elastic | 中国开发者大会

ELK日志系统分享

Alex Chen
Omniwaresoft



战略级赞助商 HUAWEI | 钻石级赞助商 普翔 | 白金级赞助商 华夏博格 神州数码 Digital China | 金牌级赞助商 iDataAPI

合作伙伴 开源中国 oschina.net 掘金 谱时 IT大咖说 otpub Broadview 百格活动 bagevent.com MAXHUB



ELK日志系统分享

Alex Chen

Technical Director

Omniwaresoft Technology Inc.

Alex.chen@omniwaresoft.com.tw

开放原始码企业级解决方案代理商

Omniwaresoft 歐立威科技股份有限公司 Omniwaresoft Technology Inc.

Who am i ?

- 开源软件爱好使用者
- 十多年程式开发、DBA及系统管理经验
- 从事开源软件企业版本销售、技术支持服务 (Elasticsearch、 MongoDB、 PostgreSQL、 Greenplum、 Hadoop、 Pentaho、 Docker…等)

Contacts: alexc168@gmail.com

alex.chen@omniwaresoft.com.tw



Omniwaresoft 歐立威科技

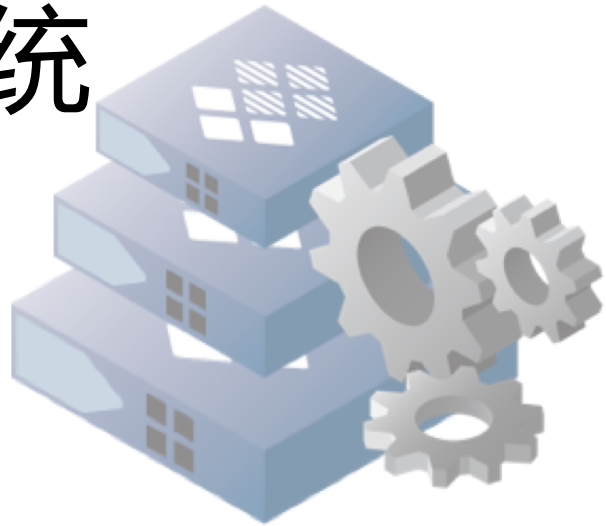
Company Confidential for internal use only

Agenda

- 网路服务管理系统
- 日志管理系统
- 讯息关键字贴标系统



网路服务管理系统



Omni waresoft 歐立威科技

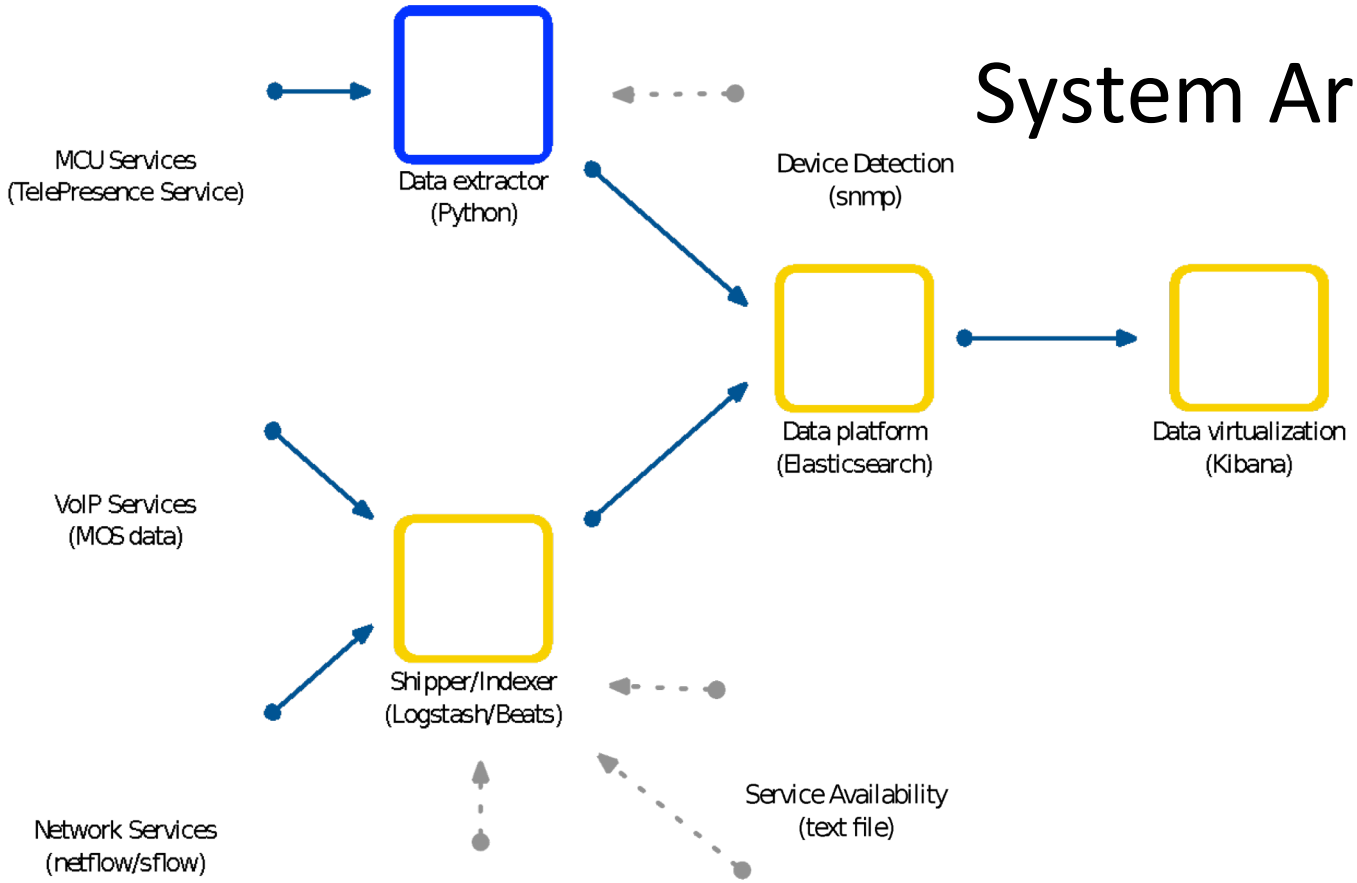
Company Confidential for internal use only

网路管理问题与挑战

- 网路设备种类及型号繁多
  - Cisco、 Dell、 Dlink
- 资讯系统不易整合
  - MRTG、 CA、 Cacti、 Zabbix、 Splunk
- 资料源格式及通讯协定众多
  - SNMP、 Netflow、 sflow、 WebService、 RDBMS、 XML、 CSV
- 资讯单一视图
  - 即时资讯及告警

