3 种网络监控故障及如何避免

ipswitch

没有人喜欢运行迟缓的系统。

系统响应缓慢导致长时间等待，这会降低贵组织的生产效率。随着时间流逝，故障无法修复，用户便会失去耐心。

如果是处理反复出现的性能故障，情况会更加糟糕。甚至平时有耐心的用户也会投诉。上级管理层开始不满。您 IT 团队的每位成员都感觉自己成了众矢之的。消极情绪四处蔓延。

没有团队想要失败。但在日益复杂的网络环境中快速找到故障原因，确非易事。遗憾的是，越是希望找到快速修复的方法，越难以得到有所帮助的流程、工具和做法。因而，失败在所难免。

每个 IT 团队都希望具备最佳表现，对发现一些常见故障有所帮助。我们还将参照企业管理协会 (EMA) 近期的研究成果，借助一些全球顶尖绩效团队的实践做法来避免这些故障。

如果此类问题反复出现，结果会更糟糕。

平时有耐心的用户也会跟着怨声不断。上级管理层开始不满。IT 团队的每一个成员都感觉自己成了众矢之的。

故障 #1：在反应模式中耗时过久

所有 IT 团队都会在反应模式中花费一些时间。每个组织都会遇到意外的服务中断。但是，衡量优秀运营团队的标准是响应性能故障与主动解决性能故障的频率。

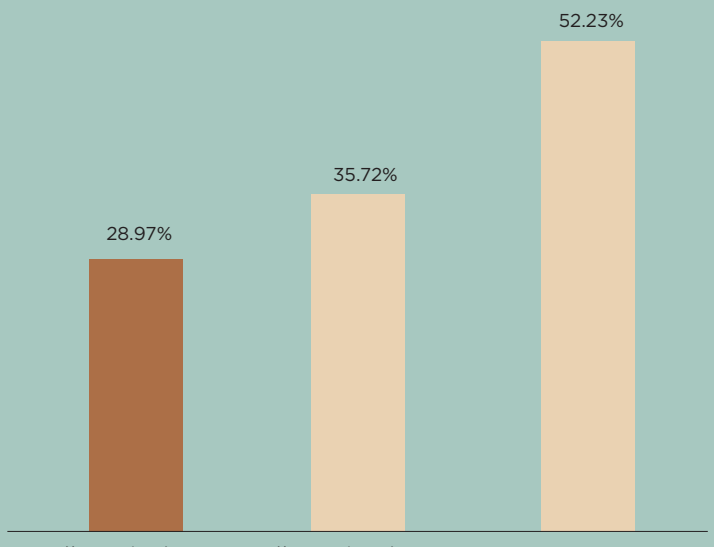
用户报告问题时，您已经在着手制定解决方案，从而在故障解决时抢先一步。如果是在用户投诉时才知道出现故障，用户很可能认为您解决问题耗时过长。

低效 IT 团队因准备不足，会花更多时间应对故障

避免策略

EMA 近期研究测量了用户首先报告服务故障（而不是通过监控）的百分比。尽管似乎有违常理，但研究表明，用户报告故障的百分比与使用的特定筒仓监控工具的数量有直接关联。

低效团队往往使用更多工具监控不同技术（网络及服务器及应用程序）。高效团队则经常依靠更少的工具，因为其中一部分工具可以监控更大范围的技术。



由终端用户首先报告问题的百分比（来自 EMA）

该研究认为，使用较少数量、但技术种类更丰富的工具，可获得优势。端到端可视性和依赖性感知警报有助于及早发现潜在问题。

在用户之前发现问题需要勤奋努力。我们必须设定基于阈值的监控警报，从而通过一种技术对可能导致下游故障的情况提供有意义的预警。

这些警报阈值应以历史性能数据为基础。在这种情况下，可以将这些阈值配置为实现良好平衡，即避免产生过多错误判断，又可准确捕获故障情况。

故障 #2：解决问题耗时过久

如上所说，在复杂网络环境中快速找到故障根源并非易事。遗憾的是，许多 IT 团队为应对故障，使用了一些毫无帮助的流程、工具及措施。依赖大量互不关联的特定技术监控工具便是典型的例子。

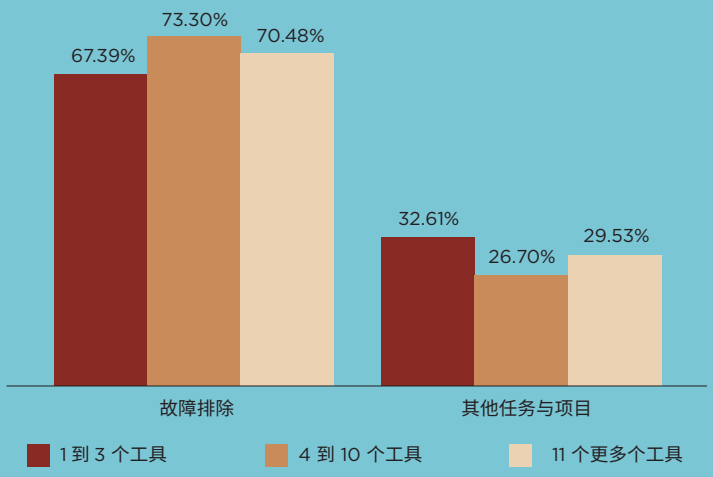
在这些情况下，诊断团队没有从“端对端”的角度审视他们要解决的问题。而这会带来一系列对可能原因的最佳猜测。随着各个诊断方法无法解决问题，时间流逝，用户开始焦急不安。

