IBM 软件
思想领袖白皮书

2011 年 10 月

打破网络不合规性的周期

满足整个合规性领域需求的最佳实践方法

IBM

简介

合规性不是一项单一的需求。它内涵丰富。

一方面，您拥有支付卡行业数据安全标准 (PCI DSS) 等业务需求和 Sarbanes-Oxley Act (SOX) 等政府制度。这些方面的不合规性可能导致罚款、丢失业务特权或者甚至导致刑事诉讼。

另一方面，您拥有组织的内部策略以及客户和业务合作伙伴的性能预期。这些方面的不合规性可能导致损坏网络，从而导致延迟、混乱和损失收入。违背服务水平协议 (SLA) 可能导致罚金。流失不满意的客户。

对于许多组织，任何方面的不合规性都是一个难以打破的周期。由于 IT 部门承担着重大日常任务负担（响应故障单以及维护和扩展服务），合规工作常常仅专注它们必须立即满足的标准。但是，最有效的合规性措施超越了有限的目标。一种能够控制从分配网络资源到更改设备配置，再到确保网络安全等的一切事务的方法，能够支持合规性，从而可以打破不合规性的周期。

本白皮书提供了一种最佳实践方法来满足所有合规性需求。该方法建立了治理 IT 操作的策略和过程，然后自动应用这些策略。它报告与合规性相关的区域（比如性能和安全性）的网络状态。而且，如果有必要，它将修复问题，将网络恢复到合规性状态。它允许量化并监控网络的策略合规程度以获取趋势信息。它是一种完整的方法，可确保组织不仅通过遵守法规标准且可通过加强网络基础设施的端到端操作来获得利益。

无论是在内部还是外部，关键在于合规性

当考虑合规性时，安全性通常是首要考虑因素。一家未能依据健康保险携带性与责任法案 (HIPAA) 保护患者信息的医院可能会遭受严重的处罚。从高端零售商处盗窃信用卡信息的计算机攻击可能导致客户流失。最令人不安的是服务水平协议。服务提供商数据中心内的一个系统故障可能中断网站（或托管应用）以及以 Internet 作为生命线的数千家公司的通信。

与此同时，几乎无法察觉其他合规性问题——可能影响组织的操作、声誉和盈利能力的问题。当客户购买 10 MB 带宽来访问 Internet 服务，但网络却错误地使用 100 MB 的带宽来进行访问时，提供商将损失收入并消耗不必要的资源。当银行的客户关系管理软件性能降低时，客户满意度和交易量都会下降。

一家为重要功能设置默认配置（包括由设备供应商预设的密码，虽然提供了方便，但不安全）的公司会面临违反 PCI 合规性的风险。例如，一家公司错误地配置了网络速度和网络双工参数，那么这家公司的性能在网络流量高峰期间会很糟糕。如果错误地设置了一个基于 IP 的网络，则可能导致低劣的语音质量和错过呼叫服务。而且由于错误配置复杂的路由协议（比如 BGP，BGP 是在远不及当今的 Internet 发展范围和任务关键性时进行设计），已导致在重要时期无法访问主要的企业网站。

这些是所有的不合规问题——甚至在它们没有违背外部制度时，它们也会违背公认的标准和最佳实践。但这些广泛的问题也有一些共性。每个问题都可能源自设备的简单错误配置，这可能导致严重的网络漏洞、中断和性能问题，将较小的错误转变为大型的故障。

复杂性和错误： 不合规性的根源

如今的企业网络非常复杂，以至于手动流程和临时解决方案无法满足合规性需求。但大部分组织都未实现全面、自动化的合规性管理方法。它们无法恰当地监控和实施策略，这些策略使它们的网络能够满足行业、政府或最佳实践标准。

随之而来的管理缺陷可能导致这些组织容易受到监管机构的财务处罚、外部黑客的攻击和内部员工的错误带来的影响。在普通安装/移动/添加/更改过程中（包括出于好心而进行的授权更改）发生的简单错误可能威胁网络的完整性以及甚至导致中断操作。

当考虑到不断增长的设备数量、种类和复杂性——以及更快的变更频率时，不合规性导致的问题就应该不足为奇了。设备比以往任何时候都变得更加异构化和更加全球分散化。可能有数百个系统参数、数十个操作系统。而且配置手册已经跟字典差不多厚。网络工程师如何使用手动方式处理这种复杂性？

