阿里云 MVP

Elasticsearch 在智能运维领域的运用

Elastic 技术专家 曾勇

elastic

阿里云 MVP

什么是智能运维？

elastic


车库咖啡订阅号

阿里云 MVP

人工智能！

elastic

阿里云 MVP

落地！

elastic

阿里云 MVP

我们具体聊聊运维的痛点！

elastic



服务器、硬件、网络 ...


软件、服务、代码...



Image Credit: https://www.flickr.com/photos/teco_kit/23908928999

阿里云 MVP

每时每刻产生大量的...

elastic


事件、日志...


ad averages: 0.00, 0.00, 0.00; up 0+00:13:17 21:04
processes: 16 sleeping, 1 on CPU
U states: 0.0% user, 0.0% nice, 0.0% system, 0.0% interrupt, 100% idle
mory: 29M Act, 6028K Wired, 8336K Exec, 14M File, 184M Free
ap:
PID USERNAME PRI NICE SIZE RES STATE TIME WCPU CPU COMMAND
684 root 43 0 17M 1800K CPU 0:00 0.00% 0.00% top
0 root 96 0 0K 2912K atath 0:00 0.00% 0.00% [system]
303 root 85 0 22M 6128K pause 0:00 0.00% 0.00% ntpd
537 root 85 0 48M 3912K kqueue 0:00 0.00% 0.00% master
529 postfix 85 0 48M 3856K kqueue 0:00 0.00% 0.00% qmgr
525 postfix 85 0 queue 0:00 0.00% 0.00% pickup
570 root 85 0 it 0:00 0.00% 0.00% login
198 root 85 0 23M 1876K kqueue 0:00 0.00% 0.00% syslogd
530 root 85 0 13M 1740K wait 0:00 0.00% 0.00% sh
532 root 85 0 13M 1352K ttyraw 0:00 0.00% 0.00% getty
519 root 85 0 13M 1352K ttyraw 0:00 0.00% 0.00% getty
568 root 85 0 13M 1352K ttyraw 0:00 0.00% 0.00% getty
484 root 85 0 11M 1320K nanoslp 0:00 0.00% 0.00% cron
1 root 85 0 13M 1316K wait 0:00 0.00% 0.00% init
539 root 85 0 15M 1104K kqueue 0:00 0.00% 0.00% inetd
150 root 85 0 11M 1072K select 0:00 0.00% 0.00% dhclient
341 root 85 0 13M 1020K kqueue 0:00 0.00% 0.00% powerd

Metrics、指标...

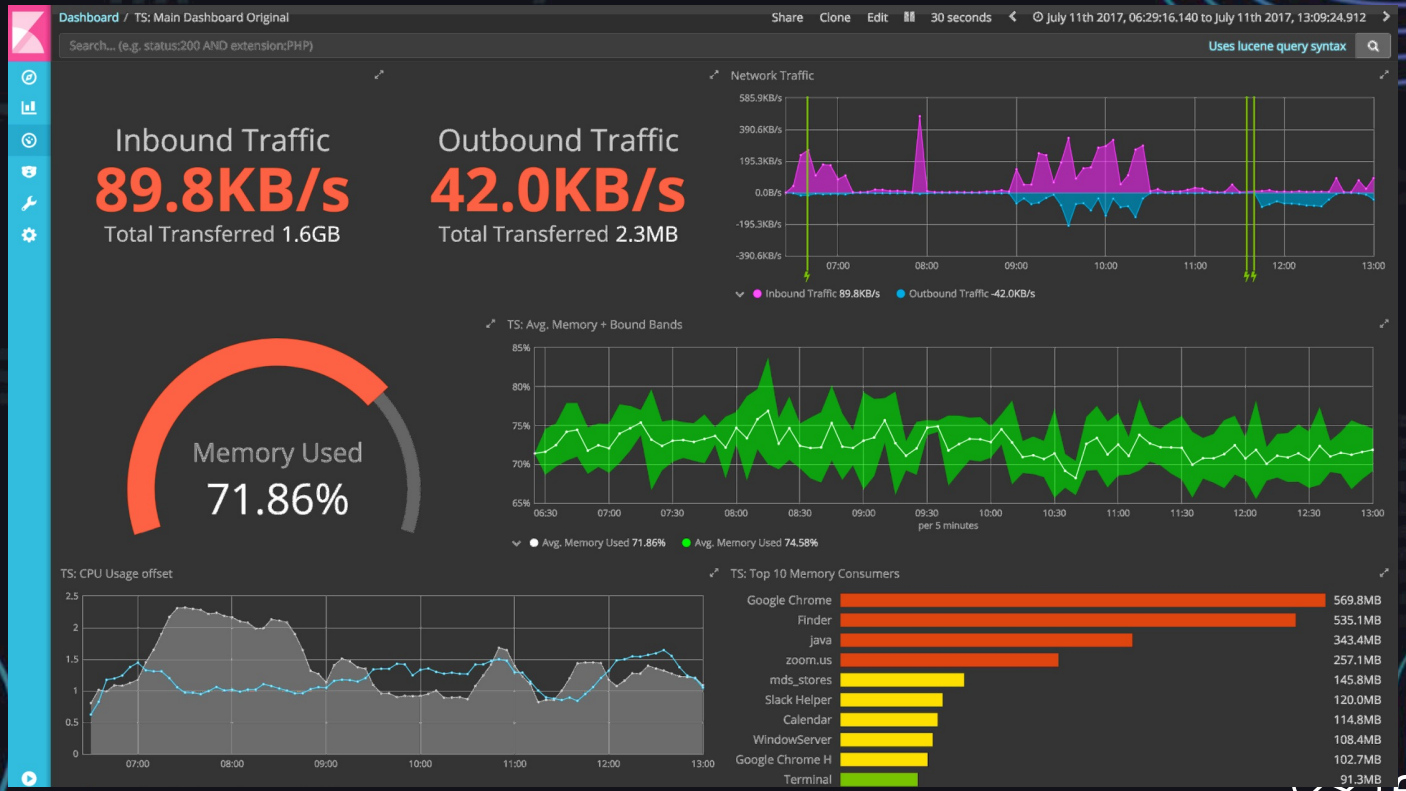
阿里云 MVP

期望得到的...

