

# 混合云认知IT服务管理

黄 卫

IBM混合云顾问工程师

# 混合云与数字化转型给传统IT服务管理带来挑战

... 由于问题的症状经常隐藏在不同环境产生的“大数据”中，管理端到端的应用质量变得越来越困难

截至2017年，超过 **50%** 的企业在使用混合云环境

PaaS用户的增加比例在2017年超过 **40%**，2012年为3% -> 应用部署变更速度↑

平均每天运维相关的数据量约 **1.3TB**



问题经由Level 1 support升级上报之后通常会需要3到4个人平均消耗5到7个人时 (man hours) 才能解决

58%的企业会用到6至40种不同的监测工具

故障平均修复时间MTTR一般为3-6个小时

▲ IT管理人员开始寻求逐渐转向**主动分析**和**预防预测性**管理模式

# 认知IT服务管理三要素

1

持续学习

2

预测与调整

3

推荐动作

## 认知分析能力

事件告警相关认知分析

( Advanced Event Analytics )



结构型大数据认知分析和预测

( IOA-PI, exploiting Watson )



大数据日志认知分析

( IOA - Log Analytics )



Available in  
2016

Access trial of Watson for IT Services Management

# 事件告警与日志相关性认知分析

Netcool 提供创新的大数据智能分析, 提高运维价值并在整个 IT 环境降低成本

## 告警事件上下文历史特征挖掘

*No complex manual intervention to setup & maintain with 5 times faster processing*

## 事件日志周期性规律分析

*Alerting before potential issues become service impacting, enabling IT to shift from reactive to proactive*

## 事件日志成对成组出现分析

*IBM Delivered content for grouping well known events. Up to 90% reduction in events out of the box*

## 事件日志相关与因果分析

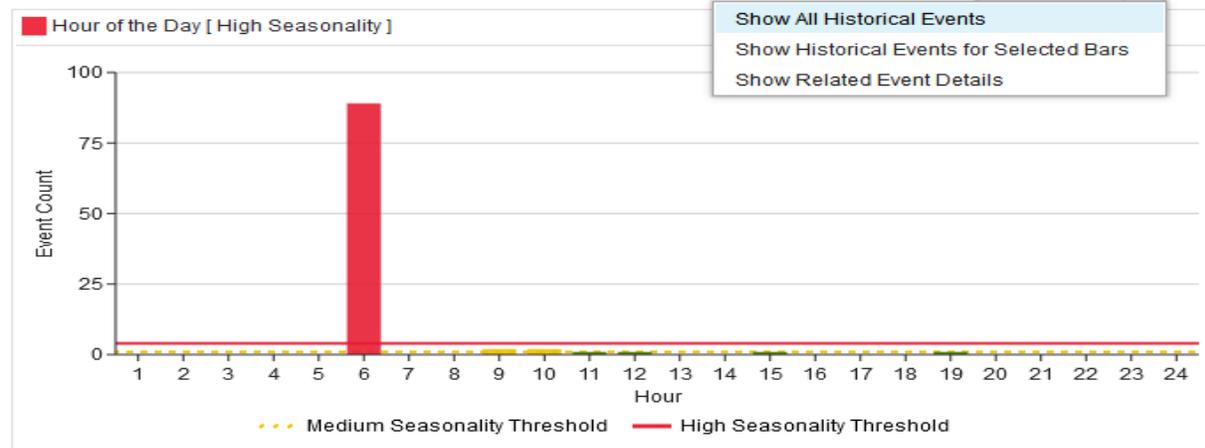
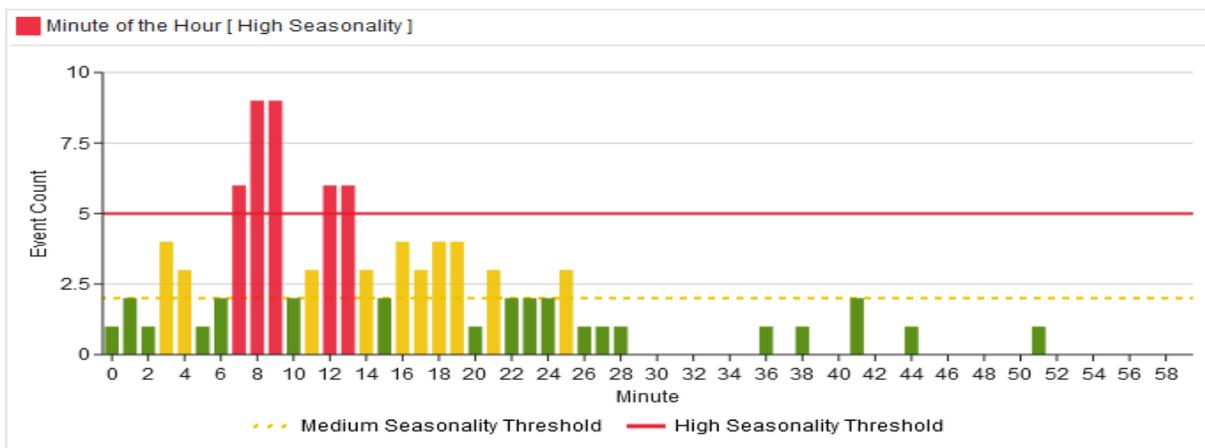
*Discover clusters of events that occur together, automatically group them for context*



