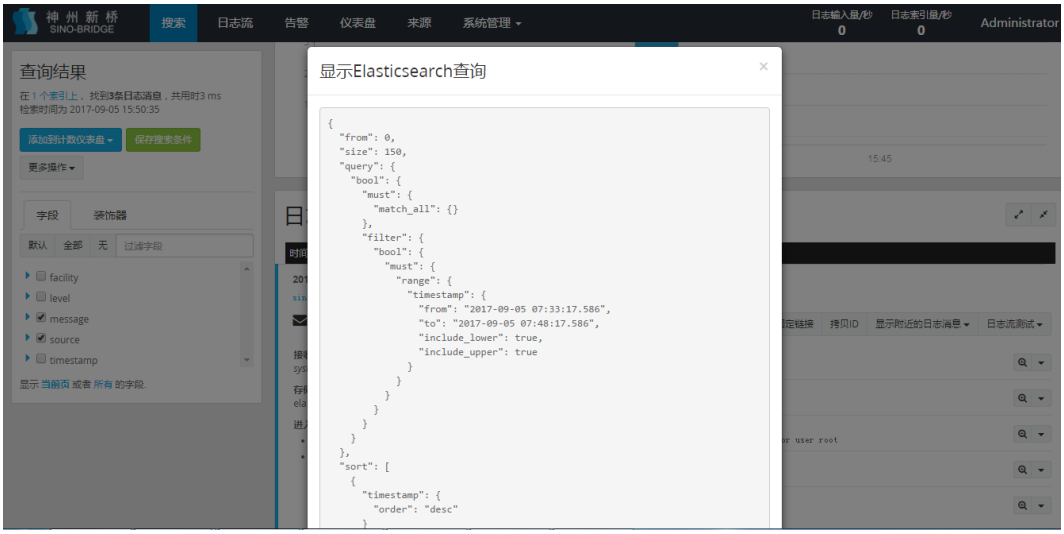
附图80. 导出为 CSV

单击【更多操作】单击【导出为 CSV】可导出当前查询的日志。

附图81. 导出文件

4.4.10 显示查询语句

单击【显示查询语句】，可显示 Elasticsearch 的查询语句：



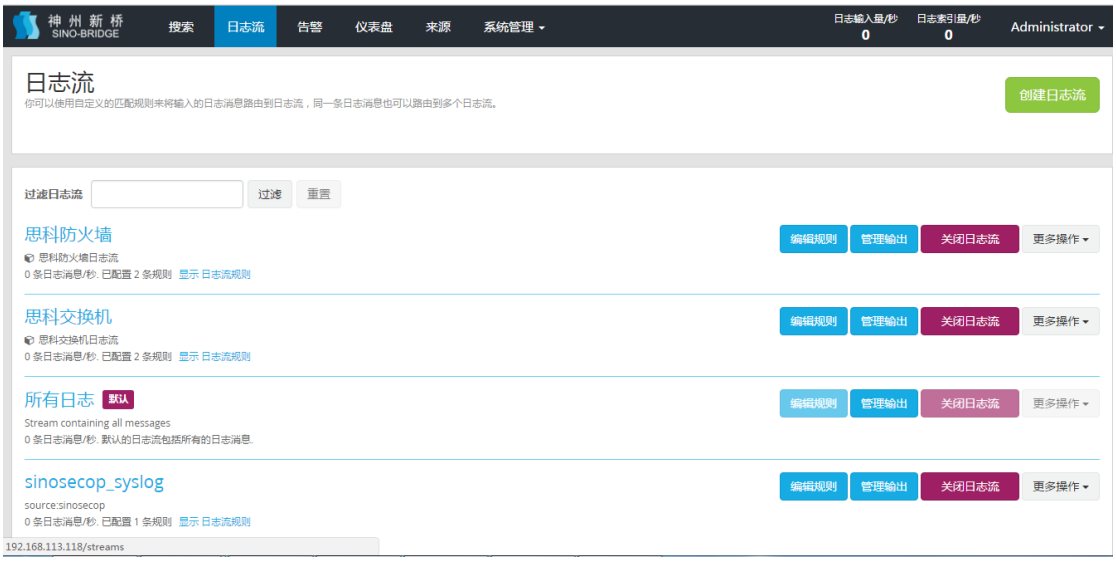
附图82. 显示查询语句

单击【复制查询】可以复制该搜索语句。

4.5 日志流

日志流可以对日志进行分流，分流后可对日志进行告警的定义，以及用户权限的

日志流是将日志消息进行分类：



附图83. 日志流页面

4.5.1 创建日志流

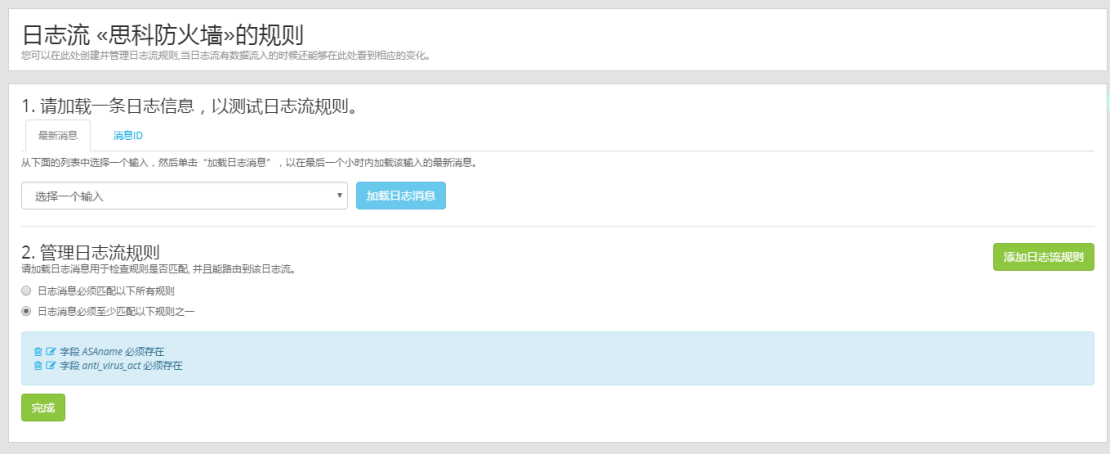
日志流页面单击【创建日志流】

附图84. 创建日志流

填写标题、描述、选择索引集，单击保存即可保存该日志流。

4.5.2 编辑规则（日志流）

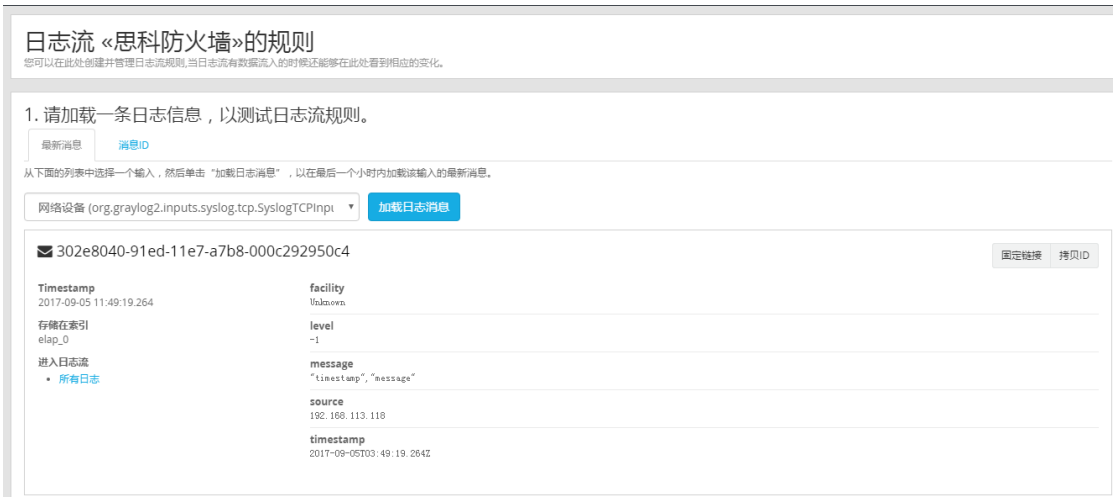
日志流页面，对单条日志留进行操作，单击编辑规则：



附图85. 编辑日志流规则

4.5.2.1 加载日志流消息

选择一个输入单击【加载日志流消息】或者输入日志消息的 ID 单击加载日志消息。



附图86. 加载日志消息

加载日志消息后可查看日志是否会路由到该日志流。

4.5.2.2 添加日志流规则

单击【添加日志流规则】

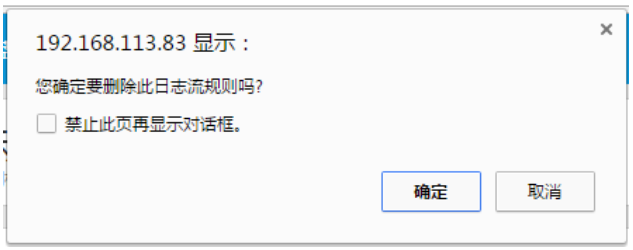
附图87. 添加日志流规则

添加日志流规则除描述选填以外，字段、类型、值均为必填。

规则反转：是将前面所定义的规则进行反转。

4.5.2.3 删除日志流规则

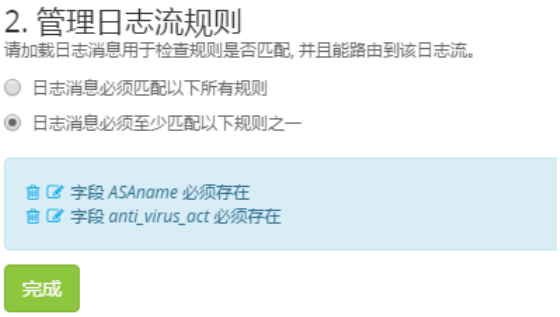
在已定义好的日志流规则前有个删除图标“  ”单击可以对该日志流规则进行删除操作：