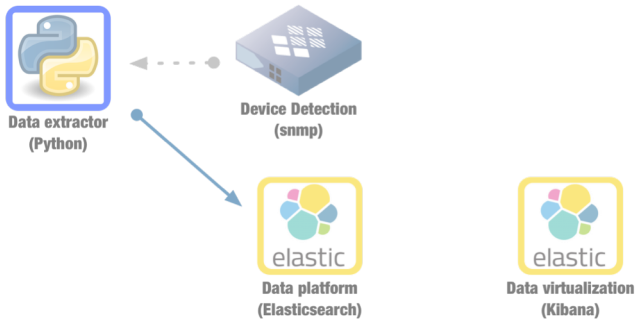


System Architecture



Omni waresoft 歐立威科技
Company Confidential for internal use only

MRTG



- Input: 基于 SNMP 采集数据

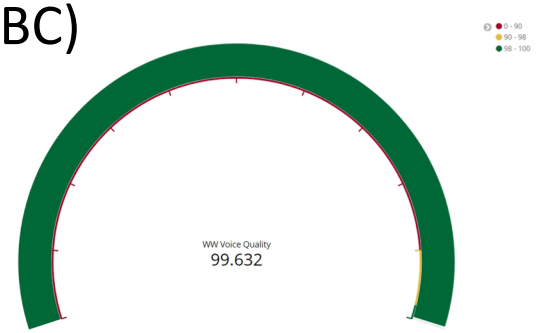


Company Confidential for internal use only

Mean Opinion Score(MOS) for VoIP



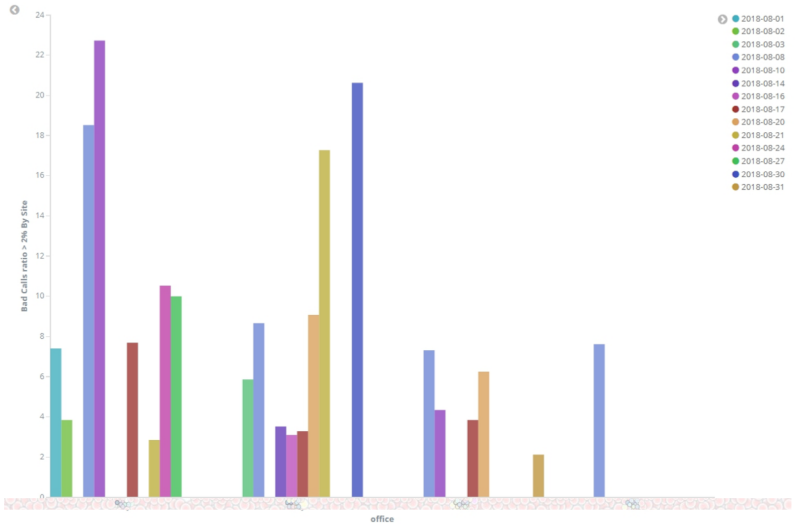
- Input: MSSQL(JDBC)



WW Voice Quality

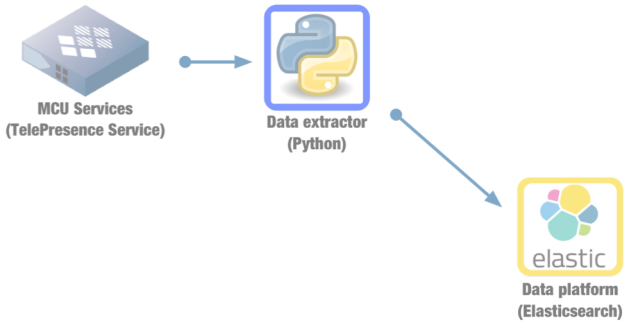
region	01	02	03	04	05	06	07	08	09	10	11	12
[redacted]	-	-	1.137	0.36	0.96	0.49	0.501	0.741	0.511	-	-	-
[redacted]	-	-	0.259	0.201	0.336	0.301	0.639	0.695	0.355	-	-	-
[redacted]	-	-	0.582	0.45	0.322	0.277	0.223	0.282	0.177	-	-	-
			0.544	**0.41**	**0.347**	**0.29**	**0.305**	**0.375**	**0.215**			

Export: Raw Formatted



Company Confidential for internal use only

Conference voice quality



- Input: Telepresence Service

Site	DateTime	Audio_Bad_Call_NO	Audio_Call_no	Bad_Call_Ratio%
[redacted]	20180719	0	5	0%
[redacted]	20180719	0	2	0%
[redacted]	20180719	0	7	0%
[redacted]	20180719	0	1	0%
[redacted]	20180719	0	14	0%

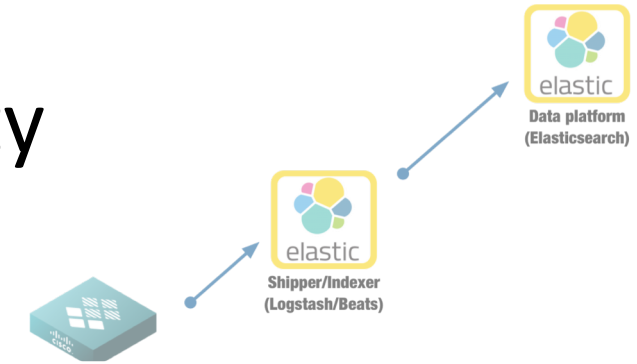
Site	DataTime	Video_Bad_Call_No#	Video_Call_no	Bad_Call_Ratio%
[redacted]	20180719	0	5	0%
[redacted]	20180719	0	2	0%
[redacted]	20180719	0	7	0%
[redacted]	20180719	1	1	100%
[redacted]	20180719	0	14	0%

Site	DataTime	Webex_Audio_Bad_Call_No#	Webex_Audio_Call_no	Bad_Call_Ratio%
HQ_To_Webex	20180725	8	1,879	0.426%
HQ_To_Webex	20180724	1	730	0.137%
HQ_To_Webex	20180719	0	170	0%
HQ_To_Webex	20180720	0	354	0%
HQ_To_Webex	20180723	0	363	0%