正是 IT 部门通常执行的繁重工作负载导致挑战变得越来越严峻。当不频繁发生系统故障或其他紧急问题时，员工仍然可以尽力处理每天的操作。 管理可能多年前就已成为基础设施一部分的设备，可能意味着如果员工希望避免发生错误，则要发现需要额外关注和时间的未归档配置。这将导致难以处理可能推迟任何与合规性相关的工作配置，这些工作与迫在眉睫的审计或或失败的审计没有直接联系。

网络层的合规性措施

甚至当问题不关乎失败的审计、黑客的漏洞或更低的系统性能时，与行业标准和最佳实践的一致性也可以帮助组织获得更出色的可控性、更高的可预测性以及来自其网络基础设施的更高价值。毕竟，技术代表着一项重大投资，组织希望使用它实现最优的能力和发挥最佳的业务优势。非充分利用和过度利用资源都可能降低组织的盈利能力，这就像路由器配置中的错误一定会降低安全性一样。

但是，可以预防或减轻影响企业安全性、服务交付或底线收入的事件。只需要一个可监控和约束网络配置以满足合规性需求的系统。事实上，合规性应该是管理网络设备的所有流程的关键驱动因素之一。必须创建并持续监控策略。错误的更改必须得以预防。 在违规时，必须迅速发布警报并完成修复工作。无论是自动接触还是手动接触网络设备，组织应该审计对网络设备的每次接触，并应该收集策略合规性数据作为促进改进的一种机制。

对许多组织而言，他们可能很熟悉监视和控制流程。最终用户级别上的远程和自动化设备更改管理的战略变得越来越普遍。它们可以提供重点保护免受恶意软件的威胁，减少 IT 工作负载，确保端点配置符合标准策略，以及加速跨数千个设备的修补和修复措施。

无论问题是遵守监管机构的指令还是遵守组织内部的标准，在网络层解决设备配置的问题都可能提供相似的收益。

需要一种全面的预先方法

企业网络时常发生变更。 但由于变更是不合规性的最大驱动因素，所以控制变更同样也具有深远意义。至少，组织需要一种方式来回顾变更，以发现谁在何时采取了什么措施，评估影响，并在适当时回滚变更和更正错误。

但是，更好的方法是采用一种抢先的解决方案，持续监控变更以限制发生人为错误和减少不合规性的可能性。抢先的合规性功能旨在帮助客户根据为一个设备预定义的合规性策略来评估配置更改的影响。因此，可以在将任何更改发送到网络之前，作为常规配置更改流程组成部分的代价不菲的合规性违规得以提前避免。一种自动化的配置管理解决方案可消除对手动流程的需要，减轻 IT 工作负担，以便合规性管理可获得首要的优先级并获得它应得的关注。自动化可使合规性成为一种持续流程，可减少发生招致制度惩罚的安全性漏洞、终止业务的系统故障或损害利润和生产力的低下性能的可能性。

在一个大型且复杂的网络中，自动化、抢先的流程可提供手动方式所无法实现的细粒度控制水平。IT 管理员可根据预定义的合规策略提前评估配置变更的影响，验证合规性，以及在变更发送到网络之前确保其准确性。如果确实出现不合规性，抢先方法还会在变更之前识别存在的任何违规，
警告 IT 更正错误的需要。

快速发展过程中的合规性

Cbeyond（一家向全美国的小型企业，IT 和通信服务的提供商）面临着实现增长目标的挑战。不断增长的网络复杂性、严格的合规性指令、较短的
维护时限和预算压力为其 IT 操作带来了越来越大的压力。

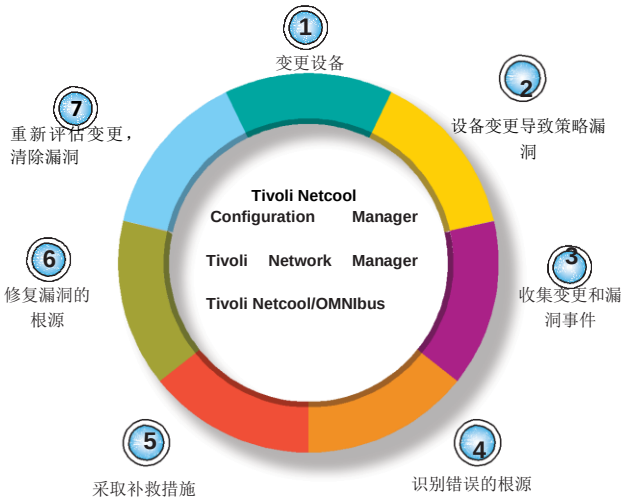
实施一个 IBM 解决方案使 Cbeyond 能够：

- 自动化配置更改并为语音和数据服务的“零接触配备”实施工程标准和策略
- 进行扩展以发现和管理数千个网络设备
- 在每次必须向网络中添加一个新设备或每次更改操作、制度或安全策略时，消除网络管理人员编写配置脚本的需要
- 自动验证设备配置并解决不合规条件
- 空出工程师和管理人员的时间，以便将其精力放在其他方面。