附图88. 删除日志流规则

4.5.2.4 日志消息匹配条件

选择日志消息匹配条件，从而可对日志路由到日志流进行限制：



附图89. 管理日志流规则

4.5.3 管理输出（日志流）

单击【管理输出】，进入管理输出页面：

附图90. 管理输出

4.5.3.1 启动新的输出

选择输出类型【启动新的输出】，（注意：输出类型不同，所需填写的内容不同）：

附图91. 启动新的输出

按照提示条件输入数据，单击保存即可。

4.5.3.2 分配现有输出

如果有预定义的输出，选择输出，单击【分配现有输出】即可。

4.5.4 启停日志流

4.5.4.1 关闭日志流

附图92. 关闭日志流

日志流是启动状态，单击【关闭日志流】

附图93. 确定关闭日志流

单击【确定】即可关闭日志流。

4.5.4.2 启动日志流

附图94. 启动日志流

日志流是停止状态，单击【启动日志流】，即可启动该日志流。

4.5.5 编辑日志流

单击【更多操作】，再单击【编辑日志流】

附图95. 编辑日志流

编辑标题、描述、或变更索引集，单击【保存】即可保存该日志流，单击【取消】将取消修改。

4.5.6 快速添加规则

单击【更多操作】，再单击【快速添加规则】：

附图96. 创建日志流规则

添加日志流规则除描述选填以外，字段、类型、值均为必填。

规则反转：是将前面所定义的规则进行反转。

4.5.7 克隆此日志流

单击【更多操作】，再单击【克隆此日志流】

附图97. 克隆日志流

克隆日志流，克隆的是日志流内的规则，标题和描述需要重新定义：

4.5.8 删除此日志流

单击【更多操作】，再单击【删除日志流】

附图98. 删除日志流

单击确定即可删除，注意！删除操作不可逆，请谨慎进行。如不用该日志流，可先进行关闭。

4.6 告警与通知

附图99. 告警与通知页面

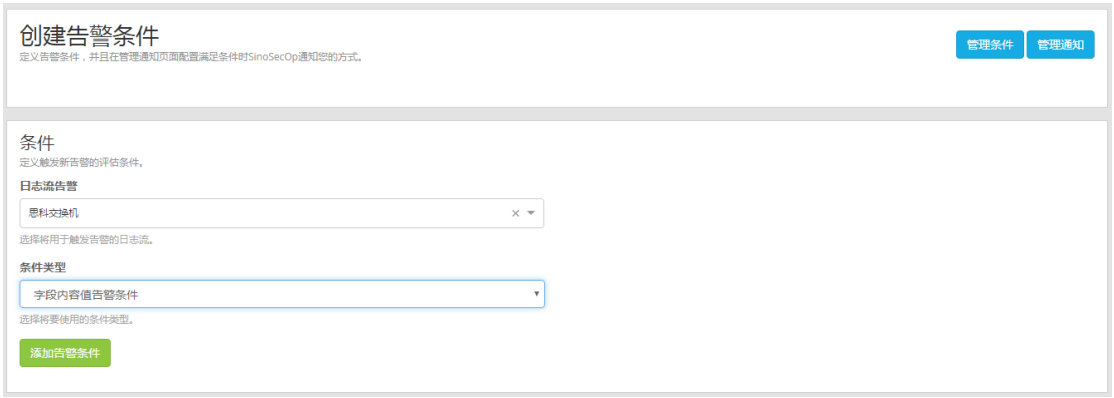
4.6.1 管理告警条件

当满足定义的告警条件时会触发告警,问题解决(状态改变)后告警状态自动变成已解决。告警分为告警条件及告警通知，告警条件可以定义触发告警的条件，告警通知作用在日志流上，当该日志流相关的告警条件被触发，将以定义告警通知是所指定的通知方式，通知给相关人员。