elastic

阿里云 MVP

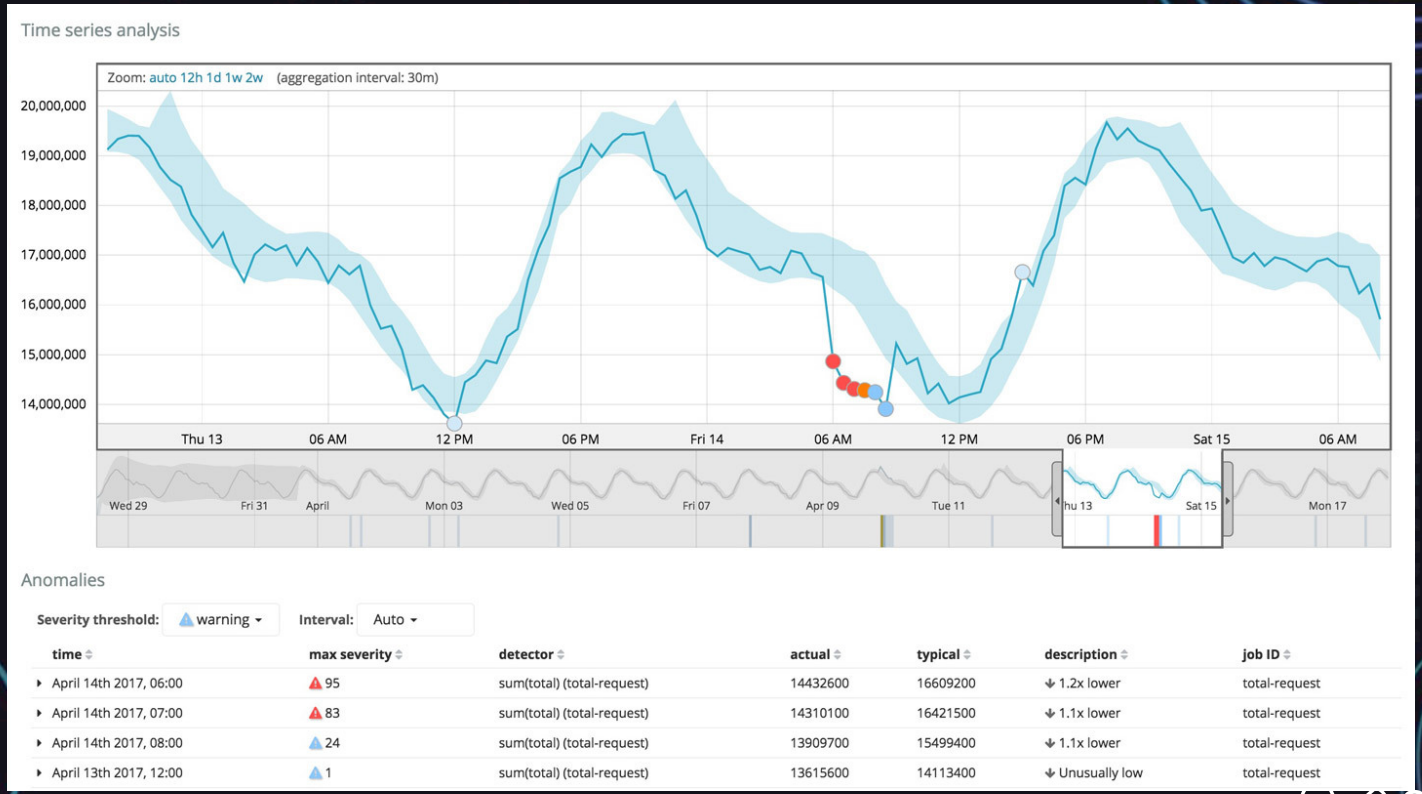
报表...



elastic

阿里云 MVP

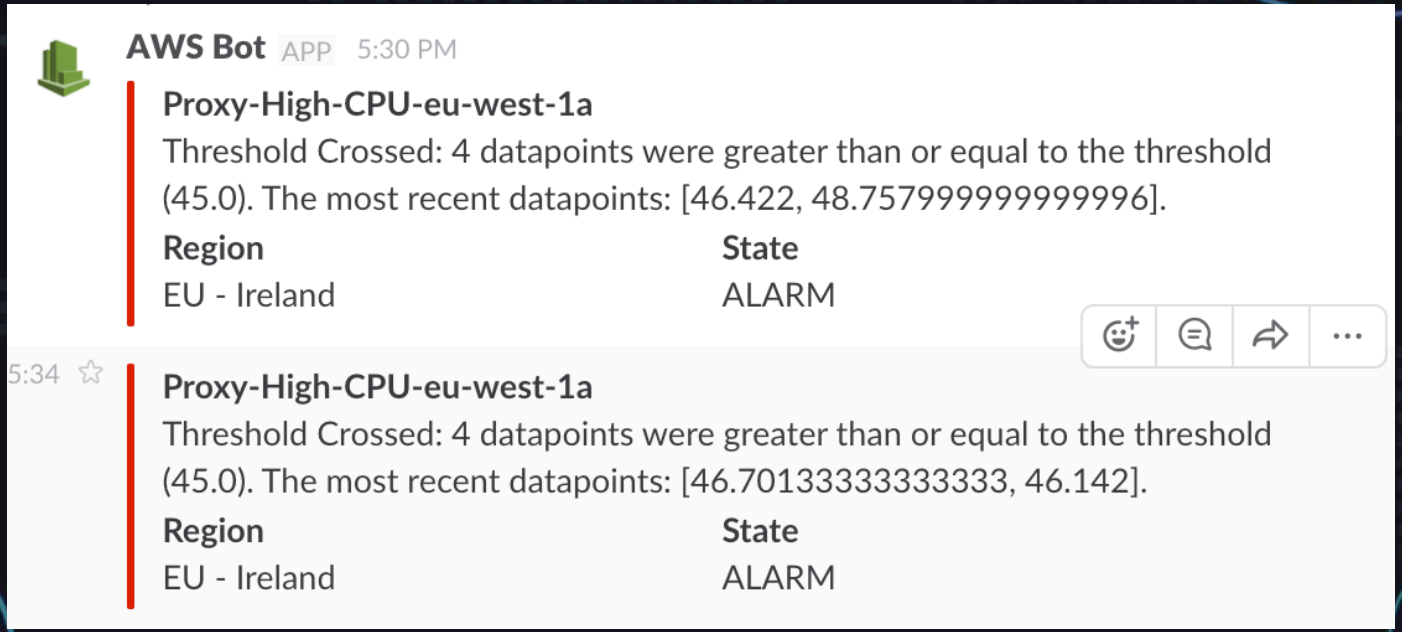
异常...



elastic

阿里云 MVP

告警...



elastic

阿里云 MVP

因为...

elastic

阿里云 MVP





elastic

阿里云 MVP

你需要...

elastic

阿里云 MVP

所有这些.