# 告警发生之周期性时间规律学习

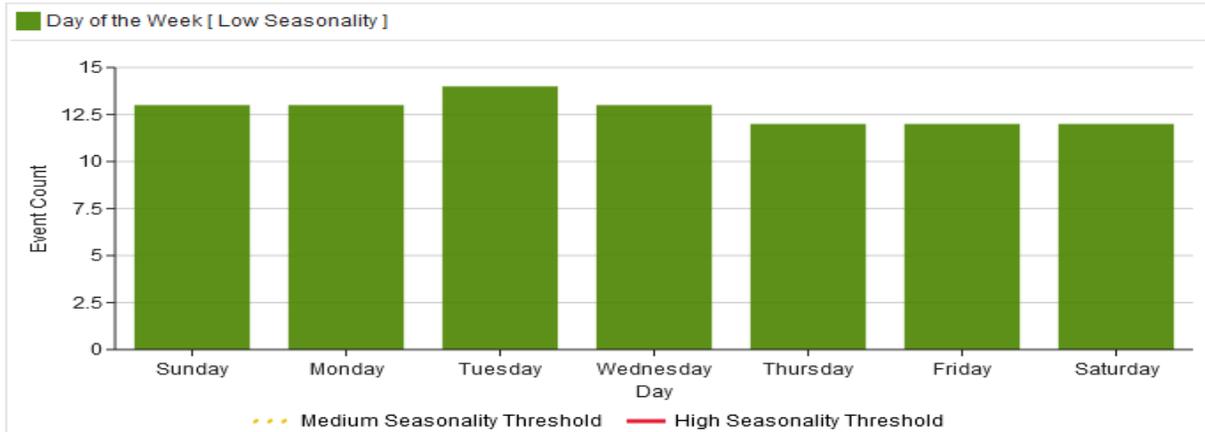
- 某应用端口Down固定发生在每天早上6点到6点半之间，且每周、每月内发生频率均衡分布

Summary:[F5](,):(UNKnowAppName)应用服务器10.3.56.3:20021状态DOWN



Actions

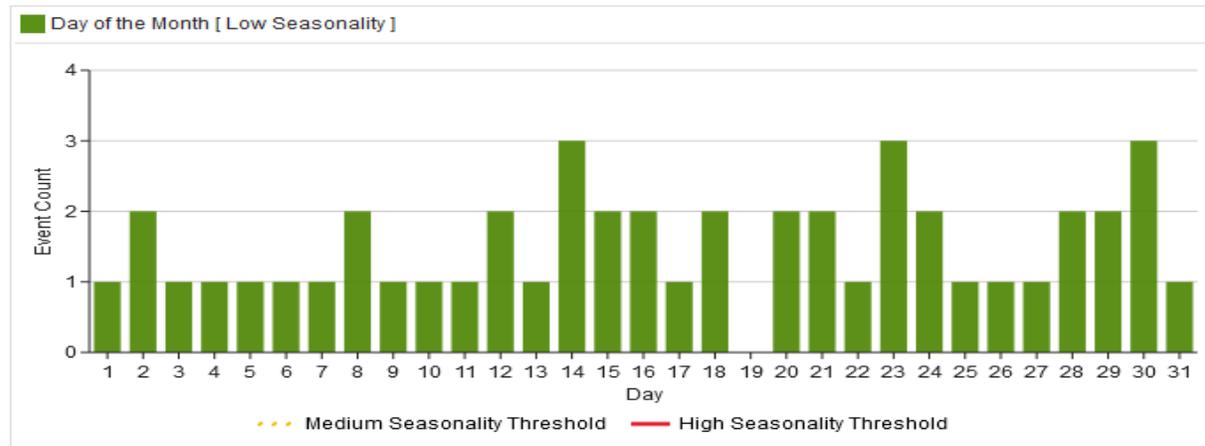
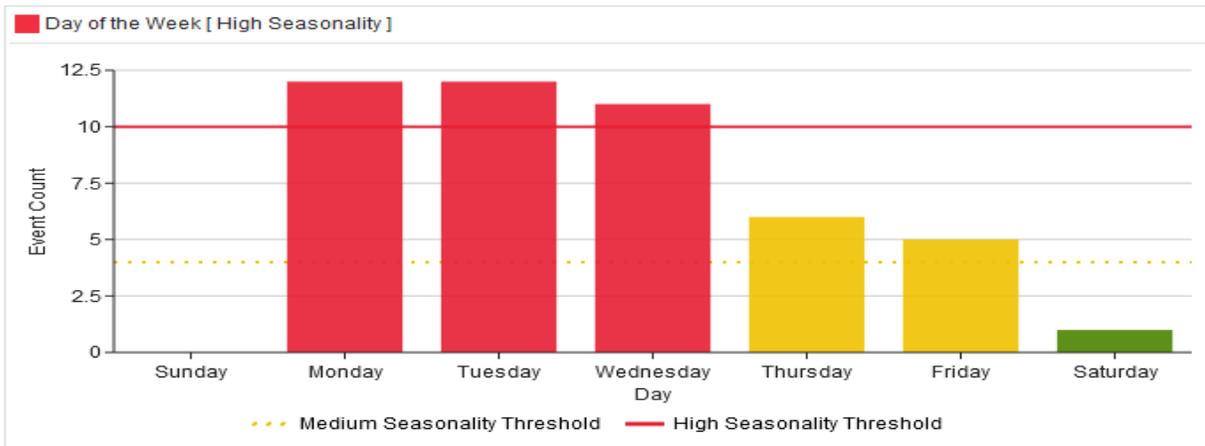
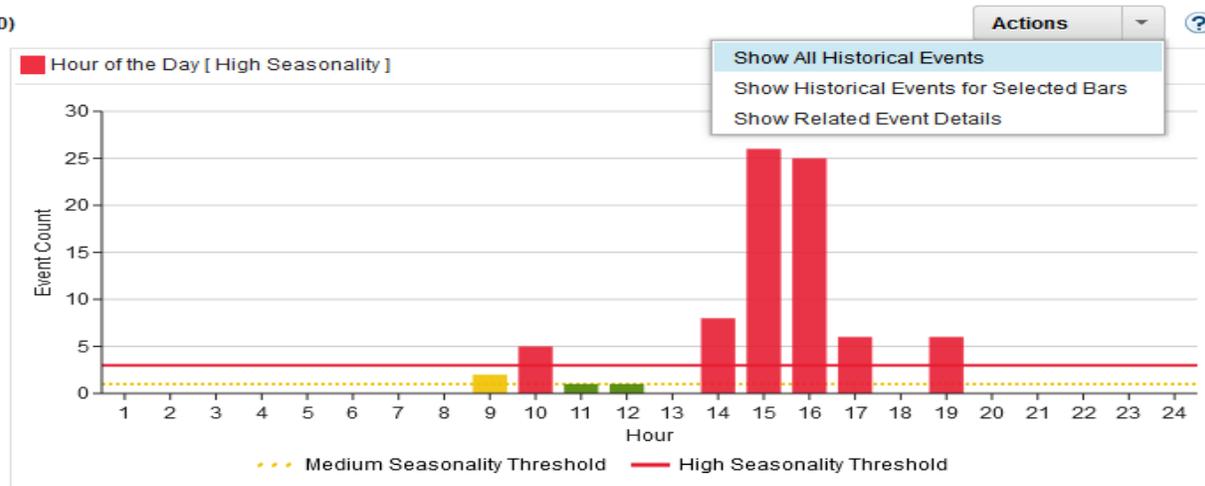
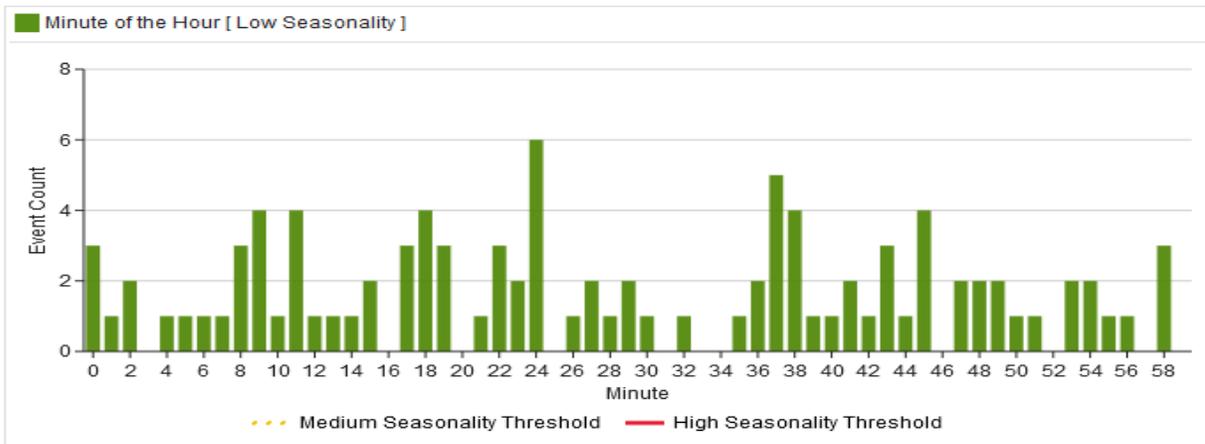
- Show All Historical Events
- Show Historical Events for Selected Bars
- Show Related Event Details