附图100. 告警条件页面

4.6.1.1 添加告警条件

单击【添加新的条件】，进入创建告警条件页面：



附图101. 添加告警条件

选择日志流及条件类型，单击添加告警条件：此时将为这个日志流添加告警条件。

附图102. 添加告警条件

按照提示，填写相关内容单击保存即可保存该告警条件。

4.6.1.2 编辑告警条件

单击条件的名称，即可进入告警条件详情页面：

附图103. 编辑告警条件

单击【编辑】可对告警条件进行编辑。

附图104. 编辑告警条件

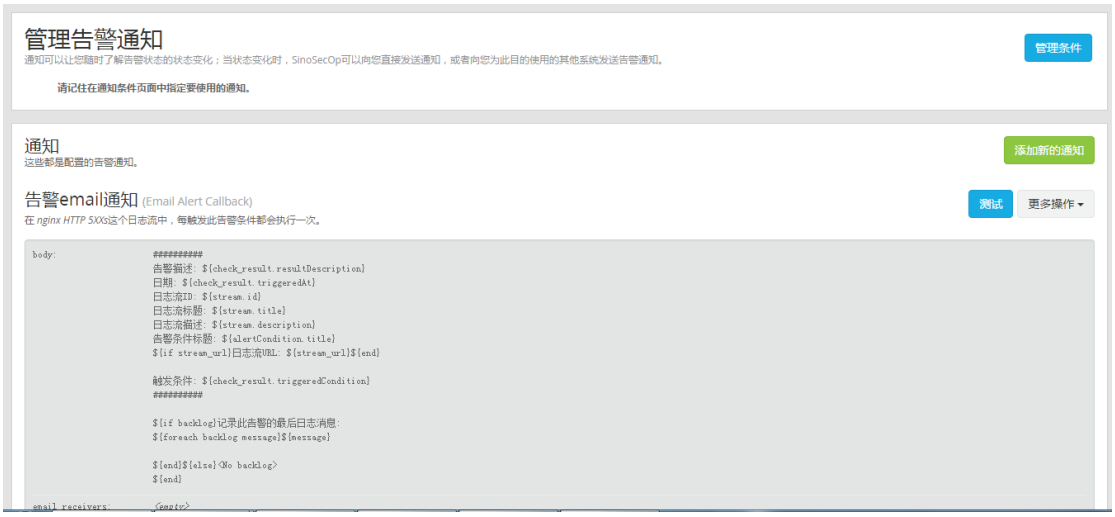
4.6.1.3 删除告警条件

附图105. 删除告警条件

管理告警条件页面，单击【操作】后单击【删除】删除告警条件。

4.6.2 管理告警通知

单击【管理通知】进入管理告警通知页面。



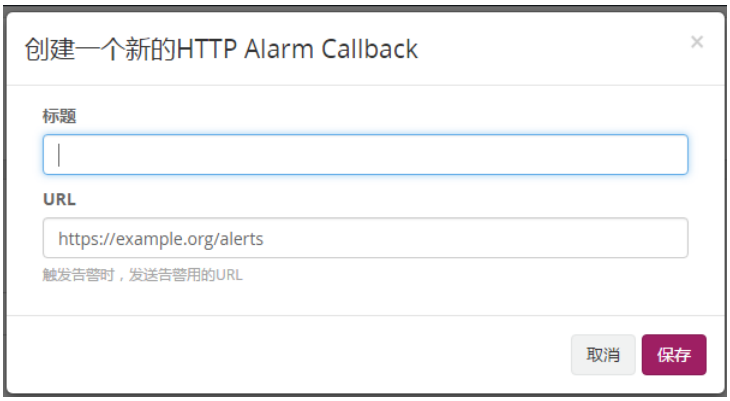
附图106. 管理告警通知页面

4.6.2.1 添加告警通知

单击【添加新的通知】，进入创建告警通知页面：

附图107. 添加告警通知

选择日志流、通知类型，单击【添加告警通知】：



附图108. 添加告警通知

输入标题单击【保存】，即可保存该通知。

4.6.2.2 测试

告警通知页面，单击【测试，可测试告警通知是否有效。

4.6.2.3 编辑告警通知

单击【更多操作】后单击【编辑】

附图109. 编辑告警通知

可对告警通知进行编辑。

4.6.2.4 删除告警通知

单击【更多操作】后单击【删除】

附图110. 删除告警通知

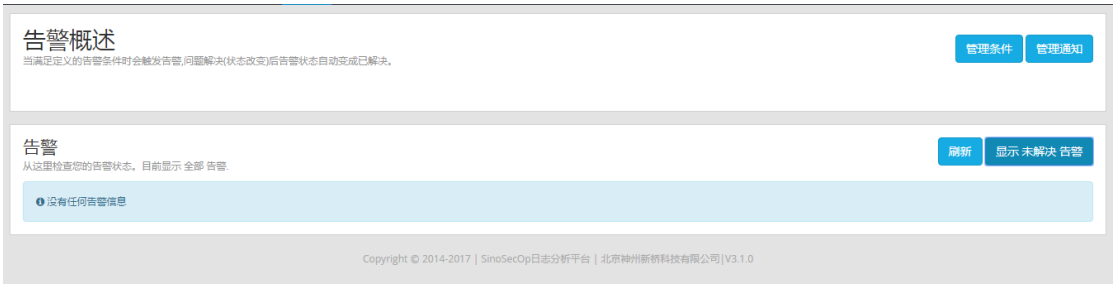
单击【确定】可删除该通知。

4.6.3 通知列表

通知列表默认显示未解决告警：

附图111. 未解决告警通知列表

单击【显示全部告警】，可显示全部告警：



附图112. 所有告警通知列表

4.7 仪表盘

使用仪表盘可以创建一个您需要的图表组；新建一个仪表盘，就可以在 SinoSecOp 的其他地方为其添加图表或数据。

附图113. 仪表盘页面

4.7.1 创建仪表盘

单击【创建仪表盘】，打开创建仪表盘窗口：

附图114. 创建仪表盘

输入所要创建的仪表盘名称和描述，单击保存可以创建一个仪表盘。

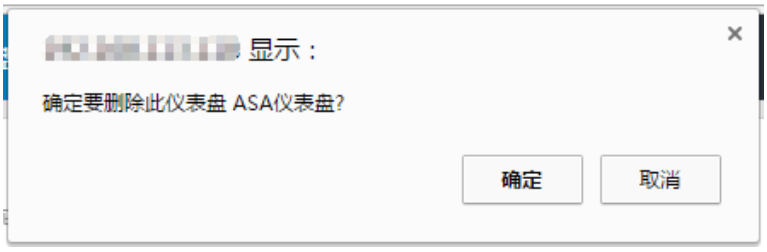
4.7.2 编辑仪表盘

单击【编辑仪表盘】可对仪表盘的名称及描述进行编辑：

附图115. 编辑仪表盘

4.7.3 删除仪表盘

单击【更多选择】后单击【删除此仪表盘】

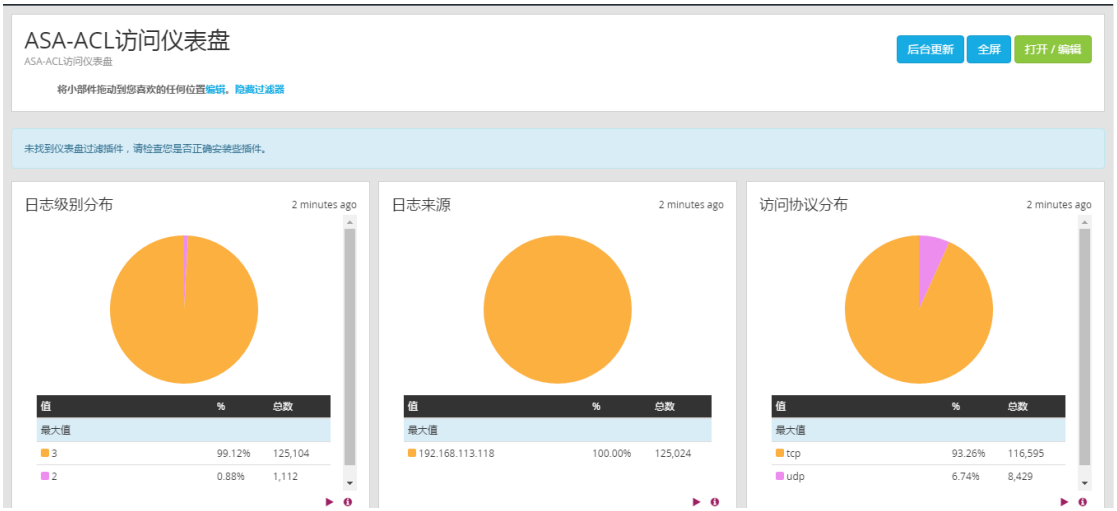


附图116. 删除仪表盘

单击【确定】即可删除该仪表盘。

4.7.4 仪表盘列表页

单击仪表盘名称，可进入仪表盘列表页：



附图117. 仪表盘列表

仪表盘内的小部件是由搜索页面添加过来的。

4.7.4.1 后台更新

单击【后台更新】将切换至后台更新，页面将不会被刷新。

4.7.4.2 全屏

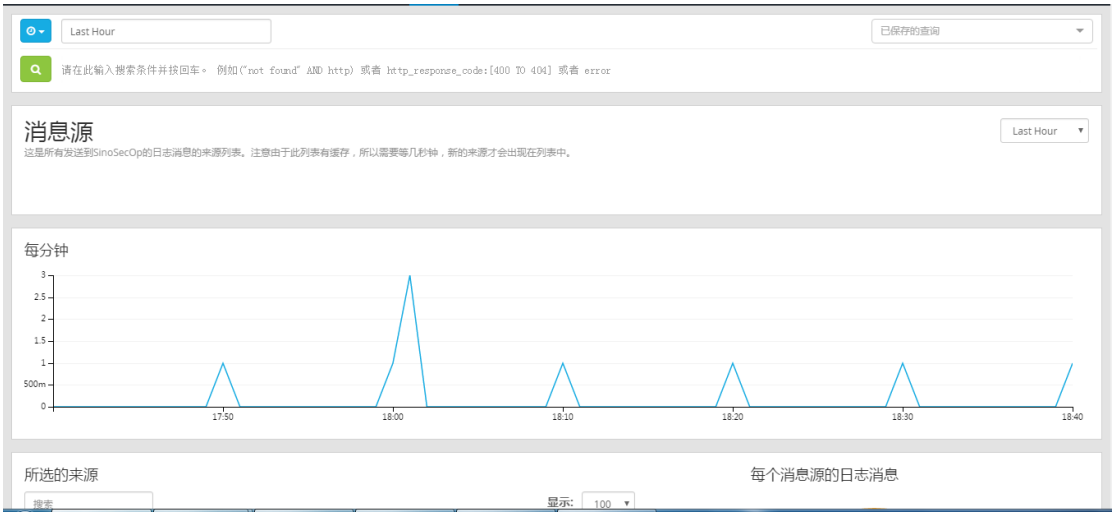
单击【全屏】，仪表盘页面将全屏显示。全屏显示时。按键盘上【esc】键将退出全屏。

