白皮书

通过开放式思科 NX-OS 获得网络可编程性和自动化

当今的组织都需要更快地部署应用，利用敏捷软件，并改善现有流程以支持软件升级。他们需要使用网络团队、服务器团队和软件团队均可以协同使用的常用工具更加高效地管理和运营网络。在不断变化是一种常态的环境中，组织需要部署以用户为中心的高质量应用，以迅速获得业务价值。要实现这些目标，必须对数据中心采取新的方法。此方法需要填补开发和运营团队之间的空白，使开发人员能够将代码快速推送到基础设施，而不会对网络的总体行为造成负面影响。

要了解改变运营需要采取的方式，请考虑当今设置和调配网络的方式。大多数组织将大部分时间用于尝试通过对网络进行调试和测试来确保网络正常工作。此外，他们使用繁琐、分散且容易出错的手动任务来调配和更改网络以满足应用需求。他们还使用手动流程识别网络问题的潜在来源并执行重复任务，耗费网络工程师的大量时间。

为了改善数据中心运营并更好地满足业务需求，企业需要实现流程自动化和进行整体架构调配。要实现这些目标，需要由 IT 团队进行文化变革。组织需要更好、更开放的库和接口，采用常用的 DevOps 工具使脚本自动化并提供更高级别的编程控制。他们需要代理和分布式流程收集和处理有关网络及其组件的状态的信息。

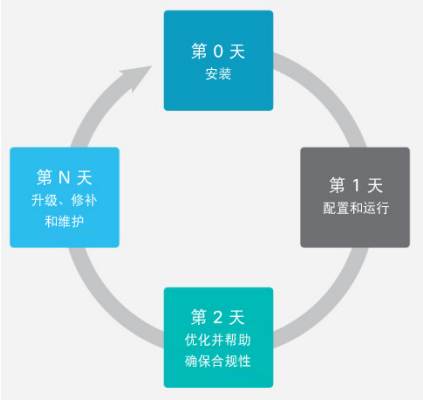
本文档探讨了一个高度可编程的网络如何实现完整网络生命周期的自动化，从而支持敏捷开发和提升运营效率。此外，本文档分析了利用可编程且开放式的 Cisco® NX-OS 软件操作系统的强大能力的多个使用案例。

- 扩展接口（NX-API 命令行界面 (CLI)、NX-API 具象状态传输 [REST] 和 Broadcom Shell 访问）
- 基于 Linux 的本地管理
- 开源工具（Ignite、预启动执行环境 [PXE] 和通电自动调配 [POAP]）
- 访客或本地 Shell 中的 Linux 容器 (LXC) 和 Red-Hat Package Manager (RPM)
- 脚本语言（例如 Python、Ruby）和数据表示法（JavaScript 对象表示法 [JSON] 和 XML）
- 配置管理和协调工具（Puppet、Chef、Ansible、OpenStack 插件和（Cisco UCS® Director）

使用案例

本文档探讨的使用案例反映了第 0 天、第 1 天和第 2 运营（图 1）以及网络 IT 团队每天开展的运营活动，例如网络故障排除、配置备份、扩展和协调。

图 1. 网络生命周期运营



第 0 天运营：安装新交换机

挑战：第 0 天的重点是尽快提出和发现在网络的生命周期内特性和功能不会有许多变化的新设备：设备名称、管理员用户名和密码、管理 IP 地址、控制台访问权限、带外管理和界面等。在典型的环境中，启动过程是手动的，可能需要数小时甚至数天。挑战：如何将此过程缩短至数分钟？

解决方法：使用开源的 Ignite 工具，以使用 POAP（升级软件映像并在 Cisco Nexus® 交换机上安装配置文件）和 PXE 促进初始的网络引导。可以在数分钟内自动发现并安装 Cisco Nexus 交换机，从而消除人为错误。Ignite 还使管理员能够定义配置模板、交换矩阵拓扑和资源池。

此外，在交换机启动期间，POAP 和 PXE 可以安装配置管理工具（如 Puppet 和 Chef）的代理。

第 1 天运营：配置和运行交换机

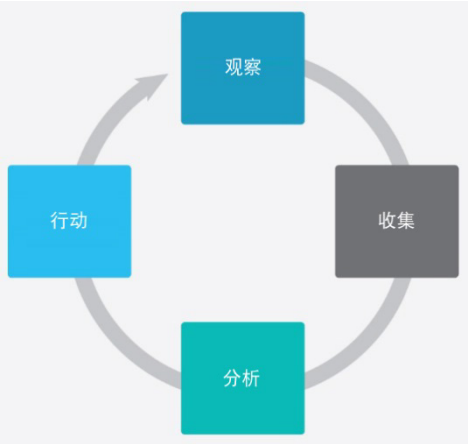
挑战：组织必须能够迅速在数据中心实施更改，以便快速添加和移除虚拟机以及创建和设置 VLAN、服务质量 (QoS) 策略、虚拟路由和转发 (VRF) 实例、虚拟端口通道 (vPC) 等。他们还必须建立虚拟机与设备之间的连接。对于帮助企业避免错误、安全漏洞和停机时间而言，快速做出更改和摆脱逐个设备进行手动配置的能力至关重要。