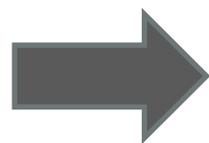
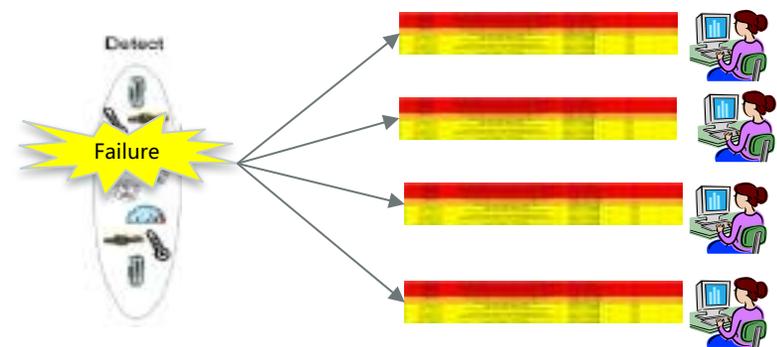
# 告警发生之周期性时间规律学习

- 某Web容器线程池使用率在下午3-4点通常会到达99%，早上9点前及晚上8点后从未发生，且每周一到周三发生频率最高，周四到周日负载逐级下降

Summary:odpapp03(odpapp03)WAS应用服务器wmsnew\_svr1的Web容器线程池使用率达到:99% (当前值:399.999,最大值:400)



# 事件告警日志发生之相关性规律学习



多个操作员在处理不同的事件，但结果问题是同一个

同一个问题触发多个工单，导致SME效率低下

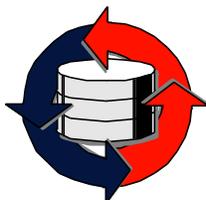
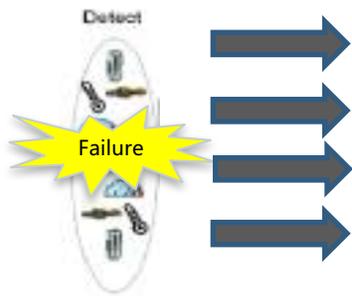
根源定位需要经验、时间和足够视野



**高成本低效率的IT运维**

部分客户可以解决该问题，但需依赖确定的场景、关联规则和专业经验，且云化环境下不具可复制性

**机器学习自动识别事件间相关性可以显著提升IT运维甚至运营效率**



Auto generated or out of the box Correlation rules

Event Clusters

Event ID	Time	Source
IBM900-4104/907-41075-41784-41	780711	Genclass
IBM900-4104/907-41075-41784-41	780711	Genclass
IBM900-4104/907-41075-41784-41	780711	Genclass



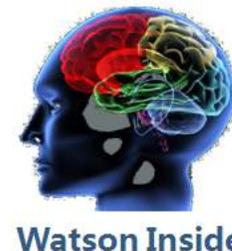
**Related Events Grouping**

IBM Delivered content for grouping well known events. Up to 90% reduction in events out of the box.

