



全球运维大会

2016

DevOps 2.0: 重塑运维价值



北京站

会议时间：12月16日 - 12月17日

会议地点：北京国际会议中心

主办单位：



云网络数据分析及应用

张天鹏 CT0@云杉网络



目录



1

云+SDN

2

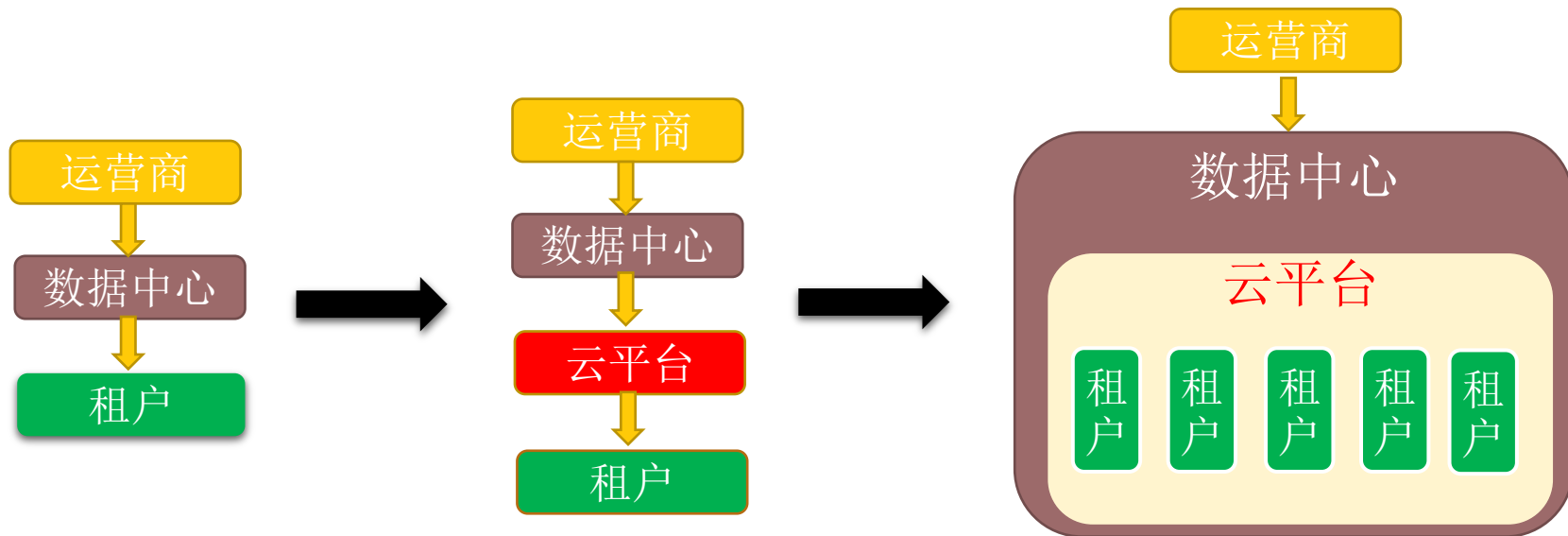
基于Flow的数据分析

3

应用案例

