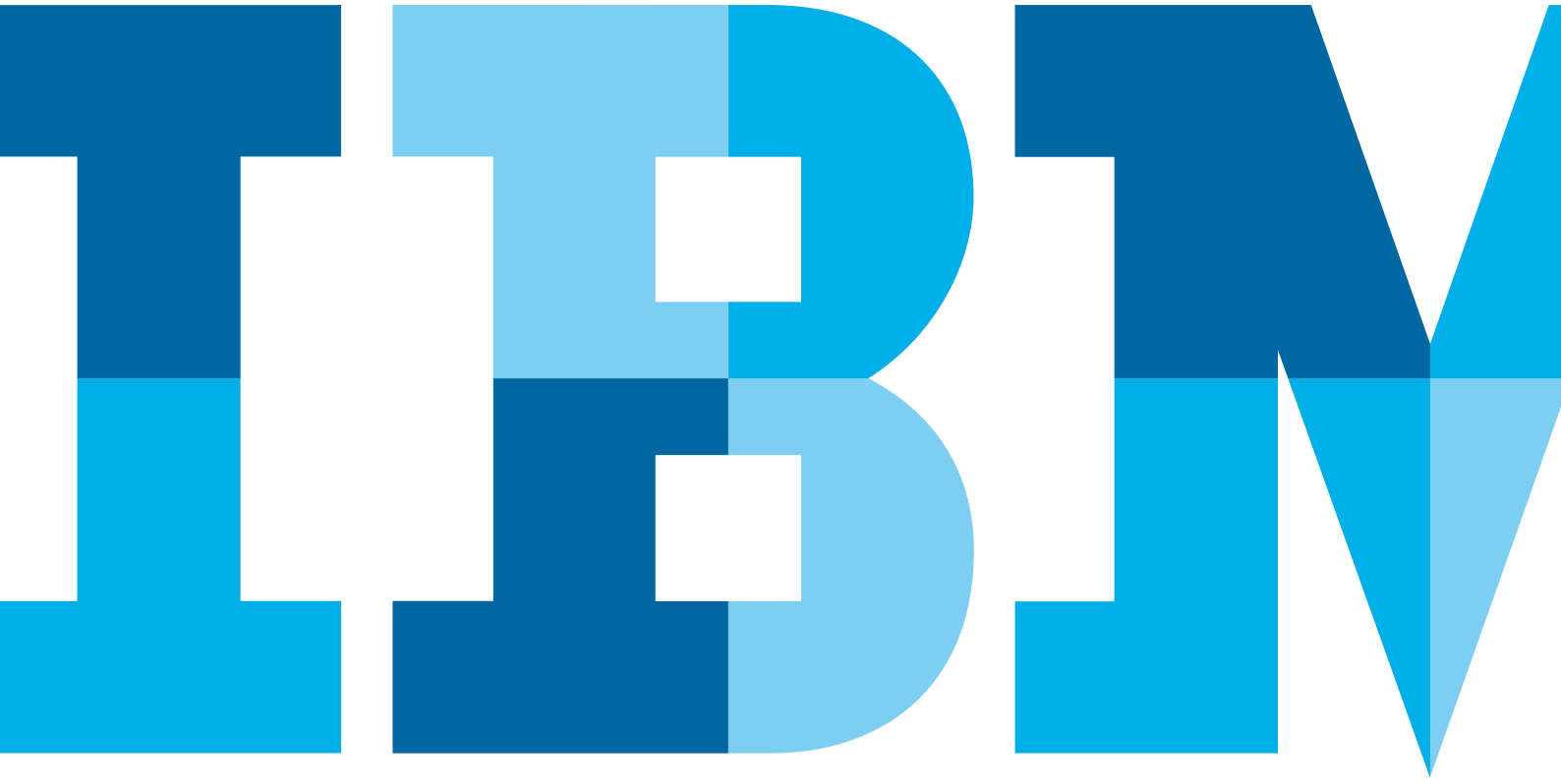
IBM软件部

数据化运维管理，
让你更为从容地面对IT运维的挑战



数据化运维管理，
让你更为从容地面对IT运维的挑战

业务发展带来新的IT运维挑战

当传统业务遇到互联网+和数位转型会缤发出多大的机会？当移动应用成为企业用户访问的主要媒介时，系统会有多大的压力？当每个企业都在认真思考拥抱O2O、C2B、B2C、B2B时，每个企业的领导者都会思考如何才能追赶市场的领先者。