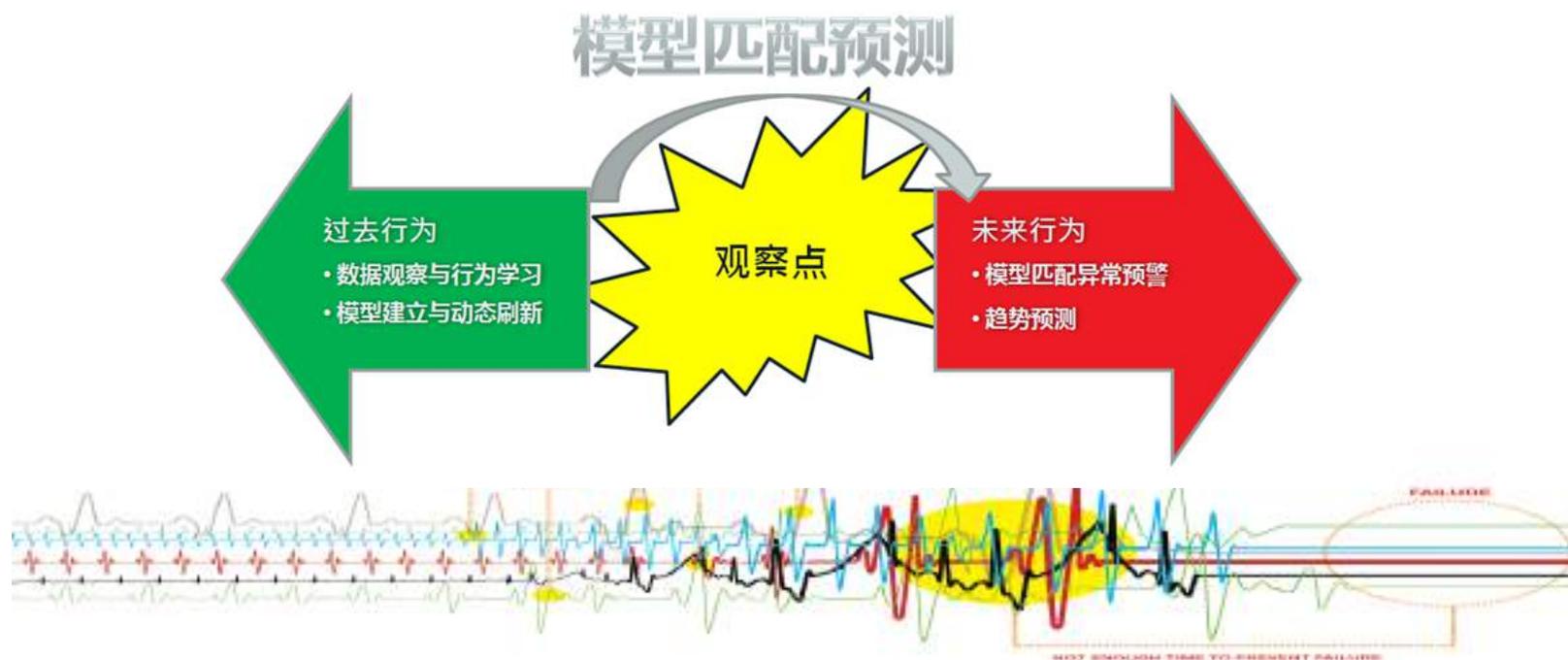
**Related Events Analytics**

Discover clusters of events that occur together, automatically group them for context.

# 结构型大数据认知分析和预测



- Predictive Insight 使用统计学工具，和行为学知算法，揭示指标间的数学关系



# 基于时间序列的KPI行为学知

## – 单个 KPI 认知分析

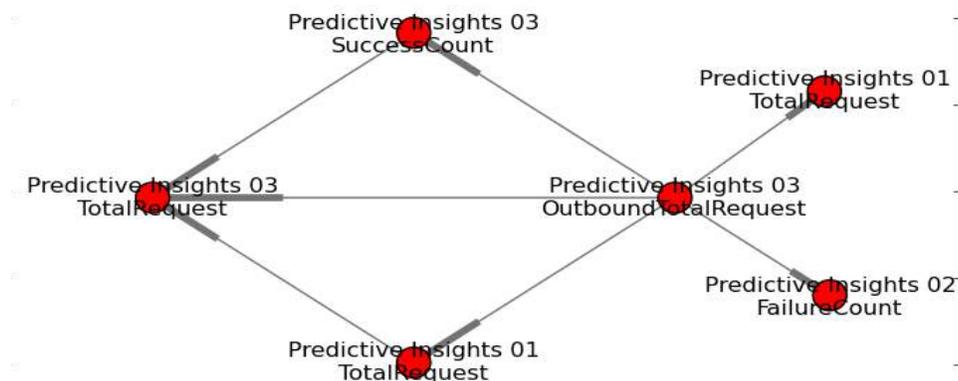
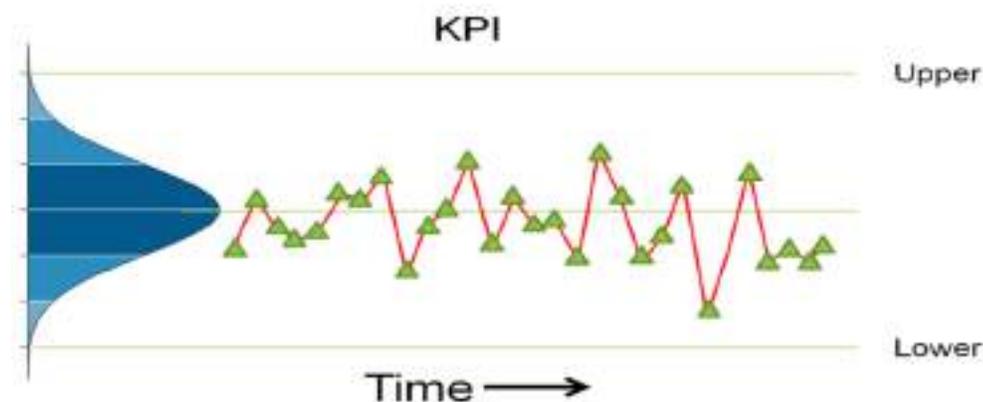
- ✓ 对每个KPI学习其历史的行为
- ✓ 当KPI偏离其历史的行为时，认为是异常
- ✓ 周期性变化分析

## – 多 KPI 认知分析

- ✓ 使用统计学方法识别KPI之间的关系，确立相关性，并确定哪个KPI指标最有可能是其相关的指标数据集合的变化根源
- ✓ 了解正常的行为模式，并在识别到行为模式与正常的行为相异时，发送警告

