

运维管理 寻找真正“主动”之路思科认证 PDF转换可能丢失  
图片或格式，建议阅读原文

[https://www.100test.com/kao\\_ti2020/644/2021\\_2022\\_\\_E8\\_BF\\_90\\_E7\\_BB\\_B4\\_E7\\_AE\\_A1\\_E7\\_c101\\_644201.htm](https://www.100test.com/kao_ti2020/644/2021_2022__E8_BF_90_E7_BB_B4_E7_AE_A1_E7_c101_644201.htm) 尽管IT运维管理的技术在不断进步，但实际上，很多系统工程师并没有真正解脱出来，原因并不复杂：“虽然已经能够获取网络设备、服务器、网络流量，甚至数据库的警告信息，但成千条警告信息堆积在一起更本没法判断问题的根源在哪里？”“虽然不少产品提供了告警过滤和压缩，但结果却并不尽人意”。面对这样的抱怨，难道我们的工程师将永远无法走出“被动的怪圈”吗？如今，在IT运维领域中，“主动”并不是一个新鲜的概念。几乎所有的宣传、产品、用户、理念都在宣扬“主动”，从被动到主动管理的升华是每个企业针对信息系统如何提高IT服务水平、如何提高系统可用性、降低运维成本，实现IT科学性的过程。很多企业在选择IT管理工具时将最终目标就定位在“主动”，希望业务系统能够“无忧”，但真正能够达成IT与业务融合的企业却是很少。很多IT运维厂商都强调，“传统被动式”的类似“救火员”角色的IT系统运维方式，根本不能适应目前需求，那么企业到底怎样才能实现真正的“主动”呢？为何丧失了“主动”的先机？在虚拟化、云计算等新兴技术的刺激下，IT正在走向一种整合的发展趋势。当然，这种整合并不局限于几台服务器的集群或组成1个数据中心，而是更多地指向了有序、有效地集中，但也会导致原有的问题也会集中在一起。中国的IT工程师习惯于将工作重心放在性能而不是质量上，放在提供支持而不是消除问题上。在“传统被动式”的管理中，就有一些技术

工程师将自己查找日志而排除问题的能力拿出来炫耀，但在“业务集中之后”，这种排查日志的技能几乎葬送了自己所有的工作时间。因此对于“问题管理”，在“集中之后”更多的企业不但需要职能的发现业务系统的问题，更是需要联动式解决问题的办法，实现减少问题发生次数的目标。将IT基础架构内由错误引起的事件和问题对业务的负面影响减到最小，并预防这些相关的事件、问题和错误的再度发生，这才是主动管理的精髓。我们知道，对于IT系统真正的主动管理，是实现业务服务管理中最重要基石之一。但有些用户在修正现有的IT管理目标是比较盲目的，因为原先没有一致而且正式的运维程序与原则，因此根本无法拟出服务等级（Service Level Agreement, SLA）。如果没有SLA，实现业务测量运营绩效与确立IT目标几乎是不可能的，也就不可能为主动管理排出精准的规划。早在2003年，业内就提出了BSM业务服务管理这一理念，将“IT与业务融合进行到底”的路线一直延续下来。但在那个时候，很多IT管理工具并没有将业务放在第一位，设计的核心没有用业务指导网络运维，因此从一开始有些人就站在了相反的起跑线上，即使用了最先进的IT运维管理系统，如今还仍然是在做底层获取的工作，虽然拥有了海量庞杂的相关数据，如果得不到提炼，则上层流程的“主动”管理必将成为空谈，业务的保障和管理就会成为无本之木。就如我们共知的那样，IT问题的发生是必然的，但未能根据业务进行基础监控的用户，将丧失在问题造成业务中断之前，就进行防止的契机，也就丧失了“主动”的条件。“主动”怎样落到实处？IT技术正在成为企业的神经中枢，越来越多的企业希望借助IT技术这一关键的战略资

源提供对关键业务的支持，提升公司的竞争优势，进而实现公司的战略目标。然而由于今天的IT组织面临着诸如日益增长的基础设施复杂性、技能方面的限制以及资金短缺等相当多的问题，因此要实现这一点并不容易。就如前面说明的那样，如果在IT系统中没有出现问题，也就没有告警信息，但这是不可能存在的一种假设。当所有的业务系统集中起来的时候，出现无数的警告信息实际上是非常正常的，这就如人生病一样，很多疾病都会造成身体上多处特征的不良反应，医生会开出多得让你厌恶的检查表格让你检查，实际上这就是看病过程中找到病源的过程。但这个过程越长，你就越加无法忍受。企业的业务系统也是如此，在问题出现时，不能将问题迅速归类，不能发现最具特征的表象，也就迟迟无法做出问题改善，“主动”也就失去了意义。很多企业用户都存在疑问，化繁为简应该不能只是空谈，但如何做到实践、也就是说如何用呢？针对这样的问题，在北塔BTIM中提出了对告警事件压缩和智能提取的独有技术，在告警信息管理中，北塔BTIM还包括了单点告警、复合告警、基线告警结合使用的技术优势，告警事件关联抑制功能真正做到了事件根原因分析，从而准确定位事件故障源，如：某业务系统，由于关注参数很多，为减轻工作量，平时只关注ping通是否正常，当ping告警触发时，抑制该业务系统服务器的CPU、MEM告警，以免这些告警信息干扰故障源判断，同时立刻关联该业务系统核心网络设备情况，再关联该业务系统连接网络设备端口情况，最终的结果可以发现，是该端口为关闭状态从而触发了告警，原来有人误操作关闭了该端口，激活该端口则恢复正常。由此可以看到，正是通过告警关联与抑制方式

实现了先进的问题根源定位能力，从而使得主动管理不再是纸上谈兵。脱离每天被繁冗的警告和报表所包围的现状，利用“主动管理”高效而清晰地描述业务系统的运行状况，立即把所有的警告信息繁为简，一目了然。IT部门必须能够提供追踪问题改善状况的评估方式，以便达成持续的改进成果，这才是“主动”的内涵。当你迅速地解决系统故障，端起一杯咖啡时，那温暖的惬意，也许正是IT运维中关于“主动管理”一词最直接、最具说服力的解释。编辑特别推荐: 关于思科认证考试的注意事项 Cisco认证总结CCNA重难点 各个方向CCIE认证投资回报分析 100Test 下载频道开通，各类考试题目直接下载。详细请访问 [www.100test.com](http://www.100test.com)