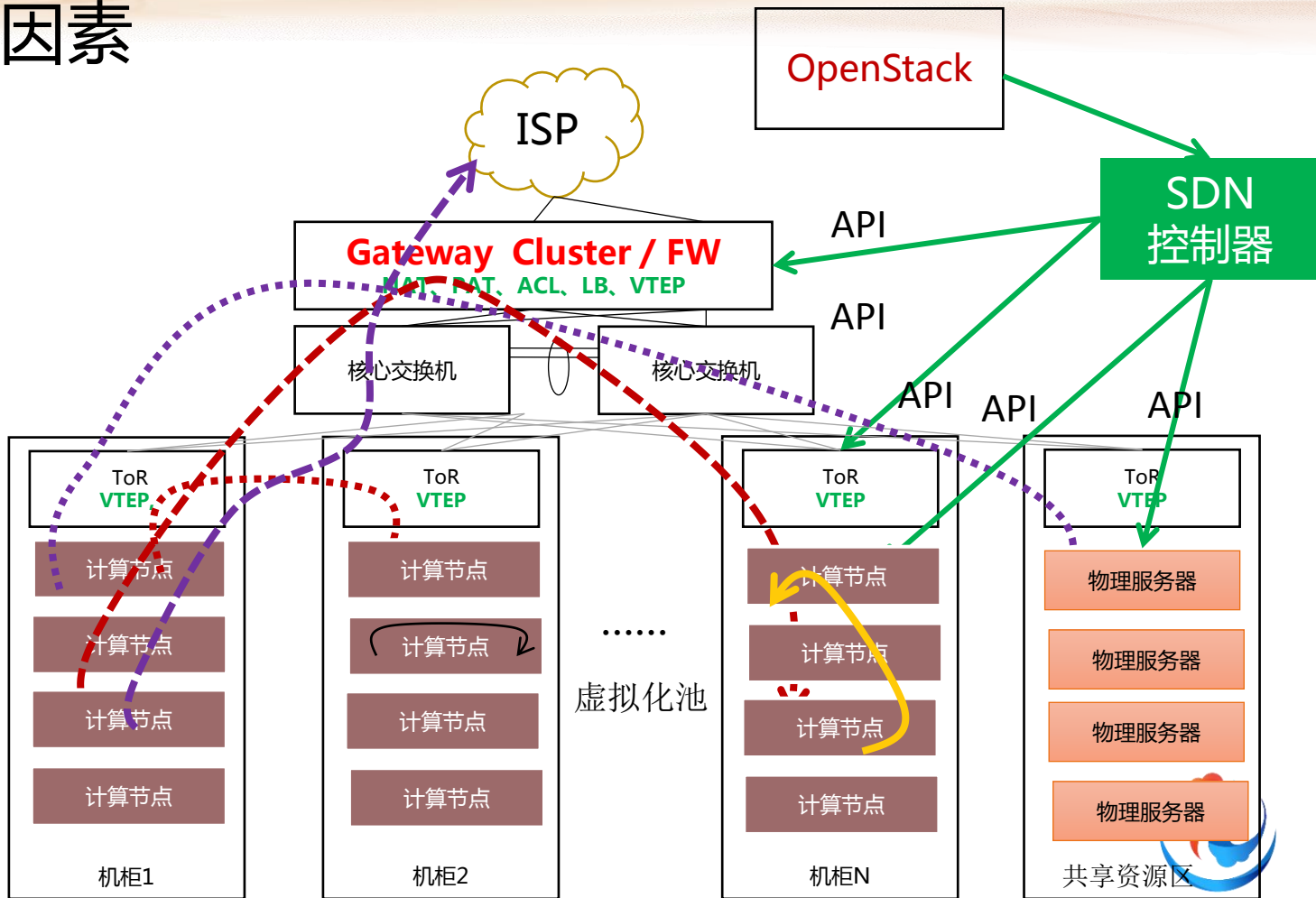


云网络差异

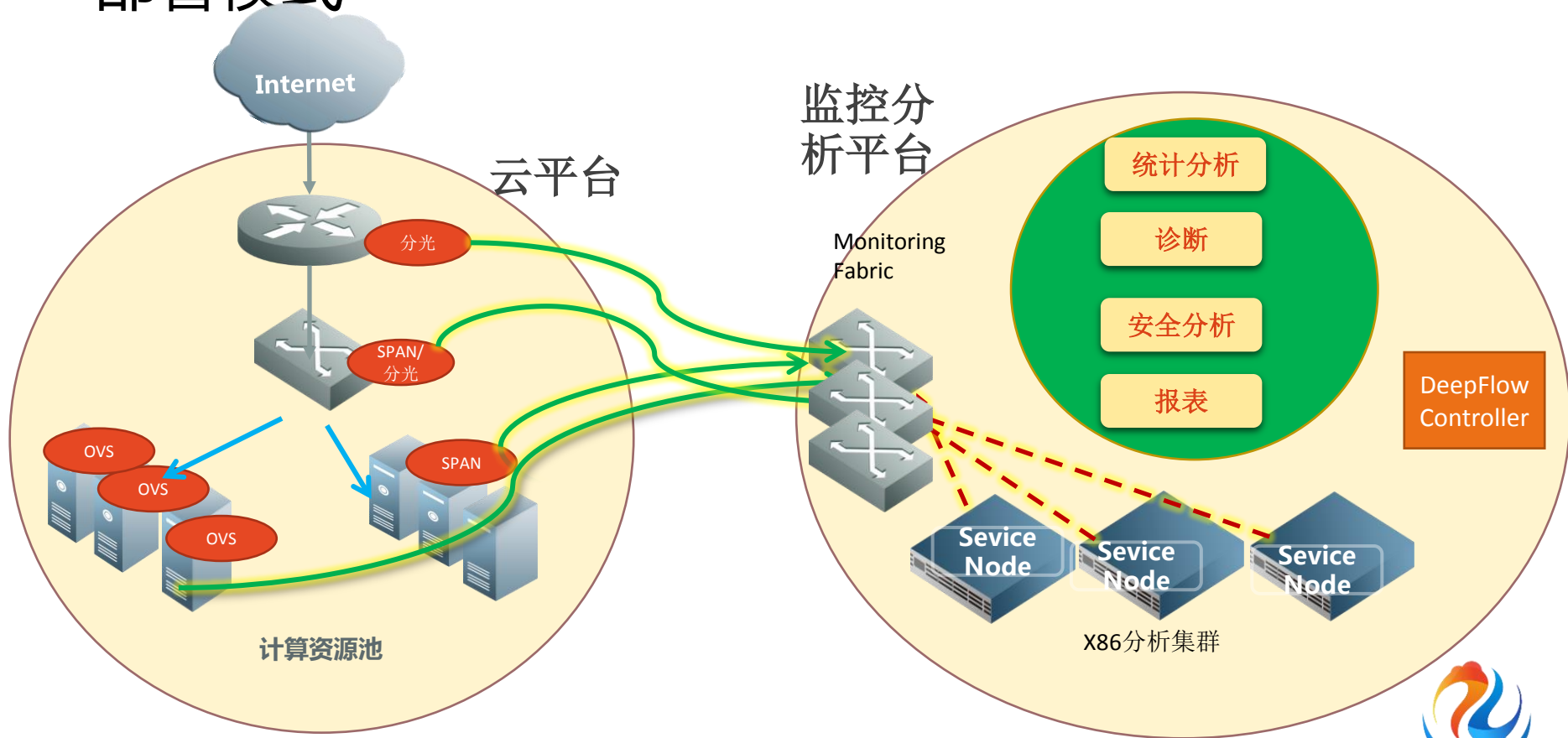


SDN关键因素

Scale问题
VTEP终结点
流量模型



部署模式



目录

1 云+SDN



2 基于Flow的数据分析

3 应用案例



基于Flow的网络分析

➤ 云网络监控困难

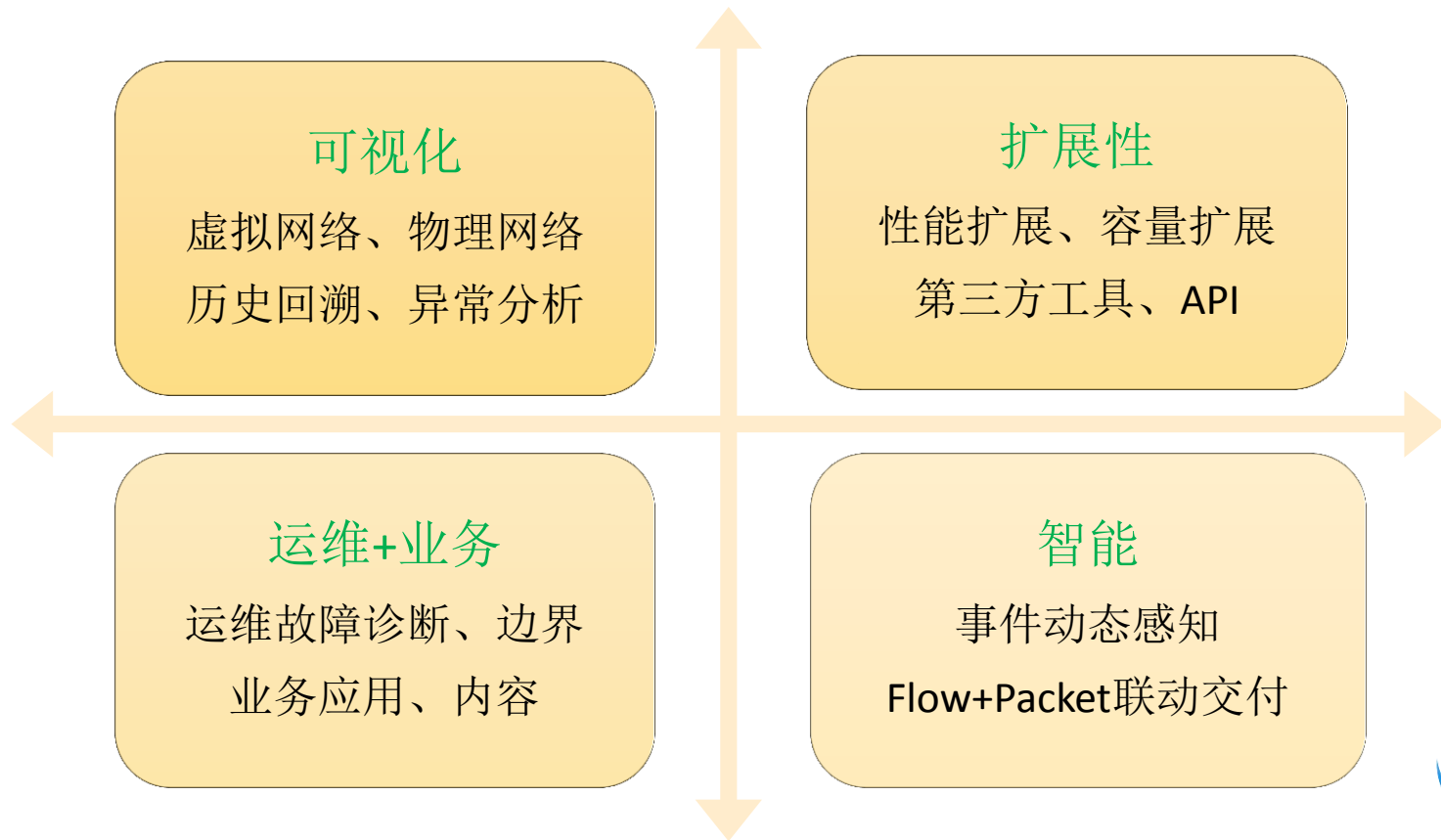
- SFlow、Netflow/IPFIX、分光、镜像
- 数据存储，如何支持海量数据？
- 分析工具如何感知云？虚拟网络流量（东西流量）如何获取？
- 如何同时支持多个分析工具？

➤ Flow的价值

- 描述连接信息，五元组、连接状态、字节数、握手关闭状态，连接时间等，自动关联云平台信息
- 轻量级，存储数据量小，时间长
- 适合行为分析，按需与DPI结合，大大提高效率
- 无需看用户数据