这一切给IT系统带来的压力让很多CTO/CIO都在寻找各种可能的系统架构、应用架构、运维架构。而其目标只有一个：快速满足业务需求并且确保用户的满意度。运维能力成为其中一个必须要考虑且日益重要的部分，因为快速拓展的业务没有有效的运维保障，任何一次的访问失败都可能导致用户的流失、企业信誉的下降、乃至竞争力的丧失。

有一点逐渐得到几乎所有的运维主管的认可–即传统的监控-分析-响应的运维模式虽然对部分成熟系统而言还是行之有效，但已经不能适应新需求的发展速度。云计算、移动计算、大数据等新兴技术在给业务系统带来巨大能力的同时也给运维带来巨大的挑战。

我们的着眼点必然也是重新思考互联网时代的运维方式。实现高效并在投资回报上带来收益。

高效的IT运维必然希望更少的人力介入，更高的自动化能力、以及更为智能的决策判断。这通常包括如下几个方面的管理实现方法：

1. 数据化管理:通过对IT运维数据的抽取、识别、分析来提升管理能力；
2. 自动化运维:通过标准化地执行管理任务来提升管理效率，降低管理成本；
3. DevOps:即开发到运维的一体化，通过连续开发、连续运维来快速落实业务需求，借助数据化管理从运维中提取对开发有帮助的诊断数据，借助于自动化来加速应用的发布和资源的调配。

高效运维的另一目的就将IT运维从一个成本中心转变为业务发展的重要支撑平台，通过数据化、自动化来节省业务运营成本，从而提升企业的核心竞争力。

数据化运维

数据化运维就是采集用户IT系统运行的各个层面数据，借助于大数据分析、机器学习、神经网络等技术，从而为IT运维提供决策判断和前瞻预判，以提升IT运维的自动化能力。

所有的IT运维组件，无论是性能管理模块、还是故障管理模块、或者配置管理模块、SLA管理模块，都是以不同类型数据来驱动的。离散的数据没有价值，所有运维数据都应该和运维管理场景关联。且竖井式的管理已无法满足现今与未来的IT运维管理要求。

- 配置数据不仅帮助了解系统的配置现状，更可以在故障分析、应用发布、灾备切换等场景中提供必要的基础数据；
- 监控数据不仅帮助了解资源使用情况及交易性能，更可以在应用诊断时提供必要的分析数据，从而给研发团队快速提供问题定位；
- 日志数据不仅帮助了解中间件和应用发生的错误信息，更可以通过文本分析来给出复合错误的排名和统计。

所以，数据化运维的实质是挖掘管理数据中隐涵的有助于提升IT管理服务能力的信息，从而为IT运维提供更为全面的支撑。

运维数据的产生和管理

配置数据管理

目标：实时扫描收集整个IT系统的配置数据，包括操作系统、中间件、数据库、网络组件、商业应用等，从而了解最新的系统组成、配置参数以及组件间的关联关系。

管理场景1: 配置查询

在管理界面输入各种查询条件, 如IP地址、服务器名、应用名等来查询对应的系统组件及其详细配置参数。或者输入诸如 "所有OS为Red Hat Enterprise Linux Version 6 Update 6、memory >= 16G, IP地址在210.90.90网段内的非J2EE或者数据库服务器" 等或者 "所有运行JDK仍为1.6的Weblogic服务器" 等查询条件来获得满足条件的系统列表。

管理场景2: 获取配置变化列表

定期生成或者在每次系统变更后生成指定时间内的配置发生过改变的对象列表报告, 以了解系统配置的变化情况、当前值、或者核对系统变更操作的正确性。或者在系统升级后检查前后版本之间的配置差异, 如J2EE JVM大小是否从500M加大到800M以满足应用的运行需要。

管理场景3: 确保集群内的系统的重要配置的一致性

对多个需要保持配置一致的系统进行配置一致性检查, 如在同一应用下的同一类型组件进行配置核对以确保其重要参数的一致性, 或者可以检查所有机器上的安全配置参数是否一致, 如net.ipv4.ip_forward = 0.