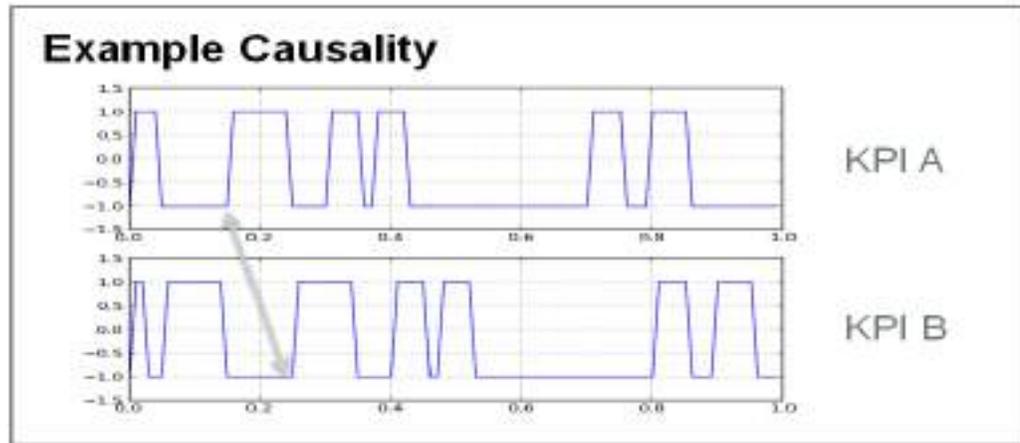
## – 基于 Granger causality test 的方法进行实现

- ✓ 由诺贝尔奖获得者，经济学家Clive Granger提出
- ✓ 使用类似“delayed correlations”等统计测试以确定因果关系
- ✓ 对大量的基于时间序列的数据进行整体分析，识别存在于这些数据中的显著因果关系



# 格林杰因果关系分析 ( Granger Causality )

If KPI A makes the future predictions of the value B significantly better than using past values of B on their own then it is considered to be Granger Causing



**DEFINITION 1: Causality.** If  $\sigma^2(X|U) < \sigma^2(X|U - Y)$ , we say that  $Y$  is causing  $X$ , denoted by  $Y_t \Rightarrow X_t$ . We say that  $Y_t$  is causing  $X_t$  if we are better able to predict  $X_t$  using all available information than if the information apart from  $Y_t$  had been used.

**DEFINITION 2: Feedback.** If

$$\sigma^2(X|U) < \sigma^2(X|U - Y),$$

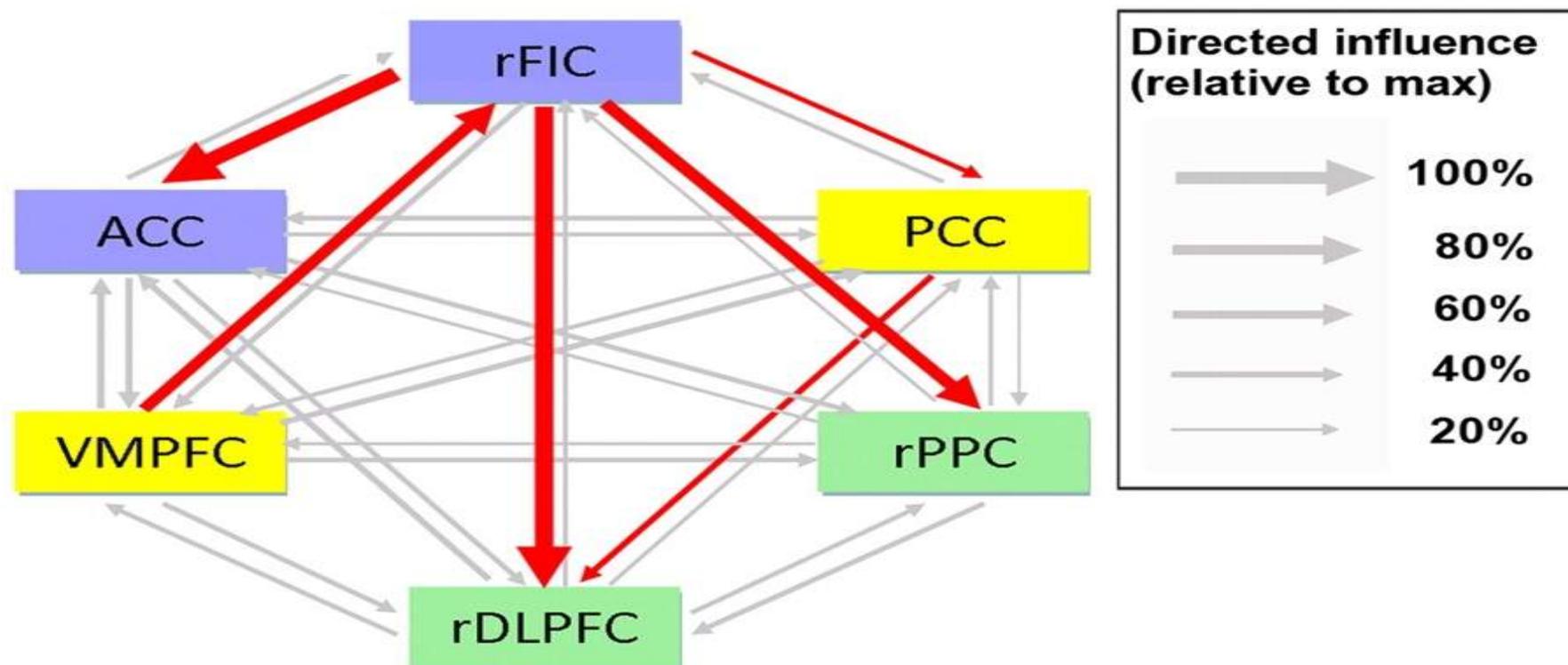
$$\sigma^2(Y|U) < \sigma^2(Y|U - X),$$

we say that feedback is occurring, which is denoted  $Y_t \Leftrightarrow X_t$ , i.e., feedback is said to occur when  $X_t$  is causing  $Y_t$  and also  $Y_t$  is causing  $X_t$ .

Granger, Clive W. J. "Investigating Causal Relations by Econometric Models and Cross-Spectral Methods." *Econometrica* 37, 424-438.

