ElasticSearch在BBD运维中的运用

BBD 运营平台 运维部

2019年9月22日

目录

- ElasticSearch在BBD的使用情况
- ElasticSearch在安全方面的应用
- 运维的痛点及解决办法
- 开源计划

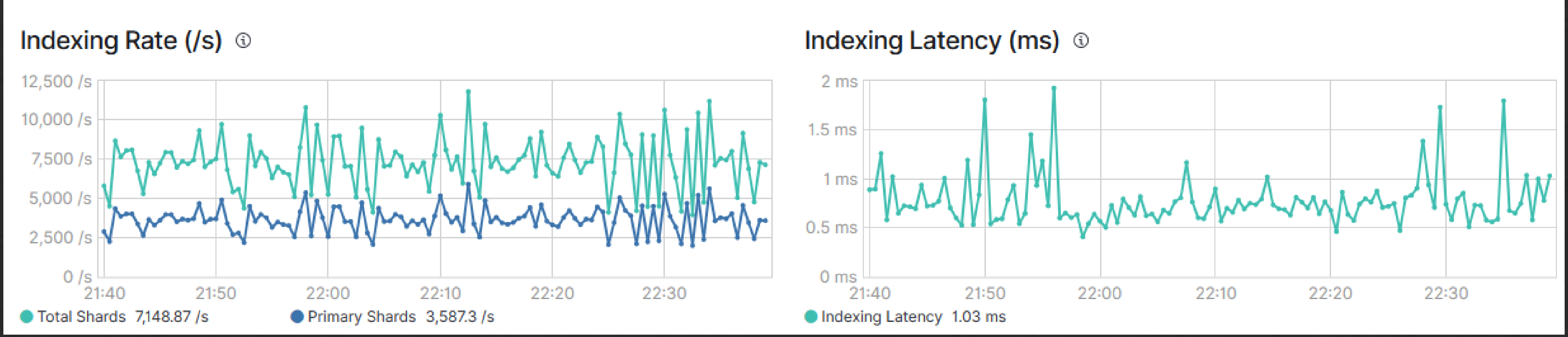
BBD ElasticSearch使用概况

- 集群数目：20+
- 数据节点：100+
- 数据量：50TB+
- 文档数：100亿+

版本绝大部分7.3，逐渐替换为7.3+

- JDK 8
- 大部分采用普通机械盘，少量采用SSD

写多读少，集群多，数据量大

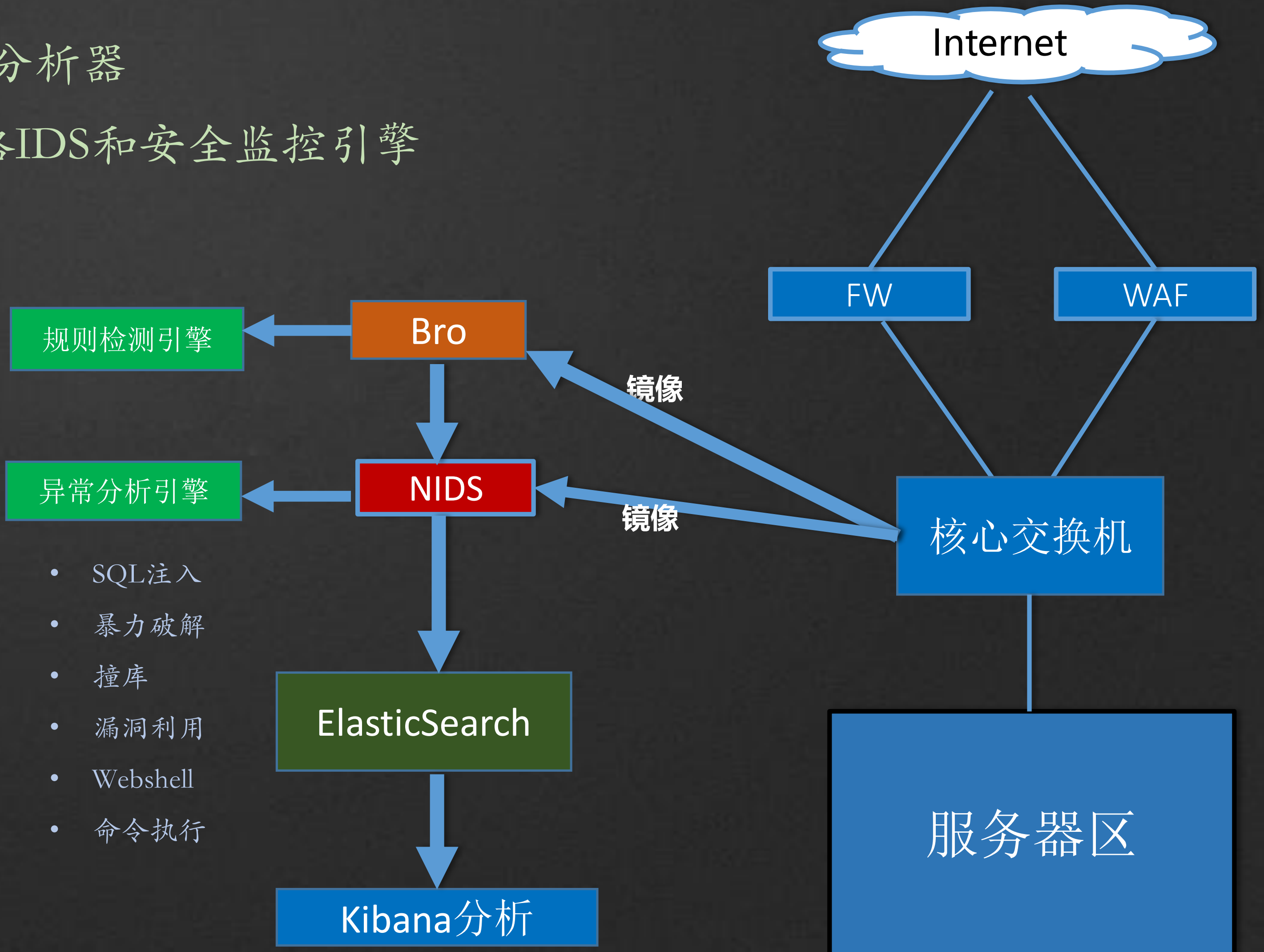


在安全方面的一些应用

流量分析与网络入侵检测

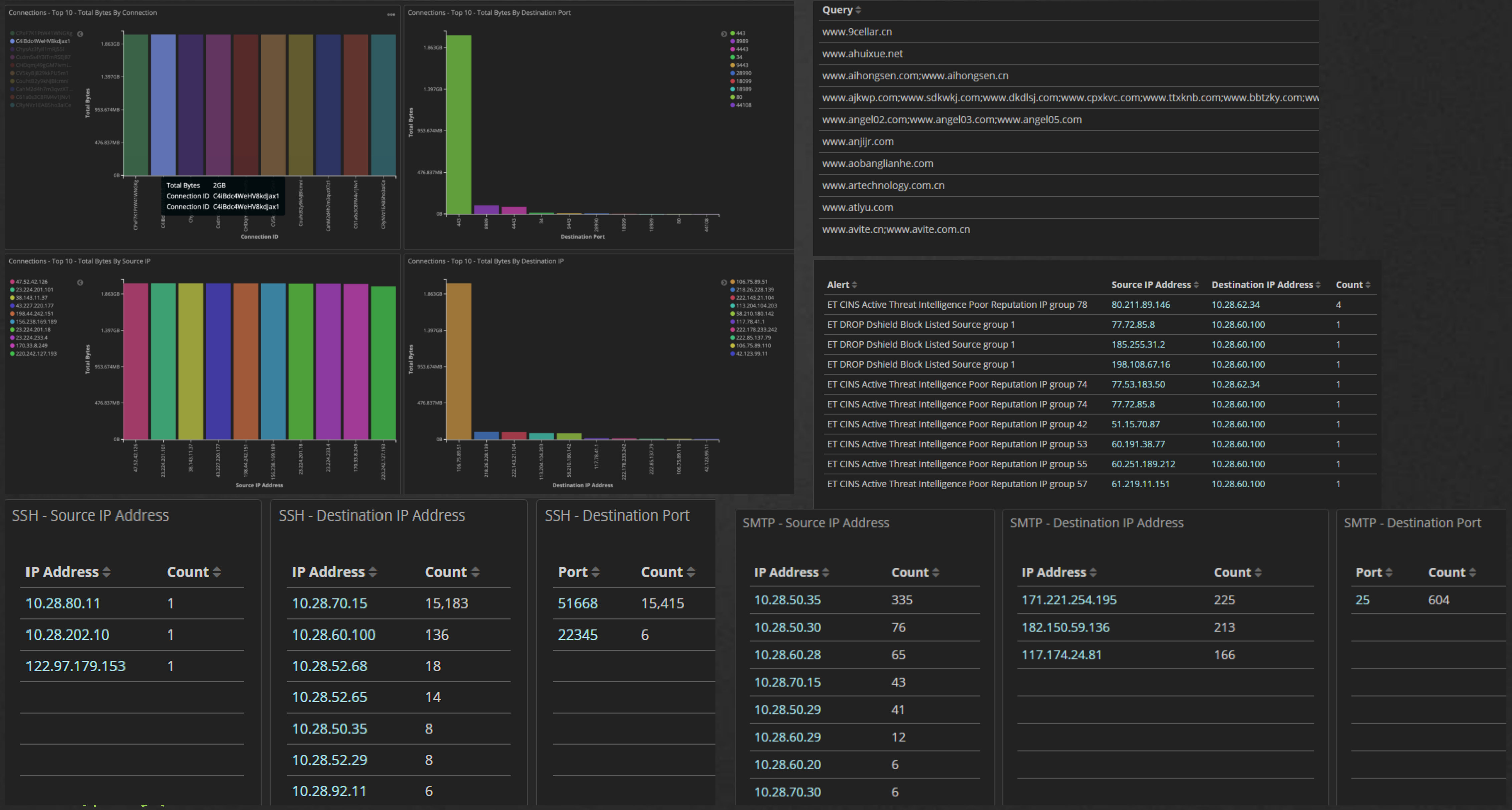
- Bro是一款被动的开源流量分析器
- Suricata是一款高性能的网络IDS和安全监控引擎

- 利用流量分析，全面感知网络情况；
- 全流量数据库可用于被动发现安全漏洞的数据源，如敏感数据未加密、不安全传输等
- 网络入侵检测，从流量最底层快速发现安全威胁和可疑安全事件



- SQL注入
- 暴力破解
- 撞库
- 漏洞利用
- Webshell
- 命令执行

流量分析与网络入侵检测



Query ⬍
www.9cellar.cn
www.ahuixue.net
www.aihongsen.com;www.aihongsen.cn
www.ajkwp.com;www.sdkwkj.com;www.dkdlsj.com;www.cpxkvc.com;www.ttxknb.com;www.bbtzky.com;ww
www.angel02.com;www.angel03.com;www.angel05.com
www.anjijr.com
www.aobanglianhe.com
www.artechnology.com.cn
www.atlyu.com
www.avite.cn;www.avite.com.cn

Alert ⬍	Source IP Address ⬍	Destination IP Address ⬍	Count ⬍
ET CINS Active Threat Intelligence Poor Reputation IP group 78	80.211.89.146	10.28.62.34	4
ET DROP Dshield Block Listed Source group 1	77.72.85.8	10.28.60.100	1
ET DROP Dshield Block Listed Source group 1	185.255.31.2	10.28.60.100	1
ET DROP Dshield Block Listed Source group 1	198.108.67.16	10.28.60.100	1
ET CINS Active Threat Intelligence Poor Reputation IP group 74	77.53.183.50	10.28.62.34	1
ET CINS Active Threat Intelligence Poor Reputation IP group 74	77.72.85.8	10.28.60.100	1
ET CINS Active Threat Intelligence Poor Reputation IP group 42	51.15.70.87	10.28.60.100	1
ET CINS Active Threat Intelligence Poor Reputation IP group 53	60.191.38.77	10.28.60.100	1
ET CINS Active Threat Intelligence Poor Reputation IP group 55	60.251.189.212	10.28.60.100	1
ET CINS Active Threat Intelligence Poor Reputation IP group 57	61.219.11.151	10.28.60.100	1

SSH - Source IP Address

IP Address ⬍	Count ⬍
10.28.80.11	1
10.28.202.10	1
122.97.179.153	1

SSH - Destination IP Address

IP Address ⬍	Count ⬍
10.28.70.15	15,183
10.28.60.100	136
10.28.52.68	18
10.28.52.65	14
10.28.50.35	8
10.28.52.29	8
10.28.92.11	6

SSH - Destination Port

Port ⬍	Count ⬍
51668	15,415
22345	6

SMTP - Source IP Address

IP Address ⬍	Count ⬍
10.28.50.35	335
10.28.50.30	76
10.28.60.28	65
10.28.70.15	43
10.28.50.29	41
10.28.60.29	12
10.28.60.20	6
10.28.70.30	6