Omniwaresoft 歐立威科技
Company Confidential for internal use only

CA Performance/High Availability

- Input: netflow/sflow



Netflow: Dashboard Navigation

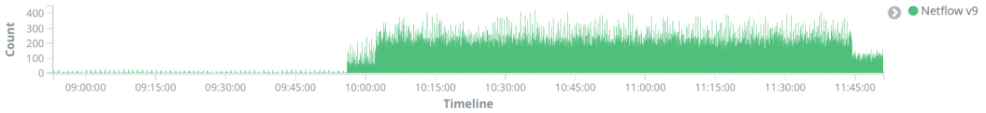
Overview | Conversation Partners | Traffic Analysis | Top-N | Geo Location | Autonomous Systems | Flow Exporters | Raw Flow Records

4

Netflow: Flow Records

1,275,290
Flow Records

Netflow: Flow Records



Netflow: Flow Records

1–50 of 1,275,290

Time	netflow.src_addr	netflow.src_port_name	netflow.dst_addr	netflow.dst_port_name	netflow.protocol_name	netflow.bytes	netflow.packets
October 5th 2018, 11:51:08.000	10.27.131.105	TCP/41028	10.9.2.11	TCP/443 (https)	TCP	373	4
October 5th 2018, 11:51:08.000	172.21.135.99	TCP/8080 (http-alt)	172.25.89.201	TCP/59546	TCP	40	1
October 5th 2018, 11:51:08.000	10.2.67.253	UDP/12366	10.2.1.252	UDP/12346	UDP	160	1
October 5th 2018, 11:51:08.000	10.21.11.199	TCP/3891 (rtc-pm-port)	10.241.1.1	TCP/3260 (iscsi-target)	TCP	224	4
October 5th 2018, 11:51:08.000	10.84.17.150	TCP/63330	10.189.111.116	TCP/445 (microsoft-ds)	TCP	232	4
October 5th 2018, 11:51:08.000	172.21.100.5	TCP/1433 (ms-sql-s)	172.25.89.204	TCP/56780	TCP	132	3
October 5th 2018, 11:51:08.000	10.1.5.249	UDP/161 (snmp)	172.21.140.182	UDP/57130	UDP	80	1
October 5th 2018, 11:51:08.000	10.84.17.165	TCP/59534	10.41.73.150	TCP/445 (microsoft-ds)	TCP	232	4
October 5th 2018, 11:51:08.000	10.84.17.126	TCP/59940	10.65.44.151	TCP/445 (microsoft-ds)	TCP	232	4

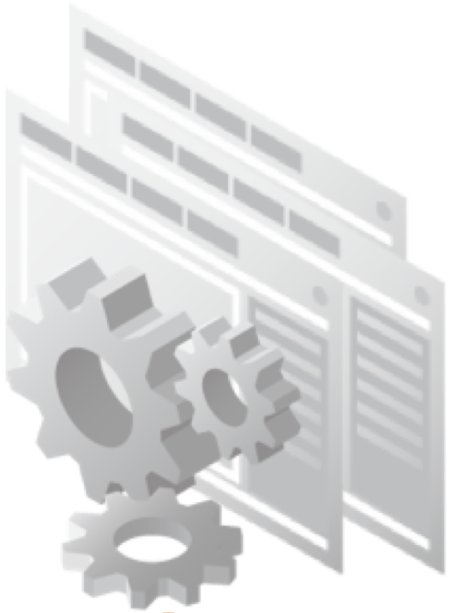
Omni waresoft 歐立威科技

Company Confidential for internal use only

Next step…

- Service Availability (text file)
- SSL VPN Services (text file)
- VDI Services (text file)
- …