4.7.4.3 打开/编辑

单击【打开/编辑】，可对各个小部件的位置及大小进行调整。也可对小部件进行编辑和删除。

4.8 来源（日志）

这是所有发送到 SinoSecOp 的日志消息的来源列表。

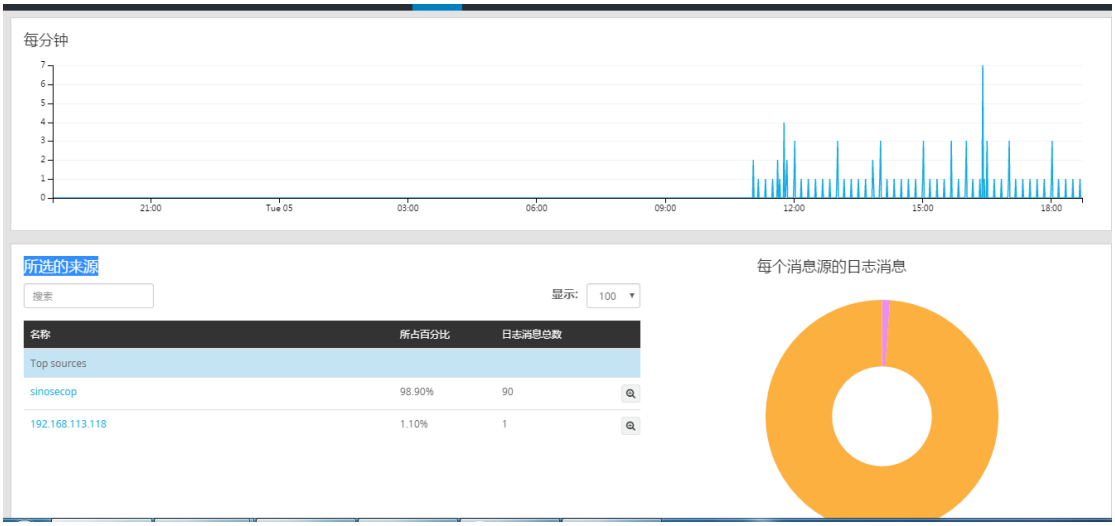


附图118. 来源页面

4.8.1 按时间统计消息的来源

附图119. 按时间统计来源

选择时间段，可以显示该时间段内的消息数量及消息来源



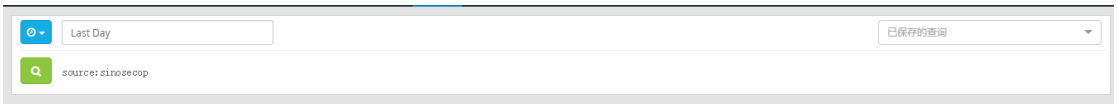
附图120. 所选的来源

4.8.2 按照日志来源查询日志

单击所选来源模块的查询按钮：

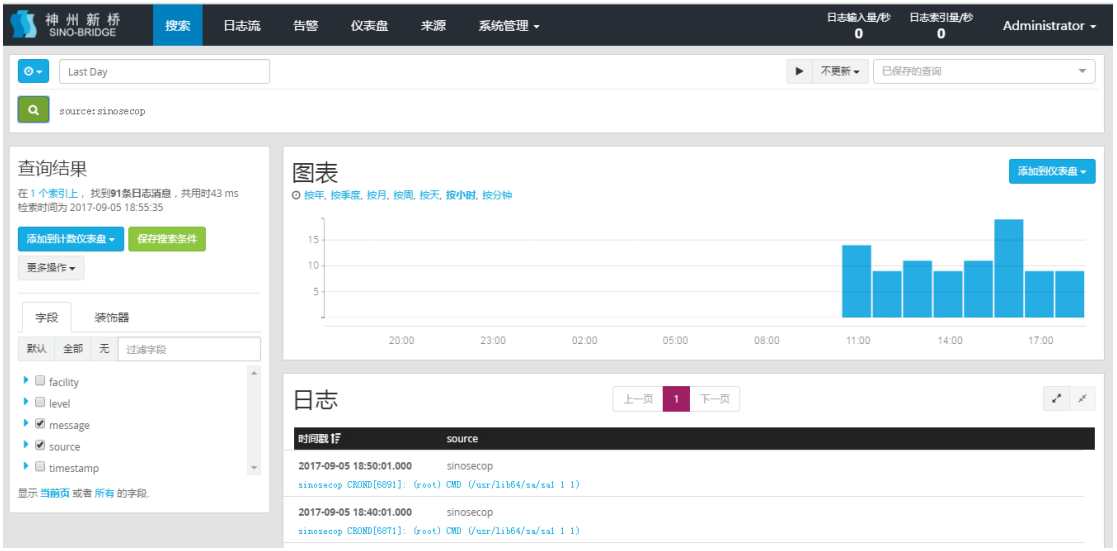
附图121. 添加到搜索条件

可添加至搜索条件：



附图122. 添加到了搜索条件

单击查询按钮，看产看该来源下的所有日志：



附图123. 查看日志消息

4.9 系统管理

4.9.1 概览

概览页面可以看到系统的状态：包括通知、系统任务、SinoSecOp 集群、ElasticSearch 集群的状态，以及失败的索引，各组件的时间信息。

附图124. 概览

4.9.1.1 通知

SinoSecOp 会发出通知，方便处理一般性的问题。

4.9.1.2 系统任务

系统任务是 SinoSecOp 节点基于某些原因而运行的一个长期任务，部分任务提供了进度信息并可以被停止。并指明有没有活动的系统任务。

4.9.1.3 SinoSecOp 集群

指出 SinoSecOp 集群的集群 ID 与节点数。

4.9.1.4 Elasticsearch 集群

指出 Elasticsearch 的集群状态与分区数。

4.9.2 配置

配置页面可以设置搜索配置、消息处理顺序等。

附图125. 配置

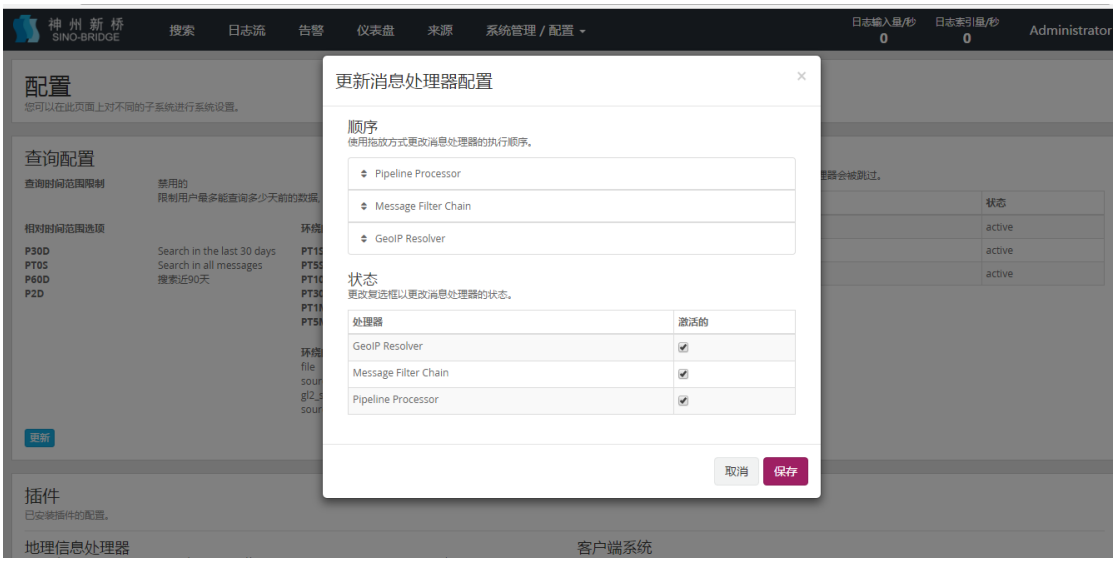
4.9.2.1 查询配置

搜索配置：单击搜索配置下的更新可对搜索项进项配置。

附图126. 查询配置

4.9.2.2 消息处理器配置

单击消息处理程序配置下的更新，可配置消息处理器的顺序，但一般不要动默认的顺序。



附图127. 更新消息处理器配置

4.9.2.3 插件

单击插件下的更新，可选择是否启用地理信息处理器，可也查看数据库文件的路径。

附图128. 更新地理信息处理器配置

4.9.3 节点

此页面提供 SinoSecOp 集群节点的实时概况，您可以随时【暂停消息处理】。在恢复处理之前，处理缓冲区将不会接收任何新的日志消息。

附图129. 节点

4.9.3.1 详细信息（节点）

单击详细信息可以看到该节点的信息：

附图130. 节点详细信息

该页面下【内存/堆 usage】显示出了 JVM 目前已占用堆空间大小，及堆空间所有占用的最大内存。【缓冲区】显示了缓冲区在短时间缓存日志消息的情况。【磁盘日志】显示了磁盘日志的配置路径，最早的条目，最大长度，最大周期，刷新的规则，以及使用的情况等。

4.9.4 输入

SinoSecOp 支持 Beats、ELF AMQP、ELF HTTP、ELF Kafka、ELF TCP、ELF UDP、

JSON path from HTTP API、Random HTTP message generator、Raw/Plaintext AMQP、Raw/Plaintext Kafka、Raw/Plaintext TCP、Raw/Plaintext UDP、SNMP UDP、Syslog AMQP、Syslog Kafka、Syslog TCP 、Syslog UDP。

4.9.4.1 启动新的输入

选择【系统管理】【输入】，在选择一个输入的下拉框中确定你所想要输入的类型，如 Syslog UDP, 最后单击【启动新的输入】

附图131. 启动新的输入

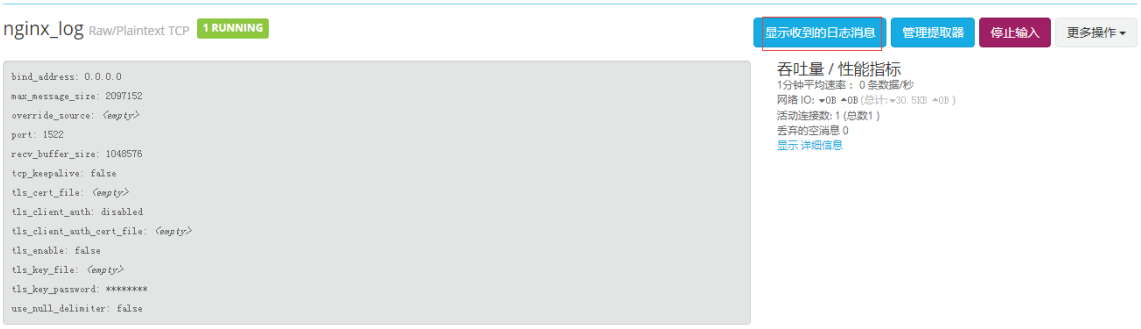
【启动新的输入】之后，会弹出相关需要填写的信息：

附图132. 启动新的输入

填写需要启用的节点、侦听地址和端口，也可以选择全局启用。

4.9.4.2 显示收到的消息

在【输入】页面下单击【显示收到的日志消息】



附图133. 显示收到的消息

即可跳转到该输入对应接收到的日志：

附图134. 跳转到日志

4.9.4.3 管理提取器

日志提取器将会作用在这个输入的每一条日志消息上。使用提取器，可以将文本数据转换成字段，便于稍后过滤和分析。例如：从日志消息中抽取 HTTP 返回码，将其转换成数字字段 http_response_code，并附加到日志消息上。