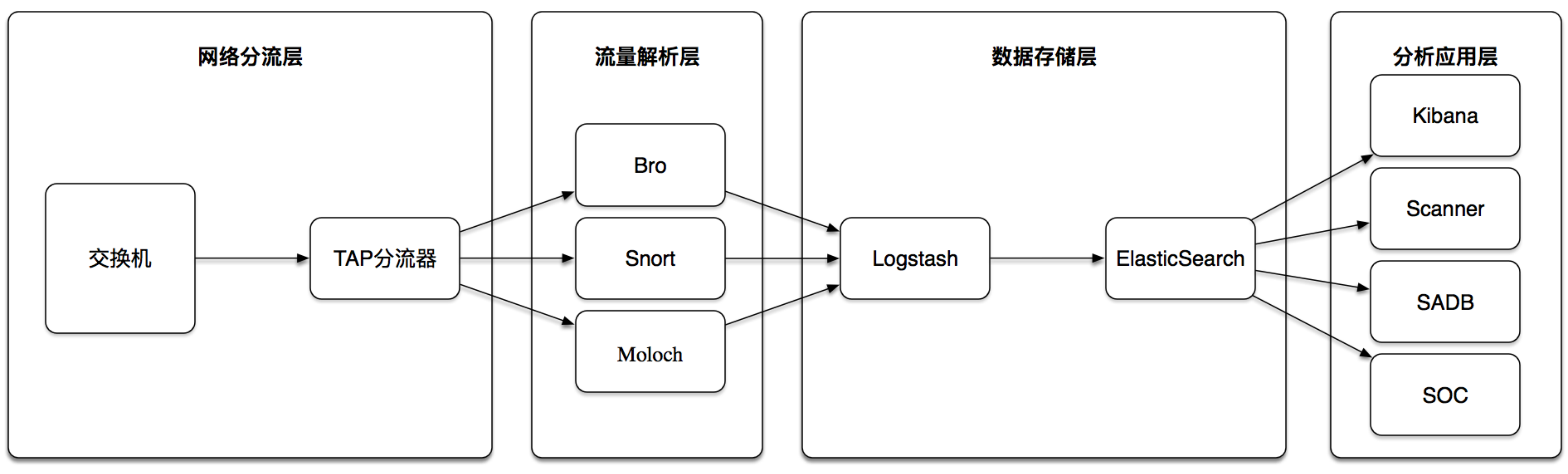
SMTP - Destination IP Address

IP Address ⬍	Count ⬍
171.221.254.195	225
182.150.59.136	213
117.174.24.81	166

SMTP - Destination Port

Port ⬍	Count ⬍
25	604

流量回溯

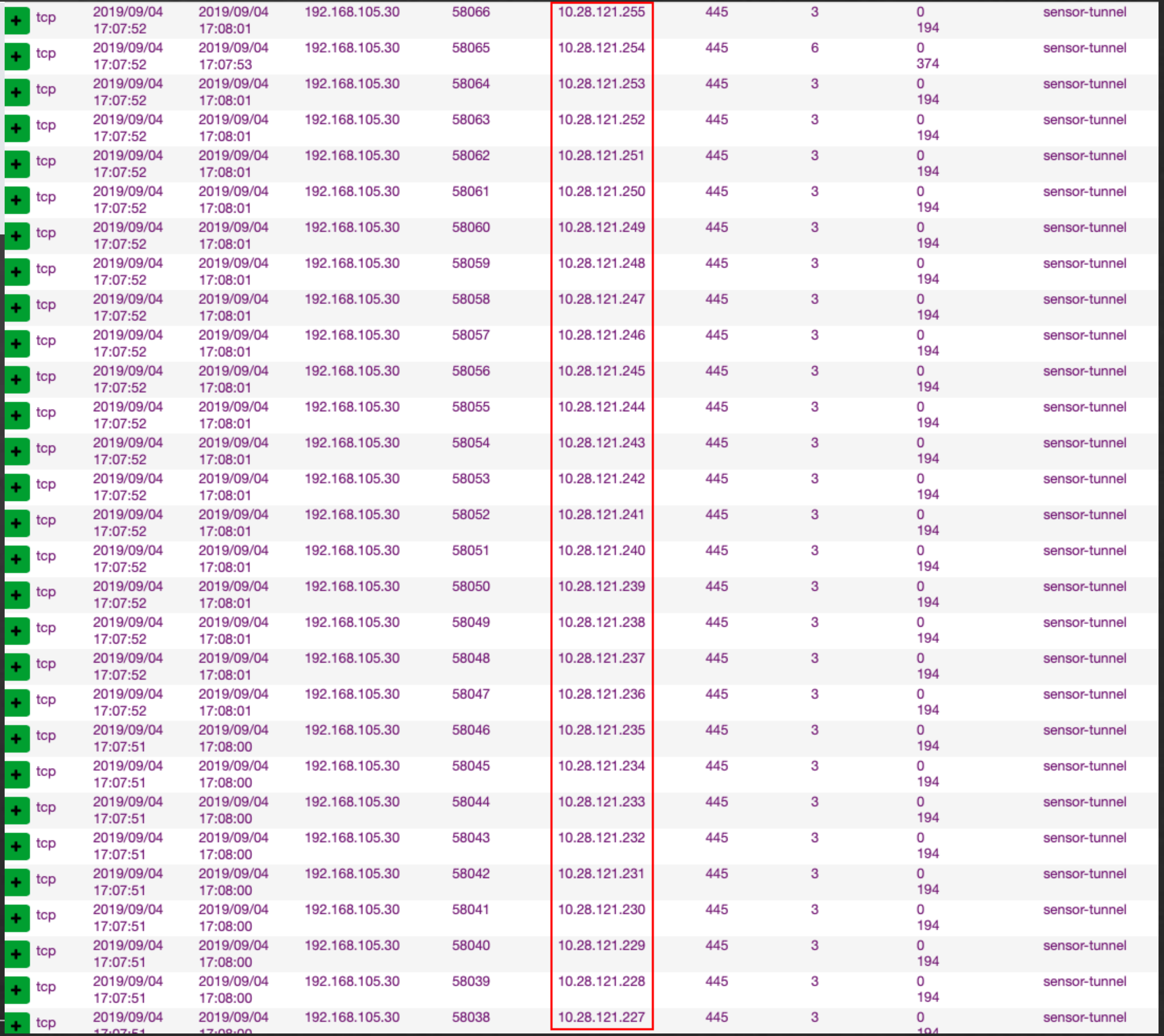


Moloch是一款开源的大规模全量包捕获、索引及存储系统

- 安全分析与取证
  - 基于原始网络流量，对安全事件、安全告警进行二次确认。
- 网络故障排查与调试
  - 通过网络抓包，对网络故障进行排查，对网络相关配置进行复核验证。

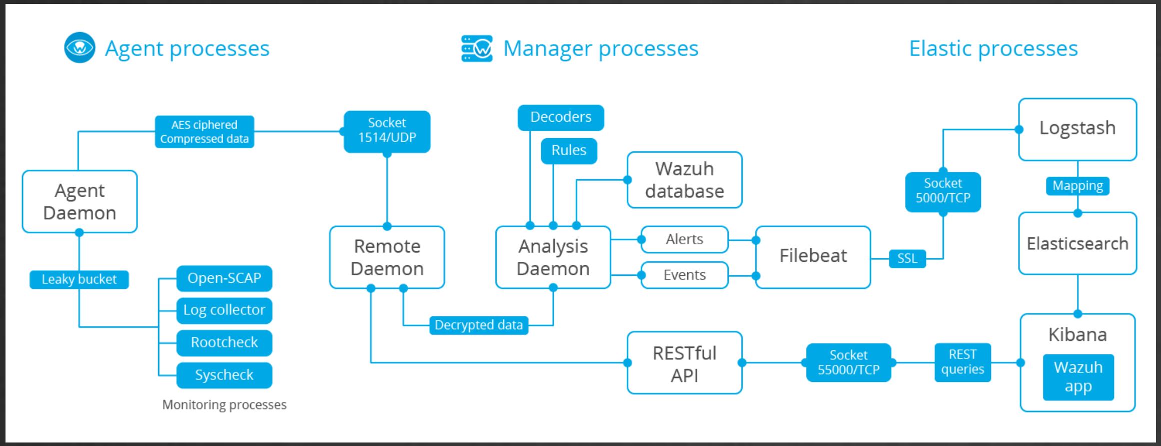
安全取证案例

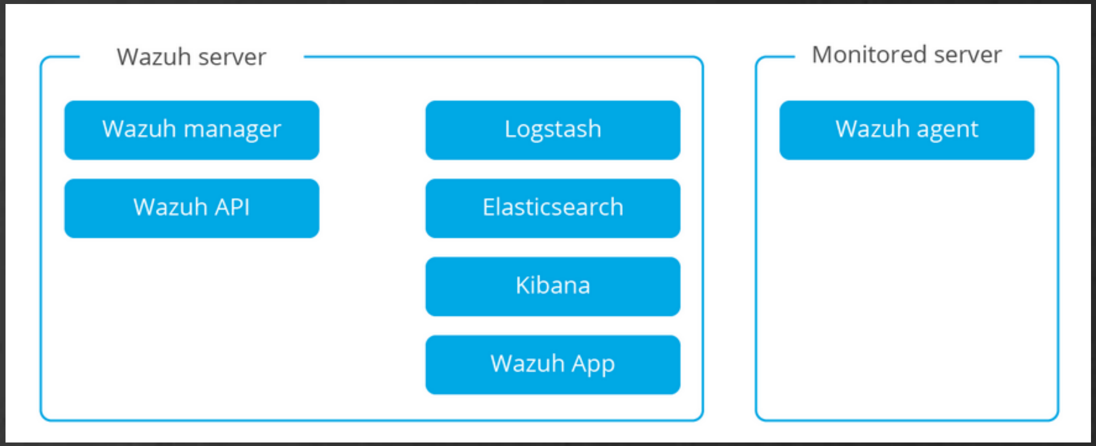
检测到交换机ArpMiss攻击，请注意!
> 时间: 2019-09-04T07:04:24.422Z
> 源IP: <MISSING VALUE>
> 日志: Attack occurred.(AttackType=Arp Miss Attack, SourceInterface=XGigabitEthernet0/0/2, SourceIP=192.168.105.30, AttackPackets=31 packets per second)



+	tcp	2019/09/04 17:07:52	2019/09/04 17:08:01	192.168.105.30	58066	10.28.121.255	445	3	0 194	sensor-tunnel
+	tcp	2019/09/04 17:07:52	2019/09/04 17:07:53	192.168.105.30	58065	10.28.121.254	445	6	0 374	sensor-tunnel
+	tcp	2019/09/04 17:07:52	2019/09/04 17:08:01	192.168.105.30	58064	10.28.121.253	445	3	0 194	sensor-tunnel
+	tcp	2019/09/04 17:07:52	2019/09/04 17:08:01	192.168.105.30	58063	10.28.121.252	445	3	0 194	sensor-tunnel
+	tcp	2019/09/04 17:07:52	2019/09/04 17:08:01	192.168.105.30	58062	10.28.121.251	445	3	0 194	sensor-tunnel
+	tcp	2019/09/04 17:07:52	2019/09/04 17:08:01	192.168.105.30	58061	10.28.121.250	445	3	0 194	sensor-tunnel
+	tcp	2019/09/04 17:07:52	2019/09/04 17:08:01	192.168.105.30	58060	10.28.121.249	445	3	0 194	sensor-tunnel
+	tcp	2019/09/04 17:07:52	2019/09/04 17:08:01	192.168.105.30	58059	10.28.121.248	445	3	0 194	sensor-tunnel
+	tcp	2019/09/04 17:07:52	2019/09/04 17:08:01	192.168.105.30	58058	10.28.121.247	445	3	0 194	sensor-tunnel
+	tcp	2019/09/04 17:07:52	2019/09/04 17:08:01	192.168.105.30	58057	10.28.121.246	445	3	0 194	sensor-tunnel
+	tcp	2019/09/04 17:07:52	2019/09/04 17:08:01	192.168.105.30	58056	10.28.121.245	445	3	0 194	sensor-tunnel
+	tcp	2019/09/04 17:07:52	2019/09/04 17:08:01	192.168.105.30	58055	10.28.121.244	445	3	0 194	sensor-tunnel
+	tcp	2019/09/04 17:07:52	2019/09/04 17:08:01	192.168.105.30	58054	10.28.121.243	445	3	0 194	sensor-tunnel
+	tcp	2019/09/04 17:07:52	2019/09/04 17:08:01	192.168.105.30	58053	10.28.121.242	445	3	0 194	sensor-tunnel
+	tcp	2019/09/04 17:07:52	2019/09/04 17:08:01	192.168.105.30	58052	10.28.121.241	445	3	0 194	sensor-tunnel
+	tcp	2019/09/04 17:07:52	2019/09/04 17:08:01	192.168.105.30	58051	10.28.121.240	445	3	0 194	sensor-tunnel
+	tcp	2019/09/04 17:07:52	2019/09/04 17:08:01	192.168.105.30	58050	10.28.121.239	445	3	0 194	sensor-tunnel
+	tcp	2019/09/04 17:07:52	2019/09/04 17:08:01	192.168.105.30	58049	10.28.121.238	445	3	0 194	sensor-tunnel
+	tcp	2019/09/04 17:07:52	2019/09/04 17:08:01	192.168.105.30	58048	10.28.121.237	445	3	0 194	sensor-tunnel
+	tcp	2019/09/04 17:07:52	2019/09/04 17:08:01	192.168.105.30	58047	10.28.121.236	445	3	0 194	sensor-tunnel
+	tcp	2019/09/04 17:07:51	2019/09/04 17:08:00	192.168.105.30	58046	10.28.121.235	445	3	0 194	sensor-tunnel
+	tcp	2019/09/04 17:07:51	2019/09/04 17:08:00	192.168.105.30	58045	10.28.121.234	445	3	0 194	sensor-tunnel
+	tcp	2019/09/04 17:07:51	2019/09/04 17:08:00	192.168.105.30	58044	10.28.121.233	445	3	0 194	sensor-tunnel
+	tcp	2019/09/04 17:07:51	2019/09/04 17:08:00	192.168.105.30	58043	10.28.121.232	445	3	0 194	sensor-tunnel
+	tcp	2019/09/04 17:07:51	2019/09/04 17:08:00	192.168.105.30	58042	10.28.121.231	445	3	0 194	sensor-tunnel
+	tcp	2019/09/04 17:07:51	2019/09/04 17:08:00	192.168.105.30	58041	10.28.121.230	445	3	0 194	sensor-tunnel
+	tcp	2019/09/04 17:07:51	2019/09/04 17:08:00	192.168.105.30	58040	10.28.121.229	445	3	0 194	sensor-tunnel
+	tcp	2019/09/04 17:07:51	2019/09/04 17:08:00	192.168.105.30	58039	10.28.121.228	445	3	0 194	sensor-tunnel
+	tcp	2019/09/04 17:07:51	2019/09/04 17:08:00	192.168.105.30	58038	10.28.121.227	445	3	0 194	sensor-tunnel