其他可能的任务包括配置边界网关协议 (BGP)、验证 NX-OS BGP 软件的特定版本在交换机上以一种简化的方式运行，以及通过设置访问控制列表 (ACL) 快速做出响应以遏制对网络的某些攻击。IT 面临的挑战是在整个网络中快速执行所有这些操作。

解决方法：Cisco Nexus 交换机支持配置管理工具，例如基于代理的 Puppet 和 Chef 以及无代理的 Ansible。这些工具使组织能够通过构建一致且可重复的流程执行图 2 所示的任务，以实施和验证更改，以及处理基础设施中发生的异常和违规。通过创建交换机可以定期使用的一个集中式配置存储库，这些工具使 IT 只需稍加努力就能够高效且一致地管理基础设施。有关详细信息，请参阅 GitHub。

IT 管理员还可以在 NX-OS（对象模型）中使用 NX-API REST 功能配置和检查对象的状态。对象可以是交换机上的物理端口或特定功能，如 BGP、VRF 实例和 VLAN。使用对象模型可实现配置的分层和标准化表示，无需传递 CLI 命令和脚本。

图 2. 配置和运行交换机

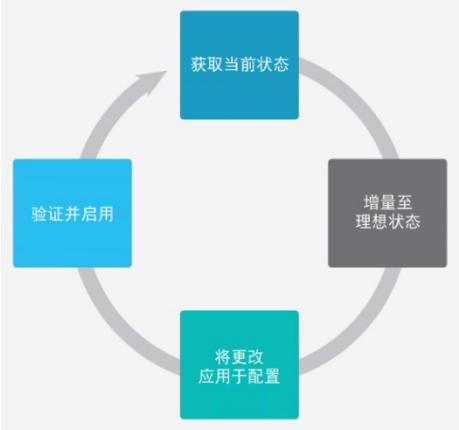


第 2 天运营：优化网络并帮助确保合规性

挑战：关于在网络中进行更改的持续请求通常需要花时间进行规划和实施。这些请求包括更新交换机映像、修补软件以及创建安全策略以支持应用需求，并且通常是手动执行的。手动流程往往导致部署延迟和增加发生错误的可能性，可能会导致安全漏洞和低效的运营模式。此外，优化交换机行为以支持应用需求可能非常繁琐，而且在不中断网络的情况下安全而简单地持续添加功能升级可能很复杂。

解决方法：如图 3 所示，网络管理员可以在中央存储库定义需要更改和更新的内容，以及哪些交换机和端口将受到影响。使用配置管理工具（例如 Puppet）可实现将应用快速集成到客户的运营工具链并从中央存储库触发配置。借助此流程，大型的交换机部署可在几分钟内完成更新。此功能以对计算节点使用的相同方式执行。

图 3. 优化网络并帮助确保合规性



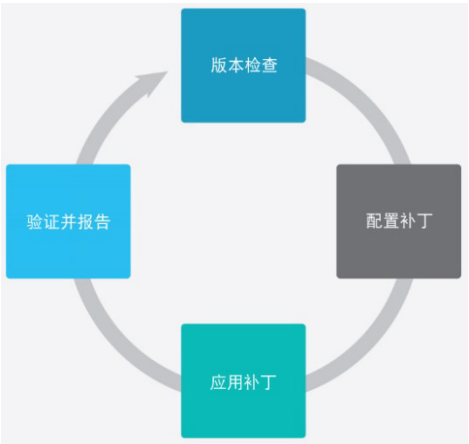
第 N 天运营：软件升级、修补和维护

挑战：大多数组织无法承担使设备离线一段时间以更新软件所带来的损失。为了避免中断，他们在非高峰时段实施更新，导致环境的工作效率较低。

解决方法：此使用案例的核心是开放式 NX-OS 的可扩展性，它将标准的软件包管理工具（例如 RPM 和 YUM）用于软件管理。相同的工具可以用于开放式 NX-OS 流程修补，以及用于在交换机上安装外部或定制开发的程序。组织可以安装本地 RPM 和第三方应用，像在 Linux 服务器上运行流程。基于 RPM 的软件包使组织能够仅加载所需的服务和软件包，并且他们可以使用 RPM 执行修补，而不是实施整体升级（图 4）。

