集中监控管理解决方案

目　录

1. 客户需求和业务驱动力

1.1.客户需求和驱动力

随着各行业企业的 IT 基础设施越来越庞大，管理的复杂度不断增加，对故障响应和处理的实时性要求越来越高，对关键性能指标 KPI 变化的掌控要求也越来越高。同时，管理扁平化趋势也越来越明显，传统分专业和应急式的监控管理架构已不能适应越来越多用户的要求，需要有集中化、端到端的监控管理解决方案。

多专业、层次化、以及设备类型的多样化，造成上传的管理信息内容差别较大，数据量过大，企业缺乏有效的技术手段掌控全网全专业健康情况，急需告警标准化、分析、压缩、关联和收敛能力。

面向业务和面向业务客户感知运营的转变，要求有针对故障涉及的 IT 资源和服务的分析，便于确定故障影响范围，快速处理故障。

- **实时性：**告警数据量巨大，需要有良好的告警采集处理手段确保实时性；
- **标准化：**各专业，各厂家告警字段定义不同，梳理告警需要有大量的工作；
- **集中化：**扁平化的管理结构，在告警标准化的基础上，统一处理各个专业的告警，需要明确告警关联及预处理规则；
- **影响性分析：**在告警集中化的基础上，明确告警、IT资源和业务的关联关系，建立起告警影响性分析的模型。

1.2.解决方案概述

企业业务服务的可用性，依赖于企业 IT 基础架构端到端的可用性和性能。因此，IT 监控和运维应该从业务服务的角度，对 IT 基础架构实现面向业务的集中的端到端的管理。但是由于历史原因和技术的局限性，许多企业还存在着多个竖井式的，分散的技术领域的管理。无法通过一个统一的窗口，看到业务服务所依赖的端到端的基础架构的状态，实现面向业务服务的集中管理。Tivoli 集中监控管理解决方案关注于整合企业所有竖井式管理工具，实现端到端的信息采集，分析处理，业务关联，从而实现企业基础架构和服务的集中监控和管理。Tivoli 集中监控解决方案基于 IBM Tivoli Netcool 套件，遵循 SOA 架构，采用层次化逐级收敛的设计模式，将采集，核心处理及应用展现分离。便于扩展管理新接入 IT 设备、系统及应用，或者扩展新的应用功能，而不需要对核心服务和架构进行修改，实现 IT 环境全专业端到端的集中监控、自动派单和展现。

IBM 集中监控管理方案提供同 CMDB、配置管理系统、性能管理系统、电子工单管理系统等的接口，可以实现网元故障告警、性能告警、应用与系统平台告警的统一管理，如：告警过滤、故障压缩、影响性分析、关联分析、告警监视、告警处理等功能。此外 IBM 集中监控管理系统还提供强大的规则引擎，方便用户自定义告警处理规则。