# 格林杰因果关系分析 ( Granger Causality )

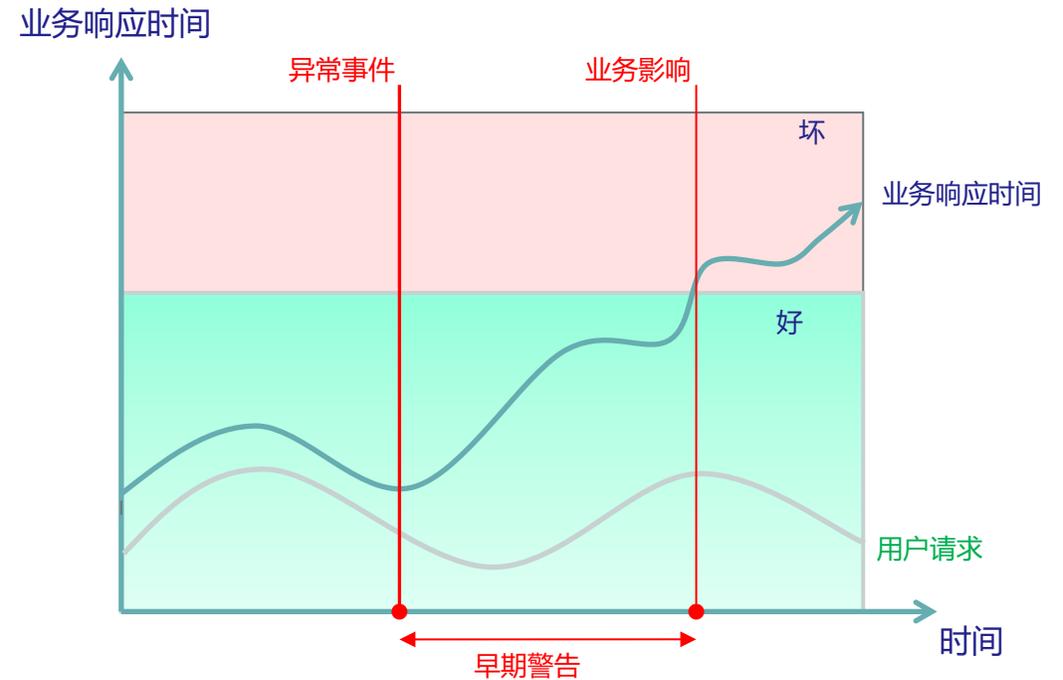
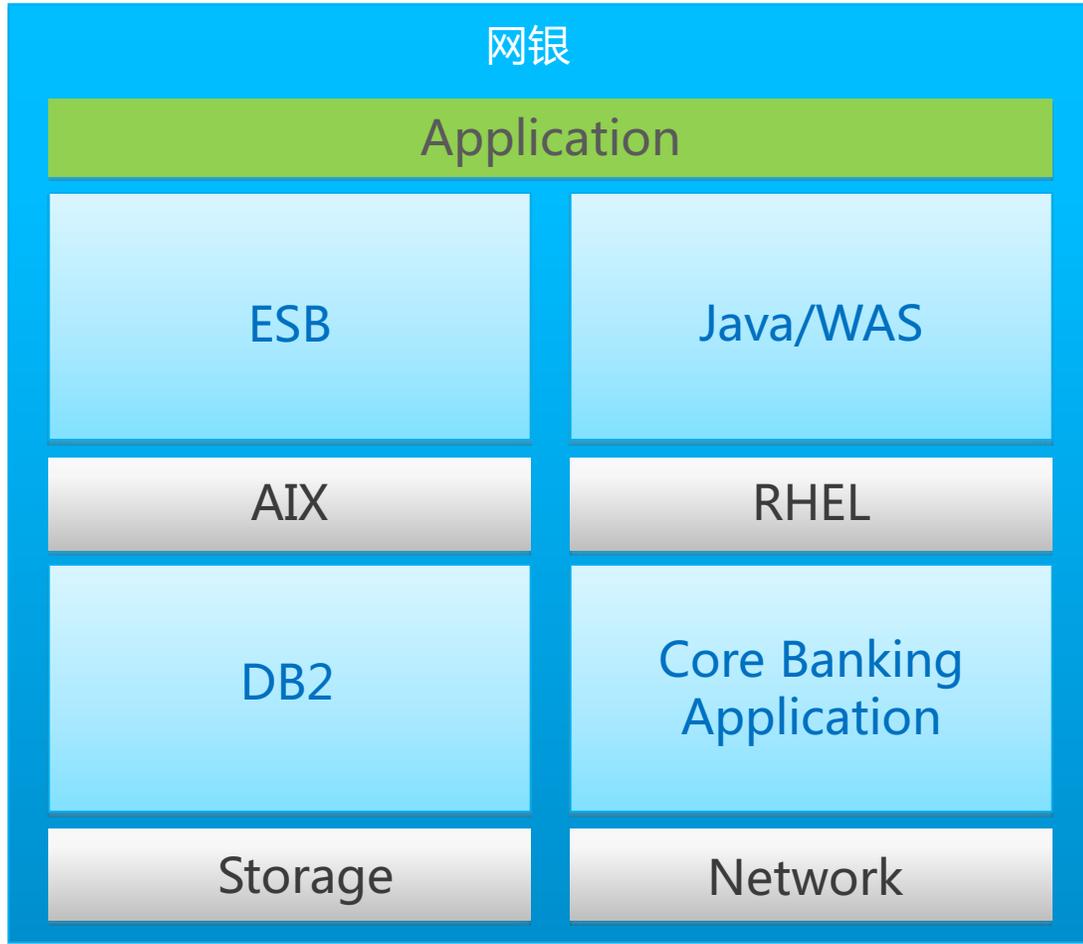
格林杰因果关系描述，箭头指示因果，粗细描述关系强弱:



Sridharan, D., Levitin, D.J. & Menon, V. A critical role for the right fronto-insular cortex in switching between central-executive and default-mode networks. *Proceedings of the National Academy of Sciences of the United States of America* 105, 12569-12574 (2008).