在【输入】页面下单击【管理提取器】

附图135. 管理提取器

常用的操作是：加载一个消息样例，可以从输入加载最新的日志消息，也可以通过消息 ID 手动选择日志消息。

4.9.4.4 停止输入

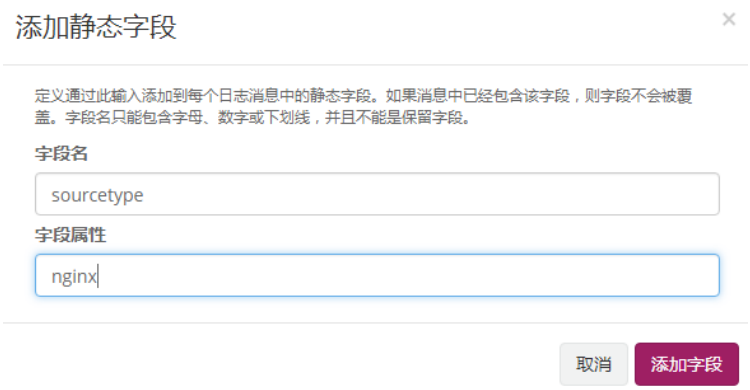
在【输入】页面下单击【停止输入】，即可停止该日志的输入。

4.9.4.5 编辑输入

在【输入】页面下单击【更多操作】，可对建立的输入进行两次编辑，详见【5.3.1.1】

4.9.4.6 添加静态字段

在【输入】页面下单击【更多操作】，选择【添加静态字段】，这一操作主要是为了配置日志分流的，定义通过此输入添加到每个日志消息中的静态字段。如果消息中已经包含该字段，则字段不会被覆盖。字段名只能包含字母、数字或下划线，并且不能是保留字段。



附图136. 添加静态字段

在输入时填加完静态字段后，我们就可以在创建日志分流编辑分流规则时，依据此静态字段而对日志进行分流处理：

附图137. 编辑日志流规则

4.9.4.7 删除输入

在【输入】页面下单击【更多操作】，选择【删除输入】，即可删除所创建的输入。

4.9.5 输出

SinoSecOp 节点可以将日志消息输出到指定的位置。您可以在这里启动或终止您想要的输出，然后将其分配给日志流，以实时转发日志流中的所有消息。在【系统管理】【输出】启动新的输出时，可以选择 STDOUT Output 或 ELF Output。