以下功能缩短了维护窗口并使组织无需将整个交换机关闭就可以更新特定的模块：在内核中根据需要加载和卸载模块，隔离功能、服务和用户应用中的故障，以及执行流程的平稳重新启动和删除。

图 4. 软件升级、修补和维护

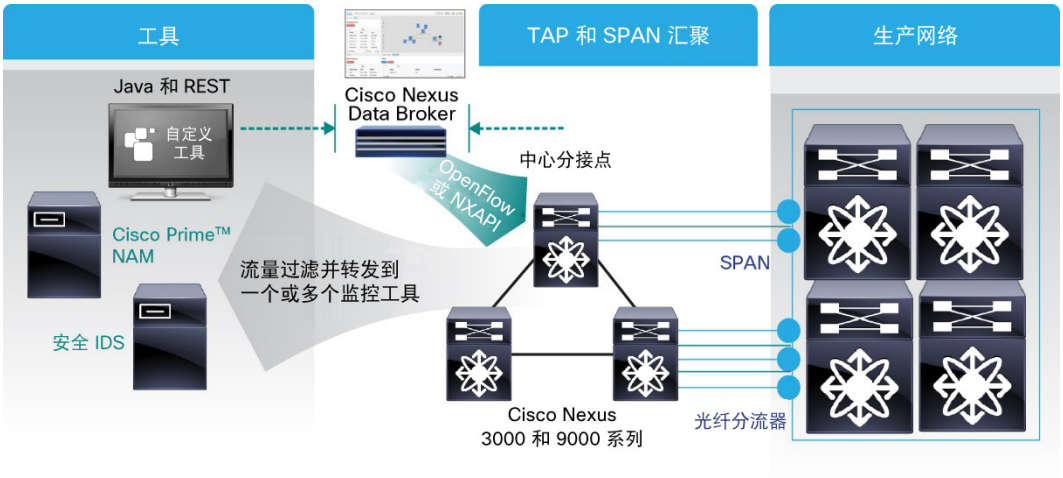


可视性、监控和故障排除

挑战：对于许多组织而言，诊断和查找问题的来源可能是一个困难而漫长的过程。逐个设备进行的监控、维护和分析可能过于繁琐，尤其是在大型网络中，组织通常依赖网络测试接入点 (TAP) 收集数据。通过 TAP 以及通过思科交换端口分析器 (SPAN) 和远程 SPAN (RSPAN) 收集的生产流量对 IT 极具价值，而以可管理的方式访问更多数据可以帮助确定交换机内部发生的情况。

解决方法：Cisco Nexus 3000 和 9000 系列交换机支持的 Cisco Nexus Data Broker 取代传统的定制矩阵交换，允许您构建一个您可以在 1、10、40 和 100 GPS 互联的可扩展 TAP 和 SPAN 汇聚基础设施。您可以将端口用于 TAP 和 SPAN 以及传统的以太网连接。IT 可以通过基于 Web 的 GUI 或 REST API 访问数据代理应用。数据代理为需要监控大量业务关键型流量的企业客户提供简单、可扩展且具成本效益的解决方案（图 5）。

图 5. 可视性、监控和故障排除



此外，使用 Linux Bash 完全访问 ioctl 和 netdevice 接口库使客户可以安装工具，例如 tcpdump。这些工具通过分接到端口和 VLAN 并将输出发送到收集器端口，提供额外的设备可视性和性能信息。采用此方法，组织不需要在每个设备上放置物理分流器。

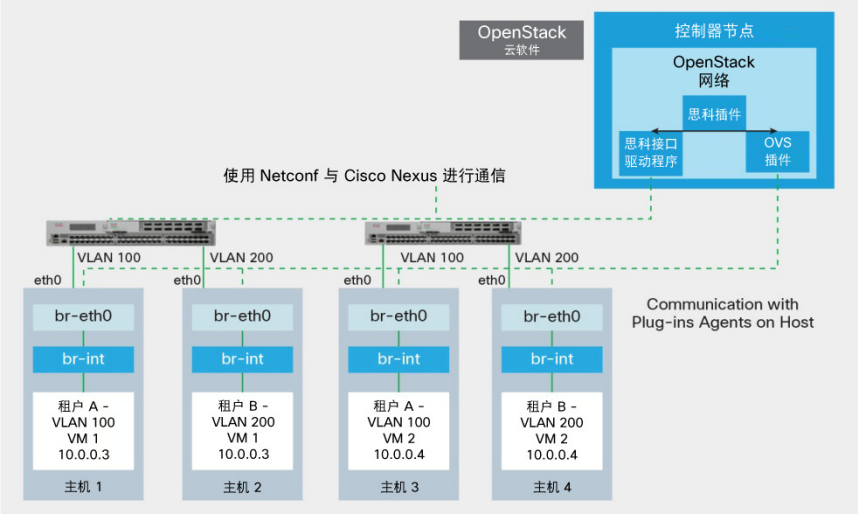
使用 RPM 功能，可以将第三方监控应用（例如 Splunk 转发器、Tcollector 或 ganglia）安装在安全容器中，并提供进一步的可视化和分析。