通过持续监控确保合规性

有效的配置管理系统将通过扫描网络，收集设备配置和依据标准模板或网络管理员定义的规则来分析配置，并借助定义策略和验证配置的流程确保持续的合规性。如果解决方案发现某个策略已被违反，它将发出
警报并智能地修复不合规性条件。

IBM Tivoli Netcool 产品套件整合



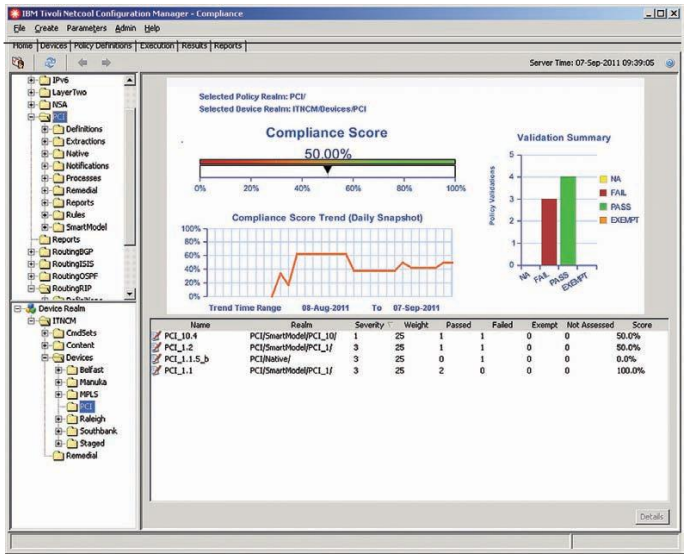
IBM 变更和合规性管理解决方案与事件和网络管理解决方案进行集成，使 IT 人员能够解决反复发生的网络问题，显著减少需要采取手动更正措施的事件数量。

持续监控问题（许多组织常常将其实施为一种迭代流程，从管理最常见的问题开始，稍后添加其他策略）可能涵盖对所有需求的合规性，从政府或行业机构建立的安全标准，到服务水平协议定义的业务需求，再到内部需求，比如补丁管理或在安装设备之前更改默认密码。配置管理可以通过以下流程提供策略监控：

- **网络发现：**查找并识别硬件组件和固件细节，以及设备配置和拓扑关系。 精确的网络图是 PCI DSS 等制度标准的一项需求。
- **漏洞和配置评估：**评估每种网略设备以便遵守应用到一组用来执行特定角色的设备的策略合规性。应该量化并监控合规性以便获取其趋势信息。
- **修复和加固：**实现可从开箱即用、通用的标准开始，稍后可依据每种网络的拓扑结构、网络技术和管理战略进行扩展。以便满足这些独特的网络需求的策略。
- **变更审计：**检测不合规性，发出警报并提出修复操作。在错误配置中，应该自动化回滚。对比配置的能力拥有无穷的潜力，必须记录系统变更。
- **问题预防：**以标准方式通过模块化和参数化的命令脚本提供功能。
  要自动化数据收集，应该集成配置、变更、事件以及网络管理的分析和报告。
- **审计：**记录对设备进行的每次访问，其中不仅包括脚本化和自动化的访问，还包括完整的键击日志。必须捕获谁进行了何种更改，更改的原因和关联的票证编号。必须检测带外更改。
- **身份验证、访问控制和授权管理：** 细粒度地控制查看或编辑设备配置、查看报告、创建命令模板或编辑和应用策略的能力。所有操作都必须可供用户跟踪。

自动化的 IBM 解决方案减少了错误和漏洞

如今，IBM® Tivoli® Netcool® Configuration Manager 为网络管理员提供了他们在大型、复杂、不断变化的网络中管理配置和合规性所需的工具。 Tivoli Netcool Configuration Manager 旨在帮助保护网络免受外部攻击，预防不合规性罚金所导致的收入损失，以及同时满足内部和外部服务水平协议，Tivoli Netcool Configuration Manager 可从数百个设备扩展到成千上万个设备，以控制网络配置的所有方面。