# 多KPI相关性认知学习和预警

目标：自学习各指标数据间的正常算法关系



- PI学习到，“业务响应时间”与“用户请求”有正相关因果关系 – 且随着用户负载增加而变慢。
- 如果这一正常历史规律被破坏，比如说由于内存泄漏，造成即使用户请求数下降了，业务响应时间还很高，异常预警信号将立即发出。
- 问题被发现，尽管这时业务服务质量仍处于“好”的区间

正在发生的问题可被检测出来，尽管从阈值或监控数据的绝对值衡量仍属正常。

# 多KPI相关性认知学习和预警

某银行基于PI测试系统录入历史生产数据进行分析，发现除双11外，PI报出在11月13日的指标异常明显增多



# 多KPI相关性认知学习和预警

经上下文钻取发现，11月13日上午8:30左右报出2个指标异常预警：**失败交易数**和**交易总时长**，均和贵金属营运系统相关，并列多个因子指标，包括贵金属交易数和交易成功时长从缓慢然后到急剧升高，随后是交易失败数和队列等待数从缓慢到急剧升高，9:30左右2个MQ队列阻塞至上限，PI Granger分析给出指标间因果关系，可明显看出导致该问题的主要原因为贵金属并发交易数过大导致交易处理时间过长。

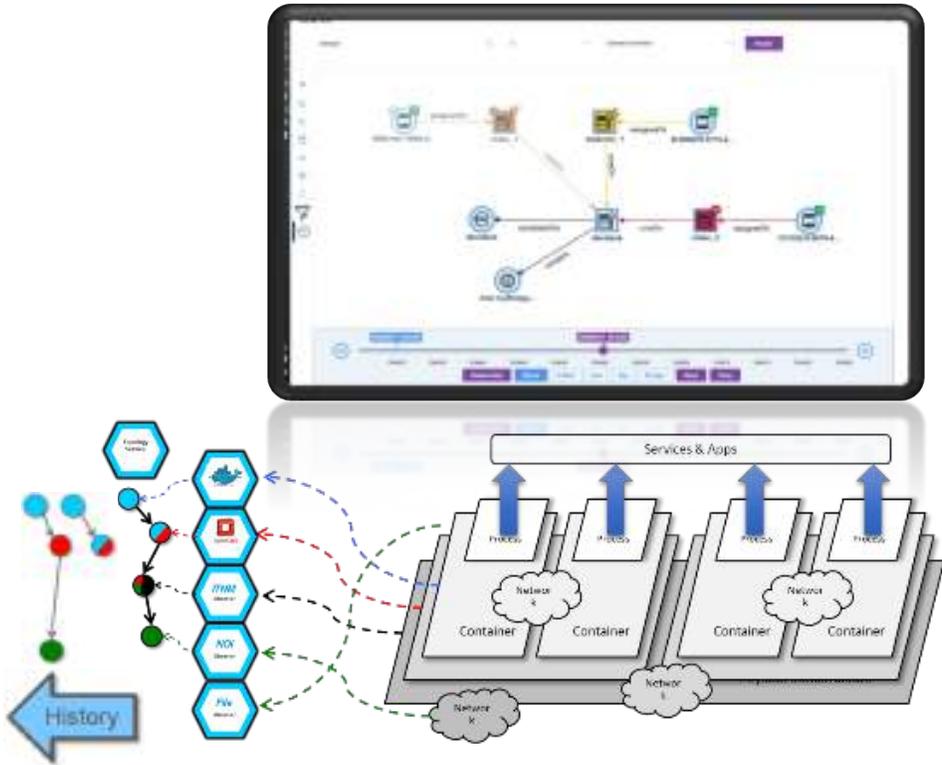




# 混合云端到端服务拓扑管理



NOI提供覆盖混合云NFV & SDN动态基础架构与服务的端到端可视化与敏捷管理能力



- 端到端的OSI7层拓扑实时跟踪
- 上下文数据和功能整合以快速定位和修复问题
- 客户交易、网络服务、底层基础架构映射与关联
- 动态可变实时拓扑与历史拓扑比对 - 快速定位变更与依赖
- 基于容器和微服务设计
  - 快速部署和生效
  - 新功能快速迭代 (devops)
  - 弹性伸缩
  - 自修复