可扩展性、自动化和协调

挑战：客户努力从开源工具自动化和协调数据中心资源，以优化运营和降低成本。在当今的环境中，这些功能因缺乏与网络设备集成而受到限制。此外，客户必须构建一个高效的架构，以便可以帮助他们轻松快速地扩展以匹配自动化和协调需求。

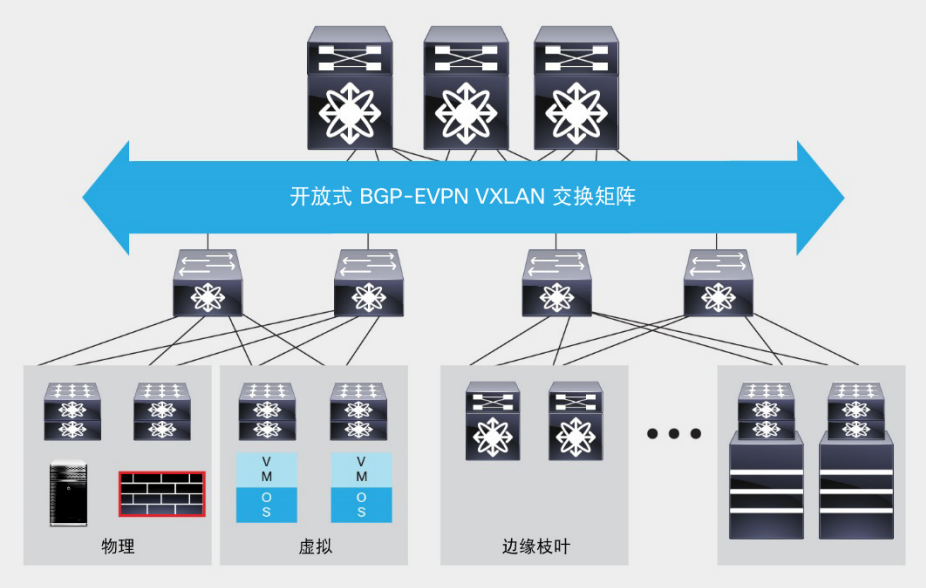
解决方法：使用 Cisco Nexus 的 OpenStack ML2 网络插件而不是 CLI，客户可以从单个位置创建和协调网络资源。客户还可以选择将 Cisco UCS Director 用于协调。使用 OpenStack 或 Cisco UCS Director 的能力使客户可以从单个位置协调网络、计算和存储资源（图 6）。

图 6. 可扩展性、自动化和协调



使用基于标准的 BGP 和以太网 VPN (EVPN) 的下一代虚拟可扩展局域网 (VXLAN) 交换矩阵可以克服“泛洪和学习”流程的扩展和工作负载移动性局限。客户可以构建可编程的软件定义网络 (SDN) 重叠网络，以云规模提供多租户和透明主机移动性。此外，随着 Puppet 和 Chef 代理以及无代理的 Ansible 集成到 Cisco Nexus 交换机，您可以毫不费力地实施 VXLAN 调配和自动化（图 7）。

图 7. 开放式 VXLAN 交换矩阵



结论

采用 Cisco Nexus 交换机的开放系统方法，IT 可以更快地调配网络，缩短故障后的恢复时间，并在环境中获得服务器管理员熟悉的灵活性（图 8）。

图 8. 开放式思科 NX-OS 基础设施

相关详细信息

- 思科 DevNet 社区
- 有关 NX-OS 的详细信息和使用案例
- 开源存储库：GitHub

美洲总部
Cisco Systems, Inc.
加州圣何西

亚太地区总部
Cisco Systems (USA) Pte.Ltd.
新加坡

欧洲总部
Cisco Systems International BV
荷兰阿姆斯特丹

思科在全球设有 200 多个办事处。 地址、电话号码和传真号码均列在思科网站 **www.cisco.com/go/offices** 中。

美国印刷 C11-736824-00 03/16