避免策略

EMA 研究还发现了使用监控工具数量和故障排除耗时之间的关联。正如您所想，在这种情况下，工具并非越多越好。

筒仓工具通常配置为检测责任行业专家 (SME) 认为有问题的地方。这可能与负责端到端服务的相关人员为发现下游问题潜在原因而寻找的状况不同。在一级服务交付栈作为“健康”条件通过的状况可能在更高层级导致灾难结果。

“过多筒仓工具”监控方法通常会大大延长您进行修理的平均时间 (MTTR)，尤其是在更复杂的 IT 环境中。此外，采用一个到三个监控工具的 IT 团队在其他任务和项目上使用近 33% 的工作时间。即，与采用四个或更多工具的团队相比，他们在有意义项目上的工作时间多出 10 -20%。



故障 #3：未能找到并解决根本原因

问题越复杂，越是难以快速找到问题原因。一些问题，尤其是牵扯中间软件、应用程序及数据库之间相关依赖的问题，更是难以解决。如果诊断团队在查找问题的实际原因中遇到困难，会越发急于快速解决问题。通常快速重启服务器可解决性能故障。服务恢复，皆大欢喜，对不对？

实际上，高效 IT 团队意识到这种方法可能会带来久拖不决的问题，之后会反复出现，使其困扰不堪。通过重启解决的服务故障越多，为解决重复故障耗费时间的百分比越大。

避免策略

您很难找到每个问题的根源。但是，高效 IT 团队却能找到更多，从而减少‘僵尸’问题。但是，较少的工具到底是如何提高故障根源检出率呢？

奥秘就在于，这些团队使用监控多项技术的工具，从而获得更多端对端环境监控视角。据企业管理协会 (EMA) 所说，“虽然离散网络管理工具通常无法揭示这些工具和其他工具收集的量度数据之间的相互依赖性，但多功能管理系统可揭示这些相互关联，并且可将这些关联以自定义仪表板、报告到依赖感知警报等各种形式提供给网络运行使用。

使用一个工具提供综合性端对端环境监控视角，可获得多重功效。在用户报告问题之前，您就可以收到相关警报，加快解决问题的速度。将这两种收益相结合，让您赢得更多时间，在客户有挫败情绪之前，轻松找到问题根源。由此，高效率团队可以找到更多问题根源，减少‘僵尸’问题。

使用 WhatsUp® Gold 避免 3 种网络监控故障

WhatsUp® Gold 是数以万计 IT 专业人士最喜欢的网络监控工具。它允许您在 Windows、LAMP 和 Java 环境下，监控网络、服务器、虚拟机、应用程序、传输流量和配置的任何组合。更重要的是，可以利用灵活、实惠的许可证来完成所有操作，该许可证允许您随意混合和匹配您正在监控的内容。不需要购买应用程序、网络设备或网络流量来源的单个许可证——它们均包含在内。

使用强大和易于使用的架构图、仪表板和警报积极地监控网络、流量、物理服务器、VM和应用程序。独特的交互式架构图能快速显示端对端网络、基础设施和虚拟健康度，提供所有连接设备的背景资料，及其如何动态回应交流，为您提供最快解答。

WhatsUp Gold 让您直接从交互式架构图或工作区启动管理任务，简化了工作流程。在物理、虚拟、无线和依赖项视图之间轻松转换，加速根本原因分析。工作流程经过优化且很直观，可从网络架构图启动，或从易于自定义的仪表板和启动。结果是能更简单、更直观地排除故障，让您比以往更快找出并解决问题。

关于 Ipswitch

目前 4.2 万家公司的 100 多万用户在 116 个国家管理超过 15 万个网络，Ipswitch 设计并开发了行业领先的软件，可在云、虚拟环境及本地环境中轻松实现全天候(24/7) 高性能安全交付运行。全球 IT 团队可依靠 Ipswitch 25 年的创新历史，使用 Ipswitch MOVEit® 安全文件传输、Ipswitch WhatsUp® Gold 网络监控及 Ipswitch WS_FTP® 等服务，从而优化并保护商务交易、应用程序及基础设施。Ipswitch 丰富的产品组合可直接获取，或通过与领先 IT 供应商及公司快速拓展的全球合作伙伴体系建立战略联盟，我们的产品组合可提高应用程序及网络性能，监控各种 IT 环境，并确保安全数据交换符合 PCI、HIPAA、GDPR 及其他行业及政府数据安全及管理要求。

公司在美国、欧洲、亚洲及拉丁美洲均设有办事处。要了解更多信息，请访问 https://tw.ipswitch.com/ 或关注公司 LinkedIn 及 Twitter。要了解 Ipswitch 战略联盟或全球合作伙伴网络，请访问 https://tw.ipswitch.com/partners。

ipswitch

了解如何轻松避免这 3 种网络监控故障。

下载 30 天免费试用版
Ipswitch WhatsUp® Gold ›