1.3.技术挑战

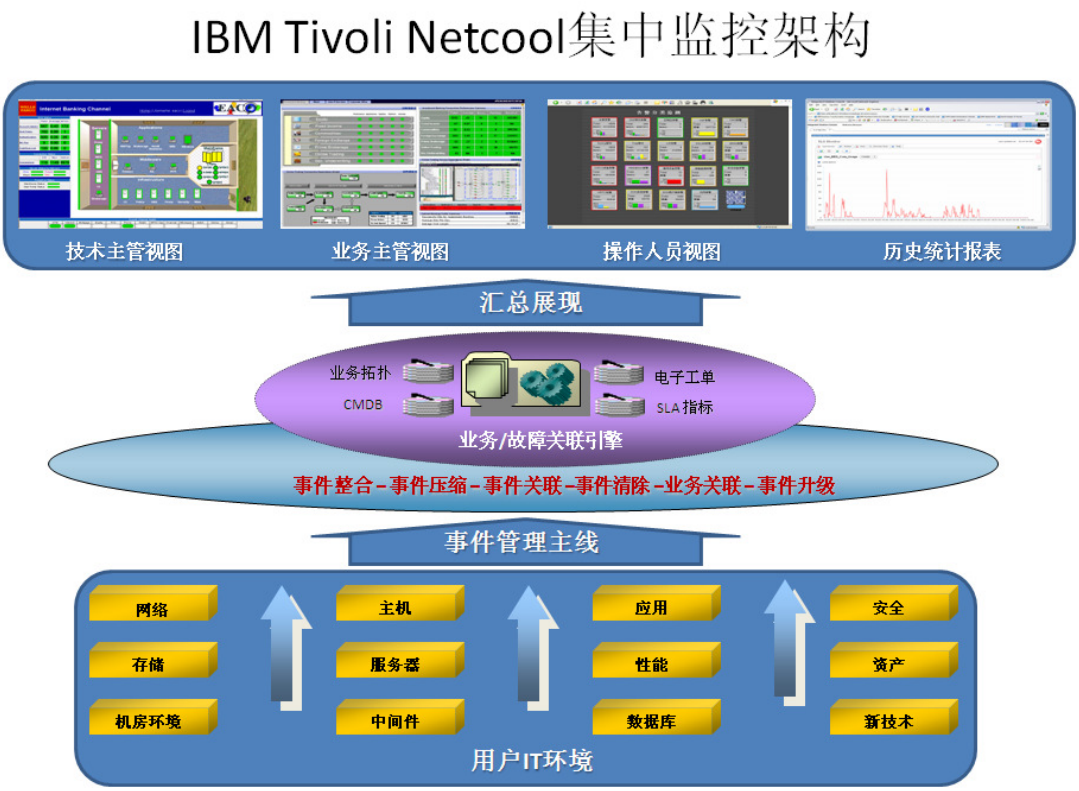
- **如何实现多厂商跨专业设备支持与覆盖广泛，无需大量定制，是集中监控管理区别于其他项目的显著要求：**IBM Tivoli Netcool 提供超过针对一千多种不同网络环境的采集探针，可以支持目前业界几乎所有的IT设备与 EMS；
- **如何确保效率与技术的先进性是集中监控管理成功的必要条件：**IBM Tivoli Netcool核心内存DB的

事件处理能力超过2千条事件/秒（包括事件压缩，分析，业务关联）；

- **如何与CMDB关联分析和RCA能力是集中监控管理的最核心功能要求：** IBM Tivoli Netcool所提供的强大的事件采集处理能力，再加上其灵活的影响分析引擎，可以充分保证在任何资源故障发生以后，快速定位其对相关业务的影响，从而让运维人员能在第一时间获得任何业务故障的报警提示和根源所在；
- **如何提高灵活性是集中监控管理可持续成功的保证：**IBM Tivoli Netcool所提供的Integrated Portal可以灵活的嵌入或集成任意第三方基于WEB的应用，可以根据用户特定的业务配置关系建立业务逻辑视图。同时又提供全面的集成第三方管理平台的接口模块。

建立集中化的监控管理平台，实现故障信息的全生命周期统一管理，提供相应的影响性分析报告，让用户清楚地了解网络状况及业务影响情况，并能快速相应处理告警，大大提高了告警处理的效率，提高了告警的实时性、准确性，使故障对网络的影响降低，提高网络可用性。

2. IBM 集中监控管理解决方案架构



IBM 集中监控管理系统主要架构由三个层次构成：采集层、服务层、应用层。

- **Layer 1 - 采集层**

在这一层次的采集器（Probe&Monitor）可直接从用户 IT 环境（如网络设备、主机应用等）实时采集故障及性能状态变化数据，采用 IBM Tivoli Netcool 的统一采集模块来实现。

- **Layer 2 - 服务层**

各专业事件在这一层次经过汇总、压缩、关联和自动清除，并结合 CMDB 和业务服务配置等信息实现故障根源定位、业务关联和业务服务的影响性分析，其结果可服务于电子工单的自动生成、监控应用展现或历史统计分析服务。