云网分析需求



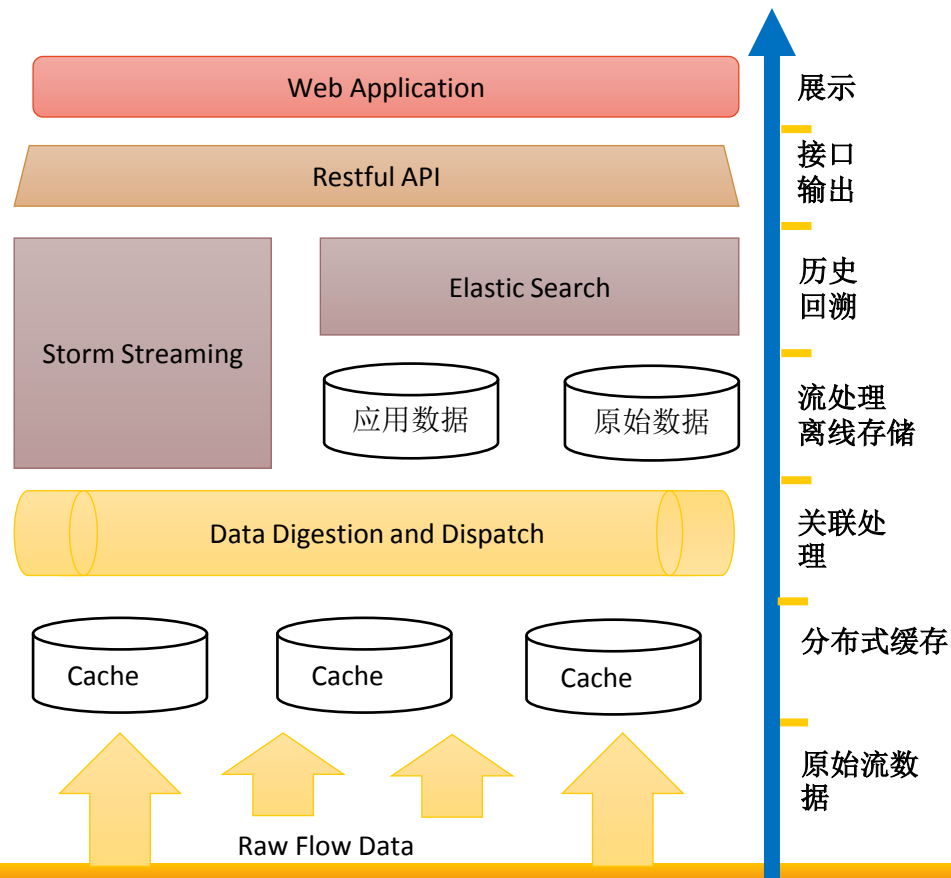
软件定义探针

➤ SDN + Flow + DPI+ Traffic Intelligence + Cloud

- SDN：利用SDN优势，提供高效灵活的控制管理
- Flow：全时、全网，为网络行为分析提供依据
- Packet：DPI应用，内容深度检测
- Traffic Intelligence：包截断，流截断，内容隐藏，包头改写等
- Cloud Adapter：学习云的资源、配置、状态等信息