日志管理系统



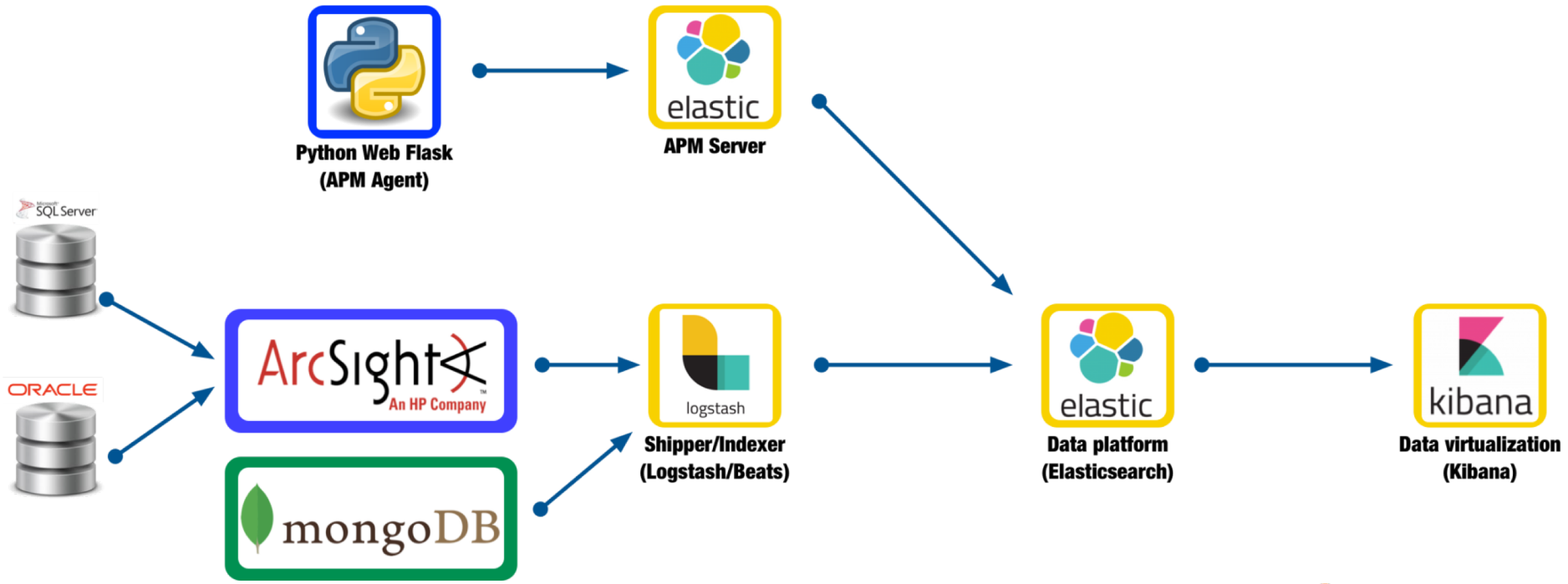
Omni waresoft 歐立威科技

Company Confidential for internal use only

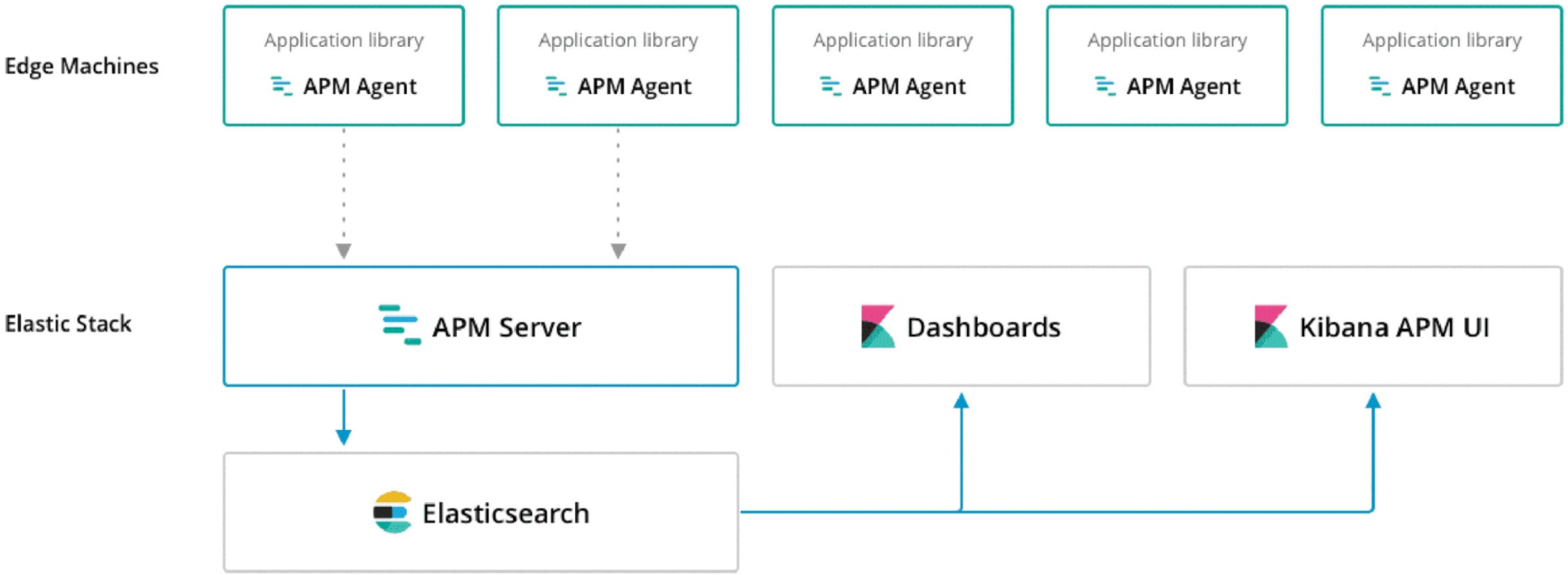
日志管理问题与挑战

- 应用系统效能管理
  - Python Web Flask
- ODS 日志管理种类众多
  - MongoDB logs
  - System logs
  - ARCSight

System Architecture



Elastic APM



Company Confidential for internal use only

APM Server (Linux)

```
1. 下载 APM 封装包，并安装
curl -L -O https://artifacts.elastic.co/downloads/apm-server/apm-server-6.2.0-x86_64.rpm
sudo rpm -vi apm-server-6.2.0-x86_64.rpm

2. 设定 APM index template, dashboards
apm-server setup
```

```
4. 启动 APM 服务
apm-server -e
```

```
3. 设定 APM 组态档
apm-server:

  # Defines the host and port the server is listening on
  host: "localhost:8200"

setup.kibana:

  # Kibana Host
  # Scheme and port can be left out and will be set to the default (http and 5601)
  # In case you specify and additional path, the scheme is required: http://localhost:5601/path
  # IPv6 addresses should always be defined as: https://[2001:db8::1]:5601
  host: "172.16.251.200:5601"

output.elasticsearch:
  # Array of hosts to connect to.
  hosts: ["172.16.251.200:9200"]
```

Omni waresoft 歐立威科技

Company Confidential for internal use only

APM Agent

```
1. 安装 Python APM Agent
pip install elastic-apm[flask]

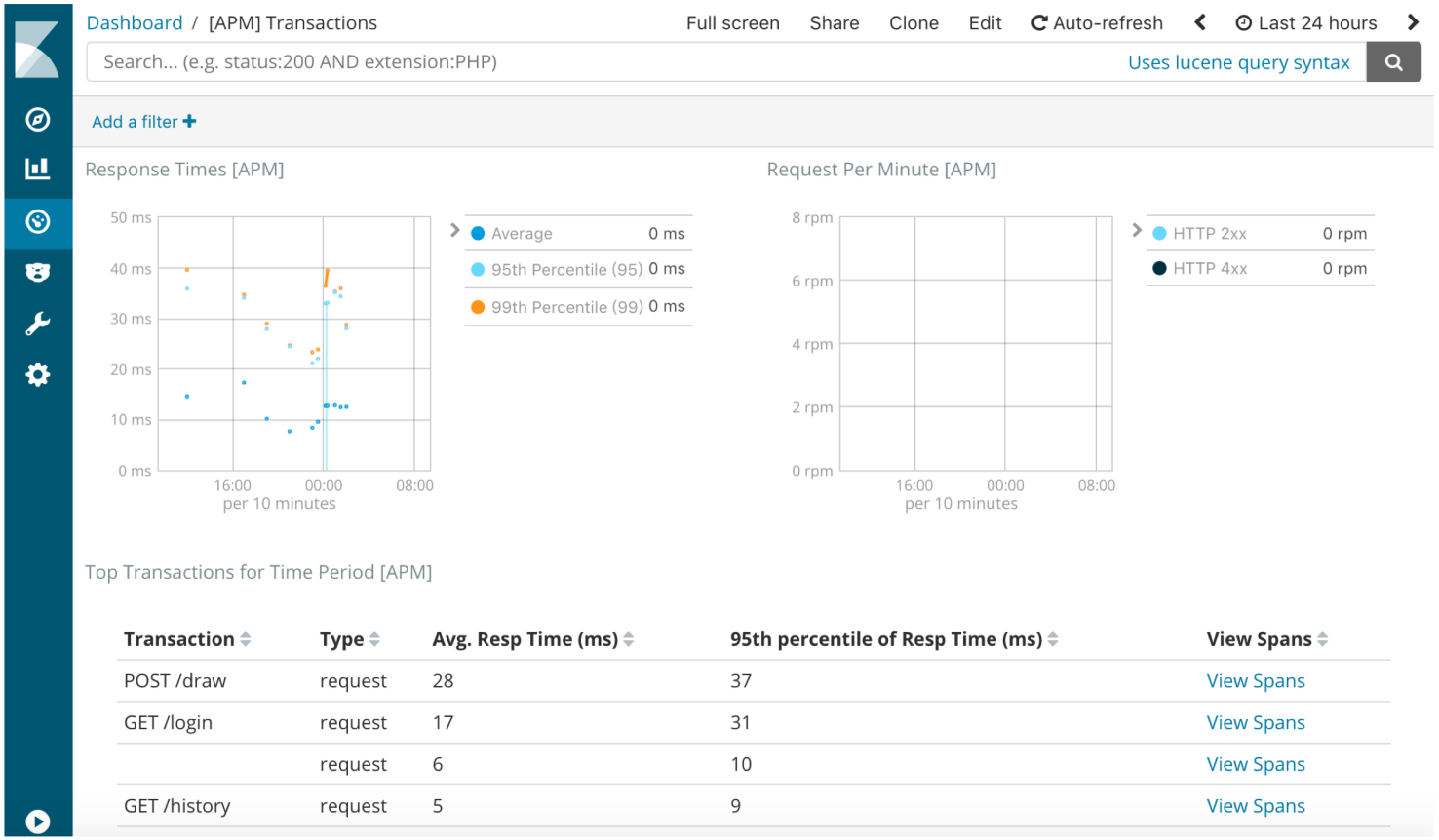

2. 设定 Agent 资讯到程式码
from datetime import datetime
from flask import Flask, g, render_template, request
from elasticapm.contrib.flask import ElasticAPM

app = Flask(__name__)
app.config['ELASTIC_APM'] = {
  'SERVICE_NAME': 'Flask',
  'SERVER_URL': 'http://localhost:8200'  # <--- APM Server
}
apm = ElasticAPM(app)


3. 启动 Flask Web Server
python flaskWSLab.py
```