- **Layer 3 - 应用展现层**

面向用户各管理角色的人员提供所需的综合监控和查询调用功能等。

3. 集中监控管理功能概述

面向业务服务 IT 综合监控平台功能需求主要包括：综合事件数据采集与集成、统一的事件管理平台、与资源配置数据库的集成、事件综合呈现、业务服务管理等。

集中监控管理系统主要实现如下功能：

- 综合事件数据采集与集成，主要实现与客户现有 IT 管理系统的事件级集成系统监控的告警事件集成，主要包括：
  - ✧ 系统监控的告警事件集成
  - ✧ 应用监控的告警事件集成
  - ✧ 网络监控的告警事件集成
  - ✧ 各类硬件监控的告警事件集成
  - ✧ 机房环境监控的告警事件集成
  - ✧ 桌面机监控的告警事件集成
  - ✧ 安全监控的告警事件集成
  - ✧ Service Desk 的集成等

- 统一的事件管理平台主要完成对各类事件的集中存储、压缩、过滤、相关性分析、自动化处理等工作，其主要功能包括：
  - ✧ 告警事件压缩
  - ✧ 告警事件过滤
  - ✧ 告警事件相关性处理
  - ✧ 告警事件通知
  - ✧ 告警级别调整
  - ✧ 告警事件自动处理
  - ✧ 管理平台的高可用性设计等

- 与资源配置数据库的集成主要完成 IT 综合监控平台与客户的资源配置数据库的实时集成，从而实现实时采集的事件信息的配置资源信息的丰富和与业务的关联，其主要功能包括：
  - ✧ 预集成的资源配置数据库的连接功能
  - ✧ 与告警事件实时关联
  - ✧ 利用资源配置数据库，对实时告警事件信息丰富和业务关联
  - ✧ 利用资源配置数据库，实现实时告警事件与告警事件处理建议的关联
  - ✧ 基于资源数据库的告警关联分析

- 事件综合呈现主要完成综合的集中事件展现工作，其主要功能包括：
  - ✧ 提供 IT 基础架构告警事件总揽视图
  - ✧ 提供面向各个业务和应用的基础架构监控视图
  - ✧ 实现用户分级分权呈现
  - ✧
- 业务服务管理主要目标是建立业务服务模型，实现端到端的面向业务和服务的运维管理，其主要功能包括：
  - ✧ 基于业务的 IT 基础架构模型管理
  - ✧ 业务服务实时监控
  - ✧ 业务服务告警产生
  - ✧ 业务服务 SLA 指标设置和指标监控

建立面向业务服务的 IT 综合监控平台，将实现：

- ■ 将客户已有系统管理软件无缝集成到统一的 IT 综合监控平台中。
- ■ 实现面向不同被监控领域事件的汇总、重复事件压缩、事件的相关性处理。
- ■ 通过 IT 综合监控平台，有效的减少需要技术人员人工处理的事件量。

- 通过集中的事件平台实现统一的 IT 基础架构运行状况的实时监控和展现。
- 通过 IT 综合监控平台项目的实施，完成与故障工单系统的唯一接口。
- 实现综合的 IT 故障和事件统计分析报表，为各种业务发展提供必要的 IT 基础设施综合数据支撑。
- 通过 IT 综合监控平台的建设，进一步加快对 IT 基础设施各类问题的综合发现能力,大大提高对 IT 基础设施的问题定位速度。
- 在 IT 基础架构监控的基础上，建立业务系统的应用模型，监测支持业务流程的 IT 基础架构所有组件的运行状

4. 解决方案特点

本方案选择 IBM Tivoli Netcool 做为构建平台，IBM Tivoli Netcool 在实时故障管理及服务水平管理领域中是行业的领导者，该产品具有以下功能特性：