软件架构



目录

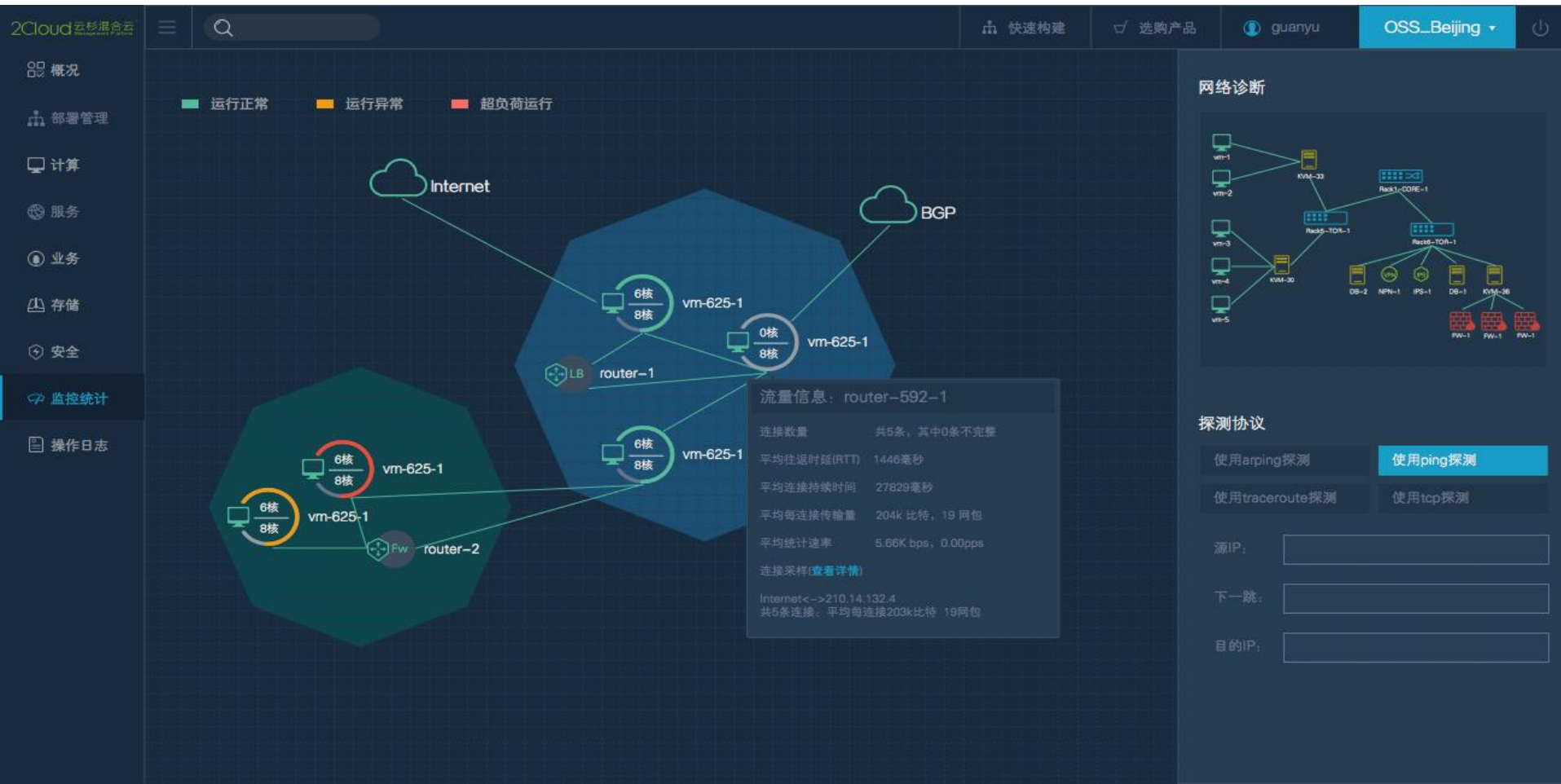
1 云+SDN

2 基于Flow的数据分析

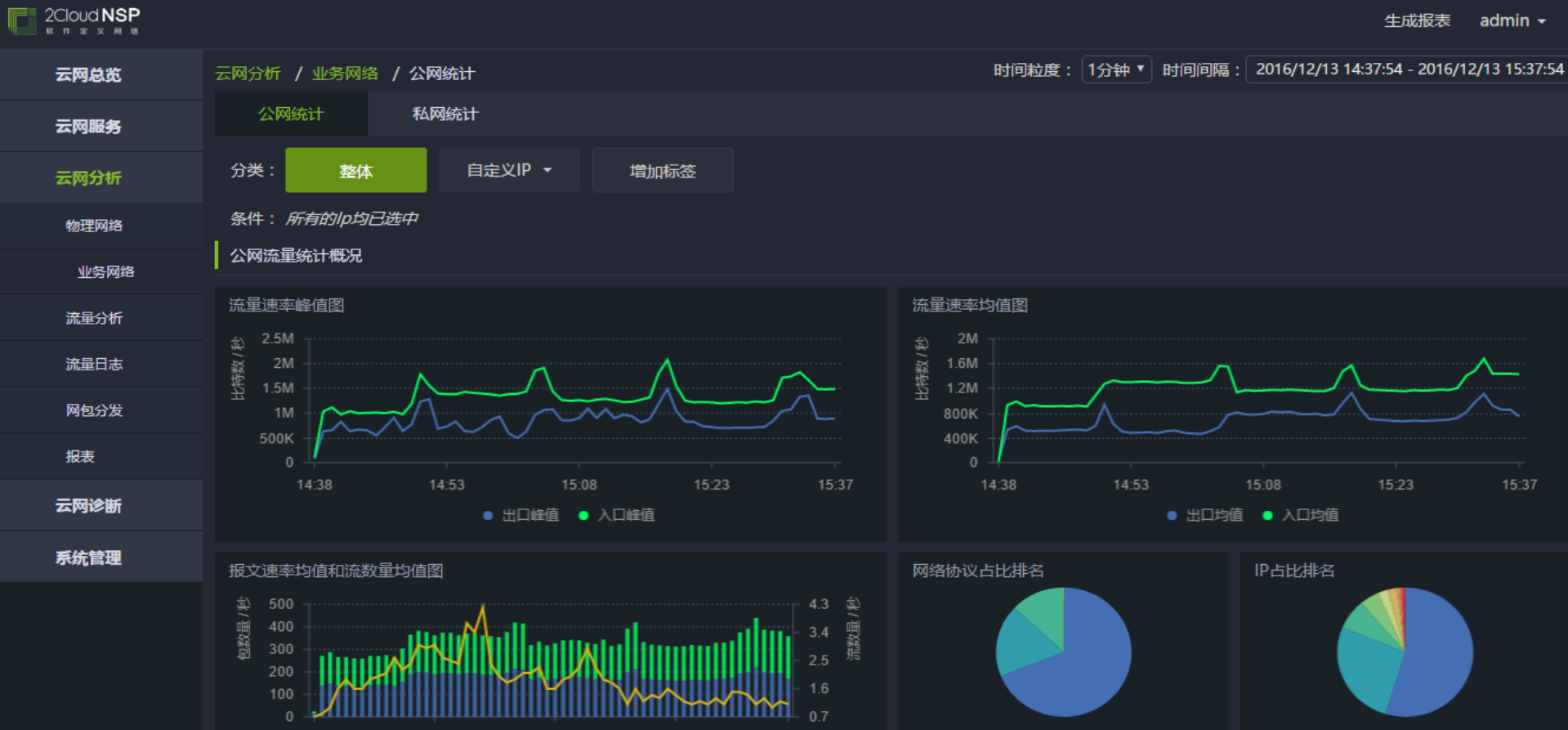
➔ 3 应用案例



资源、位置、流量关联分析



自定义分析内容



网络行为统计

云网总览

云网分析 / 流量分析

时间粒度: 1分钟 时间间隔: 2016/12/13 18:21:06 - 2016/12/13

云网服务

外部访客地域...

外部服务地域...

访问信息

TCP连接

网流特征统计

TCP会话分析

云网分析

大流分析(流的字节数大小)



0-10K 10K-100K 100K-1M 1M-100M 100M-1G 1G-Infinity

物理网络

业务网络

流量分析

流量日志

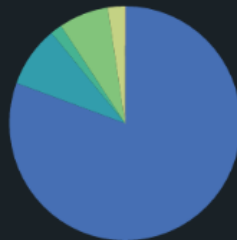
网包分发

报表

云网诊断

系统管理

长流分析(流的持续秒数)



0-1 1-5 5-10 10-60 60-3600 3600-Infinity

大流详细信息(流的字节数大小)

搜索

范围 ^

计数 ^

0-10K

5405

10K-100K

0

100K-1M

0

1M-100M

0

100M-1G

0

长流详细信息(流的持续秒数)