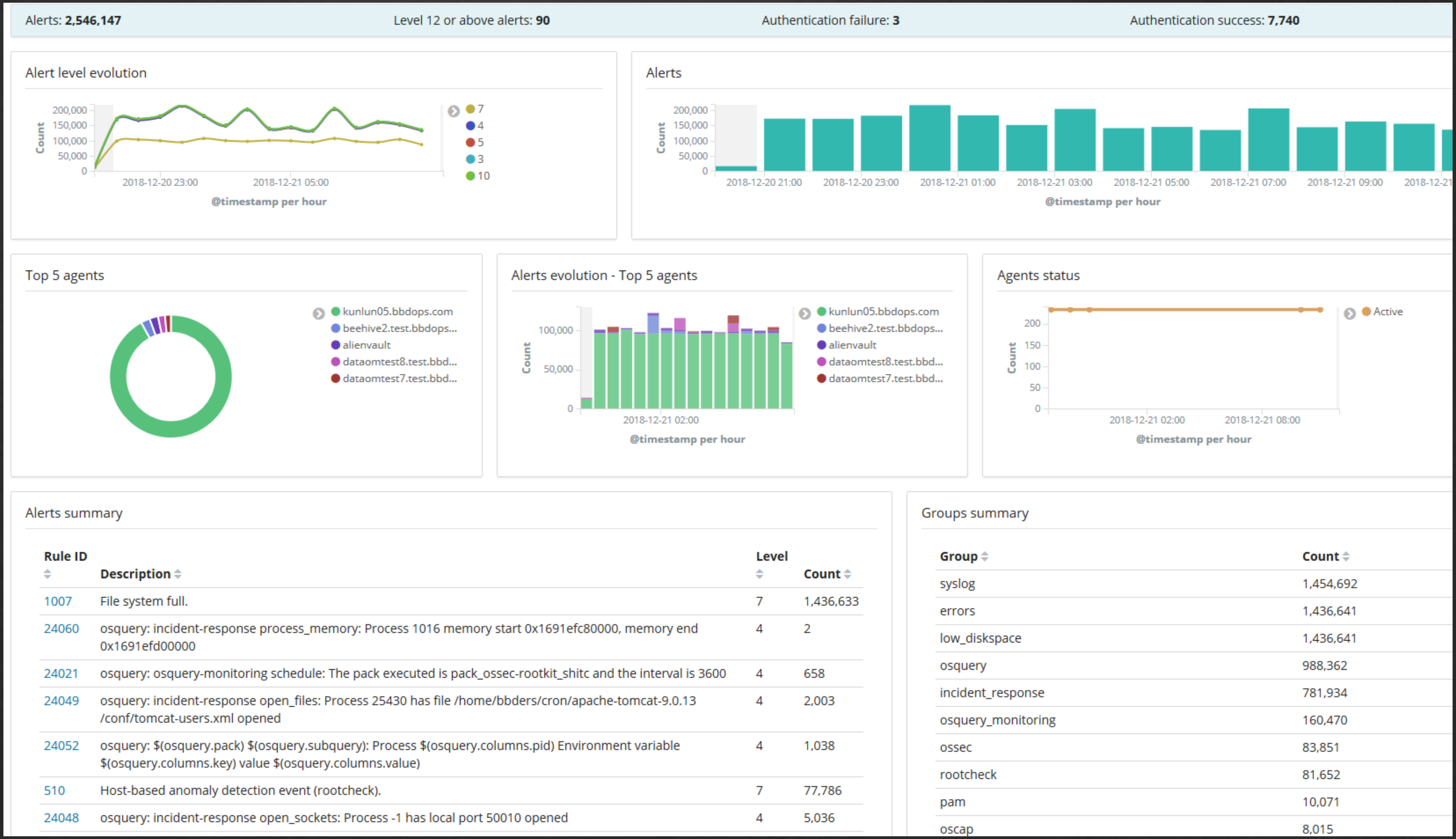
主机入侵检测





- 日志收集与分析
  - 收集各种类型主机日志，同时支持命令输出结果分析，发现各种主机事件。
- 系统文件完整性校验
  - 如果配置足够细，可以检查任意文件的改动。
- 异常与恶意行为检查，如木马、rootkit等。检查系统是否已经感染木马，是否存在异常行为
- 被动式漏洞扫描。对软件包检查，检查系统漏洞情况，尽可能早地发现安全漏洞
- 安全策略及合规性检查。可配置预定义的安全基线与策略，确保配置符合安全策略，及合规标准
- 资产清单。资产信息可细化至端口、进程、软件包等。

主机入侵检测



Alerts: **2,546,147** Level 12 or above alerts: **90** Authentication failure: **3** Authentication success: **7,740**

Alert level evolution

Alerts

Top 5 agents

Alerts evolution - Top 5 agents

Agents status

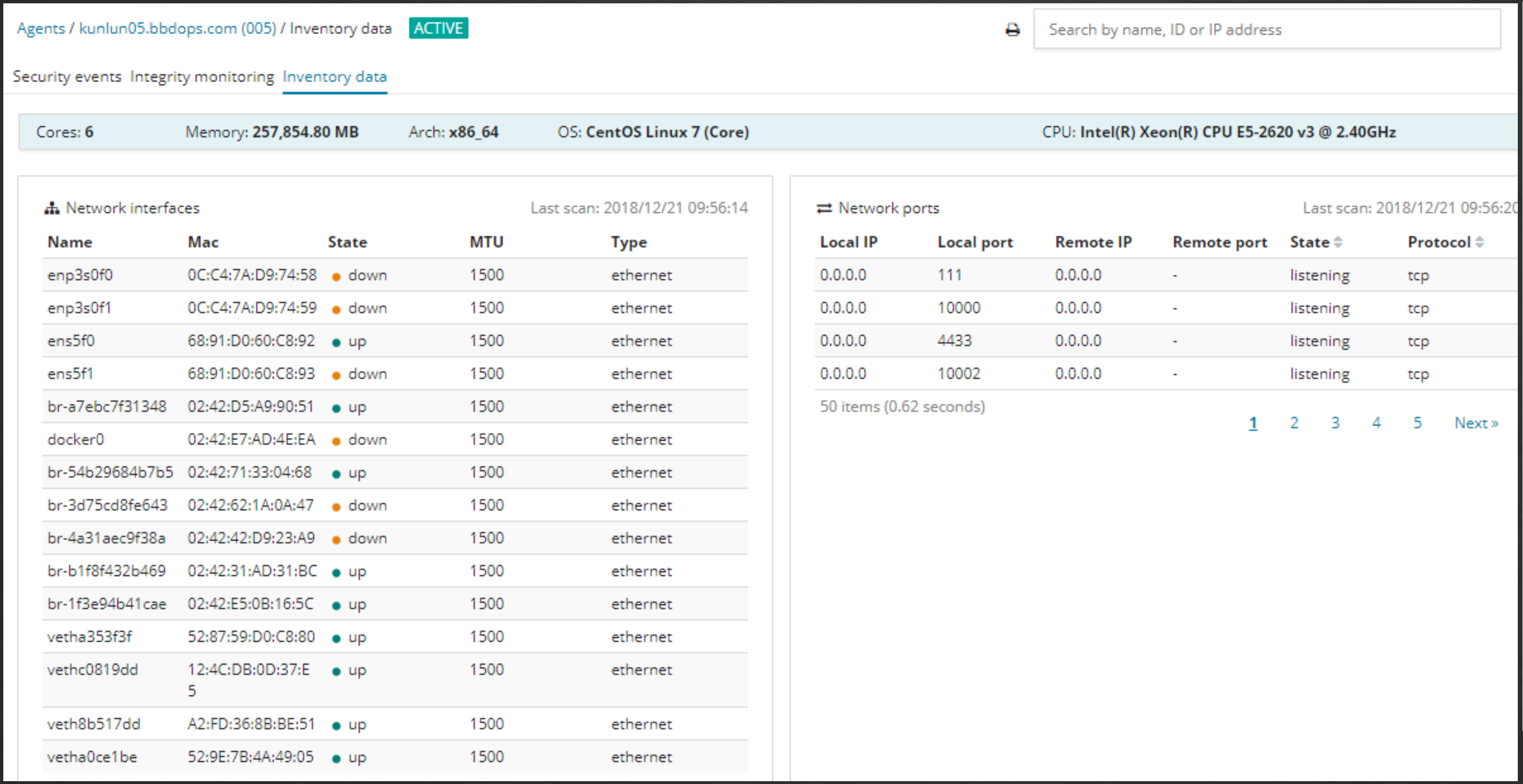
Alerts summary

Rule ID ⬍	Description ⬍	Level ⬍	Count ⬍
1007	File system full.	7	1,436,633
24060	osquery: incident-response process_memory: Process 1016 memory start 0x1691efc80000, memory end 0x1691efd00000	4	2
24021	osquery: osquery-monitoring schedule: The pack executed is pack_ossec-rootkit_shitc and the interval is 3600	4	658
24049	osquery: incident-response open_files: Process 25430 has file /home/bbders/cron/apache-tomcat-9.0.13 /conf/tomcat-users.xml opened	4	2,003
24052	osquery: $(osquery.pack) $(osquery.subquery): Process $(osquery.columns.pid) Environment variable $(osquery.columns.key) value $(osquery.columns.value)	4	1,038
510	Host-based anomaly detection event (rootcheck).	7	77,786
24048	osquery: incident-response open_sockets: Process -1 has local port 50010 opened	4	5,036

Groups summary

Group ⬍	Count ⬍
syslog	1,454,692
errors	1,436,641
low_diskspace	1,436,641
osquery	988,362
incident_response	781,934
osquery_monitoring	160,470
ossec	83,851
rootcheck	81,652
pam	10,071
oscap	8,015

主机入侵检测



Agents / kunlun05.bbdops.com (005) / Inventory data ACTIVE

Search by name, ID or IP address

Security events Integrity monitoring Inventory data

Cores: 6 Memory: 257,854.80 MB Arch: x86_64 OS: CentOS Linux 7 (Core) CPU: Intel(R) Xeon(R) CPU E5-2620 v3 @ 2.40GHz

Network interfaces Last scan: 2018/12/21 09:56:14

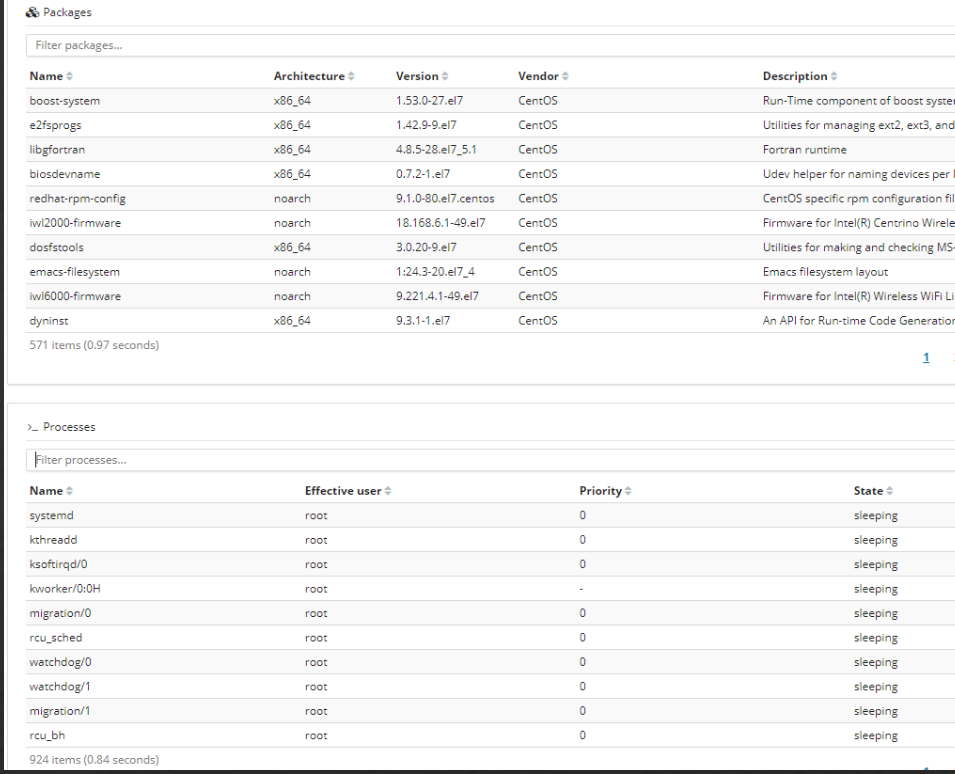
Name	Mac	State	MTU	Type
enp3s0f0	0C:C4:7A:D9:74:58	● down	1500	ethernet
enp3s0f1	0C:C4:7A:D9:74:59	● down	1500	ethernet
ens5f0	68:91:D0:60:C8:92	● up	1500	ethernet
ens5f1	68:91:D0:60:C8:93	● down	1500	ethernet
br-a7ebc7f31348	02:42:D5:A9:90:51	● up	1500	ethernet
docker0	02:42:E7:AD:4E:EA	● down	1500	ethernet
br-54b29684b7b5	02:42:71:33:04:68	● up	1500	ethernet
br-3d75cd8fe643	02:42:62:1A:0A:47	● down	1500	ethernet
br-4a31aec9f38a	02:42:42:D9:23:A9	● down	1500	ethernet
br-b1f8f432b469	02:42:31:AD:31:BC	● up	1500	ethernet
br-1f3e94b41cae	02:42:E5:0B:16:5C	● up	1500	ethernet
vetha353f3f	52:87:59:D0:C8:80	● up	1500	ethernet
vethc0819dd	12:4C:DB:0D:37:E5	● up	1500	ethernet
veth8b517dd	A2:FD:36:8B:BE:51	● up	1500	ethernet
vetha0ce1be	52:9E:7B:4A:49:05	● up	1500	ethernet

Network ports Last scan: 2018/12/21 09:56:20

Local IP	Local port	Remote IP	Remote port	State	Protocol
0.0.0.0	111	0.0.0.0	-	listening	tcp
0.0.0.0	10000	0.0.0.0	-	listening	tcp
0.0.0.0	4433	0.0.0.0	-	listening	tcp
0.0.0.0	10002	0.0.0.0	-	listening	tcp

50 items (0.62 seconds)

1 2 3 4 5 Next »



Packages

Filter packages...

Name	Architecture	Version	Vendor	Description
boost-system	x86_64	1.53.0-27.el7	CentOS	Run-Time component of boost syste
e2fsprogs	x86_64	1.42.9-9.el7	CentOS	Utilities for managing ext2, ext3, and
libgfortran	x86_64	4.8.5-28.el7_5.1	CentOS	Fortran runtime
biosdevname	x86_64	0.7.2-1.el7	CentOS	Udev helper for naming devices per
redhat-rpm-config	noarch	9.1.0-80.el7.centos	CentOS	CentOS specific rpm configuration fil
iwl2000-firmware	noarch	18.168.6.1-49.el7	CentOS	Firmware for Intel(R) Centrino Wirele
dosfstools	x86_64	3.0.20-9.el7	CentOS	Utilities for making and checking MS-
emacs-filesystem	noarch	1:24.3-20.el7_4	CentOS	Emacs filesystem layout
iwl6000-firmware	noarch	9.221.4.1-49.el7	CentOS	Firmware for Intel(R) Wireless WiFi Li
dyninst	x86_64	9.3.1-1.el7	CentOS	An API for Run-time Code Generatio

571 items (0.97 seconds)

1

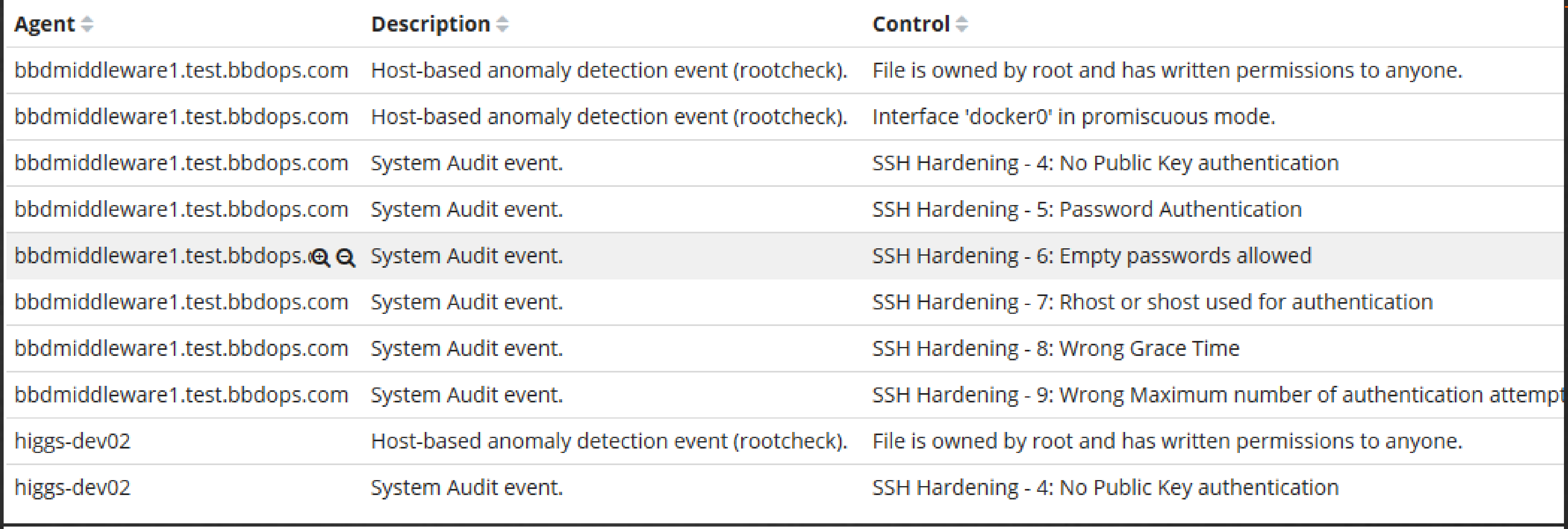
>_ Processes

Filter processes...