管理场景4: 生产和灾备的一致性检查

定期扫描检查比对生产和灾备系统之间对应系统的配置是否存在差异, 以确保系统在进行灾备切换后应用可以顺利运行。

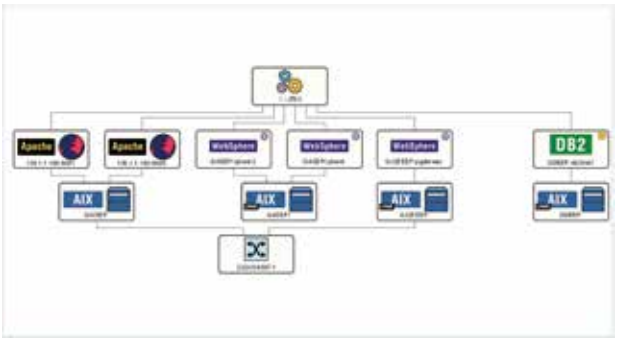
IBM解决方案:

IBM Application Dependence Discovery Manager (TADDM)主要提供以下三个方面的管理能力:

1. 帮助了解当前的配置情况和详细配置参数

TADDM提供了超过70种的扫描传感器以收集各种商业系统的配置数据:

并且可以通过配置或者手工设置来获得业务应用的组成和关联情况:



2. 帮助了解系统的配置变化

TADDM在每次扫描后会计算是否存在配置发生变化的情况, 如果是则生成告警事件并且可以生成变化报告:

3. 帮助了解系统之间的差异性

TADDM提供了基线比对、历史比对、关系比对等多种组件配置参数比对以发现配置信息的不一致性。

客户案例：

IBM帮助一国内银行成功实施配置数据的集中采集、差异比对，总的配置数据项超过100万。客户每天定期扫描来发现配置的变化，并且对生产和灾备系统进行定期检查以发现配置不一致的对象，从而极大地减少了维护人力且灾备切换的成功率也有了很好的保障。

监控数据管理

目标：实时获取IT系统组件的性能和故障数据，了解从网络、系统到应用，从交易到事务的运行数据，从而及时发现性能瓶颈和故障发生，并且可以实时切换到诊断模式来获取应用运行详细信息，诸如请求、Java Method调用、JSP调用、JDBC访问或者 Message Queue访问等，从而为应用故障提供有用的诊断数据。

管理场景1：全方位IT运行监控

IT运维最基本却又是最不可缺少的部分，无论是网络、系统、中间件、应用组件都需要实时获取其运行状况，性能和故障数据。

管理场景2：交易性能管理

获取应用交易各个环节的性能数据，从客户端访问、到HTTP服务器、J2EE服务器、乃至和后端数据库之间应用访问性能数据，从而了解最终用户的访问感受、各个区域客户的访问性能、了解哪个交易出现了性能问题、交易的哪段出现了性能瓶颈。

管理场景3：为DevOps提供生产环节的诊断信息

DevOps提倡连续发布、连续管理，这意味着灰度发布将是连续发布的重要方式，部分测试也前移到生产环节，此时就需要运维系统可以在日常监控和应用诊断分析之间无缝切换，实时获得生产环境中的应用实际运行数据；特别是及时抓取新发布应用中是否存在“坏小孩”，加速应用的上线进程。

IBM解决方案：

IBM Tivoli Network Manager提供了网络的故障数据、拓扑数据和性能数据的获取，并且提供了基于二层拓扑的故障根源分析;而在网络故障事件管理上，Tivoli Network Manager用于业界领先的知识库从而可以快速、准确地分析网络故障。