搜索

范围 ^

计数 ^

0-1

4356

1-5

456

5-10

88

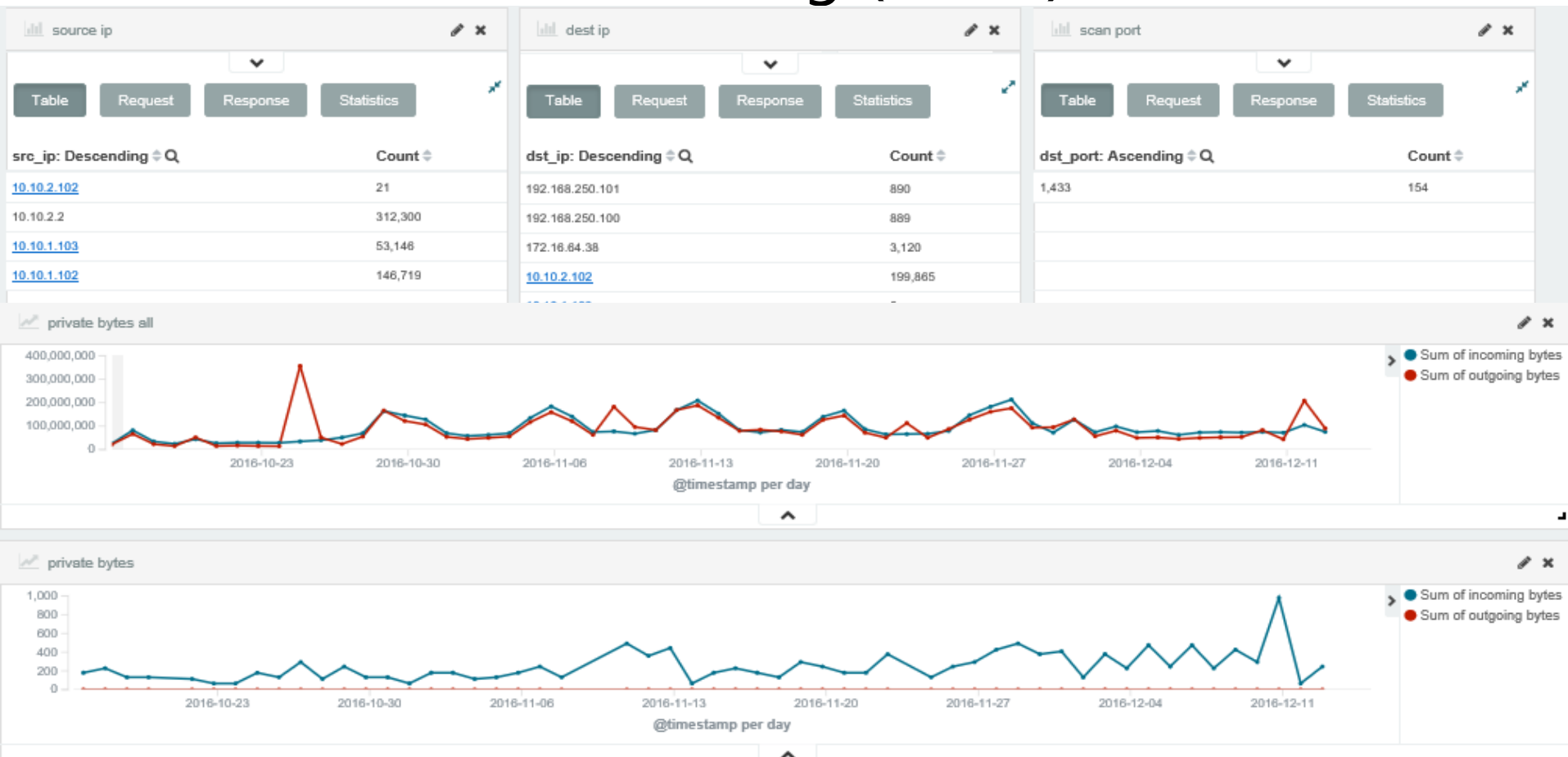
10-60

375

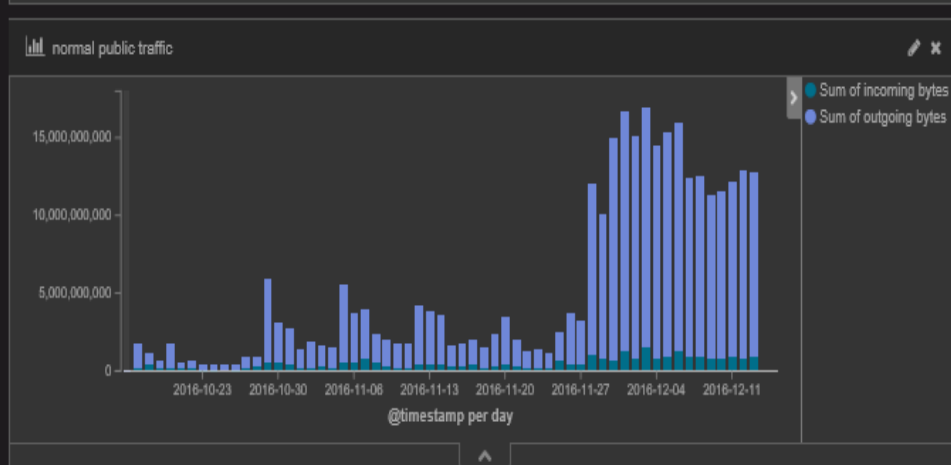
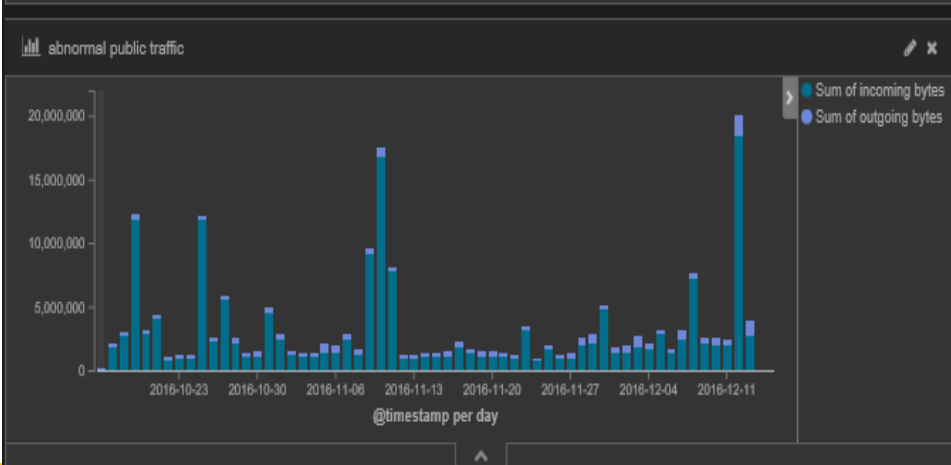
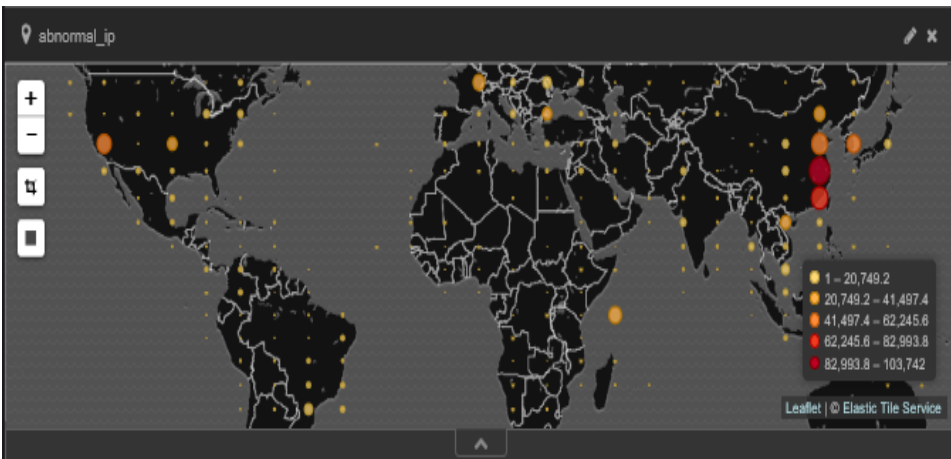