预定义集成并已发布



Network Manager Operations Insight

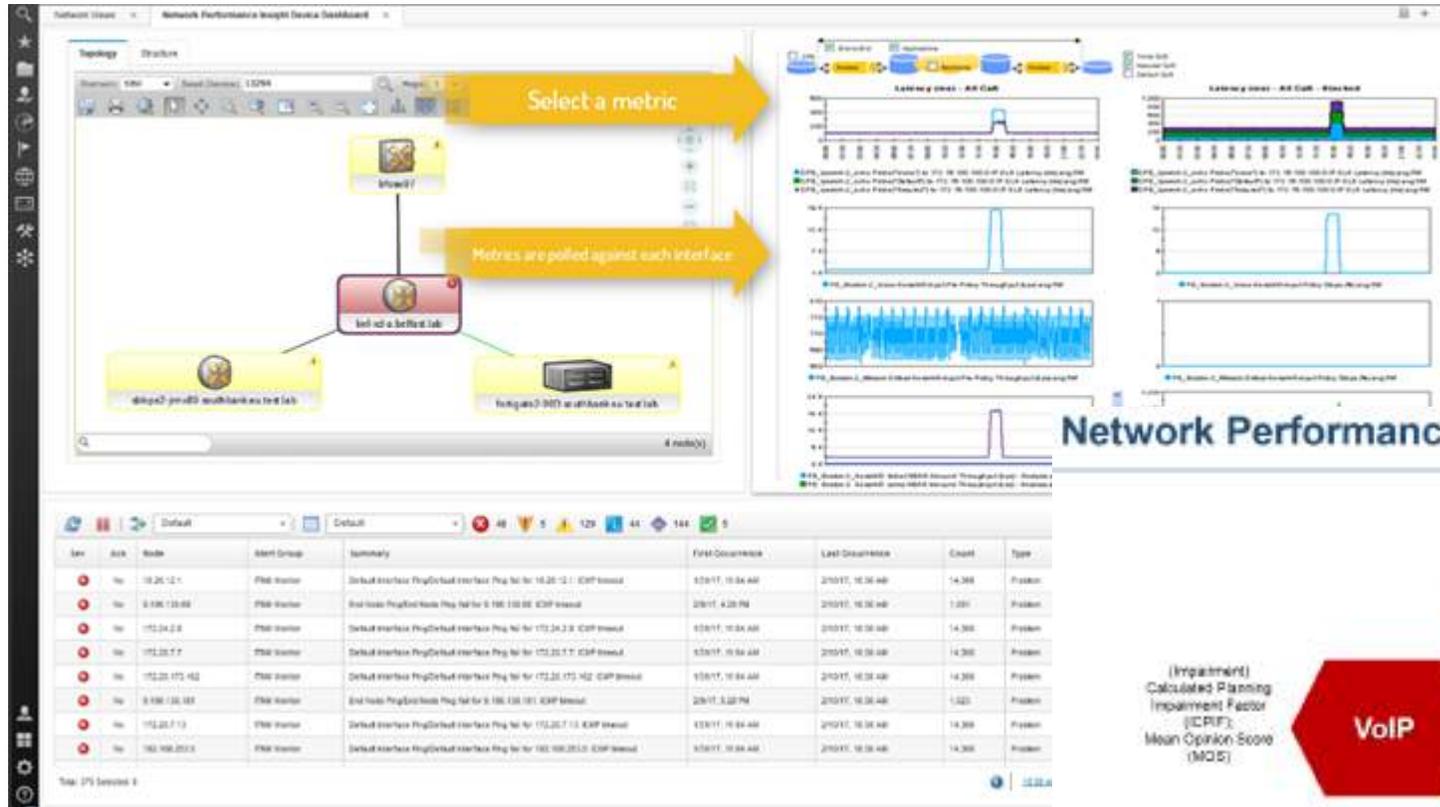
File

Supported by Rapid & Continuous delivery of new Observers



Supported on Linux only

# 告警、性能、拓扑相关性认知分析与诊断



Network Performance Insight – QoS metrics scope



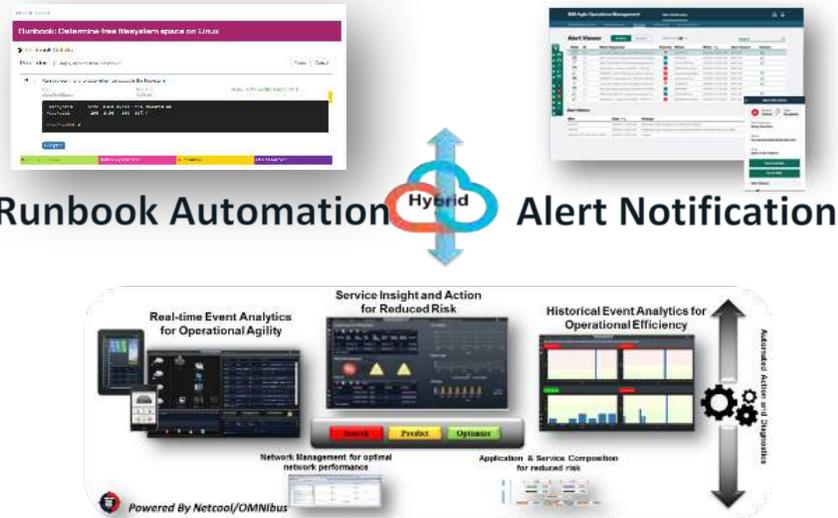
# 混合云敏捷运维与知识共享

提升运维自动化能力：日常操作自动化，交流与知识共享，以加速解决日常运维常见问题。  
迅速延伸已有Netcool方案能力，和快速投资回报的实现



## Runbook Automation

Create and Execute Runbooks and Automated tasks for **faster, more repeatable and consistent problem resolution**



## Alert Notification

Escalation policies, notifications, and alert analytics for **driving greater efficiencies** in responding to IT situations and customer problems

**Designed to work seamlessly with existing solutions** – work with on-prem tools with the benefits of Cloud

**Improve ROI** - immediate value add and improved ROI on existing investments

Continuously **drive operational efficiency and knowledge** – built-in tracking and analysis of automated IT operational activity

# IBM认知IT服务管理路线图



应急救火



基于洞察以提升效率



基于洞察以提前预判



基于Watson的认知决策

Value In market today

Roadmap

A fully Cognitive Solution



Cognitive Data Scientist

针对结构化数据如性能指标的机器学习，动态建模和异常探测，如IOA-Predictive Insights.

事件告警日志拓扑等非结构化流数据分析、认知学习，如Netcool Operations Insight.

Cognitive, on machine data

The cognitive on ramp

基于Watson认知分析助手的7x24不间断关注，更广泛的知识 and 经验提供 (倾听、学习和交互)

IT运维大数据平台构建，冷数据分析，如IOA-Log Analysis; 基于确定场景或模型的关联学习和分析，如Impact RCA.

Analytics Solutions

# IBM认知IT服务管理 – 价值提供



运输制造

世界领先的某运输设备制造商，制造卡车、客车、建筑设备、船舶和工业发动机，依靠Netcool管理其网络基础设施，**监控事件需人工干预数量减少达90%**



电信运营商

美国大型电信运营商，通过使用Netcool显著提高他们的服务水平，能够监控到更多事件、以更快的响应速度和预见能力。借助Netcool对客户问题的响应和解决速度 – **MTTR 提升95%**



金融服务

某欧洲跨国银行借助Predictive Insights的预警预测能力，**3个月内业务故障率下降了85%**



物联网

世界领先的模具设备制造商使用Netcool及APM监控EVA设备整体运行状态，以快速定位和解决设备生产和运行问题，**显著提升了设备质量和客户满意度**



电信运营商

某跨国电信运营商，通过Netcool集中管控约8万台设备，每天数百万事件量，**减少平均修复时间达84%**，由此**贡献业务年增长率70%**



更多 IBM 混合云IT服务管理相关信息，请扫描



**IBM ITSM 产品与服务咨询热线：400-668-0529**

**或者给我们写信**

**[ibmcloud@cn.ibm.com](mailto:ibmcloud@cn.ibm.com)**