IBM Performance Manager则提供了从系统到交易、子系统乃至事务的全面监控，其监控数据涵盖了系统和应用的各个层面：

同时也提供了J2EE和.Net应用的诊断级别的数据，而切换只在瞬间：

IBM performance Manager不仅支持传统的应用组件，诸如WebSphere、Oracle等，更支持众多的开源组件以满足互联网应用环境的需求，包括：Jboss、Tomcat、MySQL、Node.JS、Python、mongoDB、PHP、Ruby on Rails、Postgre SQL等。

客户案例：

IBM Tivoli Network Manager在国内各个行业都有很多部署客户。而IBM应用监控管理(APM)也在很多金融行业、制造行业的客户那里有很多实现案例。

日志数据管理

目标：收集系统和应用运行时产生的海量日志数据。当每天的日志量从几十G到上百G，乃至几个T，传统的日志分析手段已经无法适用。更需要借助于近几年日将成熟的大数据技术来对日志数据进行收集、索引和KPI计算，而管理员则通过检索、KPI分析等方式来进行问题的快速定位和排错。同时依赖于KPI数据来进行得聚合分析可以了解故障全局发生的频度和分类。

管理场景1：检索含有错误关键词的日志

根据含有特征的关键词来检索错误信息，如ERRCODE=19211，java.lang.NULLPointerException等。

管理场景2：组合查询以了解特定范围的特定信息

如需要了解“在最近的10天内发生在服务器HTP012”上的“错误最多的十大Java classes”。

管理场景3：基于指定条件的自动告警

如数据源WASLOG.1上严重等级为”WARNING”的情况在5分钟发生了4次，即产生告警并通知到指定的管理员。

IBM解决方案：

IBM Operation Analytics - Log Analysis基于IBM在大数据上的技术积累，提供单一整合平台，将不同专业的日志、问题单、手册等结构化与非结构化数据进行集中采集和日志索引，从而让相关应用团队针对实时与历史数据与资料进行搜索分析；如出现问题的前后2分钟日志或者特定告警码在多个服务器上产生的日志，加速故障根源的搜寻。

IBM Operation Analytics - Log Analysis提供了WebSphere、MQ、BPM、DataPower、IIB、TSM、DS8000、SCCD、BMC Remedy（？）等的开箱即用日志智能分析包，以及针对不同数据库(如：DB2，Oracle)和HTTP

server的日志智能分析包，从而可以快速了解日志内涵。

客户案例：

IBM利用Operation Analytics - Log analysis在国内协助某银行透过整合各专业的日志加以搜索分析，将问题定位效率提升超过30倍。

管理数据聚合分析

IT运维数据的采集及在各专业域内的使用只是数据化管理的第一步。正如任何的决策都需要一个聪明的大脑，数据化运维也希望可以汇聚所有的管理事件和KPI数据，从而可以借助于多维度统计分析、机器学习等技术来前瞻性地基于规律或者模型来预测将要发生的问题。

智能化事件管理

目的：我们看到很多客户都已经采用一个或者多个产品来监控系统的各个层面，但又往往抱怨过多的监控事件不仅无法有效地处理真正重要的问题，时刻在疲于奔命，所有的问题定位与根源分析往往依赖于运维人员的经验。现在受惠于更进一步的分析技术，数据化运维不仅希望可以将所有层面的告警信息进行集中汇聚，和相关配置信息等关联分析以确定优先级;更希望基于一段时间内的告警历史的学习，生成基于告警发生频率和可信度为维度的统计报告;并且通过下钻报告来发现特定告警的发生规律，比如某些告警只在周一上午频繁发生等，从而可以结合此类规律并结合具体的系统配置来进行问题解决或者设计特定的告警响应和处理策略，从而减少告警数据量，提升告警数据的有效性。

管理场景1：汇聚告警并且进行事件规则处理和事件丰富

当一个IT系统的监控由多个不同的工具来实现则就一定需要一个集中的事件处理引擎来汇聚这些工具产生的告警事件，至少应该包括：网络、系统、应用的性能和故障告警、日志中发现的告警信息、配置参数发生的改变;更进一步如果在一个虚拟化的环境中，则还需要容量失衡的告警数据以及虚拟化系统的动态改变的报告。