IBM Tivoli Netcool Configuration Manager 图形化地显示趋势、摘要和评分，展示网络设备的合规性水平。

一个涵盖手动和自动化设备变更、全面的用户安全性和审计历史的完善的功能集合，可衡量对预设标准的合规性，主动监控网络，从而使所需的标准得以维护，以及在必要时提供回滚和修复。

通过支持标准化流程，Tivoli Netcool Configuration Manager 的自动化功能可显著减少发生人为错误的机会。命令集是可重用的模板，可自动化常规任务，比如跨数百或数千个网络设备变更 SNMP 社区字符串。可采用参数来表示每个命令集，从而化简化操作——用户仅需知道关键参数，而不是完整的命令语法。而且可以创建经常采用模板的库，以便增强支持操作。

Tivoli Netcool Configuration Manager 的一项称为 SmartModels® 的功能，进一步增强了管理，借助一个带有用户友好的编辑器的设备配置，拦截非法的命令以预防将它们发送到设备上，无需重新启动即可将不合规的设备返回已知的正确状态，而且无需实际更改网络即可模拟网络更改，使管理员能够提前解决与更改相关的问题。

结束语

合规性范围—从行业或政府机构建立的外部制度到针对组织独特的操作需要创建的内部策略——需要多种功能。组织必须建立策略来治理 IT 操作，自动化这些规则的应用，报告与合规性相关的区域的网络状态，修复问题以将网络恢复到合规状态。

Tivoli Netcool Configuration Manager 提供了一个强大的解决方案，因为它可以涵盖丰富的网络设备，所以它可以快速减少操作成本。它的单一平台方法提供了对策略创建、部署和管理的细粒度控制，以便验证法规、安全、操作和其他合规性需求。

更多信息

如需进一步了解 IBM Tivoli Netcool Configuration Manager 的更多信息，请联系您的 IBM 代表或 IBM 业务合作伙伴，或者访问 **ibm.com**/software/tivoli/products/netcool-configuration-manager

关于 IBM Tivoli 软件

IBM 的 Tivoli 软件可帮助组织有效地管理信息技术 (IT) 资源、任务和流程，以满足不断变化的业务要求，提供灵活且响应能力强的 IT 服务管理，同时降低成本。Tivoli 产品组合囊括安全性、遵从性、存储、性能、可用性、配置、运营和 IT 生命周期管理软件，并且以一流的 IBM 服务、支持和研究团队作为坚强后盾

。

此外，IBM Global Financing 可帮助您以最经济高效和战略性的方式获得您的业务所需的 IT 解决方案。我们将与信用合格的客户展开合作，定制一个 IT 财务解决方案来满足您的业务目标，实现有效的现金管理，以及改善您的总体拥有成本。IBM Global Financing 是您投资关键 IT 投资和向前推进您业务的最智慧选择。有关更多信息，请访问：**ibm.com**/financing

© 版权所有 IBM Corporation 2011

IBM Corporation Software Group
Route 100
Somers，NY 10589
U.S.A.

在美国印制
2011 年 10 月
保留所有权利

IBM、IBM 徽标、ibm.com 和 Tivoli 是国际商业机器公司在的商标。如果这些和其他 IBM 商标在本文中第一次出现时标记了商标符号（® 或 ™），均代表在本文出版之际，它们是 IBM 在美国或其他国家注册的商标或普通法规定的商标。此类商标在其他国家/地区也可能是注册商标或普通法规定的商标。有关 IBM 商标的最新列表，请访问 ibm.com/legal/copytrade.shtml 的 “Copyright and trademark information” 部分。Smartmodels® 是 IBM 公司 Intelliden, Inc. 的注册商标。

其他公司、产品或服务名称可能是其他公司的商标或服务标志。

本文中提到 IBM 产品和服务并不表示它们在所有 IBM 运营的国家或地区都提供。

截止初始发布之日，产品数据已进行准确性审校。产品数据随时可能变更，恕不另行通知。

本文档中的信息按 “原样” 提供，不承担任何隐含或明确的担保。 IBM 对特定用途的适用性或不侵权性不做任何保证。 IBM产品的担保依据是其遵循的协议（比如 《IBM 客户协议》、《有限保证声明》、《国际程序许可协议》）中的条款和条件。

客户负责确保遵守法律要求。客户自行负责获得有法定资格的律师对任何相关法律和法规要求的认定和解释的意见，该意见可能会影响客户的业务和客户为了遵守此类法律所需要采取的任何行动。IBM 不提供法律意见、声明或保证，其服务或产品将确保客户遵守所有法律。

请回收利用

TIW14112-USEN-00