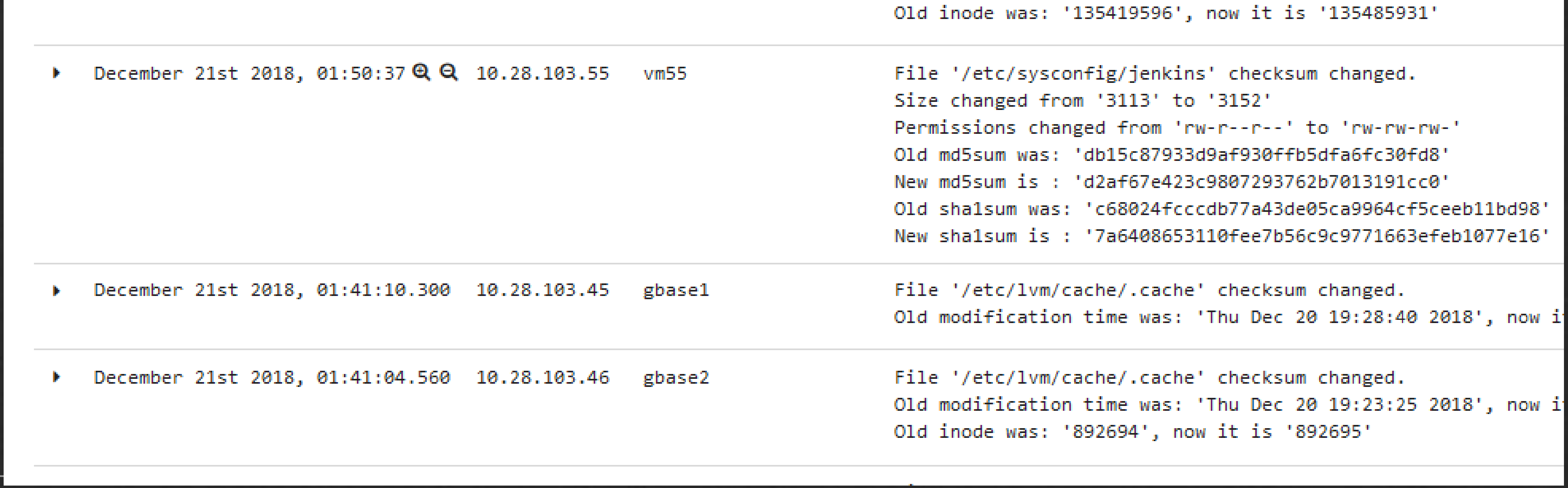
Name	Effective user	Priority	State
systemd	root	0	sleeping
kthreadd	root	0	sleeping
ksoftirqd/0	root	0	sleeping
kworker/0:0H	root	-	sleeping
migration/0	root	0	sleeping
rcu_sched	root	0	sleeping
watchdog/0	root	0	sleeping
watchdog/1	root	0	sleeping
migration/1	root	0	sleeping
rcu_bh	root	0	sleeping

924 items (0.84 seconds)

主机入侵检测

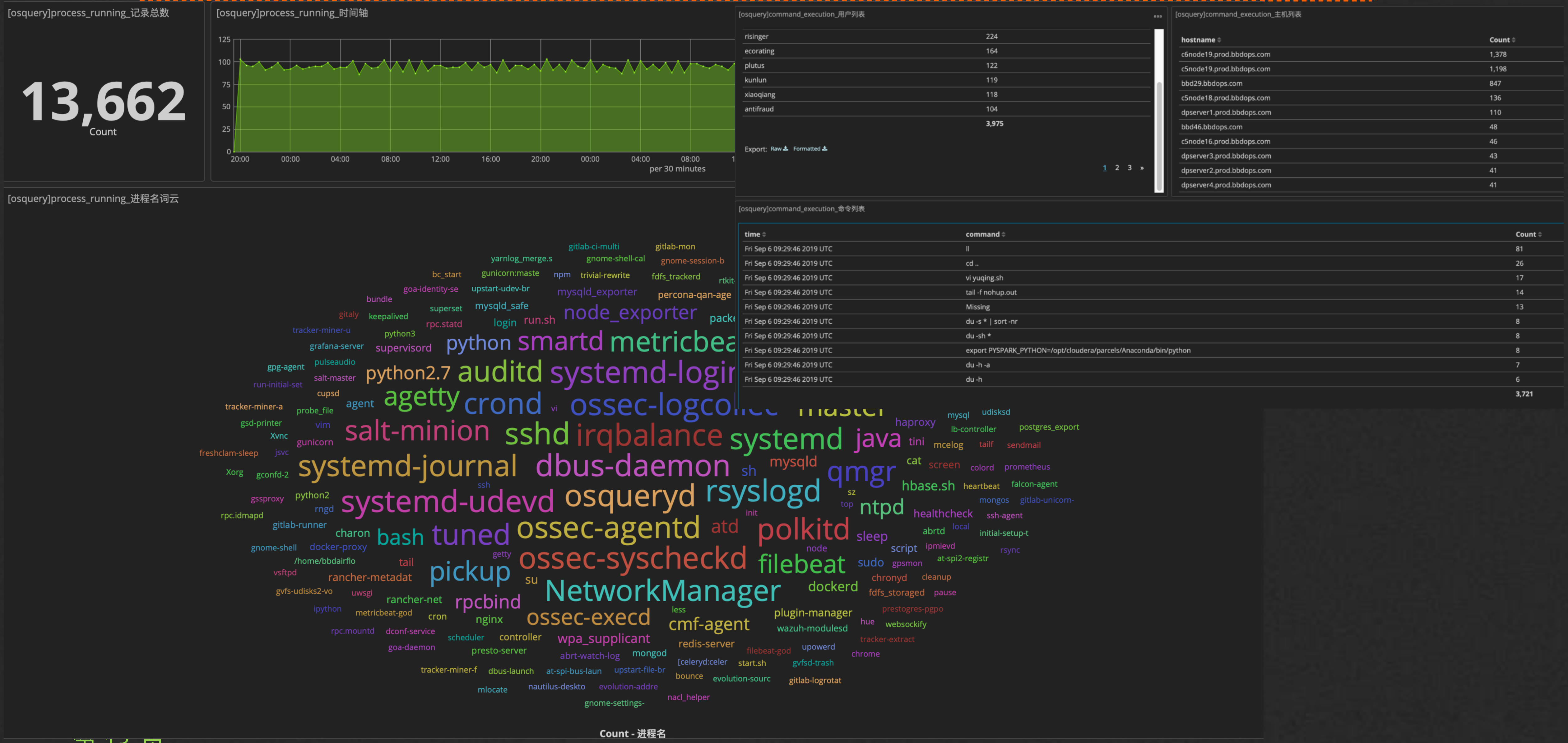


Agent	Description	Control
bbdmiddleware1.test.bbdops.com	Host-based anomaly detection event (rootcheck).	File is owned by root and has written permissions to anyone.
bbdmiddleware1.test.bbdops.com	Host-based anomaly detection event (rootcheck).	Interface 'docker0' in promiscuous mode.
bbdmiddleware1.test.bbdops.com	System Audit event.	SSH Hardening - 4: No Public Key authentication
bbdmiddleware1.test.bbdops.com	System Audit event.	SSH Hardening - 5: Password Authentication
bbdmiddleware1.test.bbdops.c	System Audit event.	SSH Hardening - 6: Empty passwords allowed
bbdmiddleware1.test.bbdops.com	System Audit event.	SSH Hardening - 7: Rhost or shost used for authentication
bbdmiddleware1.test.bbdops.com	System Audit event.	SSH Hardening - 8: Wrong Grace Time
bbdmiddleware1.test.bbdops.com	System Audit event.	SSH Hardening - 9: Wrong Maximum number of authentication attempt
higgs-dev02	Host-based anomaly detection event (rootcheck).	File is owned by root and has written permissions to anyone.
higgs-dev02	System Audit event.	SSH Hardening - 4: No Public Key authentication



```
                                                        Old inode was: '135419596', now it is '135485931'

  December 21st 2018, 01:50:37   10.28.103.55   vm55    File '/etc/sysconfig/jenkins' checksum changed.
                                                        Size changed from '3113' to '3152'
                                                        Permissions changed from 'rw-r--r--' to 'rw-rw-rw-'
                                                        Old md5sum was: 'db15c87933d9af930ffb5dfa6fc30fd8'
                                                        New md5sum is : 'd2af67e423c9807293762b7013191cc0'
                                                        Old sha1sum was: 'c68024fcccdb77a43de05ca9964cf5ceeb11bd98'
                                                        New sha1sum is : '7a6408653110fee7b56c9c9771663efeb1077e16'

  December 21st 2018, 01:41:10.300   10.28.103.45   gbase1    File '/etc/lvm/cache/.cache' checksum changed.
                                                              Old modification time was: 'Thu Dec 20 19:28:40 2018', now i

  December 21st 2018, 01:41:04.560   10.28.103.46   gbase2    File '/etc/lvm/cache/.cache' checksum changed.
                                                              Old modification time was: 'Thu Dec 20 19:23:25 2018', now i
                                                              Old inode was: '892694', now it is '892695'
```

主机入侵检测



[osquery]process_running_记录总数

13,662
Count

[osquery]process_running_时间轴

[osquery]process_running_进程名词云

[osquery]command_execution_用户列表

risinger	224
ecorating	164
plutus	122
kunlun	119
xiaoqiang	118
antifraud	104
	3,975

Export: Raw Formatted

1 2 3 »

[osquery]command_execution_主机列表

hostname	Count
c6node19.prod.bbdops.com	1,378
c5node19.prod.bbdops.com	1,198
bbd29.bbdops.com	847
c5node18.prod.bbdops.com	136
dpserver1.prod.bbdops.com	110
bbd46.bbdops.com	48
c5node16.prod.bbdops.com	46
dpserver3.prod.bbdops.com	43
dpserver2.prod.bbdops.com	41
dpserver4.prod.bbdops.com	41

[osquery]command_execution_命令列表

time	command	Count
Fri Sep 6 09:29:46 2019 UTC	ll	81
Fri Sep 6 09:29:46 2019 UTC	cd ..	26
Fri Sep 6 09:29:46 2019 UTC	vi yuqing.sh	17
Fri Sep 6 09:29:46 2019 UTC	tail -f nohup.out	14
Fri Sep 6 09:29:46 2019 UTC	Missing	13
Fri Sep 6 09:29:46 2019 UTC	du -s * | sort -nr	8
Fri Sep 6 09:29:46 2019 UTC	du -sh *	8
Fri Sep 6 09:29:46 2019 UTC	export PYSPARK_PYTHON=/opt/cloudera/parcels/Anaconda/bin/python	8
Fri Sep 6 09:29:46 2019 UTC	du -h -a	7
Fri Sep 6 09:29:46 2019 UTC	du -h	6
		3,721

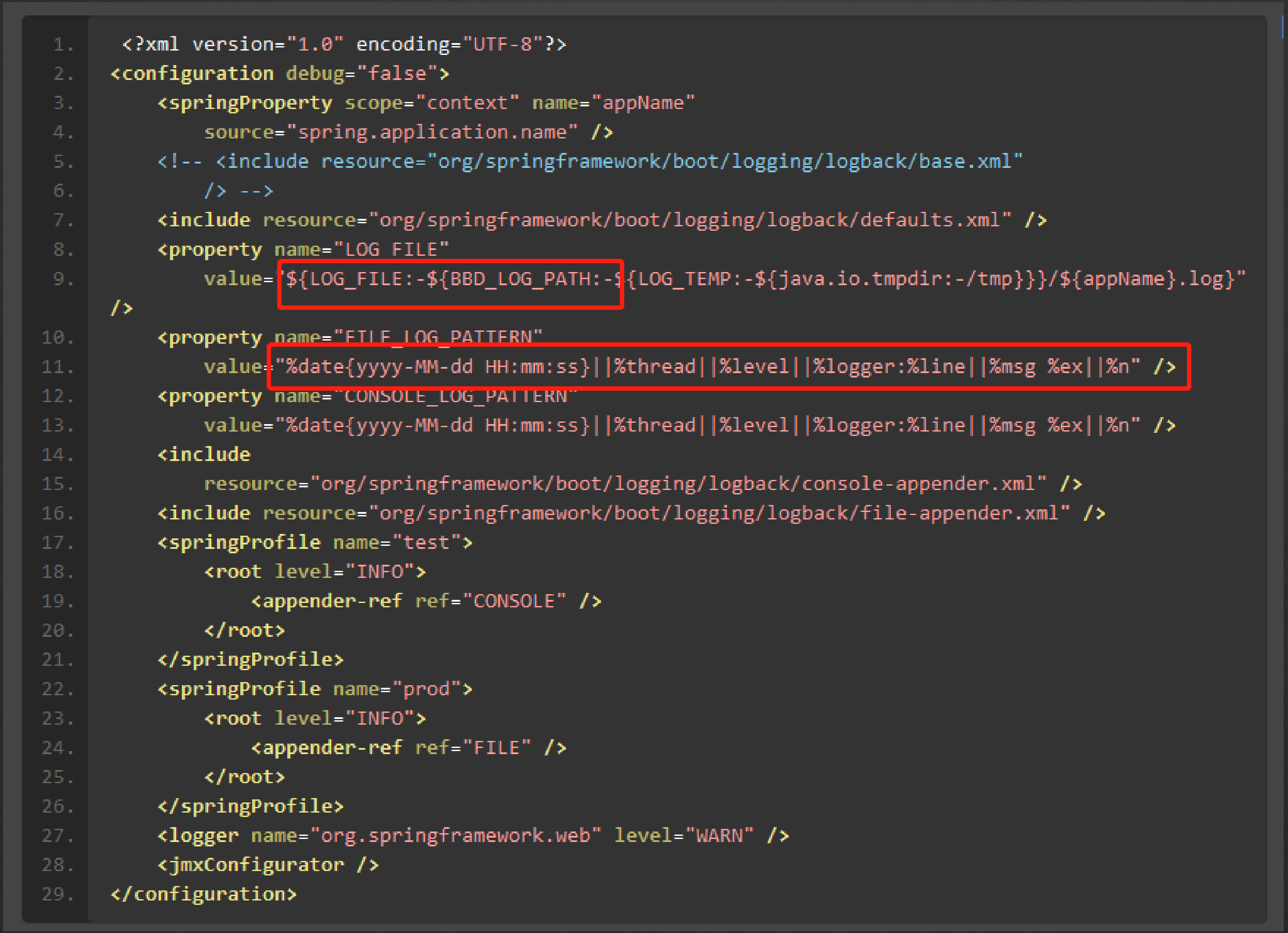
在日志、监控的一些应用

应用日志

应用日志采用ElasticSearch存储，主要是堆栈不好处理。

- 以两个竖线||隔开，而非空格
- 日期格式：%date{yyyy-MM-dd HH:mm:ss}
- 最后追加的不是回车换行符，而是"||"加一个回车换行符;
- 明确`堆栈`信息的输出，和message信息放一起;
- 通过环境变量定义日志输出目录