Data sources **Visualizations**
Machine Learning Unstructured
Query language *Drill down* **Log correlation**
Highly available Fast **Real-time** **Alerting**
Secure Reports ***Scalable*** SaaS
Enrichment **APIs** Advanced Analytics **Dashboards**

elastic

阿里云 MVP

Elastic 提供 所有这些.

Data sources **Visualizations**
Machine Learning Unstructured
Query language *Drill down* **Log correlation**
Highly available Fast **Real-time** **Alerting**
Secure Reports ***Scalable*** SaaS
Enrichment **APIs** Advanced Analytics **Dashboards**

elastic

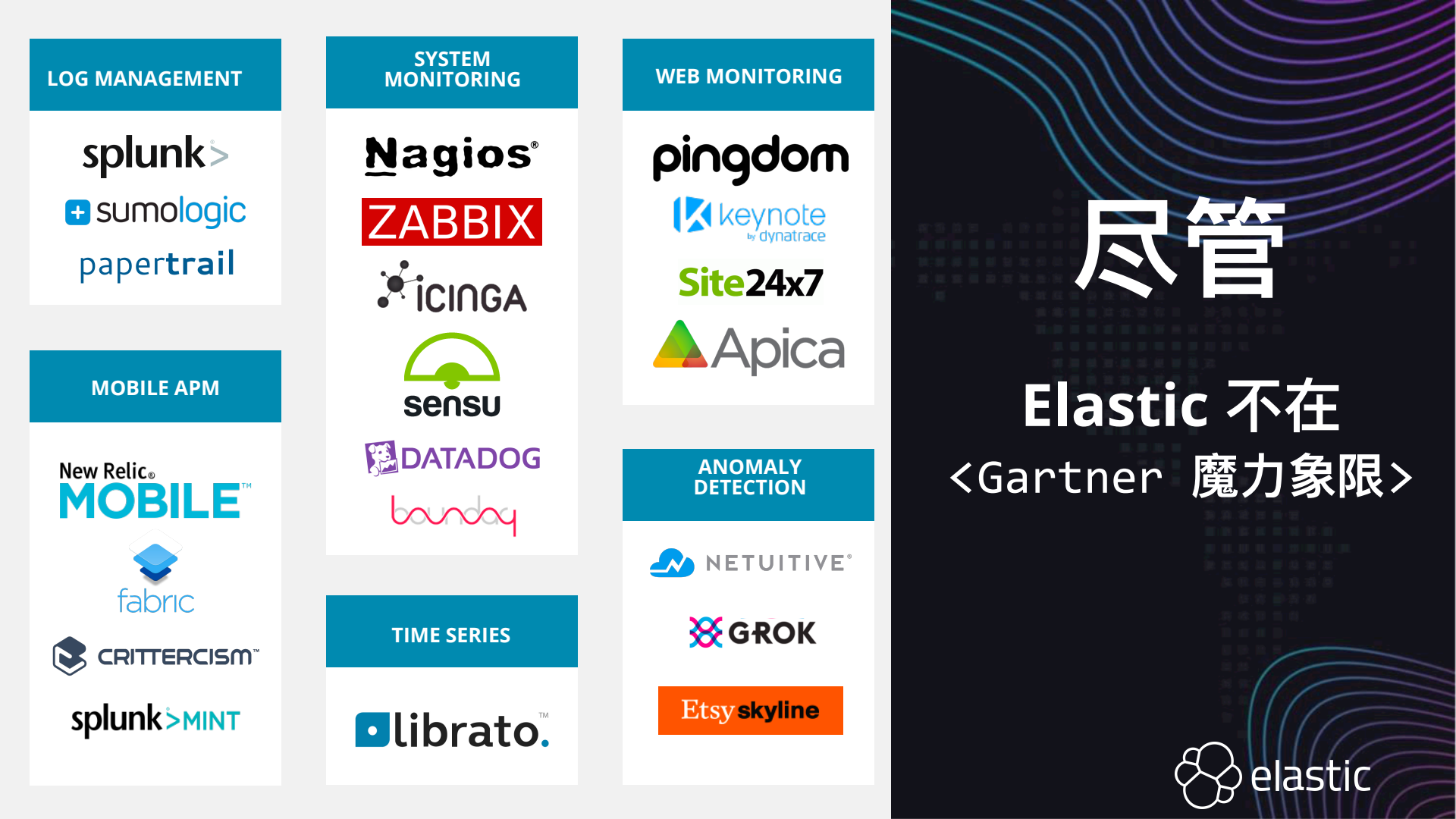
阿里云 MVP

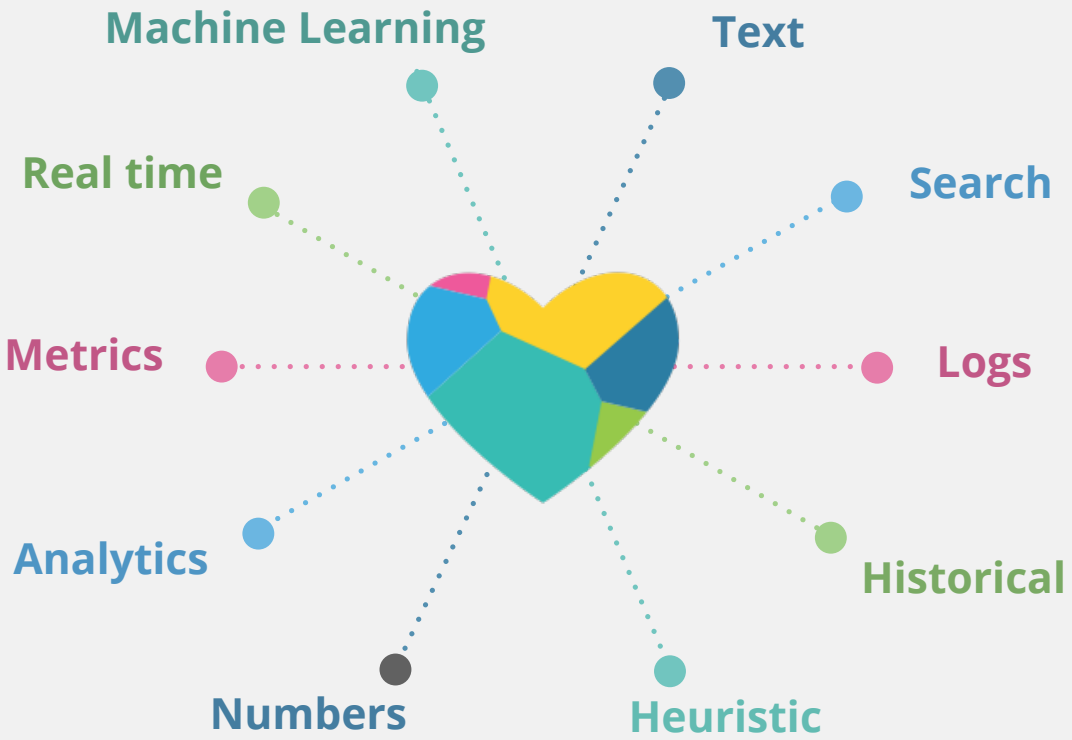
Elastic 为什么不一样?

elastic


NETSUITE
Yale
ACTIVISION
NERSC
YODEL
seek
BNP PARIBAS
FANDANGO
esri
IBM
UBER
Walmart
RIOT GAMES
Sprint
verizon
CONCUR
CATHAY PACIFIC
FICO
MAYO CLINIC
USGS
science for a changing world
NETFLIX
PSA PEUGEOT CITROËN
NASA
BLIZZARD ENTERTAINMENT
Goldman Sachs
MZ
MACHINE ZONE
theguardian
Kroger
trainline
NVIDIA
WARNER BROS.

用户无处不在


LOG MANAGEMENT
splunk>
sumologic
papertrail
MOBILE APM
New Relic MOBILE
fabric
CRITTERCISM
splunk>MINT
SYSTEM MONITORING
Nagios
ZABBIX
ICINGA
sensu
DATADOG
boundary
TIME SERIES
librato
WEB MONITORING
pingdom
keynote by dynatrace
Site24x7
Apica
ANOMALY DETECTION
NETUITIVE
GROK
Etsy skyline
尽管
Elastic 不在
<Gartner 魔力象限>
elastic



不过

多样性
才是我们的长处

elastic

阿里云 MVP

回到话题

elastic

阿里云 MVP

运维之监控！

- 监控指标的收集
- 监控数据的存储
- 监控数据的分析
- 监控数据的告警

elastic

阿里云 MVP

运维之监控！

- 监控指标的收集 
- 监控数据的存储
- 监控数据的分析
- 监控数据的告警

elastic

阿里云 MVP

Metricbeat, Filebeat, Auditbeat & Logstash

System
- Linux
- MacOS
- Windows
- Perfmon

Custom apps
- JMX/Jolokia
- PHP-FPM
- Golang
- Dropwizard

Storage
- Ceph

… …

Containers
- Docker
- Kubernetes

Virtualization
- vSphere

Datastores
- MySQL
- PostgreSQL
- MongoDB
- Couchbase
- Aerospike

Cloud
- AWS
- GCP
- DigitalOcean

Queues
- Redis
- Kafka
- RabbitMQ

Security
- ArcSight

Caches
- Memcached

Network
- Netflow
- Packets

Web servers