而事件处理规则和事件丰富则给予了处理引擎更为前面处理告警事件，并且过滤非重要的事件;提升重要事件的等级并且基于事件所关联的周边信息，诸如应用的重要等级、是否有引起系统性能超用的业务事件、是否是节假日等来进行是否需要告警的判断。

管理场景2：根据事件规律来预先设定处理预案

大量的事件通常都是有规律的发生，那如何可以更早地了解到这种趋势并且可以为此设定处理预案以在相关事件发生时可以自动进行各种处理操作？从简单的文件分区满了自动归档指定目录文件并且释放空间；到较为复杂的应用交易缓慢则自动重启某些应用进程；或者更为复杂的自动增加计算节点并且将现在的应用处理从2节点扩展3节点等等。

事件的分析结果将作为自动化告警、自动化操作的触发器和推动器，越是完善成熟的事件分析可以实现更为精准的自动化操作。

IBM解决方案：

IBM NetCool Operation Insight继承了NetCool OMNIBus的强大事件收集能力以及NetCool Impact的灵活

分析规则定制和执行能力，并在此基础上对事件进行自动化的历史统计和模式匹配，自动计算根原因和衍生告警，从而可以更为智能地对告警事件进行归类和根源判断。

客户案例：

IBM基于NetCool Operations Insight的强大事件分析能力帮助很多全球性的客户提升了IT运维数据的处理能力，其卓越能力可以帮助客户：

- 将告警事件的分析时间减少75%；
- 被关注的事件重复率减少50%；
- 可以减少30%以上的事件处理操作。

而这一切的一个直接结果就是显著减少事件单创建数量，减少运维人员的工作量。

KPI预测分析

目的：除了告警事件之外，是否也可以从大量的告警KPI中挖掘有价值的信息来提前了解可能潜在发生的问题呢?当机器学习和认知计算逐渐成为业务系统的重要组成基因，那IT数据运维必然也需要引入这些技术来获得与前不同的管理能力–纳入海量KPI并且以此建立起KPI之间的关系模型，从而在相关性被破坏时就关注可能引发的故障，并且了解哪些KPI是导致后续故障的根本起源。

管理场景1：识别单个KPI基于学习基线的异常

对单个KPI学习并建立其性能基线，对于偏离性能基线的情形进行告警。可通过参数的设置忽略单次的背离基线的行为，而仅对连续的背离基线的行为进行告警单KPI指标的基线分析和告警。

管理场景2：多KPI指标的相关性分析

对于被关注的KPI数据，系统会自动的进行学习，并识别各KPI之间是否有关联关系。如果有关联关系，系统会学习其运行数据，识别出这些KPI之间“正常”的行为模式，并持续对其行为进行跟踪。当发现KPI之间的行为与正常的行为模式不一致的时候，进行告警并提供图形化的数据。

IBM解决方案：

IBM Operations Analytics – Predictive Insights是IT数据运维领域的前瞻性产品，即通过机器学习来自动建立KPI模型并且逐步向认知计算发展以有机结合多种不同算法的结果来提升预测判断的准确性。

IBM Operations Analytics – Predictive Insight内嵌了沃森分析法，它从复杂的虚拟和物理基础架构中，学习健康的指标数据之间的关系;它对跨越整个服务的指标之间的数学关系进行学习和模型化，自学习过程不需要复杂的人工干预。通过对指标数据的连续时间区间的行为追踪，确定指标的正常行为基线，一旦学习完毕，IBM Operations Analytics – Predictive Insight会持续追踪指标变化，一旦检测或预测到指标的行为偏差，它将产生异常行为告警。

小结

数据化运维的特征就是运维数据的整合、收敛、规则处理、自动化分析，借用大数据技术、机器学习等新技术更快、更全面、更准确地对运维数据进行分析和挖据，不仅指导问题的处理过程更可以在逐步获得对故障的预测判断，从而变救火为防火。

IBM Corporation
Software Group
Route 100
Somers, NY 10589

2015年10月