60-3600

126

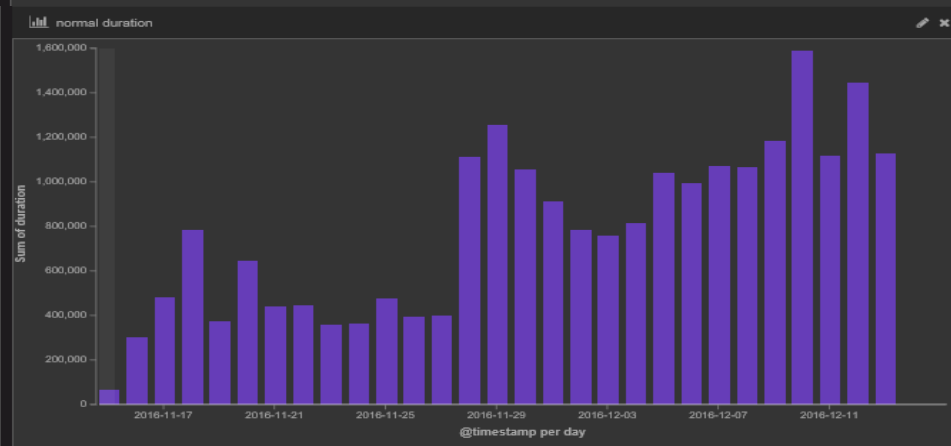
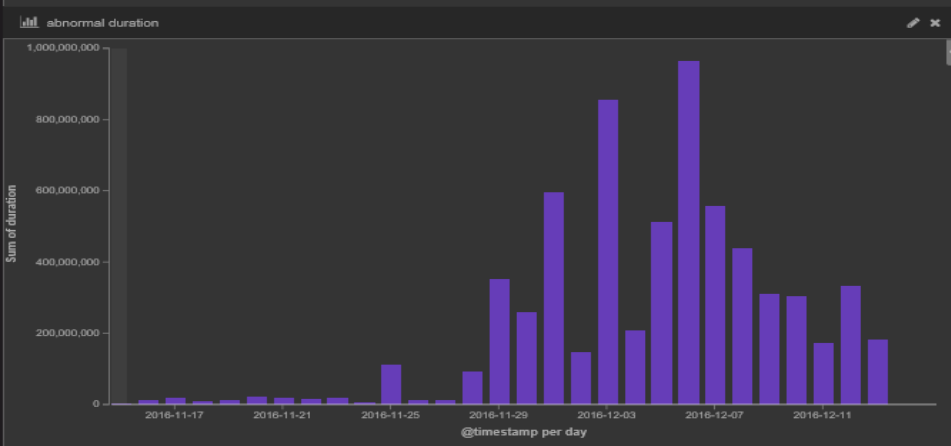
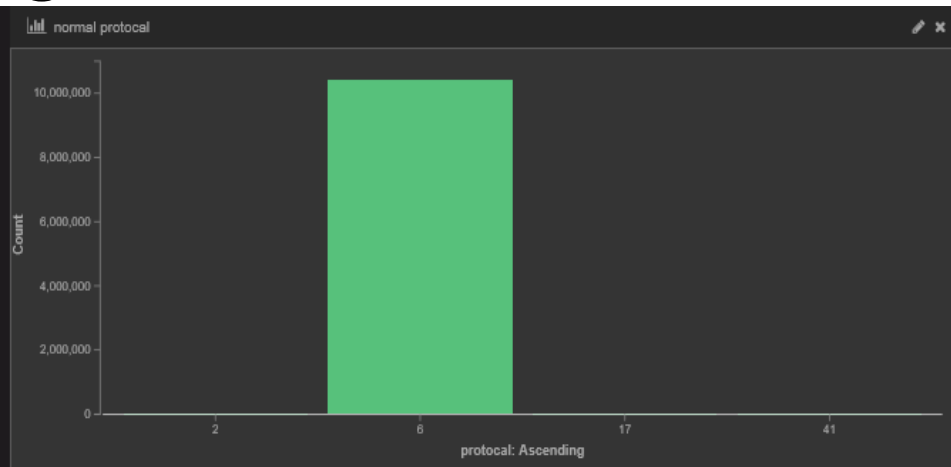
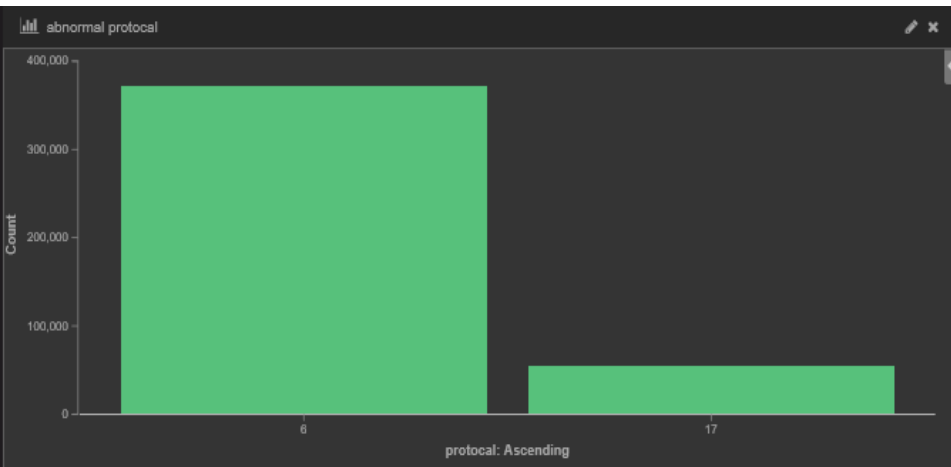
Flow & Machine Learning (内网)