- **专业性**：IBM Tivoli Netcool管理软件是以故障管理为核心、以业务模型为基础、以业务高可用性为出发点、采用分布式结构、通过面向对象技术实施综合监控管理的唯一专业软件。在IBM Tivoli Netcool系统中，集中监控模型完全由用户定制，可以是一个端到端的应用、一项业务服务、一个商业客户、一个VPN网络或是一个端到端的服务连接，IBM Tivoli Netcool能够将管理事件或告警信息与对应的监控模型进行快速有机的关联，从而真实地描述现实中的IT环境和业务环境状态，确保业务服务的高可用性。
- **实时性**：IBM Tivoli Netcool提供一个驻留内存主动式面向对象的数据库，按对象方式存储事件和服务数据。采用“PUSH”机制，可以使服务定义和事件管理实时运行在极高事件产生频率的网络中。
- **适应性**：IBM Tivoli Netcool可与用户现有体系结构无缝集成并可以快速实现调整。软件可以在全部主流UNIX操作系统和Windows上运行，数据采集探针可支持超过一千种网络设备和环境的数据采集。整个系统易于配置和管理 ，具有友好的人机交互界面。
- **定制性**：IBM Tivoli Netcool可定制体现在两方面。第一，方便与现有IT环境集成，可以提供从各种已有管理平台中收集数据。第二，提供二次开发接口，可以根据用户的具体需要进行定制。
- **扩展性**：从技术角度讲，不可能预测IT环境中事件发生率。小的IT环境可能产生大量事件，而大规模的IT环境也可能产生相对比例小的事件。IBM Tivoli Netcool软件的分布式的主动式数据库结构，使得管理平台的信息采集和集成速度足够快，并可以满足扩展性的要求。