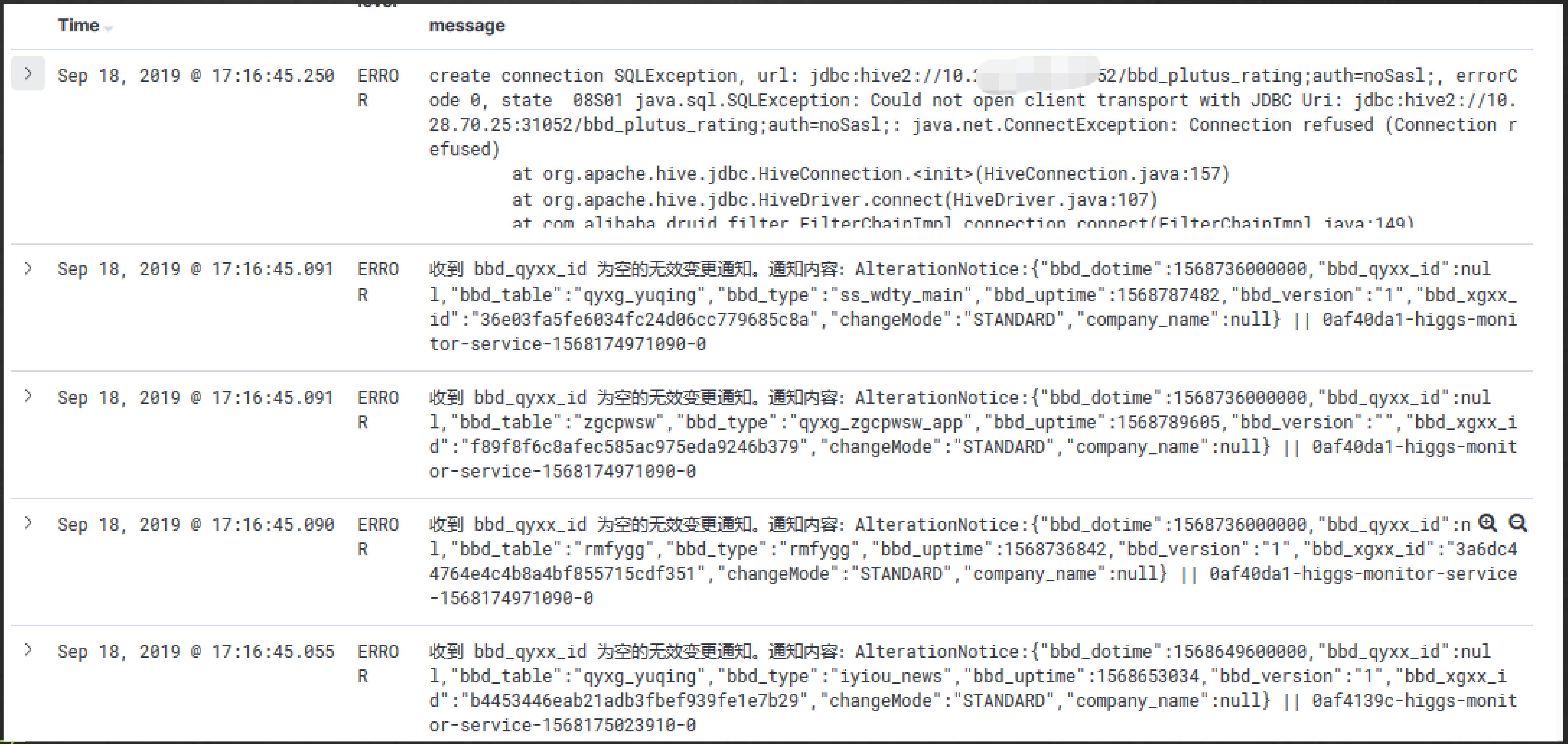
应用日志



```xml
 <?xml version="1.0" encoding="UTF-8"?>
<configuration debug="false">
    <springProperty scope="context" name="appName"
        source="spring.application.name" />
    <!-- <include resource="org/springframework/boot/logging/logback/base.xml"
        /> -->
    <include resource="org/springframework/boot/logging/logback/defaults.xml" />
    <property name="LOG_FILE"
        value="${LOG_FILE:-${BBD_LOG_PATH:-${LOG_TEMP:-${java.io.tmpdir:-/tmp}}}/${appName}.log}"
/>
    <property name="FILE_LOG_PATTERN"
        value="%date{yyyy-MM-dd HH:mm:ss}||%thread||%level||%logger:%line||%msg %ex||%n" />
    <property name="CONSOLE_LOG_PATTERN"
        value="%date{yyyy-MM-dd HH:mm:ss}||%thread||%level||%logger:%line||%msg %ex||%n" />
    <include
        resource="org/springframework/boot/logging/logback/console-appender.xml" />
    <include resource="org/springframework/boot/logging/logback/file-appender.xml" />
    <springProfile name="test">
        <root level="INFO">
            <appender-ref ref="CONSOLE" />
        </root>
    </springProfile>
    <springProfile name="prod">
        <root level="INFO">
            <appender-ref ref="FILE" />
        </root>
    </springProfile>
    <logger name="org.springframework.web" level="WARN" />
    <jmxConfigurator />
</configuration>
```

- logback对Spring的扩展：logback-spring.xml
- springProperty、springProfile

应用日志

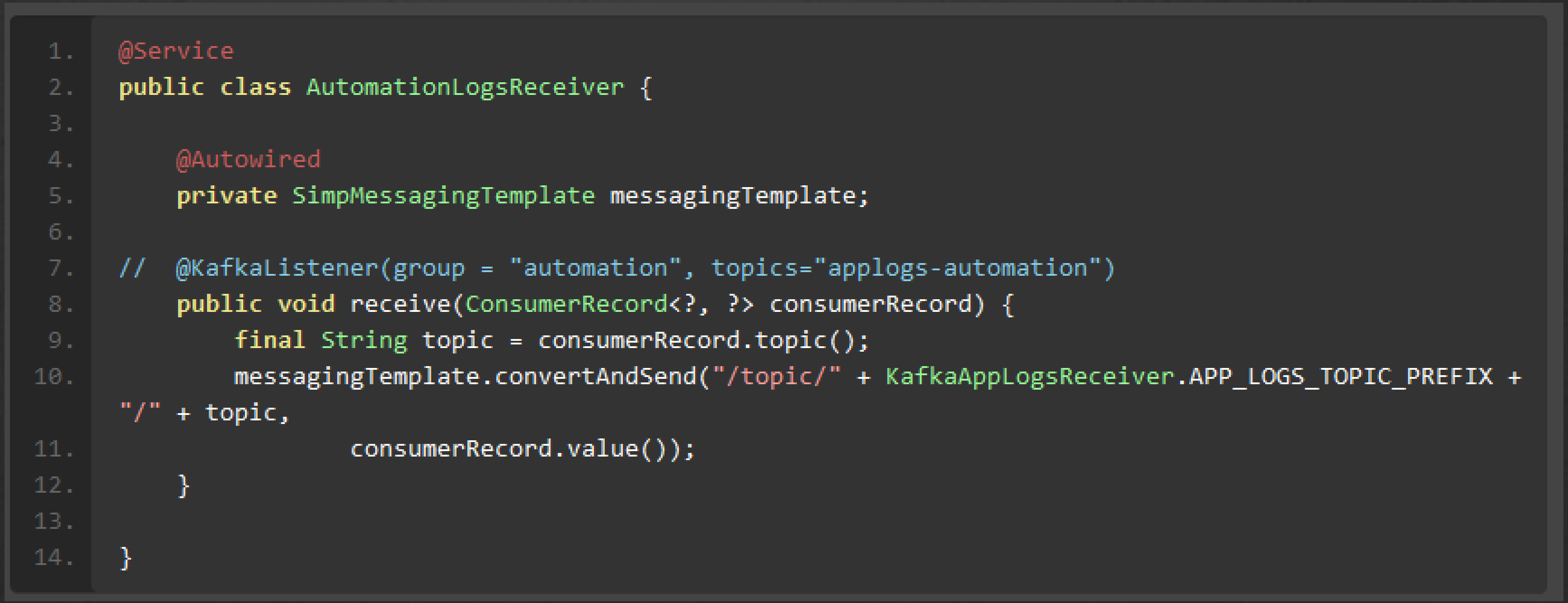


```
    Time              level   message

>   Sep 18, 2019 @ 17:16:45.250   ERRO   create connection SQLException, url: jdbc:hive2://10.[redacted]52/bbd_plutus_rating;auth=noSasl;, errorC
                                  R      ode 0, state  08S01 java.sql.SQLException: Could not open client transport with JDBC Uri: jdbc:hive2://10.
                                         28.70.25:31052/bbd_plutus_rating;auth=noSasl;: java.net.ConnectException: Connection refused (Connection r
                                         efused)
                                                 at org.apache.hive.jdbc.HiveConnection.<init>(HiveConnection.java:157)
                                                 at org.apache.hive.jdbc.HiveDriver.connect(HiveDriver.java:107)
                                                 at com.alibaba.druid.filter.FilterChainImpl.connection_connect(FilterChainImpl.java:149)

>   Sep 18, 2019 @ 17:16:45.091   ERRO   收到 bbd_qyxx_id 为空的无效变更通知。通知内容: AlterationNotice:{"bbd_dotime":1568736000000,"bbd_qyxx_id":nul
                                  R      l,"bbd_table":"qyxg_yuqing","bbd_type":"ss_wdty_main","bbd_uptime":1568787482,"bbd_version":"1","bbd_xgxx_
                                         id":"36e03fa5fe6034fc24d06cc779685c8a","changeMode":"STANDARD","company_name":null} || 0af40da1-higgs-moni
                                         tor-service-1568174971090-0

>   Sep 18, 2019 @ 17:16:45.091   ERRO   收到 bbd_qyxx_id 为空的无效变更通知。通知内容: AlterationNotice:{"bbd_dotime":1568736000000,"bbd_qyxx_id":nul
                                  R      l,"bbd_table":"zgcpwsw","bbd_type":"qyxg_zgcpwsw_app","bbd_uptime":1568789605,"bbd_version":"","bbd_xgxx_i
                                         d":"f89f8f6c8afec585ac975eda9246b379","changeMode":"STANDARD","company_name":null} || 0af40da1-higgs-monit
                                         or-service-1568174971090-0

>   Sep 18, 2019 @ 17:16:45.090   ERRO   收到 bbd_qyxx_id 为空的无效变更通知。通知内容: AlterationNotice:{"bbd_dotime":1568736000000,"bbd_qyxx_id":n
                                  R      l,"bbd_table":"rmfygg","bbd_type":"rmfygg","bbd_uptime":1568736842,"bbd_version":"1","bbd_xgxx_id":"3a6dc4
                                         4764e4c4b8a4bf855715cdf351","changeMode":"STANDARD","company_name":null} || 0af40da1-higgs-monitor-service
                                         -1568174971090-0

>   Sep 18, 2019 @ 17:16:45.055   ERRO   收到 bbd_qyxx_id 为空的无效变更通知。通知内容: AlterationNotice:{"bbd_dotime":1568649600000,"bbd_qyxx_id":nul
                                  R      l,"bbd_table":"qyxg_yuqing","bbd_type":"iyiou_news","bbd_uptime":1568653034,"bbd_version":"1","bbd_xgxx_i
                                         d":"b4453446eab21adb3fbef939fe1e7b29","changeMode":"STANDARD","company_name":null} || 0af4139c-higgs-monit
                                         or-service-1568175023910-0
```