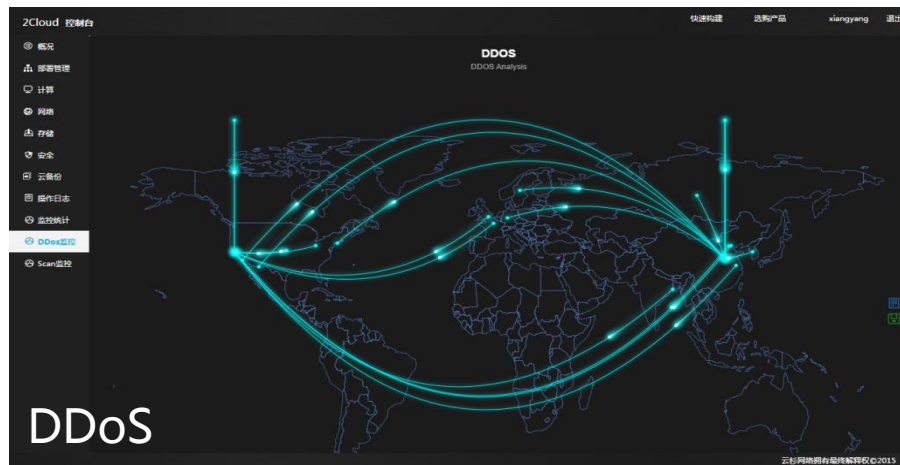
Flow & Machine Learning (公网)



Flow & Machine Learning (公网)



第三方服务集成（绿盟）



历史溯源

- 大规模存储
- 快速检索
- Root cause

APT攻击

- 异常行为发现
- 非signature检测

内部攻击

- 内部网络行为违规
- 内部异常行为检测

网络可视化

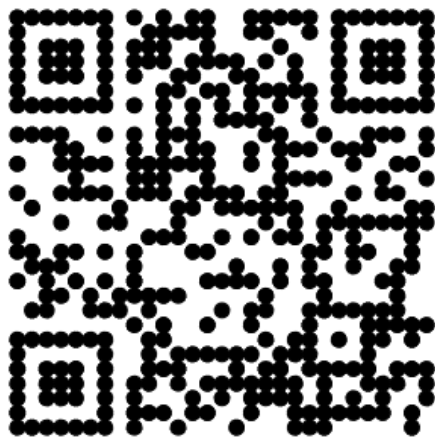
- 直观态势
- 应急响应速度

DevOpsDays 即将首次登陆中国



DevOps 之父 Patrick Debois 与您相约

DevOpsDays 北京站 2017年3月18日



门票早鸟价仅限前100名，请从速哟

<http://2017-beijing.devopsdayschina.org/>



GOPS2016
Beijing



想第一时间看到
高效运维社区公众号
的好文章吗？

请打开高效运维社区公众号，点击右上角小人，如右侧所示设置就好





Thanks

高效运维社区
开放运维联盟

荣誉出品