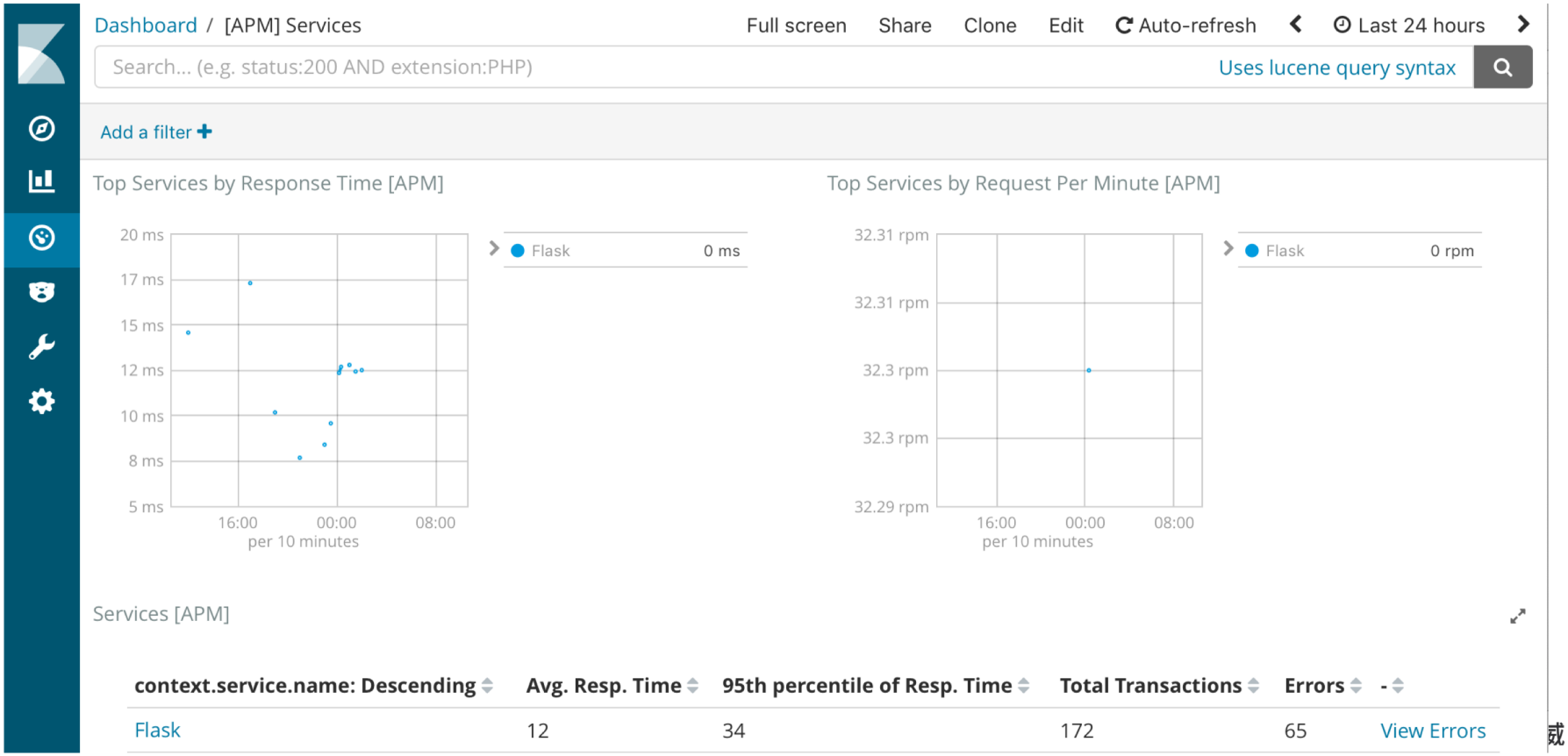
APM Transactions



Transaction	Type	Avg. Resp Time (ms)	95th percentile of Resp Time (ms)	View Spans
POST /draw	request	28	37	View Spans
GET /login	request	17	31	View Spans
	request	6	10	View Spans
GET /history	request	5	9	View Spans