4.9.5.1 启动新输出

【系统管理】【输出】【启动新的输出】，编辑您想要输出的标题。

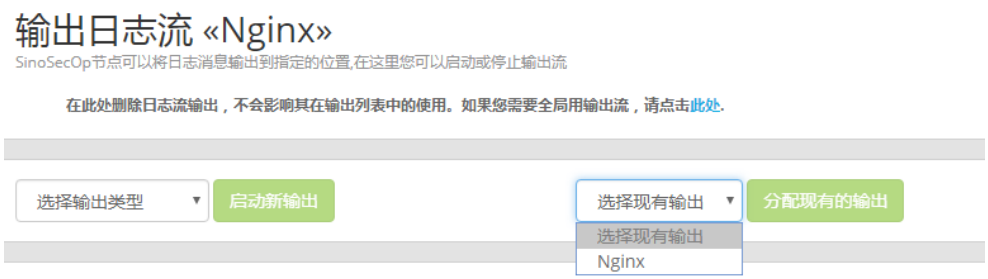
附图138. 启动新的输出

4.9.5.2 编辑（输出）

在【启动新的输出】页面下，单击【编辑】，即可编辑新的输出。如编辑可选字段前缀

附图139. 编辑新的输出

在所创建的日志流上，单击【管理输出】，可以选择【启动新的输出】，也可以选择【分配现有的输出】，如刚创建的 Nginx 输出。



附图140. 分配现有输出

4.9.5.3 全局删除（输出）

在【启动新的输出】页面下，单击【全局删除】，即可删除新的输出。

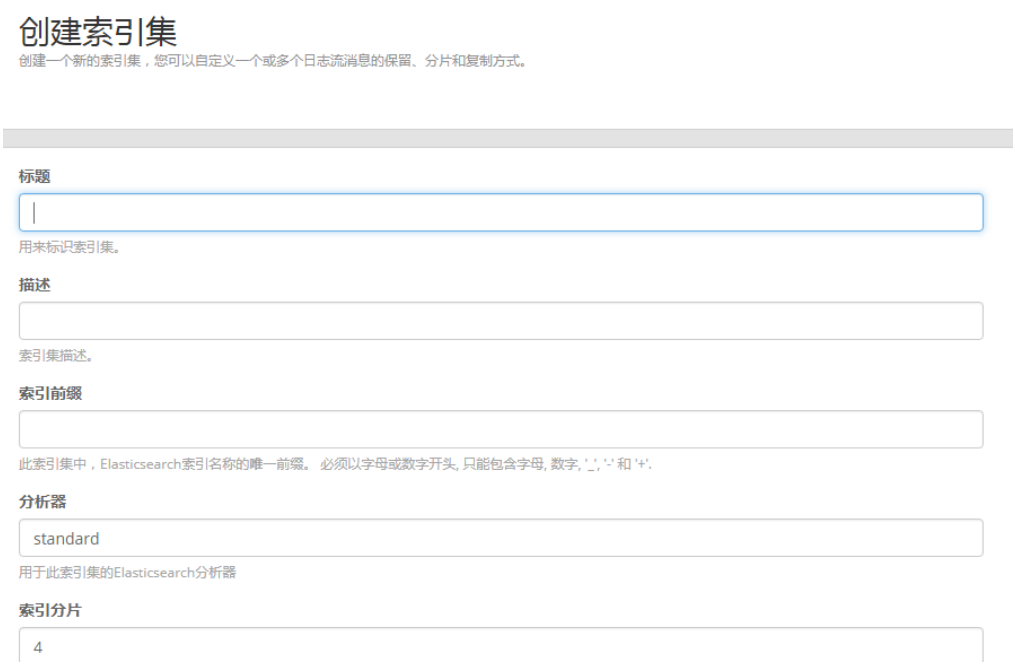
4.9.5.4 输出支持列表

4.9.6 索引

日志流将消息写入索引集，索引集用于保留、分片和复制存储的数据。通过配置索引集，可以给特定的日志流设置不同的数据保留时间。一般情况下，我们使用默认的索引集即可。

4.9.6.1 创建索引集

【系统管理】【索引】【创建索引集】即可创建索引集



附图141. 创建索引集

4.9.6.2 编辑（索引）

在【索引】页面下，找到所创建的索引，单击【更多选项】，选择【编辑】，即可编辑相应的索引。

4.9.6.3 删除（索引）

在【索引】页面下，找到所创建的索引，单击【更多选项】，选择【删除】，即可删除相应的索引。

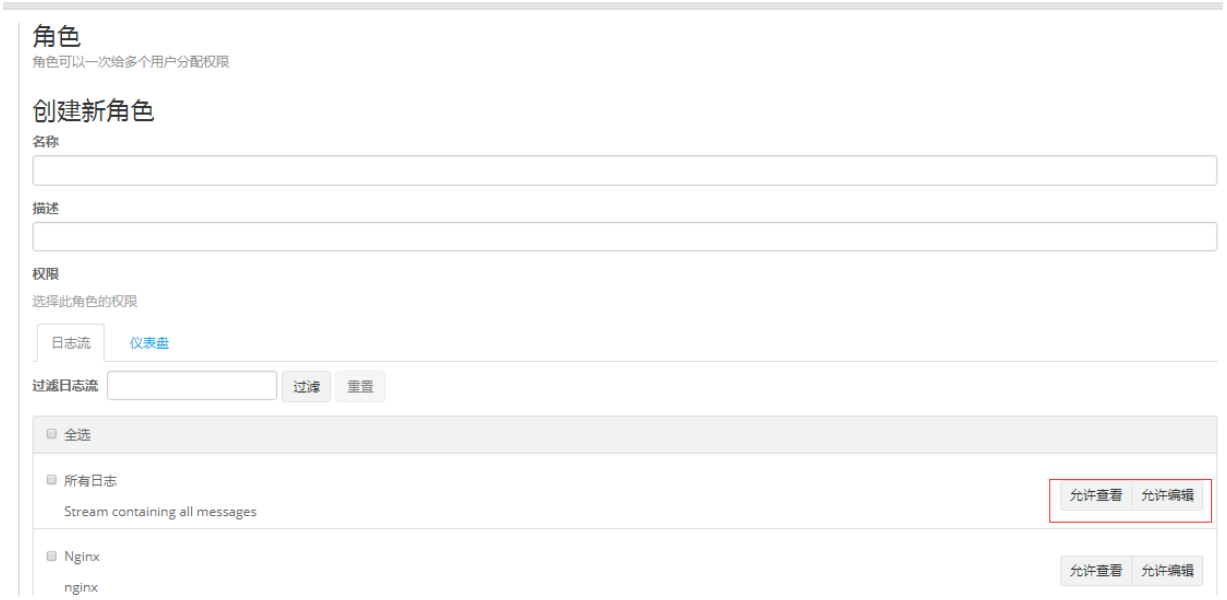
4.9.7 认证

【系统管理】【认证】，认证的管理，主要是配置 SinoSecOp 的身份验证提供程序并管理此 SinoSecOp 集群的活动用户。如【添加新用户】

附图142. 用户管理页面

4.9.7.1 角色管理

角色可以一次给多个用户分配权限，如内建的 Admin（授予用户所有管理权限），内建的 Reader（授予用户基本查询权限），可【添加新角色】，选择其所对应的权限，注意，命名角色时，至少要有一个权限才能保存。



附图143. 角色管理页面

4.9.7.2 用户管理

【添加新用户】使用此页面创建新的用户。这里创建的用户及权限不仅适用于 Web 界面，也适用于服务器节点的 REST API。

附图144. 创建新的用户

如上图，在创建用户时，可在角色一栏可添加或减少角色，使创建的新用户拥有不同的权限。角色与用户的关系是：角色是用来定义用户的权限的。

4.9.8 扩展包

扩展包加速了特定数据源的设置过程。扩展包可以包括输入/提取器，流和仪表盘。譬如您已经在一个节点上设置好了输入，输出，日志流，提出器等，想要把这些平移到另一个节点，此时，不必再重新设一遍，扩展包就可以帮忙，把需要平移的在复选框中选择就行，最后下载扩展包，上传到另一个节点，再应用就行了。

4.9.8.1 创建一个新的扩展包

【系统管理】【扩展包】【创建一个新的扩展包】即可创建一个新的扩展包，填写扩展包名称等，选择您所需要的选项，最后下载扩展包即可，扩展包是一个.json 的文件。

附图145. 创建扩展包

4.9.8.2 导入扩展包

在【扩展包】页面下选择【导入扩展包】，选择之前下载好的扩展包，单击上传。

附图146. 导入扩展包

4.9.8.3 应用扩展包

在【扩展包】页面下，选择您所上传的扩展包，然后单击【应用扩展包】

附图147. 应用扩展包

4.9.8.4 删除扩展包

在【扩展包】页面下，选择您所上传的扩展包，然后单击【删除扩展包】

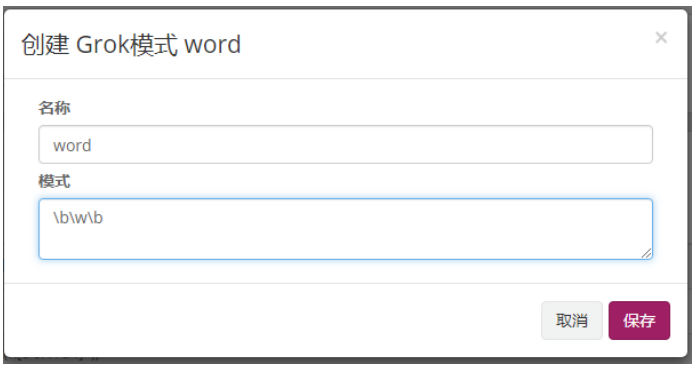
附图148. 删除扩展包

4.9.9 Gork 模式

【系统管理】【Grok 模式】这是在日志提取器中可用的 Grok 模式列表。 您可以手动添加 Grok 模式，也可以通过导入模式文件，添加一组 Grok 模式。此页面下可以看到已经有好些默认的 Grok 模式了。