- Apache
- Nginx

Other
- HAProxy
- Zookeeper
- Prometheus
- Graphite
- Icinga

elastic

阿里云 MVP

运维之监控！

- 监控指标的收集 
- 监控数据的存储 
- 监控数据的分析
- 监控数据的告警

elastic

阿里云 MVP

运维之监控！

- 监控指标的收集 
- 监控数据的存储 
- 监控数据的分析
- 监控数据的告警 

elastic

阿里云 MVP

运维之监控！

- 监控指标的收集
- 监控数据的存储
- 监控数据的分析
- 监控数据的告警



人工智能 亦或 只能人工

elastic

#	system.process.cgroup.cpu.cfs.period.us
#	system.process.cgroup.cpu.cfs.quota.us
#	system.process.cgroup.cpu.cfs.shares
t	system.process.cgroup.cpu.id
t	system.process.cgroup.cpu.path
#	system.process.cgroup.cpu.rt.period.us
#	system.process.cgroup.cpu.rt.runtime.us
#	system.process.cgroup.cpu.stats.periods
#	system.process.cgroup.cpu.stats.throttled.ns
#	system.process.cgroup.cpu.stats.throttled.periods
t	system.process.cgroup.cpuacct.id
t	system.process.cgroup.cpuacct.path
#	system.process.cgroup.cpuacct.percpu.1
#	system.process.cgroup.cpuacct.percpu.2
#	system.process.cgroup.cpuacct.percpu.3
#	system.process.cgroup.cpuacct.percpu.4
#	system.process.cgroup.cpuacct.stats.system.ns
#	system.process.cgroup.cpuacct.stats.user.ns
#	system.process.cgroup.cpuacct.total.ns

CPU Metrics

也还行，
也就几千个指标！

elastic

#	system.process.cgroup.cpu.cfs.period.us
#	system.process.cgroup.cpu.cfs.quota.us
#	system.process.cgroup.cpu.cfs.shares
t	system.process.cgroup.cpu.id
t	system.process.cgroup.cpu.path
#	system.process.cgroup.cpu.rt.period.us
#	system.process.cgroup.cpu.rt.runtime.us
#	system.process.cgroup.cpu.stats.periods
#	system.process.cgroup.cpu.stats.throttled.ns
#	system.process.cgroup.cpu.stats.throttled.periods
t	system.process.cgroup.cpuacct.id
t	system.process.cgroup.cpuacct.path
#	system.process.cgroup.cpuacct.percpu.1
#	system.process.cgroup.cpuacct.percpu.2
#	system.process.cgroup.cpuacct.percpu.3
#	system.process.cgroup.cpuacct.percpu.4
#	system.process.cgroup.cpuacct.stats.system.ns
#	system.process.cgroup.cpuacct.stats.user.ns
#	system.process.cgroup.cpuacct.total.ns

CPU Metrics

也还行，
也就~~几千~~个指标！

几万？

elastic




BOOM!