5. 目标市场及成功客户

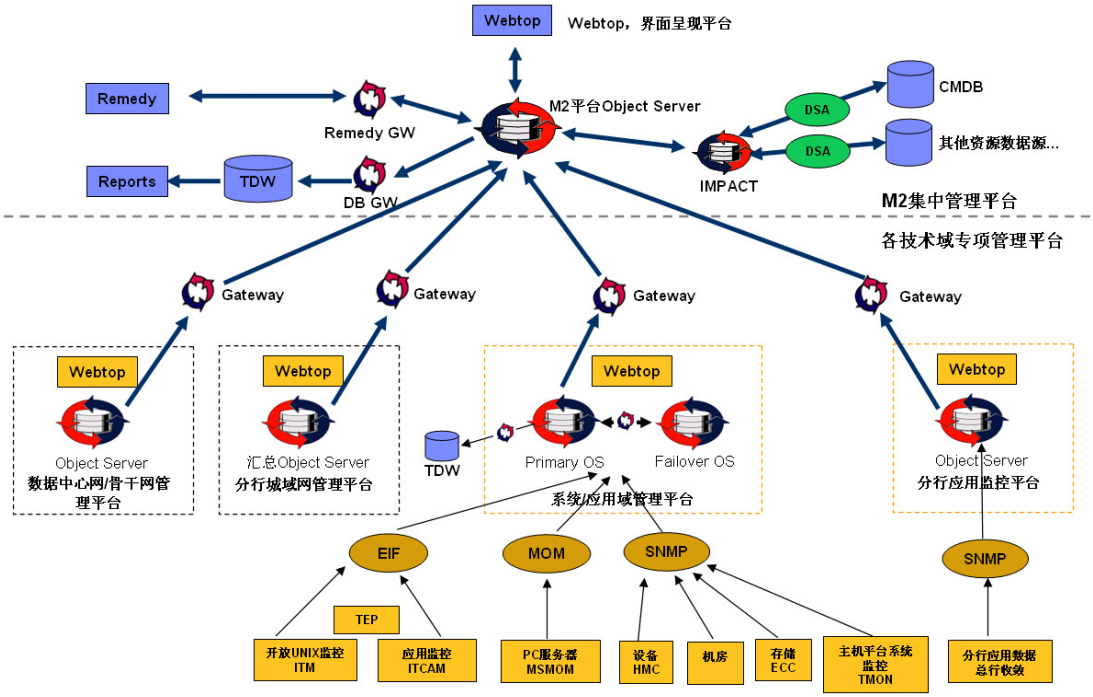
目标市场：

- 需要集中监控和管理跨平台、多专业、复杂异构的IT基础架构的用户
- 需要实现从网络、系统、关键应用等端到端集中监控的用户

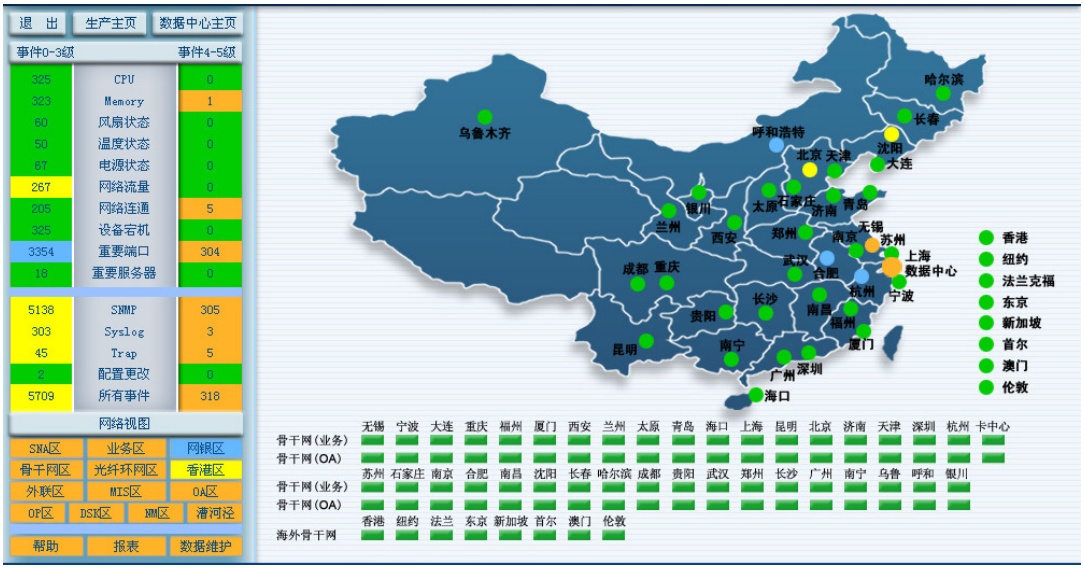
成功客户：

- 国内某商业银行

国内某商业银行采用 IBM Tivoli Netcool 综合监控解决方案建设其跨专业端到端的集中监控管理系统，覆盖从网络、主机服务器、数据库、应用等所有专业资源和设备，范围从全行到数据中心的全面管理。采用 3 级分布集中式管理架构，由建设于总行的 IBM Tivoli Netcool 综合监控平台负责监控所有 IT 专业资源的状态和关键业务服务的端到端状态和能力，并基于所接收的重要 IT 事件，实时关联各专业资源存储于 CMDB 内的配置信息，实现告警关联压缩、前转通知和业务服务的影响性分析，极大的提高了 IT 运维监控效率。其总体部署架构如下：



监控图例如下：


退 出
生产主页
数据中心主页
事件0-3级
事件4-5级
325 CPU 0
323 Memory 1
60 风扇状态 0
50 温度状态 0
67 电源状态 0
267 网络流量 0
205 网络连通 5
325 设备宕机 0
3354 重要端口 304
18 重要服务器 0
5138 SNMP 305
303 Syslog 3
45 Trap 5
2 配置更改 0
5709 所有事件 318
网络视图
SNA区
业务区
网银区
骨干网区
光纤环网区
香港区
外联区
MIS区
OA区
OP区
DSM区
NM区
灌河径
帮助
报表
数据维护
哈尔滨
长春
乌鲁木齐
呼和浩特
沈阳
北京
天津
大连
银川
太原
石家庄
青岛
济南
兰州
西安
郑州
南京
无锡
苏州
上海
数据中心
成都
重庆
武汉
合肥
杭州
宁波
长沙
南昌
贵阳
福州
厦门
昆明
南宁
深圳
广州
海口
香港
纽约
法兰克福
东京
新加坡
首尔
澳门
伦敦
骨干网(业务)
骨干网(OA)
无锡 宁波 大连 重庆 福州 厦门 西安 兰州 太原 青岛 海口 上海 昆明 北京 济南 天津 深圳 杭州 卡中心
苏州 石家庄 南京 合肥 南昌 沈阳 长春 哈尔滨 成都 贵阳 武汉 郑州 长沙 广州 南宁 乌鲁 呼和 银川
香港 纽约 法兰 东京 新加坡 首尔 澳门 伦敦
海外骨干网