4.9.9.1 创建模式

在【Grok 模式】页面下，单击【创建模式】



附图149. 创建 Grok 模式

在【名称】下面自定义一个名子，如'word'，在【模式】下面写上您所要匹配的正则表达式即可，最后【保存】，注意不能与现有的模式名称重名，否则无法创建。

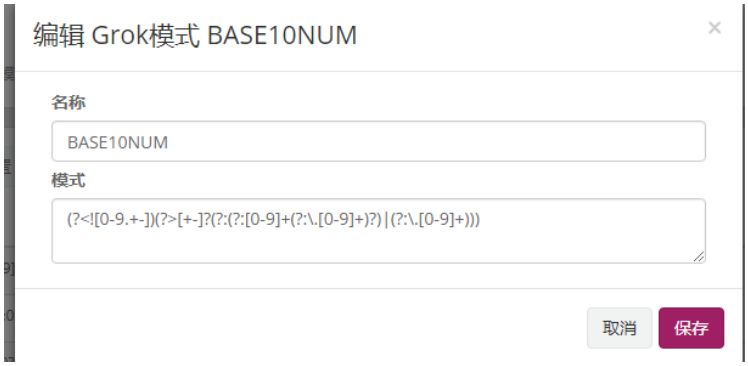
4.9.9.2 导入模式文件

在【Grok 模式】页面下，单击【导入模式文件】，选择模式文件，并注意是否要替换现在模式，最后上传即可。

附图150. 导入 Grok 模式

4.9.9.3 编辑（Gork 模式）

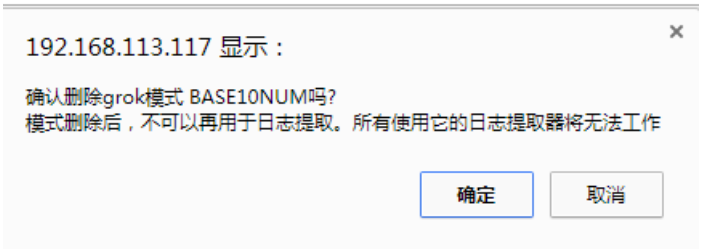
在【Grok 模式】下，选择一个模式，单击【编辑】按钮即可



附图151. 编辑 Grok 模式

4.9.9.4 删除（Gork 模式）

在【Grok 模式】下，选择一个模式，单击【删除】按钮，根据提示选择是否要删除。

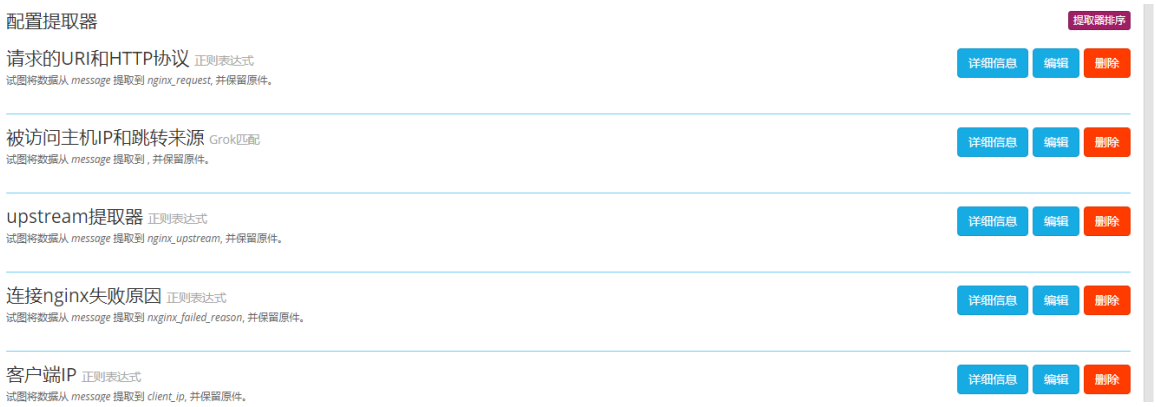


附图152. 删除 Grok 模式

5 专题：日志提取器

5.1 日志提取器的管理

通常情况下，可能过如下方式管理提取器：【系统管理】【输入】选择要管理的输入，然后单击【管理提取器】



附图153. 日志提取器页面

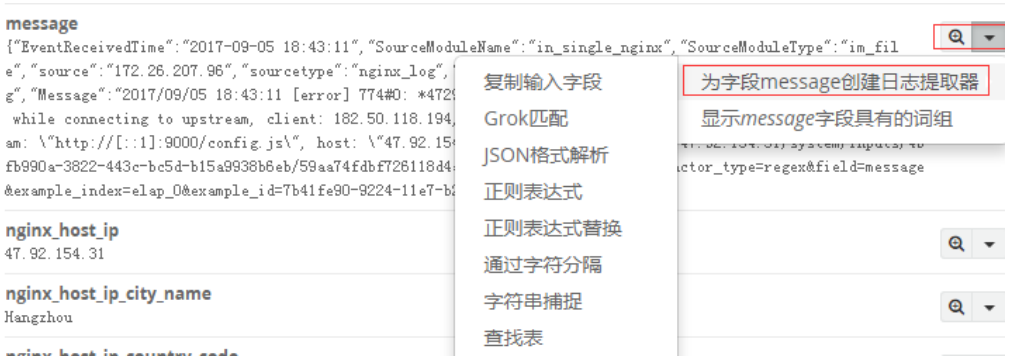
此界面下可对提取器进行拖动排序，单击【提取器排序】即可。

附图154. 提取器排序

【详细信息】【编辑】【删除】就直接操作吧。

5.2 写一条完整的提取器

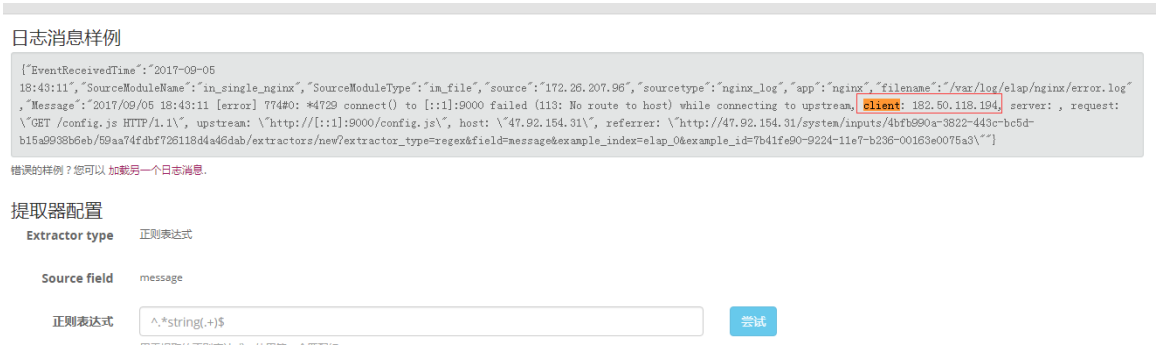
当接入完日志后，在【搜索】页面下，会显示出已经接入的日志信息，我们单击其中一条日志，为这条日志创建提取器，创建提取器时，主要是选择 Grok 匹配、正则表达式、JSON 格式解析等。



附图155. 创建提取器

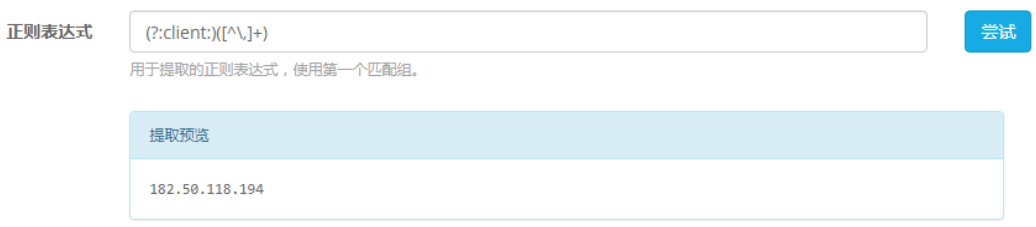
5.2.1 基于正则表达式的提取器

我们此处选择正则表达式，比如我们要提取一下 nginx 日志的客户端 ip 这一字段



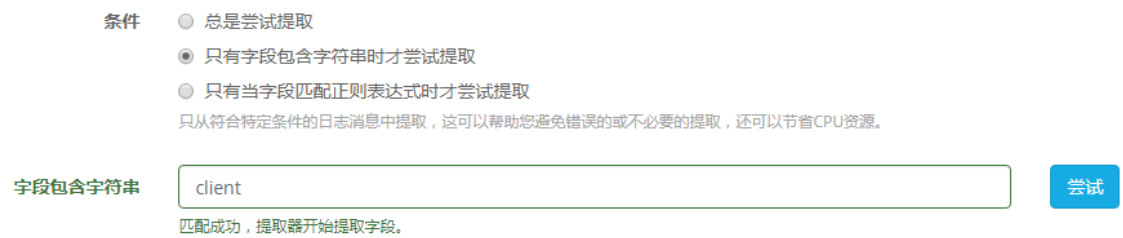
附图156. 正则提取器

在正则表达式输入框中写入正确的正则，单击【尝试】



附图157. 尝试提取结果

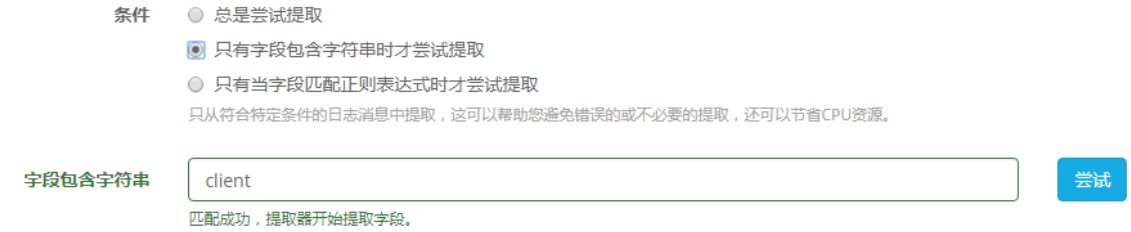
还可以选择适当的条件进一步匹配



附图158. 设置比配条件

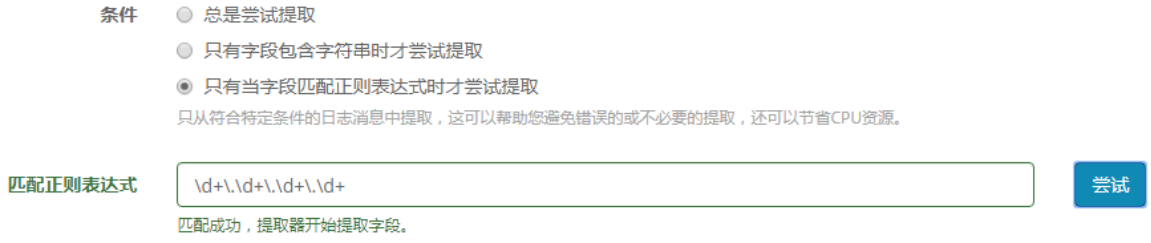
【总是尝试提取】即意味着每条日志都会被此提取器去尝试提取，只从符合特定条件的日志消息中提取，这可以帮助您避免错误的或不必要的提取，还可以节省 CPU 资源。

【只有字段包含字符串时才尝试提取】即选择一个日志消息中的关键词，输入【字段包含字符串】一栏，单击【尝试】，当匹配成功时，可避免不必要的提取，这是一个比较精确的做法。