阿里云 MVP

ELASTIC 的人工智能，智能运维。

elastic

阿里云 MVP

~~ELASTIC 的人工智能，智能运维。~~

ELASTIC 的机器学习。

elastic

阿里云 MVP

先看看监控数据

- 三大类
  - Logging
  - Tracing info
  - Metrics

elastic

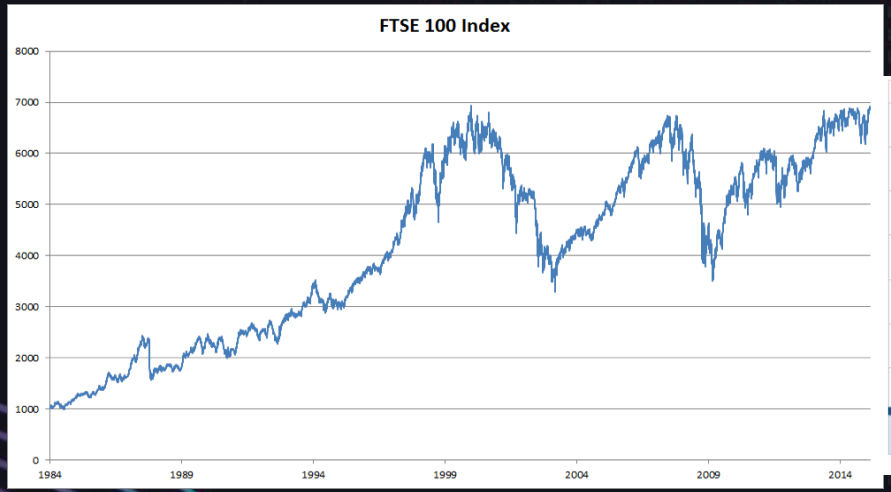
阿里云 MVP

都是时序型数据！

elastic

阿里云 MVP

什么是时序型数据？