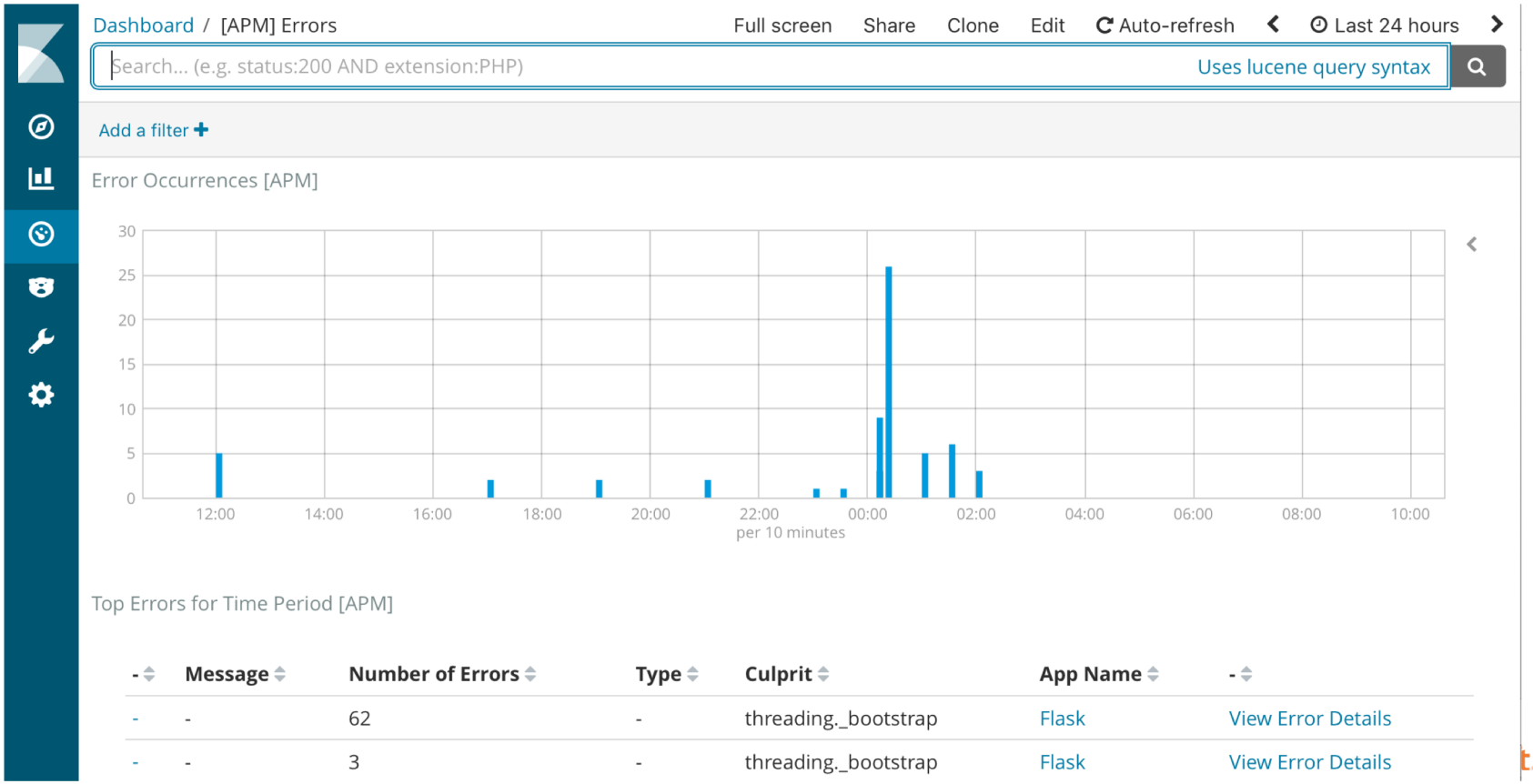
Omni waresoft 歐立威科技
Company Confidential for internal use only

APM Services



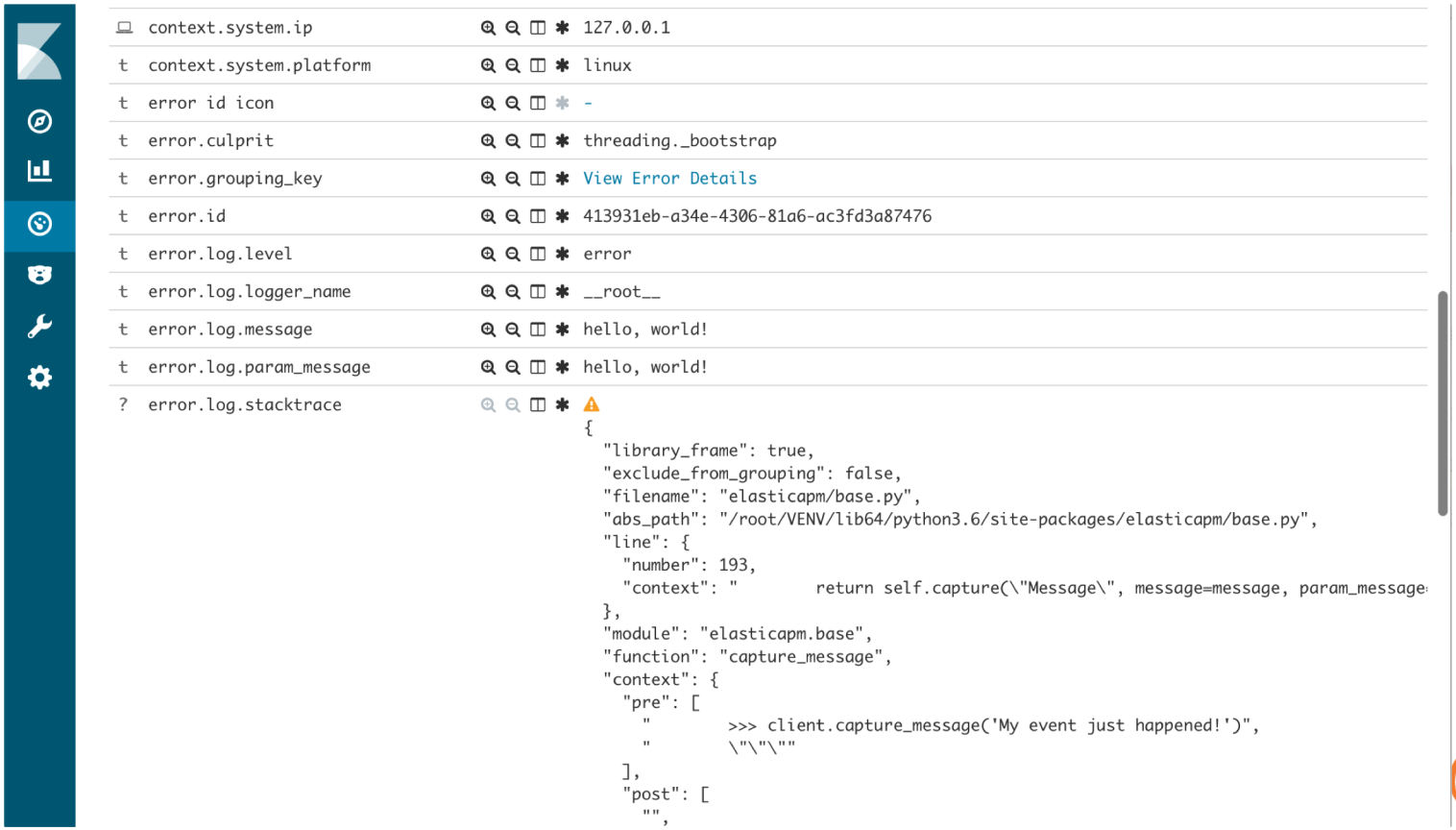
Company Confidential for internal use only