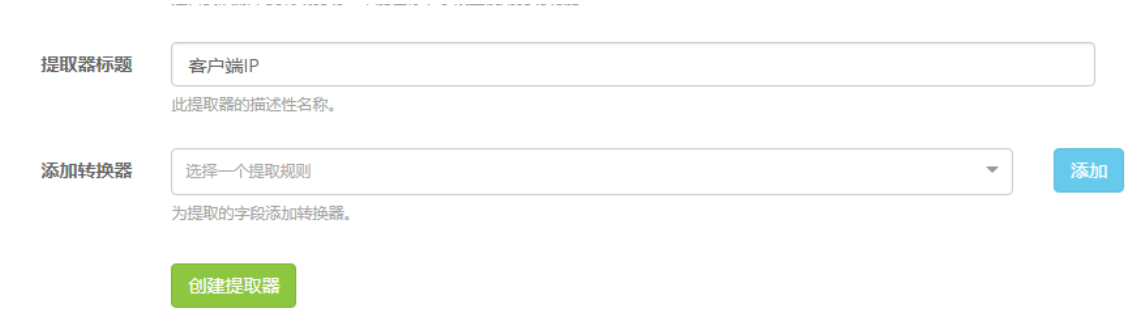
附图159. 设置比配条件

【只有当字段匹配正则表达式时才尝试提取】即选择日志中的某个词，用正则表示出来。



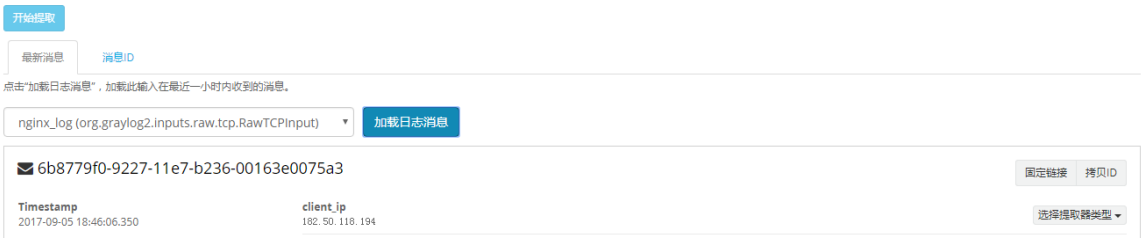
附图160. 设置比配条件

最后，写上提取器名称，单击【创建提取器】



附图161. 创建提取器

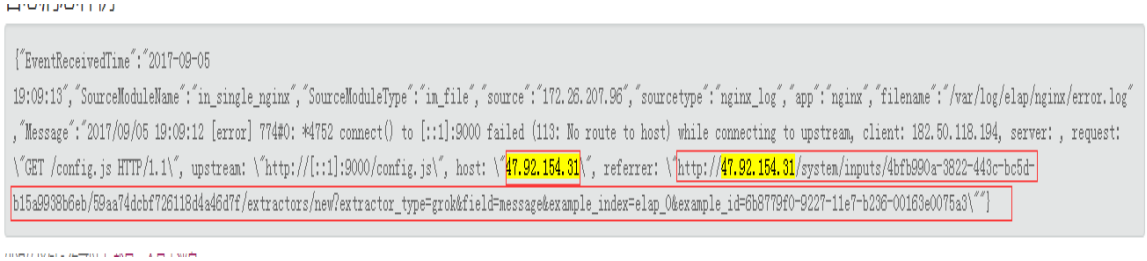
验证：【输入】【管理提取器】【开始提取】【加载日志消息】，如果能正确地提取出我们所定义的字段，则说明这个提取器是没问题的。



附图162. 测试提取器

5.2.2 基于 Grok 模式的提取器

譬如下面一条日志，我们要以 Grok 模式的方式提取出被访问的主机 IP 和整个 Referrer.



附图163. 日志

看看 Grok 是怎么写的：

附图164. Grok 提取

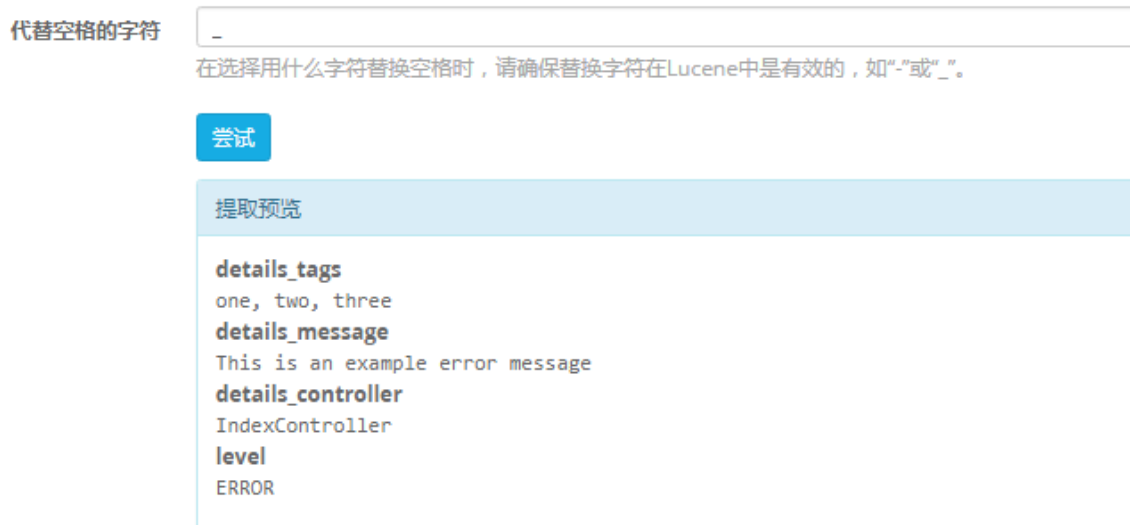
5.2.3 基于 JSON 的提取器

一般情况下，基于 JSON 的提取器只需要填写对应的分隔符即可尝试提取，如下面的条 json 格式的日志

填写分隔符：

附图165. Json 提取

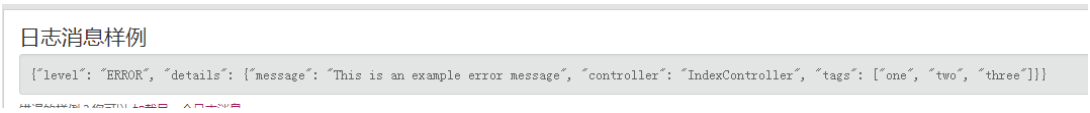
尝试提取：



附图166. Json 提取

5.2.4 基于字符串分割的提取器

字符器分割的提取器比较简单，只需根据日志消息中的特定字符作为分割字符即可，其中目标索引指的是第几个这样的分割符对应的字段。如下面这条消息：



附图167. 消息样例

我们将 “, 作为一个分隔符，尝试：

附图168. 字符串分隔提取

5.2.5 基于字符串捕捉的提取器

字符串捕捉，即一个字符代表了一个位置，我们只需字符输入所在的“开始位置”与“结束位置”即可，例如：

附图169. 字符串捕捉

5.3 时间格式化

时间格式化有时也称时间对齐，目的是解决 timestamp 的时间与日志产生时间不一致问题，如有以下时间格式：

yyyy:年	例：2017（yy 则表示年份后两位）
MM:月	例：08
DD/dd:日	例：30
HH:时	例：17
mm:分	例：30
ss:秒	例：50
SSS:毫秒	例：563

事例：

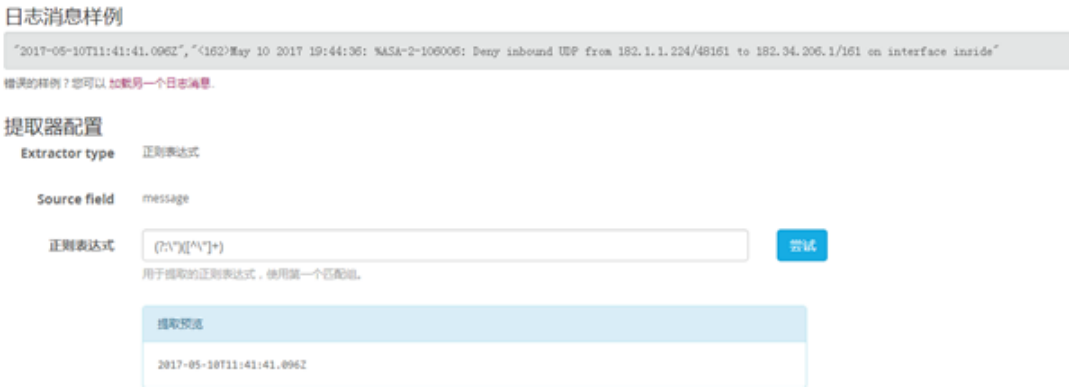
2017-08-30 17:30:50.563 可以表示为 yyyy-MM-dd HH:mm:ss.SSS May 10 2017 19:44:36　可以表示为 MMM dd yyyy HH:mm:ss 2017-05-10T11:44:56.746Z　可以表示为 yyyy-MM-dd’T’HH:mm:ss.SSS’Z’

具体步骤：

1. 提取字段：

附图170. 提取字段

2. 填写正则表达式提取出来时间：



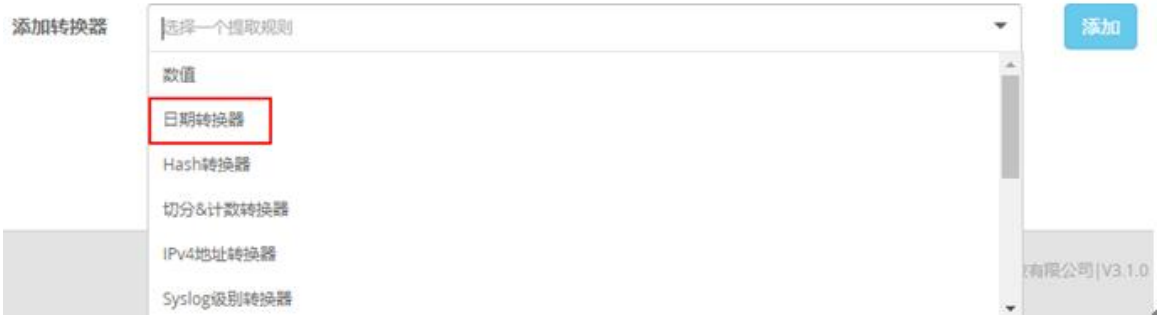
附图171. 设置时间格式

3. 填写存储字段名称为 timestamp 和提取器标题

附图172. 储存提取器标题

4. 添加转化器

若时间格式为“yyyy-MM-dd HH:mm:ss.SSS”，添加转化器时选择日期转换器：



附图173. 添加转换器

填写时间格式和时区：

附图174. 填写格式和时区

若时间格式为“yyyy-MM-dd’T’HH:mm:ss.SSS’Z’”，添加转换器选择复杂日期转换：

附图175. 复杂日期转换器

填写时区：

附图176. 填写时区

创建提取器，更新日志后 timestamp 字段值自动更新。

6 图表目录

附图目录

表格目录