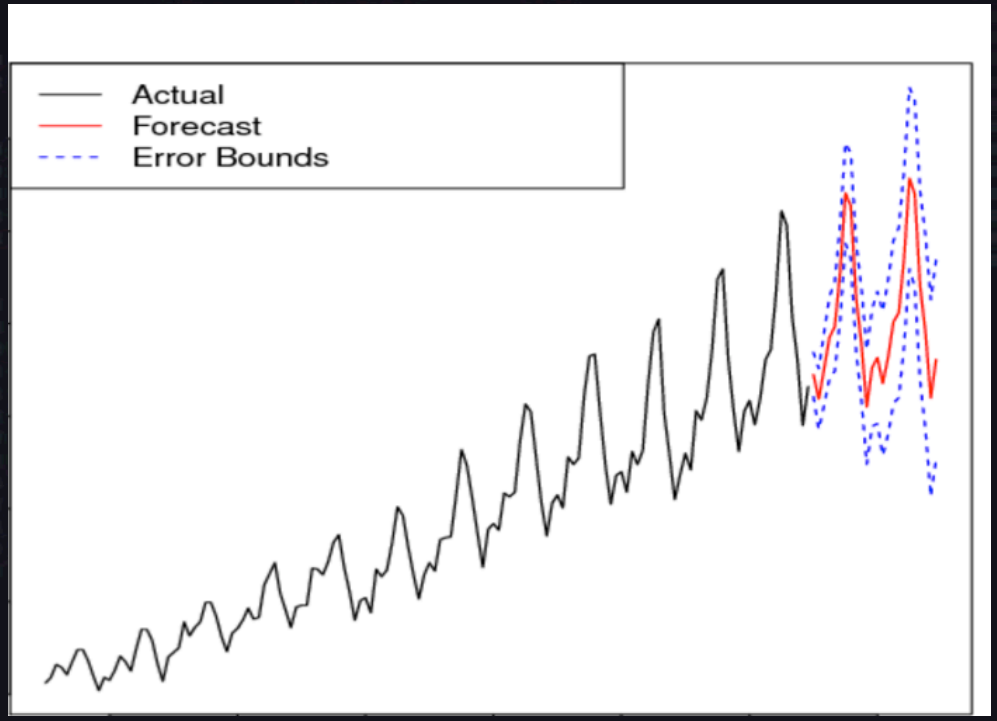




elastic

阿里云 MVP

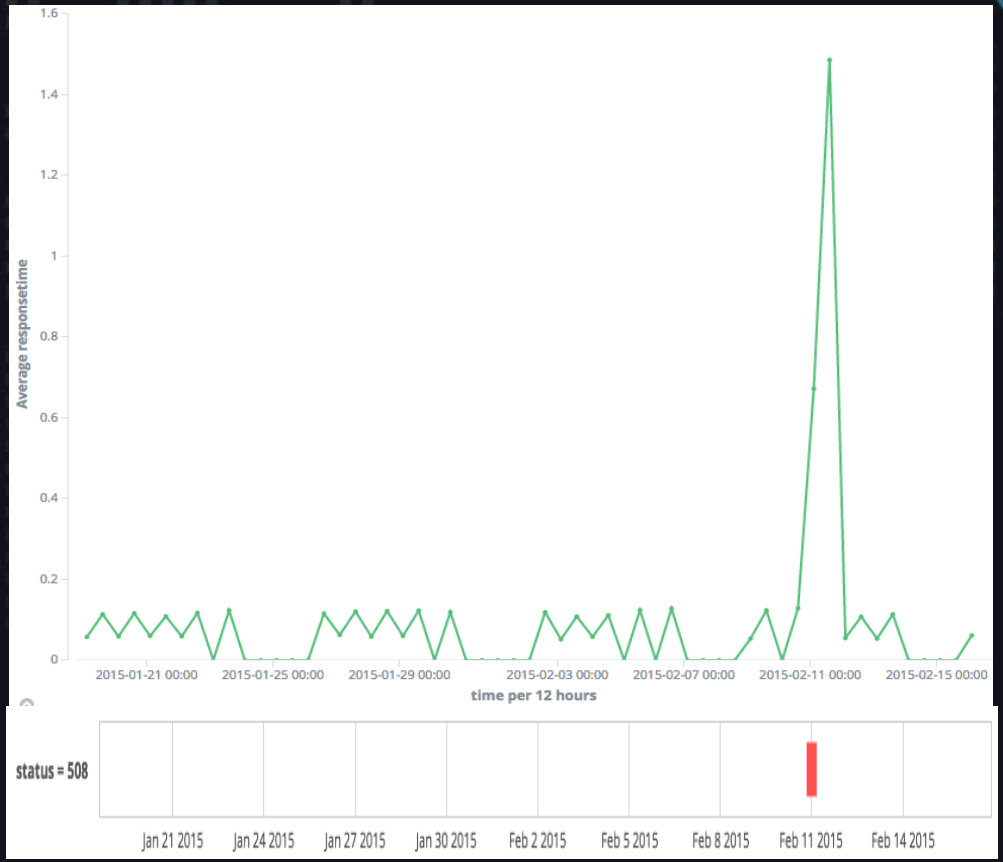
为什么使用时序型数据？



elastic

阿里云 MVP

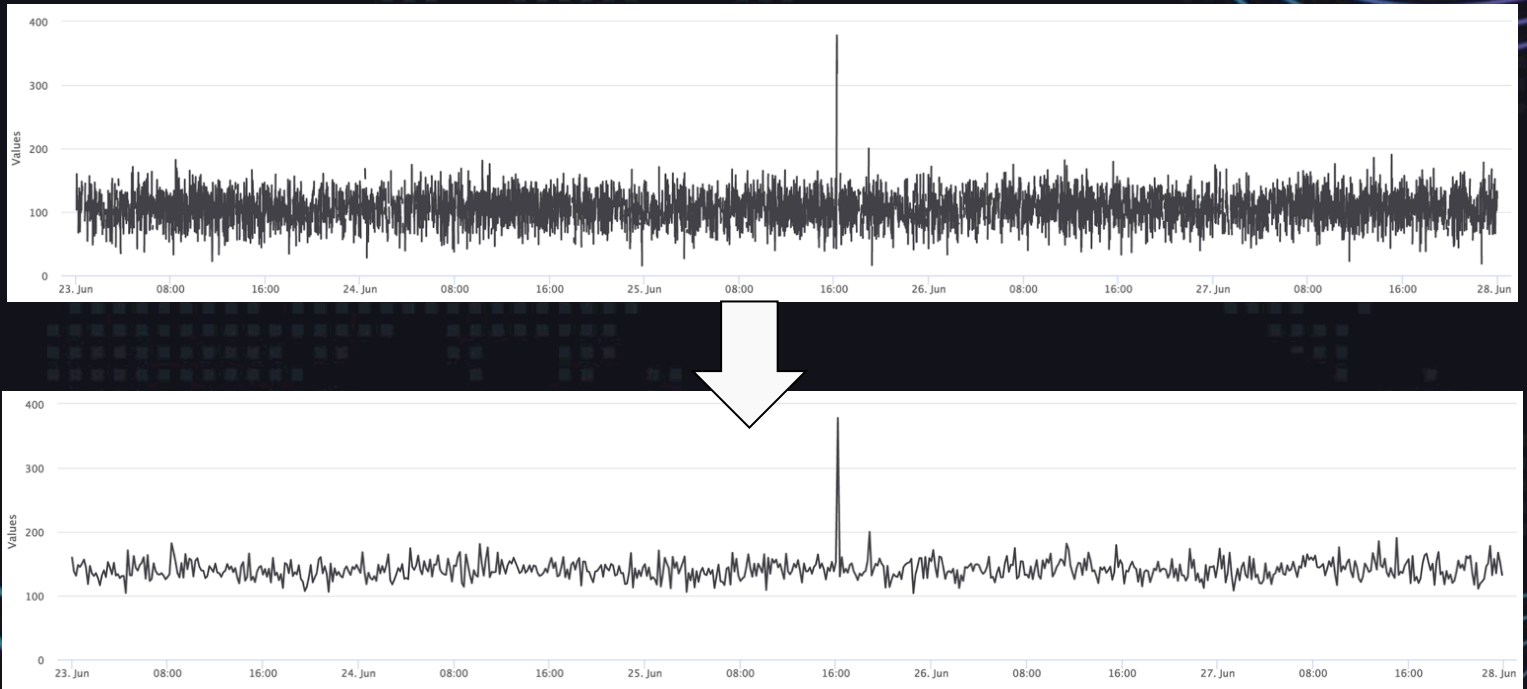
为什么使用时序型数据？



elastic

阿里云 MVP

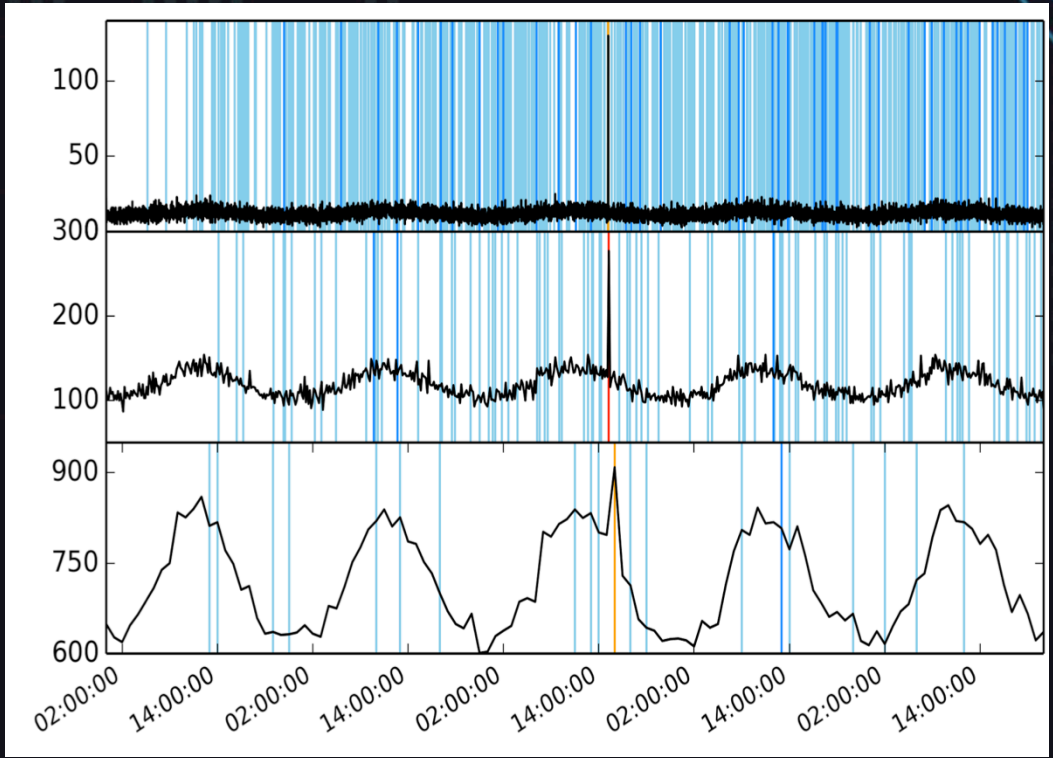
Bucketing