APM Errors



歐立威科技
Company Confidential for internal use only

APM Error Details



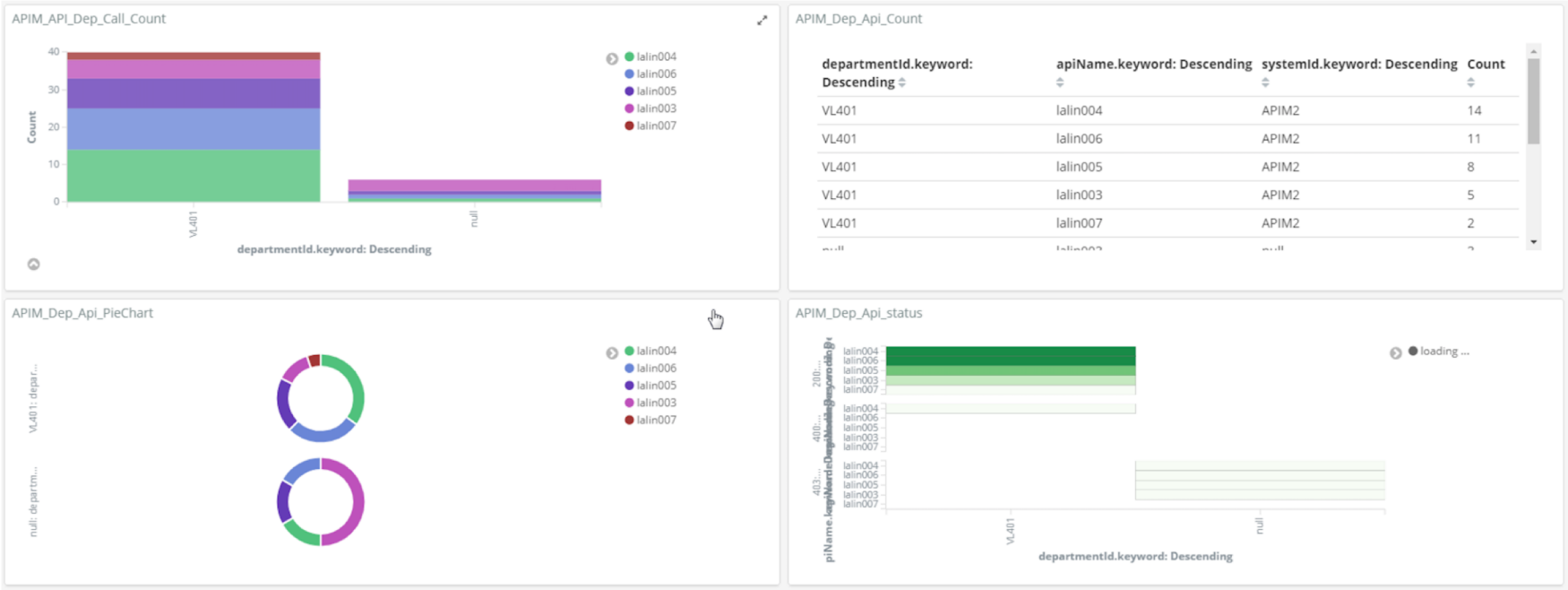
	context.system.ip	127.0.0.1
t	context.system.platform	linux
t	error id icon	-
t	error.culprit	threading._bootstrap
t	error.grouping_key	View Error Details
t	error.id	413931eb-a34e-4306-81a6-ac3fd3a87476
t	error.log.level	error
t	error.log.logger_name	__root__
t	error.log.message	hello, world!
t	error.log.param_message	hello, world!
?	error.log.stacktrace	


```
{
  "library_frame": true,
  "exclude_from_grouping": false,
  "filename": "elasticapm/base.py",
  "abs_path": "/root/VENV/lib64/python3.6/site-packages/elasticapm/base.py",
  "line": {
    "number": 193,
    "context": "        return self.capture(\"Message\", message=message, param_message
  },
  "module": "elasticapm.base",
  "function": "capture_message",
  "context": {
    "pre": [
      "        >>> client.capture_message('My event just happened!')",
      "        \"\"\""
    ],
    "post": [
      "",
```


Omni waresoft 歐立威科技

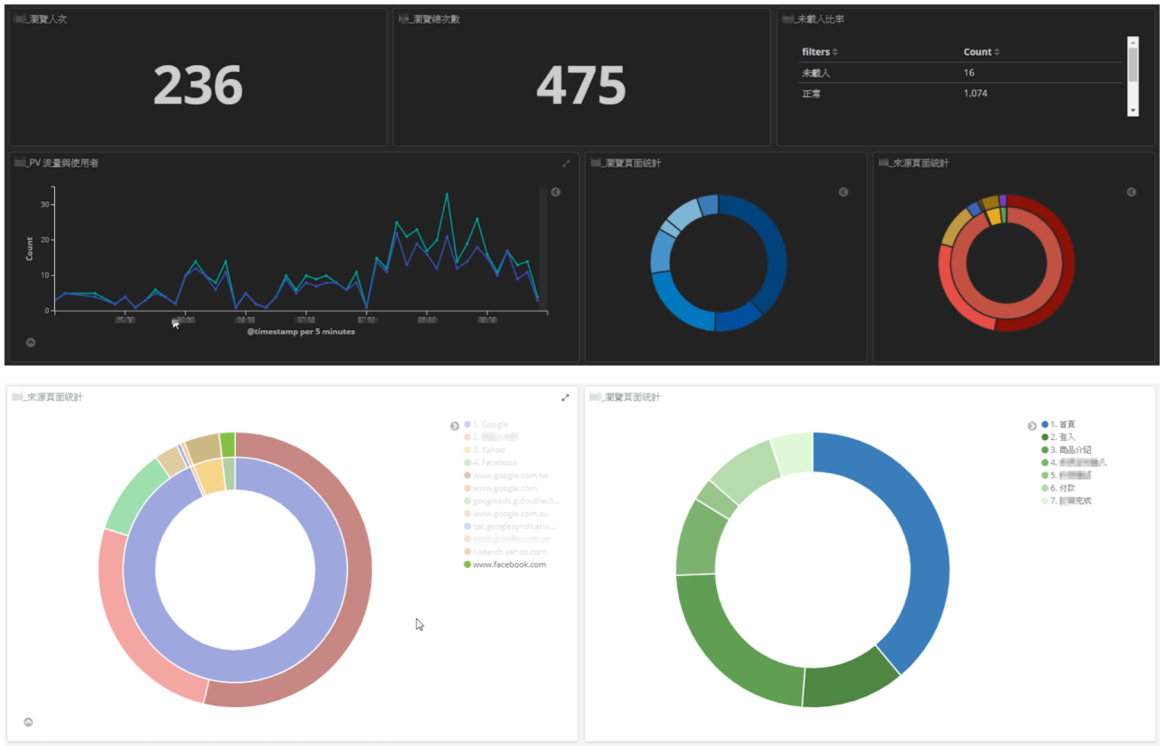
Company Confidential for internal use only