应用日志-实时展示

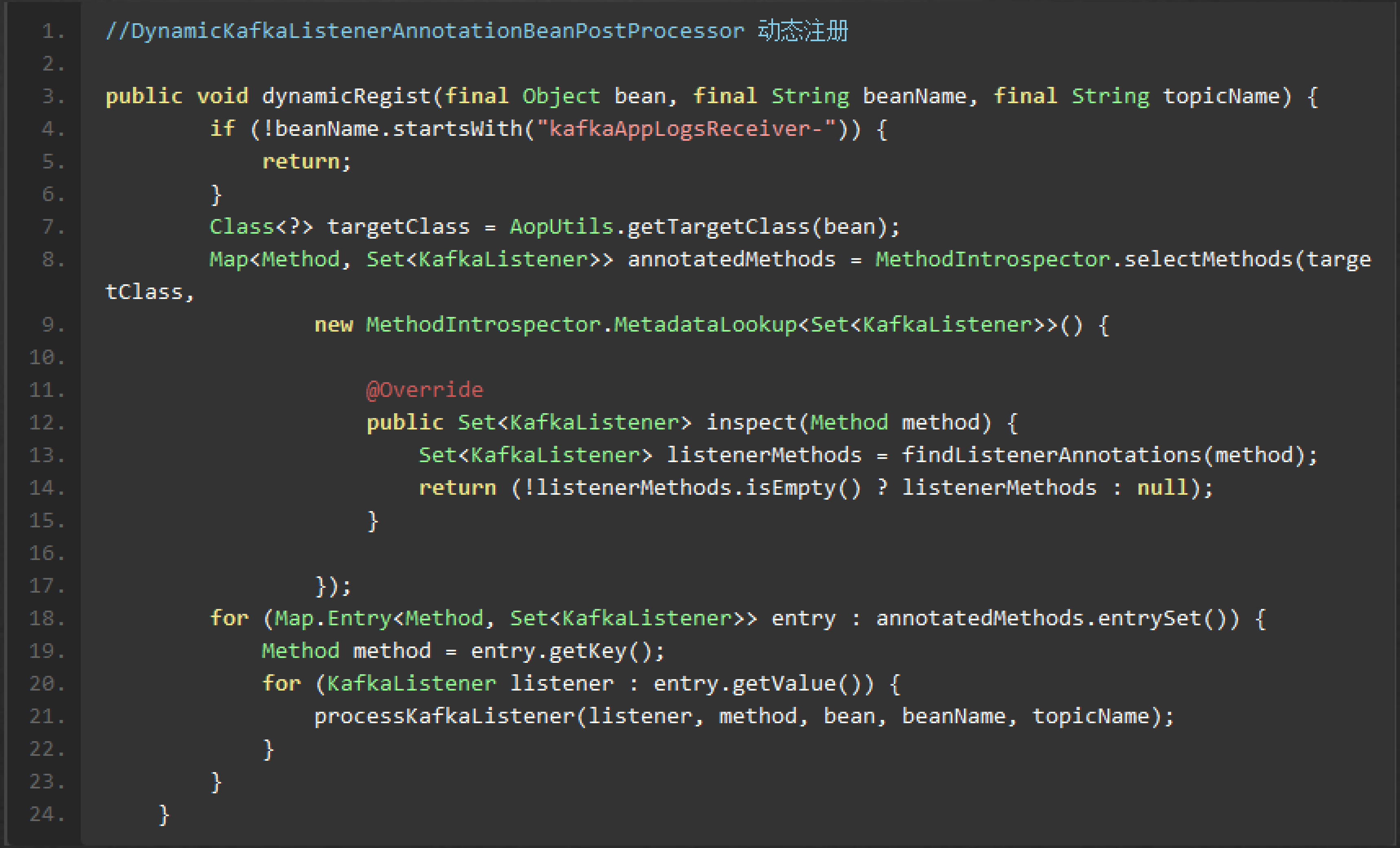
Web界面实时输出最新的应用日志。

Spring Data @kafkaListener



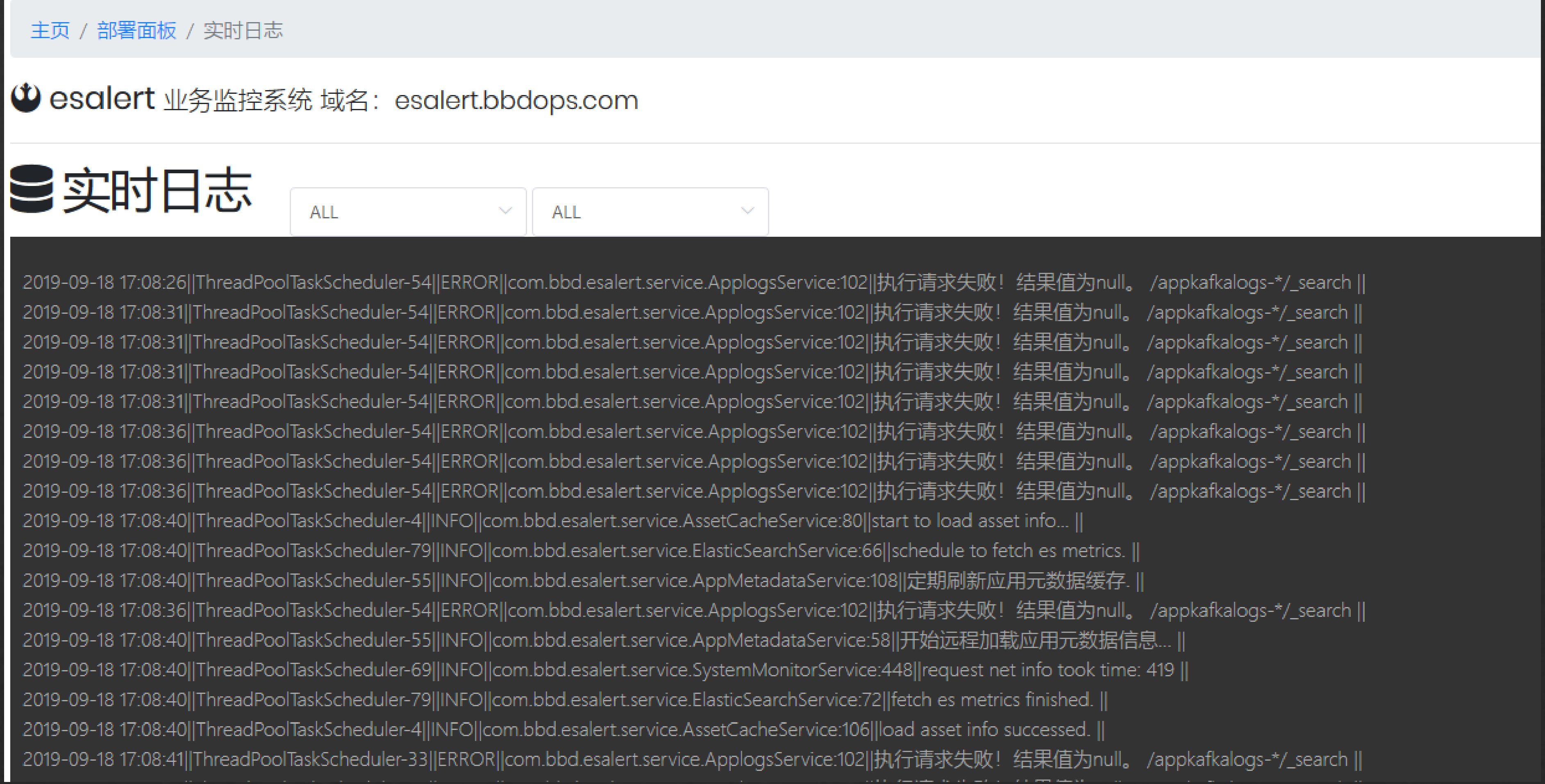
```java
@Service
public class AutomationLogsReceiver {

    @Autowired
    private SimpMessagingTemplate messagingTemplate;

//  @KafkaListener(group = "automation", topics="applogs-automation")
    public void receive(ConsumerRecord<?, ?> consumerRecord) {
        final String topic = consumerRecord.topic();
        messagingTemplate.convertAndSend("/topic/" + KafkaAppLogsReceiver.APP_LOGS_TOPIC_PREFIX + "/" + topic,
                consumerRecord.value());
    }

}
```

应用日志-实时展示



```java
//DynamicKafkaListenerAnnotationBeanPostProcessor 动态注册

public void dynamicRegist(final Object bean, final String beanName, final String topicName) {
    if (!beanName.startsWith("kafkaAppLogsReceiver-")) {
      return;
    }
    Class<?> targetClass = AopUtils.getTargetClass(bean);
    Map<Method, Set<KafkaListener>> annotatedMethods = MethodIntrospector.selectMethods(targetClass,
        new MethodIntrospector.MetadataLookup<Set<KafkaListener>>() {

          @Override
          public Set<KafkaListener> inspect(Method method) {
            Set<KafkaListener> listenerMethods = findListenerAnnotations(method);
            return (!listenerMethods.isEmpty() ? listenerMethods : null);
          }

        });
    for (Map.Entry<Method, Set<KafkaListener>> entry : annotatedMethods.entrySet()) {
      Method method = entry.getKey();
      for (KafkaListener listener : entry.getValue()) {
        processKafkaListener(listener, method, bean, beanName, topicName);
      }
    }
  }
```

应用日志-实时展示



主页 / 部署面板 / 实时日志

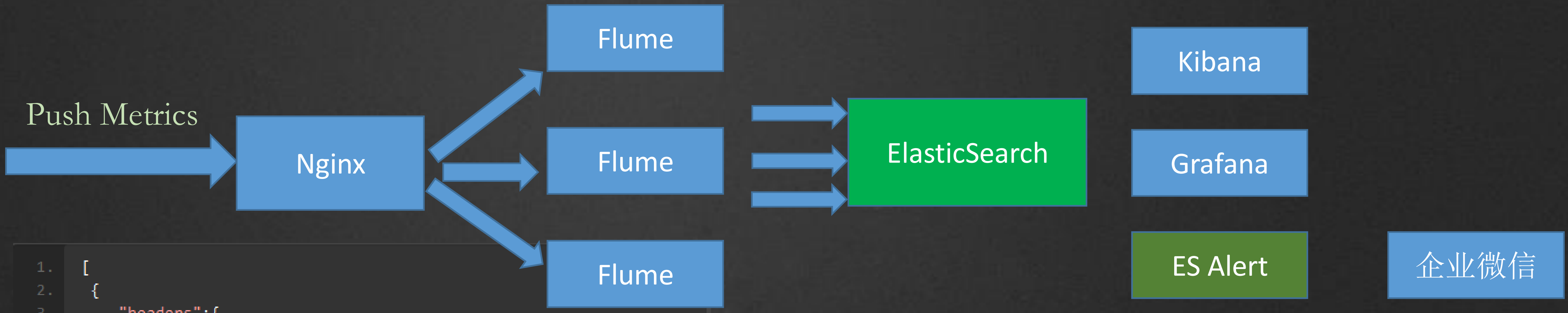
esalert 业务监控系统 域名： esalert.bbdops.com

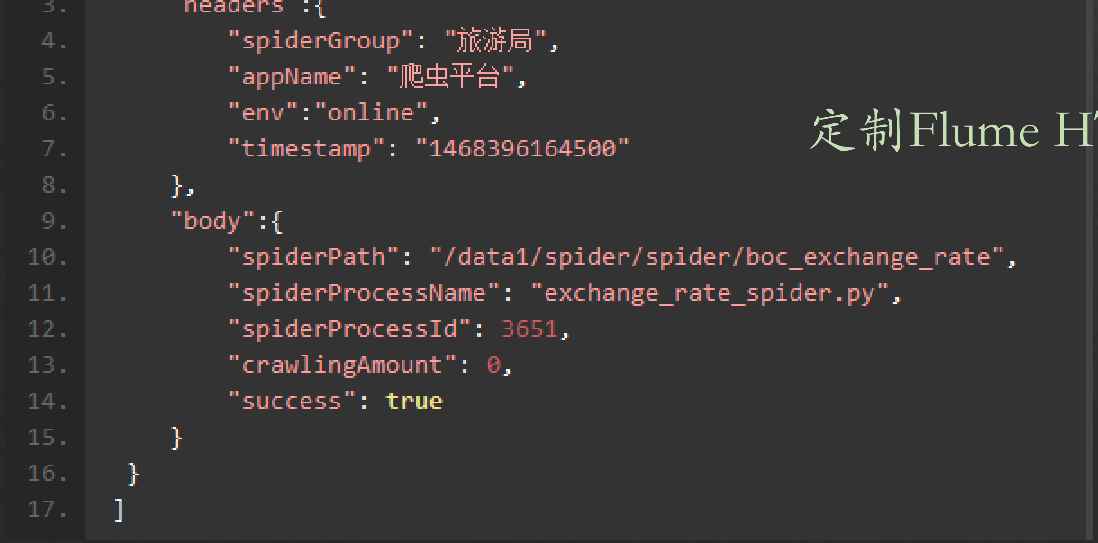
实时日志

ALL ALL

```
2019-09-18 17:08:26||ThreadPoolTaskScheduler-54||ERROR||com.bbd.esalert.service.ApplogsService:102||执行请求失败！ 结果值为null。 /appkafkalogs-*/_search ||
2019-09-18 17:08:31||ThreadPoolTaskScheduler-54||ERROR||com.bbd.esalert.service.ApplogsService:102||执行请求失败！ 结果值为null。 /appkafkalogs-*/_search ||
2019-09-18 17:08:31||ThreadPoolTaskScheduler-54||ERROR||com.bbd.esalert.service.ApplogsService:102||执行请求失败！ 结果值为null。 /appkafkalogs-*/_search ||
2019-09-18 17:08:31||ThreadPoolTaskScheduler-54||ERROR||com.bbd.esalert.service.ApplogsService:102||执行请求失败！ 结果值为null。 /appkafkalogs-*/_search ||
2019-09-18 17:08:31||ThreadPoolTaskScheduler-54||ERROR||com.bbd.esalert.service.ApplogsService:102||执行请求失败！ 结果值为null。 /appkafkalogs-*/_search ||
2019-09-18 17:08:36||ThreadPoolTaskScheduler-54||ERROR||com.bbd.esalert.service.ApplogsService:102||执行请求失败！ 结果值为null。 /appkafkalogs-*/_search ||
2019-09-18 17:08:36||ThreadPoolTaskScheduler-54||ERROR||com.bbd.esalert.service.ApplogsService:102||执行请求失败！ 结果值为null。 /appkafkalogs-*/_search ||
2019-09-18 17:08:36||ThreadPoolTaskScheduler-54||ERROR||com.bbd.esalert.service.ApplogsService:102||执行请求失败！ 结果值为null。 /appkafkalogs-*/_search ||
2019-09-18 17:08:40||ThreadPoolTaskScheduler-4||INFO||com.bbd.esalert.service.AssetCacheService:80||start to load asset info... ||
2019-09-18 17:08:40||ThreadPoolTaskScheduler-79||INFO||com.bbd.esalert.service.ElasticSearchService:66||schedule to fetch es metrics. ||
2019-09-18 17:08:40||ThreadPoolTaskScheduler-55||INFO||com.bbd.esalert.service.AppMetadataService:108||定期刷新应用元数据缓存. ||
2019-09-18 17:08:36||ThreadPoolTaskScheduler-54||ERROR||com.bbd.esalert.service.ApplogsService:102||执行请求失败！ 结果值为null。 /appkafkalogs-*/_search ||
2019-09-18 17:08:40||ThreadPoolTaskScheduler-55||INFO||com.bbd.esalert.service.AppMetadataService:58||开始远程加载应用元数据信息... ||
2019-09-18 17:08:40||ThreadPoolTaskScheduler-69||INFO||com.bbd.esalert.service.SystemMonitorService:448||request net info took time: 419 ||
2019-09-18 17:08:40||ThreadPoolTaskScheduler-79||INFO||com.bbd.esalert.service.ElasticSearchService:72||fetch es metrics finished. ||
2019-09-18 17:08:40||ThreadPoolTaskScheduler-4||INFO||com.bbd.esalert.service.AssetCacheService:106||load asset info successed. ||
2019-09-18 17:08:41||ThreadPoolTaskScheduler-33||ERROR||com.bbd.esalert.service.ApplogsService:102||执行请求失败！ 结果值为null。 /appkafkalogs-*/_search ||
```