elastic

阿里云 MVP

Bucket 的选择



elastic

阿里云 MVP

监督型机器学习。

elastic

阿里云 MVP

非监督型机器学习。

elastic

阿里云 MVP

时序型指标
特征化，模型化！

elastic

阿里云 MVP

让机器去帮你
监控海量指标，发现异常！

elastic

阿里云 MVP

DEMO

elastic

阿里云 MVP

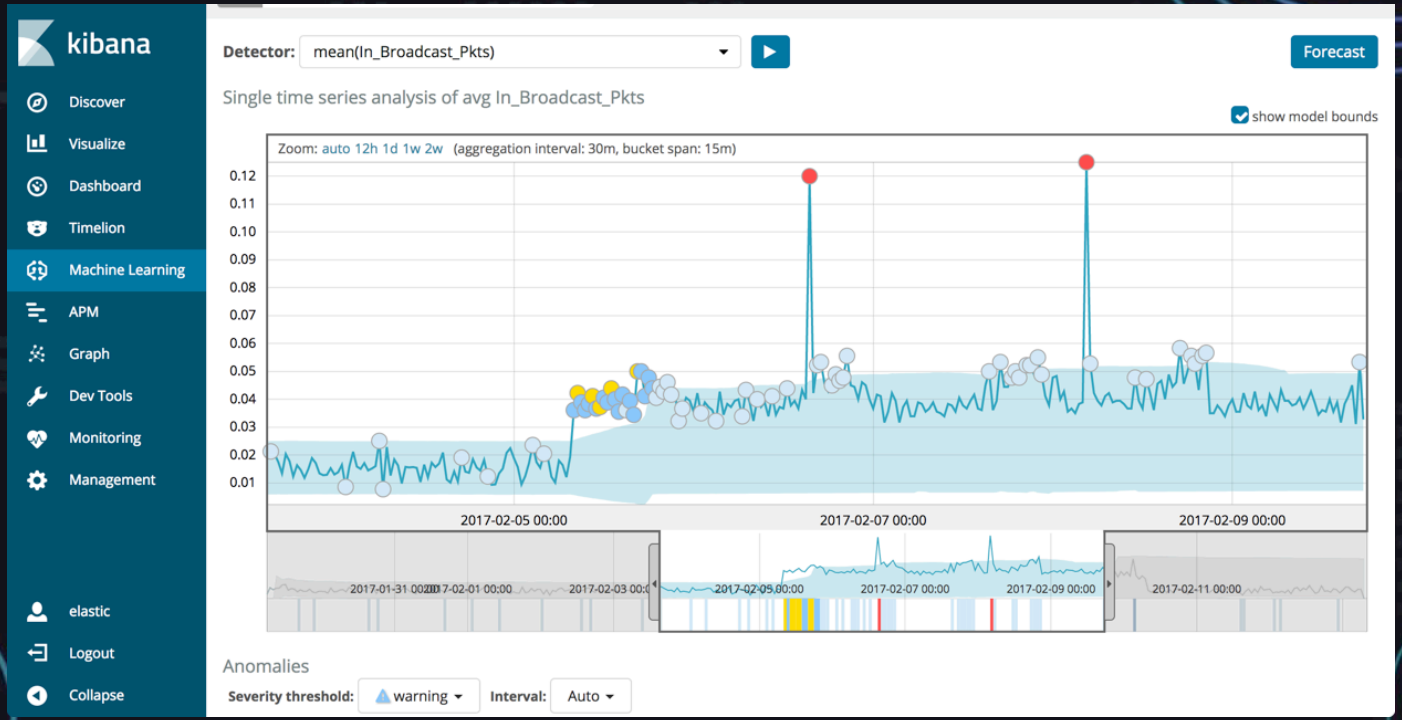
IT-OPS-KPI



elastic