AP Logs



Omniwaresoft 歐立威科技
Company Confidential for internal use only

AP Logs


236
475
filters
Count
未載入
16
正常
1,074
@timestamp per 5 minutes
www.facebook.com

讯息关键字贴标系统



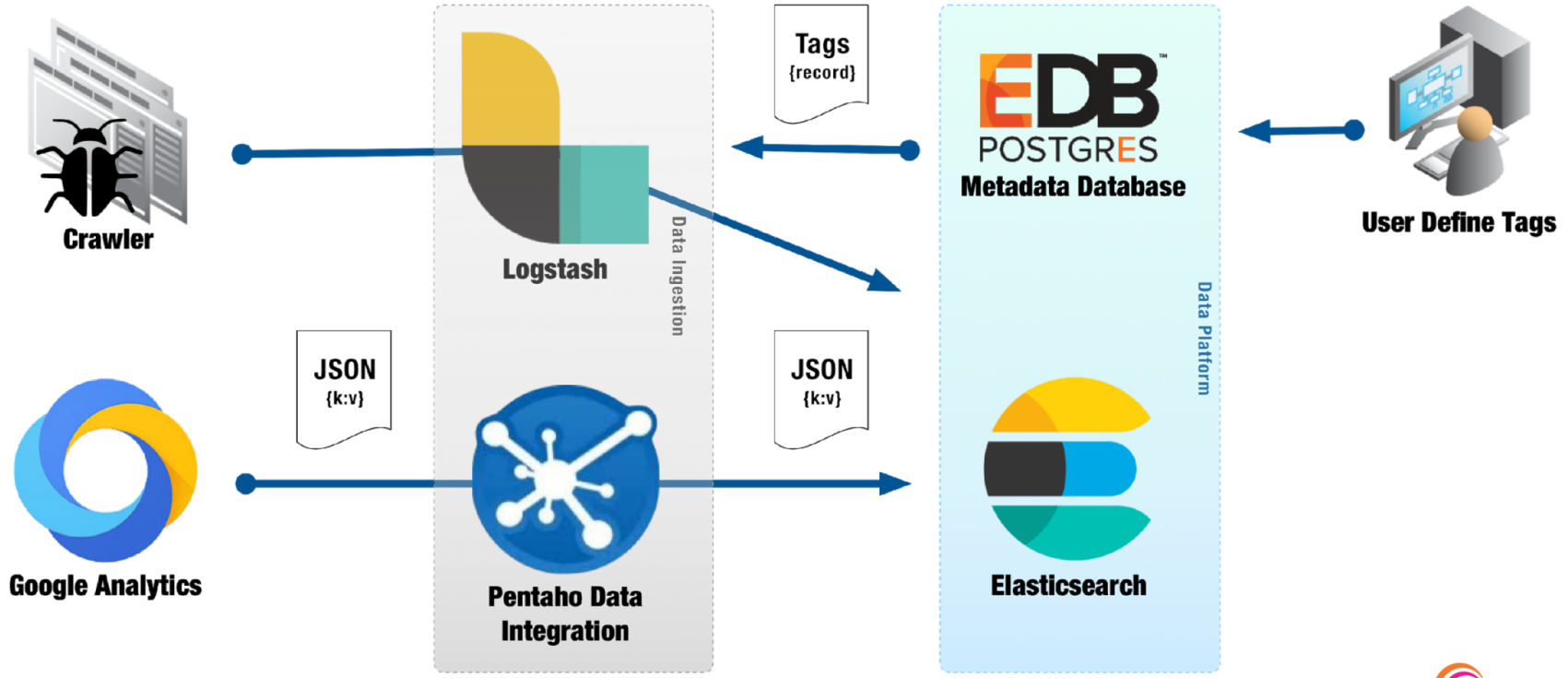
Omniwaresoft 歐立威科技

Company Confidential for internal use only

贴标系统问题与挑战

- 贴标处理时间太长
  - RDBMS Oracle
- 贴标规则不易维护
  - RDBMS: Oracle
  - SQL Statement

System Architecture



貼标管理




```
if [product_name] =~ /Computer|Digital|Camera/ {
    mutate {
        add_field => { "[tag1]" => "3C" }
    }

    if [vendor_name] =~ /Lenovo|Dell|ASUS/ {
        mutate {
            add_field => { "[tag2]" => "Notebook" }
        }
        if [spec_desc] =~ /Intel Core i9|Intel Core i7|AMD Ryzen7|AMD Ryzen5/ {
            mutate {
                id => "CPU"
                add_field => { "[tag3]" => "CPU" }
            }
        } else if [spec_desc] =~ /2GB|4GB|8GB|16GB/ {
            mutate {
                id => "RAM"
                add_field => { "[tag3]" => "RAM" }
            }
        }
    }
}
```

Tag1: 3C

ex: Computer, Digital Camera

Tag2: Notebook

ex: Lenovo,Dell,ASUS

Tag3: CPU

ex: Intel Core i9,
Intel Core i7,
AMD Ryzen 7,
AMD Ryzen 5…

Company Confidential for internal use only



Omni waresoft 歐立威科技
Company Confidential for internal use only



elastic
中文社区

专业、垂直、纯粹的 Elastic 开源技术交流社区
https://elasticsearch.cn/

elastic