爬虫Metrics上报统计

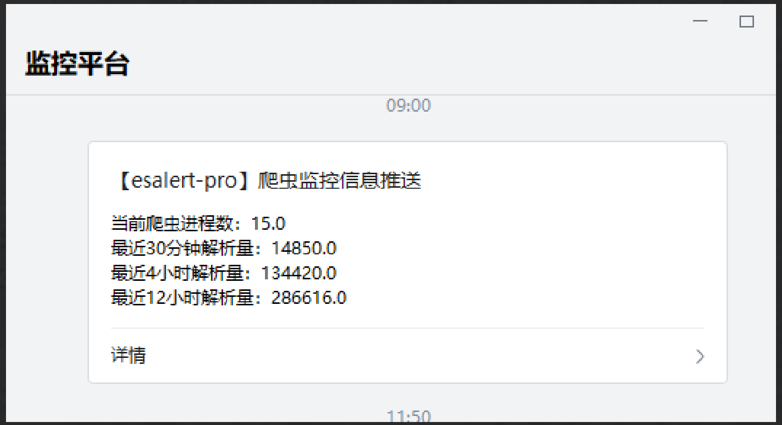




```
[
 {
    "headers":{
        "spiderGroup": "旅游局",
        "appName": "爬虫平台",
        "env":"online",
        "timestamp": "1468396164500"
    },
    "body":{
        "spiderPath": "/data1/spider/spider/boc_exchange_rate",
        "spiderProcessName": "exchange_rate_spider.py",
        "spiderProcessId": 3651,
        "crawlingAmount": 0,
        "success": true
    }
 }
]
```

定制Flume HTTP Source

企业微信告警通知



监控平台

09:00

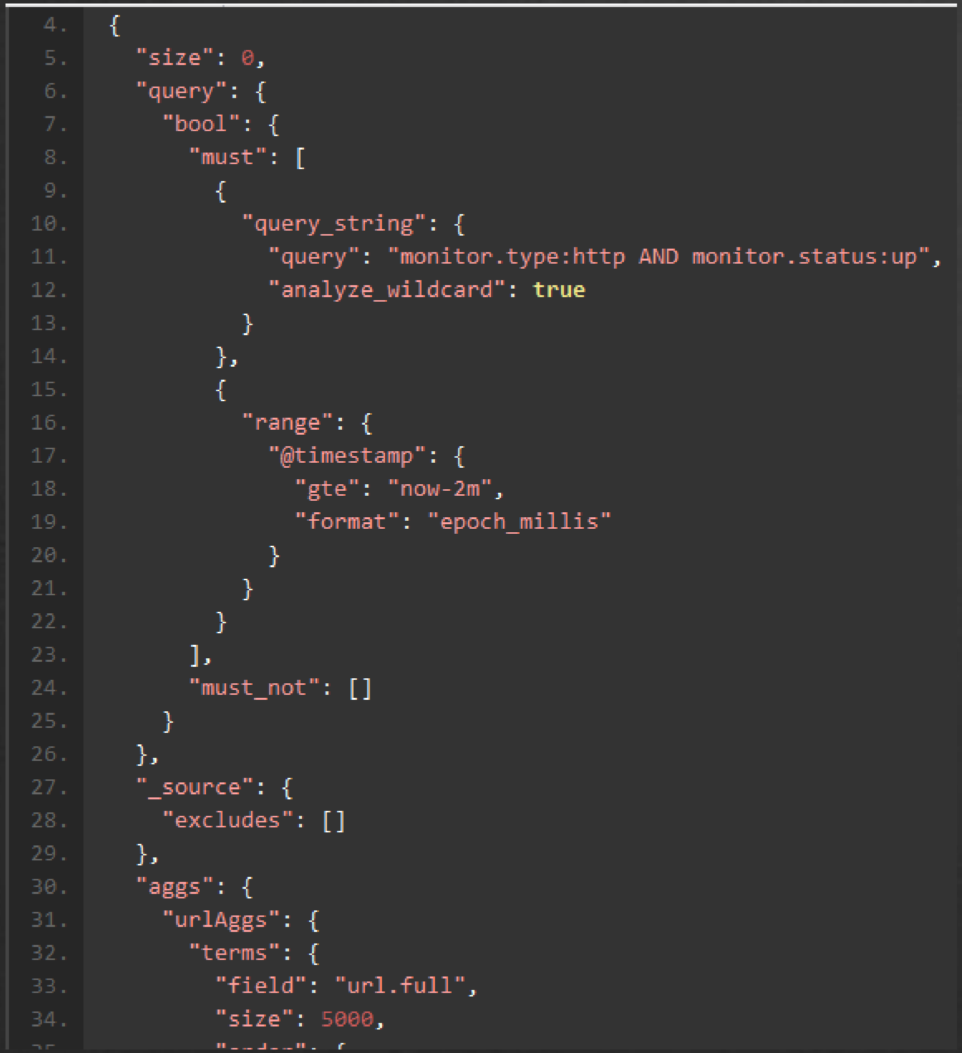
【esalert-pro】爬虫监控信息推送

当前爬虫进程数：15.0
最近30分钟解析量：14850.0
最近4小时解析量：134420.0
最近12小时解析量：286616.0

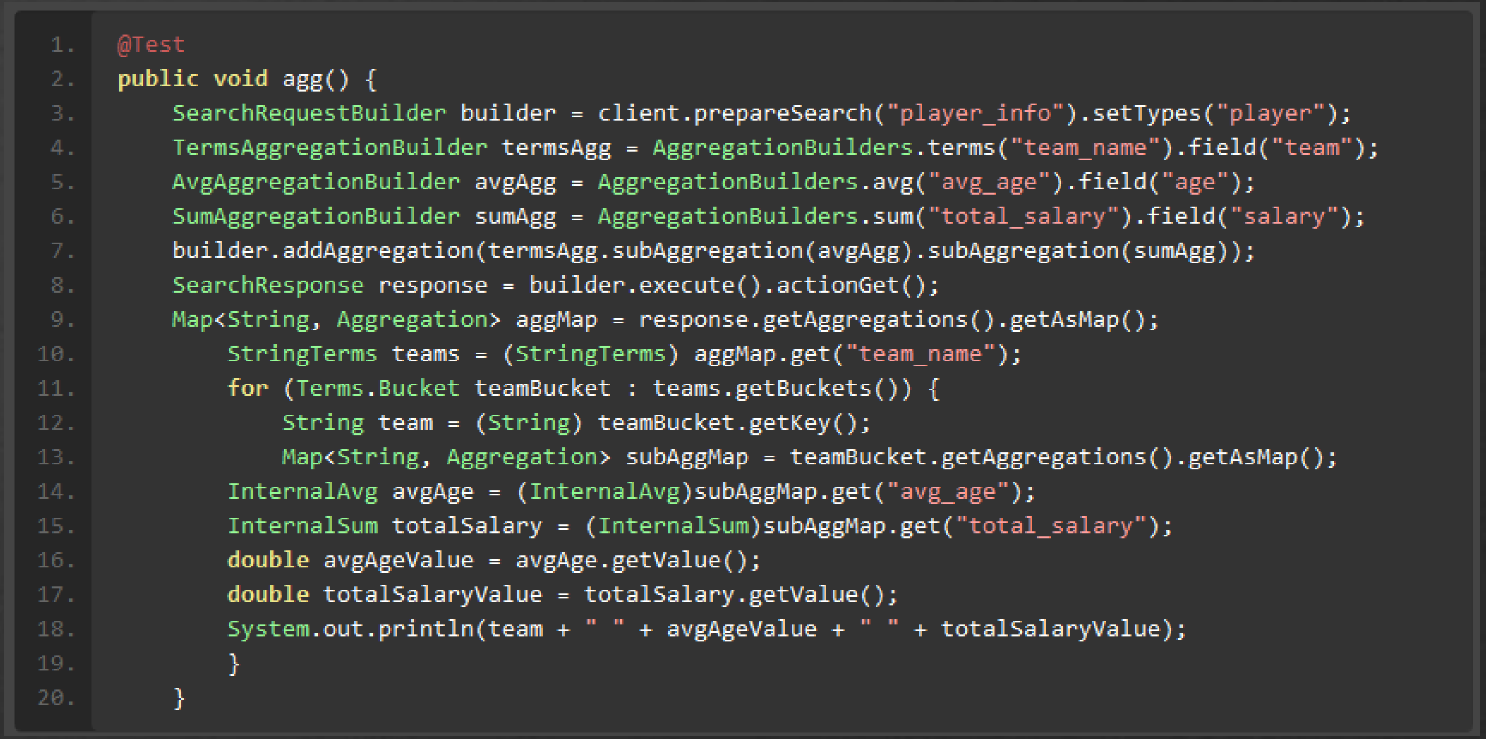
详情

11:50

ElasticSearch Query DSL



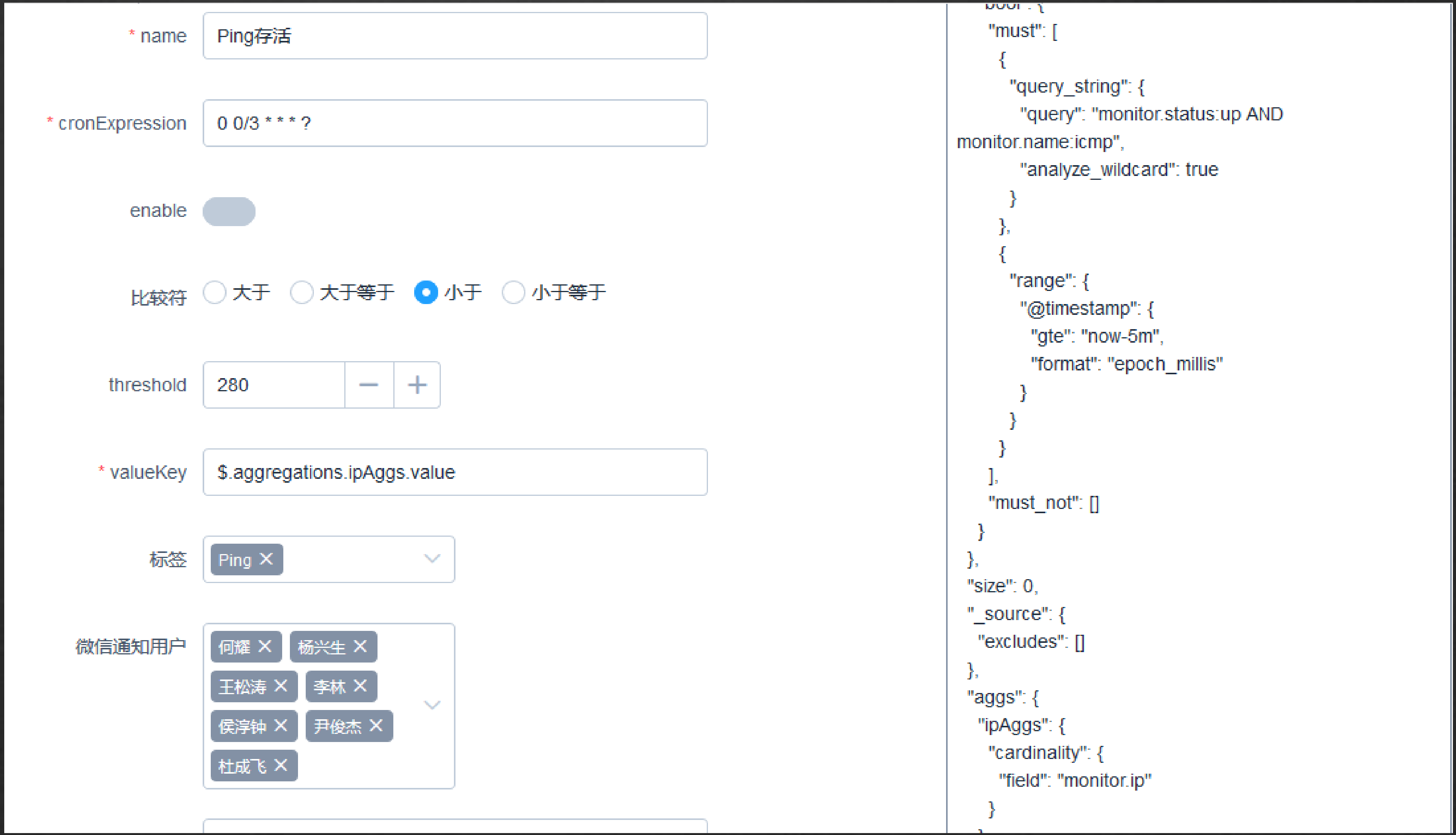
```
{
  "size": 0,
  "query": {
    "bool": {
      "must": [
        {
          "query_string": {
            "query": "monitor.type:http AND monitor.status:up",
            "analyze_wildcard": true
          }
        },
        {
          "range": {
            "@timestamp": {
              "gte": "now-2m",
              "format": "epoch_millis"
            }
          }
        }
      ],
      "must_not": []
    }
  },
  "_source": {
    "excludes": []
  },
  "aggs": {
    "urlAggs": {
      "terms": {
        "field": "url.full",
        "size": 5000,
        "order": {
```



```
@Test
public void agg() {
    SearchRequestBuilder builder = client.prepareSearch("player_info").setTypes("player");
    TermsAggregationBuilder termsAgg = AggregationBuilders.terms("team_name").field("team");
    AvgAggregationBuilder avgAgg = AggregationBuilders.avg("avg_age").field("age");
    SumAggregationBuilder sumAgg = AggregationBuilders.sum("total_salary").field("salary");
    builder.addAggregation(termsAgg.subAggregation(avgAgg).subAggregation(sumAgg));
    SearchResponse response = builder.execute().actionGet();
    Map<String, Aggregation> aggMap = response.getAggregations().getAsMap();
        StringTerms teams = (StringTerms) aggMap.get("team_name");
        for (Terms.Bucket teamBucket : teams.getBuckets()) {
            String team = (String) teamBucket.getKey();
            Map<String, Aggregation> subAggMap = teamBucket.getAggregations().getAsMap();
        InternalAvg avgAge = (InternalAvg)subAggMap.get("avg_age");
        InternalSum totalSalary = (InternalSum)subAggMap.get("total_salary");
        double avgAgeValue = avgAge.getValue();
        double totalSalaryValue = totalSalary.getValue();
        System.out.println(team + " " + avgAgeValue + " " + totalSalaryValue);
        }
    }
```

- 可读性更强、原生支持
- 便于验证、调试

ElasticSearch DSL



* name: Ping存活

* cronExpression: 0 0/3 * * * ?