阿里云 MVP

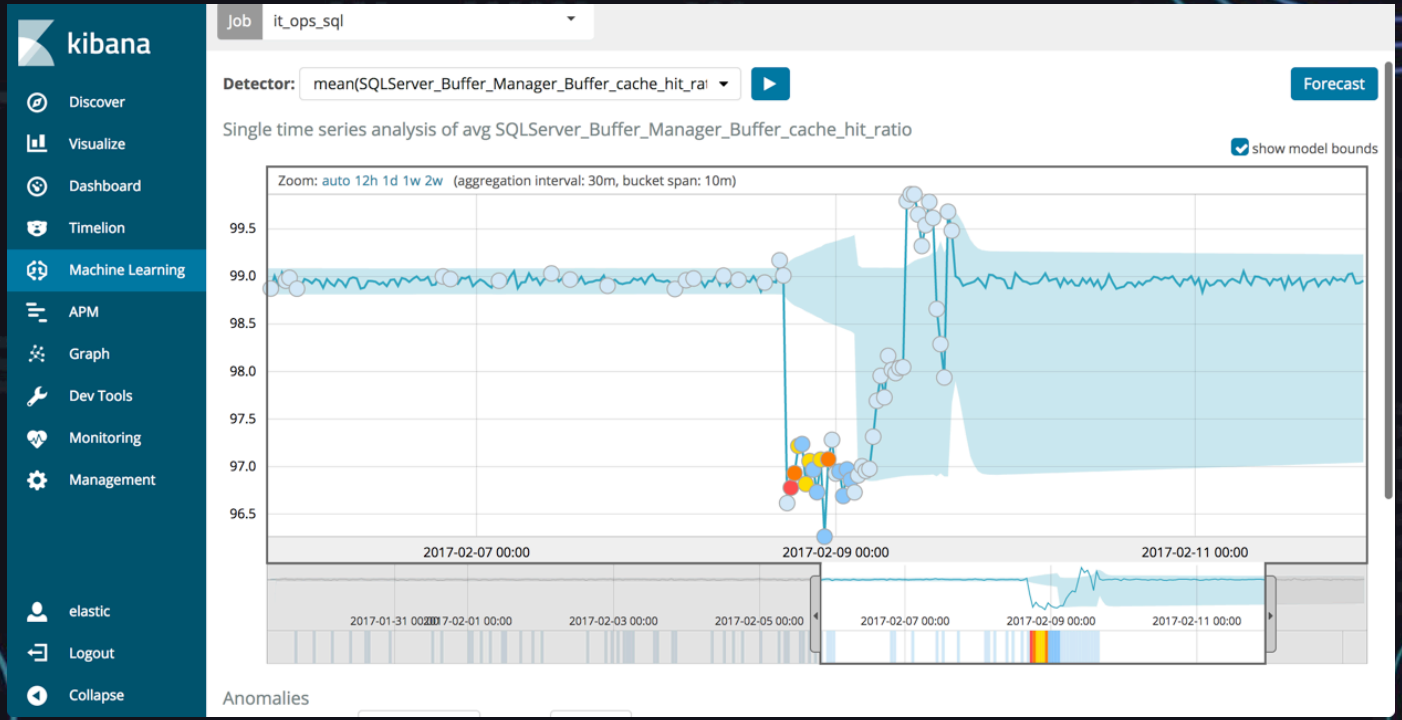
IT-OPS-NETWORK



elastic

阿里云 MVP

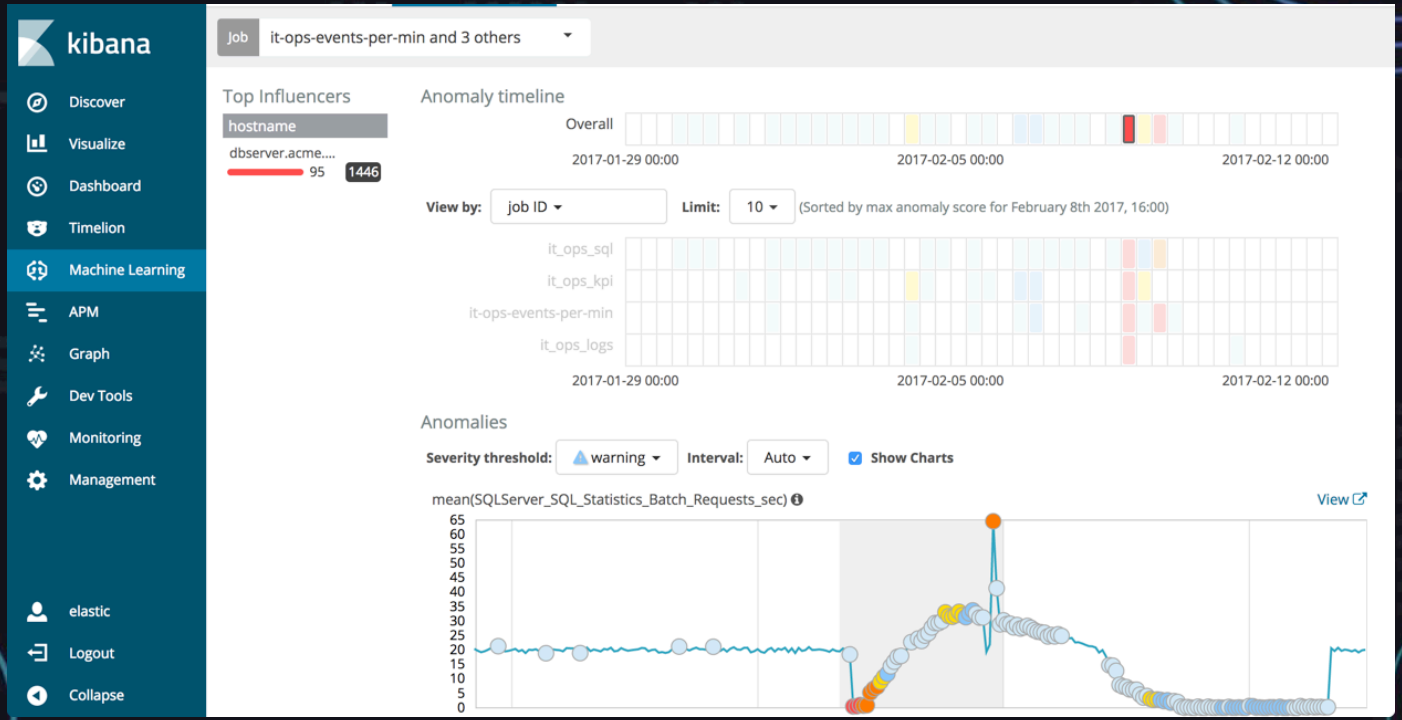
IT-OPS-SQL



elastic

阿里云 MVP

关联分析



elastic

阿里云 MVP

总结

- 运维已进入精细化智能化时代
- AI 不会让运维失业
- 让机器做机器擅长的
- Elastic 让运维分析更简单

elastic

Thanks!