enable

比较符: ○ 大于 ○ 大于等于 ● 小于 ○ 小于等于

threshold: 280

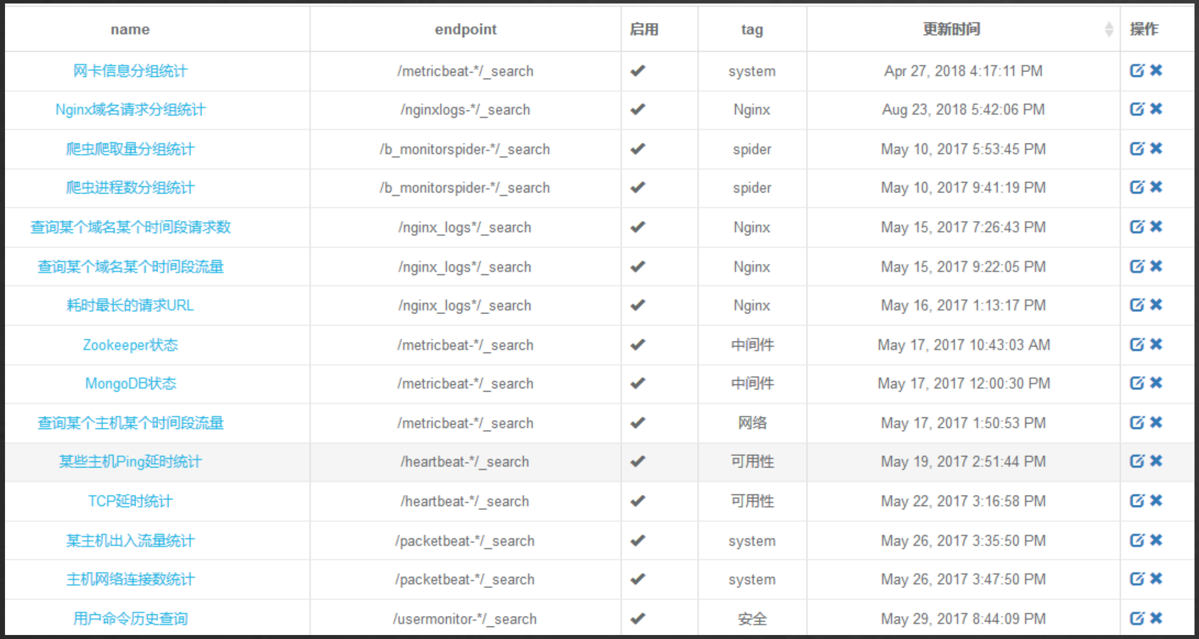
* valueKey: $.aggregations.ipAggs.value

标签: Ping ✕

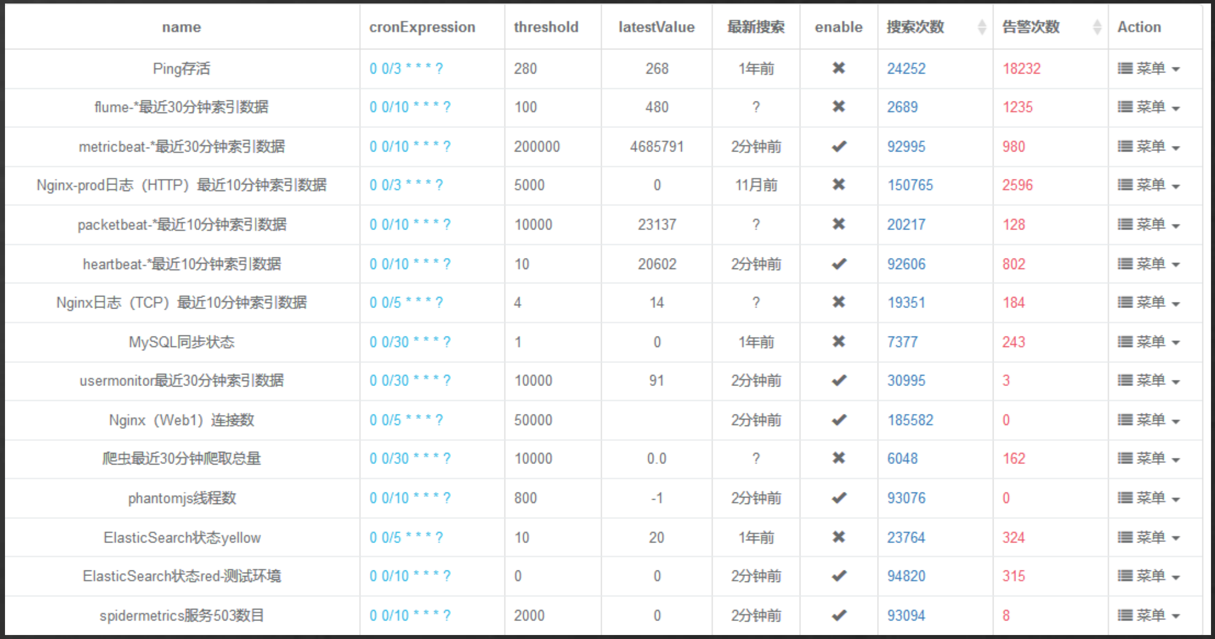
微信通知用户: 何耀 ✕ 杨兴生 ✕ 王松涛 ✕ 李林 ✕ 侯淳钟 ✕ 尹俊杰 ✕ 杜成飞 ✕

```
    "bool": {
      "must": [
        {
          "query_string": {
            "query": "monitor.status:up AND
monitor.name:icmp",
            "analyze_wildcard": true
          }
        },
        {
          "range": {
            "@timestamp": {
              "gte": "now-5m",
              "format": "epoch_millis"
            }
          }
        }
      ],
      "must_not": []
    }
  },
  "size": 0,
  "_source": {
    "excludes": []
  },
  "aggs": {
    "ipAggs": {
      "cardinality": {
        "field": "monitor.ip"
      }
```

ElasticSearch DSL



name	endpoint	启用	tag	更新时间	操作
网卡信息分组统计	/metricbeat-*/_search	✓	system	Apr 27, 2018 4:17:11 PM	✎ ✗
Nginx域名请求分组统计	/nginxlogs-*/_search	✓	Nginx	Aug 23, 2018 5:42:06 PM	✎ ✗
爬虫爬取量分组统计	/b_monitorspider-*/_search	✓	spider	May 10, 2017 5:53:45 PM	✎ ✗
爬虫进程数分组统计	/b_monitorspider-*/_search	✓	spider	May 10, 2017 9:41:19 PM	✎ ✗
查询某个域名某个时间段请求数	/nginx_logs*/_search	✓	Nginx	May 15, 2017 7:26:43 PM	✎ ✗
查询某个域名某个时间段流量	/nginx_logs*/_search	✓	Nginx	May 15, 2017 9:22:05 PM	✎ ✗
耗时最长的请求URL	/nginx_logs*/_search	✓	Nginx	May 16, 2017 1:13:17 PM	✎ ✗
Zookeeper状态	/metricbeat-*/_search	✓	中间件	May 17, 2017 10:43:03 AM	✎ ✗
MongoDB状态	/metricbeat-*/_search	✓	中间件	May 17, 2017 12:00:30 PM	✎ ✗
查询某个主机某个时间段流量	/metricbeat-*/_search	✓	网络	May 17, 2017 1:50:53 PM	✎ ✗
某些主机Ping延时统计	/heartbeat-*/_search	✓	可用性	May 19, 2017 2:51:44 PM	✎ ✗
TCP延时统计	/heartbeat-*/_search	✓	可用性	May 22, 2017 3:16:58 PM	✎ ✗
某主机出入流量统计	/packetbeat-*/_search	✓	system	May 26, 2017 3:35:50 PM	✎ ✗
主机网络连接数统计	/packetbeat-*/_search	✓	system	May 26, 2017 3:47:50 PM	✎ ✗
用户命令历史查询	/usermonitor-*/_search	✓	安全	May 29, 2017 8:44:09 PM	✎ ✗

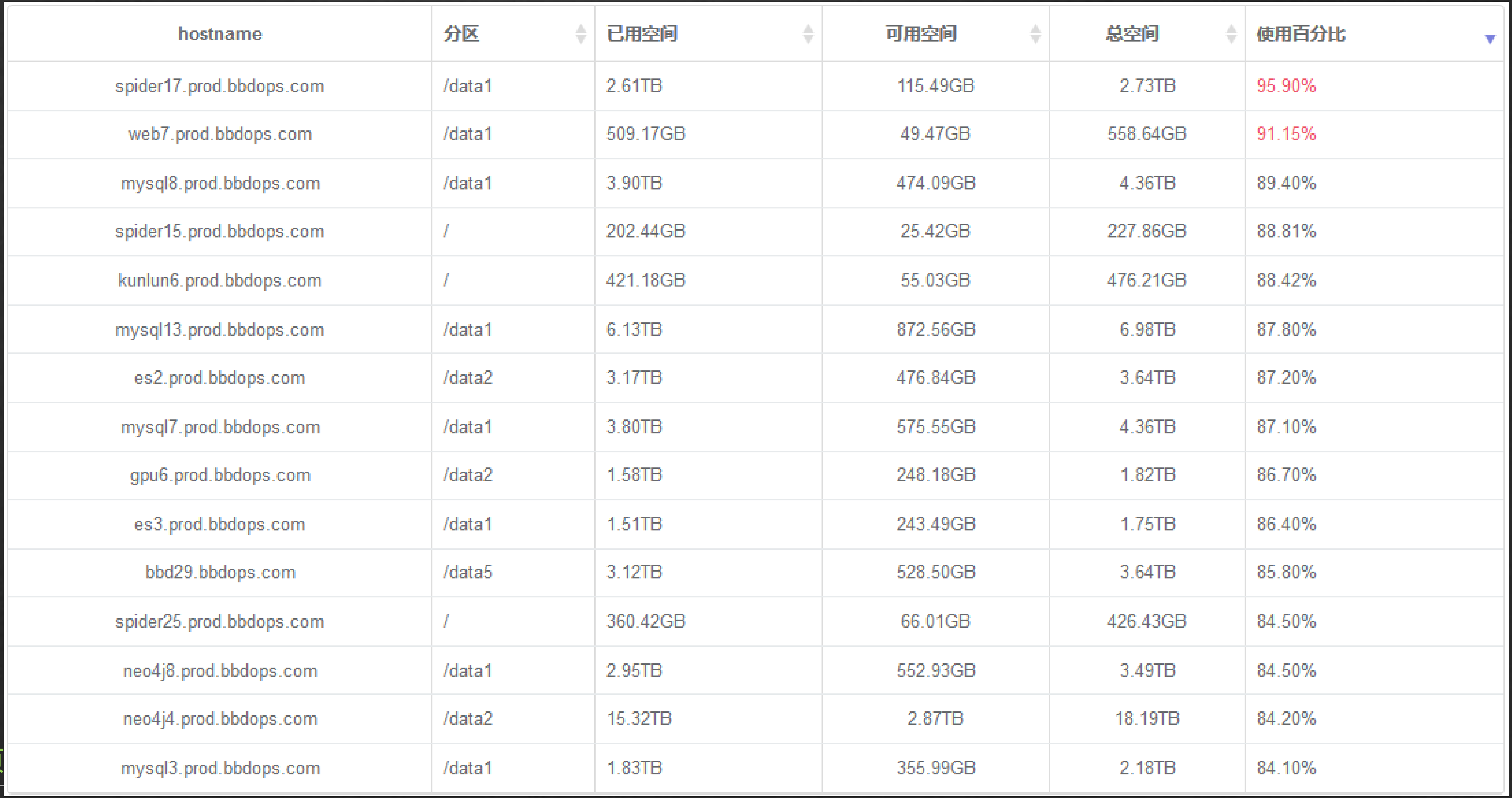


name	cronExpression	threshold	latestValue	最新搜索	enable	搜索次数	告警次数	Action
Ping存活	0 0/3 * * * ?	280	268	1年前	✗	24252	18232	☰ 菜单 ▾
flume-*最近30分钟索引数据	0 0/10 * * * ?	100	480	?	✗	2689	1235	☰ 菜单 ▾
metricbeat-*最近30分钟索引数据	0 0/10 * * * ?	200000	4685791	2分钟前	✓	92995	980	☰ 菜单 ▾
Nginx-prod日志（HTTP）最近10分钟索引数据	0 0/3 * * * ?	5000	0	11月前	✗	150765	2596	☰ 菜单 ▾
packetbeat-*最近10分钟索引数据	0 0/10 * * * ?	10000	23137	?	✗	20217	128	☰ 菜单 ▾
heartbeat-*最近10分钟索引数据	0 0/10 * * * ?	10	20602	2分钟前	✓	92606	802	☰ 菜单 ▾
Nginx日志（TCP）最近10分钟索引数据	0 0/5 * * * ?	4	14	?	✗	19351	184	☰ 菜单 ▾
MySQL同步状态	0 0/30 * * * ?	1	0	1年前	✗	7377	243	☰ 菜单 ▾
usermonitor最近30分钟索引数据	0 0/30 * * * ?	10000	91	2分钟前	✓	30995	3	☰ 菜单 ▾
Nginx（Web1）连接数	0 0/5 * * * ?	50000		2分钟前	✓	185582	0	☰ 菜单 ▾
爬虫最近30分钟爬取总量	0 0/30 * * * ?	10000	0.0	?	✗	6048	162	☰ 菜单 ▾
phantomjs线程数	0 0/10 * * * ?	800	-1	2分钟前	✓	93076	0	☰ 菜单 ▾
ElasticSearch状态yellow	0 0/5 * * * ?	10	20	1年前	✗	23764	324	☰ 菜单 ▾
ElasticSearch状态red-测试环境	0 0/10 * * * ?	0	0	2分钟前	✓	94820	315	☰ 菜单 ▾
spidermetrics服务503数目	0 0/10 * * * ?	2000	0	2分钟前	✓	93094	8	☰ 菜单 ▾

ElasticSearch Query DSL

Alert Definition

ElasticSearch DSL



hostname	分区	已用空间	可用空间	总空间	使用百分比
spider17.prod.bbdops.com	/data1	2.61TB	115.49GB	2.73TB	95.90%
web7.prod.bbdops.com	/data1	509.17GB	49.47GB	558.64GB	91.15%
mysql8.prod.bbdops.com	/data1	3.90TB	474.09GB	4.36TB	89.40%
spider15.prod.bbdops.com	/	202.44GB	25.42GB	227.86GB	88.81%
kunlun6.prod.bbdops.com	/	421.18GB	55.03GB	476.21GB	88.42%
mysql13.prod.bbdops.com	/data1	6.13TB	872.56GB	6.98TB	87.80%
es2.prod.bbdops.com	/data2	3.17TB	476.84GB	3.64TB	87.20%
mysql7.prod.bbdops.com	/data1	3.80TB	575.55GB	4.36TB	87.10%
gpu6.prod.bbdops.com	/data2	1.58TB	248.18GB	1.82TB	86.70%
es3.prod.bbdops.com	/data1	1.51TB	243.49GB	1.75TB	86.40%
bbd29.bbdops.com	/data5	3.12TB	528.50GB	3.64TB	85.80%
spider25.prod.bbdops.com	/	360.42GB	66.01GB	426.43GB	84.50%
neo4j8.prod.bbdops.com	/data1	2.95TB	552.93GB	3.49TB	84.50%
neo4j4.prod.bbdops.com	/data2	15.32TB	2.87TB	18.19TB	84.20%
mysql3.prod.bbdops.com	/data1	1.83TB	355.99GB	2.18TB	84.10%

开源计划

- ElasticSearch Query DSL Repository
- ES Alert
- ~~多集群管理~~
- 基于Google Flutter的运维管理APP
- 自动化发布
- CMDB

开

源

谢谢大家

BBD运维团队欢迎您的加入！

何耀